

Agenda

Reliability and Security Technical Committee

December 7, 2022 | 11:00 a.m.–4:30 p.m. Eastern

Virtual Meeting

ATTENDEE WebEx Link: [Join Meeting](#)

Agenda

Introductions and Chair's Remarks

1. NERC Distributed Energy Resources (DER) Strategy* – Information – JP Skeath, NERC Staff

NERC has proactively been working with industry stakeholders to identify bulk power system (BPS) reliability risks associated with the increasing DER levels and has developed a DER strategy to identify the current and future strategic actions necessary to ensure reliable operation of the BPS. This is an informational presentation of NERC's DER strategy and will cover the strategy's core tenets in detail.

2. White Paper: Battery Energy Storage and Multiple types of DER Modeling* – Approve- Shayan Rizvi, SPIDERWG Chair | Wayne Guttormson, Sponsor

The NERC SPIDERWG investigated the potential modeling challenges associated with new technology types being rapidly integrated into the distribution system. The SPIDERWG weighed updating or altering the recommended modeling framework and found that previous modeling guidance held in the face of two or more dominant technology types of DER at a T-D Interface. Further, the SPIDERWG determined that control mechanisms rather than “fuel sources” is more appropriate for transient dynamic parameterization and the study assumptions to characterize the “fuel source” rather than developing two or more sets of models. SPIDERWG also provided a set of sanity checks for TPs or PCs to use two or more aggregate dynamic models to capture the totality of DER behind a T-D interface.

This white paper shares industry experience with DER BESSs and other forms of distributed energy storage modeling to highlight industry best practices, discuss lessons learned from studies performed with DER BESSs, and highlight model application and parameterization within industry software and tools. The white paper also provides potential modeling practices to parameterize differing technology types under the SPIDERWG recommended modeling framework. The SPIDERWG received RSTC comments and made conforming revisions to the white paper. The SPIDERWG is requesting RSTC approval.

3. Reliability Guideline: Parameterization of the DER_A Model for Aggregate DER* – Approve - Shayan Rizvi, SPIDERWG Chair | Wayne Guttormson, Sponsor

This guideline provides background material on the recommended DER modeling framework, including the concepts of retail-scale DERs (R-DERs) and utility-scale DERs (U-DERs), information on relevant interconnection standards (IEEE Std. 1547-2003, IEEE Std. 1547a-2014, IEEE Std. 1547-2018, and CA Rule 21), and how the DER_A model parameters can be modified to account for a

mixture of vintages of inverter-interfaced DER. The block diagram of the DER_A model is annotated and described so that Transmission Planners (TPs) and Planning Coordinators (PCs) are able to understand the relevant control logic of the dynamic model with respect to the various rules. TPs and PCs are also provided a set of recommendations for developing the modeling parameters for the DER_A dynamic model. These recommendations can also be extrapolated to Transmission Operators (TOPs), Reliability Coordinators (RCs), and other entities performing positive sequence stability simulations of the BPS where an aggregate representation of DERs is required.

The recommendations developed in this guideline are based on extensive testing of the DER_A dynamic model in the Western Electricity Coordinating Council (WECC) Modeling and Validation Work Group (MVWG) as well as industry expertise and studies discussed in detail in the NERC System Planning Impacts of DER Working Group (SPIDERWG) modeling subgroup. This guideline also serves as a useful reference for building DER models and selecting representative DER model parameters in situations where more detailed information is not yet available.

This guideline has been posted for 45 day industry comment and includes the response to those comments and the SPIDERWG is seeking RSTC approval.

4. SPIDERWG Standards Authorization Requests - FAC-001 and FAC-002* – Request RSTC Comments - Shayan Rizvi, SPIDERWG Chair | Wayne Guttormson, Sponsor

In order to “avoid adverse impacts on the reliability of the Bulk Electric System,” Distribution Providers (DPs) “must document and make [f]acility interconnection requirements available” . Documentation and availability of DP generation interconnection requirements allows for necessary coordination across the transmission – distribution interface (T-D Interface) to maintain BES reliability. The purpose of FAC-002-4 is “to study the impact of interconnecting new or changed Facilities on the Bulk Electric System (BES)”. Recent studies and presentations to SPIDERWG indicate that if aggregate DER is integrated without adequate interconnection studies, reliable operation of the BES is likely to be impacted (e.g., contingencies worsened by aggregate DER tripping off-line). These SARs were developed per the approved NERC Reliability Standards Review and developed per a milestone plan presented to the RSTC EC.

5. Whitepaper: Security Integration Strategy* – Information – Dan Goodlett, NERC Staff

The ERO Reliability Risk Priorities Report identified an increase in cyber-physical risks as a high priority for the electricity sector. Through collaboration with industry stakeholders, NERC is focused on addressing cyber–physical risks to the BPS. The Security Integration Strategy outlines priorities to increase the integration of cyber and physical security into conventional planning, design, and operations engineering practices. The strategy identifies areas of focus where security integration can be enhanced to support a more secure, reliable, and resilient BPS. This presentation will cover the strategy and its core tenets.

6. White Paper: Cybersecurity for Distributed Energy Resources and DER Aggregators* – Approve – Brian Burnett, SITES | Marc Child, Sponsor

This white paper provides industry with guidance regarding activities underway to further secure the electricity ecosystem under rapid grid transformation, specifically in the area of cybersecurity efforts for distributed energy resources (DERs) and DER Aggregators. NERC is working with industry stakeholders to advance cybersecurity controls for DERs as the penetration of these

resources continues to grow in many areas across North America. This paper is informational and seeks to help provide clarity and guidance to industry stakeholders in this area. SITES is seeking RSTC approval.

1:00 - 1:30 p.m. – LUNCH – (30 mins)

7. Whitepaper: Zero Trust* – Request RSTC Comments – Brian Burnett, SITES | Marc Child, Sponsor

SITES formed a subteam for Zero Trust to develop this whitepaper with the purpose of providing clarity to the electric industry on the applicability of concepts to electric operations technology environments and enabling valuable use cases addressing barriers to adoption such as legacy technology and compliance. The SITES white paper informs the electricity sector on zero trust (ZT) concepts and provides considerations and recommendations regarding the adoption of ZT controls in operational technology (OT) and industrial control system (ICS) environments. The paper leverages the concept ZT maturity models for varying levels of implementation by registered entities and recommends entities develop their own roadmap for security and technology maturation. Finally, the paper describes considerations regarding ZT adoption by registered entities and the NERC Critical Infrastructure Protection (CIP) standards. SITES is seeking RSTC comments.

8. BCSI in the Cloud Tabletop Exercise (Technical Reference)* – Request RSTC Comments – Brent Sessions, SWG Chair | Monica Jain, Sponsor

The BCSI in the Cloud TTX Technical Reference is a document package. The files are meant to go together to capture the experiences of the tabletop exercise and to show some examples of the types of information exchanged. This package is not considered compliance guidance or guidelines, but instead a technical reference that industry and the ERO might find useful to prepare their own tabletop exercises to test their particular cloud environments. This is the first attempt at this process with the primary objective of learning for all involved parties, including the cloud service provider. Our intended strategy is to encourage other entities to utilize the process and document their experiences so the process can be further improved, and a library of experiences can be developed over time for each iteration. The SWG are asking the RSTC to review the document set and provide comments.

9. TOCC Field Test Update* – Information – Megan Sauter, Drafting Team Chair

During the September 2021 RSTC meeting, the RSTC was presented with information regarding a proposed CIP-002 Transmission Owner Control Centers (TOCCs) Field Test. The Field Test document was sent to RSTC members for a comment period ending on Thursday, September 30, 2021. Comments were considered and incorporated into the TOCC Field Test document. The RSTC endorsed the Field Test document which was then approved by the Standards Committee (SC) for implementation. This agenda item will provide an update on the implementation of the Field Test.

10. 2022 Case Quality Metrics Assessment* – Information – Olushola Lutalo, NERC Staff

This Annual Interconnection-Wide Model Assessment provides an unbiased and technically justified review of the powerflow and dynamics cases created for Interconnection-wide modeling purposes for the Eastern Interconnection (EI), Western Interconnection (WI), and Texas Interconnection (TI). Based on the results of the 2022 Case Quality Metrics Assessment, NERC will

provide list of observations for the MOD-032 designees with recommendations on which metrics to focus on to help improve model quality for base cases developed in the future.

2:30 - 2:45 p.m. – Break

11. Standing Committee Coordination Group (SCCG) Update* - Information – Rich Hydzik, RSTC Vice Chair

Per the SCCG scope document, the SCCG is to “provide quarterly reports to the standing committees for inclusion in their public Agenda posting on cross-cutting initiatives addressing risks to the reliability, security, and resilience of the BPS. This report shall be prepared in advance and voted on by the SCCG at the SCCG’s quarterly meetings.”

12. Forum and Group Reports* – Information

- a. North American Generator Forum* – Wayne Sipperly
- b. North American Transmission Forum* – Roman Carter

13. RSTC 2022-2023 Calendar Review – Stephen Crutchfield

2022 Meeting Dates	Time	Platform	Location
March 21, 2023*	1:00 – 4:00 p.m.	Full In-Person Meeting	Tampa/Atlanta
March 22, 2023	8:30 a.m. – 4:00 p.m.		
March 23, 2023	8:30 a.m. – 12:30 p.m.		
June 20, 2023*	1:00 – 4:00 PM	Hybrid (Committee Members Only In-Person)	MRO – St. Paul, MN
June 21 2023	8:30 a.m. – 4:00 p.m.		
June 22, 2023	8:30 a.m. – 12:30 p.m.		
September 19, 2023*	1:00 – 4:00 PM	Hybrid (Committee Members Only In-Person)	WECC – Salt Lake City, UT
September 20, 2023	8:30 a.m. – 4:00 p.m.		
September 21, 2023	8:30 a.m. – 12:30 p.m.		
December 6, 2023	Please reserve entirety of both days	Fully Virtual	N/A
December 7, 2023			

**This will be an informational session to review the RSTC work plan including specific high interest groups with a detailed review of their work plan. May also have some information items presented, mostly geared toward forward looking topics.*

14. Other Matters, Chair’s Closing Remarks and Adjournment

*Background materials included.

NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.
- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a

legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC Reliability Standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising Reliability Standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of Reliability Standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Reliability & Security Guidelines

- Formulated from best and/or optimal practices
- Suggested approaches or behaviors
- “HOW” certain objectives can be met
- Recommendations for how objectives “could” or “should” be accomplished

Reference Documents, Whitepapers and Technical Reports

- Documented technical concepts
- Definitions of technical terms
- Defined methods or approaches
- Can be used as justification to support “WHY” certain practices are needed

Implementation Guidance

- Provides examples or approaches for “HOW” Registered Entities could demonstrate compliance with Reliability Standard requirements.
- Used in Compliance Monitoring and Enforcement activities

Submitted to ERO

Standard Authorization Request

- Defines scope, reliability benefit, and technical justification for a new or modified Reliability Standard or definition.
- Identifies “WHAT” requirements are needed to ensure the reliable operation of the BPS

Submitted to SC

Reliability Assessment Reports

- Independent and objective evaluations of BPS reliability conducted by the ERO
- Subgroup used to gain industry perspectives, expertise, and validation
- Requires BOT approval

Reliability & Security Guidelines

- **ACCEPT** for public comment
 - Is guidance needed on this topic?
 - Are there major flaws?
- **APPROVE**
 - Has the public and committee comments been sufficiently addressed?
 - Do you agree with the recommended guidance?

Reference Documents, Whitepapers and Technical Reports

- **APPROVE**
 - Does it provide sufficient detail to support technical, security, and engineering SMEs?
 - Has it been peer reviewed and supported by a technical subgroup?
 - Is it foundational and/or conceptual
 - Does it contain specific recommendations?

Implementation Guidance

- **ENDORSE**
 - Does it provide examples or approaches on how to implement a Reliability Standard?
 - Does it meet the expectations identified in the Implementation Guidance Development and Review Aid?

Standard Authorization Request

- **ENDORSE**
 - Is the SAR form complete?
 - Does it contain technical justification?

Reliability Assessment Reports

- **ENDORSE**
 - Is there general agreement with findings and recommendations?
 - Was the process followed?

- **Approve:** The RSTC has reviewed the deliverable and supports the content and development process, including any recommendations.
- **Accept:** The RSTC has reviewed the deliverable and supports the development process used to complete the deliverable.
- **Remand:** The RSTC remands the deliverable to the originating subcommittee, refer it to another group, or direct other action by the RSTC or one of its subcommittees or groups.
- **Endorse:** The RSTC agrees with the content of the document or action, and recommends the deliverable for the approving authority to act on. This includes deliverables that are provided to the RSTC by other NERC committees. RSTC endorsements will be made with recognition that the deliverable is subject to further modifications by NERC Executive Management and/or the NERC Board. Changes made to the deliverable subsequent to RSTC endorsement will be presented to the RSTC in a timely manner. If the RSTC does not agree with the deliverable or its recommendations, it may decline endorsement. It is recognized that this does not prevent an approval authority from further action.

NERC Distributed Energy Resources (DER) Strategy

Action

Information

Summary

NERC has proactively been working with industry stakeholders to identify bulk power system (BPS) reliability risks associated with the increasing DER levels and has developed a DER strategy to identify the current and future strategic actions necessary to ensure reliable operation of the BPS. This is an informational presentation of NERC's DER strategy and will cover the strategy's core tenets in detail.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DER Strategy

JP Skeath, Engineer II
RAS November Meeting
November 9, 2022

RELIABILITY | RESILIENCE | SECURITY



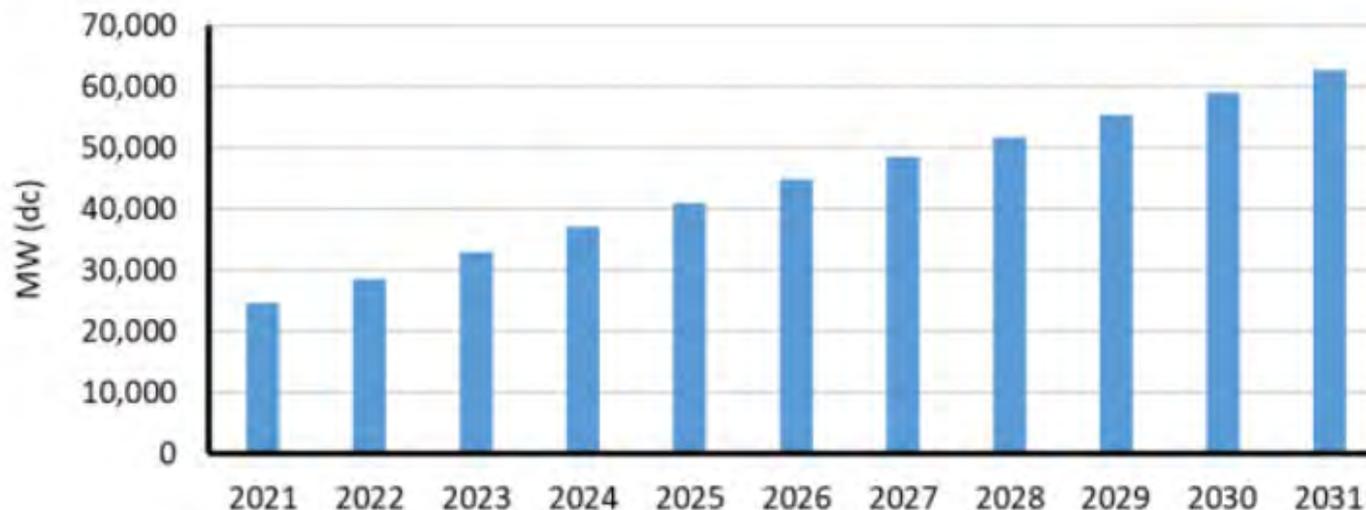


Figure 1: Cumulative Distributed Solar Photovoltaic Capacity³

https://www.nerc.com/comm/RSTC/Documents/NERC_DER%20Strategy_2022.pdf

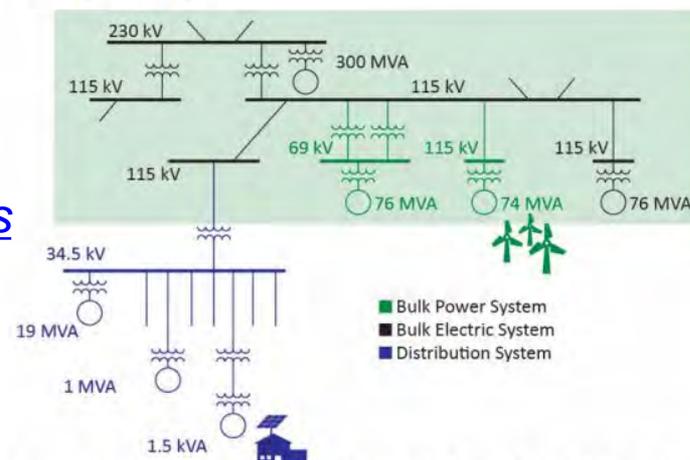


Figure 2: BES, BPS, and Distribution Graphical Examples⁴

DER Modeling

Data Collection

Modeling Tools

Verification

Modeling Usage

Studies Incorporating DER

Planning Studies

Design Criteria

Operations Planning

Operational Impacts of DER

T-D Impacts

Aggregator

Protection Systems

Decentralization

Regulatory Considerations

Aggregator

NERC Standards Enhancements

Cybersecurity

Training

Strong Foundation of Coordination between
Regulatory Agencies: FERC, NARUC, CER
Industry Stakeholders: SPIDERWG, RSTC, SC, NATF, EEI, ESIG
Ongoing Research and Design: EPRI, National Labs, Academia

A stylized map of North America, including the United States, Canada, and Mexico. The map is rendered in shades of blue and white, with a dark blue horizontal band across the middle. The text "Questions and Answers" is overlaid on this band.

Questions and Answers

White Paper: Battery Energy Storage and Multiple Types of DER Modeling

Action

Approve

Summary

The NERC SPIDERWG investigated the potential modeling challenges associated with new technology types being rapidly integrated into the distribution system. The SPIDERWG weighed updating or altering the recommended modeling framework and found that previous modeling guidance held in the face of two or more dominant technology types of DER at a T-D Interface. Further, the SPIDERWG determined that control mechanisms rather than “fuel sources” is more appropriate for transient dynamic parameterization and the study assumptions to characterize the “fuel source” rather than developing two or more sets of models. SPIDERWG also provided a set of sanity checks for TPs or PCs to use two or more aggregate dynamic models to capture the totality of DER behind a T-D interface.

This white paper shares industry experience with DER BESSs and other forms of distributed energy storage modeling to highlight industry best practices, discuss lessons learned from studies performed with DER BESSs, and highlight model application and parameterization within industry software and tools. The white paper also provides potential modeling practices to parameterize differing technology types under the SPIDERWG recommended modeling framework. The SPIDERWG received RSTC comments and made conforming revisions to the white paper. The SPIDERWG is requesting RSTC approval.

Battery Energy Storage and Multiple Types of DER Modeling

December 2022

Executive Summary

The NERC SPIDERWG investigated the potential modeling challenges associated with new technology types being rapidly integrated into the distribution system. The SPIDERWG weighed updating or altering the recommended modeling framework and found that previous modeling guidance held in the face of two or more dominant technology types of DER at a T-D Interface. Further, the SPIDERWG determined that control behavior rather than “fuel sources” is more appropriate for transient dynamic parameterization. This does not prevent separation of the DER into two or more sets of dynamic transient models based on “fuel source” as necessary for a particular study application¹. SPIDERWG also provided a set of sanity checks for TPs or PCs to use two or more aggregate dynamic models to capture the totality of DER behind a T-D interface. The SPIDERWG developed recommendations when modeling more than one dominant control type behind a T-D interface, found at the end of this paper (see [Recommendations](#)).

Purpose

The landscape of the power grid is constantly evolving due to the rapidly changing technologies and regulatory policies. This white paper highlights the importance of the ability to adequately model Distributed Battery Energy Storage Systems (BESS) and other forms of distributed energy storage in conjunction with the currently prevailing solar PV systems of current DER installations. The higher deployment of Distributed Energy Resources (DERs) across the country has recently increased the application of distribution-connected BESSs as they can complement DERs that are limited, non-dispatchable, variable, and intermittent in nature. BESSs are also applied to distribution systems for other objectives such as reducing customer demand charges, managing time-of-use rates, customer backup power, as well as participation in energy and ancillary service markets. BESSs, applied either in conjunction with variable DER or as stand-alone storage applications, can improve system operation, planning, and efficiency, and can act as reliable and vital source for emergency preparedness.

This white paper shares industry experience with DER BESSs and other forms of distributed energy storage modeling to highlight industry best practices, discuss lessons learned from studies performed with DER BESSs, and highlight model application and parameterization within industry software and tools. The white paper also provides potential modeling practices to parameterize differing technology types under the SPIDERWG recommended modeling framework.

Background

¹ Study assumptions such as nighttime conditions (and thus no SolarPV available) or batteries charging require the disaggregation by “fuel type” in order to properly set up the case.

SPIDERWG has published documentation on the recommended DER modeling framework to capture the distribution-connected resources that exist on the grid. While those documents have been published knowing that the dominant technology type of DER is solar PV, they are helpful and can be adapted to discuss nuances associated with battery storage or other storage devices. Further, when modeling solar PV and one of the storage technologies available, the previously published guidance is informative to produce the models. This section highlights the major points of the previous modeling guidance of the SPIDERWG materials².

DER_A Model Application

The dynamic effects of the DER units on the transmission systems are conventionally studied using the DER_A dynamic load model either as a stand-alone or incorporated with the composite load model. This model is appropriate for most applications³ since the effect of distribution unbalanced loads on the

transmission voltage are not significant to a TP's simulation⁴. The DER_A model was originally proposed for inverter-based solar and wind power generation. When using with battery energy storage, the active power command must be altered to a negative value for power absorption to represent charging mode of an energy storage. The DER_A model uses a reduced set of parameters to represent the aggregation of a large number of inverter-interfaced DERs. The DER_A model can be used to represent both Utility-Scale Distributed Energy Resources (U-DERs) and Retail-Scale Distributed Energy Resources (R-DERs) in the simulation^{5,6}. The DER_A model includes constant power factor and constant reactive power control modes, active power-frequency control with droop, dynamic voltage control, representation of a fraction of resources tripping or restore or entering momentary cessation, active power ramp rate limits, and active-reactive current priority. Thus, the DER_A model is an appropriate model to use for both charging and discharging battery energy storage.

Key Takeaway

The DER_A model can represent distributed battery energy storage systems in the dynamic transient software with proper adjustment of parameters.

At the current time, it is not anticipated that there are control interaction impacts for the DER_A model due to many DPs disabling the local voltage and frequency control blocks for the DER that interconnect to the distribution system. In general, there may be greater attention to implementing bulk grid support functionality, such as frequency regulation, in areas where DER penetration is high. However, the greater

² All of the past SPIDERWG modeling related reliability guidelines can be found here: <https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx>. Further, information on the SPIDERWG can be found on their website here: <https://www.nerc.com/comm/RSTC/Pages/SPIDERWG.aspx>

³ SPIDERWG has also identified applications where a single aggregate positive sequence dynamic model (i.e., DER_A model) would not fit in this generalization titled *Technical Report: Beyond Positive Sequence* available here: [Report \(nerc.com\)](#)

⁴ TPs primarily use Positive Sequence models to represent both the transmission and distribution system, and the DER_A model is a positive sequence dynamic transient model. This statement indicates that no new model is required to represent distribution-connected BESS in the TP's set of models.

⁵ U-DER and R-DER are modeling designations to break up the DER into two distinct categories. For more information, see the published SPIDERWG guidance here: [\[LINK\]](#) (merged SPIDERWG RG from Tranche 2, if approved Dec RSTC)

⁶ There is a need to adequately parameterize the DER_A model embedded in the composite load model to reflect the DER at that location on the feeder. This may involve adapting the model framework to allow for accurate parameterization of the load components of the composite load model and the DER components.

factor is the level of understanding of these issues by the distribution entities and their opinions on how implementing these functions balance with their own system's needs. Decisions regarding local voltage regulation implementation are most frequently based on the potential benefits and adverse consequences at the distribution level, without any consideration of bulk system implications.⁷ For those instances, there may exist some control interaction between the various protection, voltage regulation, and frequency regulation schemes that are more important to capture rather than the fuel mix of the resources. Further complicating the mix are return-to-service, ride-through, and anti-island settings that can cause disruption of power from the DER. The DER_A model has the capability to model the critical set of these equipment settings, and the SPIDERWG does not propose developing a new model to capture all of the settings. Rather, the SPIDERWG recommends TPs and PCs use other models in the software (e.g., protection models) in order to capture the remainder of the behavior rather than development of a larger, integrated generator model.

Application to co-simulation algorithms

The DER_A model can be used to represent active and reactive current injection/absorption of standalone/aggregated single-phase DER units, including battery storage systems, in three-phase distribution simulators. The distribution simulator can then be coupled with a transmission simulator in a co-simulation environment through exchange of powers and voltages at the T&D coupling points. In this instance, the equipment being modeled in the DER_A model is for one POI at the distribution interface, with an explicit representation of distribution feeders and other shunt equipment on the distribution system based on the local distribution requirements to serve load in that area. The transmission system is simulated separately from the distribution system, so the aggregate model instead is at the distribution POI rather than at the T-D interface and is an adaptation of the positive sequence modeling framework to use co-simulation. In short, batteries do not alter the general guidance of DER related work in the co-simulation area.

Distributed Energy Storage FERC Order No. 2222 Implications

On September 17, 2020, the Federal Energy Regulatory Commission (FERC) approved Order 2222, enabling distributed energy resource (DER) aggregators to compete in all regional organized wholesale electric markets. The Commission defined DER in Order 2222 as follows: "These resources may include, but are not limited to, resources that are in front of and behind the customer meter, electric storage resources, intermittent generation, distributed generation, demand response, energy efficiency, thermal storage, and electric vehicles and their supply equipment – as long as such a resource is located on the distribution system, any subsystem thereof or behind a customer meter." [Emphasis added]

The final rule enables these aggregations of DER to participate in the regional organized wholesale capacity, energy, and ancillary services markets alongside traditional resources. Multiple DERs may aggregate to satisfy the minimum size requirement, specified in the Order, of 100kW along with any necessary performance requirements that they might not meet individually. It is anticipated that this Order will bring many different technology types of DER into the market, and thus into the system. While Solar PV still is the largest share of DER in the system, it is anticipated that BESSs will rise to an appreciable penetration

⁷ Voltage regulation provided by DER at the distribution level rarely has any steady-state benefit to regulation of the transmission voltage due to the decoupling effect of on-load tap changers and voltage regulators in the distribution system.

meaning that the modeling framework proposed by SPIDERWG may need adaption to account for two significant lump sums of equipment potentially having differing operational characteristics. This white paper describes those considerations; however, the impacts of a DER Aggregator are greater than modeling efforts for two or more technology types in an aggregated generation resource (akin to a virtual power plant with many fuel types). SPIDERWG’s *White Paper: BPS Reliability Perspectives on the DER Aggregator*⁸ contains discussion on the various aspects of interfacing with the DER Aggregator, and has ongoing work to address the various aspects.

Modeling of Distribution-Connected BESS

So far, the SPIDERWG has investigated a few modeling aspects of BESSs. They have compared the electrical response of the battery energy storage equipment in the positive sequence model versus a more explicit representation of the charge, discharge, and state of charge in an EMT software. The comparison showed that the DER_A model captured the large disturbance behavior of the resource, and there were not many times when the EMT software model showed a more accurate representation than the positive sequence model. Further, these differences are not unique to battery storage, and thus were not used for drawing conclusions on modeling of battery storage.

Key Takeaway

Tracking of state of charge is not a critical component to modeling distribution-connected BESS in transmission transient dynamic studies. The DER_A model is sufficient.

While the exploratory simulation has shown that the modeling framework in the other SPIDERWG reliability guidelines is sufficient, there are a few discussion points to ensure when accounting for battery energy storage on the distribution system. These batteries can vary between a 7kW wall-mounted pack to a 1-2 MW shipping container sized battery system that can integrate into community solar farms, or interconnect at the distribution system at a separate Point of Interconnection as a standalone energy storage facility. The guidance in the reliability guidelines covers the different technology types for DER; however, when a TP builds a distribution equivalent behind the T-D Interface to explicitly build out the SPIDERWG modeling framework⁹ then the TP can begin to place what was originally at the head of the equivalent feeder in the

Key Takeaway

The modeling framework in SPIDERWG documents accounts for distribution-connected battery storage, yet batteries are being interconnected in a way that can modify wide-area study assumptions. This indicates an increase of data to model appropriately.

framework throughout the, now non-equivalent represented, distribution system. Further, there is a real interest for larger, U-DER modeled facilities to add large batteries to their installation post-commissioning. These modify the voltage and frequency response of the plant and require some information to be sent to the DP to finish the interconnection, but also to the TP so that proper adjustments are made to align the transmission planning study assumptions¹⁰. These modifications to

⁸ Available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SPIDERWG_White_Paper_-_BPS_Perspectives_on_DER_Aggregator_docx.pdf

⁹ This is opposed to having the composite load model representation perform this function for the TP. Most major software has an automated and manual capability to add in the distribution equivalent.

¹⁰ Primarily around dispatch and whether these batteries will be injecting or absorbing current.

the facility capabilities underscore the sheer amount of study work and coordination of relevant information to ensure bulk system reliability. As other SPIDERWG documents and industry stakeholders have identified good modeling data is already hard to obtain to populate these power system models to represent the aggregate equipment. Batteries, their various control schemes, and potential for multiple operational profiles of the distribution-connected resources will only complicate the development of models¹¹.

Modeling of Two or More Dominant DER Technology Types at a T-D Interface

In the past SPIDERWG documents, the proposed DER modeling framework had two electrical locations for a generator record specified to account for U-DER and R-DER. The framework is reproduced for reference in [Figure 1](#). When using this framework, it was typical to have each individual DER above the defined individual modeling threshold to be at the head of the feeder, with exceptions placed behind the feeder impedance should the feeder impedance be a factor¹² in determining the impact to the T-D interface for those larger utility scale installations. This framework does not change for modeling the impacts of DER BESSs, and is only adapted when more than one dominant technology type impacts the operational profile at the T-D Interface. SPIDERWG recommends that the modeling framework here be adapted to account for the control types and parameters for the equipment represented, including representing larger scale installations further away from the head of the feeder if that is more representative.

¹¹ The NERC Standards Project 2022-02 is working through a portion of the modeling information and wide-area planning studies for all of DER. The Project webpage is available here: <https://www.nerc.com/pa/Stand/Pages/Project2022-02ModificationstoTPL-001-5-1andMOD-032-1.aspx>.

¹² In these cases, this would indicate that a shift to more explicit modeling of the distribution system which the recommended DER modeling framework does not cover. The DER modeling framework is appropriate for instances where specific information (e.g., DER location throughout the system, distribution voltage regulation equipment settings, etc.) is not available or desired to be explicitly represented by the TP.

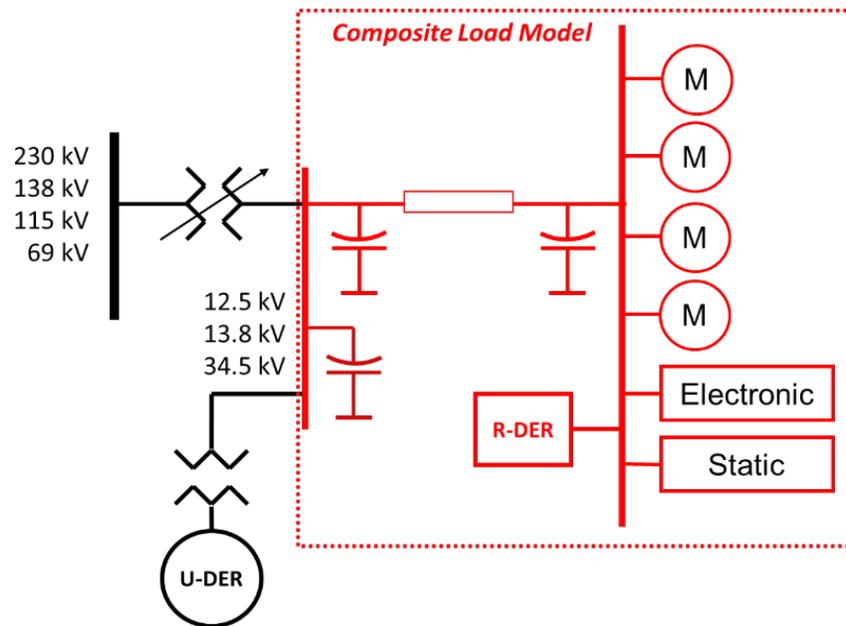


Figure 1: Recommended DER Modeling Framework

Battery Energy Storage Systems Using the DER Modeling Framework

Typically, for bulk connected BESSs, the transient dynamic model¹³ representing the equipment pays close attention to the state of charge and outputs its value to a plotting tool for dynamic simulations in order for the study team to track the energy capability of the battery. The DER_A model lacks the ability to track or initialize the BESS's state of charge and has no loop to deplete the energy of the battery for output. This would mean that in an aggregation with various discharge time constants and levels of charge, there exists no method to accurately describe the tracking of aggregate state of charge, maximum state of charge in relationship to total aggregation capacity, or other various parameters that describe a single facility's operational behavior. In the SPIDERWG investigation, however, this complexity was not seen as a need for use in transient dynamic studies. Rather, the set of study assumptions can be informed by assumed availability of charge for the resources and accounted for by dispatch assumptions for transient dynamic modeling and other Transmission Planning functions¹⁴. Thus, the modeling framework can be directly used for capturing the impact of distribution-connected batteries.

In summary, the SPIDERWG modeling framework and the DER_A model are a convenient and recommended approach to capturing the impact of distribution-connected BESSs. There exist no current issues with controllers and the state of dynamic transient models allows for both power absorption and discharge from the equipment. There are various reasons why an aggregate model should be disaggregated,

¹³ This is typically the second generation renewable model reec_c.

¹⁴ The Resource Planner, however, may need some different modeling assumptions when performing their analysis. However, this is outside the scope of this paper and the scope of changes is likely to mirror separation of fuel types rather than detailed modeling parameters.

primarily the control behavior of the represented devices¹⁵. The SPIDERWG recommends “fuel type” for BESSs be readily available for scenario development.

Adaption of the Modeling Framework for Two or more Dominant Technology Types

The NERC SPIDERWG has performed various simulations to show potential coincident impact of different technology types in this and in the *Technical Report: Beyond Positive Sequence* document that describes potential indicators for a more detailed representation of the distribution system and DER¹⁶. Many of the findings in that report were based on one technology, solar PV, with various equipment settings based on what version of IEEE 1547 the equipment was certified to. The potential to require two different dynamic models to capture the expected large disturbance behavior seen at the T-D Interface was based on the difference in settings coded into the equipment and various functions enabled or disabled. This serves as the basis for the SPIDERWG recommendations for modeling more than one dominant technology type at a T-D Interface. In practical investigation, however, the SPIDERWG members noted that the technology or “fuel” type is not as important as the inverter settings for most studies. At this time, technology type (e.g., battery storage, solar PV, or super capacitors) is less important opposed to the various “smart features” that inverter manufacturers are adding to their equipment. In particular, the frequency and voltage controls. Two aggregations may be needed in order to model these controls.

Key Takeaway

When modeling two or more dominant technology types, the modeling framework is sufficient. Control logic on voltage or frequency is more important than technology types. Study assumptions may also dictate when to lump into two aggregations. A prominent example is an instance of battery charging while solar PV is injecting active power to the system.

Taking BESSs as an example, the need for careful parameterization of the DER models is highlighted when the BESSs charging while solar PV DERs at the T-D Interface are producing power. In this scenario, not all DER locations have both a BESS and a solar PV system, but in aggregate the T-D Interface sees a variety of motor load, electronic load, BESS charging characteristics, solar PV generation output, and a variety of other impacts. When lumping, solar PV generating and BESS charging, the need to carefully parameterize the transient dynamic model of the lumped solar PV and BESS is enhanced in order to ensure the current commands and limits are appropriate for such a scenario. In particular, the frequency response settings of the aggregation should be checked by the TP for accuracy.

One complicating factor for using the present modeling framework is that distribution planners typically have feeder plans to ensure the feeder remains within 0.95 and 1.05 p.u. voltage per the ANSI requirements at end-user feeds. The present composite load model automatically adjusts the feeder impedance to ensure the end of the modeled equivalent feeder is within those boundaries. Thus, the

¹⁵ This is typically captured by the “vintage” of IEEE 1547 (e.g., 1547-2003, 1547-2014, etc.) as that dictates the trip behavior. With 1547-2018, some of these behaviors have an allowable range of settings, which can play into a TP’s decision to disaggregate on such control behavior. UL 1741 SA or UL 1741 SB certification also can play a factor in deciding to disaggregate.

¹⁶ Available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Beyond_Positive_Sequence_Technical_Report.pdf

transmission planner would need to include this adjustment in their planning practices if the TP is modeling the T-D interface explicitly to account for the electrical distance to head of feeder for the control of multiple aggregations of DER. The SPIDERWG does not consider this a deviation of the framework as it simply transitions from an automated process in the composite load model into something the TP parameterizes manually.

While the industry transitions between one dominant technology type to a future two or more dominant technology types (in terms of penetration at the T-D Interface), the modeling framework does not need to be adjusted; however, there are parameters that would need to be tracked and adjusted during the transition. For example, a 1MVA non-frequency regulating aggregation coupled with a 0.1 MVA of 5% droop characteristic is a 1.1 MVA aggregation with a 55% droop bound by 1 MVA min and 1.1 MVA max¹⁷. In a practical modeling application, the above is awkward in present load modeling builds with only one input for generation as it requires aggregation of the “smart features” to be done for each applicable interconnection requirements of the resources. In future load models, there are plans for multiple generation components, which would make the above calculation step moot¹⁸ for building one aggregation out of the various control features.

Recommendations

The SPIDERWG recommends that TPs and PCs use the recommended modeling framework in [Figure 1](#) to model multiple separate DER control aggregations behind a T-D Interface. To determine when a TP or PC can separate the aggregate DER into two or more smaller DER aggregations, the SPIDERWG recommends to ensure the following have been accomplished prior to investing the time and resources to maintain two or more aggregate models behind a T-D interface:

- The state of dynamic load modeling for that T-D interface should be of the same or higher model quality than the DER modeling component.
- The new models should be of higher quality when separated from the existing aggregation and provide more information at the T-D interface separated. (e.g., tracking of frequency responsive DER)
- The percent penetration of the control to be separated should be significant at the T-D interface
- The case assumptions should be aligned with the need to separate the existing aggregation into multiple.

¹⁷ Note, the higher percentage droop the larger speed (frequency) different to move the total MVA of the unit. Thus, for a 5% speed change at 55% droop, this 1.1 MVA aggregation will move 9.09% of its nameplate or 0.1 MVA, confirming that the aggregation is parameterized appropriately.

¹⁸ As the planner can simply place each separately parameterized aggregation in the model and it automatically handles the reflection of the aggregate at the T-D Interface.

Further, if the T-D interface is selected for using a method in the *Beyond Positive Sequence* technical report¹⁹, the SPIDERWG recommends to walk through the following²⁰:

- TPs should understand the distribution composition, distribution model, load characteristics, and voltage/frequency control logic in order to capture the scope of distribution model buildout for their study.
- TPs should compare distribution voltage and frequency response characteristics to local transmission system characteristics and constraints to gather required data flags and information to exchange in the simulation platforms.
- TP should determine the setup convenience to build the model and interface between the distribution solver and transmission solver and note areas of long setup times.

¹⁹ Whenever the TP moves to a more explicit model representation there is a need for increased computation power and data management needs. This is largely understood by most TPs, but is worthwhile to note that the methods in this report require more explicit model representation than the recommended model framework outside of the listed recommendations.

²⁰ This is not a recommendation for or against using tools outside of positive sequence, but a list of high level determinations in order to ensure a smoother study plan.

Battery Energy Storage and Multiple Types of DER Modeling

September-December 2022

Executive Summary

The NERC SPIDERWG investigated the potential modeling challenges associated with new technology types being rapidly integrated into the distribution system. The SPIDERWG weighed updating or altering the recommended modeling framework and found that previous modeling guidance held in the face of two or more dominant technology types of DER at a T-D Interface. Further, the SPIDERWG determined that control mechanisms—behavior rather than “fuel sources” is more appropriate for transient dynamic parameterization. This does not prevent separation of the DER into two or more sets of dynamic transient models based on “fuel source” as necessary for a particular study application¹, and the study assumptions to characterize the “fuel source” rather than developing two or more sets of models. SPIDERWG also provided a set of sanity checks for TPs or PCs to use two or more aggregate dynamic models to capture the totality of DER behind a T-D interface. The SPIDERWG developed recommendations when modeling more than one dominant control type behind a T-D interface, found at the end of this paper (see [Recommendations](#)).

Purpose

The landscape of the power grid is constantly evolving due to the rapidly changing technologies and regulatory policies. This white paper highlights the importance of the ability to adequately model Distributed Battery Energy Storage Systems (BESS) and other forms of distributed energy storage in conjunction with the currently prevailing Solar-solar PV systems of current DER installations. The higher deployment of Distributed Energy Resources (DERs) across the country has recently increased the application of distribution-connected BESSs as they can complement DERs that are limited, non-dispatchable, variable, and intermittent in nature. BESSs are also applied to distribution systems for other objectives such as reducing customer demand charges, managing time-of-use rates, customer backup power, as well as participation in energy and ancillary service markets. DERs with BESSs, applied either in conjunction with variable DER or as stand-alone storage applications, DERs with BESSs can improve system operation, planning, and efficiency, and can act as reliable and vital source for emergency preparedness.

This white paper shares industry experience with DER BESSs and other forms of distributed energy storage modeling to highlight industry best practices, discuss lessons learned from studies performed with DER BESSs, and highlight model application and parameterization within industry software and tools. The white paper also provides potential modeling practices to parameterize differing technology types under the SPIDERWG recommended modeling framework.

¹ Study assumptions such as nighttime conditions (and thus no SolarPV available) or batteries charging require the disaggregation by “fuel type” in order to properly set up the case.

Commented [JS1]: From Edison:
“My apologies for a late response on my review. I did not have a lot of specific comments. My general impression of the document, however, was that it did not seem to be as clearly written as it could have been. I may need to re-read it and it might become clearer. One thing that would help would be a clear and concise summary of each recommendation, either in the section where that particular topic is covered or in a summary section. The current write-up seems to be a loosely connected technical discussion without a clear unifying them or readily identifiable guidance.

I appreciate the workgroup great work on both papers.

Commented [JS2R1]: Thank you for your comment. Clarity added around recommendations

Commented [AWJ3]: This sentence is a little difficult to read, is there a way to rephrase it a little?

Commented [JS4R3]: Reworded in to two sentences.

Formatted: Cross Reference Char

Commented [RW5]: Implication here is that D-BESS are only applied in conjunction with variable DER.

Commented [JS6R5]: Changes made as identified.

Background

SPIDERWG has published documentation on the recommended DER modeling framework to capture the distribution-connected resources that exist on the grid. While those documents have been published knowing that the dominant technology type of DER is solar PV, they are helpful and can be adapted to discuss nuances associated with battery storage or other storage devices. Further, when modeling solar PV and one of the storage technologies available, the previously published guidance is informative to produce the models. This section highlights the major points of the previous modeling guidance of the SPIDERWG materials².

DER_A Model Application

The dynamic effects of the DER units on the transmission systems are conventionally studied using the DER_A dynamic load model either as a stand-alone or incorporated with the composite load model. This model is appropriate for most applications³ since the effect of distribution unbalanced loads on the transmission voltage imbalance are not significant to a TP's simulation⁴. The DER_A model was originally proposed for inverter-based solar and wind power generation. When using with battery energy storage, the active power command must be altered to a negative value for power absorption, to represent charging mode of an energy storage. The DER_A model uses a reduced set of parameters to represent the aggregation of a large number of inverter-interfaced DERs. The DER_A model can be used to represent both Utility-Scale Distributed Energy Resources (U-DERs) and Retail-Scale Distributed Energy Resources (R-DERs) in the simulation^{5,6}. The DER_A model includes constant power factor and constant reactive power control modes, active power-frequency control with droop, dynamic voltage control, representation of a fraction of resources tripping or restore or entering momentary cessation, active power ramp rate limits, and active-reactive current priority. Thus, the DER_A model is an appropriate model to use for both charging and discharging battery energy storage.

Key Takeaway

The DER_A model can represent distributed battery energy storage systems in the dynamic transient software with proper adjustment of parameters.

At the current time, it is not anticipated that there are control interaction impacts for the DER_A model due to many DPs disabling the local voltage and frequency control blocks for the DER that interconnect to the

Commented [RW7]: This statement, while technically correct, is irrelevant and misleading because it implies that the phase-by-phase behavior of DER is not relevant. It is relevant in that DER responds differently to unbalanced transmission faults than to balanced faults creating the same positive sequence voltage magnitude. Also, the loss of significant DER on only certain phases following a transmission unbalanced fault can create a lingering amount of steady-state imbalance in the transmission voltage lasting until the DER return to service, typically 5 minutes later. These unbalance issues are covered by other documents and are not specific to the issue of BESS modeling, so it is best to leave this issue aside here.

Commented [JSBR7]: Keeping the sentence as the audience would be interested in cases where phase by phase distribution has an impact on the parameterization or usage of an equivalent model. (covered in other RGs), however there was a push to develop a different BESS model for D-connected equipment. Added clarity.

Formatted: Superscript

² All of the past SPIDERWG modeling related reliability guidelines can be found here: <https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx>. Further, information on the SPIDERWG can be found on their website here: <https://www.nerc.com/comm/RSTC/Pages/SPIDERWG.aspx>

³ SPIDERWG has also identified applications where a single aggregate positive sequence dynamic model (i.e., DER_A model) would not fit in this generalization titled *Technical Report: Beyond Positive Sequence* available here: [Report \(nerc.com\)](https://www.nerc.com/comm/RSTC/Pages/SPIDERWG.aspx)

⁴ TPs primarily use Positive Sequence models to represent both the transmission and distribution system, and the DER_A model is a positive sequence dynamic transient model. This statement indicates that no new model is required to represent distribution-connected BESS in the TP's set of models.

⁵ U-DER and R-DER are modeling designations to break up the DER into two distinct categories. For more information, see the published SPIDERWG guidance here: [LINK](#) (merged SPIDERWG RG from Tranche 2, if approved Dec RSTC when available)

⁶ There is a need to adequately parameterize the DER_A model embedded in the composite load model to reflect the DER at that location on the feeder. This may involve adapting the model framework to allow for accurate parameterization of the load components of the composite load model and the DER components.

distribution system. In general, there may be greater attention to implementing bulk grid support functionality, such as frequency regulation, in areas where DER penetration is high. However, the greater factor is the level of understanding of these issues by the distribution entities and their opinions on how implementing these functions balance with their own system's needs. Decisions regarding local voltage regulation implementation are most frequently based on the potential benefits and adverse consequences at the distribution level, without any consideration of bulk system implications.² For those instances, there may exist some control interaction between the various protection, voltage regulation, and frequency regulation schemes that are more important to capture rather than the fuel mix of the resources. Further complicating the mix are return-to-service, ride-through, and anti-island settings that can cause disruption of power from the DER. The DER_A model has the capability to model the critical set of these equipment settings, and the SPIDERWG does not propose developing a new model to capture all of the settings. Rather, the SPIDERWG recommends TPs and PCs use other models in the software (e.g., protection models) in order to capture the remainder of the behavior rather than development of a larger, integrated generator model.

Application to co-simulation algorithms

The DER_A model can be used to represent active and reactive current injection/absorption of standalone/aggregated single-phase DER units, including battery storage systems, in three-phase distribution simulators. The distribution simulator can then be coupled with a transmission simulator in a co-simulation environment through exchange of powers and voltages at the T&D coupling points. In this instance, the equipment being modeled in the DER_A model is for one POI at the distribution interface, with an explicit representation of distribution feeders and other shunt equipment on the distribution system based on the local distribution requirements to serve load in that area. The transmission system is simulated separately from the distribution system, so the aggregate model instead is at the distribution POI rather than at the T-D interface and is an adaptation of the positive sequence modeling framework to use co-simulation. In short, batteries do not alter the general guidance of DER related work in the co-simulation area.

Distributed Energy Storage FERC Order No. 2222 Implications

On September 17, 2020, the Federal Energy Regulatory Commission (FERC) approved Order 2222, enabling distributed energy resource (DER) aggregators to compete in all regional organized wholesale electric markets. The Commission defined DER in Order 2222 as follows: "These resources may include, but are not limited to, resources that are in front of and behind the customer meter, electric storage resources, intermittent generation, distributed generation, demand response, energy efficiency, thermal storage, and electric vehicles and their supply equipment – as long as such a resource is located on the distribution system, any subsystem thereof or behind a customer meter." [Emphasis added]

The final rule enables these aggregations of DER to participate in the regional organized wholesale capacity, energy, and ancillary services markets alongside traditional resources. Multiple DERs may aggregate to satisfy the minimum size requirement, specified in the Order, of 100kW along with any necessary

² Voltage regulation provided by DER at the distribution level rarely has any steady-state benefit to regulation of the transmission voltage due to the decoupling effect of on-load tap changers and voltage regulators in the distribution system.

Commented [RW9]: I have seen no instances where decisions regarding implementation of grid support functions depend on whether specific feeders or distribution systems have penetration levels where backflow occurs. Also, the wide-area risks of DER tripping due to transmission faults does not depend on whether individual buses have backflow. It is a matter of area-wide penetration and if area-wide penetration is 90%, there could be no backflow anywhere but yet there could be a massive post-fault generation/load mismatch.

Commented [JS10R9]: Content additions accepted with a few clarity edits on one sentence.

Commented [RW11]: Very speculative comment. How is this of particular relevance to BESS modeling?

Commented [JS12R11]: Added some text to relate to BESS modeling.

Commented [RW13]: I don't understand the particular relevance of this entire paragraph to the specific guidance related to BESS modeling. These functions are applied, or not applied, on DER of all types of energy source, and the implementation and settings of these functions are generally not different for PV and BESS.

Commented [JS14R13]: Moved D

performance requirements that they might not meet individually. It is anticipated that this Order will bring many different technology types of DER into the market, and thus into the system. While Solar PV still is the largest share of DER in the system, it is anticipated that BESSs will rise to an appreciable penetration meaning that the modeling framework proposed by SPIDERWG may need adaption to account for two significant lump sums of equipment potentially having differing operational characteristics. This white paper describes those considerations; however, the impacts of a DER Aggregator are greater than modeling efforts for two or more technology types in an aggregated generation resource (akin to a virtual power plant with many fuel types). SPIDERWG's *White Paper: BPS Reliability Perspectives on the DER Aggregator*⁸ contains discussion on the various aspects of interfacing with the DER Aggregator, and has ongoing work to address the various aspects.

Modeling of Distribution-Connected BESS

So far, the SPIDERWG has investigated a few modeling aspects of BESSs. They have compared the electrical response of the battery energy storage equipment in the positive sequence model versus a more explicit representation of the charge, discharge, and state of charge in an EMT software. The comparison showed that the DER_A model captured the large disturbance behavior of the resource, and there were not many times when the EMT software model showed a more accurate representation than the positive sequence model. Further, these differences are not unique to battery storage, and thus were not used for drawing conclusions on modeling of battery storage.

Key Takeaway
Tracking of state of charge is not a critical component to modeling distribution-connected BESS in transmission transient dynamic studies. The DER_A model is sufficient.

While the exploratory simulation has shown that the modeling framework in the other SPIDERWG reliability guidelines is sufficient, there are a few discussion points to ensure when accounting for battery energy storage on the distribution system. These batteries can vary between a 7kW wall-mounted pack to a 1-2 MW shipping container sized battery system that can integrate into community solar farms, ~~or, or interconnect at the distribution level system at a separate Point of Interconnection as a standalone utility-scale energy storage facilities facility.~~

Key Takeaway
The modeling framework in SPIDERWG documents accounts for distribution-connected battery storage, yet batteries are being interconnected in a way that can modify wide-area study assumptions. This indicates an increase of data to model appropriately.

The guidance in the reliability guidelines covers the different technology types for DER; however, when a TP builds a distribution equivalent behind the T-D Interface to explicitly build out the SPIDERWG modeling framework⁹ then the TP can begin to place what was originally at the head of the equivalent feeder in the framework ~~all~~ throughout the, ~~now non-equivalent represented,~~ distribution system.

Commented [RW15]: This is unclear. Is this an admission that the previously stated framework with all U-DER at the head of the feeder does not reflect what is really happening? If so, that is a welcome improvement.

⁸ Available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SPIDERWG_White_Paper_-_BPS_Perspectives_on_DER_Aggregator_docx.pdf

⁹ This is opposed to having the composite load model representation perform this function for the TP. Most major software has an automated and manual capability to add in the distribution equivalent.

Further, there is a real interest for larger, U-DER modeled facilities to add large batteries to their installation post-commissioning. These modify the voltage and frequency response of the plant and require some information to be sent to the DP to finish the interconnection, but also to the TP so that proper adjustments are made to align the transmission planning study assumptions¹⁰. These modifications to the facility capabilities underscore the sheer amount of study work and coordination of relevant information to ensure bulk system reliability. As other SPIDERWG documents and industry stakeholders have identified good modeling data is already hard to obtain to populate these power system models to represent the aggregate equipment. Batteries, their various control schemes, and potential for multiple operational profiles of the distribution-connected resources will only complicate the development of models¹¹.

Modeling of Two or More Dominant DER Technology Types at a T-D Interface

In the past SPIDERWG documents, the proposed DER modeling framework had two electrical locations for a generator record specified to account for U-DER and R-DER. The framework is reproduced for reference in Figure 1. When using this framework, it was typical to have each individual ~~DER~~ U-DER above the defined individual modeling threshold to be at the head of the feeder, with ~~some documented~~ exceptions placed behind the feeder impedance should the feeder impedance be a factor¹² in determining the impact to the T-D interface for those larger utility scale installations. This framework does not change for modeling the impacts of DER BESSs, and is only adapted when more than one dominant technology type impacts the operational profile at the T-D Interface. SPIDERWG recommends that the modeling framework here be adapted to account for the control types and parameters for the equipment represented, including representing larger scale installations further away from the head of the feeder if that is more representative.

Commented [JS16R15]: The framework has two buckets to use for DER: one at the head and one after the equivalent feeder impedance. The names should be just "DER" as the categories of U-DER and R-DER are modeling designations to help simplify.
Added additional clarity.

Formatted: Font: 12 pt

Commented [RW17]: I strongly question whether this should be indicated as an implied unusual circumstance. In my experience, the MAJORITY of U-DER are located well out on the distribution feeder, closer to the ultimate load than to the substation, to where they have major impact on distribution voltage. If the stated framework were correct, why are distribution voltage issues created by U-DER such a major issue?

Commented [JS18R17]: Changes made to statement to reflect that U-DER are modeling related terms and that the realized facility is simply "DER".

¹⁰ Primarily around dispatch and whether these batteries will be injecting or absorbing current.

¹¹ The NERC Standards Project 2022-02 is working through a portion of the modeling information and wide-area planning studies for all of DER. The Project webpage is available here: <https://www.nerc.com/pa/Stand/Pages/Project2022-02ModificationstoTPL-001-5-1andMOD-032-1.aspx>.

¹² In these cases, this would indicate that a shift to more explicit modeling of the distribution system which the recommended DER modeling framework does not cover. The DER modeling framework is appropriate for instances where specific information (e.g., DER location throughout the system, distribution voltage regulation equipment settings, etc.) is not available or desired to be explicitly represented by the TP.

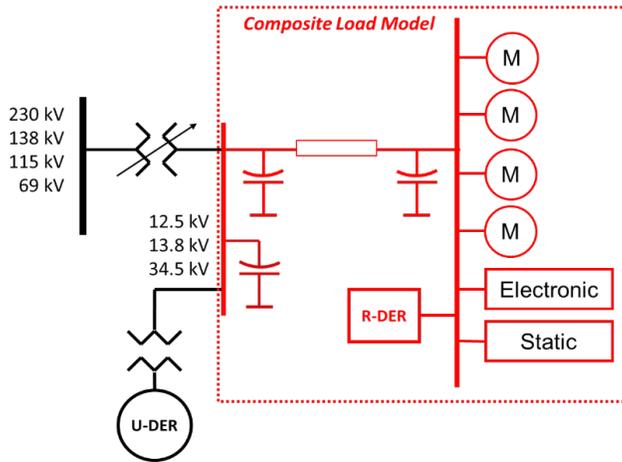


Figure 1: Recommended DER Modeling Framework

Battery Energy Storage Systems Using the DER Modeling Framework

Typically, for bulk connected BESSs, the transient dynamic model¹³ representing the equipment model pays close attention to the state of charge and outputs that its value to a plotting tool for dynamic simulations in order for the study team to track the energy capability of the battery. The DER_A model lacks the ability to track or initialize the BESS's state of charge and has no loop to deplete the energy of the battery for output. This would mean that in an aggregation with various discharge time constants and levels of charge, there exists no method to accurately describe the tracking of aggregate state of charge, maximum state of charge in relationship to total aggregation capacity, or other various parameters that describe a single facility's operational behavior. In the SPIDERWG investigation, however, this complexity was not seen as a need for use in transient dynamic studies. Rather, the set of study assumptions can be informed by assumed availability of charge for the resources and accounted for by dispatch assumptions for transient dynamic modeling and other Transmission Planning functions¹⁴. Thus, the modeling framework can be directly used for capturing the impact of distribution-connected batteries.

~~At the current time, it is not anticipated that there are control interaction impacts for the DER_A model due to many areas DPs disabling the local voltage and frequency control blocks for the DER that interconnect to the distribution system. In general, there may be greater attention to implementing bulk grid support functionality, such as frequency regulation, in areas where DER penetration is high. However, the greater factor is the level of understanding of these issues by the distribution entities and their opinions on how implementing these functions balance with their concerns about the speculated impacts these functions~~

¹³ This is typically the second generation renewable model reec_c.

¹⁴ The Resource Planner, however, may need some different modeling assumptions when performing their analysis. However, this is outside the scope of this paper and the scope of changes is likely to mirror separation of fuel types rather than detailed modeling parameters.

Commented [RW19]: Check the sentence. Something seems to be missing.

Commented [JS20R19]: Clarity added.

~~might have on distribution concerns. Decisions regarding local voltage regulation implementation are most frequently based on the potential benefits and adverse consequences at the distribution level, without any consideration of bulk system implications.¹⁵ In a system where DER deliver power to load outside of their own distribution system (and thus wheel the power through a transmission system), these control schemes are likely to be enabled to ensure the reliability of the interconnected bulk system (e.g., using IEEE 1547-2018 Category III parameter ranges over Category II or Category I ranges). For those instances, there may exist some control interaction between the various protection, voltage regulation, and frequency regulation schemes. Further complicating the mix are return to service, ride through, and anti-island settings that can cause disruption of power from the DER. The DER_A model has the capability to model the critical set of these equipment settings, and the SPIDERWG does not propose developing a new model to capture all of the settings. Rather, the SPIDERWG recommends TPs and PCs use other models in the software (e.g., protection models) in order to capture the remainder of the behavior rather than development of a larger, integrated generator model.~~

In summary, the SPIDERWG modeling framework and the DER_A model are a convenient and recommended approach to capturing the impact of distribution-connected BESSs. There exist no current issues with controllers and the state of dynamic transient models allows for both power absorption and discharge from the equipment. ~~There are various reasons why an aggregate model should be disaggregated, primarily the control behavior of the represented devices¹⁶. The SPIDERWG recommends “fuel type” for BESSs be readily available for scenario development, and the trip settings associated with the equipment are the primary reason identified by SPIDERWG for separating distribution-connected BESS in one aggregation from solar PV in a separate aggregation at the T-D interface.~~

Adaption of the Modeling Framework for Two or more Dominant Technology Types

The NERC SPIDERWG has performed various simulations to show potential coincident impact of different technology types in this and in the *Technical Report: Beyond Positive Sequence* document that describes potential indicators for a more detailed representation of the distribution system and DER¹⁷. Many of the findings in that report were based on one technology, ~~Solar solar~~ PV, with various equipment settings based on what version of IEEE 1547 the equipment was certified to. The potential to require two different dynamic models to capture the expected

Key Takeaway

When modeling two or more dominant technology types, the modeling framework is sufficient. Control logic on voltage or frequency is more important than technology types. Study assumptions may also dictate when to lump into two aggregations. A prominent example is an instance of battery charging while solar PV is injecting active power to the system.

¹⁵ ~~Voltage regulation provided by DER at the distribution level rarely has any steady state benefit to regulation of the transmission voltage due to the decoupling effect of on-load tap changers and voltage regulators in the distribution system.~~

¹⁶ This is typically captured by the “vintage” of IEEE 1547 (e.g., 1547-2003, 1547-2014, etc.) as that dictates the trip behavior. With 1547-2018, some of these behaviors have an allowable range of settings, which can play into a TPs decision to disaggregate on such control behavior. UL 1741 SA or UL 1741 SB certification also can play a factor in deciding to disaggregate.

¹⁷ Available here: [LINK AFTER PUBLICATION](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Beyond_Positive_Sequence_Technical_Report.pdf)
https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Beyond_Positive_Sequence_Technical_Report.pdf

Commented [RW21]: I have seen no instances where decisions regarding implementation of grid support functions depend on whether specific feeders or distribution systems have penetration levels where backflow occurs. Also, the wide-area risks of DER tripping due to transmission faults does not depend on whether individual buses have backflow. It is a matter of area-wide penetration and if area-wide penetration is 90%, there could be no backflow anywhere but yet there could be a massive post-fault generation/load mismatch.

Commented [JS22R21]: Content additions accepted with a few clarity edits on one sentence.

Commented [RW23]: Very speculative comment. How is this of particular relevance to BESS modeling?

Commented [JS24R23]: Added some text to relate to BESS modeling.

Commented [RW25]: I don't understand the particular relevance of this entire paragraph to the specific guidance related to BESS modeling. These functions are applied, or not applied, on DER of all types of energy source, and the implementation and settings of these functions are generally not different for PV and BESS.

Commented [JS26R25]: That should be the point. That the resource type isn't a factor to disaggregate for the study; however, should be logged for system scenario development (in terms of case set up and dispatch order, etc.)

Discuss as group

Commented [RW27]: Why is it assumed that trip settings for BESS and PV would differ? In general, the DP requires the same settings for all DER, or at least all inverter-based DER.

It seems that the predominate reason to disaggregate is to separate the vintages of DER: those installed according to IEEE 1547-2003 and UL-1741 versus more recent DER interconnected in accordance with IEEE 1547-2018 and/or certified to UL 1741 SA or 1741 SB.

Commented [JS28R27]: Same as above for need to review. Added content to help give examples on the vintage here, which should have been the main point.

large disturbance behavior seen at the T-D Interface was based on the difference in settings coded into the equipment and various functions enabled or disabled. This serves as the basis for the SPIDERWG recommendations for modeling more than one dominant technology type at a T-D Interface. In practical investigation, however, the SPIDERWG members noted that the technology or “fuel” type is not as important as the inverter settings for most studies. At this time, technology type (e.g., battery storage, solar PV, or super capacitors) is less important opposed to the various “smart features” that inverter manufacturers are adding to their equipment. In particular, the frequency and voltage controls. Two aggregations may be needed in order to model these controls.

~~There is an exception to focusing solely on control behavior when parameterizing for wide spread dispatch assumptions in a study. Taking BESSs as an example, the need for modeling careful parameterization of the DER models two separate aggregations is highlighted when the BESSs charging act as load while Solar solar PV DERs at the T-D Interface are producing power. In this scenario, not all DER locations have both a BESS and a Solar solar PV system, but in aggregate the T-D Interface sees a variety of motor load, electronic load, BESS charging characteristics, Solar solar PV generation output, and a variety of other impacts. Focusing on the DER portions, lumping both Solar PV output and BESS charging modes on its face is counterintuitive in the framework. Past SPIDERWG guidance has recommended planners and modelers to separate the generation components from the load components at the T-D Interface in order to move from netting the DER from load into an explicit generation record that can capture the resource’s output in simulation. When lumping the two components (i.e., Solar solar PV generating and BESS charging), the need to carefully parameterize the transient dynamic model of the lumped solar PV and BESS is enhanced in order to ensure the current commands and limits are appropriate for such a scenario. In particular, the frequency response settings of the aggregation should be checked by the TP for accuracy. result is that DER is netting with load. To prevent this, the SPIDERWG recommends to adapt the modeling framework when capturing multiple dominant operational characteristics at the T-D Interface. In this example, this would mean disaggregating the BESS charging from the Solar PV active power injection into two separate aggregations focusing on their control behavior.~~

One complicating factor for using the ~~current-present~~ modeling framework is that distribution planners typically have feeder plans to ensure the feeder remains within 0.95 and 1.05 p.u. voltage per the ANSI requirements at end-user feeds. ~~The current-present composite load model automatically adjusts the feeder impedance to ensure the end of the modeled equivalent feeder is within those boundaries. Thus, the transmission planner would need to include this adjustment in their planning practices if the TP is modeling the T-D interface explicitly to account for the electrical distance to head of feeder for the control of multiple aggregations of DER. The SPIDERWG does not consider this a deviation of the framework as it simply transitions from an automated process in the composite load model into something the TP parameterizes manually.~~

While the industry transitions between one dominant technology type to a future two or more dominant technology types (in terms of penetration at the T-D Interface), the modeling framework does not need to be adjusted; however, there are parameters that would need to be tracked and adjusted during the transition. For example, a 1MVA non-frequency regulating aggregation coupled with a 0.1 MVA of 5% droop

Formatted: Justified

Commented [RW29]: The reasons for modeling load and generation separately should not apply in the case of BESS in charging mode and other DER (PV) generating. The reasons for modeling ordinary load separate from generation is because the load dependence on voltage and frequency is no the same as inverter-based generation, and also because the tripping behavior of DER differs from that of load (which generally does not trip from a disturbance with the exception of contactor-controlled loads and stalled motors). However, a BESS in charging mode uses exactly the same power electronic converter as in the discharging mode and should have exactly the same tripping characteristics as other DER. The frequency and voltage dependencies should also be completely, or at least substantially, identical. Therefore, the suggestion that BESS should be disaggregated from other DER does not appear to be technically justified.

Commented [JS30R29]: Complete as per commenter and SPIDERWG meeting 11/1/2022

Formatted: Justified

Commented [RW31]: This may accurately be the case, but this is really stupid. Distribution systems typically have voltage regulators (small-ratio LTC autotransformers) that support feeder-end voltage, as well as capacitor banks that support voltage.

It would generally be far more accurate to leave the impedance as it is (assuming that a reasonable estimate is made of this impedance, even on a generic basis) and relax the voltage criteria.

Commented [JS32R31]: It is confirmed to be the case in load modeling. The reason software does this is due to the comment’s rationale for why it should not. Since we are modeling equivalents here, I’m not sure altering the way it is done in modeling is needed.

Complete as per commenter.

Commented [RW33]: This will make the modeled feeder impedance variable as a function of the DER dispatch, which is even more of a reason to consider this existing load model approach unrealistic.

Commented [JS34R33]: Complete as per commenter.

characteristic is a 1.1 MVA aggregation with a 55% droop bound by 1 MVA min and 1.1 MVA max¹⁸. In a practical modeling application, the above is awkward in ~~current-present~~ load modeling builds with only one input for generation as it requires aggregation of the "smart features" to be done for each ~~unique control type~~ applicable interconnection requirements of the resources. In future load models, there are plans for multiple generation components, which would make the ~~above~~ calculation step ~~above-moot~~¹⁹ for building one aggregation out of the various control features.

Recommendations

The SPIDERWG recommends that TPs and PCs use the recommended modeling framework in ~~Figure 1~~ ~~Figure X-X~~ to model multiple separate DER control aggregations behind a T-D Interface. To determine when a TP or PC can separate the aggregate DER into two or more smaller DER aggregations, the SPIDERWG recommends to ensure the following have been accomplished prior to investing the time and resources to maintain two or more aggregate models behind a T-D interface:

- The state of dynamic load modeling for that T-D interface should be of the same or higher model quality than the DER modeling component.
- The new models should be of higher quality when separated ~~than from~~ the existing aggregation and provide more information at the T-D interface separated. (e.g., tracking of frequency responsive DER)
- The percent penetration of the control to be separated should be significant at the T-D interface
- The case assumptions should be aligned with the need to separate the existing aggregation into multiple.

Further, if ~~the~~ T-D interface ~~be is~~ selected for using a method in the *Beyond Positive Sequence* technical report²⁰, the SPIDERWG recommends to walk through the following²¹:

- TPs should understand the distribution composition, distribution model, ~~load characteristics~~, and voltage/frequency control logic in order to capture the scope of distribution model buildout for their study.
- TPs should compare distribution voltage and ~~frequency~~ ~~response~~ characteristics to local transmission system characteristics and constraints to gather required data flags and information to exchange in the simulation platforms.
- TP should determine the setup convenience to build the model and interface between the distribution solver and transmission solver and note areas of long setup times.

¹⁸ Note, the higher percentage droop the larger speed (frequency) different to move the total MVA of the unit. Thus, for a 5% speed change at 55% droop, this 1.1 MVA aggregation will move 9.09% of its nameplate or 0.1 MVA, confirming that the aggregation is parameterized appropriately.

¹⁹ As the planner can simply place each separately parameterized aggregation in the model and it automatically handles the reflection of the aggregate at the T-D Interface.

²⁰ Whenever the TP moves to a more explicit model representation there is a need for increased computation power and data management needs. This is largely understood by most TPs, but is worthwhile to note that the methods in this report require more explicit model representation than the recommended model framework outside of the listed recommendations.

²¹ This is not a recommendation for or against using tools outside of positive sequence, but a list of high level determinations in order to ensure a smoother study plan.

Commented [RW35]: Again, it is the differences in control characteristics that are relevant and require disaggregation, and not usually the "fuel type".

Control characteristics are often related to vintage of interconnection, but also may differ between utility-scale and BTM DER. Most often, U-DER is located quite distant from the substation and is thus in the midst of the load. Thus, what is shown as "R-DER" in the framework would need to model both BTM (small scale) and that portion (typically the majority) of utility-scale DER that is located far out in the distribution system and is thus very inadequately modeled by the "U-DER" location shown in the SPIDER framework.

Commented [JS36R35]: SPIDERWG has members who don't see larger DER located further out on the feeder electrically, but rather closer to feeder head.

Formatted: Heading 1, Left

Formatted: Font: 12 pt

Commented [AWJ37]: I presume there is a figure that needs to be added and labeled?

Commented [JS38R37]: Yes, added.

Commented [RW39]: Is this Figure 1?

Commented [JS40R39]: Yes.

Commented [RW41]: These suggestions appear to be general to all DER representation and there is not much here that is specific to BESS representation.

Commented [JS42R41]: Yes. These are generic representation for modeling two or more aggregates, not specific to BESS but includes BESS.

Commented [AWJ43]: Should this be from?

Commented [JS44R43]: Yes

Formatted: Indent: Left: 0.5", No bullets or numbering

Commented [AWJ45]: Does this word belong?

Commented [JS46R45]: Clarity added

Commented [RW47]: Distribution frequency should not have any significant difference from transmission frequency, particularly within the response bandwidth of any DER frequency regulation characteristics.

Commented [JS48R47]: Agreed that frequency doesn't change. Response

White Paper: Parameterization of the DER_A Model for Aggregate DER

Action

Approve

Summary

This guideline provides background material on the recommended DER modeling framework, including the concepts of retail-scale DERs (R-DERs) and utility-scale DERs (U-DERs), information on relevant interconnection standards (IEEE Std. 1547-2003, IEEE Std. 1547a-2014, IEEE Std. 1547-2018, and CA Rule 21), and how the DER_A model parameters can be modified to account for a mixture of vintages of inverter-interfaced DER. The block diagram of the DER_A model is annotated and described so that Transmission Planners (TPs) and Planning Coordinators (PCs) are able to understand the relevant control logic of the dynamic model with respect to the various rules. TPs and PCs are also provided a set of recommendations for developing the modeling parameters for the DER_A dynamic model. These recommendations can also be extrapolated to Transmission Operators (TOPs), Reliability Coordinators (RCs), and other entities performing positive sequence stability simulations of the BPS where an aggregate representation of DERs is required.

The recommendations developed in this guideline are based on extensive testing of the DER_A dynamic model in the Western Electricity Coordinating Council (WECC) Modeling and Validation Work Group (MVWG) as well as industry expertise and studies discussed in detail in the NERC System Planning Impacts of DER Working Group (SPIDERWG) modeling subgroup. This guideline also serves as a useful reference for building DER models and selecting representative DER model parameters in situations where more detailed information is not yet available.

This guideline has been posted for 45 day industry comment and includes the response to those comments.

1
2
3
4
5
6
7
8
9

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Guideline

Parameterization of the DER_A Model for
Aggregate DER

December 2022

10
11
12
13
14
15
16
17
18
19

RELIABILITY | RESILIENCE | SECURITY



28
29

**3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com**

30 Table of Contents

31	Preface	iv
32	Preamble	v
33	Metrics	vi
34	Executive Summary	vii
35	Introduction	viii
36	Applicability	viii
37	Related Standards	viii
38	Purpose	viii
39	Background	ix
40	Historic DER Model Usage and Development	ix
41	DER Data Collection	ix
42	Synchronous DER Models	xi
43	Second Generation Renewable Energy System Models	xii
44	DER Modeling Framework	xiii
45	Overview of the DER_A Model	xvii
46	Chapter 1: Annotated DER_A Block Diagram	1
47	Active Power-Frequency Controls	1
48	Frequency Tripping Logic Input	1
49	Reactive Power-Voltage Controls	2
50	Active-Reactive Current Priority Logic	2
51	Example Consideration of Q Priority and P Priority	3
52	Fractional Tripping	4
53	Fractional Tripping Derivation	5
54	Voltage Source Interface Representation	8
55	Chapter 2: Parameterization of the DER_A Model	9
56	Parameterization Notes	10
57	Chapter 3: Practical DER_A Model Implementation	14
58	Chapter 4: DER_A Model Benchmarking and Testing	18
59	Appendix A: Contributors	20
60	Appendix B: References	21
61	Appendix C: DER_A Block Diagram	23
62	Guideline Information and Revision History	24
63	Errata	25

64
65
66

67 **Preface**

68
69 Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise
70 serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric
71 Reliability Corporation (NERC) and the six Regional Entities, is a highly reliable and secure North American bulk power
72 system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of
73 the grid.

74
75 Reliability | Resilience | Security
76 *Because nearly 400 million citizens in North America are counting on us*

77
78 The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table
79 below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while
80 associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



81
82

MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

83

84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99

Preamble

The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews reliability guidelines in accordance with the procedures set forth in the RSTC Charter. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact BPS operations, planning, and security. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability guidelines are not binding norms or parameters nor are they Reliability Standards; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices set forth in this guideline. Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be done with consideration of system design, configuration, and business practices.

100 Metrics

101 Pursuant to the Commission’s Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC
102 ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review
103 consistent with the RSTC Charter.
104

105 **Baseline Metrics**

106 All NERC reliability guidelines include the following baseline metrics:

- 107 • BPS performance prior to and after a reliability guideline as reflected in NERC’s State of Reliability Report and
108 Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments)
- 109 • Use and effectiveness of a reliability guideline as reported by industry via survey
- 110 • Industry assessment of the extent to which a reliability guideline is addressing risk as reported via survey
- 111

112 **Specific Metrics**

113 The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure
114 and evaluate its effectiveness, listed as follows:
115

- 116 • Ascertain use of DER_A model in planning studies
 - 117 ▪ Ascertain software used in the planning studies with the DER_A model implemented.
- 118 • Ascertain applicability of DER_A model, when using adequately parameterized models, to showcase
119 aggregate behavior of DER opposed to use of other models.
 - 120 ▪ Benchmarking of DER_A model versus a validated, more detailed representation (e.g., PSCAD
121 representation) to align at the T-D Interface, when performed¹.
- 122 • Parameterization of DER_A model using defaults or engineering judgement provided in this reliability
123 guideline versus parameters developed from field measurements or individual utilities and jurisdiction
124 requirements.
125
126

¹ This requires validation of transmission and distribution elements outside of the DERs modeled. SPIDERWG members have found that in current benchmarking efforts the validated representation is an ongoing effort to improve a variety of models and not just the dynamic response of the inverter-based DER represented by the DER_A dynamic model.

127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148

Executive Summary

This guideline provides background material on the recommended DER modeling framework, including the concepts of retail-scale DERs (R-DERs) and utility-scale DERs (U-DERs), information on relevant interconnection standards (IEEE Std. 1547-2003, IEEE Std. 1547a-2014, IEEE Std. 1547-2018, and CA Rule 21), and how the DER_A model parameters can be modified to account for a mixture of vintages of inverter-interfaced DER. The block diagram of the DER_A model is annotated and described so that Transmission Planners (TPs) and Planning Coordinators (PCs) are able to understand the relevant control logic of the dynamic model with respect to the various rules. TPs and PCs are also provided a set of recommendations for developing the modeling parameters for the DER_A dynamic model. These recommendations can also be extrapolated to Transmission Operators (TOPs), Reliability Coordinators (RCs), and other entities performing positive sequence stability simulations of the BPS where an aggregate representation of DERs is required.

The recommendations developed in this guideline are based on extensive testing of the DER_A dynamic model in the Western Electricity Coordinating Council (WECC) Modeling and Validation Work Group (MVWG) as well as industry expertise and studies discussed in detail in the NERC System Planning Impacts of DER Working Group (SPIDERWG) modeling subgroup. This guideline also serves as a useful reference for building DER models and selecting representative DER model parameters in situations where more detailed information is not yet available.

149 Introduction

150 151 **Applicability**

152 This reliability guideline is applicable to TPs, PCs, and other users of DER models for representing aggregate or stand-
153 alone inverter-based DERs.

154 155 **Related Standards**

156 The topics covered in this guideline are intended as useful guidance and reference materials as TPs and PCs create
157 DER models and modeling assumptions for use in studies generally conducted in the long-term planning and
158 operations planning horizons. While this guidance does not provide compliance guidance of any sort, the concepts
159 apply generally to the following standards:

- 160 • MOD-032
- 161 • MOD-033
- 162 • TPL-001
- 163 • PRC-006
- 164 • FAC-002
- 165 • IRO-008
- 166 • IRO-010

167 168 **Purpose**

169 With the proliferation of distributed energy resources (DER), modeling capabilities and practices should be adapted
170 and refined so that transmission planning and operations planning engineers can differentiate between actual end-
171 use loads and DER resources. In the past, and at lower penetrations of DER integrating into the distribution system,
172 net load reduction has been used. Net load reduction is the result of the same or greater demand with an offset due
173 to DER. However, these practices may not be sustainable moving forward as the distribution system continues to
174 integrate more DER. Increasing DER penetration will impact the BES, resulting in changes in transmission loading
175 levels, voltage regulation, and determination of operating limits. It is important to accurately represent the total end-
176 use load and its composition, and model the amount of DER as a separate resource. This will allow entities to
177 adequately represent the impact of future DER integration as well as the performance of DER during transmission
178 system events. Distribution Providers (DPs) should coordinate with their Transmission Planners (TPs) and Planning
179 Coordinators (PCs) to ensure sufficient data for load composition and DER resources is provided, as necessary, for
180 reliable planning and operation of the BES. While many of these resources are not considered BES, sharing of this
181 information is important for developing representative models and performing system studies².

182
183 The purpose of this guideline document is to provide a common framework and modeling parameterization for the
184 DER_A dynamic model for entities to consider for modeling DER in transient stability and powerflow simulations. The
185 framework recommended in this guideline is expected to be particularly useful for representing load and DER in
186 Interconnection-wide studies. More detailed, localized studies may require additional or more advanced modeling,
187 as deemed necessary or appropriate. The modeling practices described here may also be modified to meet the needs
188 of particular systems or utilities, and are intended as a reference point for Interconnection-wide modeling practices.
189

² Transmission planning simulations take into account both BES and non-BES equipment in order to accurately depict the impact on the BES. While DERs are inherently non-BES (as they connect to the distribution system), modeling information is required in order to represent the resources in simulation.

Background

The NERC DERTF published a report³ in February 2017 that focused on connection modeling and reliability considerations for DER. The report provided definitions of DERs, an overview of data and modeling needs, characteristics of nonsynchronous DERs, and potential reliability impacts of DERs on the BPS.

The NERC LMTF⁴ worked in coordination with the NERC DERTF, and published two detailed guidelines on modeling DERs as either stand-alone generating resources or as part of the CLM:

- The *Reliability Guideline: Modeling DER in Dynamic Load Models*, published in December 2016, established a framework for modeling DERs in steady-state powerflow and dynamic simulations.
- The *Reliability Guideline: Distributed Energy Resource Modeling*, published in September 2017, utilized the framework established in the preceding guideline, and provided default parameter values for various DER dynamic models.

At the time of development of that guideline, the DER_A model was still under development and testing and was therefore only briefly mentioned. With the DER_A model now implemented and tested across the major commercial software vendors, the SPIDERWG provided background and guidance on parameterizing the DER_A model for representing aggregate or stand-alone inverter-based DER resources. This was published in the *Reliability Guideline: Parameterization of the DER_A Dynamic Model*.

This reliability guideline, titled *Reliability Guideline: Parameterization of the DER_A Dynamic Model for Aggregate DER*, combines the two LMTF/DERTF reliability guidelines with the SPIDERWG reliability guideline to provide the same technical guidance, but housed in one document. This was done as part of an effectiveness and efficiency review in the RSTC.

The following sections briefly describe the DER modeling framework and the definitions and terminology used in that framework. Further, definitions that are used in multiple SPIDERWG documents are posted to the SPIDERWG webpage and are useful for understanding the terms used in this guideline⁵. Models used prior to the DER_A model are also summarized below. Guidance contained in the background and chapters of this document are focused to TPs and PCs; however, other users of the DER_A dynamic model such as RCs and TOPs can also find this guidance useful to their studies.

Historic DER Model Usage and Development

DER model development for use in transmission planning models began with a framework and dynamic model behavior to represent the resources on the distribution system. While some synchronous facilities exist, the historical information has shown that solar PV has been and continues to be the largest technology type of DER. This section describes an overview of data collection for various uses of a DER model.

DER Data Collection

Tps and PCs are required to collect steady-state and dynamic models for Interconnection-wide base case creation. As part of this process, as outlined in MOD-032-1, each PC and each of its TPs jointly develop data requirements and reporting procedures for the PC's planning area. In addition to the aggregate demand collected from the Distribution Provider (DP), accurate modeling of DER should also be included in the data collection process. Accurate modeling of DER as part of the overall demand and load composition is critical for accurate and representative modeling of the overall end-use load in both the powerflow and dynamics cases. DPs (and RPs, if applicable) should coordinate with their respective TP and PC to provide sufficient data to accurately represent the aggregate loads, aggregate R-DER

³ https://www.nerc.com/comm/Other/essntlrbltysrvkstskfrDL/Distributed_Energy_Resources_Report.pdf.

⁴ [https://www.nerc.com/comm/PC/Pages/Load%20Modeling%20Task%20Force%20\(LMTF\)/Load-Modeling-Task-Force.aspx](https://www.nerc.com/comm/PC/Pages/Load%20Modeling%20Task%20Force%20(LMTF)/Load-Modeling-Task-Force.aspx).

⁵ Available here: <https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Terms%20and%20Definitions%20Working%20Document.pdf>

and distinct U-DER in their system for both steady-state and dynamic models. At a minimum, TPs and PCs should have the following information related DER (also reproduced in [Table I.1](#)):

- DER modeled as U-DER
 - Type of generating resource (e.g., reciprocating engine, wind, solar PV, battery energy storage)
 - Distribution bus nominal voltage where the U-DER is connected
 - Feeder characteristics for connecting U-DER to distribution bus, if applicable
 - Location, both electric and geographic. Related to bulk system bus
 - Capacity of each U-DER resource (Pmax, Qmax, rated MVA, rated power factor, capability curve of U-DER reactive output with respect to different real power outputs down to Pmin)
 - Vintage of IEEE 1547 (e.g., -2018) or other relevant interconnection standard requirements that specify DER performance of legacy and modern DER (e.g., CA Rule 21)
 - Actual plant control modes in operation – voltage control, frequency response, active-reactive power priority
- DER modeled as R-DER
 - Type of generating resource (e.g., reciprocating engine, wind, solar PV, battery energy storage)
 - Aggregate capacity (Pmax, Qmax) of R-DER behind the T-D Interface and a reasonable representation of the aggregate “capability curve” of reactive output with respect to different real power outputs down to Pmin.
 - Location, both electric and geographic. Related to bulk system bus
 - Vintage of IEEE 1547 (e.g., -2018) or other relevant interconnection standard requirements that specify DER performance of legacy and modern DER (e.g., CA Rule 21)

Table I.1: Data Collection Applicability to U-DER and R-DER

Description	U-DER	R-DER
Type of generating resource (e.g., reciprocating engine, wind, solar PV, battery energy storage)	X	X
Distribution bus nominal voltage	X	
Information characterizing the distribution circuits (X, R)	X	X
Capacity and capability (Pmax, Qmax, reactive capability with respect to real power output)	X	X
Rating (rated MVA, rated power factor)	X	X
Vintage of IEEE 1547 (e.g., -2018) or other relevant interconnection standard requirements that specify DER performance of legacy and modern DER (e.g., CA Rule 21)	X	X
Control modes – voltage control, frequency response,	X	
Location (electrical bus and geographic area)	X	X

Note: The technical capabilities and default settings of R-DER for frequency response, volt/var control, and P/Q priority as specified by the revised IEEE Std 1547 should also be considered

This information will help the PC, and TP in more representative modeling⁶ of U-DER and R-DER. In situations where this data is not readily available, the entities should use engineering judgment to map the model parameters to expected types of operating modes. The technical capabilities and default settings of R-DER for frequency response, volt/var control, and P/Q priority as specified by the revised IEEE Std 1547 should also be considered.

⁶ In some instances a complete dynamic and steady-state model can be provided should the TP and PC allow and approve of it. In this case, much of the listed equipment information, as well as supplemental protection and other models, can be placed inside the file without needing to report the information to the TP/PC outside of the model submittal.

Further, while the above has been focused on TPs and PCs, DER models are available in the software tools that are used by Reliability Coordinators (RCs) and Transmission Operators (TOPs) in order to perform their Real-time Analyses (RTAs), and Operational Planning Analyses (OPAs). Should the RC desire to model aggregate DER at one of their monitored buses in simulation, the guidance on parameterizing the model should be applicable to describe the powerflow and transient dynamic behavior.

Synchronous DER Models

Small, synchronous DER connected at the distribution level can be modeled using standard synchronous machine models. TPs and PCs should determine if any synchronous DER should be modeled, as applicable, and develop reasonable model parameters for these resources in coordination with the DPs as necessary. It is recommended to use the genqec model for representing synchronous machines⁷. The classical machine model, gencls, should not be used to model DER to avoid any unintentional poorly damped oscillations. In most situations, a generator model alone will capture the dynamic behavior of the machine in sufficient detail; however, if data is available and the PC or TP find it necessary, a suitable governor and excitation system may also be modeled. Table I.2 shows examples of model parameters for a steam unit, small hydro unit, and gas unit for reference. These default parameters are used solely as a base set to start from assuming zero information about the synchronous DER. These parameters should change in order to accurately represent the characteristics of the synchronous DER to be modeled.

Table I.2: Synchronous DER Default Model Parameters

Parameter	Steam	Small Hydro	Gas	“Really Small”
MVA	14	32	15	5
T'd0	6	6	6.5	7
T''d0	0.035	0.027	0.03	0.03
T'q0	1	0	1	0.75
T''q0	0.035	0.065	0.03	0.05
H	3	1.7	4.2	3
D	0	0	0	0
Xd	1.8	1.45	1.6	2.1
Xq	1.7	1.05	1.5	2.0
X'd	0.2	0.47	0.2	0.2
X'q	0.4	1.05	0.3	0.5
X''d	0.18	0.33	0.13	0.18
X''q	0.18	0.33	0.13	0.18
Xl	0.12	0.28	0.1	0.15
S(1.0)	0.2	0.2	0.1	0.05
S(1.2)	0.6	0.6	0.4	0.3

The tripping profile of IEEE 1547 is applicable for synchronous DER for the states that have adopted the standard. As most states adopted the 1547-2003 version, the tripping profiles for synchronous DER are more likely to behave like that version of the standard. For states that have adopted 1547-2018, the trip profiles are applicable to synchronous

⁷ The model parameters listed may not be a complete set for genqec; however, the other parameters are more suited for limitations on bulk equipment, and the software defaults are adequate for default parameters. Still, should the resource require alterations from the listed table, the general guidance to adapt the parameters to model the equipment still holds.

DER as well as inverter-based DER. Parameterization of the voltage thresholds on these models can be parameterized to account for the tripping assumptions in this reliability guideline.

As there is a potential to aggregate an amount of synchronous DER (using synchronous models) akin to the inverter-based DER (modeled by DER_A), the same guidance in the chapters below hold with respect to altering the parameters based on engineering judgement to reflect the aggregate behavior of that particular T-D composition. The synchronous models are not directly an aggregate model⁸, so care will be needed in parameterizing the models to reflect aggregate behavior and supplemental models may be needed. The T-D Interface represents a variety of points of interconnection for synchronous DER and an aggregate model is a suitable representation; however, the TP or PC can model all synchronous DER individually as indicated in the DER Modeling Framework section below.

Second Generation Renewable Energy System Models

The second generation generic renewable energy system models were developed between 2010 and 2013 and have since been adopted by the most commonly used commercial software vendors. The suite of models that have been developed can be used to model different types of renewable energy resources, including:

- Type 1 Wind Power Plants
- Type 2 Wind Power Plants
- Type 3 Wind Power Plants
- Type 4 Wind Power Plants
- Solar PV Power Plants
- Battery Energy Storage Systems (BESS)

These models were originally developed to represent large utility-scale resources connected to the BPS at transmission level voltage⁹, and provide the greatest degree of flexibility and modeling capability from the commercial software vendor tools using generic models. However, the flexibility also results in a significant number of settings and controls that must be modeled that may be cumbersome for representing DER. If modeling DER using the second generation models, a set of generic parameters can be used for specific studies such as generation interconnection system impact studies (e.g., large capacity resources relative to the local interconnecting network) or other special studies. The generic models for these studies should be accompanied by sufficient model and parameter validation for large DER owners to ensure the model represents the installed equipment.

Where actual equipment is to be modeled, specific data from the equipment vendor or at least an understanding of the actual equipment control strategy and performance (e.g., constant power factor control vs. voltage control) is extremely important and should be used. The dynamic behavior of renewable energy systems that are connected to the grid using a power electronic converter interface (i.e., Type 3 and Type 4 wind turbine generators, solar PV, and battery storage) are dominated by the response of the power electronic converter. The converter is a power electronic device and its dynamic response is more a function of software programming than inherent physics as in the case of synchronous machines. Therefore, the concept of default and typical parameters is much less applicable to renewable energy systems than other technologies¹⁰. For example, setting `lvplsw = 1` describes the flag that turns on low voltage power logic and is used to emulate the behavior typical of some vendor equipment under low voltage conditions. However, `lvplsw` is a function of the software and vendor controls in the power converter, and should be

⁸ It is not anticipated to impose major functional differences in response when using the `genqec` model as an aggregate model. However, parameters changes are expected and care needs to be taken when adjusting to represent aggregate behavior. It is not anticipated to have a consequential impact in simulation at this time due to the lower share of synchronous DER in the totality of the DER on the system.

⁹ P. Pourbeik, J. Sanchez-Gasca, J. Senthil, J. Weber, P. Zadehkhosht, Y. Kazachkov, S. Tacke, J. Wen and A. Ellis, "Generic Dynamic Models for Modeling Wind Power Plants and other Renewable Technologies in Large Scale Power System Studies", IEEE Transactions on Energy Conversion, published on IEEE Xplore 12/13/16, DOI 10.1109/TEC.2016.2639050.

¹⁰ Generic models representing renewable energy systems include a common model structure that allows for representing different types of control strategies and characteristics. These models can be tuned or configured to represent specific vendor equipment by adjusting the model parameters.

set according to the respective vendor characteristics to be emulated, if that information is available. The default example values in software for modeling DER as a second generation renewable model should be altered to reflect the distribution-connected alterations and equipment settings. This reliability guideline focuses on the der_a dynamic model, which is a model to represent aggregate dynamic behavior. These second generation renewable models are more appropriate for single plant representations. The SPIDERWG recommends the use of the der_a dynamic model for representing aggregate DERs in simulation¹¹ rather than using the second generation renewable models, which could be used for representation of a single, larger plant connected to the distribution system.

DER Modeling Framework

For the purposes of steady-state and dynamic modeling of DERs in BPS reliability studies, DERs can be defined as either utility-scale DERs, U-DERs, or R-DERs, defined as follows:

- **U-DER:** DERs directly connected to, or closely connected to, the distribution bus¹² or connected to the distribution bus through a dedicated,¹³ non-load serving feeder. These resources are typically three-phase interconnections and can range in capacity (e.g., 0.5 to 20 MW).
- **R-DER:** DERs that offset customer load, including residential,¹⁴ commercial, and industrial customers.¹⁵ Typically, the residential units are single-phase while the commercial and industrial units can be single- or three-phase facilities.¹⁶

Both U-DERs and R-DERs can be differentiated and should be accounted for in powerflow base cases and dynamic simulations. Modeling U-DERs and R-DERs in the powerflow provides an effective platform for linking this data to the dynamics records and ensuring that the dynamics of these resources are accounted for. R-DERs represent the truly distributed resources throughout the distribution system whose controls are generally reflective of IEEE Std. 1547¹⁷ vintages or other relevant requirements for the region they are being interconnected. U-DERs are typically relatively large, stand-alone installations that may have more complex controls or requirements associated with their interconnection. The vintage of IEEE Std. 1547 is an indicator for a large set of controls; however, the interconnection requirements of that local area may be over and above, so looking at the requirements of a particular interconnection for these larger, stand-alone installations will be a better representation of the equipment's operation. That said, IEEE 1547 would be applicable to the equipment, and any settings would be above and beyond.

¹¹ It is possible to use the der_a model to represent a single plant; however, careful parameterization is required to ensure the aggregate dynamic model is properly representing the single plant.

¹² The distribution bus is connected to a transmission voltage bus via the transmission/distribution transformer. Resources not directly connected to this bus do not meet the criteria for this definition.

¹³ In some cases, U-DERs may not be located on a dedicated feeder; rather, U-DERs may be installed on the load-serving feeders near the head of the feeder. In either case, the framework presented here can and should be adapted to each TP and PC needs. In this case, these larger DER installations can still be represented as U-DERs. In other cases, they may be better suited to be modeled as R-DERs. Engineering judgment should be used to determine which modeling approach is most appropriate.

¹⁴ This also applies to community DERs that do not serve any load directly but are interconnected directly to a distribution load serving feeder.

¹⁵ This often includes behind the meter generation but may also include individually metered DERs and systems that export beyond customer load at a particular site boundary.

¹⁶ For the purposes of modeling, some larger utility-scale U-DER may exist along the load-serving distribution feeder and may be electrically distant from the distribution substation. In these cases, they may be represented as R-DERs since they offset customer load. The aggregate power output can potentially exceed the total load demand of the distribution feeder.

¹⁷ IEEE Std. 1547-2003, Standard for Interconnecting Distributed Resources with Electric Power Systems, July 2003:

<https://standards.ieee.org/standard/1547-2003.html>.

IEEE Std. 1547a-2014, IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems – Amendment 1, May 2014:

<https://standards.ieee.org/standard/1547a-2014.html>,

IEEE Std. 1547-2018, IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, April 2018: <https://standards.ieee.org/findstds/standard/1547-2018.html>.

IEEE Std. 1547-2018, 6/4/2018: Errata to IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces: http://standards.ieee.org/findstds/errata/1547-2018_errata.pdf.

357 TPs and PCs should identify thresholds where U-DERs should be explicitly modeled and R-DERs should be accounted
 358 for in the powerflow and dynamics cases. The thresholds should be based on either the individual or aggregate impact
 359 of DER on the BPS:¹⁸

- 360 • Gross aggregate nameplate rating of an individual U-DER facility directly connected to the distribution bus or
 361 interconnected to the distribution bus through a dedicated, non-load serving feeder
- 362 • Gross aggregate nameplate rating of all connected R-DERs that offset customer load including residential,
 363 commercial, and industrial customers

364
 365 The thresholds for modeling U-DERs and R-DERs, determined using engineering judgment¹⁹, can be defined as
 366 follows:

- 367 • **U-DER Modeling:** Any individual U-DER facility rated at or higher than the defined individual U-DER modeling
 368 threshold should be modeled explicitly in the powerflow case at the low-side of the transmission–distribution
 369 transformer. A dynamics record should be used to account for the transient behavior²⁰ of the individual U-
 370 DER plant. Individual U-DERs less than the defined threshold should be accounted for in powerflow and
 371 dynamics as an R-DER (as described below). Multiple similar U-DERs connected to the same substation low-
 372 side bus could be modeled as an aggregate resource as deemed suitable by the TP or PC. This is also a good
 373 modeling practice to aggregate DER that is closer to the feeder head and would have less impact by the
 374 modeled feeder equivalent in the simulation. Facilities that are lower than the individual modeling threshold
 375 should either be modeled as R-DERs or as a separate aggregation near the feeder head in the framework.
- 376 • **R-DER Modeling:** If the gross aggregate nameplate rating of R-DERs connected to a feeder exceeds the
 377 defined R-DER modeling threshold defined in the TP and PC modeling practices, these R-DERs should be
 378 accounted for in dynamic simulations as part of the dynamic load model. While this may not require any
 379 explicit model representation in the powerflow base case, the amount of R-DERs can be accounted for as
 380 part of the powerflow load record and integrated into the dynamic model as an explicit DER component. The
 381 threshold for modeling R-DER should be 0 MVA, meaning that all forms of DERs be accounted for (and not
 382 netted with the load) to the extent possible. Further, this does not mean that a single generator record is
 383 required for each R-DER. Rather, establishing a threshold of 0 MVA for R-DER means that a TP or PC should
 384 represent all DER in their system²¹.

386 **Figure I.1** shows the recommended powerflow representation for accounting for U-DERs. The left side of **Figure I.1**
 387 shows the conventional powerflow representation of the load record. This has conventionally included both load and
 388 DERs (representing a net load quantity as opposed to a gross load quantity). However, the right side of **Figure I.1**
 389 shows how the transmission–distribution (T–D) transformer can be modeled explicitly and the gross load can be
 390 moved to the low side distribution bus. U-DERs above the specified threshold can be modeled explicitly via their own
 391 step-up transformers as applicable. If the U-DERs are connected through a dedicated feeder or circuit to the low-side
 392 bus, then that would also be explicitly modeled in the powerflow.

¹⁸ This may include many different types of DERs, including distributed solar PV, energy storage, synchronous generation, and other types of DERs. Including synchronous generation in the CLM as a component of R-DERs may not be possible across all software platforms.

¹⁹ SCADA data points and monitoring of native load may provide some level of engineering judgement for the amount of DER that is represented by one load record. However, determination of nameplate ratings to represent in models requires further data collection practices. TPs and PCs should interface with their DPs to obtain known DER capacities and determine the gross aggregate nameplate for their simulations.

²⁰ Depending on complexity of the actual U-DER, for inverter coupled U-DER, more sophisticated models such as the second generation generic renewable energy system models may also be used (i.e., regc_a, reec_b and repc_a). Other U-DERs (e.g., synchronous natural gas or steam-turbine generators) can also be modeled using standard models available in commercial software platforms.

²¹ TPs and PCs should establish this zero MVA threshold as a best practice for modeling as it requires data collection of resources prior to needing modeling information past a non-zero threshold. It has been reported that information needed from facilities after the non-zero threshold has been met is limited and model development is restricted for the facilities that were interconnected under that limit. The zero MVA threshold prevents data loss like this from occurring.

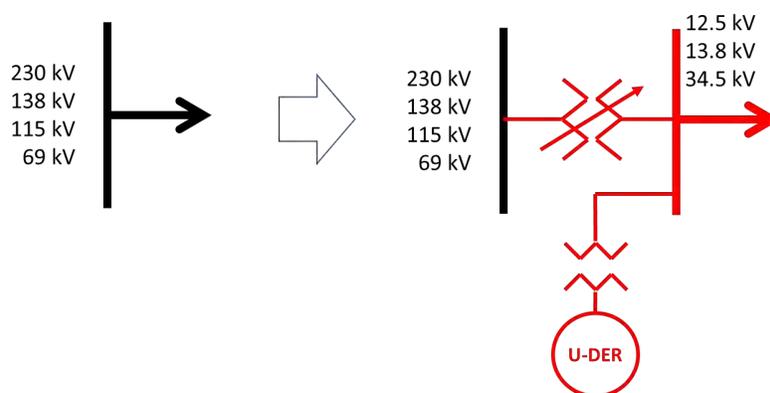


Figure I.1 Representing U-DER in the Powerflow Base Case

To capture the R-DER in the powerflow, the load records now²² have the capability to input the R-DER quantity along with the gross load amount. Figure I.2 shows an example of the R-DERs included in the powerflow load records. The red box shows the R-DERs specified and the blue box shows the net load equal to the actual load minus the R-DERs. For example 80 MW and 20 MVar of actual load with 40 MW and 0 MVar of R-DER at Bus 2.

	Number of Bus	Name of Bus	Area Name of Load	Zone Name of Load	ID	Status	MW	Mvar	MVA	S MW	S Mvar	Dist Status	Dist MW Input	Dist Mvar Input	Dist MW	Dist Mvar	Net Mvar	Net MW
1	2	Two	Top	1	1	Closed	80.00	20.00	82.46	80.00	20.00	Closed	40.00	0.00	40.000	0.000	20.000	40.000
2	3	Three	Top	1	1	Closed	220.00	40.00	223.61	220.00	40.00	Open	110.00	0.00	0.000	0.000	40.000	220.000
3	4	Four	Top	1	1	Closed	160.00	30.00	162.79	160.00	30.00	Closed	80.00	0.00	80.000	0.000	30.000	80.000
4	5	Five	Top	1	1	Closed	260.00	40.00	263.06	260.00	40.00	Open	130.00	0.00	0.000	0.000	40.000	260.000
5	6	Six	Left	1	1	Closed	400.00	0.00	400.00	400.00	0.00	Closed	200.00	0.00	200.000	0.000	0.000	200.000
6	7	Seven	Right	1	1	Closed	400.00	0.00	400.00	400.00	0.00	Closed	200.00	0.00	200.000	0.000	0.000	200.000

Figure I.2: Capturing R-DER in the Powerflow Load Records [Source: PowerWorld]

Once represented in the powerflow base case, data for the CLM can be modified to account for explicit representation of the DERs and the T/D transformer. Figure I.3 shows the dynamic representation of the CLM, where the distribution transformer impedance is not represented in the dynamic load record. Rather, it is modeled explicitly in the powerflow to accommodate one or more U-DER.²³ Any load tap changer (LTC) modeling²⁴ would be done outside the CLM, such as enabling tap changing in the powerflow²⁵ and using the *ltc1* model in dynamic simulations. Motor load and the distribution equivalent are modeled as part of the CLM, and the R-DERs are represented at the load bus based on the data entered in the load record table.

²² All commonly used commercial simulation software platforms now have the ability to represent DERs as part of the powerflow load record in an attempt to standardize and unify modeling practices for representing DERs in powerflow base cases.

²³ If only R-DERs are represented at a bus (no U-DERs), then the T-D transformer does not necessarily need to be explicitly modeled in the powerflow since it can be accounted for in the CLM dynamic record, including LTC action. However, if LTC action needs to be modeled in the steady-state analyses in any way, then explicit modeling of the T-D transformer in the powerflow may be needed.

²⁴ Utilities using transformers without under-load tap changers (ULTCs) capability but with voltage regulators at the head of the feeder could model this in the CLM with a minimal transformer impedance but active LTCs to represent the voltage regulator.

²⁵ For example, by specifying settings in the transformer record and enabling tap changing in the powerflow solution options.

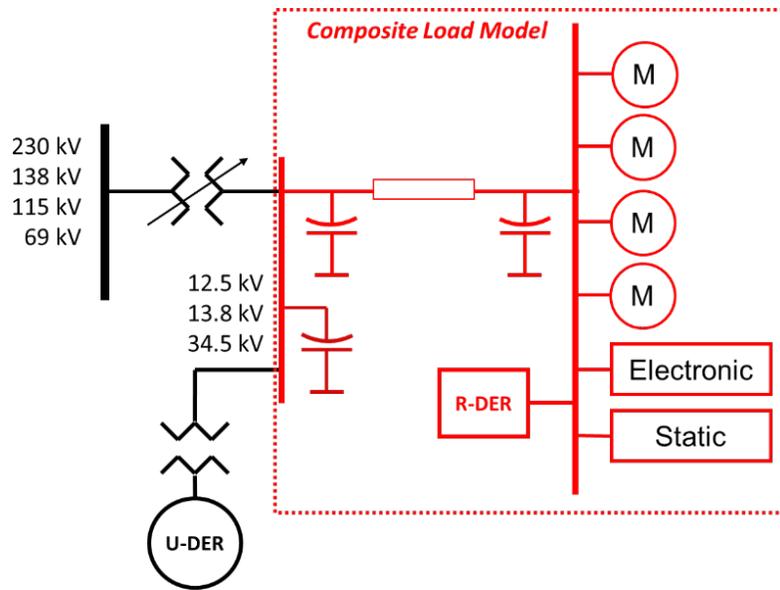


Figure I.3: CLM Representation with U-DER Represented in the Powerflow Base Case

With FERC Order 2222²⁶ introducing the DER Aggregator, the initial starting split of capacity and the type of information provided from such entities. SPIDERWG has produced a white paper that has highlighted some BPS reliability tie-ins to DER Aggregators; however, when parameterizing the steady state representation, logical flow charts as in Figure I.4 assist in providing planners a way to disaggregate information provided from a DP or a DER aggregator for representation in transmission cases. These logical flows, in short, provide a crude method to begin placed DER into model representations. It is to be noted that these percentage splits in Figure I.X are to be considered as initial default values and modifications to the values may be necessary based on the information received from a DP or a DER Aggregator.

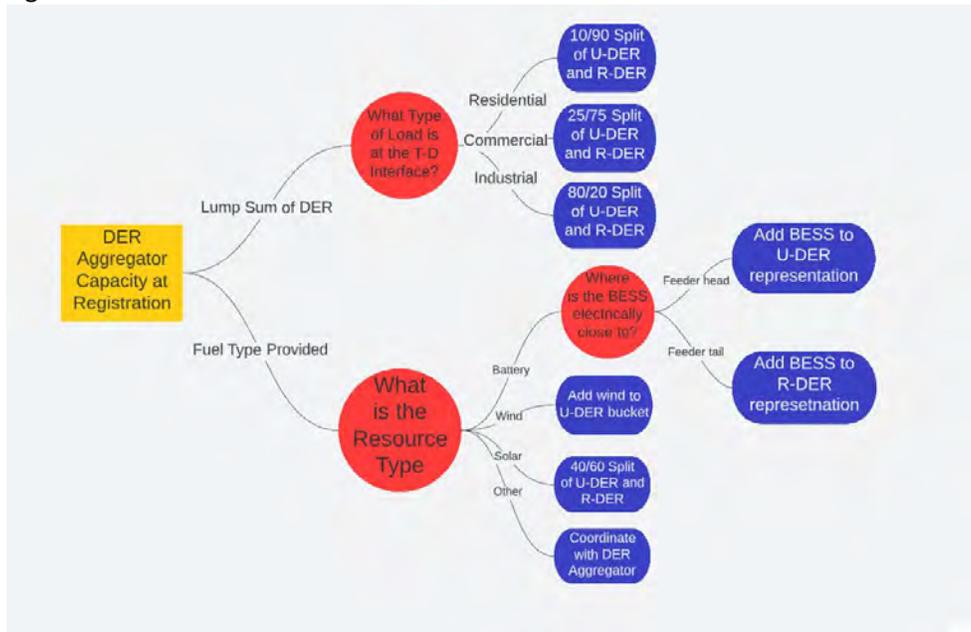


Figure I.4: Decision tree for DER Disaggregation

²⁶ The text of this order can be found here: https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf

424 Overview of the DER_A Model

425 The DER_A model is a simplified version of the second generation generic renewable energy system models (i.e.,
426 regc_a, reec_b, repc_a, lhvrt, lhfrt) used to represent inverter-based DERs (i.e., utility-scale wind, solar photovoltaic
427 (PV), and battery energy storage resources). The DER_A model uses a reduced set of parameters meant to represent
428 the aggregation of a large number of inverter-interfaced DERs. It is also an improvement over the pvd1 model in that
429 it includes additional modeling flexibility for more advanced and representative capabilities introduced in IEEE Std.
430 1547-2018 and California Rule 21. The DER_A model can be used to represent U-DERs (individual DER resources, or
431 a group of similar U-DERs) and can also be used to represent R-DERs as either a standalone DER dynamic model or as
432 part of the CLM. The DER_A model includes the following features:

- 433 • Constant power factor and constant reactive power control modes (allows voltage control to be active along
434 with PF/Q control, depending on whether voltage is within the deadband or not)
- 435 • Active power-frequency control with droop and asymmetric deadband
- 436 • Voltage control with proportional control and asymmetric deadband (may be used to either represent
437 steady-state voltage control or dynamic voltage support, depending on chosen time constants)
- 438 • Representation of a fraction of resources tripping or entering momentary cessation²⁷ at low and high voltage,
439 including a four-point piece-wise linear gain (partial tripping includes a timer feature as well)
- 440 • Representation of a fraction of resources that restore output following a low or high voltage or frequency
441 condition (representation of legacy trip and modern ride-through capabilities in a single model)
- 442 • Active power ramp rate limits during return to service after trip or enter service following a fault or during
443 frequency response
- 444 • Active-reactive current priority options (used to represent dynamic voltage support during fault events)
- 445 • The capability to represent generating or energy storage resources²⁸ (The model allows for absorption of
446 active power; however, charging and discharging as modeled in reec_c is not included. Therefore, the DER_A
447 model should not be used for devices with only a few seconds of energy injection (e.g., super capacitor
448 systems)

449 The overall block diagram for the DER_A model can be found in [Appendix C](#)
450
451

²⁷ Momentary cessation is a mode of operation during which no current is injected into the grid by the inverter during low or high voltage conditions outside the continuous operating range. This leads to no current injection from the inverter, and therefore, no active or reactive current (and no active or reactive power). Refer to the NERC *Reliability Guideline: BPS-Connected Inverter-Based Resource Performance*. The concept applies to both BPS-connected inverter-based resources and DERs:
https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Inverter-Based_Resource_Performance_Guideline.pdf.

²⁸ This guideline focuses mostly on using the DER_A model to represent generating resources, primarily distributed solar PV generation. However, the DER_A model can be used to represent energy storage, and future guidelines may be developed on this topic as necessary.

Chapter 1: Annotated DER_A Block Diagram

This chapter briefly describes the functional sections of the DER_A model and provides a high-level overview of what the various blocks represent. Refer to the DER_A specification document²⁹ for more detailed information regarding implementation. The sections below describe the general control aspects of the different functional sections of the model.

Active Power-Frequency Controls

The active power-frequency controls portion of the DER_A model are shown in **Figure 1.1**. The frequency input signal feeding the active-power frequency controls is first passed through a frequency measurement time constant, Trf . The filtered voltage is compared against a reference signal. The $fdbd1$ and $fdbd2$ parameters represent the active power-frequency control deadband for overfrequency and underfrequency, respectively. The Ddn and Dup parameters represent the overfrequency and underfrequency droop gains, respectively. Tp represents an active power measurement time constant. When active power-frequency control is enabled, $Freq_flag$ is set to 1. To disable active power-frequency control of the model, set $Freq_flag$ to 0. The frequency error is limited by $femax$ and $femin$ and goes through a PI controller with Kpg and Kig parameters. The $dPmax$ and $dPmin$ parameters limit active power upward and downward ramp rates. $Pmax$ and $Pmin$ represent the maximum and minimum power output, respectively. $Tpord$ is the power-order time constant, and it can be used to represent the small time lag for changing the power reference (when $Freq_flag = 0$) or the open-loop time constant associated with the full controls (when $Freq_flag = 1$), as specified in IEEE Std. 1547-2018. Active current command ($ipcmd$) is calculated using power-order ($Pord$) divided by filtered terminal voltage (Vt_filt), and it is limited by $Ipmax$ and $Ipmin$.

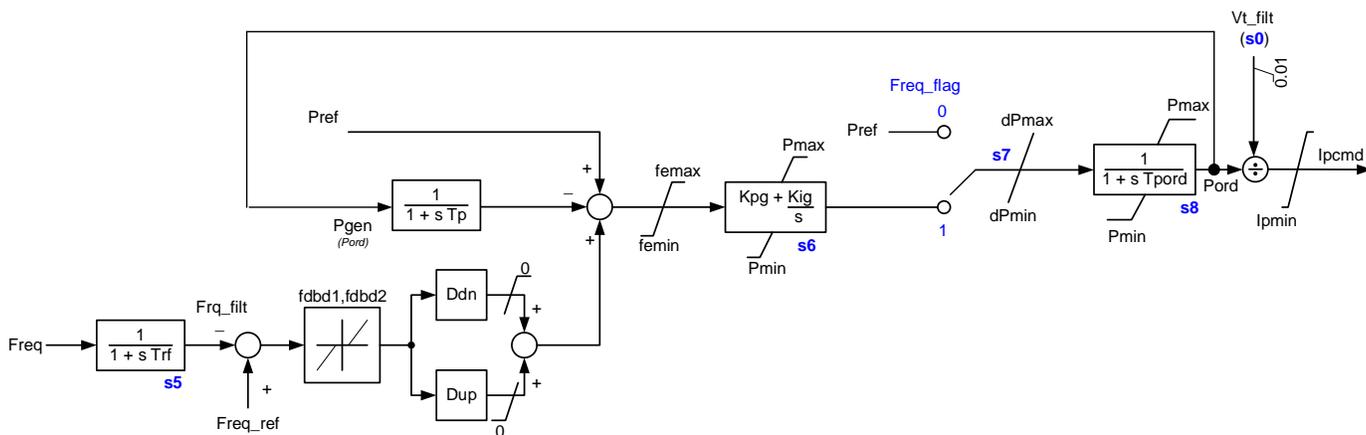


Figure 1.1: Active Power-Frequency Controls

Frequency Tripping Logic Input

The frequency input signal feeding the active-power frequency controls is first passed through a frequency measurement time constant, Trf . A low voltage inhibit logic was added to the model, which is shown in **Figure 1.2**. When voltage falls below a threshold (Vpr), then the frequency relay model is bypassed. This is common in frequency protective functions, to avoid spurious tripping during transients. In numerical simulations, this low voltage inhibit is also used to avoid tripping on numerical spikes during discontinuities.³⁰

²⁹ P. Pourbeik, "Proposal for DER_A Model," June 19, 2019: https://www.wecc.org/Reliability/DER_A_Final_061919.pdf.

³⁰ https://www.wecc.biz/Reliability/WECC_White_Paper_Frequency_062618_Clean_Final.pdf

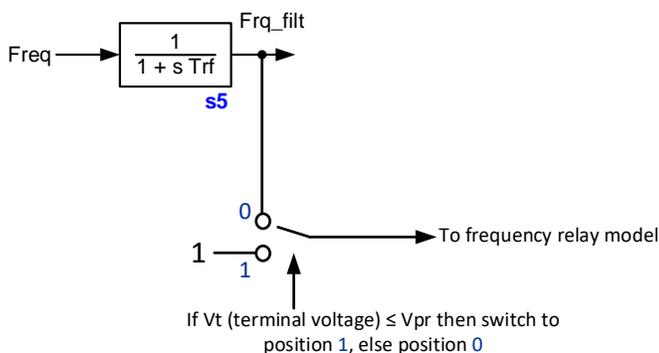


Figure 1.2: Frequency Tripping Logic Controls

Reactive Power-Voltage Controls

The reactive power-voltage controls portion of the DER_A model are shown in Figure 1.3. Setting *pflag* to 0 or 1 selects either constant reactive power control or constant power factor control, respectively. The *pfaref* parameter is internally calculated to achieve the necessary reactive power order for the current active power order. Reactive power is then divided by filtered terminal voltage (*Vt_filt*) and passed through a reactive current calculation time constant (*Tiq*). Voltage control is included in the model. Terminal voltage (*Vt*), after a measurement time constant (*Trv*), passes through a lower (*dbd1*) and upper (*dbd2*) deadband and proportional control gain (*Kqv*). Respectively, *Iqh1* and *Iql1* specify maximum and minimum limits of reactive current injection. To disable the reactive power-voltage control function of the model, set *Kqv* to 0.

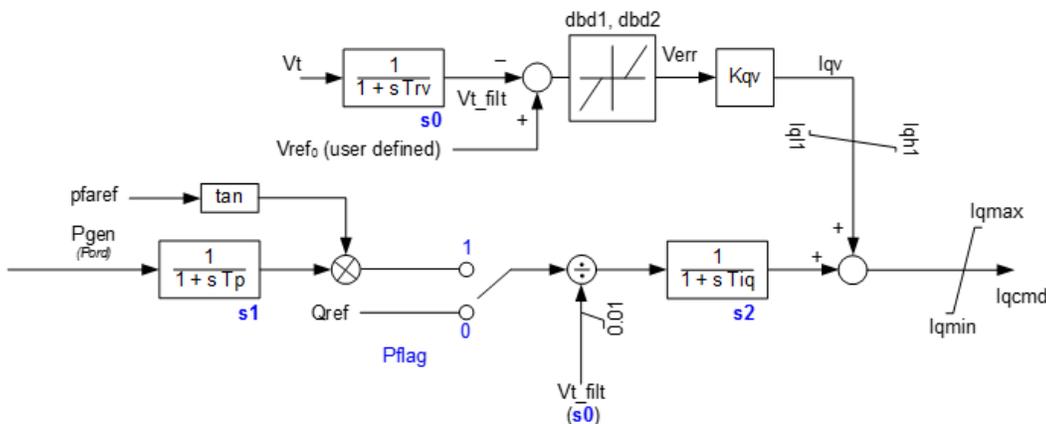


Figure 1.3: Reactive Power-Voltage Controls

Active-Reactive Current Priority Logic

With the active and reactive command values established in the active power-frequency and reactive power-voltage control elements, the command values are passed through maximum (*Ipmax/Iqmax*) and minimum (*Ipmin/Iqmin*) active and reactive current limits. Figure 1.4 shows the current limit logic and how that logic interacts with the limiters. When the *typeflag* parameter is set to 1, this denotes a DER that is a generating unit with *Ipmin* = 0 while setting it to 0 denotes a DER that is an energy storage device with *Ipmin* = -*Ipmax*.

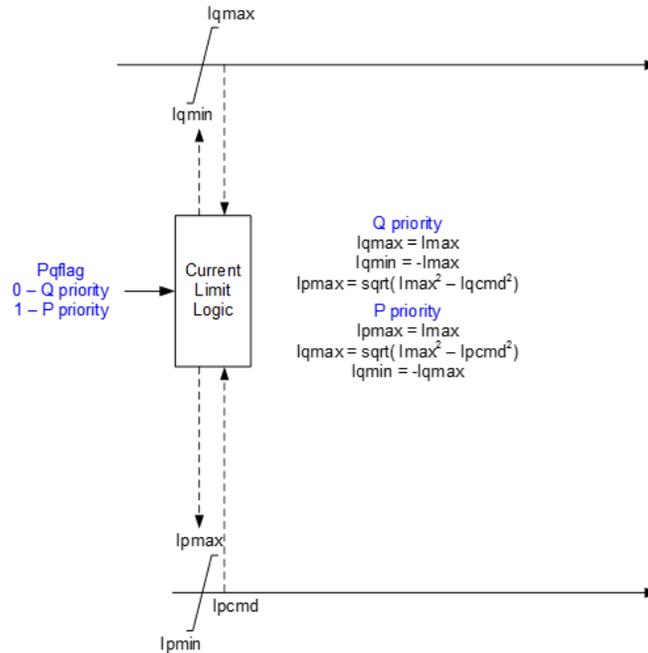


Figure 1.4: Active-Reactive Current Priority Controls

Current limits, particularly in inverter-based resources, determine how the resource response to large grid disturbances, such as faults on the BPS. The current limit logic is determined based on whether the resource is operated in active or reactive current priority and dictated by the *pqflag* parameter. The priority logic controls I_{qmax} and I_{qmin} based on the priority setting and maximum total current of the inverter (I_{max}). Figure 1.4 also shows the equations used for this control. For example, if reactive current priority is selected, then I_{qmax} and I_{qmin} are limited to I_{max} and $-I_{max}$, respectively. Based on the reactive current ordered from the controls, the active current limit is then simultaneously calculated to utilize the remaining amount of total apparent current capability (I_{max}). A circular capability curve is assumed.

Example Consideration of Q Priority and P Priority

As an example, if the magnitude of current is limited to 1.2 pu (I_{max}), and the priority scheme is defined by reactive current priority, then a maximum limit of 1.2 pu is imposed on the reactive portion of current. The maximum active current (at this reactive current limit) will be 0.0 pu = $\sqrt{1.2^2 - 1.2^2}$. However, this does not imply that the active current will always be zero. This is the limited value of active current only when the reactive current is at its limit. However, if a reactive current of 1.0 pu is sufficient for the system, as decided by the reactive power-voltage controls, then the maximum active current can be 0.66 pu = $\sqrt{1.2^2 - 1.0^2}$. Hence, the reactive power-voltage controller not only decides the amount of reactive current to be injected but also the maximum amount of active current that can be injected for the decided value of reactive current. The active current controller then decides the actual value of active current to be injected. An opposite situation occurs when an inverter is in active current priority.

Prior to approval of IEEE Std. 1547-2018, all DERs on the system were not required to have reactive power-voltage control capability. Thus, the vintage of inverters that conform to this standard should have a P priority setting. With the approval of IEEE Std. 1547-2018, which requires inverters to have reactive power-voltage control capability (with preference to reactive current), it is expected that this capability will be used by the inverter, so the current priority setting should be set to Q priority. However, the impact of setting DER to P priority versus Q priority should be assessed with detailed studies since both settings could have a positive impact.

For example, upon the occurrence of a fault, a larger percentage of gross load can trip if located electrically close to the fault and if adjacent DERs are in Q priority, compared to when adjacent DERs are in P priority. However, at locations located electrically farther away from the fault, a larger percentage of gross load can trip when adjacent DERs are in P priority compared to when adjacent DERs are in Q priority. Closer to the fault, when in Q priority and with voltage control enabled, the DER reactive current would hit I_{max} and active current reduces to zero. The intention behind this is to try and support local voltage and prevent tripping of gross load. However, when the DER's active current contribution reduces to zero due to full output of reactive current (bear in mind that this is not to be confused with momentary cessation), the net load at the load substation bus increases, which can result in voltage reducing at nearby non-DERs causing load to trip. Now, when the DER is in P priority, the net load at the load bus would be lower (assuming that the DERs have not gone into momentary cessation mode), and thus, the voltage wouldn't fall as much at nearby non-DER buses, and as a result, a trip of gross load is lesser. Farther away from the fault, due to the initial higher voltage levels (as compared to the voltage levels closer to the faults), voltage support in Q priority has a greater effect and so even though the net load may increase (due to decrease in active current contribution from DER to accommodate injection of reactive current) the voltage drop (due to increase in net load) does not counterbalance the voltage support from the DER. Therefore, there is less gross load tripping.³¹ It should be noted that this behavior may not be the norm, but it is a possibility; therefore, setting DER priority settings should be conducted based on detailed system studies.

Fractional Tripping

The DER_A model includes a fractional tripping control³² that is intended to represent a portion of the DER tripping on low or high voltage³³ as shown in [Figure 1.5](#). The *vtripflag* controls voltage tripping and the *ftripflag* controls frequency tripping separately.³⁴ *Vfrac* defines the fraction of DERs that recover after voltage returns to within acceptable limits after dropping below or above the threshold values. For frequency tripping, a single low (*fl*) and high (*fh*) frequency cutout breakpoint is implemented since frequency variation along the distribution feeder is relatively constant (as compared with voltage). Hence, there is no partial tripping due to frequency.³⁵ *Tv* is a time constant representing the time delay for voltage related partial tripping (shown in [Figure 1.5](#)).

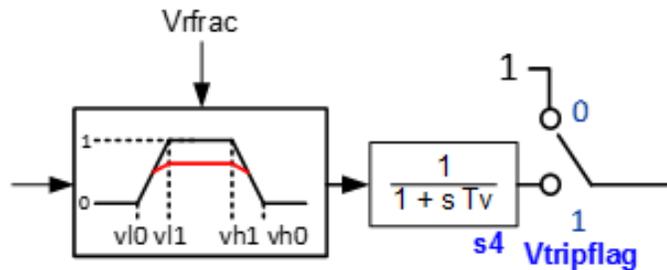


Figure 1.5: Fractional Tripping Controls

The *v/0* and *v/1* parameters are the low voltage cutout breakpoints and the *v/h0* and *v/h1* parameters are the high voltage cutout breakpoints. For example, when voltage falls below *v/1*, a fraction of the DERs will cutout, with a linearly increasing amount of DERs experiencing cutouts down to *v/0* where all DERs will have cut out. The output of

³¹ R. Quint, I. Green, D. Ramasubramanian, P. Pourbeik, J. Boemer, A. Gaikwad, D. Kosterev, C. DuPlessis, M. Osman, "Recommended DER Modeling Practices in North America," *25th International Conference and Exhibition on Electricity Distribution (CIRED)* [under review].

³² Fractional tripping should not be confused with dispatch scenario development that can take into account other outages (e.g., maintenance outages) in the powerflow models and not the dynamic transient set of models.

³³ There is no partial tripping due to frequency in the DER_A model. If there is a frequency trip, then the entire amount of DER trips.

³⁴ GE PSLF does not have these flags; however, Siemens PTI PSS[®]E, PowerWorld Simulator, and Powertech TSAT do have these flags.

³⁵ If there is a frequency trip, then the entire amount of DER trips.

the fractional tripping block is the value that gets applied to *ipcmd* and *iqcmd*.³⁶ If voltage falls outside the specified thresholds for the predefined amount of time (below *tvI0* or *tvI1* or above *tvh0* or *tvh1*), then the recovery of resources changes from the black line to the red line. This is intended to represent only a fraction of resources recovering from the decrease in voltage (*Vrfrac*); Those resources are expected to trip off-line and return to service some time beyond a typical transient simulation.

The fractional tripping logic does not represent any actual controls but is rather an attempt at emulating the fact that not all R-DERs will necessarily experience the same terminal voltage on a feeder and therefore they may not trip at the same time and for the same level of voltage excursion at the head of the feeder. Thus, this is an attempt based on much deliberation among many participants and stakeholders to come up with a method to emulate such behavior. As experience is gained with the model, this and perhaps other aspects may be refined over time.

Refer to the model specification document for more details related to model implementation and pseudo code.³⁷

Fractional Tripping Derivation

Specific data related to DERs tripping is often not available, and engineering judgment must be used to determine reasonable tripping values. These values should be based on the expected vintage of DERs and the distribution circuit characteristic. Each interconnection standard (e.g., IEEE Std. 1547-2003, IEEE Std. 1547a-2014, IEEE Std. 1547-2018) may have different ride-through and trip settings for abnormal voltage and frequency, with multiple magnitude/time duration pairs. Refer to [Table 2.1](#) and [Table 3.1](#) for initial details on setting these parameter values. It should be noted that these values may need to be changed depending on the individual system where the DER_A is applied. TPs should coordinate with their Distribution Providers (DPs) to attempt to track the proportion of DERs that could be expected to fall within each category. The proportion of DERs within each category may be inferred by DPs by assessing the date of each DER installation. The DER_A model does not include multiple points; however, these are likely not needed for stability studies in most cases. Typically, it is recommended to model the trip thresholds that relate to the shorter trip times³⁸ since this scenario is what covers most stability simulations. The thresholds are selected to account for the varied response of aggregate DERs tripping across a distribution system while taking into account the voltage drop (V_{DROP}) across the feeder.

Key Takeaway:

The DER_A model does not include multiple points for tripping; however, these are likely not needed for stability studies in most cases. Typically, it is recommended to model the trip thresholds that relate to the shorter trip times since this scenario is what covers most stability simulations.

Fractional trip settings are based on how the DERs are represented in powerflow and dynamics. There are multiple modeling options for how to set these fractional trip settings including the following (see [Figure 1.6](#)):

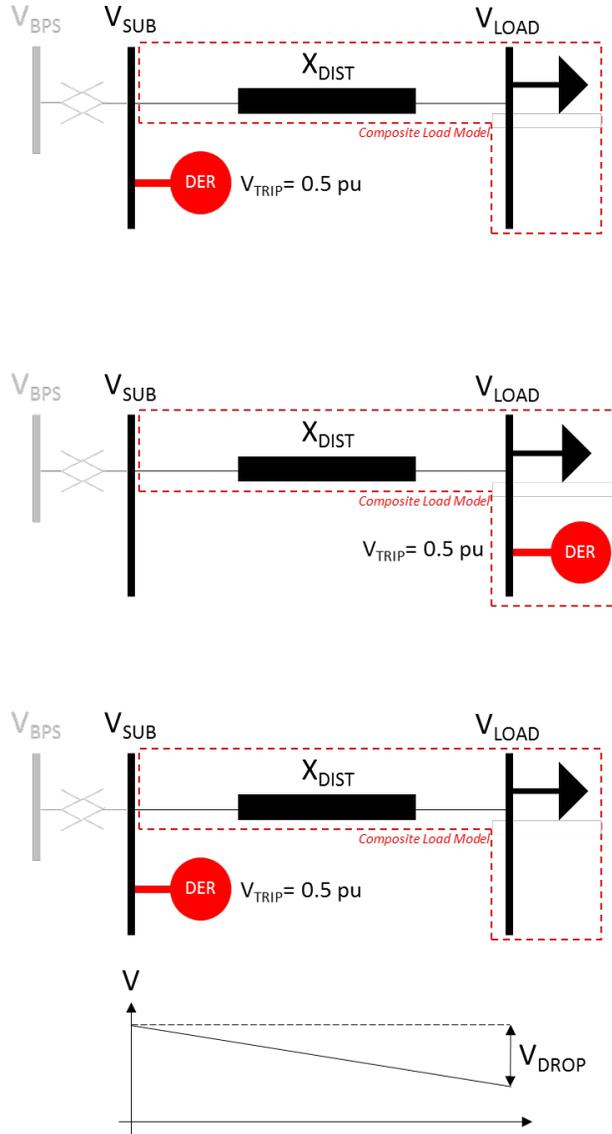
- Option 1 (Recommended for U-DERs):** The U-DER is represented in the powerflow base case as a generator, and has an associated DER_A model in dynamics. The modeled U-DER is intended to represent one or multiple U-DERs connected directly to or very close to the distribution substation. In this case, load modeling is unrelated, since the U-DER model explicitly represents a single or group of U-DERs. Partial tripping is not applied, and the DER trip settings can mirror those specified in the respective interconnection requirements. Parameters *vI0*, *vI1*, *vh0*, and *vh1* have a direct relation to those interconnection requirements. *Vrfrac* can be set to 1 or 0 depending on the vintage of DER.

³⁶ Refer to the DER_A Model Specification document for a detailed pseudo code explanation of how the fraction/partial tripping is calculated: https://www.wecc.biz/Reliability/DER_A_Final.pdf.

³⁷ P. Pourbeik, "Proposal for DER_A Model," June 19, 2019: https://www.wecc.org/Reliability/DER_A_Final_061919.pdf.

³⁸ As in, if the specification includes multiple trip magnitude-duration points, use the shortest duration point.

- 612
- 613
- 614
- 615
- 616
- 617
- 618
- 619
- 620
- 621
- 622
- **Option 2 (Recommended for R-DERs):** An aggregate amount of R-DERs spread throughout the distribution system is represented in the powerflow base case as a DER component of the load record. In dynamics, this information is integrated into the CLM with DER representation (e.g., `cmpldwg`). The equivalent distribution impedance is then represented in the CLM as well, with both load and DER represented at the load bus across the equivalent feeder impedance. Voltage drop (V_{DROP}) across the feeder is accounted for explicitly ($V_{DROP} = V_{SUB} - V_{LOAD}$). The Electric Power Research Institute (EPRI) has shown that a V_{DROP} of 2–8% is typical for most distribution feeders; a value around 5% is a reasonable assumption for DER (and load) modeling. Assuming a trip setting of 0.5 pu (see [Figure 1.6](#)), then DERs start tripping when the load bus voltage reaches 0.5 pu. All DERs have tripped when the substation bus voltage reaches 0.5 pu, meaning that the load bus voltage is at 0.45 pu. Therefore, $v/1$ equals 0.5 pu and $v/0$ equals 0.45 pu in this example. This concept can be used to determine trip settings for other standards as well.
 - **Option 3:** An aggregate amount of R-DERs spread throughout the distribution system can also be represented in the powerflow base case as a stand-alone generator. This does not necessarily follow the recommended framework described above; however, it is a modeling option. In this case, the same concept as presented in Option 2 applies with some minor modifications. In this case, the DERs are connected to the substation bus. The DERs start tripping when the implied load-side bus (distribution feeder impedance not represented) reaches 0.5 pu (so $V_{SUB} = V_{LOAD} + V_{DROP} = 0.55$ pu) and all are tripped when the substation bus voltage reaches 0.5 pu, so $v/1$ equals 0.55 pu and $v/0$ equals 0.5 pu in this example. Again, this concept can be applied to determine trip settings for other standards as well.
- 623
- 624
- 625
- 626
- 627
- 628
- 629
- 630
- 631



632

633

634

635

636

637

638

639

640

641

Figure 1.6: Fractional Trip Derivation Examples

The fractional trip settings can be used to model momentary cessation, if needed, in a relatively crude manner. For example, setting $v/1$ and $v/0$ to the momentary cessation settings will result in cessation of current below the specified thresholds. Selecting times $tv/0$ and $tv/1$ should be done with care to ensure the resources appropriately return following voltage recovery.³⁹ Note that momentary cessation is not required for Category II resources in IEEE Std. 1547-2018; however, the permissive operation range does allow for momentary cessation. TPs should consider sensitivity studies to understand the impact that this may have on studies.⁴⁰

³⁹ The settings $tv/0$ and $tv/1$ are related to the trip characteristics, and they do not apply to momentary cessation. Parameter $v/0$ can be set to the highest undervoltage point in which momentary cessation starts occurring.

⁴⁰ The fractional trip settings are not intended to match the IEEE Std. 1547 trip characteristics exactly; the DER_A model is intended to represent an aggregate behavior of DERs.

Voltage Source Interface Representation

In the DER_A model, a voltage source interface representation⁴¹ is implemented at the network interface to support numerical stability of the model in the simulation tools (see [Figure 1.7](#)).⁴² In reality, all modern inverters used on the grid-side of power electronic interfaced energy sources use a voltage source converter (VSC), specifically, a dc voltage source behind a full four-quadrant controlled dc to ac power electronic converter.⁴³ The current through the VSC is strictly controlled by the controls of the inverter. This can thus be represented as a voltage source behind an impedance. In order to develop the value of the voltage behind the impedance, the values of $ipcmd$ and $iqcmd$ are used to evaluate the voltage drop across the impedance and thereby develop the complex voltage. The representation is a voltage behind a reactance, X_e . Typical values for X_e are in the range of 0.25 pu.⁴⁴

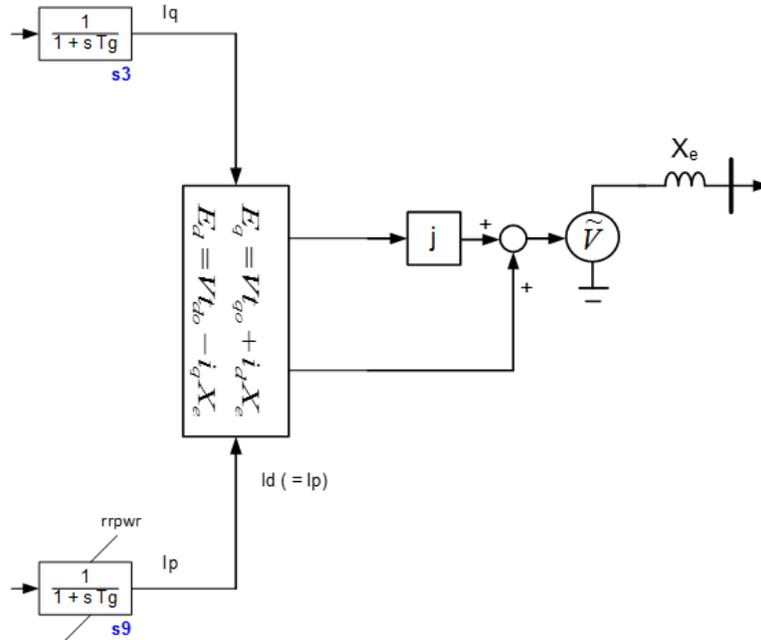


Figure 1.7: Voltage Source Representation

⁴¹ D. Ramasubramanian, Z. Yu, R. Ayyanar, V. Vittal and J. M. Undrill, “Converter Model for Representing Converter Interfaced Generation in Large Scale Grid Simulations”, IEEE Trans. PWRs, April 2016.

⁴² The *PVD1* and second generation renewable energy system models use a current source representation, which has proved to cause numerical issues in simulations—particularly at increased penetration levels of these models.

⁴³ A *typeflag* parameter exists in the model to denote whether the model is representing a generator or a battery energy storage system (BESS). The model does not explicitly represent four-quadrant control, as it does not represent a single BESS but rather an aggregated model. If the model is used to represent BESS, the model can operate with both positive and negative injection of active and reactive current.

⁴⁴ Resistance is neglected, and the reactance value (X_e) is also a default value for numerical stability. A value of X_e of around 0.25 pu seems reasonable for this model.

Chapter 2: Parameterization of the DER_A Model

A challenge with any DER model is developing a reasonable set of parameters to represent an aggregate response of many individual resources spread across a distribution system or feeder. [Table 2.1](#) provides a list of parameter values to represent different vintages of Interconnection standards. These include IEEE Std. 1547-2003, IEEE Std. 1547a-2014, IEEE Std. 1547-2018 Category II⁴⁵ defaults, and CA Rule 21 defaults. Refer to the DER_A specification document⁴⁶ or the simulation software model libraries for a description of the model parameters. It is to be noted that these parameter values are to be considered as initial default values and modifications to the values may be necessary based on the individual jurisdiction of application⁴⁷ of the model.

Table 2.1: Default DER_A Model Parameters

Param ⁴⁸	IEEE Std. 1547-2003 Default	IEEE Std. 1547a-2014 Default	CA Rule 21 Default	IEEE Std. 1547-2018 Category II Default	Notes
<i>trv</i>	0.02	0.02	0.02	0.02	† Note 1
<i>dbd1</i>	-99	-99	-99	-99	† Note 1
<i>dbd2</i>	99	99	99	99	† Note 1
<i>kqv</i>	0	0	0	0	† Note 1
<i>vref0</i>	0	0	0	0	† Note 2
<i>tp</i>	0.02	0.02	0.02	0.02	†
<i>tiq</i>	0.02	0.02	0.02	0.02	†
<i>ddn</i>	0	0	20	20	Note 3
<i>dup</i>	0	0	20	20	Note 3
<i>fdbd1</i>	-99	-99	-0.0006	-0.0006	Note 3
<i>fdbd2</i>	99	99	0.0006	0.0006	Note 3
<i>femax</i>	0	0	99	99	Note 3
<i>femin</i>	0	0	-99	-99	Note 3
<i>pmax</i>	1	1	1	1	† Note 4
<i>pmin</i>	0	0	0	0	Note 4
<i>dpmax</i>	99	99	99	99	†
<i>dpmi</i>	-99	-99	-99	-99	†
<i>tpord</i>	0.02	0.02	5	5	Note 3
<i>lmax</i>	1.2	1.2	1.2	1.2	† Note 4
<i>vl0</i>	0.44	0.44	0.49	0.44	Note 5
<i>vl1</i>	$0.44+V_{\text{DROP}}$	$0.44+V_{\text{DROP}}$	$0.49+V_{\text{DROP}}$	$0.44+V_{\text{DROP}}$	Note 5
<i>vh0</i>	1.2	1.2	1.2	1.2	Note 5
<i>vh1</i>	$1.2-V_{\text{DROP}}$	$1.2-V_{\text{DROP}}$	$1.2-V_{\text{DROP}}$	$1.2-V_{\text{DROP}}$	Note 5
<i>tvl0</i>	0.16	0.16	1.5	0.16	Note 5

⁴⁵ In IEEE Std. 1547-2018, the abnormal operating performance Category II “covers all BPS stability/reliability needs and is coordinated with existing reliability standards to avoid tripping for a wider range of disturbances of concern to BPS stability.”

⁴⁶ P. Pourbeik, “Proposal for DER_A Model,” June 19, 2019. [Online]: https://www.wecc.org/Reliability/DER_A_Final_061919.pdf.

⁴⁷ Further, some engineering analysis requires scenario development of a “best” and “worst” case scenarios. This will require engineering judgement to alter the provided parameters to reflect such scenarios.

⁴⁸ Refer to the DER_A model specification for parameter names: https://www.wecc.biz/Reliability/DER_A_Final.pdf.

Table 2.1: Default DER_A Model Parameters

Param ⁴⁸	IEEE Std. 1547-2003 Default	IEEE Std. 1547a-2014 Default	CA Rule 21 Default	IEEE Std. 1547-2018 Category II Default	Notes
<i>tv1</i>	0.16	0.16	1.5	0.16	Note 5
<i>tvh0</i>	0.16	0.16	0.16	0.16	Note 5
<i>tvh1</i>	0.16	0.16	0.16	0.16	Note 5
<i>Vrfrac</i>	0	0	1	1	Note 5
<i>fltrp</i>	59.3	59.5 OR 57.0	58.5 OR 56.5	58.5 OR 56.5	Note 6
<i>fhtrp</i>	60.5	60.5 OR 62.0	61.2 OR 62.0	61.2 OR 62.0	Note 6
<i>tfl</i>	0.16	2.0 OR 0.16	300.0 OR 0.16	300.0 OR 0.16	Note 6
<i>tfh</i>	0.16	2.0 OR 0.16	300.0 OR 0.16	300.0 OR 0.16	Note 6
<i>tg</i>	0.02	0.02	0.02	0.02	†
<i>rrpwr</i>	0.1	0.1	2.0	2.0	Note 8
<i>tv</i>	0.02	0.02	0.02	0.02	†
<i>Kpg</i>	0	0	0.1	0.1	Note 3
<i>Kig</i>	0	0	10	10	Note 3
<i>xe</i>	0.25	0.25	0.25	0.25	† Note 8
<i>vpr</i>	0.8	0.8	0.3	0.3	Note 6
<i>iqh1</i>	0	0	1	1	Note 1
<i>iq1</i>	0	0	-1	-1	Note 1
<i>pflag</i>	1	1	1	1	† Note 7
<i>fraflag</i>	0	0	1	1	Note 7
<i>paflag</i>	P priority	P priority	Q priority	Q priority	Note 7
<i>typeflag</i>	1	1	0 OR 1	0 OR 1	Note 7

664

Parameterization Notes

The following notes describe considerations and background on the parameter values selected in [Table 2.1](#). Refer to each respective interconnection standard for more information.

666

667

668

669

NOTE †: Default Parameters Not Typically Subject to Change

These parameters do not typically change across different implementations of the DER_A model. Any modification from the recommended default values should be carefully analyzed and justified.

670

671

672

NOTE 1: Voltage Control Parameters

In most existing applications, DERs do not control voltage. In such cases, the voltage control function should be disabled by setting the voltage control gain, *Kqv*, to 0. The lower and upper voltage deadbands, *dbd1* and *dbd2*, should be set large values (e.g., -99 and 99), respectively. However, interconnection standards state that the voltage control “capability” must be provided in the DER. If the capability is being utilized or required by the local utility, this setting should be modified accordingly.

673

674

675

676

677

678

When DERs are controlling voltage, the dynamic model needs to be adapted to account for this. As the model is not able to simultaneously represent both steady-state voltage control (Clause 5.3.3. voltage-reactive power mode in IEEE Std. 1547-2018) and dynamic voltage control (Clause 6.4.2. dynamic voltage support in IEEE Std. 1547-2018), a modeling compromise must be made. Therefore, it is recommended that the dynamic voltage support settings be

679

680

681

682

implemented since most simulations involve fault-type conditions with large voltage fluctuations. Reasonable default values are $trv = 0.02$, $kqv = 5$,⁴⁹ $dbd1 = -0.12$, $dbd2 = 0.1$, $iqh1 = 1$, and $iq1 = -1$.⁵⁰ Any situation where Kqv is non-zero (dynamic voltage control is enabled), care should be taken to ensure that the corresponding deadband is not too small, which would lead to voltages possibly jumping across deadband thresholds each simulation iteration.

NOTE 2: Voltage Reference

The recommended setting for $Vref0$ is 0. Setting $Vref0$ equal to 0 allows the model to set its own terminal voltage reference based on the initial conditions. This is consistent with the language in IEEE Std. 1547-2018 and in 5.3.3 (voltage-reactive power mode), which require that DERs shall be capable of autonomously adjusting reference voltage ($Vref$) with $Vref$ being equal to the (low pass filtered) measured voltage.

NOTE 3: Active Power-Frequency Control

In IEEE Std. 1547-2003 and IEEE Std. 1547a-2014, active power-frequency control is not specified. Therefore, the gains Ddn and Dup as well as the frequency errors $femax$ and $femin$ are set to 0. This disables the active power-frequency controls in the model for these two standards. In CA Rule 21 and IEEE Std. 1547-2018, the capability for resources to have active power-frequency controls installed and enabled (as default) are specified. Therefore, per the standard Dup and Ddn should be set to 20 (representing a 5% droop characteristic).⁵¹ Default deadband for both standards is set to ± 0.0006 pu, or ± 36 mHz. $Tpord$ is used to represent the specified open loop time constant of five seconds per IEEE Std. 1547-2018 and CA Rule 21, and it is set to a small value (0.02 sec) when these controls are disabled in previous IEEE Std. 1547 versions.⁵² Parameters Kpg and Kpi are not directly mapped to the interconnection standards; values describe in Table 2.1 were used in benchmark testing of the DER_A model are based on engineering judgment and were found to provide satisfactory response. Note that if the DERs are assumed to be operating at maximum available power, the Dup should be set to 0. This is explained further in Chapter 3

NOTE 4: Active Power Capability

Maximum active power output is set to a default of 1 pu. Minimum active power output is assumed to be 0 pu for generating resources but can be negative (i.e., -1 pu) for energy storage resources. These maximum and minimum active power capability values can be modified if more detailed information is known about specific DERs. Inverter-based DERs have an overload capability of around 110–120%, and therefore $Imax$ is set to 1.2 pu. Other types of DERs may have a different current limit, and this can be adjusted carefully if additional information is known. However, for most inverter-based installations (e.g., solar PV), a value of 1.2 pu is a reasonable approximation.

NOTE 5: Partial Tripping

$Vrfac$, the ratio of DERs that restore output upon voltage recovery, should be set to 0 for legacy⁵³ DERs (i.e., no DER restore output following a ride-through event), 1.0 for modern DERs (i.e., all DERs restore output following a ride-through event), and some value in between for a mix of a legacy and modern DERs based on the assumed vintage of the DER deployed. A value of $Vrfac = 0$ is a conservative assumption and should be used if no detailed DER information is available. Since CA Rule 21 and IEEE Std. 1547-2018 are relatively new standards, it can be expected that, for now, $Vrfac$ can be set at or near 0. When using the `der_a` dynamic model to represent a single plant⁵⁴, the partial tripping parameter should be set to 0 to represent the entire plant tripping.

⁴⁹ Allows for maximum reactive current injection when voltage falls below around 0.7 pu, taking into consideration the voltage deadband.

⁵⁰ Again, note that the values in Table 2.1 do not use these settings because the respective interconnection agreements do not require dynamic voltage control to be used. Hence, kqv is set to 0.

⁵¹ See Chapter 3 on recommended settings. Since most DER will be operated at maximum available power, and will not have available generating capability to respond in the upward direction for underfrequency events, Dup should be set to 0, from a practical standpoint.

⁵² Setting $tpord$ should be studied on an individual system basis.

⁵³ Use of the term “legacy” generally refers to DER compliant with IEEE Std. 1547-2003 and IEEE Std. 1547a-2014, which typically involve limited or no controls and ride-through capability.

⁵⁴ This is more common for a single, large distribution-connected generation plant. A non-zero parameter here would indicate a portion of the plant trips, which is not the desired effect.

720 The interconnection standards include different levels of trip settings: typically a longer duration trip time with
 721 magnitude closer to nominal and a shorter duration trip time with lower (or higher) magnitude away from nominal.
 722 **Table 2.1** includes values for the shorter duration trip thresholds since these values are likely the most useful and
 723 relevant settings for stability studies. Consult the relevant interconnection standards and requirements for more
 724 information on longer duration trip settings. Higher magnitude with longer duration trip settings may need to be
 725 studied in simulations involving delayed voltage recovery.

726 V_{DROP} should be set to a reasonable equivalent voltage drop across the distribution system in the range of 2–8%
 727 (reasonable default of 5%) if no detailed information is available. Voltage trip thresholds include a 0.01 pu offset from
 728 the interconnection standard values to correctly account for the beginning and completion of partial tripping.

729 The values specified in the **Table 2.1** represent R-DERs as part of the CLM. If individual or multiple similar U-DERs are
 730 represented, trip settings should be equal and set to the corresponding value in the interconnection standard. If
 731 aggregate R-DERs are to be represented by a generator record, use the methodology described in **Chapter 1** to
 732 determine correct trip settings.

733 In cases where momentary cessation of inverter-based resources needs to be represented, use $v/1$ and $v/0$ with
 734 extended trip times. Note that this may hinder the ability to capture any tripping effects due to existing model
 735 limitations. Engineering judgment and sensitivity studies should be used when applying these types of settings.
 736

737 **NOTE 6: Frequency Trip Levels**

738 High (f_{htrp}) and low (f_{ltrp}) frequency tripping has different thresholds in a few of the interconnection standards, as
 739 described in **Table 2.1**. Again, each has a specified time threshold. The frequency thresholds closer to nominal
 740 frequency have a longer duration while the thresholds further from nominal have a shorter duration.

741 In simulations where frequency does not fall below under-frequency load shedding (UFLS) levels, the setting values
 742 for CA Rule 21 and IEEE Std. 1547-2018 are not significant.⁵⁵ However, the settings representing IEEE Std. 1547-2003
 743 and IEEE Std. 1547a-2014 are relevant, particularly for the thresholds closer to nominal frequency. IEEE Std. 1547-
 744 2003 has only one magnitude and time value. IEEE Std. 1547a-2014 has two thresholds, but most commonly only the
 745 59.5 Hz and 60.5 Hz thresholds, with two second timers, are applicable.

746 Disabling tripping on frequency during low voltage is implemented in almost all relay models as the relay needs a
 747 sufficient voltage waveform to measure frequency. Under fault conditions, due to the large change in voltage, the
 748 frequency calculation can result in a spurious spike, and thus, frequency tripping should be disabled. IEEE Standard
 749 C37.117⁵⁶ recommends disabling the frequency trip when the voltage is below 50–70% of nominal. For DERs, this
 750 voltage levels was increased to 80% to account for further inaccuracies in frequency calculation that may arise in
 751 positive sequence simulations.⁵⁷ The first sentence of IEEE Std. 1547-2018, Clause 6.5.1, states that when frequency
 752 meets a certain criteria and “the fundamental-frequency component of voltage on any phase is greater than 30% of
 753 nominal” then the DER can respond. However, if the frequency is outside acceptable range but voltage is less than
 754 the 30% threshold then the DER should not trip. This represents a low voltage inhibit function in the frequency
 755 tripping, and it is represented by parameter V_{pr} .⁵⁸ Regardless, study engineers should monitor for false trips by the
 756 DER_A model that may not be realistic; rather, they are an artifact of positive sequence stability simulation calculation
 757 of frequency. Close review of any frequency-related tripping is strongly recommended.

758 **NOTE 7: Control Flags**

⁵⁵ Unless specific studies are being performed to configure UFLS systems.

⁵⁶ IEEE C37.117-2007, IEEE Guide for the Application of Protective Relays Used for Abnormal Frequency Load Shedding and Restoration.

⁵⁷ https://www.wecc.biz/Reliability/WECC_White_Paper_Frequency_062618_Clean_Final.pdf.

⁵⁸ V_{pr} may also be referred to as V_{fth} .

759 The parameter *pflag* sets power factor control. If set to 1, then the power factor angle reference is used based on
760 initialization of the model. Otherwise, if set to 0, then the reactive power reference (*Qref*) will be used.

761 The parameter *freqflag* sets the active power-frequency control capability. If set to 0, then active power reference (*Pref*)
762 is used. Otherwise, if set to 1, then the active power-frequency control loop is enabled. If *freqflag* is set to 1, the resource
763 will response to over- and under-frequency disturbances. However, if the user sets *Dup* to 0, the resource will not
764 respond to underfrequency. This configuration emulates the unit(s) operating at maximum available power output.

765 The parameter *pqflag* specifies whether to use active or reactive current priority, which is effective when the current
766 limit logic is in effect. This is particularly used during response to large disturbances (i.e., faults).

767 The parameter *typeflag* specifies whether the resource is a generating resource (set to 1) or an energy storage device
768 (set to 0). Setting as an energy storage device allows absorption of active power, and it emulates distributed energy
769 storage. This does not, however, emulate charging and discharging of the resource.

770 **NOTE 8: Voltage Source Interface Representation**

771 The *rrpwr* specifies the active current ramp rate. IEEE Stds. 1547-2003 and 1547a-2014 do not specify an active
772 current ramp rate; however, IEEE Std. 1547-2018 and CA Rule 21 use an 80% recovery within 0.4 seconds that can be
773 approximated with a gain of 2 pu/sec, which equates to full recovery within 0.5 seconds. The voltage source
774 impedance also uses a default values for *Xe* of 0.25, based on robustness testing of the DER_A model during its
775 development.

776

Future Model Implementation Improvement

Commercial simulation software vendors should consider adding a new global flag for inverter-based resources (particularly renewable energy resources) that sets the maximum available power to the current power output (*Pgen*) upon initialization of the inverter-based models. This can then be changed by the user on a case-by-case basis during the simulation if necessary (e.g., to represent curtailing). For example, simulations with renewable generation dispatched at less than maximum capacity (*Pmax*) may represent less solar irradiance or lower wind speed. However, this is the maximum available power output for the assumed conditions. As more resources are being installed with the capability to provide active power-frequency control, the ability to distinguish whether units are operating at maximum available power output will be increasingly important. This parameter is similar to the baseload flag for synchronous generating resources.

777

778

779

782 **Table 2.1** in the previous chapter provides parameter values that relate to specific interconnection standards and
 783 requirements; however, many systems are faced with aggregate DERs that encompass many vintages of
 784 interconnection requirements and settings. **Table 3.1** provides a set of default parameter values for different systems
 785 based on the penetration of different IEEE Std. 1547 vintages, ranging from a system dominated by IEEE Std. 1547-
 786 2003 interconnections to a system of modern IEEE Std. 1547-2018 interconnections.⁵⁹ Also shown are default values
 787 for penetrations at 70% for 2003 vintage and 30% for 2018 vintage, as well as 30% for 2003 vintage and 70% for 2018
 788 vintage. These default values are based on engineering judgment and intended to be used as a starting point for more
 789 detailed studies and sensitivities.⁶⁰ Note that, in addition to the IEEE Std. 1547 default settings, individual utilities or
 790 jurisdictions may have additional or more stringent requirements that should be considered when developing a set
 791 of DER modeling parameters. TPs and PCs should consider any modifications to the default IEEE Std. 1547 parameters
 792 as well as local requirements and should adapt the models accordingly.

794 Parameter values that are subject to changes across interconnection vintages are highlighted in red in **Table 3.1** and
 795 described in this chapter. Note that some of the parameter values subject to change are a linear interpolation based
 796 on the penetration of specific vintages of DERs. Sensitivity studies should be performed by the TP and PC to
 797 understand the impacts of these parameter values to system study results.

Param	Early Vintage DER System IEEE Std. 1547-2003	70% of -2003 30% of -2018	30% of -2003 70% of -2018	Newer Vintage DER System IEEE Std. 1547-2018 (Category II)
<i>trv</i>	0.02	0.02	0.02	0.02
<i>dbd1</i>	-99	-99	-99	-99
<i>dbd2</i>	99	99	99	99
<i>kqv</i>	0	0	0	0
<i>vref0</i>	0	0	0	0
<i>tp</i>	0.02	0.02	0.02	0.02
<i>tiq</i>	0.02	0.02	0.02	0.02
<i>ddn</i>	0	6	14	20
<i>dup</i>	0	0	0	0
<i>fdbd1</i>	-99	-0.0006	-0.0006	-0.0006
<i>fdbd2</i>	99	0.0006	0.0006	0.0006
<i>femax</i>	0	0	99	99
<i>femin</i>	0	0	-99	-99
<i>pmax</i>	1	1	1	1
<i>pmin</i>	0	0	0	0
<i>dpmx</i>	99	99	99	99

⁵⁹ Note that application and enforcement of IEEE Std. 1547-2018 for newly interconnecting inverters is likely to take time to implement in many jurisdictions, often requiring regulatory updates to enable enhanced capabilities. Some degree of verification and alignment with these implementation timelines should be performed by each TP and PC when representing DER in BPS reliability studies.

⁶⁰ Transmission–distribution co-simulation techniques may be used to help further parameterize DER_A models based on specific distribution feeder configurations and DER penetration levels.

Param	Early Vintage DER System IEEE Std. 1547-2003	70% of -2003 30% of -2018	30% of -2003 70% of -2018	Newer Vintage DER System IEEE Std. 1547-2018 (Category II)
<i>dpmin</i>	-99	-99	-99	-99
<i>tpord</i> ⁶¹	0.02	0.02	5	5
<i>lmax</i>	1.2	1.2	1.2	1.2
<i>vl0</i>	0.44	0.44	0.44	0.44
<i>vl1</i>	0.49	0.49	0.49	0.49
<i>vh0</i>	1.2	1.2	1.2	1.2
<i>vh1</i>	1.15	1.15	1.15	1.15
<i>tvl0</i>	0.16	0.16	0.16	0.16
<i>tvl1</i>	0.16	0.16	0.16	0.16
<i>tvh0</i>	0.16	0.16	0.16	0.16
<i>tvh1</i>	0.16	0.16	0.16	0.16
<i>Vfrac</i>	0	0.3	0.7	1.0
<i>fltrp</i>	59.3	58.5	57.5	56.5
<i>fhtrp</i>	60.5	61	61.5	62.0
<i>tfl</i>	0.16	0.16	0.16	0.16
<i>tfh</i>	0.16	0.16	0.16	0.16
<i>tg</i>	0.02	0.02	0.02	0.02
<i>rrpwr</i>	0.1	0.6	1.4	2.0
<i>tv</i>	0.02	0.02	0.02	0.02
<i>Kpg</i>	0	0.1	0.1	0.1
<i>Kig</i>	0	10.0	10.0	10.0
<i>xe</i>	0.25	0.25	0.25	0.25
<i>vftth</i>	0.8	0.3	0.3	0.3
<i>iqh1</i>	0	1.0	1.0	1.0
<i>iq1</i>	0	-1.0	-1.0	-1.0
<i>pfflag</i>	1	1	1	1
<i>fraflag</i>	0	1	1	1
<i>paflag</i>	P priority	P priority	Q priority	Q priority
<i>typeflag</i>	1	1	1	1

799
800
801
802

The following considerations are made in the development of these default parameter values and intended to provide transparency and understanding of how these parameters were devised. However, they are intended as default values that may be subject to change if more detailed information is known.

⁶¹ The active power-frequency response from DERs, if utilized in studies, should be tuned to achieve and ensure a closed-loop stable control. This parameter may need to be adapted based on this tuning.

- 803 • **Upward Frequency Responsiveness for Underfrequency Conditions (*Dup*, *Pmax*):** In this set of default
804 parameters, it is assumed that the vast majority (if not all) DERs are operated at maximum available⁶²
805 power and thus cannot provide frequency response for underfrequency conditions.⁶³ To model the
806 inability to provide response in the upward direction, the *Dup* parameter value is set to 0. This disables
807 upward movement regardless of where the DER resource(s) is dispatched relative to *Pmax* in the
808 dynamics data. This allows for easy manipulation of DER output levels without needing to modify
809 additional parameter values for each sensitivity case. Another option is to set the *Dup* parameter value
810 according to the expected performance and then modifying *Pmax* value in the dynamics data to match
811 the predisturbance output for each operating conditions studied. However, this requires an additional
812 step and may lead to unexpected frequency responsiveness from DER if not adequately handled when
813 changing DER dispatch levels.
- 814 • **Downward Frequency Responsiveness for Overfrequency Conditions (*Ddn*):** *Ddn* is modified across the
815 different penetration levels to represent an effective droop characteristic, or a response from a fractional
816 DER value based on the penetration of modern inverters. The 5% droop (*Ddn* = 20) is multiplied by a
817 linear factor based on this penetration (e.g., 70% of 20 equals 14).
- 818 • **Frequency Deadband and Error Limits (*fdb1*, *fdb2*):** When frequency response is enabled in the model,
819 the deadband settings of *fdb1* and *fdb2* as well as the frequency error settings of *femax* and *femin* need
820 to be modified to enable accurate representation of these controls. A default value is used in all cases
821 where control is enabled.
- 822 • **Voltage-Related Trip Settings and Times:** Refer to the [Chapter 1](#) for the derivation of the partial trip
823 values. Note that trip thresholds and times may vary if applying CA Rule 21. Values assume a voltage
824 drop, V_{DROD} , of 5%.
- 825 • **Fraction of Resources Recovering (*Vrfrac*):** The parameter *Vrfrac* represents the fraction of resources
826 that recover upon voltage recovery following abnormal voltage conditions. It is expected that resources
827 meeting IEEE Std. 1547-2018 will recover from abnormal voltages and ride through ^{disturbances} while IEEE
828 Std. 1547-2003 resources will likely trip and remain disconnected for the duration of stability simulations.
829 A linear multiplier is used based on the fraction of resources connected to the system. For example, for
830 a 70% IEEE Std. 1547-2018 system, *Vrfrac* equals 0.7.
- 831 • **Frequency-Related Trip Settings (*fltrp*, *fhtrp*):** Frequency-related trip settings of *fltrp* and *fhtrp* are
832 assumed to slightly vary based on the aggregate vintage of connected DERs. For the shorter-term
833 tripping, IEEE Std. 1547-2003 has trip settings at 59.3 Hz and 60.5 Hz while IEEE Std. 1547-2018 has trip
834 settings at 57.5 Hz and 62 Hz. For mixed penetrations, a linear multiplier is used to vary the level of DER
835 tripping. This is an approximate; yet, these trip settings are below the first stage of UFLS, ^{and} they are
836 therefore not likely to make a substantive impact in most stability simulations.⁶⁴ More detailed studies
837 should consider identifying more accurate information for these settings.
- 838 • **Active Current Recovery Ramp Rate (*rrpwr*):** The parameter *rrpwr* is modified across different
839 penetration levels to represent the fraction of resources that recover from abnormal voltage conditions.
840 A 2.0 pu/sec (recovery in 0.5 seconds) is used for IEEE Std. 1547-2018 resources, and a linear multiplier
841 is used for the mixed penetration conditions. For example, 70% of 2.0 pu/sec equals 1.4 pu/sec.
- 842 • **Frequency Response PI Controls (*Kpg*, *Kig*):** When frequency response controls are enabled in the model,
843 default parameter values of *Kpg* = 0.1 and *Kig* = 10 are used.

⁶² If studies are assuming that DERs are curtailed for any reason, IEEE Std. 1547-2018 vintage DERs will have the capability to respond to underfrequency events.

⁶³ This statement relates to DERs that are generating resources; this may not be the case for energy storage. Energy storage, not injecting maximum power, will be able to respond to underfrequency events following a droop characteristic.

⁶⁴ Stability studies for establishing UFLS set points, where simulated frequency can fall well below UFLS, should ensure reasonable frequency-related trip settings are used for DER.

844
845
846
847

- **Type Flag (*typeflag*):** In these default data sets, the *typeflag* is set to 1 representing a generating resource. This flag, and relevant parameter values, can also be modified to represent an energy storage resource.

Chapter 4: DER_A Model Benchmarking and Testing

To ensure that a model is usable for industry-wide studies, some form of model benchmarking and testing is typically performed by industry partners. DER_A model development and testing was led by the WECC Renewable Energy Modeling Task Force (REMTF) and NERC LMTF with EPRI providing the model benchmarking support.

EPRI performed extensive DER_A model benchmarking while working with the major commercial software vendors⁶⁵ following their implementation of the standalone DER_A model. A test system with a play-in voltage source model at the transmission bus with constant impedance load adjacent to the DERs was used for the testing. A suite of 19 tests was used to apply small and large disturbances of voltage and frequency, and then the model's active and reactive power response and set points were observed. The response of the DER_A model was compared for each test across all platforms to determine whether the models match the same general trend in response (i.e., they are considered suitably benchmarked). Refer to an EPRI white paper on this topic (reference 11 in [Appendix A](#)).⁶⁶ [Figure 4.1](#) shows an example benchmarking simulation, and it demonstrates how the DER_A model in each of the software platforms matches the same general performance characteristic.

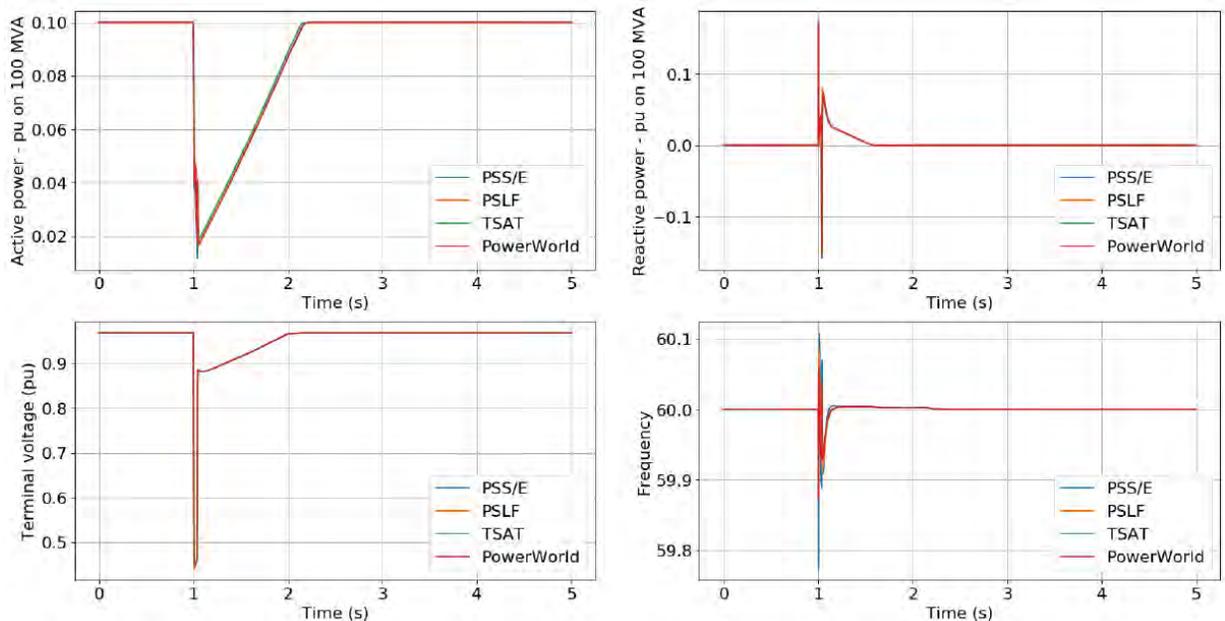


Figure 4.1: Voltage Sag Benchmarking Test Result [Source: EPRI]

To ensure that the model is numerically robust and usable in system studies on a large-scale case, CAISO has been testing the DER_A model on WECC-wide base cases for their reliability studies. [Figure 4.2](#) shows one example of the types of sensitivity studies performed by CAISO. CAISO has been testing the model with different parameter values, including CA Rule 21 and the new IEEE Std. 1547-2018 default settings. The model has performed well and is numerically robust in these studies using GE PSLFTM.⁶⁷

⁶⁵ Including GE-PSLFTM, Siemens PTI PSS[®]E, PowerWorld Simulator, and Powertech Labs TSAT.

⁶⁶ The New Aggregated Distributed Energy Resources (der_a) Model for Transmission Planning Studies. 2019 Update. White Paper. 3002015320. Electric Power Research Institute (EPRI). Palo Alto, CA (<https://www.epri.com/#/pages/product/000000003002015320/?lang=en-US>).

⁶⁷ CAISO, "CMPLDWG Composite Model with Distributed Generation DER_A CAISO Assessment," NERC LMTF Meeting, May 2018: https://www.nerc.com/comm/PC/LoadModelingTaskForceDL/CMPLDWG_DER_A_CAISO_NERC.pdf.

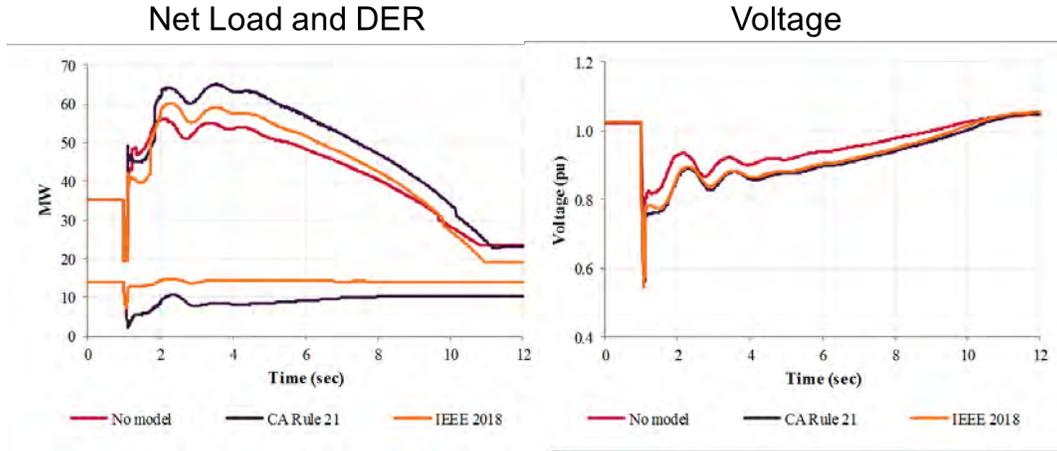


Figure 4.2: CAISO DER Study Example including DER_A Model [Source: CAISO]

873
874
875
876
877
878
879
880
881
882
883

EPRI has also performed system studies on the full Eastern Interconnection base case in coordination with Duke Energy. These studies implemented the DER_A model on 138 U-DER installations with a capacity of 1,300 MW. Figure 4.3 shows the DER response from an example simulation using these models. It shows that some of the DER_A models near the fault location respond to the disturbance with active and reactive power response, and those further away from the disturbance do not provide a significant response. Again, the implemented DER_A models are numerically robust.⁶⁸ EPRI further did analysis on the DER_A model when used as part of the composite load model to test modeled R-DER in the SPIDERWG recommended modeling framework⁶⁹. Again, the models were numerically robust.

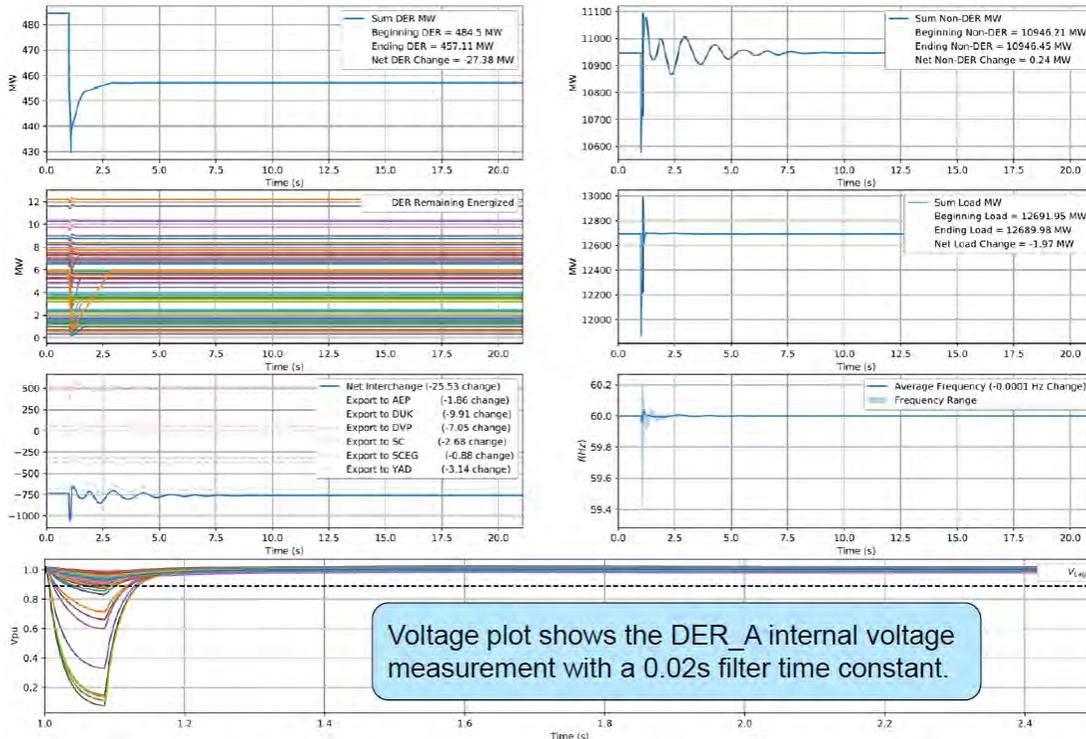


Figure 4.3: DER Study Example including DER_A Model [Source: EPRI]

884
885

⁶⁸ EPRI, “Preliminary results of DER_A model parameterization”, NERC LMTF Meeting, July 2018: https://www.nerc.com/comm/PC/LoadModelingTaskForceDL/Parameterization_of_DER_A_Model_v1_DR.pdf.
⁶⁹ EPRI, “Results on CMPLDWg – DER_A Benchmark”, NERC LMTF Meeting, July 2019: https://www.nerc.com/comm/PC/LoadModelingTaskForceDL/CMPLDWg-DER_A-benchmark_v1_DR.pdf

886 **Appendix A: Contributors**

887
888
889
890

NERC gratefully acknowledges the contributions and assistance of the following industry experts in the preparation of this guideline. NERC would like to acknowledge EPRI for the technical leadership in developing this guideline.

Name	Entity
Irina Green	Guidehouse
Mohab Elnashar	Independent Electricity System Operator
Deepak Ramasubramanian (Subgroup Colead)	EPRI
Adam Weber (Subgroup Colead)	Ameren
Jens Boemer	EPRI
Nicolas Compas	Hydro Quebec
Laura Fedoruk	Sunrun
Anish Gaikwad	EPRI
Ning Kang	Argonne National Laboratory
Dmitry Kosterev	BPA
Dean Latulipe	National Grid
Pouyan Pourbeik	PEACE®
Bill Price	General Electric
Bill Quaintance	Duke Progress
Shruti Rao	GE PSLFederal Electric
Fabio Rodriguez	Duke Florida
Juan Sanchez-Gasca	General Electric
Jay Senthil	Siemens PTI
Shayan Rizvi (SPIDERWG Chair)	NPCC
John Schmall (SPIDERWG Vice-Chair)	ERCOT
Ryan Quint (SPIDERWG Coordinator)John Skeath	NERCNorth American Electric Reliability Corporation
John Skeath (SPIDERWG Coordinator)	NERC
Mohamed Osman	NERC
Jameson Thornton	Pacific Gas and Electric
Song Wang	PacifiCorp
Shannon Mickens	SPP
Scott Jordan	SPP
Brad Marszalkowski	ISO-NE
Nick Hatton	WECC

891
892

893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941

Appendix B: References

DER_A Model Specification Document

- [1] P. Pourbeik, "Proposal for DER_A Model," September 11, 2018. [Online]: https://www.wecc.org/Reliability/DER_A_Final_061919.pdf.

Relevant Interconnection Standards

- [2] IEEE Std. 1547-2003, Standard for Interconnecting Distributed Resources with Electric Power Systems, July 2003. [Online]: <https://standards.ieee.org/standard/1547-2003.html>.
- [3] IEEE Std. 1547a-2014, IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems – Amendment 1, May 2014: <https://standards.ieee.org/standard/1547a-2014.html>,
- [4] IEEE Std. 1547-2018, IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, April 2018. [Online]: <https://standards.ieee.org/findstds/standard/1547-2018.html>.
- [5] IEEE Std. 1547-2018, 6/4/2018: Errata to IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces. [Online]: http://standards.ieee.org/findstds/errata/1547-2018_errata.pdf.
- [6] CPUC: Interconnection (Rule 21). California Public Utilities Commission. [Online]: <http://www.cpuc.ca.gov/Rule21/>.

Relevant NERC Guidelines and Reports

- [7] NERC, "Distributed Energy Resources: Connection Modeling and Reliability Considerations," Atlanta, GA, Feb 2017. [Online]: https://www.nerc.com/comm/Other/essntlrbltysrvdstskfrDL/Distributed_Energy_Resources_Report.pdf.
- [8] NERC, "Reliability Guideline: Modeling Distributed Energy Resources in Dynamic Load Models," Atlanta, GA, Dec 2016. [Online]: https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_-_Modeling_DER_in_Dynamic_Load_Models_-_FINAL.pdf.
- [9] NERC, "Reliability Guideline: Distributed Energy Resource Modeling," Atlanta, GA, Sept 2017. [Online]: https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_-_DER_Modeling_Parameters_-_2017-08-18_-_FINAL.pdf.

DER_A Parameterization References

- [10] The New Aggregated Distributed Energy Resources (der_a) Model for Transmission Planning Studies. 2019 Update. White Paper. 3002015320. Electric Power Research Institute (EPRI). Palo Alto, CA. [Online]: <https://www.epri.com/#/pages/product/000000003002015320/?lang=en-US>.
- [11] Electric Power Research Institute (EPRI) (2016): Distributed Energy Resources Modeling for Transmission Planning Studies. Summary Modeling Guidelines. 3002009485. Palo Alto, CA. [Online]: <http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002009485>.
- [12] EPRI (2017): Distributed Energy Resources Modeling for Transmission Planning Studies. Detailed Modeling Guidelines. 3002010932. Electric Power Research Institute (EPRI). Palo Alto, CA. [Online]: <https://www.epri.com/#/pages/product/000000003002010932/>.
- [13] I. Alvarez-Fernandez, D. Ramasubramanian, A. Gaikwad, J. Boemer, "Parameterization of Aggregated Distributed Energy Resources (DER_A) Model for Transmission Planning Studies," 2018 Grid of the Future Symposium, CIGRE US National Committee, Reston, VA, 2018.
- [14] EPRI (2018) Selected Case Studies Analyzing the Impact of DER on the Bulk System Voltage Performance: Impact of Aggregate Distributed Energy Resources on a Large System, EPRI, Palo Alto, CA: 2018, 3002013502.
- [15] EPRI (2018) Detailed Distribution Circuit Analysis and Parameterization of the Partial Voltage Trip Logic in WECC's DER Model (DER_A): Towards regional default settings in the absence of detailed distribution circuit data, EPRI, Palo Alto, CA: 2018, 3002013500.

942

943 **Other Reference Material**

944 [16] D. Ramasubramanian, Z. Yu, R. Ayyanar, V. Vittal and J. M. Undrill, “Converter Model for Representing
945 Converter Interfaced Generation in Large Scale Grid Simulations”, IEEE Trans. PWRs, April 2016.

946 [17] WECC, “Wind Plant Dynamic Modeling Guidelines,” Salt Lake City, UT, April 2014. [Online]:
947 <https://www.wecc.biz/Reliability/WECC%20Wind%20Plant%20Dynamic%20Modeling%20Guidelines.pdf>.

948 [18] WECC, “Solar Plant Dynamic Modeling Guidelines,” Salt Lake City, UT, April 2014. [Online]:
949 <https://www.wecc.biz/Reliability/WECC%20Solar%20Plant%20Dynamic%20Modeling%20Guidelines.pdf>.

950

959

Guideline Information and Revision History

960

Guideline Information	
Category/Topic: [NERC use only]	Reliability Guideline/Security Guideline/Hybrid: Reliability Guideline
Identification Number: [NERC use only]	Subgroup: [NERC use only]

961

Revision History		
Version	Comments	Approval Date

962

963

1
2
3
4
5
6
7
8
9

Reliability Guideline

Parameterization of the DER_A Model for
Aggregate DER

December 2022

10
11
12
13
14
15
16
17

RELIABILITY | RESILIENCE | SECURITY



21
22
26
27
28
29

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

30 **Table of Contents**

31 Preface iv

32 Preamble v

33 Metrics vi

34 Executive Summary vii

35 Introduction viii

36 Applicability viii

37 Related Standards viii

38 Purpose viii

39 Background ix

40 Historic DER Model Usage and Development ix

41 DER Data Collection ix

42 Synchronous DER Models xi

43 Second Generation Renewable Energy System Models xii

44 DER Modeling Framework xiii

45 Overview of the DER_A Model xvii

46 Chapter 1: Annotated DER_A Block Diagram 1

47 Active Power-Frequency Controls 1

48 Frequency Tripping Logic Input 1

49 Reactive Power-Voltage Controls 2

50 Active-Reactive Current Priority Logic 2

51 Example Consideration of Q Priority and P Priority 3

52 Fractional Tripping 4

53 Fractional Tripping Derivation 5

54 Voltage Source Interface Representation 8

55 Chapter 2: Parameterization of the DER_A Model 9

56 Parameterization Notes 10

57 Chapter 3: Practical DER_A Model Implementation 14

58 Chapter 4: DER_A Model Benchmarking and Testing 18

59 **Appendix A: Contributors** 20

60 **Appendix B: References** 21

61 **Appendix C: DER_A Block Diagram** 23

62 Guideline Information and Revision History 24

63 Errata 25

Table of Contents

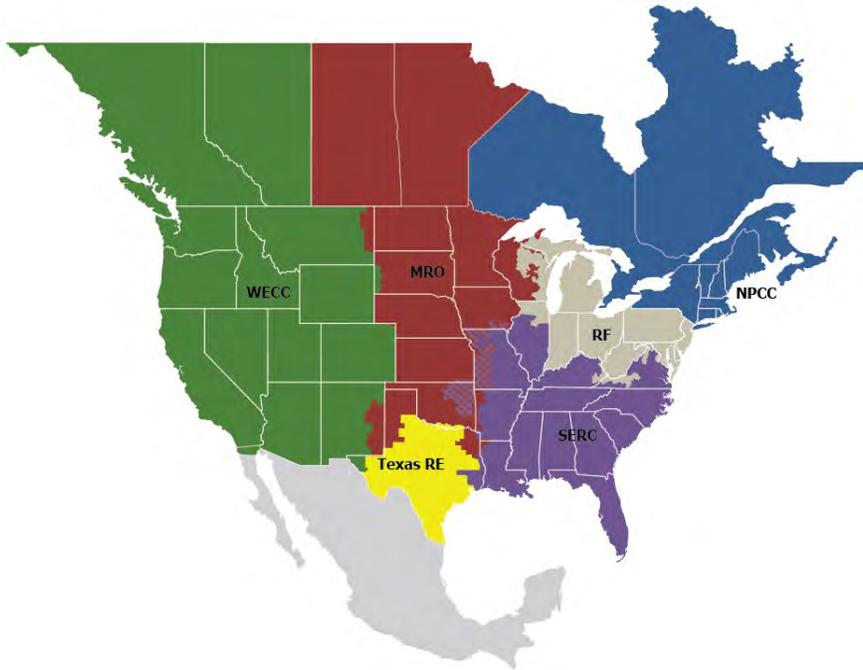
64
65
66

67 **Preface**

68
69 Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise
70 serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric
71 Reliability Corporation (NERC) and the six Regional Entities, is a highly reliable and secure North American bulk power
72 system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of
73 the grid.

74
75 **Reliability | Resilience | Security**
76 *Because nearly 400 million citizens in North America are counting on us*

77
78 The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table
79 below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while
80 associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



81
82

MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

84 **Preamble**

85

86 The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups,
87 develops and triennially reviews reliability guidelines in accordance with the procedures set forth in the RSTC Charter.
88 Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that
89 impact BPS operations, planning, and security. Reliability guidelines provide key practices, guidance, and information
90 on specific issues critical to promote and maintain a highly reliable and secure BPS.

91

92 Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and
93 compliance with applicable mandatory Reliability Standards. Reliability guidelines are not binding norms or
94 parameters nor are they Reliability Standards; however, NERC encourages entities to review, validate, adjust, and/or
95 develop a program with the practices set forth in this guideline. Entities should review this guideline in detail and in
96 conjunction with evaluations of their internal processes and procedures; these reviews could highlight that
97 appropriate changes are needed, and these changes should be done with consideration of system design,
98 configuration, and business practices.

99

100 Metrics

101 Pursuant to the Commission’s Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC
102 ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review
103 consistent with the RSTC Charter.
104

105 **Baseline Metrics**

106 All NERC reliability guidelines include the following baseline metrics:

- 107 • BPS performance prior to and after a reliability guideline as reflected in NERC’s State of Reliability Report and
108 Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments)
- 109 • Use and effectiveness of a reliability guideline as reported by industry via survey
- 110 • Industry assessment of the extent to which a reliability guideline is addressing risk as reported via survey
111

112 **Specific Metrics**

113 The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure
114 and evaluate its effectiveness, listed as follows:
115

- 116 • Ascertain use of DER_A model in planning studies
 - 117 ▪ Ascertain software used in the planning studies with the DER_A model implemented.
- 118 • Ascertain applicability of DER_A model, when using adequately parameterized models, to showcase
119 aggregate behavior of DER opposed to use of other models.
 - 120 ▪ Benchmarking of DER_A model versus a validated, more detailed representation (e.g., PSCAD
121 representation) to align at the T-D Interface, when performed¹.
- 122 • Parameterization of DER_A model using defaults or engineering judgement provided in this reliability
123 guideline versus parameters developed from field measurements or individual utilities and jurisdiction
124 requirements.
- 125 • ~~[Insert metrics specific to the content of this reliability guideline here]~~

¹ This requires validation of transmission and distribution elements outside of the DERs modeled. SPIDERWG members have found that in current benchmarking efforts the validated representation is an ongoing effort to improve a variety of models and not just the dynamic response of the inverter-based DER represented by the DER_A dynamic model.

128 **Executive Summary**

129
130 This guideline provides background material on the recommended DER modeling framework, including the concepts
131 of retail-scale DERs (R-DERs) and utility-scale DERs (U-DERs), information on relevant interconnection standards (IEEE
132 Std. 1547-2003, IEEE Std. 1547a-2014, IEEE Std. 1547-2018, and CA Rule 21), and how the DER_A model parameters
133 can be modified to account for a mixture of vintages of inverter-interfaced DER. The block diagram of the DER_A
134 model is annotated and described so that Transmission Planners (TPs) and Planning Coordinators (PCs) are able to
135 understand the relevant control logic of the dynamic model with respect to the various rules. TPs and PCs are also
136 provided a set of recommendations for developing the modeling parameters for the DER_A dynamic model. These
137 recommendations can also be extrapolated to Transmission Operators (TOPs), Reliability Coordinators (RCs), and
138 other entities performing positive sequence stability simulations of the BPS where an aggregate representation of
139 DERs is required.

140
141 The recommendations developed in this guideline are based on extensive testing of the DER_A dynamic model in the
142 Western Electricity Coordinating Council (WECC) Modeling and Validation Work Group (MVWG) as well as industry
143 expertise and studies discussed in detail in the NERC System Planning Impacts of DER Working Group (SPIDERWG)
144 modeling subgroup. This guideline also serves as a useful reference for building DER models and selecting
145 representative DER model parameters in situations where more detailed information is not yet available.

150 Introduction

151 Applicability

152 This reliability guideline is applicable to TPs, PCs, and other users of DER models for representing aggregate or stand-
153 alone inverter-based DERs.
154

155 Related Standards

156 The topics covered in this guideline are intended as useful guidance and reference materials as TPs and PCs create
157 DER models and modeling assumptions for use in studies generally conducted in the long-term planning and
158 operations planning horizons. While this guidance does not provide compliance guidance of any sort, the concepts
159 apply generally to the following standards:
160

- 161 • MOD-032
- 162 • MOD-033
- 163 • TPL-001
- 164 • PRC-006
- 165 • FAC-002
- 166 • IRO-008
- 167 • IRO-010
- 168

169 Purpose

170 With the proliferation of distributed energy resources (DER), modeling capabilities and practices should be adapted
171 and refined so that transmission planning and operations planning engineers can differentiate between actual end-
172 use loads and DER resources. In the past, and at lower penetrations of DER integrating into the distribution system,
173 net load reduction has been used. Net load reduction is the result of the same or greater demand with an offset due
174 to DER. However, these practices may not be sustainable moving forward as the distribution system continues to
175 integrate more DER. Increasing DER penetration will impact the BES, resulting in changes in transmission loading
176 levels, voltage regulation, and determination of operating limits. It is important to accurately represent the total end-
177 use load and its composition, and model the amount of DER as a separate resource. This will allow entities to
178 adequately represent the impact of future DER integration as well as the performance of DER during transmission
179 system events. Distribution Providers (DPs) should coordinate with their Transmission Planners (TPs) and Planning
180 Coordinators (PCs) to ensure sufficient data for load composition and DER resources is provided, as necessary, for
181 reliable planning and operation of the BES. While many of these resources are not considered BES, sharing of this
182 information is important for developing representative models and performing system studies².
183

184 The purpose of this guideline document is to provide a common framework and modeling parameterization for the
185 DER_A dynamic model for entities to consider for modeling DER in transient stability and powerflow simulations. The
186 framework recommended in this guideline is expected to be particularly useful for representing load and DER in
187 Interconnection-wide studies. More detailed, localized studies may require additional or more advanced modeling,
188 as deemed necessary or appropriate. The modeling practices described here may also be modified to meet the needs
189 of particular systems or utilities, and are intended as a reference point for Interconnection-wide modeling practices.
190

² Transmission planning simulations take into account both BES and non-BES equipment in order to accurately depict the impact on the BES. While DERs are inherently non-BES (as they connect to the distribution system), modeling information is required in order to represent the resources in simulation.

Background

The NERC DERTF published a report³ in February 2017 that focused on connection modeling and reliability considerations for DER. The report provided definitions of DERs, an overview of data and modeling needs, characteristics of nonsynchronous DERs, and potential reliability impacts of DERs on the BPS.

The NERC LMTF⁴ worked in coordination with the NERC DERTF, and published two detailed guidelines on modeling DERs as either stand-alone generating resources or as part of the CLM:

- The *Reliability Guideline: Modeling DER in Dynamic Load Models*, published in December 2016, established a framework for modeling DERs in steady-state powerflow and dynamic simulations.
- The *Reliability Guideline: Distributed Energy Resource Modeling*, published in September 2017, utilized the framework established in the preceding guideline, and provided default parameter values for various DER dynamic models.

At the time of development of that guideline, the DER_A model was still under development and testing and was therefore only briefly mentioned. With the DER_A model now implemented and tested across the major commercial software vendors, ~~this guideline~~ the SPIDERWG provides background and guidance on parameterizing the DER_A model for representing aggregate or stand-alone inverter-based DER resources. This was published in the *Reliability Guideline: Parameterization of the DER A Dynamic Model*.

This reliability guideline, titled *Reliability Guideline: Parameterization of the DER A Dynamic Model for Aggregate DER*, combines the two LMTF/DERTF reliability guidelines with the SPIDERWG reliability guideline to provide the same technical guidance, but housed in one document. This was done as part of an effectiveness and efficiency review in the RSTC.

The following sections briefly describe the DER modeling framework and the definitions and terminology used in that framework. Further, definitions that are used in multiple SPIDERWG documents are posted to the SPIDERWG webpage and are useful for understanding the terms used in this guideline⁵. Models used prior to the DER_A model are also summarized below. Guidance contained in the background and chapters of this document are focused to TPs and PCs; however, other users of the DER_A dynamic model such as RCs and TOPs can also find this guidance useful to their studies.

Historic DER Model Usage and Development

DER model development for use in transmission planning models began with a framework and dynamic model behavior to represent the resources on the distribution system. While some synchronous facilities exist, the historical information has shown that solar PV has been and continues to be the largest technology type of DER. This section describes an overview of data collection for various uses of a DER model.

DER Data Collection

Tps and PCs are required to collect ~~and develop~~ steady-state and dynamic models for Interconnection-wide base case creation. As part of this process, as outlined in MOD-032-1, each PC and each of its TPs jointly develop data requirements and reporting procedures for the PC's planning area. In addition to the aggregate demand collected from the Distribution Provider (DP), accurate modeling of DER should also be included in the data collection process. Accurate modeling of DER as part of the overall demand and load composition is critical for accurate and representative modeling of the overall end-use load in both the powerflow and dynamics cases. DPs (and RPs, if applicable) should coordinate with their respective TP and PC to provide sufficient data to accurately represent the

³ https://www.nerc.com/comm/Other/essntlrbltyrvctskfrcdl/Distributed_Energy_Resources_Report.pdf.

⁴ [https://www.nerc.com/comm/PC/Pages/Load%20Modeling%20Task%20Force%20\(LMTF\)/Load-Modeling-Task-Force.aspx](https://www.nerc.com/comm/PC/Pages/Load%20Modeling%20Task%20Force%20(LMTF)/Load-Modeling-Task-Force.aspx).

⁵ Available here: <https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Terms%20and%20Definitions%20Working%20Document.pdf>

Formatted: Font: Not Italic

aggregate loads, aggregate R-DER and distinct U-DER in their system for both steady-state and dynamic models. At a minimum, TPs and PCs should have the following information related DER (also reproduced in [Table I.1](#)):

- DER modeled as U-DER
 - Type of generating resource (e.g., reciprocating engine, wind, solar PV, battery energy storage)
 - -Distribution bus nominal voltage where the U-DER is connected
 - -Feeder characteristics for connecting U-DER to distribution bus, if applicable
 - Location, both electric and geographic. Related to bulk system bus
 - Capacity of each U-DER resource (Pmax, Qmax, rated MVA, rated power factor, capability curve of U-DER reactive output with respect to different real power outputs down to Pmin)
 - Vintage of IEEE 1547 (e.g., -2018) or other relevant interconnection standard requirements that specify DER performance of legacy and modern DER (e.g., CA Rule 21)
 - Actual plant control modes in operation – voltage control, frequency response, active-reactive power priority
- DER modeled as R-DER
 - ~~Type of generating resource (e.g., reciprocating engine, wind, solar PV, battery energy storage)~~
 - ~~As available, aggregate information characterizing the distribution circuits where R-DER are connected~~
 - Aggregate capacity (Pmax, Qmax) of R-DER ~~behind the T-D Interface for each feeder or load as represented in the powerflow base case~~ and a reasonable representation of the aggregate “capability curve” of reactive output with respect to different real power outputs down to Pmin.
 - Location, both electric and geographic. Related to bulk system bus
 - Vintage of IEEE 1547 (e.g., -2018) or other relevant interconnection standard requirements that specify DER performance of legacy and modern DER (e.g., CA Rule 21)

Formatted

Table I.1: Data Collection Applicability to U-DER and R-DER

Description	U-DER	R-DER
Type of generating resource (e.g., reciprocating engine, wind, solar PV, battery energy storage)	*X	X(aggregate)
Distribution bus nominal voltage	X	
Information characterizing the distribution circuits (X, R)	X	X
Capacity and capability (Pmax, Qmax, reactive capability with respect to real power output)	X	X
Rating (rated MVA, rated power factor)	X	X(aggregate)
Vintage of IEEE 1547 (e.g., -2018) or other relevant interconnection standard requirements that specify DER performance of legacy and modern DER (e.g., CA Rule 21)	X	X
Control modes – voltage control, frequency response,	*X	
Location (electrical bus and geographic area)	X	X

Note: The technical capabilities and default settings of R-DER for frequency response, volt/var control, and P/Q priority as specified by the revised IEEE Std 1547 should also be considered

This information will help the PC, and TP in more representative modeling⁶ of U-DER and R-DER. In situations where this data is not readily available, the entities should use engineering judgment to map the model parameters to

⁶ In some instances a complete dynamic and steady-state model can be provided should the TP and PC allow and approve of it. In this case, much of the listed equipment information, as well as supplemental protection and other models, can be placed inside the file without needing to report the information to the TP/PC outside of the model submittal.

266 expected types of operating modes. The technical capabilities and default settings of R-DER for frequency response,
 267 volt/var control, and P/Q priority as specified by the revised IEEE Std 1547 should also be considered.
 268

269 Further, while the above has been focused on TPs and PCs, DER models are available in the software tools that are
 270 used by Reliability Coordinators (RCs) and Transmission Operators (TOPs) in order to perform their Real-time Analyses
 271 (RTAs), and Operational Planning Analyses (OPAs). Should the RC desire to model aggregate DER at one of their
 272 monitored buses in simulation, the guidance on parameterizing the model should be applicable to describe the
 273 powerflow and transient dynamic behavior.
 274

275 Synchronous DER Models

276 Small, synchronous DER connected at the distribution level can be modeled using standard synchronous machine
 277 models. TPs and PCs should determine if any synchronous DER should be modeled, as applicable, and develop
 278 reasonable model parameters for these resources in coordination with the DPs as necessary. It is recommended to
 279 use the genqec model for representing synchronous machines⁷. The classical machine model, gencls, should not be
 280 used to model DER to avoid any unintentional poorly damped oscillations. In most situations, a generator model
 281 alone will capture the dynamic behavior of the machine in sufficient detail; however, if data is available and the PC
 282 or TP find it necessary, a suitable governor and excitation system may also be modeled. Table I.2 shows examples of
 283 model parameters for a steam unit, small hydro unit, and gas unit for reference. These default parameters are used
 284 solely as a base set to start from assuming zero information about the synchronous DER. These parameters should
 285 change in order to accurately represent the characteristics of the synchronous DER to be modeled.
 286

Table I.2: Synchronous DER Default Model Parameters

Parameter	Steam	Small Hydro	Gas	"Really Small"
MVA	14	32	15	5
T'd0	6	6	6.5	7
T''d0	0.035	0.027	0.03	0.03
T'q0	1	0	1	0.75
T''q0	0.035	0.065	0.03	0.05
H	3	1.7	4.2	3
D	0	0	0	0
Xd	1.8	1.45	1.6	2.1
Xq	1.7	1.05	1.5	2.0
X'd	0.2	0.47	0.2	0.2
X'q	0.4	1.05	0.3	0.5
X''d	0.18	0.33	0.13	0.18
X''q	0.18	0.33	0.13	0.18
XI	0.12	0.28	0.1	0.15
S(1.0)	0.2	0.2	0.1	0.05
S(1.2)	0.6	0.6	0.4	0.3

287 The tripping profile of IEEE 1547 is applicable for synchronous DER for the states that have adopted the standard. As
 288 most states adopted the 1547-2003 version, the tripping profiles for synchronous DER are more likely to behave like
 289

⁷ The model parameters listed may not be a complete set for genqec; however, the other parameters are more suited for limitations on bulk equipment, and the software defaults are adequate for default parameters. Still, should the resource require alterations from the listed table, the general guidance to adapt the parameters to model the equipment still holds.

290 that version of the standard. For states that have adopted 1547-2018, the trip profiles are applicable to synchronous
291 DER as well as inverter-based DER. Parameterization of the voltage thresholds on these models can be parameterized
292 to account for the tripping assumptions in this reliability guideline.

293
294 As there is a potential to aggregate an amount of synchronous DER (using synchronous models) akin to the inverter-
295 based DER (modeled by DER_A), the same guidance in the chapters below hold with respect to altering the
296 parameters based on engineering judgement to reflect the aggregate behavior of that particular T-D composition.
297 The synchronous models are not directly an aggregate model⁸, so care will be needed in parameterizing the models
298 to reflect aggregate behavior and supplemental models may be needed. The T-D Interface represents a variety of
299 points of interconnection for synchronous DER and an aggregate model is a suitable representation; however, the TP
300 or PC can model all synchronous DER individually as indicated in the DER Modeling Framework section below.

302 Second Generation Renewable Energy System Models

303 The second generation generic renewable energy system models were developed between 2010 and 2013 and have
304 since been adopted by the most commonly used commercial software vendors. The suite of models that have been
305 developed can be used to model different types of renewable energy resources, including:

- 306 • Type 1 Wind Power Plants
- 307 • Type 2 Wind Power Plants
- 308 • Type 3 Wind Power Plants
- 309 • Type 4 Wind Power Plants
- 310 • Solar PV Power Plants
- 311 • Battery Energy Storage Systems (BESS)

312 These models were originally developed to represent large utility-scale resources connected to the BPS at
313 transmission level voltage⁹, and provide the greatest degree of flexibility and modeling capability from the
314 commercial software vendor tools using generic models. However, the flexibility also results in a significant number
315 of settings and controls that must be modeled that may be cumbersome for representing DER. If modeling DER using
316 the second generation models, a set of generic parameters can be used for specific studies such as generation
317 interconnection system impact studies (e.g., large capacity resources relative to the local interconnecting network)
318 or other special studies. The generic models for these studies should be accompanied by sufficient model and
319 parameter validation for large DER owners to ensure the model represents the installed equipment.

322 Where actual equipment is to be modeled, specific data from the equipment vendor or at least an understanding of
323 the actual equipment control strategy and performance (e.g., constant power factor control vs. voltage control) is
324 extremely important and should be used. The dynamic behavior of renewable energy systems that are connected to
325 the grid using a power electronic converter interface (i.e., Type 3 and Type 4 wind turbine generators, solar PV, and
326 battery storage) are dominated by the response of the power electronic converter. The converter is a power
327 electronic device and its dynamic response is more a function of software programming than inherent physics as in
328 the case of synchronous machines. Therefore, the concept of default and typical parameters is much less applicable
329 to renewable energy systems than other technologies¹⁰. For example, [setting lvplsw = 1 in Table 2-3](#) describes the
330 flag that turns on ~~the so-called~~ low voltage power logic and is used to emulate the behavior typical of some vendor

⁸ It is not anticipated to impose major functional differences in response when using the genqec model as an aggregate model. However, parameters changes are expected and care needs to be taken when adjusting to represent aggregate behavior. It is not anticipated to have a consequential impact in simulation at this time due to the lower share of synchronous DER in the totality of the DER on the system.

⁹ P. Pourbeik, J. Sanchez-Gasca, J. Senthil, J. Weber, P. Zadehkhosht, Y. Kazachkov, S. Tacke, J. Wen and A. Ellis, "Generic Dynamic Models for Modeling Wind Power Plants and other Renewable Technologies in Large Scale Power System Studies", IEEE Transactions on Energy Conversion, published on IEEE Xplore 12/13/16, DOI 10.1109/TEC.2016.2639050.

¹⁰ Generic models representing renewable energy systems include a common model structure that allows for representing different types of control strategies and characteristics. These models can be tuned or configured to represent specific vendor equipment by adjusting the model parameters.

equipment under low voltage conditions. However, $lvplsw$ is a function of the software and vendor controls in the power converter, and should be set according to the respective vendor characteristics to be emulated, if that information is available. The default example values for the models below in software for modeling DER as a second generation renewable model should be altered to reflect the distribution-connected alterations and equipment settings. This reliability guideline focuses on the der a dynamic model, which is a model to represent aggregate dynamic behavior. These second generation renewable models are more appropriate for single plant representations. The SPIDERWG recommends the use of the der a dynamic model for representing aggregate DERs in simulation¹¹ rather than using the second generation renewable models, which could be used for representation of a single, larger plant connected to the distribution system. assume a DER with constant power factor control, no reactive current injection during faults, P priority on the current limits, and no frequency response capability. This is typical of most DER in service to date. The models below do not include the lhvrt and lhfrt models, which should be used if low/high voltage and frequency ride through capabilities are to be emulated.

DER Modeling Framework

For the purposes of steady-state and dynamic modeling of DERs in BPS reliability studies, DERs can be defined as either utility-scale DERs, U-DERs, or R-DERs, which the previous guidelines have defined as follows:

- **U-DER:** DERs directly connected to, or closely connected to, the distribution bus¹² or connected to the distribution bus through a dedicated,¹³ non-load serving feeder. These resources are typically three-phase interconnections and can range in capacity (e.g., 0.5 to 20 MW).
- **R-DER:** DERs that offset customer load, including residential,¹⁴ commercial, and industrial customers.¹⁵ Typically, the residential units are single-phase while the commercial and industrial units can be single- or three-phase facilities.¹⁶

Both U-DERs and R-DERs can be differentiated and should be accounted for in powerflow base cases and dynamic simulations. Modeling U-DERs and R-DERs in the powerflow provides an effective platform for linking this data to the dynamics records and ensuring that the dynamics of these resources are accounted for. R-DERs represent the truly distributed resources throughout the distribution system whose controls are generally reflective of IEEE Std. 1547¹⁷ vintages or other relevant requirements for the region they are being interconnected. U-DERs are typically relatively large, stand-alone installations that may have more complex controls or requirements associated with their interconnection. The vintage of IEEE Std. 1547 is an indicator for a large set of controls; however, the interconnection

¹¹ It is possible to use the der a model to represent a single plant; however, careful parameterization is required to ensure the aggregate dynamic model is properly representing the single plant.

¹² The distribution bus is connected to a transmission voltage bus via the transmission/distribution transformer. Resources not directly connected to this bus do not meet the criteria for this definition.

¹³ In some cases, U-DERs may not be located on a dedicated feeder; rather, U-DERs may be installed on the load-serving feeders near the head of the feeder. In either case, the framework presented here can and should be adapted to each TP and PC needs. In this case, these larger DER installations can still be represented as U-DERs. In other cases, they may be better suited to be modeled as R-DERs. Engineering judgment should be used to determine which modeling approach is most appropriate.

¹⁴ This also applies to community DERs that do not serve any load directly but are interconnected directly to a distribution load serving feeder.

¹⁵ This often includes behind the meter generation but may also include individually metered DERs and systems that export beyond customer load at a particular site boundary.

¹⁶ For the purposes of modeling, some larger utility-scale U-DER may exist along the load-serving distribution feeder and may be electrically distant from the distribution substation. In these cases, they may be represented as R-DERs since they offset customer load. The aggregate power output can potentially exceed the total load demand of the distribution feeder.

¹⁷ IEEE Std. 1547-2003, Standard for Interconnecting Distributed Resources with Electric Power Systems, July 2003:

<https://standards.ieee.org/standard/1547-2003.html>.

IEEE Std. 1547a-2014, IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems – Amendment 1, May 2014:

<https://standards.ieee.org/standard/1547a-2014.html>.

IEEE Std. 1547-2018, IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, April 2018: <https://standards.ieee.org/findstds/standard/1547-2018.html>.

IEEE Std. 1547-2018, 6/4/2018: Errata to IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces: http://standards.ieee.org/findstds/errata/1547-2018_errata.pdf.

Formatted: Font: 9 pt

Formatted: Font: 9 pt

requirements of that local area may be over and above, so looking at the requirements of a particular interconnection for these larger, stand-alone installations will be a better representation of the equipment's operation. That said, IEEE 1547 would be applicable to the equipment, and any settings would be above and beyond.

TPs and PCs should identify thresholds where U-DERs should be explicitly modeled and R-DERs should be accounted for in the powerflow and dynamics cases. The thresholds should be based on either the individual or aggregate impact of DER on the BPS:¹⁸

- Gross aggregate nameplate rating of an individual U-DER facility directly connected to the distribution bus or interconnected to the distribution bus through a dedicated, non-load serving feeder
- Gross aggregate nameplate rating of all connected R-DERs that offset customer load including residential, commercial, and industrial customers

The thresholds for modeling U-DERs and R-DERs, determined using engineering judgment¹⁹, can be defined as follows:

- **U-DER Modeling:** Any individual U-DER facility rated at or higher than the defined individual U-DER modeling threshold should be modeled explicitly in the powerflow case at the low-side of the transmission–distribution transformer. A dynamics record should be used to account for the transient behavior²⁰ of the individual U-DER plant. Individual U-DERs less than the defined threshold should be accounted for in powerflow and dynamics as an R-DER (as described below). Multiple similar U-DERs connected to the same substation low-side bus could be modeled as an aggregate resource as deemed suitable by the TP or PC. This is also a good modeling practice to aggregate DER that is closer to the feeder head and would have less impact by the modeled feeder equivalent in the simulation. Facilities that are lower than the individual modeling threshold should either be modeled as R-DERs or as a separate aggregation near the feeder head in the framework.
- **R-DER Modeling:** If the gross aggregate nameplate rating of R-DERs connected to a feeder exceeds the defined R-DER modeling threshold defined in the TP and PC modeling practices, these R-DERs should be accounted for in dynamic simulations as part of the dynamic load model. While this may not require any explicit model representation in the powerflow base case, the amount of R-DERs can be accounted for as part of the powerflow load record and integrated into the dynamic model as an explicit DER component. The threshold for modeling R-DER should be 0 MVA, meaning that all forms of DERs be accounted for (and not netted with the load) to the extent possible. Further, this does not mean that a single generator record is required for each R-DER. Rather, establishing a threshold of 0 MVA for R-DER means that a TP or PC should represent all DER in their system²¹.

Figure I.1 shows the recommended powerflow representation for accounting for U-DERs. The left side of **Figure I.1** shows the conventional powerflow representation of the load record. This has conventionally included both load and DERs (representing a net load quantity as opposed to a gross load quantity). However, the right side of **Figure I.1** shows how the transmission–distribution (T–D) transformer can be modeled explicitly and the gross

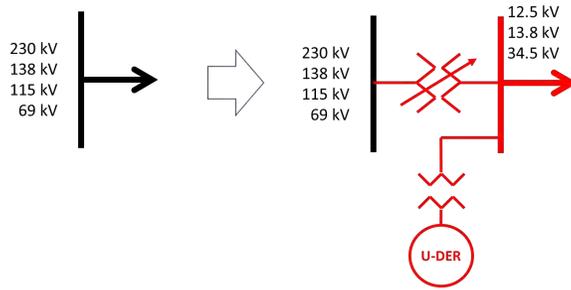
¹⁸ This may include many different types of DERs, including distributed solar PV, energy storage, synchronous generation, and other types of DERs. Including synchronous generation in the CLM as a component of R-DERs may not be possible across all software platforms.

¹⁹ SCADA data points and monitoring of native load may provide some level of engineering judgement for the amount of DER that is represented by one load record. However, determination of nameplate ratings to represent in models requires further data collection practices. TPs and PCs should interface with their DPs to obtain known DER capacities and determine the gross aggregate nameplate for their simulations.

²⁰ Depending on complexity of the actual U-DER, for inverter coupled U-DER, more sophisticated models such as the second generation generic renewable energy system models may also be used (i.e., regc_a, reec_b and repc_a). Other U-DERs (e.g., synchronous natural gas or steam-turbine generators) can also be modeled using standard models available in commercial software platforms.

²¹ TPs and PCs should establish this zero MVA threshold as a best practice for modeling as it requires data collection of resources prior to needing modeling information past a non-zero threshold. It has been reported that information needed from facilities after the non-zero threshold has been met is limited and model development is restricted for the facilities that were interconnected under that limit. The zero MVA threshold prevents data loss like this from occurring.

397 load can be moved to the low side distribution bus. U-DERs above the specified threshold can be modeled explicitly
 398 via their own step-up transformers as applicable. If the U-DERs are connected through a dedicated feeder or circuit
 399 to the low-side bus, then that would also be explicitly modeled in the powerflow.



400
 401 **Figure I.1 Representing U-DER in the Powerflow Base Case**
 402 **Figure B.1: Representing a U-DER in the Powerflow Base Case**

403 To capture the R-DER in the powerflow, the load records now²² have the capability to input the R-DER quantity along
 404 with the gross load amount. **Figure I.2****Figure B.2** shows an example of the R-DERs included in the powerflow load
 405 records. The red box shows the R-DERs specified and the blue box shows the net load equal to the actual load minus
 406 the R-DERs. For example 80 MW and 20 MVar of actual load with 40 MW and 0 MVar of R-DER at Bus 2.
 407
 408

Number of Bus	Name of Bus	Area Name of Load	Zone Name of Load	ID	Status	MW	Mvar	MVA	S MW	S Mvar	Dist Status	Dist MW Input	Dist Mvar Input	Dist MW	Dist Mvar	Net Mvar	Net MW
1	2 Two	Top	1	1	Closed	80.00	20.00	82.46	80.00	20.00	Closed	40.00	0.00	40.000	0.000	20.000	40.000
2	3 Three	Top	1	1	Closed	220.00	40.00	223.61	220.00	40.00	Open	110.00	0.00	110.000	0.000	40.000	220.000
3	4 Four	Top	1	1	Closed	160.00	30.00	162.79	160.00	30.00	Closed	80.00	0.00	80.000	0.000	30.000	80.000
4	5 Five	Top	1	1	Closed	260.00	40.00	263.06	260.00	40.00	Open	130.00	0.00	130.000	0.000	40.000	260.000
5	6 Six	Left	1	1	Closed	400.00	0.00	400.00	400.00	0.00	Closed	200.00	0.00	200.000	0.000	0.000	200.000
6	7 Seven	Right	1	1	Closed	400.00	0.00	400.00	400.00	0.00	Closed	200.00	0.00	200.000	0.000	0.000	200.000

409
 410 **Figure I.2: Capturing R-DER in the Powerflow Load Records [Source: PowerWorld]**
 411 **Figure B.2: Capturing a R-DER in the Powerflow Load Records [Source: PowerWorld]**

412 Once represented in the powerflow base case, data for the CLM can be modified to account for explicit representation
 413 of the DERs and the T/D transformer. **Figure I.3****Figure B.3** shows the dynamic representation of the CLM, where the
 414 distribution transformer impedance is not represented in the dynamic load record. Rather, it is modeled explicitly in
 415 the powerflow to accommodate one or more U-DER.²³ Any load tap changer (LTC) modeling²⁴ would be done outside
 416 the CLM, such as enabling tap changing in the powerflow²⁵ and using the *ltc1* model in dynamic simulations. Motor
 417 load and the distribution equivalent are modeled as part of the CLM, and the R-DERs are represented at the load bus
 418 based on the data entered in the load record table.
 419

²² All commonly used commercial simulation software platforms now have the ability to represent DERs as part of the powerflow load record in an attempt to standardize and unify modeling practices for representing DERs in powerflow base cases.

²³ If only R-DERs are represented at a bus (no U-DERs), then the T-D transformer does not necessarily need to be explicitly modeled in the powerflow since it can be accounted for in the CLM dynamic record, including LTC action. However, if LTC action needs to be modeled in the steady-state analyses in any way, then explicit modeling of the T-D transformer in the powerflow may be needed.

²⁴ Utilities using transformers without under-load tap changers (ULTCs) capability but with voltage regulators at the head of the feeder could model this in the CLM with a minimal transformer impedance but active LTCs to represent the voltage regulator.

²⁵ For example, by specifying settings in the transformer record and enabling tap changing in the powerflow solution options.

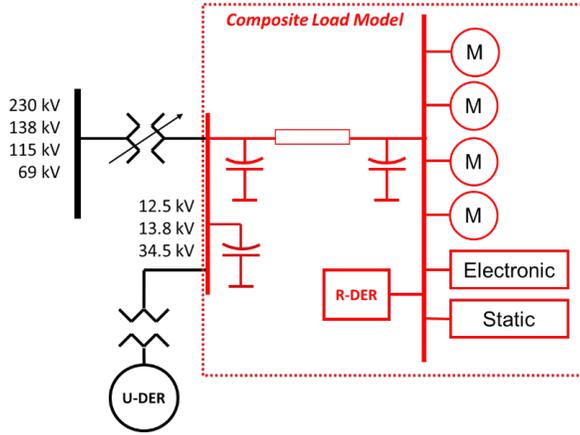


Figure I.3: Figure B.3: CLM Representation with U-DER Represented in the Powerflow Base Case

Figure B.3. CLM Representation with U-DER Represented in the Powerflow Base Case

With FERC Order 2222²⁶ introducing the DER Aggregator, the initial starting split of capacity and the type of information provided from such entities. SPIDERWG has produced a white paper that has highlighted some BPS reliability tie-ins to DER Aggregators; however, when parameterizing the steady state representation, logical flow charts as in Figure I.4 assist in providing planners a way to disaggregate information provided from a DP or a DER aggregator for representation in transmission cases. These logical flows, in short, provide a crude method to begin placed DER into model representations. It is to be noted that these percentage splits in Figure I.X are to be considered as initial default values and modifications to the values may be necessary based on the information received from a DP or a DER Aggregator.

Formatted: Keep with next

Formatted: Caption, Left, Space After: 0 pt

Formatted: Cross Reference Char

²⁶ The text of this order can be found here: https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf

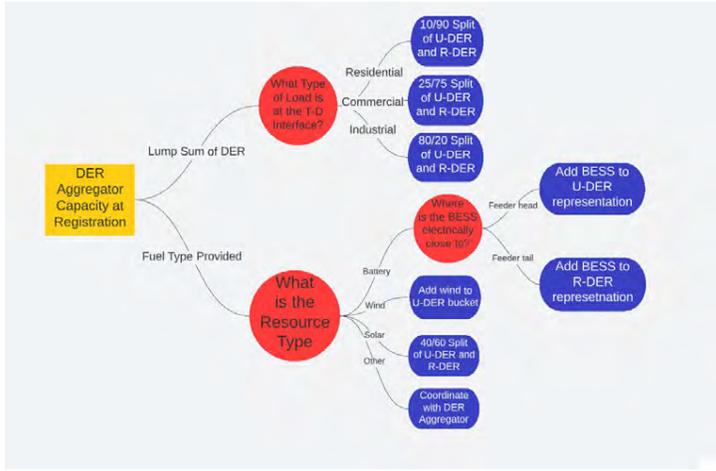


Figure I.4: Decision tree for DER Disaggregation

Formatted: Keep with next

Formatted: Caption

Overview of the DER_A Model

The DER_A model is a simplified version of the second generation generic renewable energy system models (i.e., regc_a, reec_b, repc_a, lhvrt, lhfrt) used to represent inverter-based DERs (i.e., utility-scale wind, solar photovoltaic (PV), and battery energy storage resources). The DER_A model uses a reduced set of parameters meant to represent the aggregation of a large number of inverter-interfaced DERs. It is also an improvement over the pvd1 model in that it includes additional modeling flexibility for more advanced and representative capabilities introduced in IEEE Std. 1547-2018 and California Rule 21. The DER_A model can be used to represent U-DERs (individual DER resources, or a group of similar U-DERs) and can also be used to represent R-DERs as either a standalone DER dynamic model or as part of the CLM. The DER_A model includes the following features:

- Constant power factor and constant reactive power control modes (allows voltage control to be active along with PF/Q control, depending on whether voltage is within the deadband or not)
- Active power-frequency control with droop and asymmetric deadband
- Voltage control with proportional control and asymmetric deadband (may be used to either represent steady-state voltage control or dynamic voltage support, depending on chosen time constants)
- Representation of a fraction of resources tripping or entering momentary cessation²⁷ at low and high voltage, including a four-point piece-wise linear gain (partial tripping includes a timer feature as well)
- Representation of a fraction of resources that restore output following a low or high voltage or frequency condition (representation of legacy trip and modern ride-through capabilities in a single model)
- Active power ramp rate limits during return to service after trip or enter service following a fault or during frequency response

²⁷ Momentary cessation is a mode of operation during which no current is injected into the grid by the inverter during low or high voltage conditions outside the continuous operating range. This leads to no current injection from the inverter, and therefore, no active or reactive current (and no active or reactive power). Refer to the NERC *Reliability Guideline: BPS-Connected Inverter-Based Resource Performance*. The concept applies to both BPS-connected inverter-based resources and DERs:

https://www.nerc.com/comm/PC/Reliability_Guidelines_DL/Inverter-Based_Resource_Performance_Guideline.pdf

- Active-reactive current priority options (used to represent dynamic voltage support during fault events)
- The capability to represent generating or energy storage resources²⁸ (The model allows for absorption of active power; however, charging and discharging as modeled in reec_c is not included. Therefore, the DER_A model should not be used for devices with only a few seconds of energy injection (e.g., super capacitor systems))

The overall block diagram for the DER_A model can be found in [Appendix C](#)

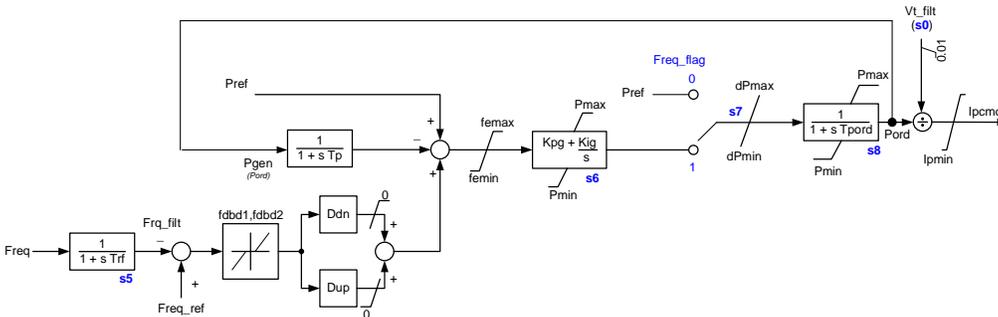
²⁸ This guideline focuses mostly on using the DER_A model to represent generating resources, primarily distributed solar PV generation. However, the DER_A model can be used to represent energy storage, and future guidelines may be developed on this topic as necessary.

465 **Chapter 1: Annotated DER_A Block Diagram**

466 This chapter briefly describes the functional sections of the DER_A model and provides a high-level overview of what
 467 the various blocks represent. Refer to the DER_A specification document²⁹ for more detailed information regarding
 468 implementation. The sections below describe the general control aspects of the different functional sections of the
 469 model.
 470
 471

472 **Active Power-Frequency Controls**

473 The active power-frequency controls portion of the DER_A model are shown in **Figure 1.1**. The frequency input signal
 474 feeding the active-power frequency controls is first passed through a frequency measurement time constant, T_{rf} . The
 475 filtered voltage is compared against a reference signal. The f_{dbd1} and f_{dbd2} parameters represent the active power-
 476 frequency control deadband for overfrequency and underfrequency, respectively. The D_{dn} and D_{up} parameters
 477 represent the overfrequency and underfrequency droop gains, respectively. T_p represents an active power
 478 measurement time constant. When active power-frequency control is enabled, $Freq_flag$ is set to 1. To disable active
 479 power-frequency control of the model, set $Freq_flag$ to 0. The frequency error is limited by f_{emax} and f_{emin} and
 480 goes through a PI controller with K_{pg} and K_{ig} parameters. The dP_{max} and dP_{min} parameters limit active power
 481 upward and downward ramp rates. P_{max} and P_{min} represent the maximum and minimum power output,
 482 respectively. T_{pord} is the power-order time constant, and it can be used to represent the small time lag for changing
 483 the power reference (when $Freq_flag = 0$) or the open-loop time constant associated with the full controls (when
 484 $Freq_flag = 1$), as specified in IEEE Std. 1547-2018. Active current command ($ipcmd$) is calculated using power-order
 485 (P_{ord}) divided by filtered terminal voltage (V_{t_filt}), and it is limited by Ip_{max} and Ip_{min} .
 486



487 **Figure 1.1: Active Power-Frequency Controls**

488 **Frequency Tripping Logic Input**

489 The frequency input signal feeding the active-power frequency controls is first passed through a frequency
 490 measurement time constant, T_{rf} . A low voltage inhibit logic was added to the model, which is shown in **Figure 1.2**.
 491 When voltage falls below a threshold (V_{pr}), then the frequency relay model is bypassed. This is common in frequency
 492 protective functions, to avoid spurious tripping during transients. In numerical simulations, this low voltage inhibit
 493 is also used to avoid tripping on numerical spikes during discontinuities.³⁰
 494
 495
 496

²⁹ P. Pourbeik, "Proposal for DER_A Model," June 19, 2019; https://www.wecc.org/Reliability/DER_A_Final_061919.pdf.

³⁰ https://www.wecc.biz/Reliability/WECC_White_Paper_Frequency_062618_Clean_Final.pdf

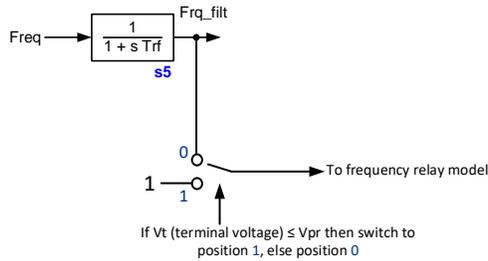


Figure 1.2: Frequency Tripping Logic Controls

Reactive Power-Voltage Controls

The reactive power-voltage controls portion of the DER_A model are shown in Figure 1.3. Setting *pflag* to 0 or 1 selects either constant reactive power control or constant power factor control, respectively. The *pfaref* parameter is internally calculated to achieve the necessary reactive power order for the current active power order. Reactive power is then divided by filtered terminal voltage (*Vt_filt*) and passed through a reactive current calculation time constant (*Tiq*). Voltage control is included in the model. Terminal voltage (*Vt*), after a measurement time constant (*Trv*), passes through a lower (*dbd1*) and upper (*dbd2*) deadband and proportional control gain (*Kqv*). Respectively, *lqh1* and *lql1* specify maximum and minimum limits of reactive current injection. To disable the reactive power-voltage control function of the model, set *Kqv* to 0.

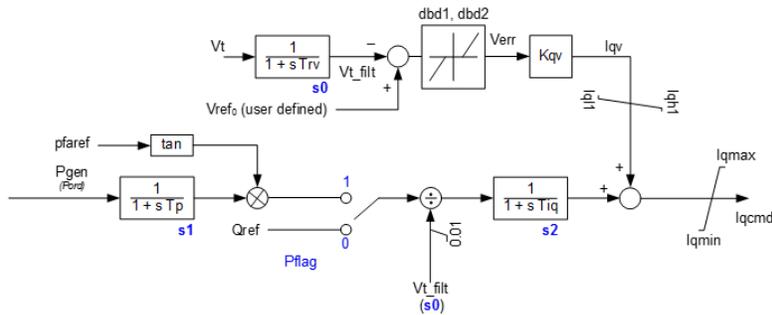


Figure 1.3: Reactive Power-Voltage Controls

Active-Reactive Current Priority Logic

With the active and reactive command values established in the active power-frequency and reactive power-voltage control elements, the command values are passed through maximum (*Ipmax/Iqmax*) and minimum (*Ipmin/Iqmin*) active and reactive current limits. Figure 1.4 shows the current limit logic and how that logic interacts with the limiters. When the *typeflag* parameter is set to 10, this denotes a DER that is a generating unit with *Ipmin* = 0 while setting it to 01 denotes a DER that is an energy storage device with *Ipmin* = -*Ipmax*.

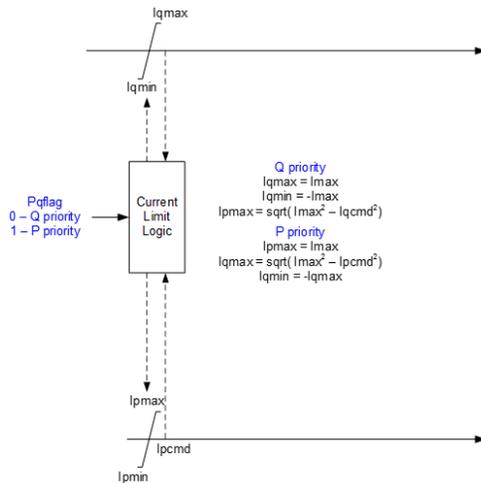


Figure 1.4: Active-Reactive Current Priority Controls

Current limits, particularly in inverter-based resources, determine how the resource response to large grid disturbances, such as faults on the BPS. The current limit logic is determined based on whether the resource is operated in active or reactive current priority and dictated by the *pqflag* parameter. The priority logic controls *Iqmax* and *Iqmin* based on the priority setting and maximum total current of the inverter (*Imax*). Figure 1.4 also shows the equations used for this control. For example, if reactive current priority is selected, then *Iqmax* and *Iqmin* are limited to *Imax* and *-Imax*, respectively. Based on the reactive current ordered from the controls, the active current limit is then simultaneously calculated to utilize the remaining amount of total apparent current capability (*Imax*). A circular capability curve is assumed.

Example Consideration of Q Priority and P Priority

As an example, if the magnitude of current is limited to 1.2 pu (*Imax*), and the priority scheme is defined by reactive current priority, then a maximum limit of 1.2 pu is imposed on the reactive portion of current. The maximum active current (at this reactive current limit) will be 0.0 pu = $\sqrt{1.2^2 - 1.2^2}$. However, this does not imply that the active current will always be zero. This is the limited value of active current only when the reactive current is at its limit. However, if a reactive current of 1.0 pu is sufficient for the system, as decided by the reactive power-voltage controls, then the maximum active current can be 0.66 pu = $\sqrt{1.2^2 - 1.0^2}$. Hence, the reactive power-voltage controller not only decides the amount of reactive current to be injected but also the maximum amount of active current that can be injected for the decided value of reactive current. The active current controller then decides the actual value of active current to be injected. An opposite situation occurs when an inverter is in active current priority.

Prior to approval of IEEE Std. 1547-2018, all DERs on the system were not required to have reactive power-voltage control capability. Thus, the vintage of inverters that conform to this standard should have a P priority setting. With the approval of IEEE Std. 1547-2018, which requires inverters to have reactive power-voltage control capability (with preference to reactive current), it is expected that this capability will be used by the inverter, so the current priority setting should be set to Q priority. However, the impact of setting DER to P priority versus Q priority should be assessed with detailed studies since both settings could have a positive impact.

For example, upon the occurrence of a fault, a larger percentage of gross load can trip if located electrically close to the fault and if adjacent DERs are in Q priority, compared to when adjacent DERs are in P priority. However, at locations located electrically farther away from the fault, a larger percentage of gross load can trip when adjacent DERs are in P priority compared to when adjacent DERs are in Q priority. Closer to the fault, when in Q priority and with voltage control enabled, the DER reactive current would hit I_{max} and active current reduces to zero. The intention behind this is to try and support local voltage and prevent tripping of gross load. However, when the DER's active current contribution reduces to zero due to full output of reactive current (bear in mind that this is not to be confused with momentary cessation), the net load at the load substation bus increases, which can result in voltage reducing at nearby non-DERs causing load to trip. Now, when the DER is in P priority, the net load at the load bus would be lower (assuming that the DERs have not gone into momentary cessation mode), and thus, the voltage wouldn't fall as much at nearby non-DER buses, and as a result, a trip of gross load is lesser. Farther away from the fault, due to the initial higher voltage levels (as compared to the voltage levels closer to the faults), voltage support in Q priority has a greater effect and so even though the net load may increase (due to decrease in active current contribution from DER to accommodate injection of reactive current) the voltage drop (due to increase in net load) does not counterbalance the voltage support from the DER. Therefore, there is less gross load tripping.³¹ It should be noted that this behavior may not be the norm, but it is a possibility; therefore, setting DER priority settings should be conducted based on detailed system studies.

Fractional Tripping

The DER_A model includes a fractional tripping control³² that is intended to represent a portion of the DER tripping on low or high voltage³³ as shown in Figure 1.5. The $vtripflag$ controls voltage tripping and the $ftripflag$ controls frequency tripping separately.³⁴ $Vfrac$ defines the fraction of DERs that recover after voltage returns to within acceptable limits after dropping below or above the threshold values. For frequency tripping, a single low (fl) and high (fh) frequency cutout breakpoint is implemented since frequency variation along the distribution feeder is relatively constant (as compared with voltage). Hence, there is no partial tripping due to frequency.³⁵ Tv is a time constant representing the time delay for voltage related partial tripping (shown in Figure 1.5).

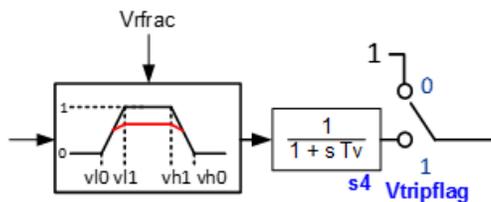


Figure 1.5: Fractional Tripping Controls

The $v/0$ and $v/1$ parameters are the low voltage cutout breakpoints and the $v/h0$ and $v/h1$ parameters are the high voltage cutout breakpoints. For example, when voltage falls below $v/1$, a fraction of the DERs will cutout, with a linearly increasing amount of DERs experiencing cutouts down to $v/0$ where all DERs will have cut out. The output of

³¹ R. Quint, I. Green, D. Ramasubramanian, P. Pourbeik, J. Boemer, A. Gaikwad, D. Kosterev, C. DuPlessis, M. Osman, "Recommended DER Modeling Practices in North America," 25th International Conference and Exhibition on Electricity Distribution (CIRED) [under review].

³² Fractional tripping should not be confused with dispatch scenario development that can take into account other outages (e.g., maintenance outages) in the powerflow models and not the dynamic transient set of models.

³³ There is no partial tripping due to frequency in the DER_A model. If there is a frequency trip, then the entire amount of DER trips.

³⁴ GE PSLF does not have these flags; however, Siemens PTI PSS[®]E, PowerWorld Simulator, and Powertech TSAT do have these flags.

³⁵ If there is a frequency trip, then the entire amount of DER trips.

Formatted: Font: 9 pt

Formatted: Font: 9 pt

the fractional tripping block is the value that gets applied to $ipcmd$ and $iqcmd$.³⁶ If voltage falls outside the specified thresholds for the predefined amount of time (below $tv0$ or $tv1$ or above $tvh0$ or $tvh1$), then the recovery of resources changes from the black line to the red line. This is intended to represent only a fraction of resources recovering from the decrease in voltage ($Vrfrac$); Those resources are expected to trip off-line and return to service some time beyond a typical transient simulation.

The fractional tripping logic does not represent any actual controls but is rather an attempt at emulating the fact that not all R-DERs will necessarily experience the same terminal voltage on a feeder and therefore they may not trip at the same time and for the same level of voltage excursion at the head of the feeder. Thus, this is an attempt based on much deliberation among many participants and stakeholders to come up with a method to emulate such behavior. As experience is gained with the model, this and perhaps other aspects may be refined over time.

Refer to the model specification document for more details related to model implementation and pseudo code.³⁷

Fractional Tripping Derivation

Specific data related to DERs tripping is often not available, and engineering judgment must be used to determine reasonable tripping values. These values should be based on the expected vintage of DERs and the distribution circuit characteristic. Each interconnection standard (e.g., IEEE Std. 1547-2003, IEEE Std. 1547a-2014, IEEE Std. 1547-2018) may have different ride-through and trip settings for abnormal voltage and frequency, with multiple magnitude/time duration pairs. Refer to [Table 2.1](#) and [Table 3.1](#) for initial details on setting these parameter values. It should be noted that these values may need to be changed depending on the individual system where the DER_A is applied. TPs should coordinate with their Distribution Providers (DPs) to attempt to track the proportion of DERs that could be expected to fall within each category. The proportion of DERs within each category may be inferred by DPs by assessing the date of each DER installation. The DER_A model does not include multiple points; however, these are likely not needed for stability studies in most cases. Typically, it is recommended to model the trip thresholds that relate to the shorter trip times³⁸ since this scenario is what covers most stability simulations. The thresholds are selected to account for the varied response of aggregate DERs tripping across a distribution system while taking into account the voltage drop (V_{DROP}) across the feeder.

Key Takeaway:

The DER_A model does not include multiple points for tripping; however, these are likely not needed for stability studies in most cases. Typically, it is recommended to model the trip thresholds that relate to the shorter trip times since this scenario is what covers most stability simulations.

Fractional trip settings are based on how the DERs are represented in powerflow and dynamics. There are multiple modeling options for how to set these fractional trip settings including the following (see [Figure 1.6](#)):

- Option 1 (Recommended for U-DERs):** The U-DER is represented in the powerflow base case as a generator, and has an associated DER_A model in dynamics. The modeled U-DER is intended to represent one or multiple U-DERs connected directly to or very close to the distribution substation. In this case, load modeling is unrelated, since the U-DER model explicitly represents a single or group of U-DERs. Partial tripping is not applied, and the DER trip settings can mirror those specified in the respective interconnection requirements. Parameters $v0$, $v1$, $vh0$, and $vh1$ have a direct relation to those interconnection requirements. $Vrfrac$ can be set to 1 or 0 depending on the vintage of DER.

³⁶ Refer to the DER_A Model Specification document for a detailed pseudo code explanation of how the fraction/partial tripping is calculated: https://www.wecc.biz/Reliability/DER_A_Final.pdf.

³⁷ P. Pourbeik, "Proposal for DER_A Model," June 19, 2019: https://www.wecc.org/Reliability/DER_A_Final_061919.pdf.

³⁸ As in, if the specification includes multiple trip magnitude-duration points, use the shortest duration point.

- 625 • **Option 2 (Recommended for R-DERs):** An aggregate amount of R-DERs spread throughout the distribution
626 system is represented in the powerflow base case as a DER component of the load record. In dynamics, this
627 information is integrated into the CLM with DER representation (e.g., cmpldwg). The equivalent distribution
628 impedance is then represented in the CLM as well, with both load and DER represented at the load bus across
629 the equivalent feeder impedance. Voltage drop (V_{DROD}) across the feeder is accounted for explicitly ($V_{DROD} =$
630 $V_{SUB} - V_{LOAD}$). The Electric Power Research Institute (EPRI) has shown that a V_{DROD} of 2–8% is typical for most
631 distribution feeders; a value around 5% is a reasonable assumption for DER (and load) modeling. Assuming a
632 trip setting of 0.5 pu (see [Figure 1.6](#)), then DERs start tripping when the load bus voltage reaches 0.5 pu. All
633 DERs have tripped when the substation bus voltage reaches 0.5 pu, meaning that the load bus voltage is at
634 0.45 pu. Therefore, $vI1$ equals 0.5 pu and $vI0$ equals 0.45 pu in this example. This concept can be used to
635 determine trip settings for other standards as well.
- 636 • **Option 3:** An aggregate amount of R-DERs spread throughout the distribution system can also be represented
637 in the powerflow base case as a stand-alone generator. This does not necessarily follow the recommended
638 framework described above; however, it is a modeling option. In this case, the same concept as presented in
639 Option 2 applies with some minor modifications. In this case, the DERs are connected to the substation bus.
640 The DERs start tripping when the implied load-side bus (distribution feeder impedance not represented)
641 reaches 0.5 pu (so $V_{SUB} = V_{LOAD} + V_{DROD} = 0.55$ pu) and all are tripped when the substation bus voltage reaches
642 0.5 pu, so $vI1$ equals 0.55 pu and $vI0$ equals 0.5 pu in this example. Again, this concept can be applied to
643 determine trip settings for other standards as well.
644

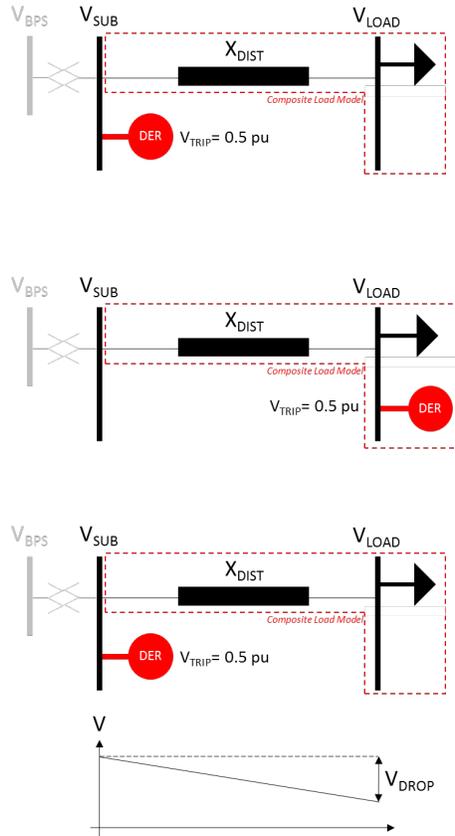


Figure 1.6: Fractional Trip Derivation Examples

The fractional trip settings can be used to model momentary cessation, if needed, in a relatively crude manner. For example, setting $v/1$ and $v/0$ to the momentary cessation settings will result in cessation of current below the specified thresholds. Selecting times $tv/0$ and $tv/1$ should be done with care to ensure the resources appropriately return following voltage recovery.³⁹ Note that momentary cessation is not required for Category II resources in IEEE Std. 1547-2018; however, the permissive operation range does allow for momentary cessation. TPs should consider sensitivity studies to understand the impact that this may have on studies.⁴⁰

³⁹ The settings $tv/0$ and $tv/1$ are related to the trip characteristics, and they do not apply to momentary cessation. Parameter $v/0$ can be set to the highest undervoltage point in which momentary cessation starts occurring.

⁴⁰ The fractional trip settings are not intended to match the IEEE Std. 1547 trip characteristics exactly; the DER_A model is intended to represent an aggregate behavior of DERs.

Voltage Source Interface Representation

In the DER_A model, a voltage source interface representation⁴¹ is implemented at the network interface to support numerical stability of the model in the simulation tools (see [Figure 1.7](#)).⁴² In reality, all modern inverters used on the grid-side of power electronic interfaced energy sources use a voltage source converter (VSC), specifically, a dc voltage source behind a full four-quadrant controlled dc to ac power electronic converter.⁴³ The current through the VSC is strictly controlled by the controls of the inverter. This can thus be represented as a voltage source behind an impedance. In order to develop the value of the voltage behind the impedance, the values of $ipcmd$ and $iqcmd$ are used to evaluate the voltage drop across the impedance and thereby develop the complex voltage. The representation is a voltage behind a reactance, X_e . Typical values for X_e are in the range of 0.25 pu.⁴⁴

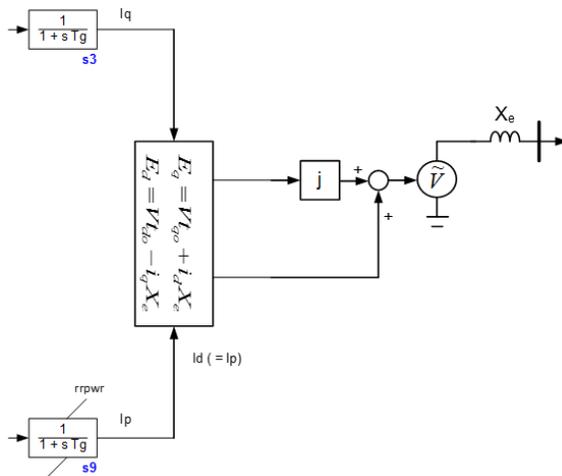


Figure 1.7: Voltage Source Representation

⁴¹ D. Ramasubramanian, Z. Yu, R. Ayyanar, V. Vittal and J. M. Undrill, "Converter Model for Representing Converter Interfaced Generation in Large Scale Grid Simulations", IEEE Trans. PWRs, April 2016.

⁴² The *PVD1* and second generation renewable energy system models use a current source representation, which has proved to cause numerical issues in simulations—particularly at increased penetration levels of these models.

⁴³ A *typeflag* parameter exists in the model to denote whether the model is representing a generator or a battery energy storage system (BESS). The model does not explicitly represent four-quadrant control, as it does not represent a single BESS but rather an aggregated model. If the model is used to represent BESS, the model can operate with both positive and negative injection of active and reactive current.

⁴⁴ Resistance is neglected, and the reactance value (X_e) is also a default value for numerical stability. A value of X_e of around 0.25 pu seems reasonable for this model.

Chapter 2: Parameterization of the DER_A Model

A challenge with any DER model is developing a reasonable set of parameters to represent an aggregate response of many individual resources spread across a distribution system or feeder. Table 2.1 provides a list of parameter values to represent different vintages of Interconnection standards. These include IEEE Std. 1547-2003, IEEE Std. 1547a-2014, IEEE Std. 1547-2018 Category II⁴⁵ defaults, and CA Rule 21 defaults. Refer to the DER_A specification document⁴⁶ or the simulation software model libraries for a description of the model parameters. It is to be noted that these parameter values are to be considered as initial default values and modifications to the values may be necessary based on the individual jurisdiction of application⁴⁷ of the model.

Table 2.1: Default DER_A Model Parameters

Param ⁴⁸	IEEE Std. 1547-2003 Default	IEEE Std. 1547a-2014 Default	CA Rule 21 Default	IEEE Std. 1547-2018 Category II Default	Notes
<i>trv</i>	0.02	0.02	0.02	0.02	† Note 1
<i>dbd1</i>	-99	-99	-99	-99	† Note 1
<i>dbd2</i>	99	99	99	99	† Note 1
<i>kqv</i>	0	0	0	0	† Note 1
<i>vref0</i>	0	0	0	0	† Note 2
<i>tp</i>	0.02	0.02	0.02	0.02	†
<i>tiq</i>	0.02	0.02	0.02	0.02	†
<i>ddn</i>	0	0	20	20	Note 3
<i>dup</i>	0	0	20	20	Note 3
<i>fdbd1</i>	-99	-99	-0.0006	-0.0006	Note 3
<i>fdbd2</i>	99	99	0.0006	0.0006	Note 3
<i>femax</i>	0	0	99	99	Note 3
<i>femin</i>	0	0	-99	-99	Note 3
<i>pmax</i>	1	1	1	1	† Note 4
<i>pmin</i>	0	0	0	0	Note 4
<i>dpmax</i>	99	99	99	99	†
<i>dpmin</i>	-99	-99	-99	-99	†
<i>tpord</i>	0.02	0.02	5	5	Note 3
<i>lmax</i>	1.2	1.2	1.2	1.2	† Note 4
<i>vl0</i>	0.44	0.44	0.49	0.44	Note 5
<i>vl1</i>	0.44+V _{DROP}	0.44+V _{DROP}	0.49+V _{DROP}	0.44+V _{DROP}	Note 5
<i>vh0</i>	1.2	1.2	1.2	1.2	Note 5
<i>vh1</i>	1.2-V _{DROP}	1.2-V _{DROP}	1.2-V _{DROP}	1.2-V _{DROP}	Note 5
<i>tvl0</i>	0.16	0.16	1.5	0.16	Note 5

⁴⁵ In IEEE Std. 1547-2018, the abnormal operating performance Category II “covers all BPS stability/reliability needs and is coordinated with existing reliability standards to avoid tripping for a wider range of disturbances of concern to BPS stability.”

⁴⁶ P. Pourbeik, “Proposal for DER_A Model,” June 19, 2019. [Online]: https://www.wecc.org/Reliability/DER_A_Final_061919.pdf.

⁴⁷ Further, some engineering analysis requires scenario development of a “best” and “worst” case scenarios. This will require engineering judgement to alter the provided parameters to reflect such scenarios.

⁴⁸ Refer to the DER_A model specification for parameter names: https://www.wecc.biz/Reliability/DER_A_Final.pdf.

Formatted: Font: 9 pt

Table 2.1: Default DER_A Model Parameters

Param ⁴⁸	IEEE Std. 1547-2003 Default	IEEE Std. 1547a-2014 Default	CA Rule 21 Default	IEEE Std. 1547-2018 Category II Default	Notes
<i>tv1</i>	0.16	0.16	1.5	0.16	Note 5
<i>tvh0</i>	0.16	0.16	0.16	0.16	Note 5
<i>tvh1</i>	0.16	0.16	0.16	0.16	Note 5
<i>Vfrac</i>	0	0	1	1	Note 5
<i>fltrp</i>	59.3	59.5 OR 57.0	58.5 OR 56.5	58.5 OR 56.5	Note 6
<i>fthrp</i>	60.5	60.5 OR 62.0	61.2 OR 62.0	61.2 OR 62.0	Note 6
<i>tfl</i>	0.16	2.0 OR 0.16	300.0 OR 0.16	300.0 OR 0.16	Note 6
<i>tfh</i>	0.16	2.0 OR 0.16	300.0 OR 0.16	300.0 OR 0.16	Note 6
<i>tg</i>	0.02	0.02	0.02	0.02	†
<i>rrpwr</i>	0.1	0.1	2.0	2.0	Note 8
<i>tv</i>	0.02	0.02	0.02	0.02	†
<i>Kpg</i>	0	0	0.1	0.1	Note 3
<i>Kig</i>	0	0	10	10	Note 3
<i>xe</i>	0.25	0.25	0.25	0.25	† Note 8
<i>vpr</i>	0.8	0.8	0.3	0.3	Note 6
<i>iqh1</i>	0	0	1	1	Note 1
<i>iq1</i>	0	0	-1	-1	Note 1
<i>pflag</i>	1	1	1	1	† Note 7
<i>fraflag</i>	0	0	1	1	Note 7
<i>paflag</i>	P priority	P priority	Q priority	Q priority	Note 7
<i>typeflag</i>	1	1	0 OR 1	0 OR 1	Note 7

677

678 Parameterization Notes

679 The following notes describe considerations and background on the parameter values selected in [Table 2.1](#). Refer to
680 each respective interconnection standard for more information.

681

682 NOTE †: Default Parameters Not Typically Subject to Change

683 These parameters do not typically change across different implementations of the DER_A model. Any modification
684 from the recommended default values should be carefully analyzed and justified.

685

686 NOTE 1: Voltage Control Parameters

687 In most existing applications, DERs do not control voltage. In such cases, the voltage control function should be
688 disabled by setting the voltage control gain, *Kqv*, to 0. The lower and upper voltage deadbands, *dbd1* and *dbd2*, should
689 be set large values (e.g., -99 and 99), respectively. However, interconnection standards state that the voltage control
690 “capability” must be provided in the DER. If the capability is being utilized or required by the local utility, this setting
691 should be modified accordingly.

692 When DERs are controlling voltage, the dynamic model needs to be adapted to account for this. As the model is not
693 able to simultaneously represent both steady-state voltage control (Clause 5.3.3. voltage-reactive power mode in
694 IEEE Std. 1547-2018) and dynamic voltage control (Clause 6.4.2. dynamic voltage support in IEEE Std. 1547-2018), a
695 modeling compromise must be made. Therefore, it is recommended that the dynamic voltage support settings be

implemented since most simulations involve fault-type conditions with large voltage fluctuations. Reasonable default values are $trv = 0.02$, $kqv = 5$,⁴⁹ $dbd1 = -0.12$, $dbd2 = 0.1$, $iqh1 = 1$, and $iq1 = -1$.⁵⁰ Any situation where Kqv is non-zero (dynamic voltage control is enabled), care should be taken to ensure that the corresponding deadband is not too small, which would lead to voltages possibly jumping across deadband thresholds each simulation iteration.

NOTE 2: Voltage Reference

The recommended setting for $Vref0$ is 0. Setting $Vref0$ equal to 0 allows the model to set its own terminal voltage reference based on the initial conditions. This is consistent with the language in IEEE Std. 1547-2018 and in 5.3.3 (voltage-reactive power mode), which require that DERs shall be capable of autonomously adjusting reference voltage ($Vref$) with $Vref$ being equal to the (low pass filtered) measured voltage.

NOTE 3: Active Power-Frequency Control

In IEEE Std. 1547-2003 and IEEE Std. 1547a-2014, active power-frequency control is not specified. Therefore, the gains Ddn and Dup as well as the frequency errors $femax$ and $femin$ are set to 0. This disables the active power-frequency controls in the model for these two standards. In CA Rule 21 and IEEE Std. 1547-2018, the capability for resources to have active power-frequency controls installed and enabled (as default) are specified. Therefore, per the standard Dup and Ddn should be set to 20 (representing a 5% droop characteristic).⁵¹ Default deadband for both standards is set to ± 0.0006 pu, or ± 36 mHz. $Tpord$ is used to represent the specified open loop time constant of five seconds per IEEE Std. 1547-2018 and CA Rule 21, and it is set to a small value (0.02 sec) when these controls are disabled in previous IEEE Std. 1547 versions.⁵² Parameters Kpg and Kpi are not directly mapped to the interconnection standards; values describe in Table 2.1 were used in benchmark testing of the DER_A model are based on engineering judgment and were found to provide satisfactory response. Note that if the DERs are assumed to be operating at maximum available power, the Dup should be set to 0. This is explained further in Chapter 3

NOTE 4: Active Power Capability

Maximum active power output is set to a default of 1 pu. Minimum active power output is assumed to be 0 pu for generating resources but can be negative (i.e., -1 pu) for energy storage resources. These maximum and minimum active power capability values can be modified if more detailed information is known about specific DERs. Inverter-based DERs have an overload capability of around 110–120%, and therefore $Imax$ is set to 1.2 pu. Other types of DERs may have a different current limit, and this can be adjusted carefully if additional information is known. However, for most inverter-based installations (e.g., solar PV), a value of 1.2 pu is a reasonable approximation.

NOTE 5: Partial Tripping

$Vrfrac$, the ratio of DERs that restore output upon voltage recovery, should be set to 0 for legacy⁵³ DERs (i.e., no DER restore output following a ride-through event), 1.0 for modern DERs (i.e., all DERs restore output following a ride-through event), and some value in between for a mix of a legacy and modern DERs based on the assumed vintage of the DER deployed. A value of $Vrfrac = 0$ is a conservative assumption and should be used if no detailed DER information is available. Since CA Rule 21 and IEEE Std. 1547-2018 are relatively new standards, it can be expected that, for now, $Vrfrac$ can be set at or near 0. When using the der a dynamic model to represent a single plant⁵⁴, the partial tripping parameter should be set to 0 to represent the entire plant tripping.

⁴⁹ Allows for maximum reactive current injection when voltage falls below around 0.7 pu, taking into consideration the voltage deadband.

⁵⁰ Again, note that the values in Table 2.1 do not use these settings because the respective interconnection agreements do not require dynamic voltage control to be used. Hence, kqv is set to 0.

⁵¹ See Chapter 3 on recommended settings. Since most DER will be operated at maximum available power, and will not have available generating capability to respond in the upward direction for underfrequency events, Dup should be set to 0, from a practical standpoint.

⁵² Setting $tpord$ should be studied on an individual system basis.

⁵³ Use of the term "legacy" generally refers to DER compliant with IEEE Std. 1547-2003 and IEEE Std. 1547a-2014, which typically involve limited or no controls and ride-through capability.

⁵⁴ This is more common for a single, large distribution-connected generation plant. A non-zero parameter here would indicate a portion of the plant trips, which is not the desired effect.

Formatted: Font: 9 pt

Formatted: Font: 9 pt

733 The interconnection standards include different levels of trip settings: typically a longer duration trip time with
 734 magnitude closer to nominal and a shorter duration trip time with lower (or higher) magnitude away from nominal.
 735 **Table 2.1** includes values for the shorter duration trip thresholds since these values are likely the most useful and
 736 relevant settings for stability studies. Consult the relevant interconnection standards and requirements for more
 737 information on longer duration trip settings. Higher magnitude with longer duration trip settings may need to be
 738 studied in simulations involving delayed voltage recovery.

739 V_{DROP} should be set to a reasonable equivalent voltage drop across the distribution system in the range of 2–8%
 740 (reasonable default of 5%) if no detailed information is available. Voltage trip thresholds include a 0.01 pu offset from
 741 the interconnection standard values to correctly account for the beginning and completion of partial tripping.

742 The values specified in the **Table 2.1** represent R-DERs as part of the CLM. If individual or multiple similar U-DERs are
 743 represented, trip settings should be equal and set to the corresponding value in the interconnection standard. If
 744 aggregate R-DERs are to be represented by a generator record, use the methodology described in **Chapter 1** to
 745 determine correct trip settings.

746 In cases where momentary cessation of inverter-based resources needs to be represented, use $v/1$ and $v/0$ with
 747 extended trip times. Note that this may hinder the ability to capture any tripping effects due to existing model
 748 limitations. Engineering judgment and sensitivity studies should be used when applying these types of settings.
 749

750 **NOTE 6: Frequency Trip Levels**

751 High (f_{htrp}) and low (f_{ltrp}) frequency tripping has different thresholds in a few of the interconnection standards, as
 752 described in **Table 2.1**. Again, each has a specified time threshold. The frequency thresholds closer to nominal
 753 frequency have a longer duration while the thresholds further from nominal have a shorter duration.

754 In simulations where frequency does not fall below under-frequency load shedding (UFLS) levels, the setting values
 755 for CA Rule 21 and IEEE Std. 1547-2018 are not significant.⁵⁵ However, the settings representing IEEE Std. 1547-2003
 756 and IEEE Std. 1547a-2014 are relevant, particularly for the thresholds closer to nominal frequency. IEEE Std. 1547-
 757 2003 has only one magnitude and time value. IEEE Std. 1547a-2014 has two thresholds, but most commonly only the
 758 59.5 Hz and 60.5 Hz thresholds, with two second timers, are applicable.

759 Disabling tripping on frequency during low voltage is implemented in almost all relay models as the relay needs a
 760 sufficient voltage waveform to measure frequency. Under fault conditions, due to the large change in voltage, the
 761 frequency calculation can result in a spurious spike, and thus, frequency tripping should be disabled. IEEE Standard
 762 C37.117⁵⁶ recommends disabling the frequency trip when the voltage is below 50–70% of nominal. For DERs, this
 763 voltage levels was increased to 80% to account for further inaccuracies in frequency calculation that may arise in
 764 positive sequence simulations.⁵⁷ The first sentence of IEEE Std. 1547-2018, Clause 6.5.1, states that when frequency
 765 meets a certain criteria and “the fundamental-frequency component of voltage on any phase is greater than 30% of
 766 nominal” then the DER can respond. However, if the frequency is outside acceptable range but voltage is less than
 767 the 30% threshold then the DER should not trip. This represents a low voltage inhibit function in the frequency
 768 tripping, and it is represented by parameter V_{pr} .⁵⁸ Regardless, study engineers should monitor for false trips by the
 769 DER_A model that may not be realistic; rather, they are an artifact of positive sequence stability simulation calculation
 770 of frequency. Close review of any frequency-related tripping is strongly recommended.

771 **NOTE 7: Control Flags**

⁵⁵ Unless specific studies are being performed to configure UFLS systems.

⁵⁶ IEEE C37.117-2007, IEEE Guide for the Application of Protective Relays Used for Abnormal Frequency Load Shedding and Restoration.

⁵⁷ https://www.wecc.biz/Reliability/WECC_White_Paper_Frequency_062618_Clean_Final.pdf.

⁵⁸ V_{pr} may also be referred to as V_{fth} .

772 The parameter *pflag* sets power factor control. If set to 1, then the power factor angle reference is used based on
773 initialization of the model. Otherwise, if set to 0, then the reactive power reference (*Qref*) will be used.

774 The parameter *frqflag* sets the active power-frequency control capability. If set to 0, then active power reference (*Pref*)
775 is used. Otherwise, if set to 1, then the active power-frequency control loop is enabled. If *frqflag* is set to 1, the resource
776 will respond to over- and under-frequency disturbances. However, if the user sets *Dup* to 0, the resource will not
777 respond to underfrequency. This configuration emulates the unit(s) operating at maximum available power output.

778 The parameter *pqflag* specifies whether to use active or reactive current priority, which is effective when the current
779 limit logic is in effect. This is particularly used during response to large disturbances (i.e., faults).

780 The parameter *typeflag* specifies whether the resource is a generating resource (set to 1) or an energy storage device
781 (set to 0). Setting as an energy storage device allows absorption of active power, and it emulates distributed energy
782 storage. This does not, however, emulate charging and discharging of the resource.

783 **NOTE 8: Voltage Source Interface Representation**

784 The *rrpwr* specifies the active current ramp rate. IEEE Stds. 1547-2003 and 1547a-2014 do not specify an active
785 current ramp rate; however, IEEE Std. 1547-2018 and CA Rule 21 use an 80% recovery within 0.4 seconds that can be
786 approximated with a gain of 2 pu/sec, which equates to full recovery within 0.5 seconds. The voltage source
787 impedance also uses a default values for *Xe* of 0.25, based on robustness testing of the DER_A model during its
788 development.
789

Future Model Implementation Improvement

Commercial simulation software vendors should consider adding a new global flag for inverter-based resources (particularly renewable energy resources) that sets the maximum available power to the current power output (*Pgen*) upon initialization of the inverter-based models. This can then be changed by the user on a case-by-case basis during the simulation if necessary (e.g., to represent curtailment). For example, simulations with renewable generation dispatched at less than maximum capacity (*Pmax*) may represent less solar irradiance or lower wind speed. However, this is the maximum available power output for the assumed conditions. As more resources are being installed with the capability to provide active power-frequency control, the ability to distinguish whether units are operating at maximum available power output will be increasingly important. This parameter is similar to the baseload flag for synchronous generating resources.

790
791
792

Chapter 3: Practical DER_A Model Implementation

Table 2.1 in the previous chapter provides parameter values that relate to specific interconnection standards and requirements; however, many systems are faced with aggregate DERs that encompass many vintages of interconnection requirements and settings. Table 3.1 provides a set of default parameter values for different systems based on the penetration of different IEEE Std. 1547 vintages, ranging from a system dominated by IEEE Std. 1547-2003 interconnections to a system of modern IEEE Std. 1547-2018 interconnections.⁵⁹ Also shown are default values for penetrations at 70% for 2003 vintage and 30% for 2018 vintage, as well as 30% for 2003 vintage and 70% for 2018 vintage. These default values are based on engineering judgment and intended to be used as a starting point for more detailed studies and sensitivities.⁶⁰ Note that, in addition to the IEEE Std. 1547 default settings, individual utilities or jurisdictions may have additional or more stringent requirements that should be considered when developing a set of DER modeling parameters. TPs and PCs should consider any modifications to the default IEEE Std. 1547 parameters as well as local requirements and should adapt the models accordingly.

Parameter values that are subject to changes across interconnection vintages are highlighted in red in Table 3.1 and described in this chapter. Note that some of the parameter values subject to change are a linear interpolation based on the penetration of specific vintages of DERs. Sensitivity studies should be performed by the TP and PC to understand the impacts of these parameter values to system study results.

Table 3.1: Default Parameter Selection for Mixed Vintages of DER

Param	Early Vintage DER System IEEE Std. 1547-2003	70% of -2003 30% of -2018	30% of -2003 70% of -2018	Newer Vintage DER System IEEE Std. 1547-2018 (Category II)
<i>trv</i>	0.02	0.02	0.02	0.02
<i>dbd1</i>	-99	-99	-99	-99
<i>dbd2</i>	99	99	99	99
<i>kqv</i>	0	0	0	0
<i>vref0</i>	0	0	0	0
<i>tp</i>	0.02	0.02	0.02	0.02
<i>tiq</i>	0.02	0.02	0.02	0.02
<i>ddn</i>	0	6	14	20
<i>dup</i>	0	0	0	0
<i>fbd1</i>	-99	-0.0006	-0.0006	-0.0006
<i>fbd2</i>	99	0.0006	0.0006	0.0006
<i>femax</i>	0	0	99	99
<i>femin</i>	0	0	-99	-99
<i>pmax</i>	1	1	1	1
<i>pmin</i>	0	0	0	0
<i>dpmx</i>	99	99	99	99

⁵⁹ Note that application and enforcement of IEEE Std. 1547-2018 for newly interconnecting inverters is likely to take time to implement in many jurisdictions, often requiring regulatory updates to enable enhanced capabilities. Some degree of verification and alignment with these implementation timelines should be performed by each TP and PC when representing DER in BPS reliability studies.

⁶⁰ Transmission–distribution co-simulation techniques may be used to help further parameterize DER_A models based on specific distribution feeder configurations and DER penetration levels.

Table 3.1: Default Parameter Selection for Mixed Vintages of DER

Param	Early Vintage DER System IEEE Std. 1547-2003	70% of -2003 30% of -2018	30% of -2003 70% of -2018	Newer Vintage DER System IEEE Std. 1547-2018 (Category II)
<i>d_{pmin}</i>	-99	-99	-99	-99
<i>tpord</i> ⁶¹	0.02	0.02	5	5
<i>l_{max}</i>	1.2	1.2	1.2	1.2
<i>v_{l0}</i>	0.44	0.44	0.44	0.44
<i>v_{l1}</i>	0.49	0.49	0.49	0.49
<i>v_{h0}</i>	1.2	1.2	1.2	1.2
<i>v_{h1}</i>	1.15	1.15	1.15	1.15
<i>tv_{l0}</i>	0.16	0.16	0.16	0.16
<i>tv_{l1}</i>	0.16	0.16	0.16	0.16
<i>tv_{h0}</i>	0.16	0.16	0.16	0.16
<i>tv_{h1}</i>	0.16	0.16	0.16	0.16
<i>V_{rfrac}</i>	0	0.3	0.7	1.0
<i>f_{l_{trp}}</i>	59.3	58.5	57.5	56.5
<i>f_{h_{trp}}</i>	60.5	61	61.5	62.0
<i>t_{fl}</i>	0.16	0.16	0.16	0.16
<i>t_{fh}</i>	0.16	0.16	0.16	0.16
<i>t_g</i>	0.02	0.02	0.02	0.02
<i>rrpwr</i>	0.1	0.6	1.4	2.0
<i>t_v</i>	0.02	0.02	0.02	0.02
<i>K_{pg}</i>	0	0.1	0.1	0.1
<i>K_{ig}</i>	0	10.0	10.0	10.0
<i>x_e</i>	0.25	0.25	0.25	0.25
<i>v_{fth}</i>	0.8	0.3	0.3	0.3
<i>i_{qh1}</i>	0	1.0	1.0	1.0
<i>i_{ql1}</i>	0	-1.0	-1.0	-1.0
<i>p_fflag</i>	1	1	1	1
<i>f_rflag</i>	0	1	1	1
<i>p_qflag</i>	P priority	P priority	Q priority	Q priority
<i>t_yeflag</i>	1	1	1	1

812

813

814

815

The following considerations are made in the development of these default parameter values and intended to provide transparency and understanding of how these parameters were devised. However, they are intended as default values that may be subject to change if more detailed information is known.

⁶¹ The active power-frequency response from DERs, if utilized in studies, should be tuned to achieve and ensure a closed-loop stable control. This parameter may need to be adapted based on this tuning.

- 816
- 817
- 818
- 819
- 820
- 821
- 822
- 823
- 824
- 825
- 826
- **Upward Frequency Responsiveness for Underfrequency Conditions (*Dup*, *Pmax*):** In this set of default parameters, it is assumed that the vast majority (if not all) DERs are operated at maximum available⁶² power and thus cannot provide frequency response for underfrequency conditions.⁶³ To model the inability to provide response in the upward direction, the *Dup* parameter value is set to 0. This disables upward movement regardless of where the DER resource(s) is dispatched relative to *Pmax* in the dynamics data. This allows for easy manipulation of DER output levels without needing to modify additional parameter values for each sensitivity case. Another option is to set the *Dup* parameter value according to the expected performance and then modifying *Pmax* value in the dynamics data to match the predisturbance output for each operating conditions studied. However, this requires an additional step and may lead to unexpected frequency responsiveness from DER if not adequately handled when changing DER dispatch levels.
 - **Downward Frequency Responsiveness for Overfrequency Conditions (*Ddn*):** *Ddn* is modified across the different penetration levels to represent an effective droop characteristic, or a response from a fractional DER value based on the penetration of modern inverters. The 5% droop (*Ddn* = 20) is multiplied by a linear factor based on this penetration (e.g., 70% of 20 equals 14).
 - **Frequency Deadband and Error Limits (*fdb1*, *fdb2*):** When frequency response is enabled in the model, the deadband settings of *fdb1* and *fdb2* as well as the frequency error settings of *femax* and *femin* need to be modified to enable accurate representation of these controls. A default value is used in all cases where control is enabled.
 - **Voltage-Related Trip Settings and Times:** Refer to the [Chapter 1](#) for the derivation of the partial trip values. Note that trip thresholds and times may vary if applying CA Rule 21. Values assume a voltage drop, V_{DROP} , of 5%.
 - **Fraction of Resources Recovering (*Vfrac*):** The parameter *Vfrac* represents the fraction of resources that recover upon voltage recovery following abnormal voltage conditions. It is expected that resources meeting IEEE Std. 1547-2018 will recover from abnormal voltages and ride through ^{disturbances} while IEEE Std. 1547-2003 resources will likely trip and remain disconnected for the duration of stability simulations. A linear multiplier is used based on the fraction of resources connected to the system. For example, for a 70% IEEE Std. 1547-2018 system, *Vfrac* equals 0.7.
 - **Frequency-Related Trip Settings (*ftrip*, *fhtrip*):** Frequency-related trip settings of *ftrip* and *fhtrip* are assumed to slightly vary based on the aggregate vintage of connected DERs. For the shorter-term tripping, IEEE Std. 1547-2003 has trip settings at 59.3 Hz and 60.5 Hz while IEEE Std. 1547-2018 has trip settings at 57.5 Hz and 62 Hz. For mixed penetrations, a linear multiplier is used to vary the level of DER tripping. This is an approximate; yet, these trip settings are below the first stage of UFLS, and they are therefore not likely to make a substantive impact in most stability simulations.⁶⁴ More detailed studies should consider identifying more accurate information for these settings.
 - **Active Current Recovery Ramp Rate (*rrpwr*):** The parameter *rrpwr* is modified across different penetration levels to represent the fraction of resources that recover from abnormal voltage conditions. A 2.0 pu/sec (recovery in 0.5 seconds) is used for IEEE Std. 1547-2018 resources, and a linear multiplier is used for the mixed penetration conditions. For example, 70% of 2.0 pu/sec equals 1.4 pu/sec.
 - **Frequency Response PI Controls (*Kpg*, *Kig*):** When frequency response controls are enabled in the model, default parameter values of *Kpg* = 0.1 and *Kig* = 10 are used.

⁶² If studies are assuming that DERs are curtailed for any reason, IEEE Std. 1547-2018 vintage DERs will have the capability to respond to underfrequency events.

⁶³ This statement relates to DERs that are generating resources; this may not be the case for energy storage. Energy storage, not injecting maximum power, will be able to respond to underfrequency events following a droop characteristic.

⁶⁴ Stability studies for establishing UFLS set points, where simulated frequency can fall well below UFLS, should ensure reasonable frequency-related trip settings are used for DER.

857
858
859
860

- **Type Flag (*typeflag*):** In these default data sets, the *typeflag* is set to 1 representing a generating resource. This flag, and relevant parameter values, can also be modified to represent an energy storage resource.

Chapter 4: DER_A Model Benchmarking and Testing

To ensure that a model is usable for industry-wide studies, some form of model benchmarking and testing is typically performed by industry partners. DER_A model development and testing was led by the WECC Renewable Energy Modeling Task Force (REMTF) and NERC LMTF with EPRI providing the model benchmarking support.

EPRI performed extensive DER_A model benchmarking while working with the major commercial software vendors⁶⁵ following their implementation of the standalone DER_A model. A test system with a play-in voltage source model at the transmission bus with constant impedance load adjacent to the DERs was used for the testing. A suite of 19 tests was used to apply small and large disturbances of voltage and frequency, and then the model's active and reactive power response and set points were observed. The response of the DER_A model was compared for each test across all platforms to determine whether the models match the same general trend in response (i.e., they are considered suitably benchmarked). Refer to an EPRI white paper on this topic (reference 11 in Appendix A).⁶⁶ Figure 4.1 shows an example benchmarking simulation, and it demonstrates how the DER_A model in each of the software platforms matches the same general performance characteristic.

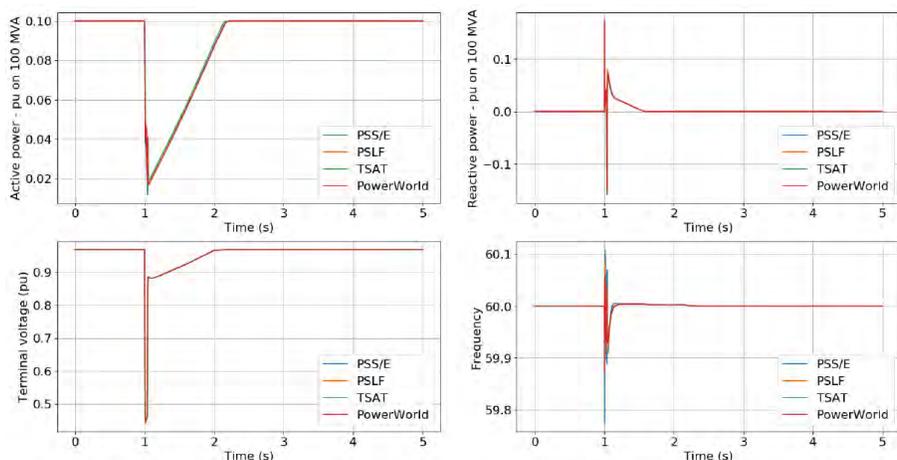


Figure 4.1: Voltage Sag Benchmarking Test Result [Source: EPRI]

To ensure that the model is numerically robust and usable in system studies on a large-scale case, CAISO has been testing the DER_A model on WECC-wide base cases for their reliability studies. Figure 4.2 shows one example of the types of sensitivity studies performed by CAISO. CAISO has been testing the model with different parameter values, including CA Rule 21 and the new IEEE Std. 1547-2018 default settings. The model has performed well and is numerically robust in these studies using GE PSLFTM.⁶⁷

⁶⁵ Including GE-PSLFTM, Siemens PTI PSS[®]E, PowerWorld Simulator, and Powertech Labs TSAT.

⁶⁶ The New Aggregated Distributed Energy Resources (der_a) Model for Transmission Planning Studies. 2019 Update. White Paper. 3002015320. Electric Power Research Institute (EPRI). Palo Alto, CA (<https://www.epri.com/#/pages/product/00000003002015320/?lang=en-US>).

⁶⁷ CAISO, "CMPLDWG Composite Model with Distributed Generation DER_A CAISO Assessment," NERC LMTF Meeting, May 2018: https://www.nerc.com/comm/PC/LoadModelingTaskForceDL/CMPLDWG_DER_A_CAISO_NERC.pdf.

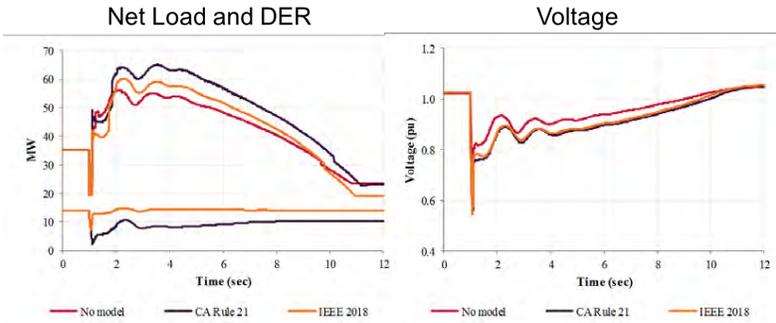


Figure 4.2: CAISO DER Study Example including DER_A Model [Source: CAISO]

EPRI has also performed system studies on the full Eastern Interconnection base case in coordination with Duke Energy. These studies implemented the DER_A model on 138 U-DER installations with a capacity of 1,300 MW. Figure 4.3 shows the DER response from an example simulation using these models. It shows that some of the DER_A models near the fault location respond to the disturbance with active and reactive power response, and those further away from the disturbance do not provide a significant response. Again, the implemented DER_A models are numerically robust.⁶⁸ EPRI further did analysis on the DER_A model when used as part of the composite load model to test modeled R-DER in the SPIDERWG recommended modeling framework⁶⁹. Again, the models were numerically robust.

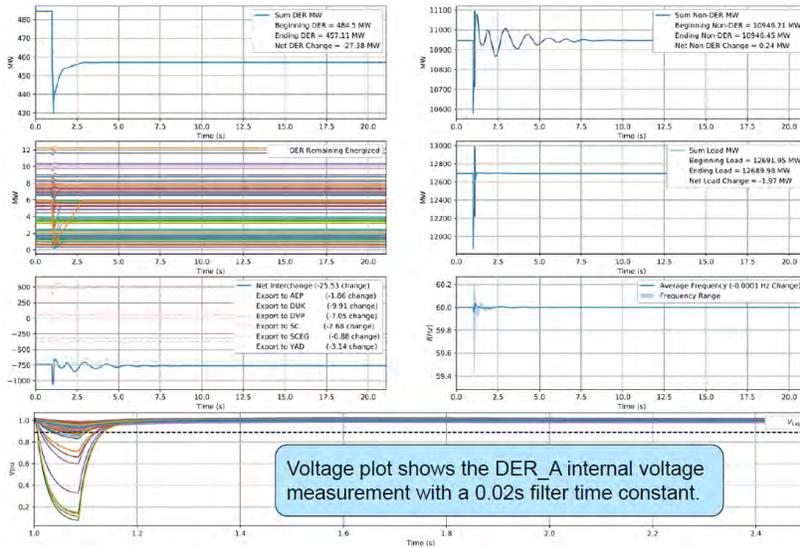


Figure 4.3: DER Study Example including DER_A Model [Source: EPRI]

⁶⁸ EPRI, "Preliminary results of DER_A model parameterization", NERC LMTF Meeting, July 2018: https://www.nerc.com/comm/PC/LoadModelingTaskForceDL/Parameterization_of_DER_A_Model_v1_DR.pdf.
⁶⁹ EPRI, "Results on CMPLDWg – DER_A Benchmark", NERC LMTF Meeting, July 2019: https://www.nerc.com/comm/PC/LoadModelingTaskForceDL/CMPLDWg-DER_A-benchmark_v1_DR.pdf

899 **Appendix A: Contributors**

900 NERC gratefully acknowledges the contributions and assistance of the following industry experts in the preparation
 901 of this guideline. NERC would like to acknowledge EPRI for the technical leadership in developing this guideline.
 902
 903

Name	Entity
Irina Green	Guidehouse
Mohab Elnashar	Independent Electricity System Operator
Deepak Ramasubramanian (Subgroup Colead)	EPRI
Adam Weber (Subgroup Colead)	Ameren
Jens Boemer	EPRI
Nicolas Compas	Hydro Quebec
Laura Fedoruk	Sunrun
Anish Gaikwad	EPRI
Ning Kang	Argonne National Laboratory
Dmitry Kosterev	BPA
Dean Latulipe	National Grid
Pouyan Pourbeik	PEACE®
Bill Price	General Electric
Bill Quaintance	Duke Progress
Shruti Rao	GE PSLFederal Electric
Fabio Rodriguez	Duke Florida
Juan Sanchez-Gasca	General Electric
Jay Senthil	Siemens PTI
Shayan Rizvi (SPIDERWG Chair)	NPCC
John Schmall (SPIDERWG Vice-Chair)	ERCOT
Ryan Quint (SPIDERWG Coordinator)John Skeath	NERCNorth American Electric Reliability Corporation
John Skeath (SPIDERWG Coordinator)	NERC
Mohamed Osman	NERC
Jameson Thornton	Pacific Gas and Electric
Song Wang	PacificCorp
Shannon Mickens	SPP
Scott Jordan	SPP
Brad Marszalkowski	ISO-NE
Nick Hatton	WECC

904
 905

Appendix B: References

DER_A Model Specification Document

- [1] P. Pourbeik, "Proposal for DER_A Model," September 11, 2018. [Online]: https://www.wecc.org/Reliability/DER_A_Final_061919.pdf.

Relevant Interconnection Standards

- [2] IEEE Std. 1547-2003, Standard for Interconnecting Distributed Resources with Electric Power Systems, July 2003. [Online]: <https://standards.ieee.org/standard/1547-2003.html>.
- [3] IEEE Std. 1547a-2014, IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems – Amendment 1, May 2014: <https://standards.ieee.org/standard/1547a-2014.html>,
- [4] IEEE Std. 1547-2018, IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, April 2018. [Online]: <https://standards.ieee.org/findstds/standard/1547-2018.html>.
- [5] IEEE Std. 1547-2018, 6/4/2018: Errata to IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces. [Online]: http://standards.ieee.org/findstds/errata/1547-2018_errata.pdf.
- [6] CPUC: Interconnection (Rule 21). California Public Utilities Commission. [Online]: <http://www.cpuc.ca.gov/Rule21/>.

Relevant NERC ~~Standards, Guidelines, Guidelines~~ and Reports

- [7] NERC, "Distributed Energy Resources: Connection Modeling and Reliability Considerations," Atlanta, GA, Feb 2017. [Online]: https://www.nerc.com/comm/Other/essntlrbltysrvctskfrcl/Distributed_Energy_Resources_Report.pdf.
- [8] NERC, "Reliability Guideline: Modeling Distributed Energy Resources in Dynamic Load Models," Atlanta, GA, Dec 2016. [Online]: https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_-_Modeling_DER_in_Dynamic_Load_Models_-_FINAL.pdf.
- [9] NERC, "Reliability Guideline: Distributed Energy Resource Modeling," Atlanta, GA, Sept 2017. [Online]: https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_-_DER_Modeling_Parameters_-_2017-08-18_-_FINAL.pdf.

DER_A Parameterization References

- [10] The New Aggregated Distributed Energy Resources (der_a) Model for Transmission Planning Studies. 2019 Update. White Paper. 3002015320. Electric Power Research Institute (EPRI). Palo Alto, CA. [Online]: <https://www.epri.com/#/pages/product/000000003002015320/?lang=en-US>.
- [11] Electric Power Research Institute (EPRI) (2016): Distributed Energy Resources Modeling for Transmission Planning Studies. Summary Modeling Guidelines. 3002009485. Palo Alto, CA. [Online]: <http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002009485>.
- [12] EPRI (2017): Distributed Energy Resources Modeling for Transmission Planning Studies. Detailed Modeling Guidelines. 3002010932. Electric Power Research Institute (EPRI). Palo Alto, CA. [Online]: <https://www.epri.com/#/pages/product/000000003002010932/>.
- [13] I. Alvarez-Fernandez, D. Ramasubramanian, A. Gaikwad, J. Boemer, "Parameterization of Aggregated Distributed Energy Resources (DER_A) Model for Transmission Planning Studies," 2018 Grid of the Future Symposium, CIGRE US National Committee, Reston, VA, 2018.
- [14] EPRI (2018) Selected Case Studies Analyzing the Impact of DER on the Bulk System Voltage Performance: Impact of Aggregate Distributed Energy Resources on a Large System, EPRI, Palo Alto, CA: 2018, 3002013502.
- [15] EPRI (2018) Detailed Distribution Circuit Analysis and Parameterization of the Partial Voltage Trip Logic in WECC's DER Model (DER_A): Towards regional default settings in the absence of detailed distribution circuit data, EPRI, Palo Alto, CA: 2018, 3002013500.

955
956
957
958
959
960
961
962
963

Other Reference Material

- [16] D. Ramasubramanian, Z. Yu, R. Ayyanar, V. Vittal and J. M. Undrill, "Converter Model for Representing Converter Interfaced Generation in Large Scale Grid Simulations", IEEE Trans. PWRs, April 2016.
- [17] WECC, "Wind Plant Dynamic Modeling Guidelines," Salt Lake City, UT, April 2014. [Online]: <https://www.wecc.biz/Reliability/WECC%20Wind%20Plant%20Dynamic%20Modeling%20Guidelines.pdf>.
- [18] WECC, "Solar Plant Dynamic Modeling Guidelines," Salt Lake City, UT, April 2014. [Online]: <https://www.wecc.biz/Reliability/WECC%20Solar%20Plant%20Dynamic%20Modeling%20Guidelines.pdf>.

964 **Appendix C: DER_A Block Diagram**

965
966 This appendix serves to house the entirety of the block diagram of the DER_A dynamic model.
967

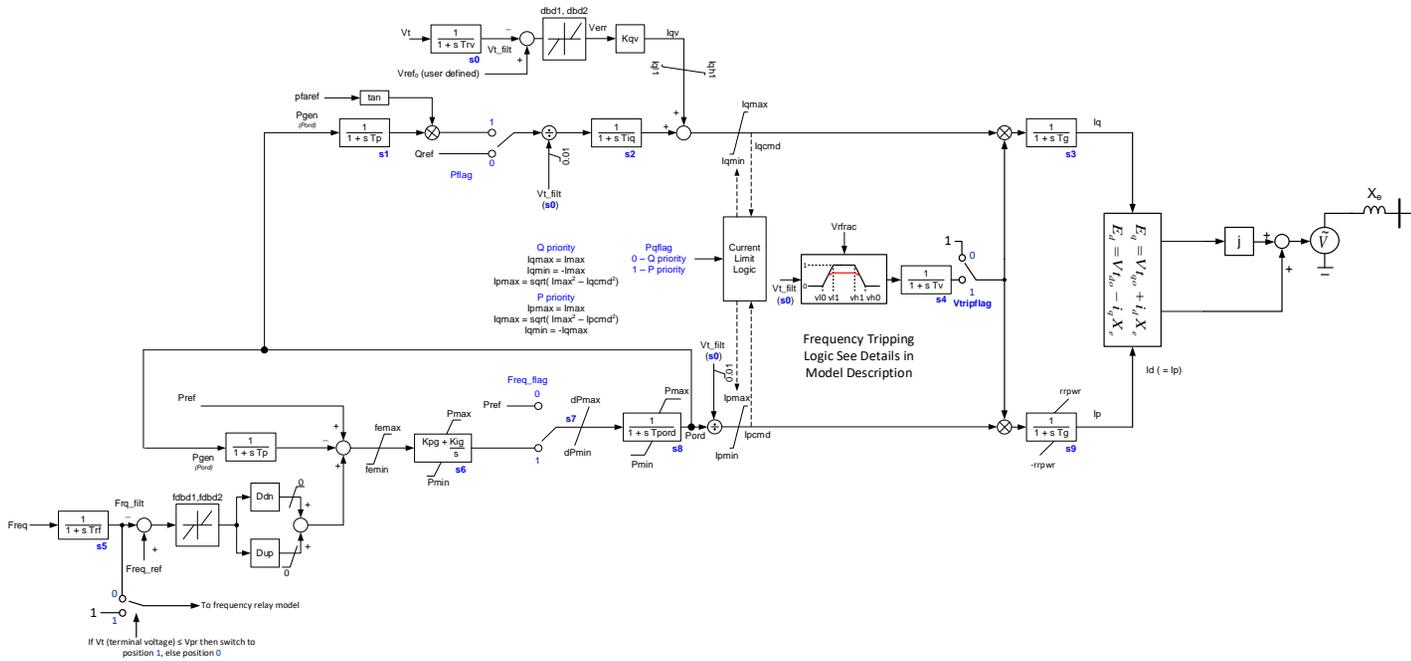


Figure C.1: DER_A Model Block Diagram

968
969
970
971

972 **Guideline Information and Revision History**

973

Guideline Information	
Category/Topic: [NERC use only]	Reliability Guideline/Security Guideline/Hybrid: Reliability Guideline
Identification Number: [NERC use only]	Subgroup: [NERC use only]

974

Revision History		
Version	Comments	Approval Date

975

976

SPIDERWG Standards Authorization Requests - FAC-001 and FAC-002

Action

Request for RSTC Comments

Summary

In order to “avoid adverse impacts on the reliability of the Bulk Electric System,” Distribution Providers (DPs) “must document and make [f]acility interconnection requirements available”. Documentation and availability of DP generation interconnection requirements allows for necessary coordination across the transmission – distribution interface (T-D Interface) to maintain Bulk Electric System (BES) reliability. The purpose of FAC-002-4 is “to study the impact of interconnecting new or changed Facilities on the BES”. Recent studies and presentations to SPIDERWG indicate that if aggregate DER is integrated without adequate interconnection studies, reliable operation of the BES is likely to be impacted (e.g., contingencies worsened by aggregate DER tripping off-line). These SARs were developed per the approved NERC Reliability Standards Review and developed per a milestone plan presented to the RSTC EC. The SPIDERWG is seeking a request for RSTC comments.

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	FAC-001-4 Applicability of the DP for Facility Ratings		
Date Submitted:	_/_/2022		
SAR Requester			
Name:	Shayan Rizvi, NPCC (NERC SPIDERWG Chair) John Schmall, ERCOT (NERC SPIDERWG Vice-Chair)		
Organization:	The NREC System Planning Impacts of DER Working Group (SPIDERWG)		
Telephone:	Shayan – 212-840-1070 John – 512-248-4243	Email:	Shayan – srizvi@nppc.org John – john.schmall@ercot.com
SAR Type (Check as many as apply)			
<input type="checkbox"/> New Standard	<input type="checkbox"/> Imminent Action/ Confidential Issue (SPM Section 10)		
<input checked="" type="checkbox"/> Revision to Existing Standard	<input type="checkbox"/> Variance development or revision		
<input type="checkbox"/> Add, Modify or Retire a Glossary Term	<input type="checkbox"/> Other (Please specify)		
<input type="checkbox"/> Withdraw/retire an Existing Standard			
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
<input type="checkbox"/> Regulatory Initiation	<input checked="" type="checkbox"/> NERC Standing Committee Identified		
<input type="checkbox"/> Emerging Risk (Reliability Issues Steering Committee) Identified	<input type="checkbox"/> Enhanced Periodic Review Initiated		
<input type="checkbox"/> Reliability Standard Development Plan	<input checked="" type="checkbox"/> Industry Stakeholder Identified		
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
<p>In order to “avoid adverse impacts on the reliability of the Bulk Electric System,” Distribution Providers (DPs) “must document and make [f]acility interconnection requirements available”¹. Documentation and availability of DP generation interconnection requirements allows for necessary coordination across the transmission – distribution interface (T-D Interface) to maintain BES reliability.</p>			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			

¹ Text taken from Purpose of FAC-001-4: <https://www.nerc.com/pa/Stand/Reliability%20Standards/FAC-001-4.pdf>

Requested information

The purpose of this SAR is to revise FAC-001-4 to include DP in the “Applicability” section and update the requirements to require DPs to make available their interconnection procedures for Distributed Energy Resources (DERs). This project’s goal is to ensure that the procedures for interconnection of distribution-connected generation for a DP are made available, and that those documents include procedures for studies that make a “qualified change” to their system such that the transmission – distribution interface would be impacted. The project, as discussed in the “Detailed Description” below should include language that addresses applicability for specified aggregate levels of generation.

Project Scope (Define the parameters of the proposed project):

Revise the standard to include the DP in the “Applicability” section and update the Reliability Standard Requirements to include DP Interconnection Requirements for Distributed Energy Resources (DERs). Interconnection requirements for load is not part of this proposed project.

Further, as some distribution facilities do not have an associated DP, the project scope includes flexibility to address instances where the T-D interface does not have an associated DP and addressing any resultant reliability gap.

Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification² which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition):

The following is taken from the SPIDERWG white paper *NERC Reliability Standards Review*³, which houses the industry consensus for technical changes to FAC-001-4. A revision is needed to address the impact of DERs on the BES, and the SPIDERWG recommends the DP be included in FAC-001 to have interconnection requirements made available for its system that address “qualified changes” to its system. This standard was recently modified to allow the PC to address what a “qualified change” is for each applicable GO. Similarly, the SPIDERWG identified that the DP should have these procedures available for “qualified change”. The DP should be included in the “Applicability” section. Requirements should be modified to include the DP, with SPIDERWG proposing the following requirement revisions to be in scope:

- R1, for a specified level of aggregate generation in the DPs system
- R2, for a specified level of aggregate DER installations, to trigger a reliability impact study of affected the system; and
- R3 or R4, to ensure appropriate coordination studies be performed and what a “qualified change” is for the DP system.

² The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

³ Available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Whitepaper_SPIDERWG_Standards_Review.pdf

Requested information

Additionally, considerations should be given to regional, jurisdictional, and penetration level differences for inclusion of the applicability. A discussion of the impact of DERs on the BES could be added as a separate item in the list of supplemental material that is presented at the end of the document and linked to Requirement #3. In all cases, some technical guidance (e.g., compliance implementation guideline or a reliability guideline) will be needed for use by DPs in coordination with TOs.

Further, as Appendix 5B of the NERC Rules of Procedure⁴ documents the DP registration criteria, there may exist instances where the DP's system contains a significant amount of DER that can impact the T-D Interface, but does not meet the 75MW of peak load or any other criteria listed in that document. As such, there is a need for this project to identify any gaps associated with not having a DP applicable to T-D Interfaces that have no interconnection requirements posted.

Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):

Exact costs are unknown. However, this SAR is requesting that interconnection requirements of the DP system be made available and to specify the procedural way generation components are interconnected to the distribution system. As this is focused on documentation and availability of the documentation, such changes are anticipated to be lower in comparison to hard investments to Registered Entities. It is anticipated that clearly documented and available interconnection procedures assist in optimizing the transmission – distribution interface, potentially reducing costs.

Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources):

None. The SAR will impact DPs and their equipment by adding it to the standard. Further, the PC may need to document what a “qualifying change” is in their procedures. All of these are not BES facilities nor does this SAR propose DERs to become BES facilities.

To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):

Addition of: Distribution Provider (DP)
Potentially impacted: Transmission Owner (TO), Generator Owner (GO), and Planning Coordinator (PC)

⁴ See <https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix%205B.pdf>

Requested information	
	Do you know of any consensus building activities ⁵ in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
	This SAR has been submitted through the RSTC and has been vetted by the SPIDERWG membership. The SPIDERWG membership includes BAs, RCs, TOs, TPs, TOPs, PCs, and DPs. The SPIDERWG recommended this standard be revised in <i>White Paper: SPIDERWG NERC Reliability Standards Review</i> .
	Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
	FAC-002 requires specific entities to study impacts based on the requirements of FAC-001. SPIDERWG has a separate SAR to document its FAC-002 findings from the above mentioned white paper. Project 2020-05 recently updated FAC-002, and this SAR proposes scope on top of those changes.
	Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
	The SPIDERWG considered Standards revisions alongside compliance implementation guidance and reliability guidelines. Neither compliance implementation guidance nor reliability guidelines were determined to be sufficient by SPIDERWG in their consensus-based white paper above.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
<input checked="" type="checkbox"/>	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
<input type="checkbox"/>	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
<input checked="" type="checkbox"/>	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
<input type="checkbox"/>	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
<input type="checkbox"/>	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
<input type="checkbox"/>	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

⁵ Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Reliability Principles	
<input type="checkbox"/>	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
<input type="checkbox"/>	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles ?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
None	None

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
<input type="checkbox"/> Draft SAR reviewed by NERC Staff	<input type="checkbox"/> Final SAR endorsed by the SC
<input type="checkbox"/> Draft SAR presented to SC for acceptance	<input type="checkbox"/> SAR assigned a Standards Project by NERC
<input type="checkbox"/> DRAFT SAR approved for posting by the SC	<input type="checkbox"/> SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised

2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	DER Studies in NERC FAC-002 Standard for T-D Interfaces		
Date Submitted:	MM/DD/2022		
SAR Requester			
Name:	Shayan Rizvi, NPCC (NERC SPIDERWG Chair) John Schmall, ERCOT (NERC SPIDERWG Vice-Chair)		
Organization:	The NREC System Planning Impacts of DER Working Group (SPIDERWG)		
Telephone:	Shayan – 212-840-1070 John – 512-248-4243	Email:	Shayan – srizvi@nppc.org John – john.schmall@ercot.com
SAR Type (Check as many as apply)			
<input type="checkbox"/>	New Standard	<input type="checkbox"/>	Imminent Action/ Confidential Issue (SPM Section 10)
<input checked="" type="checkbox"/>	Revision to Existing Standard	<input type="checkbox"/>	Variance development or revision
<input type="checkbox"/>	Add, Modify or Retire a Glossary Term	<input type="checkbox"/>	Other (Please specify)
<input type="checkbox"/>	Withdraw/retire an Existing Standard		
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
<input type="checkbox"/>	Regulatory Initiation	<input checked="" type="checkbox"/>	NERC Standing Committee Identified
<input type="checkbox"/>	Emerging Risk (Reliability Issues Steering Committee) Identified	<input type="checkbox"/>	Enhanced Periodic Review Initiated
<input type="checkbox"/>	Reliability Standard Development Plan	<input checked="" type="checkbox"/>	Industry Stakeholder Identified
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
The purpose of FAC-002-4 ¹ is “to study the impact of interconnecting new or changed Facilities on the Bulk Electric System (BES)”. Recent studies and presentations to SPIDERWG indicate that if aggregate DER is integrated without adequate interconnection studies, reliable operation of the BES is likely to be impacted (e.g., contingencies worsened by aggregate DER tripping off-line).			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			

¹ FAC-002-4 latest version is available here: https://www.nerc.com/pa/Stand/Project_202005_Modifications_to_FAC001_and_FAC002_/FAC-002-4_final%20Ballot_clean.pdf

Requested information

With study of DER aggregations that impact the transmission and distribution interface, reliability issues on the bulk system resulting from increasing DER penetrations can be identified prior to an event or disturbance involving these aggregate amounts of distribution-connected generation or electricity end-user Facilities.

Project Scope (Define the parameters of the proposed project):

Modify FAC-002-4, as necessary, to require the Transmission Planner (TP) and Planning Coordinator (PC) to the study of distribution-connected generation (i.e., DERs). These revisions should include study of the reliability impact of interconnection of 1) new generation or electricity end-user Facilities as well as 2) existing interconnections of generation or electricity end-user Facilities making a “qualified change” under Requirement R6. The study should address aggregate DER at the transmission and distribution interface. The TP should be part of the definition of “qualified change” for these particular studies. This project does not address studies for impact on the distribution system (performed by the DP).

Further, as some distribution facilities do not have an associated DP, the project scope includes flexibility to address instances where the T-D interface does not have an associated DP and addressing any resultant reliability gap.

Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification² which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition):

SPIDERWG recommends that a Standard Drafting Team review and modify FAC-002-4, as necessary, such that the Standard requires the study of “qualified changes” to electricity end-user Facilities related to increasing levels of aggregate DERs. Also, there should be revisions to the standard to ensure the TP and PC perform a study when aggregate DERs cause “qualified changes” to transmission to distribution interface. In order to conduct “Steady-state, short-circuit, and dynamics studies, as necessary, to evaluate system performance under both normal and contingency conditions” under R1.3 and R3, aggregate DER data is required and supplied by DPs. These findings are documented in the SPIDERWG white paper *NERC Reliability Standards Review*³.

The SPIDERWG recommends that the TP be a part of the definition of “qualified changes” to determine what change would require a study (R1 of FAC-002) for the transmission to distribution interface in their planning area, and further clarify the term “electricity end-user Facilities” in the standard as it pertains to DERs. This project should also consider having the TP be able to define the specific DER information, as

² The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

³ Available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Whitepaper_SPIDERWG_Standards_Review.pdf

Requested information

needed, in order to perform their studies under R1.3 if such specificity enhances the ability for the TP to perform their studies.

Further, as Appendix 5B of the NERC Rules of Procedure⁴ documents the DP registration criteria, there may exist instances where the DP’s system contains a significant amount of DER that can impact the T-D Interface, but does not meet the 75MW of peak load or any other criteria listed in that document. With no entity to provide modeling information for “Steady-state, short-circuit, and dynamics studies, as necessary, to evaluate system performance under both normal and contingency conditions”, there may be a need for this project to identify any associated gaps.

Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):

The material costs are unknown. This project will require more studies at the TP and PC level, potentially increasing staffing costs. Certain Regional Entities have already seen a significant increase in the staffing required for their generation interconnection queues, which can inform the Standard Drafting Team on more specific costs for this project, albeit, regionally specific. There may be a cost impact to the DP in collection and provision of aggregate DER data to the TP and PC in their collection of “Steady-state, short-circuit, and dynamics” information.

Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources):

The SAR seeks to clarify the terms "qualified changes" and "electricity end-user Facilities" for aggregate amounts of DER at the transmission to distribution interface. Some of the transmission-side equipment at the transmission to distribution interface may be classified as BES. The aggregate amounts of DER are inherently not BES.

To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):

Addition of: Distribution Provider (DP)
 Impacted: Transmission Planner (TP), and Planning Coordinator (PC)
 Potentially Impacted: Transmission Owner (TO), and Generation Owner (GO)

⁴ See <https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix%205B.pdf>

Requested information	
	Do you know of any consensus building activities ⁵ in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
	This SAR has been submitted through the RSTC and has been vetted by the SPIDERWG membership. The SPIDERWG membership includes BAs, RCs, TOs, TPs, TOPs, PCs, and DPs. The SPIDERWG recommended this standard be revised in <i>White Paper: SPIDERWG NERC Reliability Standards Review</i> .
	Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
	Recently, NERC Project 2020-05 changed the term “materially modify” to a “qualified change for the purposes of facility interconnection” and added a requirement to have the PC define the “qualified change” in this standard and in FAC-001. FAC-002 requires specific entities to study impacts based on the requirements of FAC-001. SPIDERWG has a separate SAR to document its FAC-001 findings from the above mentioned white paper. Project 2020-05 recently updated FAC-002, and this SAR proposes scope on top of those changes.
	Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
	The SPIDERWG considered Standards revisions alongside compliance implementation guidance and reliability guidelines. Neither compliance implementation guidance nor reliability guidelines were determined to be sufficient by SPIDERWG in their consensus-based white paper above.

Reliability Principles	
	Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.
<input checked="" type="checkbox"/>	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
<input type="checkbox"/>	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
<input checked="" type="checkbox"/>	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
<input type="checkbox"/>	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
<input type="checkbox"/>	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.

⁵ Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Reliability Principles	
<input type="checkbox"/>	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
<input type="checkbox"/>	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
<input type="checkbox"/>	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles ?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
None	N/A

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
<input type="checkbox"/> Draft SAR reviewed by NERC Staff	<input type="checkbox"/> Final SAR endorsed by the SC
<input type="checkbox"/> Draft SAR presented to SC for acceptance	<input type="checkbox"/> SAR assigned a Standards Project by NERC
<input type="checkbox"/> DRAFT SAR approved for posting by the SC	<input type="checkbox"/> SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised

1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

**White Paper: Security Integration Strategy
Ensuring Security of the Bulk Power System through
Cyber and Physical Security Integration into Planning, Design, and Operational
Engineering Practices**

Action

Information

Summary

The ERO Reliability Risk Priorities Report identified an increase in cyber-physical risks as a high priority for the electricity sector. Through collaboration with industry stakeholders, NERC is focused on addressing cyber-physical risks to the BPS. The Security Integration Strategy outlines priorities to increase the integration of cyber and physical security into conventional planning, design, and operations engineering practices. The strategy identifies areas of focus where security integration can be enhanced to support a more secure, reliable, and resilient BPS. This presentation will cover the strategy and its core tenets.

Security Integration Strategy

Ensuring Security of the Bulk Power System through Cyber and Physical Security Integration into Planning, Design, and Operational Engineering Practices

December, 2022

Purpose and Background

Cyber and physical security are critical facets of the bulk power system (BPS) reliability and resilience. Grid transformation is expanding the existing attack surface due to the use of emerging technologies, additional communications and industrial controls as well as remote control capabilities. These channels provide opportunities for adversaries to exploit latent vulnerabilities within the existing system as cyber security was not part of the design equation for legacy equipment, software, and networks. The introduction of new technologies and new types of entities entering electricity markets also present new cyber attack vectors. Beyond these challenges, addressing security risks associated with the changing resource mix continues to be a high priority for the industry. Focusing on and mitigating these known and emerging risks is critical to the mission of the ERO Enterprise.¹



Modern cyber security incorporates a number of security principles and concepts, including a defense-in-depth philosophy; and historically, these concepts were not substantially integrated into the planning, design, and operation of the electric grid operational technology (OT) systems. As industry attempts to leverage improved operational performance and business efficiencies, the OT environment is increasingly connected to outside networks through the incorporation of intelligent electronic devices capable of routable internet protocol (IP) communications. This rapid change comes with greater security needs from the electricity sector OT environment and requires integration of cyber and physical security controls into these systems at deeper and earlier levels than was previously necessary. NERC is introducing the concept of **security integration**, which refers to the integration of cyber and physical security aspects into conventional planning, design, and operations engineering practices.

Security Integration: The integration of cyber and physical security aspects into conventional planning, design, and operations engineering practices.

¹ [https://www.nerc.com/AboutNERC/StrategicDocuments/ERO%20Enterprise%20Long-Term%20Strategy%20\(Aproved%20December%2012,%202019\).pdf](https://www.nerc.com/AboutNERC/StrategicDocuments/ERO%20Enterprise%20Long-Term%20Strategy%20(Aproved%20December%2012,%202019).pdf)

Security integration encompasses all aspects of the conventional engineering part of the electric industry. NERC is primarily focused on integrating cyber and physical security concepts more holistically into transmission planning, engineering design, and system operations to ensure that mitigating security controls are considered as early in the process as possible, rather than as a “bolt-on”² solution. For example, security integration may entail planning a BPS that minimizes or eliminates possible risk of a widespread cyber security compromise. It also includes driving cyber security controls comprehensively into the engineering design phase. Lastly, security controls can be further integrated with system operations to enable earlier detection, more effective mitigation, and quicker recovery from security events. Addressing cyber-physical risks to the BPS through security integration in the OT environment is necessary to accomplish a complete defense-in-depth strategy for securing the grid.

The NERC Security Integration Strategy that is set forth in this document outlines the ERO priorities to enhance security integration through working collaboratively with electricity sector stakeholders. It identifies areas of focus where security integration can be enhanced to support a more secure, reliable, and resilient BPS moving forward.

Known and Emerging Risks

The ERO Reliability Risk Priorities Report has identified an increase in cyber-physical risks as a high priority for the electricity sector.³ The process of identifying, validating, and prioritizing these risks includes gathering data and information from many sources, such as stakeholder engagements, communication with government agencies,⁴ and shared public intelligence among other sources as well. Cyber and physical risks as well as the likelihood of successful attacks on devices, communication paths, and grid systems and assets increase as the reliance on digitalization grows. Vulnerabilities in the power system and related components may come in the form of incomplete contingency analysis, legacy network design, vulnerable equipment, lack of visibility to existing networks, cross sector interdependence, rapidly changing technological innovations, human factors, etc. Foreign and domestic terrorists, criminals, and nation-state adversaries—each known as advanced persistent threats— have the capability to exploit vulnerabilities and carry out sophisticated attacks given enough time, resources, and opportunities. Successful exploitation of these vulnerabilities can result in detrimental impacts to BPS reliability and resilience, which directly affects equipment integrity, public safety, the global economy, and national security.

Risk Framework

The tenets of the NERC Security Integration Strategy can be mapped to the NERC Risk Framework⁵ that guides the ERO in prioritization of risks and provides guidance on the application of ERO policies, procedures, and programs to inform resource allocation and project prioritization in the mitigation of those risks. Additionally, the NERC Risk Framework includes measuring residual risk after mitigations are deployed to enable the ERO to evaluate the success of its efforts in mitigating risks. This provides a necessary

² Bolt-on cyber security generally refers to any security controls implemented after a system or device was designed and implemented. These security measures are likely to be expensive, less effective, or only partially implemented due to design limitations without disruptive or expensive redesign and implementation efforts.

³ https://www.nerc.com/comm/RISC/Documents/RISC%20ERO%20Priorities%20Report_Final_RISC_Approved_July_8_2021_Board_Submitted_Copy.pdf

⁴ For example, Department of Energy (DOE), the Department of Homeland Security (DHS), and the Canadian Electricity Association (CEA).

⁵ https://www.nerc.com/comm/RISC/Related%20Files%20DL/Framework-Address%20Known-Emerging%20Reliability-Security%20Risks_ERRATTA_V1.pdf

feedback for future prioritization, mitigation efforts, and program improvements. The successful reduction of risk is a collaborative process between the ERO Enterprise, industry, and the technical committees, including the Reliability and Security Technical Committee (RSTC) and Reliability Issues Steering Committee (RISC). The NERC Risk Framework provides a transparent process, with industry experts in parallel with ERO Enterprise experts, which includes risk identification, deployment of mitigation strategies, and monitoring the success of these mitigations.

Six specific steps have been identified that are consistent with risk management frameworks that are used by other organizations and industries:

1. Risk Identification and Validation
2. Risk Prioritization
3. Remediation and Mitigation Identification/Evaluation
4. Deploy Mitigation
5. Measure Success
6. Monitor Residual Risk

Each of these steps will require process development, including stakeholder engagement, validation/triage approaches, residual risk monitoring, and considerations of the ERO Enterprise’s level of purview over a risk, etc. A graphical representation of the NERC Risk Framework is shown in [Figure 1](#).

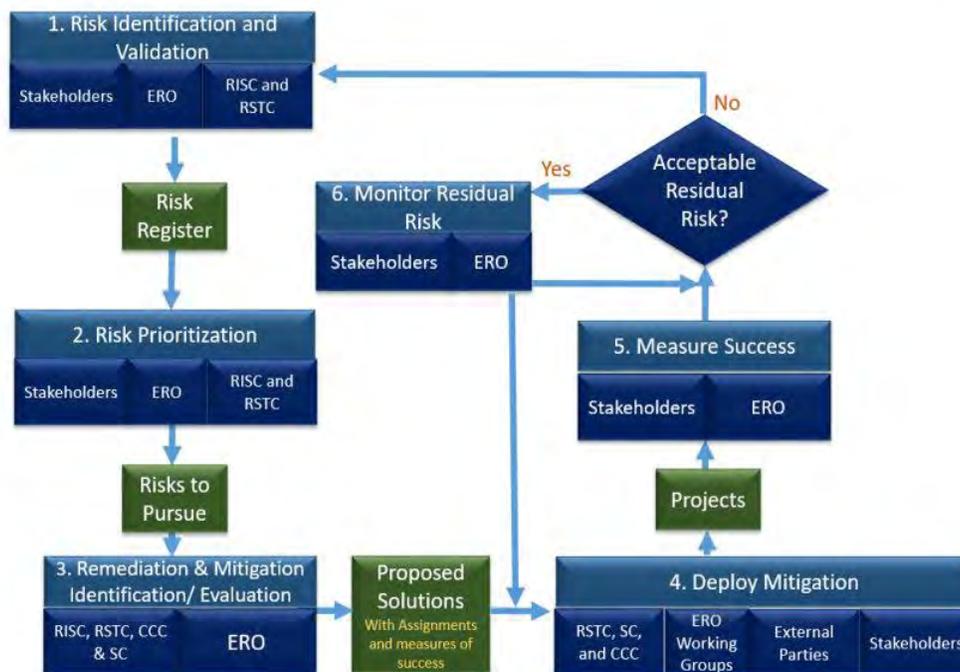


Figure 1: NERC Risk Framework

Tenets of the NERC Security Integration Strategy

The ERO Enterprise is dedicated to proactively identifying and addressing security challenges and continues to work with industry stakeholders to drive risk mitigation activities. Addressing these challenges require a multifaceted strategy to identify, prioritize, and mitigate risks that face the electricity sector OT environments. The strategy drives security integration concept in four key areas as outlined in [Figure 2](#). The core tenets of the NERC Security Integration Strategy incorporate near-term and long-term work items to ensure reliable and secure operation of the BPS. Components of the strategy with immediate priority are cyber-informed transmission planning, assessments of aggregate risks, cloud technology in the OT space, and DER and DER aggregator cyber security.

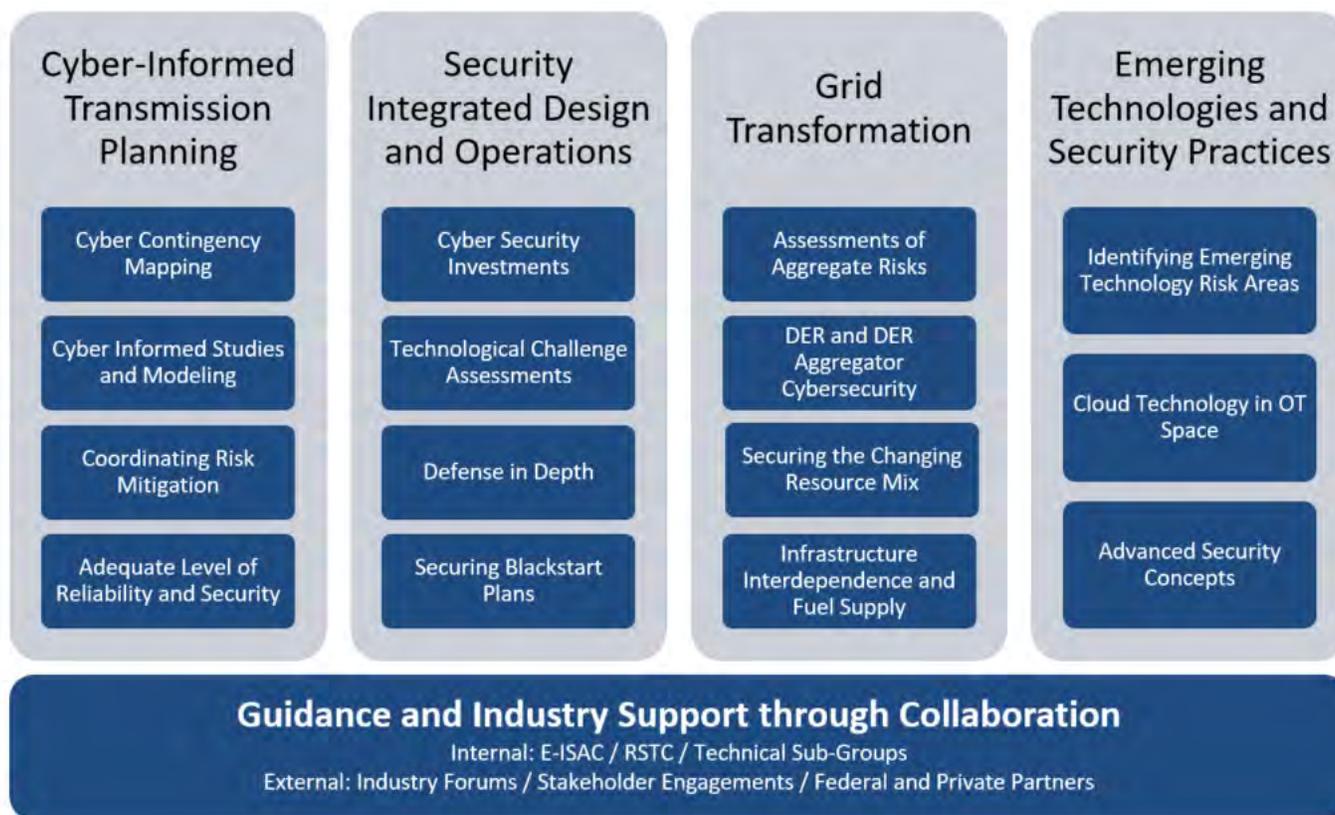


Figure 2: NERC Security Integration Strategy

The NERC Security Integration Strategy is primarily focused on risk identification and validation, prioritization, and development of possible mitigations. Future work by the ERO will explore deploying those mitigations and monitoring success collaboratively with industry.

By using anonymized data and lessons learned, NERC can explore a technical basis for incorporating cyber-informed transmission planning and additional operational controls into industry practices and possible future NERC standards enhancements. Additionally, this strategy addresses near- and long-term reliability risk issues through addressing the integration of technological advancements and emerging technologies applicable to the changing grid as well as addressing paradigm shifts, including cloud services adoption.

NERC will collaborate with industry partners to develop security guidance for aggregate “low” impacts, including development of cyber security risk scenarios in the OT space. The following sections briefly describe each tenet of the risk mitigation strategy.

Cyber-Informed Transmission Planning

Current transmission planning⁶ activities focus predominantly on physical security assessment per CIP-014 and only include cyber risk as part of the extreme contingency events in TPL-001. However, the ERO Enterprise is working collaboratively with industry experts to develop a cyber-informed transmission planning framework that can be used to integrate cyber security into steady-state and dynamic simulations of BPS reliability.

This will require enhancements to traditional transmission planning processes:

- Industry will need to determine how to identify appropriate cyber security risks and map them to associated planning contingencies used in studies. How those events will be modeled and studied will need to be explored in more detail. Addressing possible reliability risks posed by cyber security events should be addressed with corrective actions that may involve either enhancing cyber security controls or other capital projects (such as those used to address environmental events studied today). The goal is to drive towards a more cyber-resilient grid by identifying gaps and implementing appropriate mitigating security controls or prioritizing appropriate investments early in the grid planning process. This will require a paradigm shift and feedback loop between transmission planning and OT cyber security groups.
- New simulation engines and models may be needed to incorporate cyber design alternatives to understand their implications on current and future systems. Transmission planning and security team coordination can address vulnerabilities identified during studies and reduce the likelihood and impact of these vulnerabilities being exploited.
- The ERO plans to consider whether any enhancements to the existing adequate level of reliability definition are needed to fully incorporate security considerations (i.e., inclusion of adequate levels of security concepts); focus in this area will hopefully enable industry to make more concerted efforts to drive necessary mitigating security controls through an objective and repeatable planning process that links the engineering and security aspects early in project development.

Security Integrated Design and Operations

The ERO considers and encourages a shift in perspective regarding cyber security and its associated costs. Rather than being thought of as an insurance policy, concerted analysis should be given to the prospect of treating these costs as a capital investment; this is a reliability enhancement that minimizes impact and risk, improving resilience. Investments in cyber security are important factors contributing to the efficacy and maturity of a registered entity’s security program, including the technology controls implemented to protect its critical systems and data. It is more effective and efficient to support reliable operation of the BPS by integrating OT cyber security investments early in the design process for grid reinforcements rather

⁶ Transmission planning involves studying BPS performance, and it includes modeling and simulating all elements of the BPS.

than having them “bolted on” as operations and maintenance costs. Cyber-informed transmission planning may allow these and other benefits to be realized more effectively as well.

Equipment manufacturers may have networking access to large amounts of generation for maintenance, monitoring, or control that is not subject to minimum cyber-physical security standards. Analysis of the technical limitations of existing electric OT equipment must be performed in order to understand how to improve guidance and support industry when selecting and implementing next generation OT equipment capable of integrated security. In order to connect equipment to information networks, that equipment must be robust and capable of addressing security risks. The ways in which one thinks about and expect the equipment and systems to perform need to include cyber security best practices. Working with industry, NERC will provide needed guidance on how to assess technology solutions to meet rapid technological advancements in a secure way.

Segmented networks with appropriately grouped assets, designed-in security controls, hardened security-capable equipment, and other factors should be incorporated into system design and operations phases. As increasing levels of distributed energy resources (DER) come on-line, the need to add essential reliability services to the resources drives the need to ensure proper security assessments and planning as well.

Grid Transformation

The transformation of the electricity sector is primarily driven by the shift towards clean energy resources, and requires a deliberate and sustained focus from both an engineering and security perspective. Newly interconnecting inverter-based resources, such as wind, solar photovoltaic, battery energy storage, and hybrid plants, are changing how the grid is planned, operated, and designed. Furthermore, the growth of DERs and the introduction of the DER aggregator with FERC Order 2222⁷ changes the attack surface of the electricity sector. Many of these entities and the resources that they control are not subject to regulatory cyber security standards, such as the NERC Critical Infrastructure Protection (CIP) standards, and will require a collaborative and holistic approach to securing the overall electricity ecosystem. NERC is focused on identifying areas in which additional effort is needed to support entities in developing, procuring, and operating a high renewables grid of the future in a secure manner. This includes guidance around enhanced security postures, equipment standards and certification, integrated security practices, and risk assessments. Possible assessments may include exploring the concepts of aggregate risks by assessing the amount of generation any one entity or manufacturer controls, how their systems are deployed and secured, and identifying reliability risks. Regulatory visibility and oversight into these areas is key for assessing, implementing, and enforcing adequate levels of security across the BPS.

The energy transition requires a phased approach; however, the ERO must be agile and effective in driving meaningful security enhancements in this area as new resources connect to the system rapidly. Critical infrastructure interdependence continues to be of the utmost importance as the existing BPS still relies heavily on synchronous balancing resources for essential reliability services; understanding possible security vulnerabilities in the natural gas, hydro, and other critical infrastructure areas will be key to identifying possible BPS reliability issues. Analysis in this area is required to implement effective cyber

⁷ <https://www.ferc.gov/media/ferc-order-no-2222-fact-sheet>

security programs that encompass the networks and infrastructure that ensure fuel and resource availability.

Emerging Technologies

The electricity sector is experiencing a rapid change in the technologies being connected, used, and leveraged to plan and operate the BPS. Some of these technologies are still evolving or are relatively new for the adoption in the electric OT space, which may have an impact on BPS reliability moving forward. Examples include cloud technology, artificial intelligence, blockchain, DERs and DER aggregators, grid edge technologies, and others. NERC supports the adoption of emerging technologies and seeks to assist in fully realizing the potential that these technologies could have to enhance reliability and resilience of the BPS; however, leveraging and implementing these technologies in a reliable and secure manner is paramount. Key focus areas of this pillar (see [Figure 2](#)) include cloud adoption in the OT space, monitoring of emerging technologies and their deployment within the BPS, and promoting security enhancements through borderless architectures, such as zero trust, internal network security monitoring, and software-defined networking. NERC will work collaboratively with industry stakeholders to develop guidance material regarding the adoption of emerging technologies as well as conduct assessments on any necessary enhancements to the NERC CIP standards to adequately secure and leverage these technologies moving forward.

Guidance and Industry Support through Collaboration

Delivering on all aspects of this strategy requires outreach and collaboration with industry stakeholders, regulatory bodies, policy organizations, and equipment standards bodies. NERC is focused on identifying areas in which additional guidance related to enhanced security postures and integrating security with the planning, design, and operations that can be efficiently targeted. NERC is working with industry stakeholders to conduct assessments of possible risk areas and to develop guidance to support improved security practices in this area of the BPS. This includes coordinating with industry partners, such as the U.S. Department of Energy, Idaho National Laboratory (INL), the Electric Power Research Institute (EPRI), and others to drive adoption of security best practices, identify and address gaps in standards and requirements as well as to foster a security culture through focused collaboration between engineers, security professionals, and industry leadership. NERC and its Electricity-Information Sharing and Analysis Center continue to work collaboratively with a broad set of stakeholders to support these efforts.

NERC is relying on engagement and support from industry members through its Reliability and Security Technical Committee, particularly with the Security Integration and Technology Enablement Subcommittee (SITES), the Security Working Group and others. These groups can support the development and execution of components of this strategy with specific work items. This includes industry guidance materials, whitepapers, technical assessments and reports, and possibly future standard authorization requests (if needed) to move the needle towards more wholly integrated cyber and physical security within the BPS.

Milestone Plan

In support of NERC’s Security Integration Strategy, the following deliverables are planned for 2023. These include items being developed by the ERO Enterprise, in coordination with industry stakeholders as well as materials being developed by NERC SITES and planned to be submitted to the NERC RSTC:

- **Technical Report—IEEE-NERC Security Integration Report (IEEE):** It outlines the need to integrate cyber and physical security for a more reliable, resilient, and secure energy sector. Expected completion: **Q4 2022**
- **White Paper—Cyber Security for DERs and DER Aggregators (SITES):** It highlights equipment standards, device certification, and the possible need for NERC registration for DER aggregators to mitigate security risks. Expected completion: **Q4 2022**
- **White Paper—Cyber-Informed Transmission Planning (ERO Enterprise):** This cyber-informed transmission planning framework providing a roadmap for integrating cyber security aspects into transmission planning activities. Expected completion: **Q1 2023**
- **White Paper—Zero Trust (SITES):** It outlines important considerations for adoption of zero trust in OT environments. Expected completion: **Q1 2023**
- **White Paper—BES Operations in the Cloud (SITES):** It outlines important considerations for adoption of cloud technology in the electric utility environment. Expected completion: **Q2 2023**
- **White Paper—Cyber Security Maturity Models and NERC CIP Standards (ERO Enterprise):** It maps cyber security maturity model concepts to NERC CIP cyber security controls. Expected completion: **Q3 2023**
- **Assessment—Inverter-Based Resource Vendor Cyber Security:** It explores possible cyber security risks pertaining to vendor remote access for BPS inverter-based resources. Expected completion: **Q3 2023**
- **White Paper—Controls for DERs and DER Aggregator Cyber Security (SITES/NERC SPIDERWG⁸):** It provides technical details and guidance regarding cyber security for DERs and DER aggregators. Expected completion: **Q4 2023**
- **White Paper—Cyber Security for the Changing Resource Mix (SITES):** It describes recommended cyber security controls and practices for BPS-connected inverter-based resources. Expected completion: **Q4 2023**

⁸ NERC System Planning Impacts from Distributed Energy Resources Working Group

**White Paper: Cybersecurity for Distributed Energy Resources and DER Aggregators
(NERC Security Integration and Technology Enablement Subcommittee)**

Action

Approve

Background

This white paper provides industry with guidance regarding activities underway to further secure the electricity ecosystem under rapid grid transformation, specifically in the area of cybersecurity efforts for distributed energy resources (DERs) and DER Aggregators. NERC is working with industry stakeholders to advance cybersecurity controls for DERs as the penetration of these resources continues to grow in many areas across North America. This paper is informational and seeks to help provide clarity and guidance to industry stakeholders in this area. SITES is seeking RSTC approval.

Summary

The paper informs on IEEE 1547.3 cybersecurity guidance for DERs, and UL certification for device level security of DERs (including the certification roadmap and inputs). Provides recommendations of certification and standards support for DER cybersecurity by industry, security control requirements to be set by AGIRs for interconnection DER, and for DER Aggregators to become NERC Registered Entities.

Cyber Security for Distributed Energy Resources and DER Aggregators

NERC Security Integration and Technology Enablement
Subcommittee (SITES) White Paper
August 2022

Purpose

This brief paper provides industry with information regarding activities underway to further secure the electricity ecosystem under rapid grid transformation, specifically in the area of cyber security efforts for distributed energy resources (DERs) and DER aggregators. NERC is working with industry stakeholders to advance cyber security controls for DERs as the penetrations of these resources continue to grow in many areas across North America. This paper is informational and seeks to help provide clarity and guidance to industry stakeholders in this area.

Defining DER and DER Aggregator

The NERC System Planning Impacts from DERs Working Group (SPIDERWG) defines a DER as “any source of electric power located on the distribution system.”¹ This definition specifically focuses on those resources in the distribution system that can produce electric power (i.e., a generating resource) and does not include end-use loads or demand response as part of the DER definition. Conversely, the Federal Energy Regulatory Commission (FERC) DER definition outlined in FERC Order 2222² does consider load elements, including demand response, energy efficiency, and electric vehicles. The expanded FERC definition includes all DER types able to participate in regional organized wholesale electricity markets through aggregation (DER aggregators).

This document will generally refer to DERs with the NERC definition while acknowledging that DER aggregators may include DERs (with the FERC definition) that are load elements and not generating elements where used. This nuance does not critically impact the key points being made in this paper.

Understanding Security of the Electricity Ecosystem

The bulk power system (BPS) historically only included large, centralized power plants with power flowing across the transmission system, down through the distribution networks, and then to end-use consumers. A significant portion of this system was operated either with analog controls or very limited digital connectivity. However, the power system of today is undergoing a rapid transformation; the generation base is moving towards clean energy renewable resources connected through inverter technology. Large synchronous generation sites are being retired and replaced with smaller wind and solar resources, battery energy storage, and hybrid power plants. BPS connected resources are also being offset with DERs that connect to the distribution system, some of which are behind-the-meter and owned and operated by end-use consumers or third parties. Many of these systems are now connected directly to the Internet as digitalization and its associated connectivity continue to expand exponentially. Grid planners, designers, and operators are faced with managing a grid with a significant portion of the resource base connected to the distribution system with little to no direct visibility of these resources. FERC Order 2222 introduced the DER

¹ <https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Terms%20and%20Definitions%20Working%20Document.pdf>

² <https://ferc.gov/media/ferc-order-no-2222-fact-sheet>

aggregator, which will be another entity in the electricity ecosystem that will play a key reliability and security role moving forward.

This paper focuses on the security aspects of the overall electricity ecosystem. The NERC Critical Infrastructure Protection (CIP) standards apply only to bulk electric system (BES) cyber systems and their associated BES cyber assets as outlined in the currently effective version of NERC CIP-002.³ In general, the NERC CIP standards are not applicable to systems or assets connected to the distribution system. Historically, this has not been a significant risk since those systems did not have a significant impact on the overall BPS or BES. However, the changing nature of the resource mix, the potential security risks posed through DER aggregation, and the absence of regulatory standards could all present significant risks to the BPS if not properly mitigated.

Therefore, it is important to understand how the various cyber security standards, requirements, practices, and industry efforts are working together in order to secure the overall electricity ecosystem now and moving forward. Equipment needs to be built with secure technological capabilities and with suitable equipment certifications. Operational risk assessments (and mitigations) are needed to secure these systems in real-time.

Background on IEEE 1547-2018 Standard and Linkage to UL Listing

IEEE 1547, *Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*, was completely overhauled with the revision that was published in 2018 (IEEE 1547-2018).⁴ The update to the standard focused on the technical specifications, testing, and interoperability between distribution providers and DERs; it did not include cyber security requirements for DERs. IEEE 1547.3-2007, *IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems*, was originally focused on interoperability, monitoring, information exchange, and DER control but initially did not include any considerations for cyber security. The IEEE P1547.3 working group is currently revising the guide, now titled *IEEE Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*, to focus directly on cyber security measures and controls for DERs. IEEE standards are wholly voluntary and must be put into effect by a certifying organization or other Authority Governing Interconnection Requirements (AGIR).

IEEE 1547-2018 is being implemented across North America by AGIRs (e.g., state public utility commissions, regional system operators, distribution entities). Entities can ensure that equipment being manufactured complies with the requirements of IEEE 1547-2018 based on the conformance testing procedures outlined in IEEE 1547.1-2020. This standard specifies the type, production, commissioning, period tests, and evaluations that shall be performed to confirm that equipment conforms to IEEE 1547-2018. Underwriters Laboratories (UL) 1741, *Standard for Inverters, Converters, Controllers and Interconnection System Equipment for Use with Distributed Energy Resources*, is primarily a safety standard that certifies equipment pass the tests outlined in IEEE 1547.1. This enables manufacturers to certify that commercially available DERs meet the requirements of IEEE 1547-2018. **Figure 1** shows a high-level illustration of the overall process.

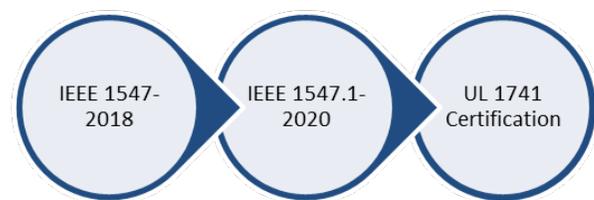


Figure 1: IEEE 1547-2018 Standard to UL 1741 Certification

³ <https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf>

⁴ <https://standards.ieee.org/ieee/1547/5915/>

Cyber Security Certification Standards Efforts

Many cyber security standards, guides, and recommended practices exist today. Each has its strengths and weaknesses. Some in-depth documents are written for product types outside of the Renewables space, whereas some documents written for Renewable Energy technology do not incorporate mandatory language for certification. To this extent, for certification purposes, there are no standards and test procedures available with a complete list of detailed auditable requirements. Since the cyber security features are spread out over multiple guides and standards, there is a need to conjoin applicable materials to produce a single standard with requirements and testable items that covers the full scope of DER cyber security certification in an understandable format for industry stakeholders. In general, these standards and guides are used to complement each other, however the standards-development effort will also filter out contradicting, outdated, or compromised technology requirements. By thorough filtering and selection, as well as stakeholder input, the requirements and testable items are defined. A national or international cyber security certification standard can aid industry stakeholders to evaluate and validate the cyber security posture of their DER or IBR devices before they are connected to the electric grid. A unified standard will not only facilitate robust cyber security within the electric grid, it will also ensure the concept of security by design is being implemented beginning at the device level for new DER systems.

Roadmap for UL Cyber Security Certification Standard

Drafting consensus-based cyber security certification standards requires effective industry leadership and regular participation from stakeholders. UL intends to make use of the best practices in existing DERs and industrial cyber security bodies of knowledge to create a standard intended specifically for certification by UL as an independent and accredited third-party laboratory (see [Figure 2](#)).⁵ UL plans to offer this cyber security certification service in addition (or as a stand-alone service) to its existing electrical safety certification services. An initial draft of the new UL standard is expected to be available for circulation among interested experts in 2022. Feedback will be gathered and suggested changes incorporated during Q3/Q4 of 2022 with publication of a UL standard by year's end. NREL and UL can streamline this effort by using in-house expertise, state-of-the-art testing facilities, and by engaging industry experts to participate in the associated UL Standards Technical Panel. UL will begin offering cyber security evaluations and certifications upon publication.⁶ This cyber security standard certification will advance the security by design principle for the next generation of technologies and will be applicable to both distributed generation and storage technologies. In 2023, UL will take the further step of assembling a standing committee of industry experts to provide ongoing input for continuous improvement and potential submission to the American National Standard Institute (ANSI) to become and accredited ANSI standard. [Figure 3](#) illustrates this process.

⁵ <https://www.nrel.gov/docs/fy22osti/81827.pdf>

⁶ <https://www.ul.com/news/ul-and-nrel-announce-cybersecurity-testing-recommendations-distributed-energy-resources-and>



Figure 2: Inputs to UL Cyber Security Certification Standard [Source: NREL]



Figure 3: Process to UL Certification and ANSI Status

Operational Security Posture of DERs

UL cyber security certification will help ensure that future DERs being installed on the grid will have security incorporated into the equipment by design. This process ensures that an adequate level of security features and controls are integrated into these system components during manufacturing and that they are tested and ready to be enabled by the user. However, these features need to be utilized to ensure a strong security posture across the entire electricity ecosystem during real-time operations. The certification of equipment capabilities and security features does not ensure that those systems are installed and operated with these security features utilized (see [Figure 4](#)). Simply having the security control functions present in the equipment does not guarantee that the controls are enabled and configured. For example, a device-level firewall that is not enabled or enabled without proper settings does not achieve the intended security objective for real-time operations. This presents BPS risk and is further reinforced by the fact that some DER classes are owned by end-use consumers (e.g., rooftop solar PV systems) and connected directly to the Internet. Often, this equipment is not intended to be programmatically accessed, configured, or otherwise alerted by the consumer from a security perspective. Additional mitigations are required.

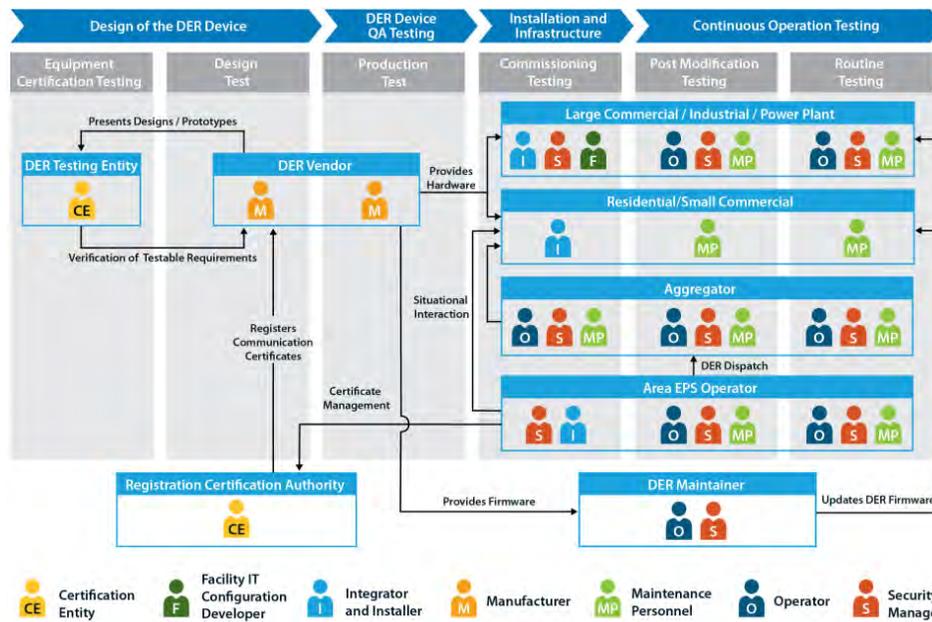


Figure 4: Roles and Responsibilities for DER Cyber Security [Source: NREL]⁷

The NERC CIP standards ensure that registered entities meet minimum requirements for BES cyber systems and can demonstrate compliance by those systems operationally; however, those standards and associated requirements are generally not applicable to entities or asset owners on the distribution system. Therefore, these systems pose a potential security risk for secure delivery of generation to end-use loads and could lead to vulnerabilities being exploited, potentially affecting many aggregated assets during an inevitable attack from cyber threat actors.⁸

Including DER assets (and asset owners) within the NERC CIP standards construct is not an effective short-term solution to this problem due to the scale and magnitude of assets and owner/operators of DERs. DER devices should be certified and tested so that the equipment is capable of enhanced security measures. AGIRs should ensure that these functions are configurable post-installation, and the specific security controls and implementations should be engineered to mitigate known and potential threats to the electric sector by utilizing a risk-based approach. NERC will work with industry groups (e.g., the National Association of Regulatory Utility Commissioners), distribution providers, and other key stakeholders to help support the operational security of DERs moving forward.

Cyber Security Risks of the DER Aggregator

Introduced in FERC Order No. 2222, the DER aggregator is a market entity that is able to collect and aggregate multiple DER owners and leverage their collective capacity in order to participate in an electrical wholesale market. The DER aggregator will typically use existing communication networks to provide telemetry and other information from the DER to the DER aggregator and up to the independent system operator/regional transmission organization. Those communications networks are likely owned by third-parties and many individual DERs are likely Internet-connected and accessed through routable protocols. ***The reliability and cyber security risks posed by the DER aggregator are not the same as those posed by individual DERs since the potential compromise of a DER Aggregator could have a significantly greater aggregate impact to the BPS. The compromise of any one DER is likely to have a minimal impact on the BPS; however, the compromise of a DER aggregator could affect hundreds or thousands of individual assets controlled by a centralized DER aggregator.***

⁷ <https://www.nrel.gov/docs/fy22osti/81827.pdf>

⁸ https://csrc.nist.gov/glossary/term/threat_actor

DER aggregators have a unique role in the system and they have no standardized cyber security requirements pertaining to their function in the electricity sector. Additionally, they are not anticipated to incorporate as a “control center” in the traditional sense. The system they bid into is operated by and secured by the market operator (ISO/RTO), and their operating signals are for non-owned equipment that previous sections of this paper have described as moving towards an enhanced cyber security posture through UL certification. However, the interfaces they connect across and infrastructure they use to monitor and control their equipment are likely to be conventional Enterprise information technology (IT) equipment protected under an IT security program. Such security controls may be lacking in the operational technology (OT) environment.

If compromised, the DER aggregator can impact a large amount of electrical assets (in MVA). The possible inclusion of cyber security certification of the equipment under a DER aggregator’s control should not be viewed as ensuring proper security controls are in place for the DER aggregator’s OT systems. Device level UL certification is a good first step, but DER aggregators should adopt an OT cyber security program that includes security controls that address the risks associated to their unique role in a secure electric infrastructure.

Currently available reference material can be used to assist both OEM’s of DER technologies⁹ and DER aggregators¹⁰ in securing devices as well as communications used for monitoring and control of DERs. Additionally, the update to IEEE 1547.3 with guidelines on DER cyber security is available as draft.¹¹

Recommended Industry Actions Moving Forward

The following are recommended actions that NERC and its stakeholders should take to support a secure electricity ecosystem with increasing levels of DERs (generation), load-side flexible resources, and DER aggregators:

- **DER Cyber Security Certification:** NERC and industry stakeholders should actively support DER cyber security certification initiatives and provide expertise related to BPS impacts of growing DERs and the introduction of the DER aggregator. Efforts such as those pursued by UL to ensure that future DER equipment is designed, tested, and commercially installed with sufficient cyber security controls in place will help secure the overall electricity ecosystem. Without necessary cyber security controls designed in to the components and systems, security risks could be introduced and expensive and/or less effective bolt-on security measures could be necessary in the future.
- **Cyber Security in Distribution Interconnection Requirements:** Similar to how the AGIR establishes necessary equipment performance specifications in IEEE 1547, the AGIR could also be responsible for establishing requirements that ensure newly interconnection DERs are equipped and operationally configured with specific cyber security controls in place. This will require modifications to the IEEE 1547 standard to ensure that cyber security is included in the standards body rather than as an informational guide (i.e., focusing on including some or all aspects of the IEEE 1547.3 guide into the main body of the IEEE 1547 standard).
- **DER Aggregator Registration:** NERC and industry stakeholders have acknowledged that the concept of the DER aggregator is not presently addressed in NERC registration criteria, constituting a reliability and security gap if DER aggregators start actively controlling and operating significant amounts of DERs. In aggregate, these resources will have an impact on the BES. The NERC Reliability and Security Technical Committee and its stakeholder groups should determine the extent of DER aggregator participation in wholesale electricity markets today and in the future and identify possible reliability and security risks these entities could pose if

⁹ <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series>

¹⁰ <https://csrc.nist.gov/publications/detail/sp/1800-32/final>

¹¹ <https://standards.ieee.org/ieee/1547.3/10173/>

compromised. NERC will assess these reliability and security impacts and determine if the DER aggregator should be included as a NERC registered entity under certain situations.

- **Proactive Understanding of DER and DER Aggregator Cyber Security Risks:** Industry stakeholders should actively engage in understanding the risk posed with growing levels of DERs and the introduction of DER aggregators. Cyber security risks exist throughout the product lifecycle: equipment design, testing, commissioning, and operation. Understanding the aggregate risks posed by DERs and DER aggregators and how to mitigate them will better posture the BPS for reliable operation of DERs.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

White Paper: Cybersecurity for Distributed Energy Resources and DER Aggregators

Brian Burnett, SITES Chair

Marc Child, RSTC Sponsor

Reliability and Security Technical Committee Meeting

December 6, 2022 | St. Paul, MN

RELIABILITY | RESILIENCE | SECURITY



The paper informs on IEEE 1547.3 cybersecurity guidance for DERs, and UL certification for device level security of DERs (including the certification roadmap and inputs). Provides recommendations of certification and standards support for DER cybersecurity by industry, security control requirements to be set by AGIRs for interconnection DER, and for DER Aggregators to become NERC Registered Entities.

- Drivers
 - Rapid grid transformation, in particular distributed energy resources (DERs)
 - Cybersecurity controls are lagging behind other technology advances such as smart inverters
 - IEEE 1547.3 is under revision – “IEEE Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems”
 - Underwriters Laboratories (UL) 1741 – “Standard for Inverters, Converters, Controllers and Interconnection System Equipment for use with Distributed Energy Resources” – is a safety certification and does not address cybersecurity
- These two initiatives are working together to address a unified standard for cybersecurity for commercially available DERs

- This white paper serves to:
 - Educate on IEEE and UL efforts
 - Provide the background, purpose, and scope of that effort
- Subsequent updates of this white paper will:
 - Notify and inform NERC stakeholders on results of the project
 - Amplify messaging to encourage awareness and adoption of the standard

- Updates resulting from RSTC comments received
 - Comments highlighting need for technical details are being incorporated into scope of a follow up technical paper being developed by joint SPIDERWG and SITES collaboration subteam
 - Paragraph added (below) providing security control reference material for securing communications

Currently available reference material can be used to assist both OEM's of DER technologies¹, and DER aggregators² in securing devices as well as communications used for monitoring and control of DER's. Additionally, the update to IEEE 1547.3 with guidelines on DER cyber security is available as draft³.

¹ <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series>

² <https://csrc.nist.gov/publications/detail/sp/1800-32/final>

³ <https://standards.ieee.org/ieee/1547.3/10173/>

SITES requests the RTSC approve this whitepaper

A stylized map of North America, including the United States, Canada, and Mexico. The map is rendered in shades of blue and grey. A horizontal blue band with a gradient from dark to light blue passes behind the map, serving as a background for the title text.

Questions and Answers

**White Paper: Zero Trust for Electric OT
(NERC Security Integration and Technology Enablement Subcommittee)**

Action

Request for Comments

Background

SITES formed a subteam for Zero Trust to develop this whitepaper with the purpose of providing clarity to the electric industry on the applicability of concepts to electric operations technology environments and enabling valuable use cases addressing barriers to adoption such as legacy technology and compliance.

Summary

The SITES white paper informs the electricity sector on zero trust (ZT) concepts and provides considerations and recommendations regarding the adoption of ZT controls in operational technology (OT) and industrial control system (ICS) environments. The paper leverages the concept ZT maturity models for varying levels of implementation by registered entities and recommends entities develop their own roadmap for security and technology maturation. Finally, the paper describes considerations regarding ZT adoption by registered entities and the NERC Critical Infrastructure Protection (CIP) standards.

Zero Trust Security for Electric OT

NERC Security Integration and Technology Enablement

Subcommittee (SITES) White Paper

October 2022

Introduction

The purpose of this white paper is to inform the electricity sector about zero trust (ZT) concepts and to provide considerations and recommendations regarding the adoption of ZT controls in operational technology (OT) and industrial control system (ICS) environments. This paper describes some of the key differences between OT and information technology (IT) environments; however, this paper's focus is specifically on the implementation considerations in the OT environment. This paper also leverages the concepts of ZT maturity models for varying levels of implementation by registered entities. Lastly, this paper describes considerations regarding ZT adoption by registered entities and the NERC Critical Infrastructure Protection (CIP) standards.

What is Zero Trust?

Computer networks have been traditionally designed to follow a “bastion” model wherein strong, multi-layered perimeter defenses are utilized to prevent intrusion. Defenses inside the bastion are typically far less robust, and the average user can traverse a network to access those resources they desire once admitted. Internal security controls and monitoring are potentially less robust and assume that an authenticated user is “trusted” so their actions receive less scrutiny than they do at the network boundary. In a zero trust architecture (ZTA), no user or device is implicitly trusted and undergoes access and authorization tests continually. Additionally, these tests grant access to data, not to networks. The concept of ZT shifts cyber security control design philosophy from the old adage of “trust, but verify” to “never trust, constantly verify.”

ZT as Defined by the National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) defines ZT as a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.¹ The basic premise of ZT is there is no implicit trust granted to user or systems based on their physical or network location because there is no trust of any network, user, or device.²

NIST further defines ZTA as an enterprise cyber security plan that utilizes ZT concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a ZT enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.³

¹ https://csrc.nist.gov/glossary/tem/zero_trust

² https://www.nerc.com/pa/Stand/Project_201602_Modifications_to_CIP_Standards_RF/2016-02_CIP-005_and_Zero_Trust_Webinar_Slides_02192020.pdf

³ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

Tenets of Zero Trust

ZTA is designed and deployed with adherence to the following ZT basic tenets:

- **All data sources and computing services are considered resources.** A network may be composed of multiple classes of devices. A network may also have small footprint devices that send data to aggregators/storage, software as a service, systems that send instructions to actuators, and other functions. Also, an enterprise may decide to classify personally owned devices as resources if they can access enterprise-owned resources.
- **All communication is secured regardless of network location.** Network location alone does not imply trust. Access requests from assets located on enterprise-owned network infrastructure (e.g., inside a legacy network perimeter) must meet the same security requirements as access requests and communication from any other network not owned by an enterprise. In other words, trust should not be automatically granted based on the device being on enterprise network infrastructure. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.
- **Access to individual enterprise resources is granted on a per-session basis.** Trust in the requester is evaluated before the access is granted; access should also be granted with the least privileges needed to complete the task. Additionally, authentication and authorization to one resource will not automatically grant access to a different resource.
- **Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.** An organization protects resources by defining what resources it has, who its members are (or the ability to authenticate users from a federated community), and what access to resources those members need. For ZT, client identity can include the user account (or service identity) and any associated attributes assigned by the enterprise to that account or artifacts to authenticate automated tasks. Requesting asset state can include device characteristics like software versions installed, network location, time/date of request, previously observed behavior, and installed credentials. Behavioral attributes include but are not limited to automated subject analytics, device analytics, and measured deviations from observed usage patterns. Policy is the set of access rules based on attributes that an organization assigns to a subject, data asset, or application. Environmental attributes may include such factors as requestor network location, time, reported active attacks, etc. These rules and attributes are based on the needs of the business process and acceptable level of risk. Resource access and action permission policies can vary based on the sensitivity of the resource/data. Least-privilege principles are applied to restrict both visibility and accessibility.
- **The enterprise monitors and measures the integrity and security posture of all owned and associated assets.** No asset is inherently trusted. The enterprise evaluates the security posture of the asset when evaluating a resource request. An enterprise implementing ZTA should establish continuous diagnostics and mitigation or a similar system to monitor the state of devices and applications and should apply patches/fixes as needed. Assets that are discovered to be subverted, have known vulnerabilities, and/or are not managed by the enterprise may be treated differently (including denial of all connections to enterprise resources) than devices owned by or associated

with the enterprise that are deemed to be in their most secure state. This may also apply to associated devices (e.g., personally owned devices) that may be allowed to access some resources but not others. This, too, requires a robust monitoring and reporting system in place to provide actionable data about the current state of enterprise resources.

- **Resource authentication and authorization are dynamic and strictly enforced before access is allowed.** This is a constant cycle of obtaining access, scanning and assessing threats, adapting, and continually re-evaluating trust in ongoing communication. An enterprise implementing a ZTA would be expected to have identity, credential, and access management as well as asset management systems in place. This includes the use of multifactor authentication for access to some or all enterprise resources. Continual monitoring, with possible re-authentication and reauthorization, occurs throughout user transactions as defined and enforced by policy, (e.g., time-based, new resource requested, resource modification, anomalous subject activity detected) which strives to achieve a balance of security, availability, usability, and cost-efficiency.
- **The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.** An enterprise should collect data about asset security posture, network traffic, and access requests; process that data; and use any insight gained to improve policy creation and enforcement. This data can also be used to provide context for access requests.

To summarize, a user accesses data through the intermediation of applications in a ZT world. They do not traverse networks whenever it can be avoided. Network based access, such as that conferred by virtual private networks, is avoided. Identity management and access controls (e.g., conditional, role based) are enforced at the application. The world of ZT thus resembles modern mobile applications, and many of the services in use today use this model, such as Office 365. ZT embeds comprehensive security monitoring; granular, dynamic, and risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus specifically on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources.

Zero Trust Maturity Model

ZT should be considered a forward-thinking strategy for control design. However, while real-time, trustless, and policy-based algorithmically-driven access decisions across an organization's technology footprint are a pinnacle to be strived for, it is best to realize a sliding scale maturity model from implicit trust controls to less trust and then to trustless. Across all industries, ZT is a paradigm shift that is accompanied by a roadmap to gradually implement least trust controls. It is important to understand that available technology solutions can provide incremental steps forward on an entity's ZT maturity roadmap, but such vendors may or may not advertise their products as ZT.

The Cybersecurity and Infrastructure Security Agency (CISA) has defined a ZT maturity model with five distinct pillars (see [Figure 1](#)). Each pillar may be advanced independently, but an organization is likely to see cross-pillar interoperability and dependencies that require process and technology coordination as they

reach advanced maturity. CISA's maturity model shown in [Figure 2](#) further develops these pillars across three levels of maturity: traditional, advanced, and optimal.

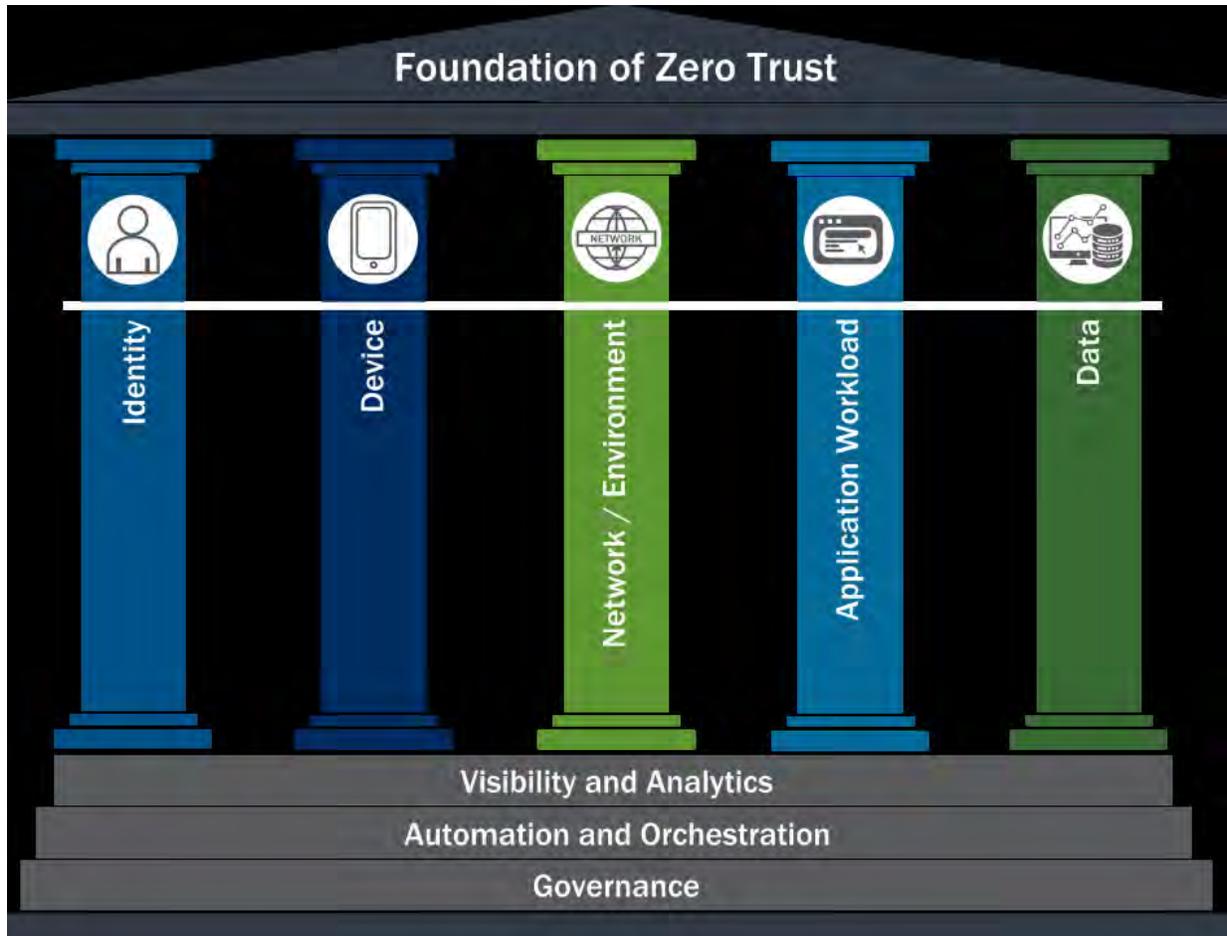


Figure 1: CISA's Foundation for ZT

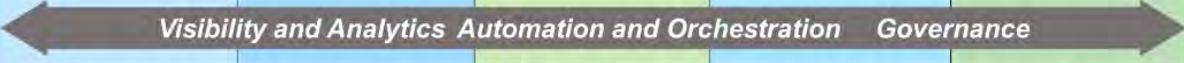
	Identity	Device	Network / Environment	Application Workload	Data
Traditional					
	<ul style="list-style-type: none"> • Password or multifactor authentication (MFA) • Limited risk assessment 	<ul style="list-style-type: none"> • Limited visibility into compliance • Simple inventory 	<ul style="list-style-type: none"> • Large macro-segmentation • Minimal internal or external traffic encryption 	<ul style="list-style-type: none"> • Access based on local authorization • Minimal integration with workflow • Some cloud accessibility 	<ul style="list-style-type: none"> • Not well inventoried • Static control • Unencrypted
					
Advanced					
	<ul style="list-style-type: none"> • MFA • Some identity federation with cloud and on-premises systems 	<ul style="list-style-type: none"> • Compliance enforcement employed • Data access depends on device posture on first access 	<ul style="list-style-type: none"> • Defined by ingress/egress micro-perimeters • Basic analytics 	<ul style="list-style-type: none"> • Access based on centralized authentication • Basic integration into application workflow 	<ul style="list-style-type: none"> • Least privilege controls • Data stored in cloud or remote environments are encrypted at rest
					
Optimal					
	<ul style="list-style-type: none"> • Continuous validation • Real time machine learning analysis 	<ul style="list-style-type: none"> • Constant device security monitor and validation • Data access depends on real-time risk analytics 	<ul style="list-style-type: none"> • Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted 	<ul style="list-style-type: none"> • Access is authorized continuously • Strong integration into application workflow 	<ul style="list-style-type: none"> • Dynamic support • All data is encrypted
					

Figure 2: CISA's ZT maturity model

Application of Principles

Trustless Example

What does it mean to be trustless? Consider an example of a system operator logging into a supervisory control and data acquisition (SCADA) human-machine interface (HMI) or workstation and opening their application client. First, it is taken for granted that the workstation has network access; however, under a ZTA implementation, trustless network access controls would replace this assumed or implied workstation network access authorization. A ZT policy decision engine would perform an algorithmic evaluation of a number of risk factors, such as the workstation's current security patch levels, completed anti-malware scans status, mac address validation, security certificate validation, and/or access authorization to the specific network subnet or virtual local area network (VLAN), such as the control center operator VLAN.

Passing all checks results in the workstation being granted network access, but failing one or more tests could result in a quarantining action whereby the network connection is re-assigned to a remediation VLAN that limits connectivity to only what is necessary for the system to communicate with patching, anti-virus, and other system management servers. Additionally, it is important to understand that in a truly trustless design, the access decision is one that is continually re-evaluated overtime. This ensures adherence to security polices and doesn't allow perpetual access based off prior access decision outcomes.

Similarly, when an operator attempts to authenticate into their SCADA client, additional ZT policies are evaluated against the policy engine: Does the operator have the proper roles or group membership assignments necessary to be authorized for the SCADA application? Does this access request fall within normal operating hours as defined within the policy? Does this login match with the user's previous system usage behavior? These factors are combined with the source system (the workstation) evaluations previously mentioned. What is the real-time security risk state of the organization at this time? For example, has malware recently been detected? All of these real-time and dynamic evaluations determine if access is granted and to what extent. Dependent on the measured and evaluated risk of the request, access could be denied, granted, or granted with lesser privileges until remediation is achieved. Alternatively, the authentication could be elevated to a multi-factor authentication prompt to address elevated risk.

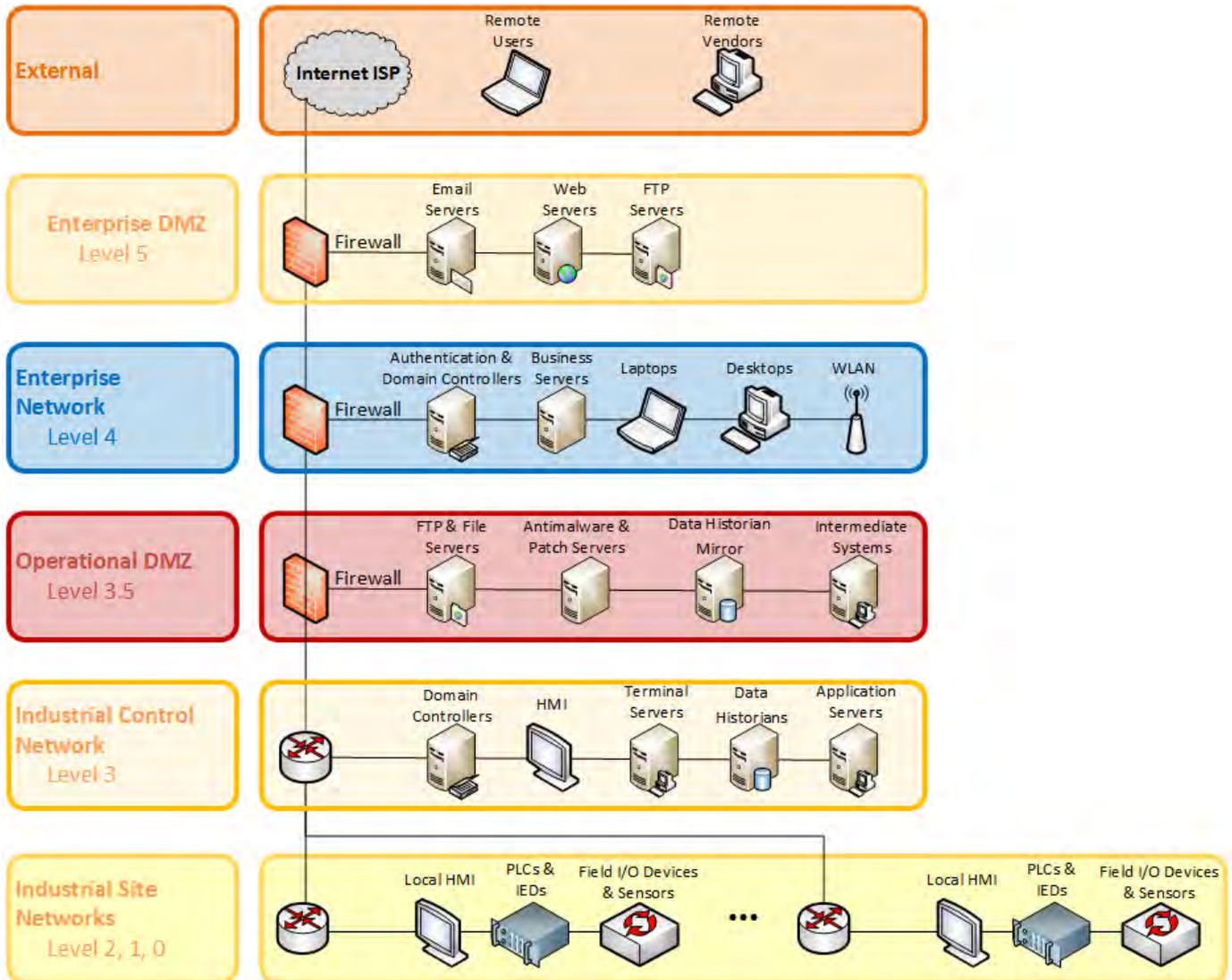
The example controls given above may seem excessive, or they may be perceived as creating undo operational risk. These are fair concerns, and they emphasize the need for utilities to approach ZT with their own roadmap to maturity. Recognize that controls at the upper end of ZT maturity come with an equal cost of technical complexity and administrative burden.

Zero Trust in OT/ICS Environment

In OT/ICS environments, it is important to consider ZT in terms of securing and protecting critical processes, not just data. In other words, when implementing ZT in OT/ICS one must not only consider access and authorization to the data hosted by a data source but managing access to the data source device itself.

Within many (most) OT/ICS environments, a distinction has to be made between the different subsystem capability and functional (Purdue model⁴) levels when considering the implementation of ZT (see [Figure 3](#)).

⁴ [Purdue Enterprise Reference Architecture - Wikipedia](#)



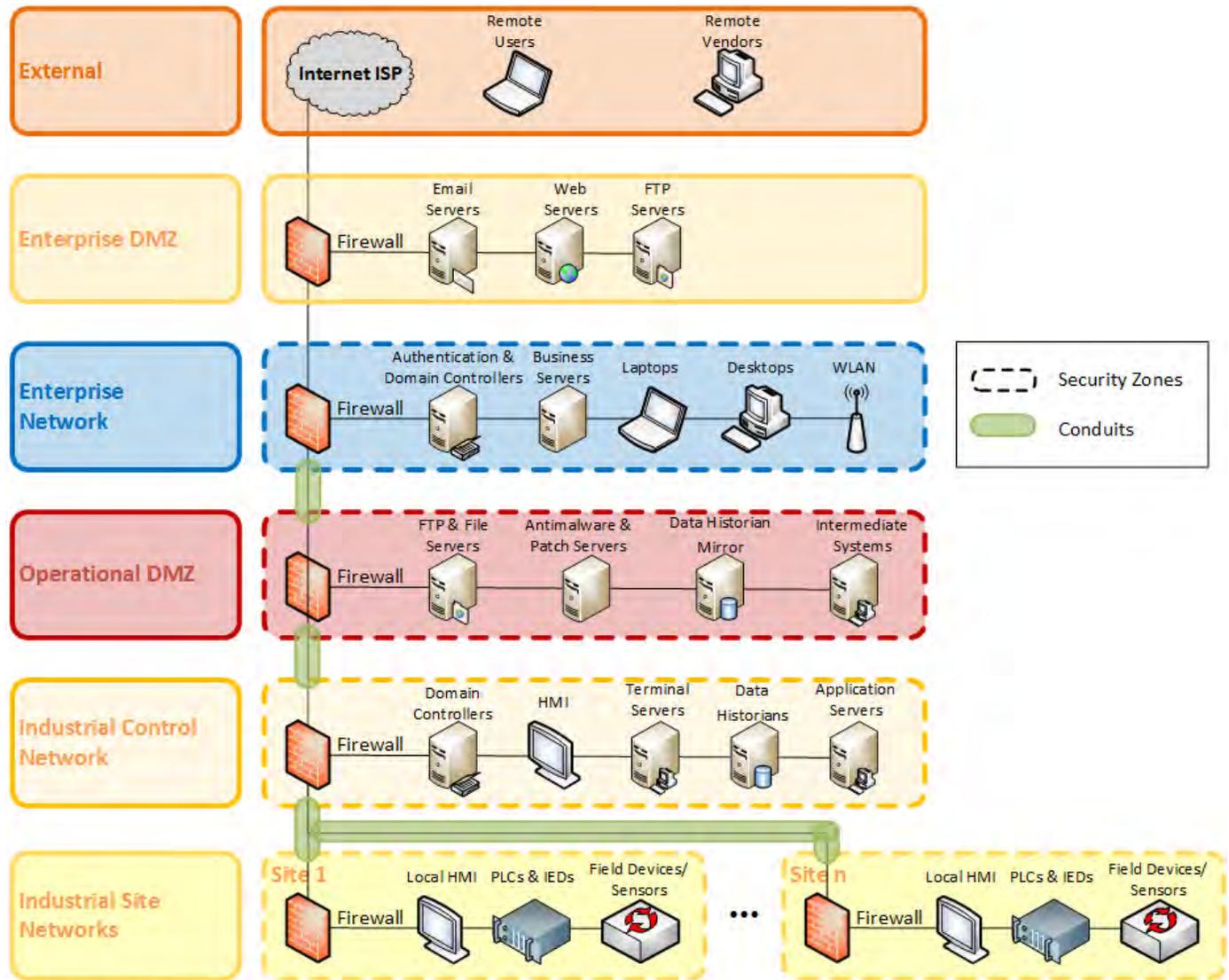
Adapted from the ISA representation of the Purdue Model

Figure 3: ICS Network by Purdue Model

Lower level (Purdue level 0-1) ICS systems and devices (e.g., IEDs, PLCs, sensors) lack the capability of granular access controls on the device itself and must rely on perimeter, gateway, and/or front end systems to implement ZT controls.

On the other hand, many OT support and control systems (Purdue Level 3 and up), such as historians, HMIs, PACS, and EACMS, are built on platforms that allow for on-device deployment of ZT controls through granular access management via built-in capabilities or through the use of add-ons, such as endpoint security applications.

The Purdue model is useful for understanding concepts like network segmentation and grouping devices based on function and/or criticality. However, since ZT does not base authorization and trust on the physical or network location of devices and systems, an alternate approach to the Purdue model needs to be considered for devices and systems that are not capable of deploying ZT access controls. The ISA/IEC 62443 model of security zones and conduits (see **Figure 4**) offers a more granular approach for identifying appropriate and applicable ZT controls that can be implemented within an ICS/OT environment.



IEC/ISA 62443 Security Zones & Conduits

Figure 4: ICS Network by IEC/ISA 62443 Model

Grouping systems and devices that are on the same level within the Purdue model into different security zones allows for establishing ZT access controls even between peer systems on the same level. Security zones can be defined by facility, location, or subsystem within a facility. For example, a utility can define

each substation as a single security zone or create separate zones within each substation for an approach that parallels establishing NERC CIP electronic security perimeters (see [Figure 5](#)).

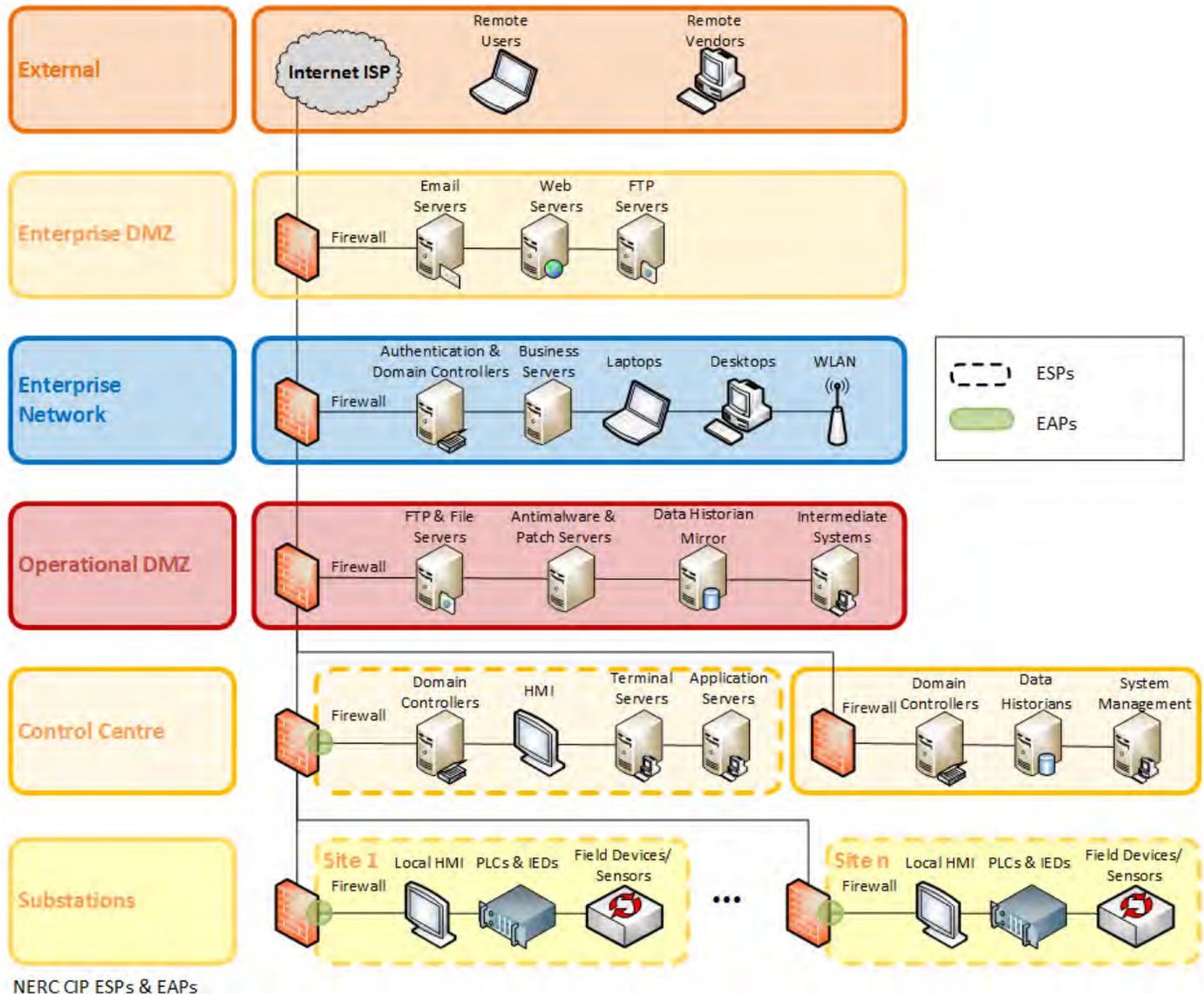
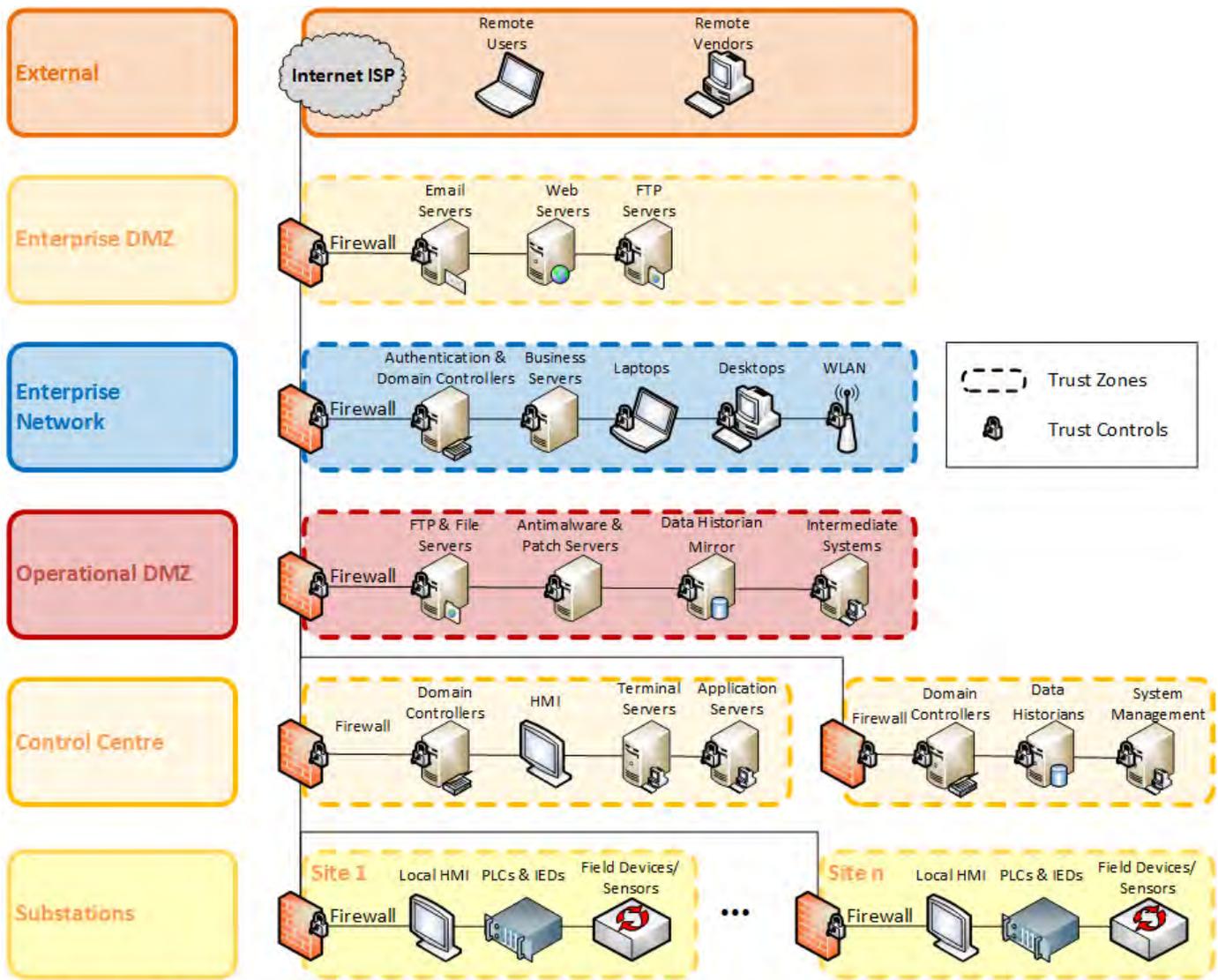


Figure 5: ICS Network by NERC CIP Electronic Security Perimeters

This mixed capability approach ZT can be implemented at a zone level in the areas where the devices within that zone are not capable of implementing host-based security controls (e.g., a substation security zone firewall filtering external inbound/outbound traffic at an application-level) and more granular controls in security zones where the devices are capable of host-based security controls (e.g., a server in the ICS demilitarized zones (DMZ) that filters all connections to the services it hosts). See [Figure 6](#).



Zero Trust Security Zones & Controls

Figure 6: ICS Network by Trust Zones

In light of these mixed capability environments and other factors, there is no “one size fits all” approach that can be put forward to implement ZT across an organization’s entire OT/ICS environment. Rather, the components of ZTA need to be separated and applied where they are capable of being deployed. The ability and extent to which ZTA components can be deployed must be assessed on a per site, facility, and subsystem basis. However, assets planned for the future are alleviated of some of these constraints, and ZTA should be part of the design and planning phases moving forward.

Another important consideration when implementing ZT is exception and failure handling. In most IT environments, it is safe and appropriate to block access (fail-closed) when authentication and authorization cannot be definitively established. In an OT/ICS environment, ZT cannot be deployed in a fail-closed implementation for every subsystem or resource. There are always critical subsystems and resources that

have to fail-open and be able to communicate and coordinate, otherwise the system itself may fail or cease to function, and/or lead to cyber-physical impacts, including the potential for loss of life.

Practical Use-Case for OT/ICS

While the need to secure the bulk power system's critical infrastructure is greater than ever before, and the paradigm shift to ZT is the obvious direction for the future of cyber security, there is still a clear need to approach the use case of ZTA for electric OT systems with caution and careful analysis. Additionally, smaller utilities must be wary of advancing too quickly into the cutting edge and taking on too great an administrative or technological burden without appropriately evolving their governance processes and support staff needed to achieve ZT maturity. Below, the practical use-case for electric OT is explored through benefits, challenges, and recommendations.

Benefits

- Reduced threat surface and associated risk reduction
- Maximized use of authentication
- Increased visibility into all user activity
- The ability to dynamically provide access based on real time assessments
- Reduce an attacker's ability to move laterally within your organization
- Limit possibility for data exfiltration
- Protection against both internal and external threats
- Lowered reliance on point solutions designed to detect/stop specific types of threat activity
- Improved overall security posture

Challenges

- Early adopters may face challenges with the lack of standardization.
- ZT focuses on preventative controls rather than detective controls. Improperly implemented preventative controls could pose additional operational risks for electric OT systems. Comprehensive testing is required including scenarios for handling false positives.
- Diversity of vendor technology offerings may lead to an incomplete approach which may create control gaps.
- Legacy devices may have incompatibility with ZT solutions using agent/server implementations, SSL certificates, or secure protocols.
- Teleprotection low latency requirements may place constraints on viable ZT security solutions.
- There are increased administrative and technical burdens.
- ZT models rely on strictly defined permissions within policies. People, roles, locations, and hardware assets may change, so ZT policies require upkeep and maintenance to be effective.

Recommendations

- Develop or improve cyber security governance when addressing remediation efforts identified in cyber vulnerability assessments, risk assessments, incident response activities, or other internal assessments by taking advantage of these opportunities to advance organizational ZT maturity
- Prioritize establishing an OT cyber security program or improving existing programs
- Perform a cyber risk assessment of electric OT systems
- Take an asset inventory, or validate existing inventories
- Perform a comprehensive controls assessment of the electric OT systems to identify ZT control improvement opportunities.
- Develop a ZT roadmap in order to transition to a ZTA (utilize existing models like CISA's ZT maturity model)
- Within the roadmap, define maturity transition steps for OT (independently from IT if necessary)

Implementation Effort

For OT/ICS environments, implementing ZT is an evolutionary process that requires coordination between multiple business units and disciplines. Utilities have multiple groups that hold responsibility for different areas and components of their OT/ICS environment, such as field operations, substations, control centers, engineering, and IT and security. Leadership buy-in and direction is critical to these undertakings.

Making changes to site network infrastructure as well as access management processes and controls may likely only be feasible when a facility is new, is undergoing major upgrades, or during large scheduled maintenance outages and must be carefully planned, deployed, and validated to help ensure no negative impact to operations. Because of this, it will likely take years with careful planning and full support from all operational areas and leadership to implement ZT in stages across an organization's entire OT/ICS environment. Some legacy systems and facilities may not be feasibly updateable to ZTA, and cyber security programs will need to account for the risk posed by these facilities by implementing less robust compensating controls.

For many organizations, the first steps in staging and applying ZT in OT/ICSs will follow after implementing ZT in their IT environments and then most probably targeting the IT/OT DMZs and operational control centers. These areas typically utilize more modern and flexible digital platforms with multipurpose commodity operating system-based servers and workstations as well as advanced network infrastructures that undergo more frequent refresh cycles and upgrades. These comparatively abbreviated refresh cycles allow for more opportunities to move toward ZTA and are more likely to provide full-scale redundancy to mitigate unforeseen negative impacts of a staged ZTA rollout. Deploying ZT within the IT/OT DMZs and control centers also provides the best cost/benefit return as it addresses a majority of the concerning attack surface and threat landscape.

As previously discussed, due to the large range of OT/ICS system device capabilities and associated limitations, it may not be realistic to consider a device level data source approach for implementing ZT

beyond the DMZs and control centers. Instead, an organization may need to consider an entire facility or subsystem (substation, local HMI, SPS/RAS) as a single data source for deploying ZT measures and controls.

However, advances in technology and enhanced industry needs in the face of evolving and sophisticated cyber threats means OT equipment manufacturers are increasingly offering more robust cyber security capabilities in their product lines that will help facilitate industry wide movement to systems designed with and capable of ZTA. These more modern systems include authentication and cryptographic mechanisms, among other things, and are less of a technical challenge to implement. Entities should consider these newer technology offerings when creating their ZT roadmaps.

Compliance Consideration

General Approach

Entities must maintain their current compliance programs and responsibilities regardless of adopting any new cyber security controls and associated architectures, such as ZT. Consideration of proposed implementations must be evaluated against applicable CIP standards as would any change to the environments subject to CIP jurisdiction.

Identity and Access Management

With ZT controls, processing an authorization request for system access may be enhanced to include additional evaluation criteria, such as device security posture, time-based behavioral data, and current organizational risk. But these are in addition to system privileges or permissions pre-mapped to roles, groups, or other identity criteria of accounts that form a strong basis of any authorization control. An organization's processes that govern baseline system privileges or permissions are designed with business justification, and they follow role-based access control (RBAC) per best practices and are likely best suited as evidence for the control objectives associated to electronic access authorization.

Authentication

Some ZTAs may utilize a service gateway to intercept all incoming requests for resource (system or data) access and present the point of authentication at that gateway. In the design of these ZTA solutions, the same CIP compliance considerations must be given to the new technological components as is given to existing applicable systems, such as Electronic Access Control & Monitoring Systems and BES Cyber Assets.

Software Defined Networking

Organizations should carefully consider how to align dynamic policy-based software defined networking (SDN) with CIP's use of logical network access and defined ESP's. When employing ZT policies with SDN, both the network location of individual systems and allowed inbound or outbound communication at network boundaries access control lists can be dynamic. The policy rules established at the SDN controller may offer criteria to redirect or disable communication (causing dynamic update to ACL's) as well as relocate or quarantine systems (causing VLAN change). However, there is often a resulting "base state" of configuration for the network through these policies, and then a "deviation state" due a higher state of security or reliability need. As a single system example, SDN policy may result in an assignment of a virtual desktop to a particular VLAN. It may then deviate from that assignment when an additional policy-based

evaluation identifies that the workstation is missing recent security patches. This moves the system out of its base state assigned VLAN within an Electronic Security Perimeter and into a deviation state quarantine VLAN (likely a DMZ, potentially outside the ESP) that only allows the necessary ACL-restricted communication to serve security patching services. To aid in evidencing requirements for ESP’s and inbound/outbound communication, it is recommended to orient written control processes to maintain CIP compliance around the use of SDN’s policies by clearly explaining base state versus deviation states. Such efforts require collaboration and input from subject matter experts within the organization, including compliance, security, and network engineers.

Zero Trust Controls Guidance

Among the types of controls making up ZTA, some are more suited than others for deployment across electric OT and IT-centric systems. **Table 1** provides general guidance on control compatibility for various environments. Furthermore, design guidance is provided for common ZT controls.

Table 1: Control Compatibility			
	Control Center & OT DMZ	Substations	Generation DCS
Network Segmentation and Software Defined Networks	++	++	++
Application Layer (Deep Packet Inspection) Gateways	++	+	+
Secure Remote Access	++	+	+
Secure Protocols	++	X	X
Endpoint Protection	++	X	X
Enhanced Identity Access Management	++	+	+

Legend: ++: Multiple/widely supported options; granular device-specific controls can be implemented

+: Limited/complex options, dependent on system-specific architecture; likely only system/site/network level controls can be implemented

X: Very limited, if any, options, dependent on system-specific architecture; May not be feasible to deploy controls (cost/benefit, operational impacts)

Network Segmentation and Software Defined Networks

Network segmentation allows entities to limit attack surfaces and prevent lateral network movement of attackers. It is a critical component and an early maturity step for ZT roadmaps. SDN allows organizations to create network segmentation faster and easier through automatic configuration of firewalls, switches, and routers. It offers more agile and flexible approaches to isolate or segment both VLANs and applications than traditional tools through the use of policy-based configuration and security to establish least trust. The following are aspects of SDN and network segmentation as part of successful ZTA implementations:

- Establish security zones with application layer inspection gateways between zones
- Micro-segmentation of group related workloads or resources for the purpose of establishing granular VLANs
- Separate management traffic from operational traffic even within single facility/site
- Use secure logical overlay networks to establish SDN and build software defined perimeters
- Provides means to implement ZT for devices not capable of deploying on-device security
- Network Access Controls—Provides conditional network access upon policy-based security assessment of end point device configurations and/or behaviors

Application Layer (Deep Packet) Inspection Gateways

A variety of devices are capable of traffic monitoring or control, contributing to ZT maturity by inspecting network packets up to the application layer. These devices work hand-in-hand with network segmentation and SDNs. Different solutions may be deployed either internally or at the perimeter of networks. Some may include additional features enabling network and data flow mapping, asset and configuration inventories, and intrusion detection or intrusion prevention capabilities. Examples of these technologies and their feature sets include the following:

Next Generation Firewalls

- Deployed at perimeters (north/south traffic) or internally if software-based (east/west traffic) to establish security zones
- Application-level access control for inbound/outbound traffic
- Malicious code detection
- Support for OT protocols—provides packet-level ability to allow/deny protocol-specific messages
- SSL decryption for packet inspection

Data-diodes

- Deployed at perimeters or internally
- Enforcement of one-way communications for strict data flow control

Passive Security Monitoring

- Ability to monitor OT/ICS traffic protocols, flows, and time analysis attributes providing insights into normal network conditions and detection of anomalous conditions
- Support for OT protocols—provides packet-level ability to recognize protocol-specific messages

Secure Remote Access

Secure remote access includes solutions that provide access to applications and services that utilize connection brokering, encryption, and intermediate systems. Depending on individual solution capabilities, additional features may include trustless policy-based identity and access management to grant conditional access. Examples of secure remote access solutions include service gateways and terminal servers with virtual application delivery or virtual desktop availability deployed at a network perimeter within a secure DMZ. Other features may include the following:

- Support for multifactor authentication and single sign-on
- Session policy controls: re-authentications and session timeouts
- Session monitoring and enhanced logging
- Data loss prevention
- Bandwidth control
- Inline malware prevention

Secure Protocols–YES

An important aspect of integrating security into an entity's technology footprint with an emphasis on least trust is to standardize use of secure protocols over legacy and unsecure protocols. It is crucial that industry continues to push their original equipment manufacturers to support and build in functionality for leading protocol innovations. Likewise, it is the responsibility of entities to ensure that the selection and procurement of new technology prioritizes compatibility with the newest protocols. Furthermore, it must be ensured that implementation and configuration includes architecting the ability to turn on or switch to an updated protocol later when all integrations and endpoints are fully compatible. If this designed-in approach is not taken, it is much more likely that a legacy/unsecure protocol will continue to be utilized due to the inconvenience and technological burden of change. Finally, it should be noted that intermediate technology such as port servers, proxies, or gateways may be necessary to facilitate secure protocol use in OT networks due to the presence of legacy devices. Below are examples of secure protocols being evaluated for use in the electricity OT field:

- mTLS
- IPSEC
- DNP3-SA v5/v6
- IEC62351

Endpoint Protection

Endpoint Protection solutions include endpoint detection and response with signature based and heuristic analysis to continuously monitor, detect, and respond to cyber threats (like ransomware and malware) as well as active intrusions by threat actors. Other solutions specialize in detection through configuration baseline monitoring of file integrity, software, services, and logical network ports. Additional features may include the following:

- Policy-based application whitelisting
- Host based software firewalls
- Endpoint security auditing
- Domain and URL web filtering

Enhanced Identity and Access Management

The concept of least privilege is not new, but it is brought forth with renewed vigor in the paradigm shift of a ZT controls philosophy where the achievement of the “least” is examined in greater detail. Therefore, identity and access management under a ZT maturity roadmap seek to provide technology solutions to further scrutinize the how, what, and when for authorization, authentication, and access to applications and data. Newer technologies incorporate sophisticated policy based intelligence to support both RBAC or attribute-based access control (ABAC) strategies while enabling risk-based decisions, such as raising authentication from single factor to multi factor and granting reduced privilege to a resource. For example, instead of outright success or deny of access, dynamic access may be granted while locking out some features, specific categories of data, or simply reducing privileges to read-only over full edit/full control.

The implementation between ABAC and RBAC are significantly different with more complexity and automated control being delivered with ABAC and easier implementation but less granular controls with RBAC. Both are well worth exploring for implementation to support ZT practices. Additionally, entities may consider requiring out of band approval for system management access. This is a best practice implementation to remediate the ability of an attacker to approve elevated system access on a node they have successfully infiltrated. The out of band approval process restricts request and access granting to systems and networks that are not accessible by the grantor systems and networks.

Conclusion

The traditional secure perimeter defense model for cyber security is no longer sufficient to address cyber security threats faced by critical infrastructure, such as the electric sector. ZT is a paradigm shift towards an enhanced and capable cyber security plan. Security policy enforcement becomes data-centric—what data requires protection—instead of network-centric or device-centric. The emphasis is on entity identity and context over location within a perimeter. Research and testing must be completed to successfully transition with minimal disruption.

Industry also needs to continue to develop equipment and software capable of delivering on ZT principles. Advanced applications (e.g., real time contingency applications) and support applications (e.g., historians) offer likely paths for testing of implementations of ZT controls. Engineering access to equipment also offers a possible avenue to enable and test these concepts. Entities can collaborate and assist one another through memberships in various organizational groups. Government can provide tax incentives for infrastructure investments, grants for industry organizations promoting cyber security, and funding to assist less capable smaller entities with the process of moving to a more defensible electric infrastructure.

ZT implementation requires attention, focus, and planning. Stakeholder buy-in and executive support at the highest levels are essential for success. Developing a ZT environment in the OT space will take time and deliberate action. Some organizations have not started, some already have an existing network infrastructure in place that can accommodate ZT, and some may have already begun the transition to ZT. Regardless of where an entity is currently, all organizations should take the necessary steps to assess the value of ZT to their IT and OT security programs in support of BPS infrastructure and develop a roadmap to mature technology and controls towards ZTA with an emphasis on realistic time lines and resources to move themselves forward on the maturity scale. A well thought out implementation process will allow an organization to incorporate ZT incrementally where appropriate within new designs. It is crucial for the industry to take these steps of maturity to ensure resilience of the BPS against cyber threats and protect the critical function of providing secure and reliable electricity.

Appendix A References and Resources

Control Design

- [NIST SP 800-207 - Zero Trust Architecture](#)
- [NSA - Segment Networks and Deploy Application-Aware Defenses](#)
- [NIST SP 800-162 - Guide to Attribute Based Access Control \(ABAC\) Definition and Considerations](#)

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

White Paper: Zero Trust for Electric OT

Brian Burnett, SITES Chair

Marc Child, RSTC Sponsor

Reliability and Security Technical Committee Meeting

December 6, 2022 | St. Paul, MN

RELIABILITY | RESILIENCE | SECURITY



The paper informs on zero trust (ZT) concepts and provides considerations and recommendations regarding the adoption of ZT controls in operational technology (OT) and industrial control system (ICS) environments. The paper leverages CISA's Zero Trust Maturity Model for varying levels of implementation by registered entities and recommends entities develop their own roadmap for security and technology maturation. Finally, the paper describes considerations regarding ZT adoption by registered entities and the NERC Critical Infrastructure Protection (CIP) standards.

- Drivers

- Innovation leading to increased connectivity into critical electric OT networks, including monitoring, data transference, and remote access to substations and generation facilities
- Proliferation of available technology solutions advertised under the ZT umbrella by vendors, including penetration into the OT market space
- Paradigm shift within the cyber security industry for trust zones or “castle mentality” to be replaced or enhanced with boundary less, trustless based security controls to keep up with the increasing danger of cyber threats

- This white paper serves to:
 - Educate on ZT fundamental concepts, viable controls for electric OT, and benefits/challenges of implementation for electric OT
 - Recommend entities develop a technological roadmap and follow a ZT maturity model
 - Provide compliance considerations for registered entities
 - Provoke additional thought leadership on ZT in the electric sector

SITES requests the RTSC provide comments on this whitepaper

A stylized map of North America, including the United States, Canada, and Mexico. The map is rendered in shades of blue and grey. A horizontal blue band with a gradient from dark to light blue passes behind the map, serving as a background for the title text.

Questions and Answers

BCSI in the Cloud Tabletop Exercise (Technical Reference)

Action

RSTC Request for Comments

Summary

The BCSI in the Cloud TTX Technical Reference is a document package. The files are meant to go together to capture the experiences of the tabletop exercise and to show some examples of the types of information exchanged. File contents:

1. "20221012 BCSI In the Cloud TTX Generic Process Document User Guide v5.1 bs2.docx" is the generic process document outlining how to prepare and execute a tabletop exercise. This document is meant to be revised and improved as more entities use it and gain experience
2. "20221012 BCSI Cloud Technical Reference v4.2 bs2 DRAFT.docx" contains the key takeaways and experiences of the exercise. These experiences were used to make the current version of the generic process document.
3. BCSI Cloud Storage Exercise_08182022_v3 Final.pdf outlines the key takeaways from the ERO, WECC, and MRO standpoint (all participated in the tabletop exercise)
4. RSAW CIP-004-6_2015_v1 BCSI in Cloud Generic v3.docx is a generic RSAW example for CIP-004-6 used for the exercise
5. RSAW CIP-011-2_ BCSI in Cloud Generic.DOCX is a generic RSAW example for CIP-011-2 used for the exercise

This package is not considered compliance guidance or guidelines, but instead a technical reference that industry and the ERO might find useful to prepare their own tabletop exercises to test their particular cloud environments. This is the first attempt at this process with the primary objective of learning for all involved parties, including the cloud service provider. Our intended strategy is to encourage other entities to utilize the process and document their experiences so the process can be further improved, and a library of experiences can be developed over time for each iteration.

We are asking the RSTC to review the document set and comment. Note that the document "BCSI Cloud Storage Exercise_08182022_v3 Final.pdf" is an ERO-owned document and does not require RSTC endorsement. However, the ERO has indicated it will entertain comments on this document.

Technical Reference

BCSI in the Cloud Tabletop Exercise Version: DATE

Primary Interest Groups

- Balancing Authority (BA)
- Distribution Provider (DP)
- Generator Operator (GOP)
- Generator Owner (GO)
- Reliability Coordinator (RC)
- Transmission Operator (TOP)
- Transmission Owner (TO)

This document is designed to convey experiences learned from the NERC Security Working Group and ERO Enterprise BCSI tabletop exercise. It is not intended to establish new requirements under NERC’s Reliability Standards, modify the requirements in any existing reliability standards, or provide an Interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other legitimate ways to fulfill the obligations of the requirements that are not expressed within this supporting document. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC’s Reliability Standard.

Contents

Primary Interest Groups	1
Introduction.....	2
Tabletop Exercise Strategy	3
Create and Test a Consistent Process for Evaluating a Cloud Environment.....	3
Use the Tabletop Process to Learn.....	3
Technical Reference Deliverables	4
Process Participants	4
Initial Tabletop Exercise	4
Time and Resources (Estimated).....	4
Tabletop Exercise	5
Responsible Entity Tabletop using Microsoft Azure	5

Scope 5

Summary Experience Gained 5

Preparation for Tabletop Exercise..... 6

Reliability Standard Audit Worksheets (RSAWS) 7

Roles and Responsibilities 8

Evidence 8

 General Evidence Takeaways 8

 Detail of Evidence Provided and Associated Discussion: 9

FedRAMP Certification for Public Agency Cloud Environments 12

Tools and Technology 13

Process..... 13

Other Key Takeaways 13

Appendix A: Relationship Between Deliverable Documents 15

Appendix B: Table of Evidence Cross-Reference..... 16

Document Maintenance..... 19

Introduction

Industry interest in adopting commercially available cloud environments continues to increase substantially. [FERC’s Notice of Inquiry \(NOI\)](#) sought comments regarding the potential benefits and risks associated with the use of virtualization and cloud computing services in association with bulk electric system operations, as well as whether barriers exist in the Commission-approved Critical Infrastructure Protection Reliability Standards that impede the voluntary adoption of virtualization or cloud computing services.

Compliance Enforcement Authorities (CEA) and entities are challenged by how to evaluate and audit security controls for BES Cyber System Information (BCSI) stored in a cloud service provider (CSP) off premise environment, where a responsible entity or CEA does not have physical access to the BCSI storage system at a CSP’s data centers and cloud service provider personnel potentially have logical access to such data.

On a more basic level, more information is needed for responsible entities, regional RE’s, the ERO, and FERC about how to prepare for an audit of an information protection program that includes repositories in a cloud environment.

The following efforts and work products are related to virtualization and cloud computing (specifically around BCSI and not BES operations):

- NERC Standards Project 2016-02: Virtualization ([here](#))
CIP V5 Transition Advisory Group (V5 TAG) White Paper ([here](#))
- NERC Standards Project 2019-02: BCSI Access Management ([here](#)):
- NERC Compliance Monitoring and Enforcement Program (CMEP) Practice Guide: BES Cyber System Information ([here](#))
- NERC Security Guideline: Supply Chain Risks Related to Cloud Service Providers ([here](#))
- NERC Security Guideline: Primer for Cloud Solutions and Encrypting BCSI ([here](#))
- FERC NOI on Virtualization and Cloud Computing Services ([here](#))
Comments on FERC NOI on Virtualization and Cloud Computing Services ([here](#))

This purpose in this Lesson Learned document is to continue in these efforts and create an awareness of the considerations made and ensure controls are commensurate with the risks.

Tabletop Exercise Strategy

There is a lack of practical experience implementing, monitoring, and demonstrating compliance with the current NERC CIP Standards for BCSI cloud-based storage. Recognizing the myriad of ways a cloud environment can be implemented and managed using a consistent process to validate and/or test controls for BCSI in a cloud environment is imperative to ensuring the confidentiality of BCSI in a CSP environment.

Create and Test a Consistent Process for Evaluating a Cloud Environment

The first part of the strategy is to provide a consistent process for evaluating the compliance of a particular cloud environment. The NERC Security Working Group (SWG) developed an initial process document for performing a tabletop exercise that mimics actual audit conditions. As more tabletops are performed, the process itself can be optimized for efficient use. The process is vendor agnostic. The process document itself is managed by the NERC SWG and will be updated on a regular basis. This Technical Reference document represents the first tabletop exercise performed using the SWG process document.

Use the Tabletop Process to Learn

The second part of the strategy is for a responsible entity (including its CSP) and the ERO Enterprise to use the process for a particular cloud implementation (IaaS, PaaS, SaaS), and pass on the experience to the industry. Over time, a knowledgebase is developed, and common best practices will emerge for both the ERO and industry. Essentially, the process becomes repeatable and educates the ERO and industry about potentially successful approaches for meeting security objectives for NERC CIP Standards applicable in the cloud environments and successfully managing cloud-centric risks. Tabletop exercises should also produce a more accurate picture of how the audit process will realistically work, similar to a mock audit, which exercises processes such as interviews as well as the examination of the compliance evidence itself.

Technical Reference Deliverables

The process document address what the Technical Reference package will contain, e.g. the updated process document, categories of evidence provided, key auditor and/or risk management questions, etc. Driven by the process document, the deliverable packages will provide consistent information from exercise to exercise. **Use of the process and/or the deliverables provided by the process does not guarantee demonstration of compliance for any particular entity.**

[Appendix A](#) shows the relationship between the 4 documents in the deliverable package. The charts help simplify the navigation steps as package is read, with the arrows showing the suggested order to read the documents based on starting with the results or starting with the process.

[Appendix B](#) is a table showing a detailed cross-reference of evidence, standards/requirements, and description which maps into the ERO Enterprise document [\[NEED TO LINK HERE\]](#) Slide 24 evidence list. The ERO Enterprise document [\[Link to document for Q&A\]](#) also references to this Appendix B.

Process Participants

The process calls for the CSP, responsible entity, and the ERO Enterprise to participate so all three organizations can learn from all perspectives and ensure a more effective audit and value for other CMEP activities involving cloud environments.

Initial Tabletop Exercise

This exercise provided a review of BCSI in a CSP environment for the participating responsible entity, ERO and CSPs seeking to serve the electric sector. The exercise created the following value:

- Providing NERC and industry with possible security controls available for responsible entities storing BCSI at non-entity locations, e.g. the CSP data center
- Experience to develop guidance and audit approaches for responsible entities considering storage of BCSI in a CSP environment. The current standards do not specifically address BCSI in CSP environments and the NERC Reliability Standards under development could leverage the experiences from this exercise.
- Providing industry and the ERO with considerations for interpretation of existing NERC CIP standards and what security considerations may be required in the future
- Allowing the participating responsible entity to collaborate with the ERO Enterprise and CSP to establish a “test” audit scenario for cloud storage of BCSI
- Provided the ERO Enterprise a “live” display of what controls can be utilized to protect cloud hosted BCSI as well as what evidence artifacts could demonstrate meeting and exceeding an audit
- Helps industry to address shared responsibly model issues between entities and cloud providers
- Provided context with the [NERC ERO Enterprise CMEP Practice Guide for BES Cyber System Information](#).

Time and Resources (Estimated)

1. Total participants in the 4-hour exercise: 22 people
 - a. 3 from Microsoft

- b. 14 from the responsible entity
 - c. 5 from the ERO Enterprise, including NERC, WECC, and MRO
 - d. NOTE: Not all participants were needed for the entire 4 hours from the responsible entity
2. Hours of effort for preparation activities for the responsible entity: 48 hours
 - a. About 4 of those hours were shared between the responsible entity and MS. MS had their documentation already prepared.
 3. Hours of effort for follow-up activities for the responsible entity: 40 hours
 4. Total data request questions (after action activity): 20
 5. Number of evidence files produced: 75
 6. This exercise was Version 1.0. The intent behind the Technical Reference deliverables is to reduce preparation time for the responsible entity, the CSP, and ERO Enterprise by not having to produce the process and Technical Reference documents from scratch. The more the tabletop process is exercised, the more can be learned from it and efficiencies can be gained through better preparation, better questions/answers, and better understanding

Tabletop Exercise

Responsible Entity Tabletop using Microsoft Azure

In May 2020, a tabletop exercise was conducted for BCSI in the Cloud as part of an activity coordinated with the NERC SWG. The Microsoft Azure environment is secured using the [Federal Risk and Authorization Management Program \(FedRAMP\)](#) framework in a “commercial high” environment. The entity manages the encryption keys within the environment using a “customer lockbox” solution.

Scope

Scope of the exercise included:

- CIP-004-6 R1 Part 1.1, R2 (all Parts)
- CIP-004-6 R4 Parts 4.1, 4.4, R5 Parts 5.1, 5.3
- CIP-011-2 R1 (all Parts)

Summary Experience Gained

While further detailed below, here is a summary list of the key Experiences from this exercise.

1. CSP documentation was found valuable by ERO to help understand the cloud environment and to supplement the responsible entity’s compliance documentation.

2. As a first of a kind, proof of concept, CSP engagement was essential for the development of RSAW narratives, documentation of environment and security controls, data request responses, etc. (This should not be expected nor needed for regular CMEP engagements.)
3. The responsible entity, ERO Enterprise, and the CSP all use different terminology to describe certain functionality and environments. The responsible entity needs to take extra care to make sure the CSP understands what certain terms mean in the CIP context.
 - a. For example, logs produced from the cloud analytics may not look like what an auditor may expect, necessitating extra explanation, highlighting, and perhaps justification.
 - b. Another example is that the CSP may call backups an application rather than a function.
4. Expect a deep dive on the following items:
 - a. Methods used to protect BCSI in storage (at rest), in transit and use
 - b. Encryption key management
 - c. Access control, particularly as it relates to CSP personnel
 - d. Active Directory(ies), including updating and synchronization
 - e. Security control considerations not called out by the CIP standards (e.g. data sovereignty, services, etc.)
 - f. How unauthorized access to BCSI is prevented after cloud services are terminated.
 - g. Any CSP certifications that are relevant to the controls/protections being applied to secure the responsible entity's BCSI, including how those controls/protections are monitored, audited, etc.
5. It is recommended that the responsible entity update their Information Protection Program (CIP-011 R1.2), Cyber Security Awareness (CIP-004 R1) and CIP Training (CIP-004 R2) materials to address nuances specific to cloud services/environment
6. A schematic or compilation of the environment will be needed for the auditor to understand the environment.
7. These topics need further exploration with the ERO to come to a conclusion:
 - a. whether "use" of data for computing is the same as "use" of BCSI (per CIP-011-2 R1.2). (Note: page 3 of the approved RSTC Security Guideline on this topic it states "Data in use refers to data that is being used or modified by an end-user.")
 - b. whether documentation related to any relevant CSP certification and associated controls could be utilized to provide direct evidence of compliance with the applicable NERC CIP requirements.

Preparation for Tabletop Exercise

1. The process document in Appendix A provides for preparation timelines and tasks. Early communication with the CSP is critical for establishing and ensuring objectives are understood from the beginning.
2. Consider using a test environment with test, draft, or example data to minimize any potential compliance issues. The responsible entity, ERO Enterprise, and CSP should evaluate and assess all relevant aspects and have complete comfort to look at any aspect of the test environment. All evidence provided should be marked as "draft", "unofficial", "example", etc. if based on actual compliance evidence.

3. The test environment should have all controls in place, including monitoring, logging, and policies that identify issues and prevent misconfiguration.
4. If using a copy of production information, recommend obfuscating/masking data such that no sensitive information is disclosed.
5. Using test documents based on operational documents, such as “draft” versions of policies, plans, and procedures is useful because it makes adoption of changes (if needed) easier to operational documents.
6. Scheduling ERO Enterprise and CSP resources may be challenging— schedule ahead of time.
7. Prepare RSAWs for the requirements relevant to the tabletop exercise only. This exercise did not utilize the NERC Evidence Request Tool (ERT). Use of the ERT may be a consideration for future exercises.
8. When preparing RSAWs, share them with the CSP early on and work to add their information that may be relevant to the narrative.
9. Preparation of filesharing was critical. Training was performed on the tools for the external (ERO Enterprise/CSP) participants for the file access part of the exercise.
10. Internal review of the submitted documentation was done as if for a mock or actual audit. This prevented low-quality evidence from being submitted.
11. Following the preparation steps in Appendix A assured the exercise itself took only about 4 hours.
12. Non-Disclosure agreements (NDAs) were signed where necessary—do not leave out this important step. Some CSPs may need this to proceed with the exercise.
13. ERO Enterprise participants should pick a “lead” for questions ahead of the exercise. This can be handled on the pre-meeting 7 days in advance according to Appendix A of the process document.
14. Be prepared to answer both compliance questions as well as risk-based questions you may have to answer for a self-report with a risk engineer.

Reliability Standard Audit Worksheets (RSAWS)

1. Generally, narratives were limited to relevance to the tabletop. An overview of the responsible entity’s overall access management program was included since it also manages access to BCSI.
2. Given this is the first exercise using this process, the CSP also provided narratives and evidence as to what they do for access control and protection of data for the “underlay” of the cloud environment. Feedback from the ERO Enterprise indicated this was useful information for understanding but wasn’t central to their evaluation. The recommendation is to consider including CSP documentation separately listed out by requirement unless it is directly applicable to answering the question in the RSAW.
3. The responsible entity used the regional-specific version of the RSAW, but this is no longer required.
4. Responsible entity and CSP narratives were separate in the RSAW. For example:

Entity Response

[Entity narrative]

CSP Response

[CSP narrative]

This keeps editing to a minimum and ensures the ERO clearly understand which party is providing the narrative.

5. The responsible entity does not edit any of the CSP narratives or evidence. Both are provided “as-is”. This prevents versioning problems and makes overall management of the RSAW preparation easier.

Roles and Responsibilities

1. The responsible entity led the process for organizing the implementing the tabletop exercise. A single point of contact should be established to manage tasks and be a communication hub. This also include after-action reports, follow-ups, and closing out the activity.
2. Use the Teams table in the process document to assign roles and responsibilities. The responsible entity will also need to assign internal roles and responsibilities as they would in a regular audit and ensure the appropriate departments are participating. Internal departments to consider beyond compliance are process owners, cloud implementation team, system administrators, administrative support (for notetaking and data requests), cyber security, and the IT compliance team.
3. Ensure the CSP stays engaged in the process. This was successful in this exercise and the CSP was able to clarify certain aspects about the environment, contract, and processes. The CSP may need to learn how a NERC audit is conducted.

Evidence

General Evidence Takeaways

1. Where possible, the Registered Entity’s identification of the relevant Standard and Requirement is indicated at the beginning of each heading.
2. All evidence was labeled via watermark as “Draft”, “Example” or other label indicating it was for the exercise. Information potentially classified as BCSI was labeled as BCSI as well. All evidence was treated as BCSI regardless of labelling.
3. The responsible entity used evidence it determined relevant to the cloud, such as example reports of access authorizations to the environment.
4. All documents were highlighted to show the entities controls implemented relevant to their SaaS environment to minimize the ERO searching the documents. (Evidence Formatting)

Detail of Evidence Provided and Associated Discussion:

1. Access Control Program Documentation
2. Cloud Service(s) Procurement Documentation: The ERO will read the contracts provided. Ensure relevant contract sections are highlighted. Referenced documents in the contract should also be provided and highlighted, e.g. a reference to a subscriber agreement. Below are the specific documents provided for this exercise:
 - a. Responsible entity procurement agreement from the responsible entity showing what Azure product was purchased and shows the executed procurement (e.g. dated signatures). This was examined to ensure the contract was properly executed meeting entity/vendor legal requirements and when it became effective.

[This link describes the different contract types and terms listed below.](#)

- b. [MS Online Services DPA \(Data Protection Addendum\)](#)
 - c. [Microsoft Online subscription agreement](#)
 - d. [Microsoft Online Services Terms](#)
3. CIP-004-6 R4-R5: Expect detailed questions about logical access control into the environment, for example:
 - a. How the responsible entity controls access, including timely removal of access. This will include a technical discussion if directory services are used, and what happens if certain parts of the access control system fail. Evidence from the technical system will need to be provided (e.g. system-generated logs).

Recommend having an example showing how the environment is isolated to allow only trusted networks.
 - b. Expect a thorough examination of how the CSP controls access to the responsible entity tenant “overlay” and data (“customer data”), including process, procedures, and contract requirements. Evidence may be requested, so know how to address that. Responsible entities should perform prior preparation with the CSP. For this exercise, the CSP provided procedures and contract language about how customer data is protected from CSP system and application administrators access unless specifically authorized by the customer, and only for a fixed period of time. The CSP procedures should address technical controls to prevent unauthorized access.
 - i. This examination includes understanding how access is controlled between tenants, subscriptions, and other partitions found in the cloud environment.

- c. The ERO Enterprise asked for a list of services authorized into the cloud environment in order to understand the different applications and/or services that may have access to the environment. For this exercise, the test environment was isolated in that it did not have a network share, server, or any other delivery system in front of it. The CSP may need certain services for the environment itself to function, namely for security monitoring, logging, and analytics. Ensure these are included and how changes to those services are controlled. Are they authorized by the Responsible Entity?
 - d. Be prepared to show that the list of responsible entity authorized users matches the list of cloud environment authorized users.
 - i. The responsible entity should also ensure a subject matter expert can demonstrate user roles to show the users identity flows from the directory services (e.g. Active Directory, OpenLDAP), if used. If single sign-on (SSO) is used, prepare for a technical discussion about policies and procedures on how it is to be used from a Responsible Entity user standpoint.
 - ii. Prepare for a discussion of management groups and how those work to ensure the principle of least-permission.
 - e. Ensure that all administrative accounts needed to manage the cloud environment itself are included in the access control program, including shared accounts and those that exist only on the “CSP side.”
 - f. In this exercise, the responsible entity had detailed discussions showing what happens when a user is authorized for cloud access in the responsible entity’s access control system and how that information passes to the cloud environment. The responsible entity worked with the ERO Enterprise to identify adequate evidence to show process either succeeding or failing. The reason for this discussion was to show how a gap between the cloud access control and Responsible Entity access control systems is minimized for access granting and removal.
4. CIP-004-6 R4-R5 and CIP-011-2 R1.2 (Evidence presentation): Evidence in the Azure environment consisted of a set of pre-configured policy templates that set certain monitoring, logging, access controls, and replication settings. A suggested improvement is to have an Excel report showing all the detailed settings of the environment. The policy templates were also necessary to show compliance with the policies via the available tools and dynamic compliance reports.
- a. Most of this evidence for the exercise was screenshots of settings from web pages. The ERO Enterprise participants indicated this was not their preferred method of presenting evidence artifacts.
 - b. Expect to show that the policy is specifically applied to the test environment though a demonstration, screenshot, report, or log.
5. Cloud Security Model and Certification(s): If using a CSP environment that is covered by a certification (in this case FedRAMP), expect to discuss how the certification relates to the

applicable CIP requirements, whether there are any 3rd party verification of those associated controls, and how the responsible entity maintains awareness of the certification status (including any findings/mitigations from a 3rd party audit). The objective is to ensure the Responsible Entity:

- a. understands each party's responsibilities under the shared responsibility model,
- b. has implemented what it is responsible for under that shared responsibility model, and
- c. knows how to reassess its security posture if/when the certification is revoked or there are findings from 3rd party audits.

Also be prepared to provide assurance the environment has the stated certification. This can be done online or with provided reports from the CSP.

6. CIP-011-2 R1.2: Be ready for a deep technical discussion of methods used to ensure the confidentiality of data-at-rest (i.e. encryption). Be able to explain how the encryption works and who controls the keys. In this exercise, the responsible entity controls the keys, and demonstrated the tool used to rotate the keys. The responsible entity also showed logs produced when the keys are rotated, created, or removed. The CSP may need to be involved in this conversation depending on the technical process.
 - a. Be prepared to discuss the scope the keys are applied to, e.g. the entire subscription, a certain tenant or environment.
7. CIP-011-2 R1.2: A technical discussion of data transmission (in-transit) is likely. Ensure an SME can show what version of encryption is being used for data in transit, e.g. TLS v1.2.
8. CIP-011-2 R1.2: For this exercise, the Responsible Entity had a requirement in their information protection program that all data be kept within the continental United States. As a result, the ERO Enterprise asked how geo-replication of the test environment (replication between different geographical locations) was performed. Evidence included a list of the policies that prevent selection of replication locations outside the continental United States, including the actual technical policy definition and a screenshot of the replication set-up process showing that a violation of the policy will fail to deploy.
9. CIP-011 R1.2: Be prepared to demonstrate how unauthorized access to BCSI is explicitly prevented when a CSP subscription is terminated. Demonstrating the ability to delete BCSI in the environment, drop all encryption keys, or deleting the container itself would likely be required to ensure access to BCSI following termination of CSP subscription has been precluded.
 - a. Recommendation is to ensure that encryption keys are dropped and the BCSI container is deleted prior to disassociation, along with the documentation the deletion was completed successfully.
 - b. For this exercise, the CSP also keeps backups 90 days after subscription termination. Be prepared to discuss assurance the CSP cannot access the content of the backup copy.
 - c. Responsible entity also provided Microsoft procedures for canceling the Azure subscription, data management, and data access management. These were available online from Microsoft. Have similar documents available from your CSP.

10. Draft list of identified BCSI repositories within the Azure environment (CIP-011-2 R1.1)
11. Draft registered entity-specific Information Classification Policy and Procedures document that includes: (CIP-011-2 R1)
 - a. Requirement to geo-replicate and data residency only in the continental USA
 - b. Definition of “Automated Information Processing System”, a defined term used in WAPA-specific policies, modified to include the cloud service providers approved by the responsible entity.
 - c. Physical storage procedure requires FedRAMP CSP environments of medium or higher (as the Responsible Entity is a federal agency).
 - d. Requirement for electronic storage that keys must be controlled by the responsible entity in a cloud environment for this particular tabletop scenario, with annual key rotation at a minimum and on an as-needed basis.
12. A draft document describing the responsible entity’s overall cybersecurity awareness program. (CIP-004-6 R1 and R2 Part 2.1.5). For the exercise the Responsible Entity supplied the information to show awareness performed for handling of BCSI information includes BCSI within a cloud environment.
 - a. Includes examples of various cyber-awareness publications that address cloud-related cybersecurity issues
13. Example of changes to the responsible entity’s annual cyber security training slides showing cloud-specific information: (CIP-004-6 R2)
 - a. Definition of “cloud computing”
 - i. A suggestion from the ERO Enterprise was to ensure to point out that a cloud environment is external to the responsible entity.
 - b. Slide about requirements for local administrator accounts updated to include cloud management accounts
 - c. Updated list of approved systems designated for storing BCSI includes MS Azure. This includes an updated description of access-control system roles that include Microsoft Azure.
 - d. *Note there is no requirement to specifically address cloud-specific BCSI handling procedures.* Given this was the first iteration of this exercise, draft training/awareness was included in the scope for completeness. Other exercises may not find this is necessary to put this in scope.
14. CIP Exceptional Circumstances document updated to include critical connectivity to or availability of cloud-based services containing BES Cyber System Information repositories under the “Imminent failure of hardware, software, or equipment” section. (CIP-004-6 R2.2, R4.1)

FedRAMP Certification for Public Agency Cloud Environments

Extensive conversations took place about FedRAMP, which is required for this registered entity as a public agency, and how it provides assurance of the security posture for the CSP's "underlay" infrastructure. The auditors want to know how the responsible entity controls access into their tenant "overlay" and to BCSI within that environment. (CIP-004-6 R4, R5 and CIP-011-2 R1.2)

This is a new concept for CMEP activities and no specific conclusions were reached during the exercise as to the extent that FedRAMP certification could be used to provide direct evidence of compliance. The responsible entity is planning on continuing that discussion with the ERO Enterprise and CSP.

Tools and Technology

Process

1. The overall tabletop process was considered a success by the participants. Suggested improvements:
 - a. Begin with the CIP-004 access control program discussion. This allows the ERO Enterprise to understand the responsible entity's access control program.
 - b. Preparation effort is what kept the tabletop exercise to the planned 4 hours. Those steps have been incorporated into the latest version of the process document. Keeping to the established timetable also assured maximum time efficiency, which is an objective of the tabletop process.
 - c. The responsible entity needs to keep in contact with the ERO Enterprise participants and the CSP, as after-action activities such as data requests may require some added communication.
 - d. Have a notetaker present as well as someone to handle data requests. Also encourage all participants to take their own notes, with the intention of sharing them with the team. This captures perspectives from all participants.
 - e. Make sure to include introductions at the beginning of the exercise. This helped verbal communication immensely. On WebEx, also make sure, if possible, that participant's names and organization are shown, e.g. "John Smith, ABC Utility".
 - f. The ERO Enterprise needed to have offline conversations after the exercise to determine what additional questions to ask, and to determine generally how the evidence might meet compliance requirements and make recommendations on evidence clarity and quality.

Other Key Takeaways

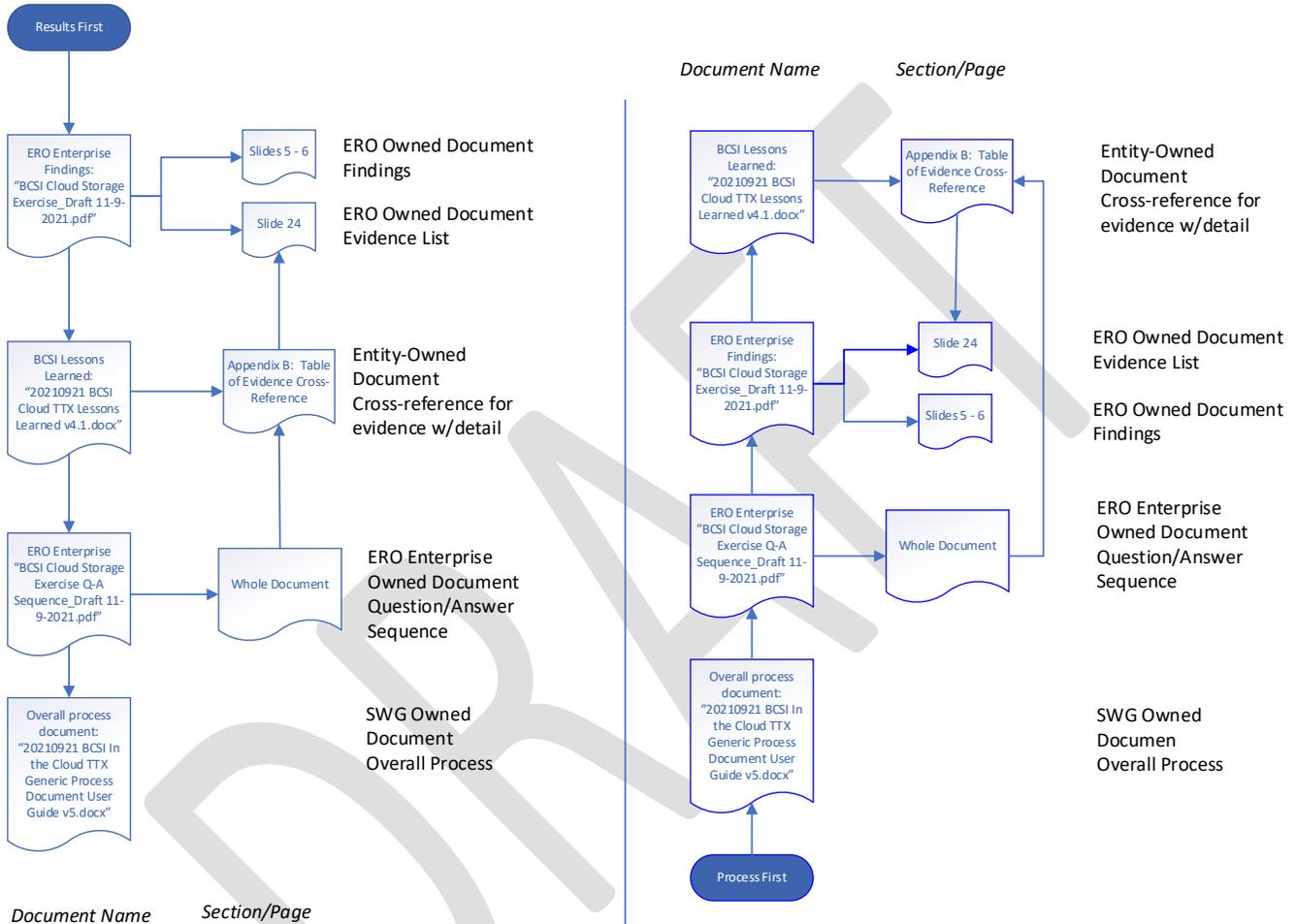
1. As the responsible entity, be able to explain why the CSP is trusted by your organization, and how you maintain that trust. Examples include certifications, risk evaluation during the procurement process, etc. Some organizations have a formal authority to operate process that could be used to answer these questions.

2. Do not assume the auditor has expert experience for every aspect of cloud computing. The tabletop exercise value is to educate the ERO Enterprise and CSP as well as the responsible entity. Extra effort is needed to make sure that participants understand the questions being asked and understand the answers being given. If not, take the time to get that understanding while the participants are assembled.
3. This initial set of deliverables took longer than planned to assemble, review, and release. A future improvement to the process should be to put timeline objectives for the after-action activities to decrease this part of the process.

DRAFT

Appendix A: Relationship Between Deliverable Documents

Use this diagram to follow the relationship between the documents of the deliverable package. The arrows indicate how to read through the documents. The approach on the left is looking with the results first. The approach on the right is looking at the process first.



Appendix B: Table of Evidence Cross-Reference

This table maps documents to the evidence list maintained by the ERO team. “Not used” means the data was asked for but not used beyond review by the ERO. It is a placeholder to keep the file references consistent.

Reference Number	Name	Standard	Req	Description
1	CSP Business Agreement	N/A	N/A	Business Agreement. Included in CIP-004-6 R1.1 as part of overall security model
2	Isolation Choices	CIP-004-6	R4-R5	Tenant isolation and access control between tenants
3	HTTPS	CIP-011-2	R1.2	Shows HTTPS connectivity and encryption qualities (data in transit)
4	Customer Managed Keys	CIP-004-6	R4-R5	Screenshot showing settings for customer-managed encryption keys
5	Not Used	N/A	N/A	Not Used
6	Access solution	CIP-004-6	R4-R5	Describes Microsoft "Just In Time" access control process in context of Microsoft support staff having access to the tenant
7	Not Used	N/A	N/A	Not Used
8	Business Agreement Order	N/A	N/A	Purchase Order showing purchase of cloud environment was executed (a valid agreement)
9	RE RFI-1	CIP-004-6 / CIP-011-2		Entity response to ERO Enterprise RFI-1. Responses include topics relevant to both CIP-004 and CIP-011, and covered both audit and self-report scenarios
10	Network Isolation Example	CIP-004-6	R4	Screenshot of settings demonstrating customer environment is containerized and isolated from other tenant environments.
11	TLS Policy 1	CIP-011-2	R1.2	Screenshot of technical policy forcing TLS version for data in transit
12	TLS Policy Shown	CIP-011-2	R1.2	Screenshot showing technical policy setting for TLS meets automated compliance check

13	Location Policy Detail	CIP-011-2	R1.2	Screenshot showing technical policy setting demonstrating that data centers that support this Azure service are known and controlled by the entity.
14	Geo-Replication Policy	CIP-011-2	R1.2	Screenshot showing technical policy controlling geo-replication is enabled and active. Used with #13 to demonstrate that data centers that support this Azure service are known and controlled by the entity.
15	Encryption Fundamentals	CIP-011-2	R1.2	Document from Microsoft used as an extra reference to further explain how Microsoft accomplishes encryption for data at rest.
16	Key Vault Config	CIP-004-6	R4-R5	Document from Microsoft describing how the Key Vault product securely stores secrets and keys
17	AD Config	CIP-004-6	R4-R5	Entity document with details on how Active Directory is configured via federation services
18	AD Config 2	CIP-004-6	R4-R5	Screenshots showing AD Federated services are enabled, AD account synchronized from entity on-prem domain controllers only, and AD groups replicated to Azure from entity only. Also some technical explanation of how removals from the entity on-prem AD controllers would work.
19	AD Sync	CIP-004-6	R4-R5	Screenshot showing details of AD sync status and AD federation settings
20	Subscription Cancellation	CIP-004-6	R4, R5.3	Microsoft document with procedure for canceling the subscription, used to understand how CSP access to BCSI is prevented by the entity information protection program following termination of services.

21	Trusted Services	CIP-004-6	R4, R5.3	Microsoft procedure for configuration of storage firewalls and virtual networks, used to understand how CSP access to BCSI is prevented by the entity information protection program following termination of services.
22	Data Management	CIP-004-6	R4, R5.3	Microsoft document explaining data retention and data deletion on physical storage devices, used to understand how CSP access to BCSI is prevented by the entity information protection program following termination of services.
23	Data Access Management	CIP-004-6	R4, R5.3	Microsoft document describing who can access entity data and on what terms. Includes descriptions of operational processes governing customer data, how access is limited, and how "subprocessor" access to customer data is managed. Used to understand how CSP access to BCSI is prevented by the entity information protection program following termination of services.
24	RE RFI-2	CIP-004-6 / CIP-011-2	Multiple	Entity response to ERO Enterprise RFI-2. Responses include topics relevant to both CIP-004 and CIP-011, and covered both audit and self-report scenarios.
25	BCSI designated storage memo	CIP-004-6	R4.4	Entity document identifying the designated storage location for BCSI (included cloud location).
26	Create Resource Fail	CIP-011-2	R1.2	Screenshot showing a create resource failure resulting from a geo-location policy enforcement.

Document Maintenance

Version	Date	Who	Notes
1.0	08-August-2022	Sessions	Initial version (Draft)

DRAFT

Cloud Implementation Tabletop Exercise User Guide

Version 5.1: August 11, 2022

Overview

The purpose of this exercise is to review and evaluate cloud-based technologies and the ability of an entity to demonstrate compliance with NERC CIP requirements. The scope includes a study of the features and specifications of cloud technologies and potential services that may correlate to applicable requirements of the CIP Reliability Standards. The result of this effort may include the development of implementation guidance, lessons learned, NERC Standard Authorization Requests, or industry white papers.

Assessment Scope

This exercise is limited solely to a review of using cloud technologies to transfer, store, and use NERC defined BCSI and does not review or consider cloud based BCS. Participating Registered Entities may want to consider a cloud provider with which they have an existing relationship or contract, or include a cloud service, or cloud provider which they may be interested in for future services.

The Scenario Being Tested

- Responsible Entity (RE): [RE]
- Cloud Service Provider (CSP): [CSP]
- Cloud Security Framework: [FedRAMP, NIST, another framework]
- Encryption: [Customer Managed | CSP Managed | Other (describe)]
- CSP Service: [IaaS, PaaS, SaaS, etc.]
- Object(s): [Describe the objects being evaluated, e.g., file share, BLOB, etc.]
- Method: Remote document review and interview with sample RSAWs and sample evidence
- 3rd Party Audit Organization (3PAO) (if applicable): [3PAO]
- Compliance Scope
 - CIP-004-6 R1 P1.1, R2 P2.1 – 2.3, R4 P4.1, 4.4, R5 P5.1 – 5.3
 - CIP-011-2 R1 P1.1 – 1.2, R2 P2.1 – 2.2

NOTE: If a participating Registered Entity is currently storing and/or utilizing BCSI in the cloud, and they choose to include the analysis of such in this tabletop exercise, no waiver of compliance will be offered/available.

Team

Role	Description	Individuals
Vendor(s)	Participation with Participants in Tabletop exercise to identify controls, evidence, etc.	[Names, Company]
Auditor(s)	Provide subject matter expertise from auditor and CMEP perspective	[Names, Company]
SWG Member(s)	Provide subject matter expertise from Responsible Entity perspective; Provide overall direction and leadership to the Tabletop; Schedule meetings; Escalate key issues and recommendations on behalf of Tabletop Team.	[Names, Company]
NERC/ERO Rep	Provide subject matter expertise; Support resolution of key issues and recommendations escalated for the Tabletop Team.	[Names, Company]
FERC Rep(s)	Provide subject matter expertise from the FERC perspective	[Names, Company]
[RE] Rep(s)	Functional subject matter experts for implementation Solicit support from their cloud service providers; Work with vendors to identify controls, evidence, etc.; Attend meetings; Escalate issues if necessary.	[Names, Company]

Objectives

- This tabletop exercise provides a framework to develop and improve an assessment process for BCSI in a cloud environment.
- Review evidence to demonstrate compliance with the CIP Standards based on controls implemented by the Responsible Entity and/or [Cloud Security Framework] certification processes. Determine if evidence and controls are sufficient to demonstrate CIP Compliance as they pertain to BCSI requirements in CIP-004-6 and CIP-011-2 specifically.
- Provide Responsible Entities and their cloud services providers with guidance and information regarding the controls and evidence that are necessary to demonstrate compliance with the CIP Reliability Standards.
- Provide experiences about the assessment approach and the way evidence provided for CIP interrelates with NIST-based controls as governed by [Cloud Security Framework].
- Provide experiences about the tabletop process to make future assessments with different scenarios valuable to all stakeholders.
- Note that several tabletop exercises using different scenarios may need to be completed to offer quality guidance.

Phase 1

CIP-011-2 — Cyber Security — Information Protection R1

1. Confirm the Responsible Entity has a method to classify Method(s) to identify information that meets the definition of BES Cyber System Information, including identifying cloud-based repositories.
2. Determine contract-based responsibilities for information classification between [CSP] and [RE].
3. Determine, along with the Responsible Entity's processes and procedures, if existing types of certifications for [Cloud Security Framework] may also be utilized to demonstrate sufficient vendor controls, e.g., NIST controls listing with [Cloud Security Framework] evidence of controls testing for the following:
 - a. Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.
4. Determine and document identified deficiencies

Follow-Up Activities

1. Identify next steps including potential industry deliverables/reporting, additional phases or efforts, and standards revision recommendations
2. Create deliverables such as experiences, if possible, or, if not possible, implementation guidance, if such development of such guidance is possible

3. Develop and implement a communication plan for resulting deliverables and/or provide standards revision recommendations to the standards committee
4. Develop planning team for additional phases

Phase 2

CIP-004-6 – Access Management Program - Granting and Revoking electronic and physical Access to BCSI.

1. Identify the requirements and expectations for Access Management and Access Revocation (Refer to Standard) and the set of data to be collected from both [CSP Service] and [RE] access authorization and access control systems.
2. Identify the evidence required to prove compliance
3. Identify applicable technical controls from both [CSP] and [RE] can apply
4. Determine the process and effort involved for producing evidence between the [RE] and [CSP] for both the access control process and controls evidence

Follow-Up Activities

1. Create experiences, if possible, or, if not possible, implementation guidance, if such development of such guidance is possible
2. Develop a communication plan for resulting deliverables

Phase 3

Assessment of implemented controls between [CSP] and [RE] and Approaches to be Considered: Encryption and [Cloud Security Framework] framework)

1. Determine if existing types of certifications for [Cloud Security Framework] may be utilized to demonstrate sufficient vendor controls, e.g., NIST controls listing with [Cloud Security Framework] evidence of controls testing.
2. Determine how data encryption and key management responsibilities have an effect on demonstrating compliance.
3. Determine if the [3PAO] report provides sufficient evidence to demonstrate BCSI requirements.
4. Map
 - a. Outcomes from [CSP Service] to the identified requirements and controls, where possible. This can be accomplished using the applicable RSAWs.
 - b. Methods, approaches, and policies that were effective in implementing the technical controls of the CIP requirements. These can be addressed in the RSAWs.

- c. Issues that were encountered and how they were resolved or if they were not resolved, e.g., a deficiency was identified.
- d. Where outcomes differed from expectations (i.e., easier or more difficult than expected).
- e. CIP requirements that posed particularly difficult challenges.
- f. What would have been done differently with the benefit of hindsight?
- g. Business or supply chain challenges that were encountered and how they were addressed.
- h. Determine and document identified deficiencies

Follow-Up Activities

1. Identify next steps including potential industry deliverables/reporting, additional phases or efforts, and standards revision recommendations
2. Create deliverables such as experiences, if possible, or, if not possible, implementation guidance, if such development of such guidance is possible
3. Develop and implement a communication plan for resulting deliverables and/or provide standards revision recommendations to the standards committee
4. Develop planning team for additional phases

See [Appendix D](#) for a list of deliverables to be produced and associated ownership responsibilities.

Appendix A Preparation Activities for [RE]

This section is a basic checklist of activities the responsible entity should perform to ensure an effective exercise. Dates are based on experiences from the previous exercises.

60 - 90 Days in Advance

1. Update the BCSI in the Cloud process document (this document) with the correct information and communicate it to the CSP. Ensure the CSP is aligned with the objectives and scope of the tabletop plan.
2. Set up test environment working with the CSP. Determine:
 - a. Type of object to use (e.g., file share, generic information store, etc.)
 - b. Controls that are implemented around the object
 - c. Dashboard reports
 - d. Activity logs and associated reports
 - e. Relevant CSP documentation about the controls, dashboard, reports, and automation supporting the environment. These can include CSP-provided documentation if directly relevant.

45 Days in Advance

3. Determine date, time, and duration of the activity
 - a. *Recommendation: Use a scheduling tool such as Doodle*
4. Recruit exercise team members as outlined in this document
 - a. Contact SWG chair to send out a call for volunteers or use direct contact with your RRO, ERO representatives
 - b. *Recommendation: Ensure you have full contact information for each exercise team member, especially mobile phone*
5. Create a schedule for involved participants and groups (internal and external)
6. Begin assessment of RSAWs and evidence to find gaps (policies, processes, procedures)
7. Ensure remote tools are configured, scheduled, etc. Tools include secure file transfer (Box, Kiteworks, etc.) and remote meeting (Zoom, Webex, etc.).
 - a. Set file transfer tool to allow for viewing but not downloading documentation

30 Days in Advance

8. First internal draft of RSAWs completed, including narratives and evidence
9. Confirm schedules for participants

10. Ensure non-disclosure agreements are in place for the ERO/RRO and CSP
11. Ensure backup plans are in place in the event of network, VPN, or tool failure. *Recommendation: Have a phone conference bridge set up to fall back to.*
12. Pre-tabletop virtual meeting scheduled for external exercise participants (e.g., vendor, ERO, RRO representatives). See Appendix B for sample agenda. Meeting should be scheduled approximately 7 days in advance of the tabletop.
13. Advise internal management of the tabletop activity. *Recommendation: Schedule a senior leader to give a short welcome message to the exercise team at the start of the tabletop.*

14 Days in Advance

14. Final review of RSAWs, narratives, and evidence
 - a. Ensure internal stakeholders are aware of the documentation and are prepared to be asked questions
15. Final availability check for exercise team members

7 Days in Advance

16. RSAWs, narratives, evidence, team members, and CSP environment are set and will not be changed unless there is a technical issue.
17. Files uploaded to file transfer tool so external parties can begin assessment
18. Facilitate pre-tabletop virtual meeting
19. Ensure all team members can access the documentation on the file transfer site **(CRITICAL)**

1 Day in Advance

20. Reach out to external team members to ensure they are set and there are no last-minute problems or issues
21. Email out the backup plans in case of tool or network failure to all team members. (See Appendix C.)

Day of Tabletop

22. Allow at least two hours of time prior to the activities for last-minute troubleshooting and questions
23. Start the remote meeting tool at least 30 minutes in advance.
24. At the start of the tabletop, schedule in 15 minutes to go over the agenda for the day and introduce team members.

Appendix B Agenda for Pre-Tabletop Meeting

1. Review the general schedule for the exercise
2. Review the objectives and expectations of the exercise
3. Discuss confidentiality for [RE] and [CSP]-specific information
4. Ensure everyone can access the information via the file transfer tool
5. Discuss and decide the assessment team tools (e.g., blank RSAW)
6. Feedback desired from the audit team
7. Format and distribution of notes
8. Review of expected output from this exercise (e.g., experiences)
9. Post-tabletop activities review
10. Q&A for the assessment team

DRAFT

Appendix C Example Backup Procedures in the Event of Network/Tool Failure

Condition	Action – [RE]	Action – Outside [RE]	Resources Impacted	Workaround
[RE] VPN Fails	Switch off VPN and rejoin WebEx	None	We will lose access to [CSP] portal and internal [RE] file repository. Delay around 10 minutes while people get reconnected.	We have screenshots of the portal in the RSAW evidence. Meeting host has a local copy of the files in the repository s/he can display on the meeting tool
Meeting host computer audio fails or is wonky	Switch to phone audio	Switch to phone audio	Delay of 5 minutes to get reconnected.	Switch to phone audio
Virtual meeting host has issues	Host will rejoin by phone or computer	None	Host should automatically fall back to another participant to keep the meeting up. No delay.	Alternate hosts will take over facilitating the exercise.
Participant is cut off because of freeze, reboot, ISP dies, etc.	Send meeting host a text at [xxx-xxx-xxxx]	Send host a text at [xxx-xxx-xxxx]	May have to pause until participant returns – will decide on the fly. Probably no delay.	Participant can call in via phone to the meeting.
Secure file transfer server fails/inaccessible	Host will call the appropriate help line	None	Critical impact as Kiteworks is the data repository for this exercise. Significant delay to get restored.	May have to reschedule the exercise if the delay is > 1 hour
Meeting tool fails/inaccessible, total failure except for secure file transfer server	Call into the conference bridge.	Call into the conference bridge.	Loss of screen display, but voice will still work. Delay of probably 10 minutes.	Dial [yyy-yyy-yyyy]. When prompted, dial your conference code (zzzzz) and then hit the pound sign (#). If prompted for your name, say your name and then hit the pound (#) again. Text meeting host if you have issues joining.
100% technological failure	Host to send texts to all participants of the issue	None until contacted	No file transfer server, no conference bridge, no internet, no VPN	Reschedule tabletop

Appendix D Deliverables Package

The following deliverables should be produced for experiences. There is an important division of ownership among the different deliverables:

1. **Owner: Responsible Entity**
 - a. Updated Technical Reference document in NERC format
 - i. Recommendations for producing evidence (e.g., cloud tools, reports, format, etc.)
 - ii. Pitfalls or other areas of compliance or security risk identified during the exercise
 - iii. Improvements to the process (preparation, timing, communication, etc.)
 - b. RSAWs with generic types of evidence provided for the relevant requirements
 - c. Non-public internal notes, other material used to create a public version (redacted) of the Technical Reference package
2. **Owner: Cloud Service Provider**
 - a. CSP procedures, business agreements, product and service descriptions, general cloud security model
 - b. Ensure to communicate with the CSP to determine what appropriate information to put into the experiences or Technical Reference document
3. **Owner: Security Working Group**
 - a. Updated process document considering feedback from the Responsible Entity
 - b. Reviewed public version of Technical Reference package from the Responsible Entity
4. **Owner: ERO Enterprise (NERC).**
 - a. List of possible risk areas as perceived by the ERO, CSP, or the responsible entity (includes compliance, cyber security, or other category) and potential mitigations.

Each owner is responsible for maintaining, reviewing, and editing its own portion of the Technical Reference package. This simplifies ongoing management. The final public version of the Technical Reference document should have weblinks to the other owners' documentation to make it easy to assemble the complete set of information.

Tips and Tricks

1. The after-action activities, such as the Technical Reference document and the associated deliverables package, should be reviewed by the ERO Enterprise, CSP, and internally by the responsible entity to minimize the chance of confidential information being released.
2. This tabletop exercise was envisioned to be a virtual activity. All tools were provided by the organizing responsible entity. Tools used:
 - a. A secure file-transfer server that allowed file viewing but not downloading by external participants.
 - (1) Verification of access and functionality was performed prior to the tabletop according to the process document Appendix A.
 - (2) Auditing was turned on to monitor ERO Enterprise activity and validate proper functionality of login, access, etc.
 - b. WebEx for pre-meetings and the tabletop itself. Video was enabled when practical. Sharing of documents or live demonstrations on the screen were performed when required.
 - c. A telephone conference bridge for a back-up to the Webex.
 - d. Doodle.com for determining the best time to schedule the activity
 - e. Training for the secure file server was performed and could be enhanced in the future. Recommendation is to ensure everyone knows how to navigate the secure file server and view documents.

Document Maintenance

Version	Date	Who	Notes
1.0	1/30/2020	Martin	Initial version
2.0	6/1/2020	Sessions	New template, added Appendices, added recommendations from 5/21/2020 initial tabletop
3.0	3/17/2021	Sessions	Review and added Appendix D
4.0	9/21/2021	Sessions	Updated after SWG and ERO teams reviews

DRAFT

Reliability Standard Audit Worksheet¹

CIP-004-6 – Cyber Security – Personnel & Training

This section to be completed by the Compliance Enforcement Authority.

Audit ID: Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity: Registered name of entity being audited
NCR Number: NCRnnnnn
Compliance Enforcement Authority: Region or NERC performing audit
Compliance Assessment Date(s)²: Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method: [On-site Audit | Off-site Audit | Spot Check]
Names of Auditors: Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X	X				X			X	X		
R2	X	X	X	X	X				X			X	X		
R3	X	X	X	X	X				X			X	X		
R4	X	X	X	X	X				X			X	X		
R5	X	X	X	X	X				X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

¹ NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC’s and the Regional Entities’ assessment of a registered entity’s compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC’s Reliability Standards can be found on NERC’s website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity’s adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

² Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
P1.1			
R2			
P2.1			
P2.2			
P2.3			
R3			
P3.1			
P3.2			
P3.3			
P3.4			
P3.5			
R4			
P4.1			
P4.2			
P4.3			
P4.4			
R5			
P5.1			
P5.2			
P5.3			
P5.4			
P5.5			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-004-6 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: <ul style="list-style-type: none">• direct communications (for example, e-mails, memos, computer-based training); or• indirect communications (for example, posters, intranet, or brochures); or• management support and reinforcement (for example, presentations or meetings).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

NOTE: RE elected to put general contract description in this section for the tabletop exercise because there was no other place to put it. This might not normally need to go here in an actual audit.

RE has an active subscription with Microsoft Azure. The conditions of the subscription agreement, including customer (RE) vs. Cloud Provider (Microsoft) responsibilities are outlined in [Online Subscription Document] and [Microsoft Online Document].

The Cloud Service Provider (CSP) does not have logical, physical access to RE High and Medium Impact BES Cyber Systems and associated EACMS, PACS and PCAs.

RE provides security awareness training to its employees and vendors at least once every calendar quarter to reinforce cyber security practices for personnel with authorized electronic access to cloud-based and on-premises resources.

RE reinforces Security Awareness as explained "RE Cyber Security Awareness Program Document", by providing one or more of the following:

- Quarterly email to all RE employees and contractors containing security awareness information
- Quarterly articles on RE internal web site

Examples of awareness are in the evidence file list below.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

--

Compliance Assessment Approach Specific to CIP-004-6, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which include security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.
	Verify the Responsible Entity has reinforced security awareness at least once each calendar quarter.
	Verify the security awareness reinforcement included: <ul style="list-style-type: none">• reinforcement of cyber security practices, or• reinforcement of physical security practices associated with cyber security.
	Verify that security awareness was reinforced for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.
Note to Auditor: The Responsible Entity is not required to document that each quarter’s reinforcement was received by each of its authorized personnel. Rather, the Responsible Entity is required to demonstrate that the security awareness reinforcement was communicated to its authorized personnel as a whole, not necessarily individually.	

Auditor Notes:

R2 Supporting Evidence and Documentation

- R2.** Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]
- M2.** Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

R2 Part 2.1

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Training content on:</p> <ol style="list-style-type: none"> 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity’s incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media. 	<p>Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.</p>

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

The Cloud Service Provider (CSP) does not have logical, physical access to RE High and Medium Impact BES Cyber Systems and associated EACMS, PACS and PCAs.

The RE Cyber Security Awareness Program, “[Program Document]” addresses cyber security training topics required under requirement 2, part 2.1.5.

All RE employees are required to participate in cyber security training regardless of role, function or responsibilities as explained in “[Program Document]”. The Critical Infrastructure Protection Training training can be found in the powerpoint

presentation [Presentation] and includes content on how to handle BCSI and its storage.

RE trains system administrators who design and manage a CSP environment. Training includes controls that are controls related to shared touch points in the Azure authorization boundary and any customer applications leveraging Azure infrastructure. [Link to Azure Operational Security best practices Document].

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	<p>Verify that the training program(s) collectively include content on the following:</p> <ol style="list-style-type: none"> 1. Cyber security policies; 2. Physical access controls; 3. Electronic access controls; 4. The visitor control program; 5. Handling of BES Cyber System Information and its storage; 6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 7. Recovery plans for BES Cyber Systems; 8. Response to Cyber Security Incidents; and 9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.
	<p>Verify the Responsible Entity's training program's content is appropriate to individual roles, functions, or responsibilities.</p>
Notes to Auditor:	

1. The training program(s) must collectively include all nine training elements.
2. It is not necessary that all nine training elements be included for the training of each role, function, or responsibility.
3. Each role, function, or responsibility must receive training on all appropriate training elements.

Auditor Notes:

R2 Part 2.2

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

The Cloud Service Provider (CSP) does not have logical, physical access to RE High and Medium Impact BES Cyber Systems and associated EACMS, PACS and PCAs.

The RE access management program “[Program Document]” explains the onboarding workflow and modify access workflow. For both on-boarding or access modification activities, the workflow, supported in the RE Access Control System, checks to see if the individual is being granted access to CIP assets and, if true, requires the training validation and PRA date validation prior to initiating access authorization tasks. Section xxx discusses the processes for requiring completion of Cyber Security training.

RE during the audit period has not declared a CIP Exceptional Circumstance. In the event a condition occurs requiring RE to declare a CIP Exceptional Circumstance, RE follows guidance documented in “[Document]”.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

--

Compliance Assessment Approach Specific to CIP-004-6, R2, Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify all personnel completed the training specified in Part 2.1 prior to being granted authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

R2 Part 2.3

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.3	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> • EACMS; and • PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

The Cloud Service Provider (CSP) does not have logical, physical access to RE High and Medium Impact BES Cyber Systems and associated EACMS, PACS and PCAs.

The RE Cyber Security Awareness Program “[Program Document]” addresses R2 Part 2.3. “[Non-Completion Report]” is a sample report showing what employees have not completed the training. Follow-up actions to ensure completion include reminders sent to managers and supervisors prior to the mandatory completion date as shown in “[Example1]”. If training is not completed within required timeframes, access is removed.

RE requires all employees to participate in its annual cyber security training program utilizing online training and testing program. [Program Document] discusses the processes for requiring completion of Cyber Security Training.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify all personnel with authorized electronic access or authorized unescorted physical access to applicable Cyber Assets completed the training specified in Part 2.1 at least once every 15 calendar months.
--	---

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

R3 Part 3.1

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to confirm identity.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

A PRA for information access is not required under CIP-004-6.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

NERC Reliability Standard Audit Worksheet

Audit ID: Audit ID if available; or NCRnnnnn-YYYYMMDD

RSAW Version: RSAW_CIP-004-6_2015_v1 Revision Date: May 8, 2015 RSAW Template: RSAW2014R1.3

Compliance Assessment Approach Specific to CIP-004-6, R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include a process to confirm identity.
	Verify a process to confirm identity was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

Auditor Notes:

R3 Part 3.2

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:</p> <ol style="list-style-type: none"> 3.2.1 current residence, regardless of duration; and 3.2.2 other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. <p>If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.</p>	<p>An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to perform a seven year criminal history records check.</p>

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Please see response to P3.1.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6, R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include a process to perform a seven year criminal history records check that includes: <ol style="list-style-type: none">1. current residence, regardless of duration;2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more; and3. performing as much of the seven year criminal history records check as possible, if it is not possible to perform a full seven year criminal history records check.
	Verify a process to perform a seven year criminal history records check was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to applicable Cyber Systems and: <ul style="list-style-type: none">• A full seven year criminal history records check was completed; or• A full seven year criminal history records check was not completed, the Responsible Entity completed as much of the seven year criminal history records check as possible, and documented the reason the full seven year criminal history records check was not completed.

Auditor Notes:

R3 Part 3.3

CIP-004-6 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process to evaluate criminal history records checks.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Please see response to P3.1.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6, R3, Part 3.3

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include criteria or a process to evaluate criminal history records checks for authorizing access.
	Verify the applicable criteria or process to evaluate criminal history records checks for authorizing

access was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

Auditor Notes:

R3 Part 3.4

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.4	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s criteria or process for verifying contractors or service vendors personnel risk assessments.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Please see response to P3.1.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6, R3, Part 3.4

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include criteria or a process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.
	Verify the criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3 was implemented.

Auditor Notes:

R3 Part 3.5

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.5	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Please see response to P3.1.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6, R3, Part 3.5

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include a process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.
	For personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems, verify the applicable personnel risk assessment process was implemented at least once every seven years.

Auditor Notes:

R4 Supporting Evidence and Documentation

- R4.** Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].
- M4.** Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

R4 Part 4.1

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:</p> <ol style="list-style-type: none"> 4.1.1 Electronic access; 4.1.2 Unescorted physical access into a Physical Security Perimeter; and 4.1.3 Access to designated storage locations, whether physical or electronic, for BES Cyber System Information. 	<p>An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.</p>

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Except during a CIP exceptional circumstance described in “[Program Document]”, RE demonstrates authorization based on need using automated workflows in the RE application. The process for approving physical, informational or logical access entitlements are explained in “[Access Program Document]”.

Authorization occurs in three separate workflows in RE, and one in Microsoft:

1. The Onboard workflow requires the individual supervisors’ approval before an individual can be on boarded.
2. The Role authorization workflow is found in the document XYZ. This contains two separate approval requirements, entitlement owner(s) must approve the access and the Role Owner must approve the need.
3. The Modify/Extend Access process requires the individual supervisors’ approval as well as the entitlement owners approval before an individual’s access can be modified. The Supervisors’ approval can be found on page X of the workflow diagram the entitlement owner’s approvals can be found on page Y of the workflow diagram.

4. Authorization for access under CIP Exceptional Circumstances for MS Azure follows the Azure “Just In Time” access process shown in “[JIT Process Doc]” (also available at Link). Even in these circumstances, the RE storage area is encrypted using the RE key which would prevent access to any storage content. All items residing in the BCSI repository are encrypted with the RE key which can be rotated on demand.

To manage and authorize access to the AZURE BCSI repository RE created two parent roles “AZURE - BCSI Repository” and “Cloud Services Encryption Key Manager”. When an access role is created the workflow generates a subset of roles for user assignment; Administrator, Application User, Non Provision Admin, and Shared Accounts. This subset of roles allow users the ability to request access to logical, physical and information access on RE resources.

RE utilizes the workflow engine to authorize access and to provision accounts based on the subset roles an individual is assigned to.

The following files provide the RE roles that are associated with access to the AZURE Cloud based BCSI repository.

File1 – Role for those RE personnel responsible for managing cloud Encryption Keys

File2 – Role for those RE personnel authorized for administration of BCSI repository.

File3 - Role for those RE personnel authorized for using the BCSI repository.

File4 - Role for those RE personnel authorized for managing the BCSI repository without the authority to provision user access.

In the MS Azure environment, access control to the BCSI content is access controlled through encryption of the storage resource using customer-provided (RE) keys. “Screenshot” shows the configuration setting for RE-provided keys. Keys can be rotated on-demand, and on a periodic basis. Keys are stored in a key vault which no one can access except RE authorized personnel.

Additional CSP information (Azure)

Discusses how they control access to customer data.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6, R4, Part 4.1

This section to be completed by the Compliance Enforcement Authority

	<p>Verify the Responsible Entity has documented one or more access management programs which include a process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:</p> <ol style="list-style-type: none">1. Electronic access;2. unescorted physical access into a Physical Security Perimeter; and3. access to designated storage locations, whether physical or electronic, for BES Cyber System Information.
	<p>If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.</p>
	<p>Verify access was authorized, based on need, for:</p> <ol style="list-style-type: none">1. Electronic access;2. unescorted physical access into a Physical Security Perimeter; and3. access to designated storage locations, whether physical or electronic, for BES Cyber System Information.
<p>Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.</p>	

Auditor Notes:

R4 Part 4.2

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.</p>	<p>Examples of evidence may include, but are not limited to:</p> <ul style="list-style-type: none"> • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Quarterly verification for BCSI information stores is not required per 4.2.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

--

Compliance Assessment Approach Specific to CIP-004-6, R4, Part 4.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs which include a process to verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.
	Verify the Responsible Entity has verified at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.

Auditor Notes:

R4 Part 4.3

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.</p>	<p>An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

15 Month electronic access verification for BCSI information stores is not required per 4.3

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6, R4, Part 4.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs that, for electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.
	Verify the Responsible Entity has verified, at least once every 15 calendar months, that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct.
	Verify the Responsible Entity has verified, at least once every 15 calendar months, that user accounts, user account groups, or user role categories, and their specific, associated privileges are those that the Responsible Entity determines are necessary.

Auditor Notes:

R4 Part 4.4

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.4	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.</p>	<p>An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following:</p> <ol style="list-style-type: none"> 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

The RE Access Management Access Program, “[Program Document]” provides governance for the verification of information access for user accounts, user groups, or user role categories and verifies that the specific associated privileges are correct and necessary.

RE reports for the Azure roles are shown in “Report1”, “Report2”, “Report3”, and “Report4”.

The roles present in Azure (they are mapped in Section 12 of “[Program Document]”) can be seen in “Screen Shot”. More detail of an individual user can be seen in “Screen Shot”.

Reports are generated annually to show the reviews are complete, two examples being “[EntitlementReviewReport]” and “[CloudAnnualAccessReport]”. These two examples focus on Azure roles and access.

The list of designated BCSI storage locations are in “[List of storage locations]”.

Additional CSP information (Azure)

By default, Azure personnel do not have access to customer storage accounts, which is controlled by Storage Account Keys generated randomly when the storage account is created or later at customer's request. Access to customer storage accounts is not needed to operate Azure. All customer data in Azure Storage or SQL Database is encrypted by default and this encryption cannot be disabled.

Registered Entity Evidence (**Required**):The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (**This section to be completed by the Compliance Enforcement Authority**):

Compliance Assessment Approach Specific to CIP-004-6, R4, Part 4.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs that verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.
	Verify the Responsible Entity has verified, at least once every 15 calendar months, that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct.
	Verify the Responsible Entity has verified, at least once every 15 calendar months, that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are those that the Responsible Entity determines are necessary for performing assigned work functions.

Auditor Notes:

R5 Supporting Evidence and Documentation

- R5.** Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation*. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].
- M5.** Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R5 Part 5.1

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>A process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

RE utilizes an automated workflow to notify individuals responsible for removing physical or interactive remote access upon a termination action. The RE Access Management Program details the requirements. This applies for physical, logical, or information access. Section X shows the workflows.

Any RE employee can initiate an off boarding action using the off board option in the RE service catalog. The requester must know the employees name and if the off board is voluntary or involuntary. For involuntary requests the system will generate tasking’s to disable badges (physical access), active directory accounts and removal of access for other logical and informational access during the next check run. This check runs in [workflow application] once every hour.

“Sample.pdf” is an example of an off boarding Requested Item in Access Management program for an employee with CIP physical, information and electronic access entitlements. Highlighted TASKS on the example demonstrate access removal to physical, information and electronic CIP entitlements within 24hrs. “Sample2” shows the specific task of access removal. The directory service controls access to the designated BCSI storage locations.

RE [deploys directory service] with Azure to enable users to authenticate using on-premises credentials and access resources in the cloud. If an employee is terminated, access to the Microsoft Azure Portal can be turned off simply by removing that

employee from the on-premises directory service. "Screen Shot" and "Screen Shot 2" show this configuration setting in the Azure environment.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6, R5, Part 5.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs that include a process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).
	Verify the Responsible Entity has: <ol style="list-style-type: none"> initiated removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action; and completed the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).
	Note to Auditor: Removal of the ability for access does not necessarily require removal or disabling of the individual's accounts. The ability for access may be removed by disabling the individual's network access, confiscation of a badge, or other suitable means. Removal of Interactive Remote Access may be accomplished, for example, by disabling the individual's multi-factor authentication.

Auditor Notes:

R5 Part 5.2

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p>	<p>An example of evidence may include, but is not limited to, documentation of all of the following:</p> <ol style="list-style-type: none"> 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

RE utilizes an automated workflow for removing physical or interactive remote access upon a transfer or reassignment action. Section x of the RE Access Management Program, “[Program Doc]”, details the process. The workflow is shown in Section Y.

RE supervisors, contracting officers and contracting officer representatives can request a “Modify, Extend Access Roles” action from the system catalog. The requester can remove or add access roles/entitlements, update user specific data, update an access expiration date of a contract for contract employees, and can enable or disable badge and logical access for individuals placed on extended leave, unscheduled absence, and transfer or reassignment actions.

“Adding Access”, “Sample Removal”, and “Sample Task” show an addition and a removal to a resource (in this case it would be Azure) as part of the process to modify user access in the event of a transfer/reassignment. Access in Azure is applied through directory service groups.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6, R5, Part 5.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for reassignments or transfers to revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.
	Verify the Responsible Entity has, for reassignments or transfers, revoked the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

Note to Auditor:

Revocation of access does not necessarily require removal of the individual’s accounts. The account may be disabled in lieu of removal.

Auditor Notes:

NERC Reliability Standard Audit Worksheet

R5 Part 5.3

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.3	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	For termination actions, revoke the individual’s access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

RE utilizes an automated workflow for removing physical or interactive remote access upon a transfer or reassignment action. Section x of the RE Access Management Program, “[Program Doc]”, details the process. The workflow is shown in Section Y.

RE supervisors, contracting officers and contracting officer representatives can request a “Modify, Extend Access Roles” action from the system catalog. The requester can remove or add access roles/entitlements, update user specific data, update an access expiration date of a contract for contract employees, and can enable or disable badge and logical access for individuals placed on extended leave, unscheduled absence, and transfer or reassignment actions.

“Adding Access”, “Sample Removal”, and “Sample Task” show an addition and a removal to a resource (in this case it would be Azure) as part of the process to modify user access in the event of a transfer/reassignment. Access in Azure is applied through directory service groups.

The list of designated BCSI storage locations are in “List of Repositories”.

NERC Reliability Standard Audit Worksheet

Registered Entity Evidence **(Required)**:

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-004-6, R5, Part 5.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for termination actions to revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5, Part 5.1), by the end of the next calendar day following the effective date of the termination action.
	Verify the Responsible Entity has, for termination actions, revoked the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.

Notes to Auditor:

1. If the access was already revoked under the actions taken for Requirement R5, Part 5.1, no further action is needed.
2. Revocation of access does not necessarily require removal or disabling of the individual's accounts. The ability for access may be removed by disabling the individual's network access, confiscation of a badge, or other suitable means.
3. Removal of Interactive Remote Access may be accomplished, for example, by disabling the individual's multi-factor authentication.

Auditor Notes:

NERC Reliability Standard Audit Worksheet

R5 Part 5.4

CIP-004-6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.4	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> EACMS 	For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

N/A

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-6, R5, Part 5.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for termination
--	---

NERC Reliability Standard Audit Worksheet

	actions to revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.
	Verify the Responsible Entity, for termination actions, has revoked the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.
Note to Auditor: Revocation of access does not necessarily require removal of the individual’s accounts. The account may be disabled in lieu of removal.	

Auditor Notes:

NERC Reliability Standard Audit Worksheet

R5 Part 5.5

CIP-0046 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.5	High Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> EACMS 	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: <ol style="list-style-type: none"> 1. Workflow or sign-off form showing password reset within 30 calendar days of the termination; 2. Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or 3. Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

N/A

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

NERC Reliability Standard Audit Worksheet

Audit ID: Audit ID if available; or NCRnnnnn-YYYYMMDD

RSAW Version: RSAW_CIP-004-6_2015_v1 Revision Date: May 8, 2015 RSAW Template: RSAW2014R1.3

NERC Reliability Standard Audit Worksheet

Compliance Assessment Approach Specific to CIP-004-6, R5, Part 5.5

This section to be completed by the Compliance Enforcement Authority

	<p>Verify the Responsible Entity has documented one or more access revocation programs for termination actions to change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p> <p>The documented process(es) may include provisions for the Responsible Entity to determine and document that extenuating operating circumstances require a longer time period, and may change the password(s) within 10 calendar days following the end of the operating circumstances.</p>
	<p>If extenuating operating circumstances are invoked, verify the circumstances are documented and include a specific end date.</p>
	<p>For termination actions that do not invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 30 calendar days of the termination action.</p>
	<p>For termination actions that invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 10 calendar days following the end of the extenuating operating circumstances.</p>
	<p>For reassignments or transfers that do not invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 30 calendar days of the date that the Responsible Entity determines the individual no longer requires retention of the access.</p>
	<p>For reassignments or transfers that invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 10 calendar days following the end of the extenuating operating circumstances.</p>

Auditor Notes:

NERC Reliability Standard Audit Worksheet

Additional Information:

Reliability Standard

The full text of CIP-004-6 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 706

See FERC Order 791

NERC Reliability Standard Audit Worksheet

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFT1v0	06/17/2014	Posted for Industry Comment	New Document
DRAFT2v0	09/17/2014	CIP RSAW Development Team	Address comments received in response to DRAFT1v0.
DRAFT3v0	12/10/2014	CIP RSAW Development Team	Address comments received in response to DRAFT2v0.
DRAFT4v0	02/06/2015	CIP RSAW Development Team	Address comments from V5R SDT and address comments in response to DRAFT3v0.
DRAFT4v1	03/06/2015	CIP RSAW Development Team	Address comments from V5R SDT meeting on March 3-4, 2015.
FINALv1	05/08/2015	CIP RSAW Development Team	Address comments from final posting; review and address comments of V5R SDT.

Reliability Standard Audit Worksheet¹

CIP-011-2 – Cyber Security – Information Protection

This section to be completed by the Compliance Enforcement Authority.

Audit ID: Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity: Registered name of entity being audited
NCR Number: NCRnnnnn
Compliance Enforcement Authority: Region or NERC performing audit
Compliance Assessment Date(s)²: Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method: [On-site Audit | Off-site Audit | Spot Check]
Names of Auditors: Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X	X				X			X	X		
R2	X	X	X	X	X				X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

¹ NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC’s and the Regional Entities’ assessment of a registered entity’s compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC’s Reliability Standards can be found on NERC’s website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity’s adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

² Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

NERC Reliability Standard Audit Worksheet

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
P1.1			
P1.2			
R2			
P2.1			
P2.2			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

NERC Reliability Standard Audit Worksheet

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)



NERC Reliability Standard Audit Worksheet

R1 Supporting Evidence and Documentation

- R1.** Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
- M1.** Evidence for the information protection program must include the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-011-2 Table R1 – Information Protection			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: <ul style="list-style-type: none"> • Documented method to identify BES Cyber System Information from entity’s information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity’s information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity’s information protection program.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

- Description of responsible entity (RE) program to identify, mark, protect, and control BCSI.
- Flow chart of the information categorization process.
- List of BCSI repositories.

NERC Reliability Standard Audit Worksheet

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document
RE provided docs here					
CSP provided documentation here if applicable.					

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-011-2, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more information protection programs that have method(s) to identify information that meets the definition of BES Cyber System Information.
	Verify the Responsible Entity has implemented the method(s) to identify information that meets the definition of BES Cyber System Information.

Auditor Notes:

NERC Reliability Standard Audit Worksheet

R1 Part 1.2

CIP-011-2 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.</p>	<p>Examples of acceptable evidence include, but are not limited to:</p> <ul style="list-style-type: none"> • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Description of responsible entity (RE) program to identify, mark, protect, and control BCSI.

Flow chart of the information categorization process.

These sections include: sharing BCSI, awareness of surroundings, physical protection, protection over telecommunications circuits, encrypting during transit and at rest, and other requirements for best handling practices.

RE utilizes the following controls for the storage location in Azure:

- Storage location is encrypted at rest
 - Screenshot shows configuration setting
 - Logs show encryption keys can be rotated on demand by RE
- Storage location is encrypted in transmission
 - Screenshot shows encryption enabled for data in transmission
- Storage resource is access controlled
 - Screenshot shows role-based access
 - Screenshot shows directory service controls access
 - List shows user profile with more detail and tie to directory service
 - Please see CIP-004 RSAW for more detail on the RE access control program
- Storage location only replicates to continental US
 - Screenshot shows technical policy is enabled
- Storage location is monitored for activity

NERC Reliability Standard Audit Worksheet

- Screenshot shows the dashboard for monitoring activity
- Storage location is monitored for policy compliance by Azure monitoring services
 - Screenshot shows a dashboard for overall compliance with policies
 - Screenshot shows the detailed policies drill-down from the top-level dashboard. These tools assist RE in detecting changes to the security configuration of its storage location

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-011-2, R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more information protection programs that include procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.
	Verify the Responsible Entity has implemented the procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.

Auditor Notes:

NERC Reliability Standard Audit Worksheet

R2 Supporting Evidence and Documentation

- R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: <ul style="list-style-type: none"> • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

As shown in the previous response to P1.2 (narrative and evidence), the use of encryption for the storage location prevents access to the information by personnel unauthorized by RE, regardless of replication locations and deletion status of the information.

NERC Reliability Standard Audit Worksheet

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-011-2, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media, prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column).
	Verify that prior to the release for reuse of Cyber Assets of Applicable Systems that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity has taken action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.

Auditor Notes:

NERC Reliability Standard Audit Worksheet

R2 Part 2.2

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: <ol style="list-style-type: none"> 1. EACMS; 2. PACS; and 3. PCA 	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: <ul style="list-style-type: none"> • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

As shown in the previous response to P1.2 (narrative and evidence), the use of encryption for the storage location prevents access to the information by personnel unauthorized by RE, regardless of replication locations and deletion status of the information.

Additional CSP information (Azure)

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

NERC Reliability Standard Audit Worksheet

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-011-2, R2, Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media, prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information.
	Verify that, prior to the disposal of Cyber Assets of Applicable Systems that contain BES Cyber System Information, the Responsible Entity has taken action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroyed the data storage media.

Auditor Notes:

NERC Reliability Standard Audit Worksheet

Additional Information:

Reliability Standard

The full text of CIP-011-2 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FER Order 706

See FER Order 791

NERC Reliability Standard Audit Worksheet

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFT1v0	06/17/2014	Posted for Industry Comment	New Document
DRAFT2v0	09/17/2014	CIP RSAW Development Team	Address comments received in response to DRAFT1v0.
DRAFT3v0	12/10/2014	CIP RSAW Development Team	Address comments received in response to DRAFT2v0.
DRAFT4v0	02/06/2015	CIP RSAW Development Team	Address comments from V5R SDT and address comments in response to DRAFT3v0.
DRAFT4v1	03/10/2015	CIP RSAW Development Team	Address comments from V5R SDT meeting on March 3-4, 2015.
FINALv1	05/08/2015	CIP RSAW Development Team	Address comments from final posting; review and address comments of V5R SDT.

DRAFT

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

BCSI Cloud Storage Tabletop Exercise

ERO Enterprise Tabletop Team Members:
Lonnie Ratliff (NERC), Jess Syring (MRO), Morgan King (WECC)
August 18, 2022

RELIABILITY | RESILIENCE | SECURITY



- Limited in scope
 - Reviewed to understand environment, limited depth
 - Exercise ≠ Audit or Self-Report
- Learning experience for all participants

- Vendor-specific
- Entity-specific
- Included audit and security risk perspective
- RSAW limited to CIP-004 and CIP-011

CSP – Storage
Scenario



Invaluable exchange of information between the ERO Enterprise and the [Cloud Vendor].

Other solutions and service models should be evaluated

- Exercise conducted May 20, 2020
 - Industry team led with introduction of RSAWs for CIP-004-6 and CIP-011-2
 - Entity utilized vendor narrative for controls implemented in the CSP underlay environment
 - RSAWs helpful in understanding the qualities/capabilities of the vendor environment
 - Two vendor documents used to guide RSAW development for this exercise:
 - [NERC CIP Standards and Cloud Computing](#) (vendor document)
 - [Cloud Implementation Guide for NERC Audits](#) (vendor document, requires vendor account)
 - ERO Enterprise team notes:
 - RSAWs were underlay-focused, in addition to entity environment-specific.
 - Discussions for entity overlay around CIP-004-6 and CIP-011-2 ensued during the remainder of the exercise.

CIP-004-6	Audit Exercise Observations	Meets Requirement Measure
R2 Part 2.1.5 (Training on BCSI handling)	<ul style="list-style-type: none"> • RSAW (attestation), no vendors identified as having access to applicable to BES cyber system(s) • Vendor employees have applicable training covering all topics (in the event that access is granted to vendor employees) 	
R4 Part 4.1.3 (Access to Designated Storage Location)	<ul style="list-style-type: none"> • RSAW (attestation), no vendors identified as having access • Entity has full control of access. • Issue: Vendor may have the capability to access entity data. Reference - Q&A sequence RFI-1, Q2-4, leading to RFI-2, Q1. 	
R4 Part 4.4 (Verify access)	<ul style="list-style-type: none"> • RSAW (attestation), no vendors identified as having access • Evidence supports access grants are valid (multiple) • [Redact] AccessManagementProgram, p.53, and (Ref-9) vendor personnel do not have access • Issue: Active directory sync characteristics not fully described. Reference - Q&A sequence RFI-1, Q5 leading to observation 	 With Observation
R4 Part 5.3 (Revocation)	<ul style="list-style-type: none"> • RSAW attestation describes methods for revocation if vendor employees had access • Entity shows full control over access with automation capability (did not exercise) 	

CIP-011-2	Audit Exercise Observation	Meets Requirement Measure
R1 Part 1.1 (Methods to identify BCSI)	<ul style="list-style-type: none"> External designated storage location (DSL) identified (Ref. 25) Recommendation: Consider making cloud-specific procedures more explicit, ensuring that DSLs in-cloud are unambiguously identified as in-cloud 	
R1 Part 1.2 (Procedures for BCSI)	<ul style="list-style-type: none"> [Solution] activity log analytics show two users with access (procedural evidence) Recommendation: Consider making cloud-specific procedures more explicit Issue: Deletion of data not demonstrated. See Q&A Sequence RFI-1, Q11, following to RFI-2, Q3 	
R2 Part 2.1	<ul style="list-style-type: none"> N/A in this cloud exercise 	N/A
R2 Part 2.2	<ul style="list-style-type: none"> N/A in this cloud exercise 	N/A

Risk Consideration Categories: BCSI in the Cloud

1. Business Agreements
(Contracts)

2. Access/BCSI in Use

3. Service Model
(Environmental Constraints)

4. Encryption

5. Certifications

6. Data sovereignty

7. Data Transformation

Next slides are paired:

**Risk category general
cloud considerations**

**Cloud exercise
considerations**

4. Encryption	Risk Influence
If meeting or exceeding current NSA/NIST requirements	Reduces ↓
If public vulnerabilities for cipher are known	Increases ↑
CIP equivalent physical protections in place of encryption	Neutral
Encryption absent and no physical protections	Increases ↑

4. Encryption – Exercise Evidence	Risk Influence
HTTPS in use (Ref 3)	Neutral
Encryption keys managed by customer (Ref 4)	Reduces ↓
TLS policy = version 1.2, machine audit success shown (Ref 11, 12)	Neutral
Background on encryption usage, and “always encrypted” reinforces intent (Ref 15, 16)	Neutral

These factors are called risk influencing factors which are understood as “a set of conditions which influence the level of specified risks related to a given activity or system”

1. Business Agreements	Risk Influence	Risk if absent
Governance for vendor access to entity data	Neutral	Increases ↑
Governance for transmittal of vendor access evidence	Reduces ↓	Neutral
Declaration for encryption key management processes	Neutral	Increases ↑
Declaration for entity-specific data disposal methods	Neutral	Increases ↑
Declaration for vendor personnel background verification	Reduces ↓	Neutral
Containerization of entity content	Neutral	Increases ↑
Entity right to audit vendor or to view the details of audit results	Reduces ↓	Neutral
Notifications for access breach	Neutral	Increases ↑
General entity autonomy	Risk linked to autonomy	

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

1. Business Agreements – Exercise Evidence	Risk Influence
Agreement sets obligations (Ref 1, p.3)	Neutral
Customer retains rights to data (Ref 1, p.5)	Neutral
'Will not use' vendor declaration (Ref 1, p.5)	Neutral
'Will not disclose' vendor declaration (Ref 1, p.6)	Neutral
Third-party restrictions on data access (Ref. 1, p.6)	Reduces ↓
Customer right to audit statement (Ref 1, p.8)	Neutral
Notification agreement on access breach (Ref 1, p.8)	Neutral
Notice given for changes to tertiary providers, and tertiary providers must meet or exceed the terms in the business agreement (Ref 1, p.9)	Reduces ↓
Customer will have ability to delete data (Ref 1, p.9)	Neutral
Contract agreement signed and dated (Ref 8, p.1)	Neutral

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Three states of electronic data: At rest, in transit, and in use
What is BCSI in use?

- Consider: *Data that is processed in real-time by a Cyber Asset, and is not at rest or in transit*

2. BCSI in Use	Risk Influence
BCSI enters 'In Use' state within vendor infrastructure	Increases ↑
Access controls for BCSI in use	Neutral
On premise use of cloud technology	Reduces ↓
Encryption of BCSI in use (homomorphic encryption – future technology)	Reduces ↓

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

2. BCSI in Use – Exercise Evidence	Risk Influence
Confidentiality commitment (Ref 1, p.11)	Neutral
Security awareness and training for vendor employees from entity (Ref 1, p.11)	Neutral
Physical access limited to authorized personnel (Ref 1, p.11)	Neutral
Physical media containing customer data tracked (Ref 1, p.11)	Neutral
Access that is granted to vendor admins is tracked (Ref 1, p.11-12)	Neutral
Vendor access credentials automatically expire after time period (Ref 1, p.11)	Neutral
Customer controls access grant to vendor (Ref. 6) (Ref. 9)	Neutral
Trusted vendor services are permitted to access the service account. Issue: Access to backup or other service level accounts. Reference 21, p.14, Ref 21, p.16, RFI-1 Q2-Q4, and RFI-2 Q1.	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Less about:

- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)

There is not much risk difference between the service models. All have the potential access to data by vendors or others.

More about:

- Limiting service provider access through infrastructure architecture
- Service composition (just storage, storage + services, tertiary providers)

3. Service Model	Risk Influence
Tertiary cloud dependencies	Increases ↑

3. Service Model – Exercise Evidence	Risk Influence
Vendor employees do not have access to customer data by default (Ref 1, p.9, Ref 23)	Neutral
Tertiary providers can be identified, will meet or exceed business agreement terms (Ref 1, p.9)	Reduces ↓
Customer right to terminate tertiary providers (Ref 1, p.9)	Reduces ↓
Environment is logically isolated, implemented with VLAN and firewall configurations that are controlled by the customer. (Ref 2, 10)	Neutral
Environment enforces access against a copy of the entity AD, a push architecture from entity to the cloud environment (Ref 17, 18, 19)	Neutral
AD sync timing between customer and vendor was unexplored. The sync mechanism could permit unauthorized access if synchronization controls fail or utilize periodicities longer than permitted for revocation (see Q&A Sequence, RFI-1 Q5)	(Observation)
A full configuration export of the service environment was not available for review (see Q&A Sequence, RFI-1 Q7)	(Observation)

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Encryption is typically required in cloud environment

- Consider [NSA sources](#) and [NIST requirements](#)
- Consider cipher strength: (RSA-xxx, SHA-xxx, AES-xxx)

4. Encryption	Risk Influence
If meeting or exceeding current NSA/NIST requirements	Reduces ↓
If public vulnerabilities for cipher are known	Increases ↑
CIP equivalent physical protections in place of encryption	Neutral
Encryption absent and no physical protections	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

4. Encryption – Exercise Evidence	Risk Influence
HTTPS in use (Ref 3)	Neutral
Encryption keys managed by customer to help prevent unauthorized access (Ref 4)	Reduces ↓
TLS policy = version 1.2, machine audit success shown (Ref 11, 12)	Neutral
Background on encryption usage, and “always encrypted” reinforces intent (Ref 15, 16)	Neutral

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

- Most certifications or accreditations focus on the underlay (including access to the overlay). 3PAOs do not audit the customer data environments.
- Some certifications are objective-based. Be sure to evaluate the certification objective against CIP objectives.

5. Certifications	Risk Influence	Risk if absent
FedRAMP Certification	Neutral	Increases ↑
SOC 1 Not applicable, attestational in nature		
SOC 2 (Type 1 + Type 2) with adequacies under Security, Processing Integrity, and Confidentiality headings	Neutral	Increases ↑
SOC 3 with compliance seal	Neutral	Increases ↑
Other – draw comparisons with known certifications	Neutral	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

5. Certifications – Exercise Evidence	Risk Influence
Per business agreement, vendor follows ISO 27001, ISO 27002, ISO 27018 (Ref 1, p.7)	Neutral
Customer has access to certification reports such as FedRAMP, ISO-x, SOC, and PCI/DSS (Ref 24)	Neutral
Per business agreement, recertification performed annually by a 3PAO (Ref 1, p.8)	Reduces ↓
Latest certification reports unavailable for review due to sensitivity. In an actual audit these reports would be made available to the customer (See Q&A Sequence, RFI-1 Qx leading to RFI-2 Q4).	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

Data Sovereignty: A consideration related to the potential geographic location of the data

6. Data Sovereignty	Risk Influence
Certification or business agreement declaration of US domestic only	Neutral
Certification or business agreement declaration of US or Canada domestic only (Canadian entities)	Neutral
International or undeclared	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

6. Data Sovereignty – Exercise Evidence	Risk Influence
Core services store data at rest in specified geo-locations (Ref 1, p.9)	Neutral
Location policy detail shows entity can technically enforce geo-location of the customer environment according to a list assignment (Ref 13, 14)	Neutral
Configuration parameters show US geo-locations selected for this US-based entity, and no international selections (Ref. 24)	Neutral

Risk Influence Key: **Reduces Risk ↓** / **Increases Risk ↑** / Risk Neutral

7. Data Transformation	Risk Influence
Encryption: A strong but reversible means to protect data	Neutral
Obfuscation: A reversible clear text replacement according to a key. Easy to reverse engineer	Increases ↑
Obfuscation in Real-time communication protocols where efficient data processing is required (typically not BCSI)	Neutral
Redaction: Some electronic redaction formats retain source content	Neutral
Sanitization: Permanent and irreversible transformation of data	Reduces ↓
Access authorizations and training on program and custody controls	Neutral

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

7. Data Transformation – Exercise Evidence	Risk Influence
Vendor contractually commits to deleting entity data, backups, and cached data after customer disassociation with the vendor (Ref 20)	Neutral
Vendor provides steps for customer data deletion prior to service cancellation (Ref 22, p.1)	Neutral
Business agreement suspends customer data for a waiting period following disassociation in which the customer has no access to the data and potentially no remedy once the agreement has terminated (Ref 20)	Increases ↑
Evidence of deletion not demonstrated (See Q&A Sequence RFI-1, Q11-Q12, leading to RFI-2 Q3)	Increases ↑

Risk Influence Key: Reduces Risk ↓ / Increases Risk ↑ / Risk Neutral

In Summary:

Risk Considerations: BCSI in the Cloud	Risk Influence
1. Business agreements (contract agreements)	Neutral
2. Access/data in use	Increases ↑
3. Service model (environmental constraints)	Neutral (More to learn)
4. Encryption (data at rest or in transit)	Neutral
5. Certifications	Increases ↑ (Exercise Stop)
6. Data sovereignty	Neutral
7. Data transformation	Increases ↑

- [ERO Enterprise CMEP Practice Guide](#)
- [2019-02 Project Page](#)
- [CIPC Security Guideline, Cloud Computing](#)
- [Homomorphic encryption](#)
- [Data sovereignty](#)
- [Obfuscation in software](#)
- [Sanitization](#)

1. Business Agreement
2. Isolation Choices
3. HTTPS
4. Customer Managed Keys
5. <not used>
6. Access solution
7. <not used>
8. Business Agreement Order
9. RE RFI-1
10. Network Isolation Example
11. TLS Policy 1
12. TLS Policy Shown
13. Location Policy Detail
14. Geo-Replication Policy
15. Encryption fundamentals
16. Key Vault Config
17. AD Config
18. AD Config 2
19. AD Sync
20. Subscription Cancellation
21. Trusted Services
22. Data Management
23. Data Access Management
24. RE RFI-2
25. Program Document
26. Create Resource Fail

** Note: Evidence references above are linked descriptively (mapped) to the Industry side evidence description table within "BCSI Cloud TTX Lessons Learned – Appendix B"*

A stylized map of North America, including the United States, Canada, and Mexico. The map is rendered in shades of blue and grey. A horizontal blue band is overlaid across the middle of the map, containing the title text.

Questions and Answers

TOCC Field Test Update

Action

Information

Summary

During the September 2021 RSTC meeting, the RSTC was presented with information regarding a proposed CIP-002 Transmission Owner Control Centers (TOCCs) Field Test. The Field Test document was sent to RSTC members for a comment period ending on Thursday, September 30, 2021. Comments were considered and incorporated into the TOCC Field Test document. The RSTC endorsed the Field Test document which was then approved by the Standards Committee (SC) for implementation. This agenda item will provide an update on the implementation of the Field Test.

2022 Case Quality Metrics Assessment

Action

Information

Summary

This Annual Interconnection-Wide Model Assessment provides an unbiased and technically justified review of the powerflow and dynamics cases created for Interconnection-wide modeling purposes for the Eastern Interconnection (EI), Western Interconnection (WI), and Texas Interconnection (TI). Based on the results of the 2022 Case Quality Metrics Assessment, NERC will provide list of observations for the MOD-032 designees with recommendations on which metrics to focus on to help improve model quality for base cases developed in the future.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Case Quality Metrics

Annual Interconnection-Wide Model Assessment

November 2022

RELIABILITY | RESILIENCE | SECURITY



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

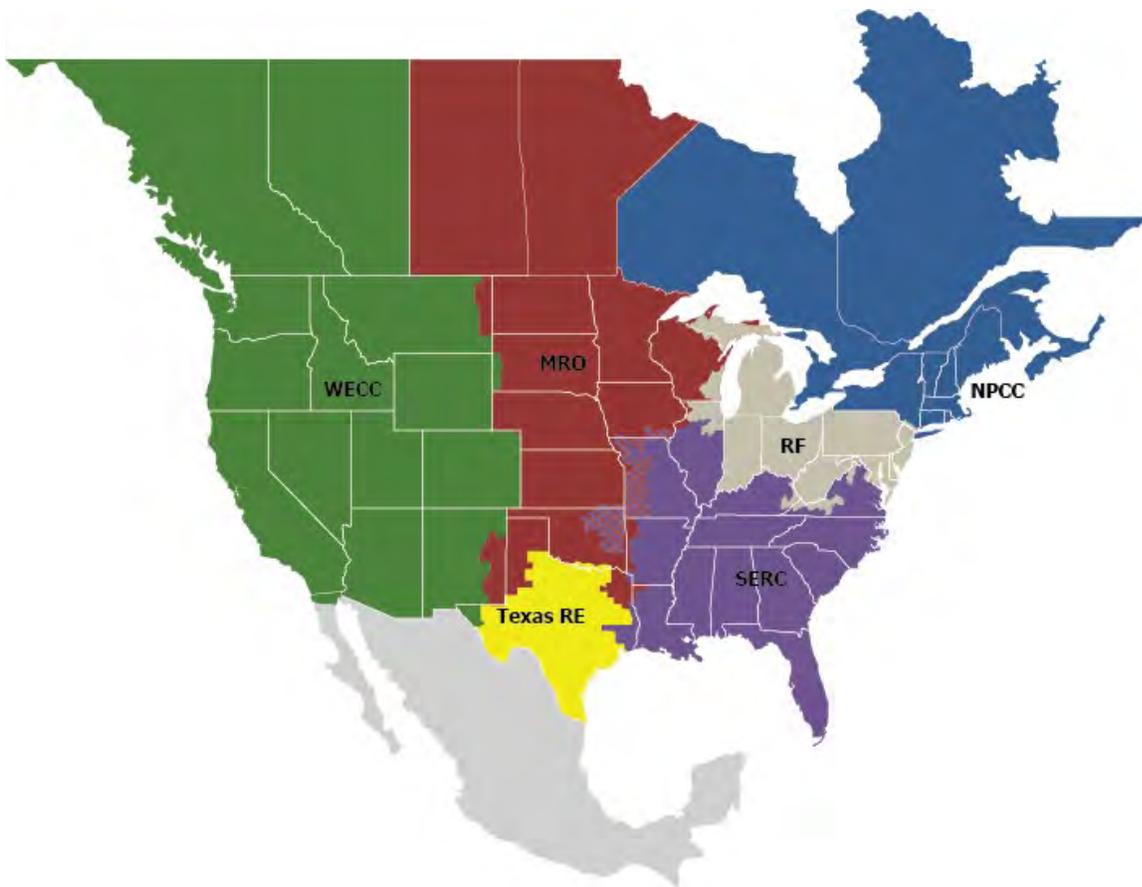
Preface	iii
Executive Summary.....	iv
Introduction	vi
Chapter 1 : Case Quality Metrics.....	1
Steady-State Powerflow Metrics.....	1
Transient Dynamics Metrics	2
Metric Categorization.....	6
Numerical Scores for Case Metrics.....	7
Dynamics Cases.....	7
Chapter 2 : Software Differences and Considerations.....	9
Software Differences	9
Other Considerations	9
Chapter 3 : Case Quality Metric Assessment	10
Notable Changes from Past Metrics.....	10
Eastern Interconnection Case Quality Metrics Assessment.....	11
2022 Summer Peak Case: 2022SUM.....	11
2022–2023 Winter Peak Case: 2022WIN.....	12
2022 Spring Light Load: 2022SLL	14
Texas Interconnection Case Quality Metrics Assessment.....	15
2024 Summer Peak Case: 2024_SP_Final_NonCnv	15
2025 Light Load Case: 2025_HWLL_Final_NonCnv	17
2028 Summer Peak Case: 2028_SP_Final_NonCnv	19
Western Interconnection Case Quality Metrics Assessment	20
2022 Summer Peak Case: 22HS3Sa	20
2022–2022 Winter Peak Case: 22HW2a.....	22
2022 Summer Light Load Case: 22LS2a	23
Chapter 4 : Observations and Recommendations	25
Observations.....	25
Recommendations.....	27
Appendix A : Yearly Comparison.....	29
Eastern Interconnection	29
Texas Interconnection	34
Western Interconnection	39

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

Powerflow and dynamics cases are the foundation of virtually all power system studies. Calculations of operating limits, planning studies, and performance analyses for various operating conditions all depend on mathematical representations of transmission topology, generation, and load. Case quality refers to the reasonableness of the data in the individual equipment models that comprise the Base Case for the characteristics and operating states desired for study. A reasonable model contains information that is mathematically correct, does not contain suspicious data entries in part or at a whole, and presumes that sufficient procedures are in place to ensure that the equipment models that have been provided are reasonable representations of the physical equipment the models are meant to represent. This *2022 Case Quality Metrics: Annual Interconnection-Wide Model Assessment* provides an unbiased and technically justified review of the powerflow and dynamics cases created for Interconnection-wide modeling purposes for the Eastern Interconnection¹ (EI), Western Interconnection (WI), and Texas Interconnection (TI).

Based on the results of the *2022 Case Quality Metrics Assessment*, NERC has provided the following list of observations for the MOD-032 designees with recommendations on which metrics to focus on to help improve model quality for base cases developed in the future:

- For EI, there are many records consistently flagged for the Generator Reactive at Limits, Generator Terminal Voltage, Natural Gas Generator Pmax, and Reactive Capability Curve metrics. All of these metrics are related to case dispatch or suspect data that involves generator reactive capability. Additionally, the WI's natural gas generation in the case does not reflect the ambient thermal impact to changes in steady-state active power limits for natural gas generators due to the effect of ambient temperature differences between the seasonal cases; all such data is suspect.
- The Generator Reactive Capability Curve check for the EI or TI remains at 0.00 due to the lack of provided generator curves. Further, no DER_A models exist in the cases and the DER_A tripping parameter check is still 0.00 for that reason.
- A majority of the metrics are below 5% while some are improving year-over-year as conversations between NERC and the MOD-032 designees continue.

Table ES.1 gives a “scorecard” for performance based on the overall assessment of cases for each Interconnection. Some metrics flag data that are more sensitive² to a study's results than others; however, each metric has similar weight in determining model quality. One of NERC's goals is to collaboratively improve model quality via various modeling improvements and initiatives while working with MOD-032 designees, utility members, and subject matter experts. It is not intended for the metrics to have a 0% in all instances as legitimate modeling differences exist; however, these are uncommon and should not be prevalent in the Base Case. For this report, the performance is evaluated so that a higher percentage signifies more records flagged in the metric, and the goal is to trend towards 0%. The scorecard colors represent those trends.

¹ The Quebec Interconnection is included in these model builds and is represented by the EI MOD-032 designees.

² For example, some metrics flag conditions that will prevent dynamic initialization and thus prevent dynamic stability simulations. This influences dynamic stability results more than the Erroneous Power Development Fractions metric. Both are important to improving Interconnection-wide Base Case quality.

Based on the observations listed in [Table ES.1](#), this report provides direct recommendations to each respective Interconnection’s MOD-032 designee. The general recommendation is to continue tracking this year-over-year assessment and improve the metrics by engaging relevant subject matter experts.

Table ES.1: Interconnection Scorecard		
Interconnection	Metrics	Evaluation
Eastern	Powerflow	Most metrics below 5% 2 metrics worsening, or consistent high score Voltage schedule conflicts major increase
	Dynamics	Most metrics below 5% 6 metrics consistent high score 1 metric worsening
Texas	Powerflow	Most metrics below 5% 1 metric worsening 1 metric consistent worsening or improving 1 metric consistent high score
	Dynamics	Most metrics below 5% 3 metrics consistent high score 2 metrics worsening 1 metric improving
Western	Powerflow	Most metrics below 5% 5 metrics improving, 4 metrics worsening
	Dynamics	Most metrics below 5% 3 metrics improving, 8 metrics worsening

Introduction

A powerflow case is a collection of steady-state models for system topology, load, generation, dispatch, and interchange that constitute a snapshot of the selected set of operating conditions. A dynamics case is a collection of dynamic models used in conjunction with a powerflow case to perform a stability analysis of system performance.

This *2022 Case Quality Metrics Assessment* tracks the quality of the base cases created by the MOD-032 designees for the purposes of Interconnection-wide modeling and subsequent system studies. The assessment reviews each of the major Interconnections (i.e., EI,³ WI, and TI). NERC works with the MOD-032 designees to select appropriate near-term base cases for each assessment. Trending the metrics provides an objective trend of Base Case quality by using technically justified metrics.

Base case quality has two principal aspects:

- **Case Data Quality:** Reasonableness of the data in the individual equipment models that comprise the case for the characteristics and operating states desired
- **Case Fidelity:** The ability of the case to accurately model measured power system behavior for the following:
 - The type of system conditions the case is intended to model such as heavy summer loads, light loads, etc.
 - The conditions measured during a distinct system event or disturbance

The metrics focus solely on the case data quality of the individual component models comprising the Base Case. Validation of case fidelity or overall model performance requires comparison of the cases to actual measured system conditions and are not included in this report. Planning Coordinators are encouraged to consider these metrics in their MOD-033 evaluation and to also include metrics on case fidelity.

³ The EI powerflow and dynamics cases include the Québec Interconnection.

Chapter 1: Case Quality Metrics

The following metrics have been developed by NERC and vetted by industry through engagement with relevant subject matter experts and previous industry stakeholder committees.⁴ The metrics are divided between steady state and dynamics to characterize what type of study the metric is most relevant for checking the quality of the case data. The metrics are updated annually by the NERC Advanced System Analytics and Modeling group. This process will change for future assessments to reflect appropriate oversight given the evolving ERO committee structure.

Steady-State Powerflow Metrics

The following list describes the steady-state powerflow metrics found under the heading **Metric Categorization**, in **Table 1.1**. These descriptions are provided for those metrics applied to the powerflow data of the Interconnection-wide Base Case models. As the metrics change, the specific number assigned to each description may change as metrics are added or retired. The steady-state powerflow metrics are as follows:

1. Dispatched generator real power output should not exceed the maximum real power capability of the unit ($P_{gen} \leq P_{max}$). Note: Although small exceedances of this P_{max} rule appear trivial, the result is the same for all exceedances: the case will not initialize in dynamics.
2. Dispatched generator real power output should not be less than the minimum real power capability of the unit ($P_{gen} \geq P_{min}$). Note: Although small exceedances of this P_{min} rule appear trivial, the result is the same for all exceedances: the case will not initialize in dynamics.
3. Scheduled area interchanges should sum to zero MW.
4. Active voltage control devices controlling the same bus should not have conflicting voltage regulation set points.
5. Transformers controlling voltage should have a voltage bandwidth that is sufficiently large in relation to the tap step of the transformer. Voltage bandwidths that are too small (or tap steps that are erroneously too large) may result in the lack of existence of a powerflow solution. The ratio of tap step (p.u.) to voltage bandwidth (p.u.) should be no less than 1.6; ratios below 1.0 are considered severe as they are extremely likely to prevent a powerflow solution from being found.⁵
6. The continuous (Rate A) and emergency (Rate B) ratings of a branch should be consistent. The continuous rating (Rate A) of the branch circuit should be less than or equal to the emergency rating (Rate B), and the ratio between the emergency rating (Rate B) and the continuous rating (Rate A) is checked against a threshold value (3.0) to identify probable errors. Selection of this ratio is based on engineering judgment.
7. Branch circuit loading should not exceed the circuit's continuous rating (Rate A); 100% of Rate A is used to identify exceedances; 105% of Rate A is used to identify severe exceedances.
8. Generator reactive power output should not be dispatched at Q_{max} or Q_{min} (if $Q_{max} \neq Q_{min}$).⁶
9. Generator reactive power limits (Q_{max} and Q_{min}) should have reasonable power factor⁷ compared with maximum active power (P_{max}) within +0.80 (producing Vars) and -0.85 (consuming Vars).
10. Parallel transformers should not have positive sequence circulating current.⁸

⁴ Such as the legacy NERC Planning Committee and the NERC Systems Analysis and Modeling Subcommittee

⁵ This metric was changed in the *2017 Case Quality Metrics Assessment* from thresholds of 2 and 1.25 for normal and severe thresholds, respectively, to 1.6 and 1.0.

⁶ Wind machines and units with $P_{gen} \leq 0$ will be omitted from this check.

⁷ Generators with $P_{max} = 0$ will be omitted to skip synchronous condensers.

⁸ Opposite direction of positive sequence current flow

11. Individual aggregate loads greater than 2 MVA⁹ and with positive active and reactive power consumption¹⁰ should have a power factor with absolute value greater than 0.5 pf.
12. The ratio of generator $R_{source}: X_{source}$ should be less than 1.0.¹¹
13. Generator terminal bus voltages should be between 0.95 and 1.05 when regulating a non-terminal bus.¹²
14. For all generator capability curves provided, no part of the piecewise function can limit a box defined by the P_{max} , P_{min} , Q_{max} , Q_{min} box. A sample figure of a correctly constructed piecewise function is in [Figure 1.1](#) where the green box is not limited by the black curve.

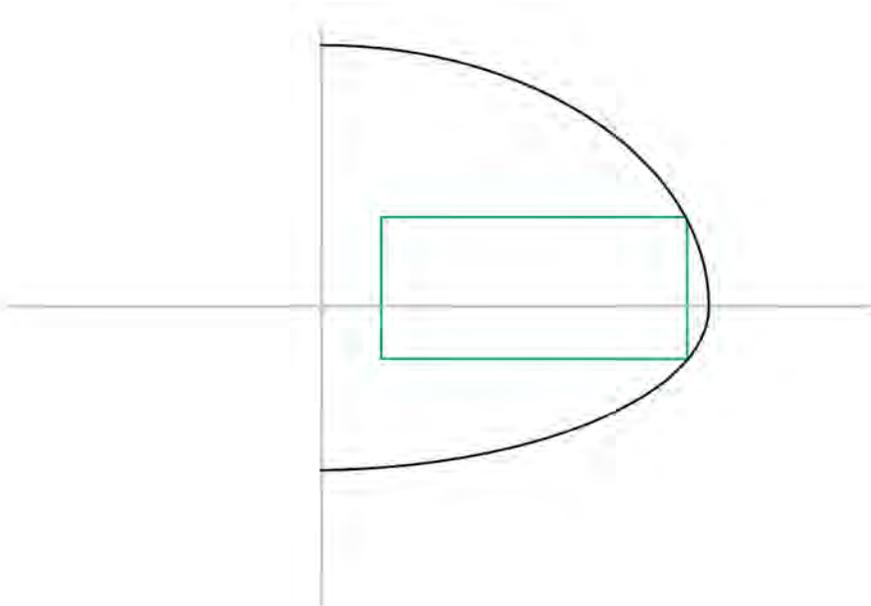


Figure 1.1: Generator Reactive Capability Box Overview

15. All non-jumper transformers should have an X/R ratio between 5 and 2,000, and transmission lines should have an X/R ratio of less than 100. Exclusions include resistances with a value of zero, and when reactance or resistance is less than zero.
16. All natural gas generators in seasonal cases should change their maximum power available due to their relationship to ambient temperature conditions. All summer P_{max} values should be less than the winter P_{max} values.

Transient Dynamics Metrics

Continuing on from the steady-state list is the transient dynamics metrics. The numbers here continue as part of the entire set of metrics applied to the Interconnection-wide base cases and focus on the dynamics portion of data provided in such cases. Hence, the numbered list does not restart at number one. Some of these metrics require both

⁹ This threshold is used to omit small loads that have little impact on the performance of the model; the focus is on pf of larger loads.

¹⁰ This avoids shunt capacitor issues (negative reactive power) and net generators (negative active power value) represented in the load values.

¹¹ Except for $X_{source} = 9999$

¹² Non-synchronous devices are excluded from this check.

powerflow and dynamic data to be loaded in the software in order to check the quality of the data and, as such, require longer processing time for larger data sets:

17. Generating units larger than the criteria threshold established for each Interconnection¹³ should have a generator model included in their dynamics record; units without a generator model are flagged as not meeting this modeling criteria.
18. Generating units larger than the criteria threshold established for each Interconnection and that have a model (but are load netted anyway) are also tallied. This additional metric is needed to help identify all generating units without active models in the case as Item 17 overlooks generators that have models but are load netted anyway, and Item 19 below overlooks generators that lack models and are dispatched out-of-service in the case.
19. Generating units larger than the criteria threshold established for each Interconnection should not be netted as negative load; any such units that are netted are flagged.
20. Generating units larger than the criteria threshold established for each Interconnection¹⁴ should not be modeled with a classical generator model.
21. User written model penetration is also tallied for use in the MOD-032 case creation process.
22. Generating units should have consistent generator reactance values. For example, the following measures are used to assess consistency of round rotor generators:
 - a. D-axis synchronous reactance (X_d) should not be less than d-axis transient reactance (X_d').
 - b. D-axis transient reactance (X_d') should not be less than d-axis subtransient reactance (X_d'').
 - c. Subtransient reactance (X_d'') should not be less than stator leakage reactance (X_l).
 - d. Q-axis synchronous reactance (X_q) should not be less than q-axis transient reactance (X_q').
 - e. Q-axis transient reactance (X_q') should not be less than q-axis subtransient reactance (X_q'').
23. Generator time constants should be consistent: $T''_{d0} \leq T'_{d0}$ and $T''_{q0} \leq T'_{q0}$ ¹⁵ and $T'_{q0} \leq T'_{d0}$ ¹⁶.
24. Generator inertia constants should be within reasonable ranges: $1.5 \leq H \leq 9.0$ for all generators greater than 20 MVA, and $1.0 \leq H \leq 10.0$ for machines less than 20 MVA.¹⁷
25. Saturation factors S (1.0) and S (1.2) should be reasonable:¹⁸
 - a. $0.03 \leq S(1.0) \leq 0.18$
 - b. $0.2 \leq S(1.2) \leq 0.85$
 - c. S(1.2) should be within 2 to 8 times S(1.0).
 - d. Severe saturation factor check:
 - i. S(1.0) and S(1.2) should be greater than zero.
 - ii. S(1.0) and S(1.2) should be less than 1.0.

¹³ 20 MVA for the EI; 10 MVA for the WI and TI

¹⁴ 50 MVA for the EI and TI; 0 MVA for the WI

¹⁵ GENTPJ (and gentpf in PSLF) has an exception to these rules since a salient pole machine is represented with $T'_{q0} = 0$. For this case, the only check used is $T''_{d0} \leq T'_{d0}$.

¹⁶ This check is not applied to GENSAL and GENSAE generator models.

¹⁷ These ranges were adopted based on industry feedback on the *2017 Case Quality Metrics Assessment*.

¹⁸ This metric was changed in the *2017 Case Quality Metrics Assessment* from an S (1.0) maximum of .12 to .18 and an S (1.2) maximum of .80 to .85.

- iii. $S(1.0)$ should be less than or equal to $S(1.2)$.
- 26. Units with a power system stabilizer (PSS) should have an excitation system model.
- 27. Generator speed damping coefficient should be equal to zero for non-classical machine models.
- 28. Turbine-governor models should have lead-time constants less than lag time constants.¹⁹
- 29. Turbine power development fractions should add up to 1.0.²⁰ An example of these fractions in the block diagrams for a turbine governor model is in [Figure 1.2](#).

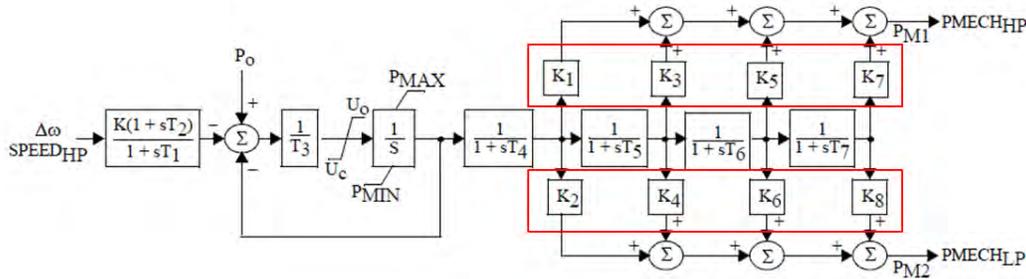


Figure 1.2: IEEEG1 Model Block Diagram (Source: Siemens PTI)

- 30. DC exciter model self-excitation parameter K_E ²¹ should be a small negative number unless $K_E = 0$ (automatically calculated by program) or $K_E = 1$ (separately excited exciter). A sample block diagram for this parameter is highlighted in [Figure 1.3](#).

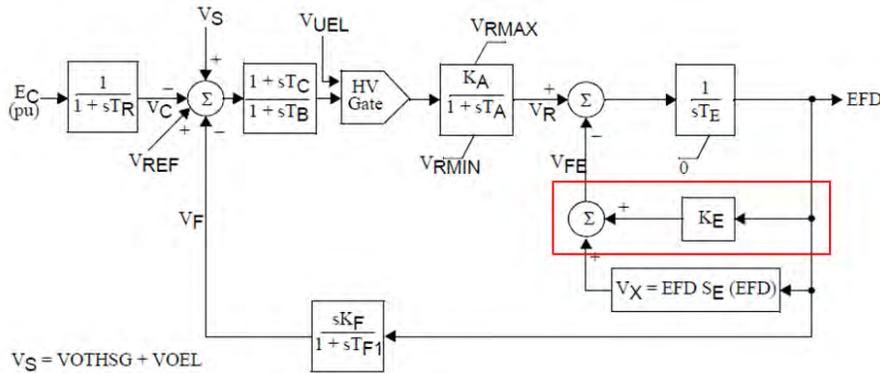


Figure 1.3: ESDC1A Model Block Diagram (Source: Siemens PTI)

- 31. Wind turbine electrical model WT3E should have $\omega_{Pmin} < \omega_{P20} < \omega_{P40} < \omega_{P60} < \omega_{P100}$.
- 32. PSS models should have reasonable parameters for the forward integration models. If $Ks3 = 1$, the parameters should be $Ks1 > 0$, $V_{stmax} > 0$, $V_{stmin} < 0$, $Tw4 = 0$, $T7 = Tw2$, $T6 > 0.033$, $T8 = m * T9$, and the input signals should be generator speed and generator electrical power. All such models that don't have these parameters or have $Ks3$ not equal to one are flagged for review. The PSS2A model, a forward integration PSS model, is found in [Figure 1.4](#).

¹⁹ This stabilizes the model as it reduces the forward path gain for high frequency changes in the input.
²⁰ This metric was corrected in the 2017 Case Quality Metrics Assessment to check if $K1+K2+K3+ \dots +K8 = 1.0$.
²¹ K_E reflects setting the shunt field rheostat for zeroing out the voltage regulator, often a small negative number.

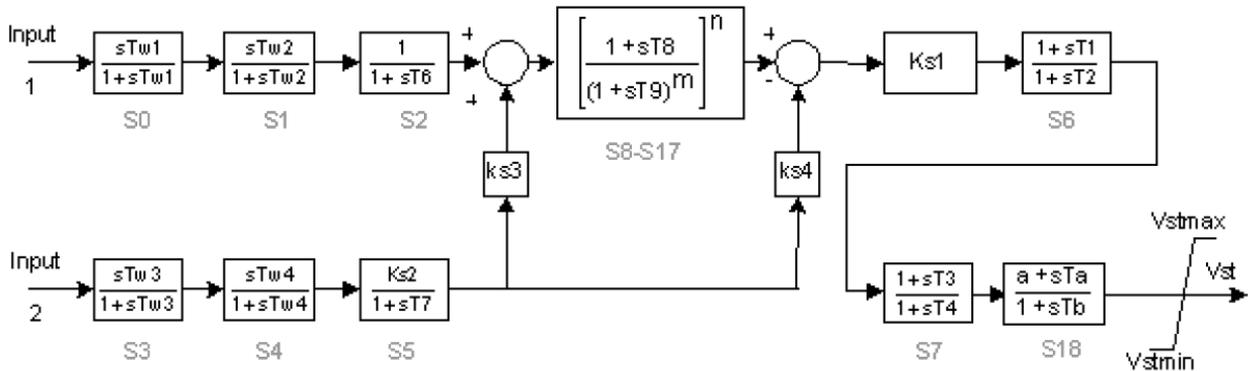


Figure 1.4: PSS2A Block Diagram [Source: GE PSLF]

33. Models should not be listed as unacceptable or not recommended on the NERC Acceptable Model List:²²
- a. Unacceptable models are tallied for all generator, exciter, stabilizer, and turbine-governor models.
 - b. Not recommended models are tallied for all generator, exciter, stabilizer, and turbine-governor models.
34. Second generation renewable models should be parameterized to site-specific conditions, namely as follows:
- a. Renewable generator models (REGC) should have a difference between the “lvpnt0” and “lvpnt1” settings that are greater than 0.1 p.u.
 - b. REGCs should have a difference between the “zerox” and “brkpt” settings that are greater than 0.1 p.u.
 - c. REGCs should have a setting of “Tg” less than 0.2 seconds.
 - d. Renewable electrical models (REEC) should have a P_{max} setting of less than 1.0 p.u. of its dynamic MVA base.
 - e. REECs should have a Q_{max} setting of less than 1.0 p.u. of its dynamic MVA base.
 - f. REECs should have a Q_{min} setting of greater than -1.0 p.u. of its dynamic MVA base.
 - g. REECs should have a non-default K_{qv} setting.
 - h. REECs for battery energy storage systems should have a large T_s value.
 - i. It is a suspect condition for a “ T_s ” value under 1,000 seconds.
 - ii. It is a severely suspect condition for a “ T_s ” value under 30 seconds.
 - i. Renewable plant models (REPC) should have a voltage control bus (or buses) and a monitored bus.
 - j. Wind turbine pitch controllers should not have identical parameters to another installation.

²² All disclosures regarding ‘acceptability’ are documented in the spreadsheet on the Modeling Assessment Page [here](#). If not listed on the spreadsheet, models are considered “acceptable.”

Metric Categorization

All of the case quality metrics are categorized by their impact to the Interconnection Base Case creation process in [Table 1.1](#). These categorization demonstrate how severe each metric is in impacting the data quality of the case. Metrics that are “bad data” are ones that find data that is blatantly incorrect and should be corrected. For example, reactance or time constant inconsistencies that are not physically possible. The term “suspect data” indicates data that looks abnormal and may or may not be in error. This should be reviewed by the MOD-032 designees more closely and addressed accordingly. “Case setup issues” are issues with how the individual elements are compiled (e.g., powerflow case or dynamics data file) and applied to create the initial operating state from which simulations would then be performed. Some metrics may have more than one indication of data (e.g., generators with a lack of modeling). These generators cannot be tracked in dynamics outside of load netting due to a lack of generator model, indicating a case setup issue. Since all Interconnections have a modeling threshold for explicit modeling, generators above that threshold also are suspect if they do not contain a dynamics model in the case.

Table 1.1: Bad and Suspect Data Metrics			
Steady-State Metrics			
Metric	Bad Data	Suspect Data	Case Setup Issue
P_{\max} Exceedances			X
P_{\min} Exceedances			X
Scheduled Interchange Sum			X
Voltage Schedule Conflicts			X
Tap Step Conflicts		X	
Tap Step Conflicts (Severe)		X	
Low Emergency Rating		X	
High Emergency Rating		X	
Thermal Overloads			X
Thermal Overloads (Severe)			X
Gen Reactive at Limits			X
Gen Reactive Limit Power Factor		X	
Positive Sequence TX Circulating Current		X	
Poor Load Power Factor		X	
Generator $R_{\text{source}}:X_{\text{source}}$ Ratio	X		
Generator Terminal Voltage			X
Generator Reactive Capability Curve		X	
X/R Ratio Check		X	
Natural Gas Generator P_{\max}	X	X	
Gens without Models		X	X
Netted Gens with Models		X	X
Netted Generators		X	
Gens with Classical Models		X	
Unacceptable Models	X		
Not Recommended Models		X	
User-Written Models ²³		(X)	
Inconsistent Reactances	X		
Inconsistent Time Constants	X		
Unreasonable Inertia Constants		X	

²³ These are not affecting Interconnection performance. This is listed here based on discussions with MOD-032 designees.

Table 1.1: Bad and Suspect Data Metrics			
Steady-State Metrics			
Metric	Bad Data	Suspect Data	Case Setup Issue
Unreasonable Saturation Factors		X	
Severe Saturation Factors	X		
PSS but no Excitation		X	
Inconsistent Speed Damping	X		
Inconsistent Lead-Lag Time Constant	X		
Erroneous Power Dev Fractions	X		
DC Exciter Self-Excitation Errors	X		
Inconsistent Type III Wind Speeds	X		

Numerical Scores for Case Metrics

Generally, the raw count of each of the instances of data issues specified in the criteria above is not, by itself, a suitable metric. Most of these raw counts need to be scaled to reflect the size of the Interconnection being evaluated. This scaling is done by expressing each of the raw counts as a percentage of the total number of elements to which the corresponding criteria is applicable in the case. Each metric is reported as a count and performance is expressed as a percentage of all data issues identified²⁴ as a percentage of all applicable models.

Note that the denominator of the fractional values will differ for each metric tested based on the number of models under test. For example, the threshold values for applicable units may be different or the metric may relate to specific types of dynamic models.

Dynamics Cases

There are some specific qualifications on a few of the dynamic metrics that are noted in the following list:

- **Generators without models:** the number of generators meeting Interconnection size criteria for modeling with no dynamics model, expressed as a percentage of total number of generators (in-service and out-of-service), meeting Interconnection size criteria for modeling
- **Netted generators with models:** the number of generators meeting Interconnection size criteria for modeling with a dynamics model but load netted anyway, expressed as a percentage of total number of in-service generators meeting Interconnection size criteria for modeling
- **Netted generators:** the number of generators meeting Interconnection size criteria for modeling that are load netted and expressed as a percentage of total number of in-service generators meeting Interconnection size criteria
- **Generators with classical models:** the number of generators meeting Interconnection size criteria for non-classical modeling with a classical model expressed as a percentage of total number of generators (in-service and out-of-service) meeting Interconnection size criteria for non-classical modeling
- **Generators with faulty reactances:** the number of generators with inconsistent reactance data (e.g., $X_d'' < X_i$) expressed as a percentage of total number of generators (in-service and out-of-service) with models for which the reactance criteria is applicable (e.g., genrou, gentpj)

In addition, for each of the dynamic metrics, the maximum real and reactive power limits for each unit found to violate the criteria are totaled. When units were whitelisted by feedback from the MOD-032 designees, these sums were not altered; however, the percentage scores were altered. The total percentage is listed for all respective

²⁴ Generally, this is a one to one relationship with the number of models associated with an identified data issue.

(generator, exciter, etc.) models in the case in terms of total number applicable for the check. For instance, a check that involves only generators will only check generator dynamic models.

Chapter 2: Software Differences and Considerations

Software Differences

Two software platforms are primarily used for assembling Interconnection-wide cases: Power Systems Simulator (PSS®E) from Siemens PTI (for the EI and TI) and Positive Sequence Load Flow (PSLF) from GE (for the WI). Because of differences in the handling of data by these two programs, the method for calculating the number of instances of criteria not being met may vary between Interconnections for some of the metrics:

- PSS®E stores voltage set point for generators and static VAR systems with the device data record whereas PSLF stores voltage set point for these devices with the bus data record. In PSLF, it is not possible to have voltage schedule conflicts for multiple generators and static VAR systems that are regulating a common location. However, transformer data records in PSLF have their own voltage regulation data.
- PSLF has a turbine type flag in the generator data to indicate if a generating unit is a wind unit.²⁵ However, this flag is not completely populated in WI base cases. Therefore, to eliminate wind units from the reactive limits check (Q_{gen} at Q_{max} or Q_{min}), the dynamics data file has to be loaded and the corresponding dynamic models have to be checked. The units with any of the following wind generator models were eliminated from the check: genwri, gewtg, gewtgx, regc_a, regc_c, wt1g, wt2g, wt3g, and wt4g. It is recommended that the turbine type flag be utilized to improve the code's speed and complexity in identifying unit fuels.
- The names of the dc exciter models differ between PSS®E and PSLF. Hence, for the check on parameter KE in dc exciters, the following models were checked in PSLF: esdc1a, esdc2a, esdc3a, esdc4b, exdc1, exdc2, exdc2a, exdc4, ieeet1, and rexs.
- PSLF has the generator MVA base specified in both the powerflow and dynamics data files. All dynamic data is then taken on the per-unit MVA base specified in the dynamics data file. In PSS®E, one value of MVA base is specified and located in the powerflow file. In evaluating generator inertia constants for the WI base cases (using PSLF), the inertia constant evaluated on the MVA base specified in the powerflow file unless the specified powerflow base was the default 100 MVA. This calculated constant is an MVA base transfer between the dynamic and powerflow MVAs if the powerflow MVA is not 100 MVA.
- Fuel types are not capable of being accessed in PSS®E. As such, for this current year's metrics, a N/A score is produced for the natural gas P_{max} check. Supplemental information may be required to check these cases for Interconnections that use PSS®E.

Other Considerations

In reading the data for a generator to determine its size, the generator MVA base value in the powerflow data record (MBASE) is not a reliable value to use for generator size since many small generators have the program default value of 100 MVA entered for this parameter. Therefore, a more comprehensive approach is used; generator MVA size is determined as the maximum value of the following:

- Dispatched MVA of the unit $\left(\sqrt{P_{gen}^2 + Q_{gen}^2}\right)$ where P_{gen} and Q_{gen} are the dispatched real and reactive output of the unit in the case
- MVA of the unit at maximum real and reactive limits $\left(\sqrt{P_{max}^2 + Q_{max}^2}\right)$ where P_{max} and Q_{max} are the maximum real and reactive output limits of the unit in the powerflow data
- MBASE value unless value is 100.0 MVA (default value) in which case this parameter is ignored

²⁵ For that matter, a variety of unit types can be specified and are used accordingly for multiple metrics.

Chapter 3: Case Quality Metric Assessment

The goal of the case quality metrics assessment is to promote good modeling practices and to strive to reduce data errors in Interconnection-wide base cases. Since the performance score is the percentage of elements that have data errors, the goal translates into attempting to drive performance scores towards zero. However, it is not expected that all performance scores reach zero. There are legitimate modeling reasons why some of the generic metrics developed by NERC in this *2022 Case Quality Metrics Assessment* could be violated (e.g., equivalence or back-to-back dc ties between Interconnections). This information is provided to industry to gauge the quality of Interconnection-wide base cases for use in studies and assessments. A more detailed report is provided to the MOD-032 designees with the goal of assisting in improving the quality of the cases.

This assessment brings to light some of the modeling issues that have been identified by working with utility members, MOD-032 designees, and modeling groups in the electric utility industry. Some metrics serve to highlight more significant modeling errors that should be addressed directly. Other metrics serve to track modeling improvements that NERC is driving such as the Modeling Notifications Process developed by the NERC Systems Analysis and Modeling Subcommittee²⁶ and now maintained by NERC staff.

The following subsections describe the performance scores for the assessment of each powerflow and dynamics case analyzed in the EI, TI, and WI. Note that performance scores greater than 5% are marked in **red**.

Notable Changes from Past Metrics

As the metrics are not infallible, many changes and alterations are supplied by industry to help gauge the quality Interconnection-wide base cases. Industry experts are able to send in suggestions and alterations to these metrics as the implementation of the scripts are posted alongside this report. Notable changes for this report are the following:

- Fixed an error when checking PSS2A and PSS2B models in PSLF for cross compound units that the wrong generator ID in the models table was used
- Fixed floating point to integer comparisons for the powerflow metrics
- Added a new metric that checks parameterization of the second generation renewable models
- Fixed an error for printing violations for cases built in PSS[®]E version 34 that printed an entire list rather than one entry of the list
- Added a requested feature for MOD-032 designees to see the nominal KV in the detailed report for items that did not pass each metric
- Fixed an error on the power factor when using qtable information in PSLF that was causing power factor to be 0 in calculation

²⁶ NERC System Analysis and Modeling Subcommittee: [https://www.nerc.com/comm/PC/Pages/System-Analysis-and-Modeling-Subcommittee-\(SAMS\)-2013.aspx](https://www.nerc.com/comm/PC/Pages/System-Analysis-and-Modeling-Subcommittee-(SAMS)-2013.aspx)

Eastern Interconnection Case Quality Metrics Assessment

The performance and score, evaluated as a percentage, for all of the Eastern Interconnection cases are tabulated in [Tables 3.1 to 3.9](#). [Tables 3.1 to 3.3](#) are for the 2022SUM Base Case; [Tables 3.4 to 3.6](#) are for the 2022WIN Base Case; [Tables 3.7 to 3.9](#) are for the 2021SLL Base Case.

2022 Summer Peak Case: 2022SUM

Table 3.1: EI Steady-State Metrics

Metric	Performance	Score (%)
P _{max} Exceedances	4/6,991	0.06
P _{min} Exceedances	1/6,759	0.01
Scheduled Interchange Sum	0.001	-
Thermal Overloads (LOADING OVER RATE A)	195/100,262	0.19
Thermal Overloads (Severe FLAGRANT LOADING OVER RATE A)	146/100,262	0.15
Low Emergency Rating (RATE A > RATE B)	27/100,262	0.03
High Emergency Rating (RATE B:RATE A RATIO TOO HIGH)	89/100,262	0.09
Voltage Schedule Conflicts	118	-
Tap Step Conflicts	39/21,810	0.18
Tap Step Conflicts (Severe)	14/21,810	0.06
Generator Reactive at Limits	734/4,469	16.42
Generator Reactive Limit Power Factor	99/5,627	1.76
Positive Sequence TX Circulating Current	0/2,634	0.00
Poor Load Power Factor	175/50,271	0.35
Generator Reactive Capability Curve	0/0	0
Generator R _{source} :X _{source} Ratio	8/6,991	0.11
X/R Ratio Check	215/93,569	0.23
Generator Terminal Voltage	114/2,789	4.07
Natural Gas Generator Pmax	N/A	N/A
Natural Gas Generator Pmax (Severe)	N/A	N/A

Table 3.2: EI Dynamics Metrics

Metric	Performance	Score (%)	P _{max} (MW)	Q _{max} (MVAR)
Generators without Models	205/6,881	2.98	7,389	2,201
Generators with Classical Models	14/5,214	0.27	6,920	3,805
Netted Generators	126/5,023	2.51	4,670	1,163
Netted Gens with Models	9/5,023	0.18	390	228
Inconsistent Reactances	40/3,770	1.06	3,869	1,909
Unacceptable Models (total)	2,469/20,200	12.36	-	-
Not Recommended Models (total)	3,694/20,200	18.29	-	-
User-Written Models ²⁷	1,410/23,980	-	-	-
Inconsistent Time Constants	3/4,018	0.07	312	186
Unreasonable Inertia Constants	411/5,027	8.18	28,744	19,012
Unreasonable Saturation Factors	482/4,018	12.00	53,152	27,539
Severe Saturation Factors	41/4,018	1.02	3,807	2,011
PSS but no Excitation	4/6,881	0.06	97	278

²⁷ These are not affecting Interconnection performance. This is listed here based on discussions with MOD-032 designees.

Table 3.2: EI Dynamics Metrics

Metric	Performance	Score (%)	P _{max} (MW)	Q _{max} (MVAR)
Inconsistent Speed Damping	122/4,847	2.52	8,035	3,785
Inconsistent Lead-Lag Time Constant	33/1,689	1.94	8,843	3,911
Erroneous Power Dev Fractions	20/525	3.81	4,644	2,157
DC Exciter Self-Excitation Errors	120/885	13.56	3,805	2,577
Inconsistent Type III Wind Speeds	0/206	0.00	0	0
Suspect PSS2A/2B parameters	335/1,908	17.56	72,064	40,996
Incorrect DER_A Tripping Parameters	0/0	0.00	0	0
Second Generation Renewable Model Parameterization ²⁸	354/1,619	21.87	-	-

Table 3.3: EI Unacceptable and Not Recommended Model Breakdown

Category	Subcategory	Performance	Score (%)
Unacceptable Models	Generator	1,174/6,676	17.59
	Exciter	429/6,351	6.75
	Stabilizer	203/2,715	7.48
	Turbine Governor	670/4,458	15.48
Not Recommended Models	Generator	3,193/6,676	47.83
	Exciter	0/6,351	0.00
	Stabilizer	0/2,715	0.00
	Turbine Governor	501/4,458	11.24
User Written Models*	Generator	344/8,351	4.12
	Exciter	140/7,512	1.86
	Stabilizer	172/3,055	5.63
	Turbine Governor	754/5,062	14.90

*Due to how PSS®E distinguishes “user-written” models in their software, this number may be higher and alters based on version of the software.

2022–2023 Winter Peak Case: 2022WIN

Table 3.4: EI Steady-State Metrics

Metric	Performance	Score (%)
P _{max} Exceedances	1/5,718	0.02
P _{min} Exceedances	0/5,718	0.00
Scheduled Interchange Sum	0	-
Thermal Overloads (LOADING OVER RATE A)	136/100,651	0.14
Thermal Overloads (Severe FLAGRANT LOADING OVER RATE A)	107/100,651	0.11
Low Emergency Rating (RATE A > RATE B)	24/100,651	0.02
High Emergency Rating (RATE B:RATE A RATIO TOO HIGH)	1/100,651	0.00
Voltage Schedule Conflicts	118	-
Tap Step Conflicts	39/21,845	0.18
Tap Step Conflicts (Severe)	14/21,845	0.06
Generator Reactive at Limits	647/3,858	16.77
Generator Reactive Limit Power Factor	68/4,755	1.43
Positive Sequence TX Circulating Current	0/2,666	0.00
Poor Load Power Factor	204/47,816	0.34

²⁸ The way this metric is scored does not lend itself to producing sums of active and reactive power, so an asterisk is used

Table 3.4: EI Steady-State Metrics

Metric	Performance	Score (%)
Generator Reactive Capability Curve	0/0	0.05
Generator $R_{source}:X_{source}$ Ratio	9/5,718	0.16
X/R Ratio Check	222/93,900	0.00
Generator Terminal Voltage	104/2,515	4.13
Natural Gas Generator Pmax	N/A	N/A
Natural Gas Generator Pmax (Severe)	N/A	N/A

Table 3.5: EI Dynamics Metrics

Metric	Performance	Score (%)	P_{max} (MW)	Q_{max} (MVAR)
Generators without Models	226/7,050	3.21	7,580	2,358
Generators with Classical Models	15/5,344	0.28	7,420	3,830
Netted Generators	78/4,306	1.81	3,074	782
Netted Gens with Models	9/4,306	0.21	844	220
Inconsistent Reactances	40/3,801	1.05	3,888	1,884
Unacceptable Models (total)	2,522/20,567	12.26	-	-
Not Recommended Models (total)	3,732/20,567	18.15	-	-
User-Written Models ²⁹	1,420/24,208	-	-	-
Inconsistent Time Constants	5/4,049	0.12	1,055	624
Unreasonable Inertia Constants	410/5,048	8.12	29,562	18,740
Unreasonable Saturation Factors	484/4,049	11.95	54,132	27,610
Severe Saturation Factors	41/4,049	1.01	3,828	2,011
PSS but no Excitation	5/7,050	0.06	97.1	278
Inconsistent Speed Damping	122/4,867	2.51	8,072	3,782
Inconsistent Lead-Lag Time Constant	33/1,713	1.93	8,942	3,911
Erroneous Power Dev Fractions	20/530	3.77	4,657	2,157
DC Exciter Self-Excitation Errors	119/888	13.40	3,958	2,585
Inconsistent Type III Wind Speeds	0/206	0.00	0	0
Suspect PSS2A/2B parameters	338/1,921	17.60	74,420	41,469
Incorrect DER_A Tripping Parameters	0/0	0.00	0	0
Second Generation Renewable Model Parameterization	421/1,738	24.22	-	-

Table 3.6: EI Unacceptable and Not Recommended Model Breakdown

Category	Subcategory	Performance	Score (%)
Unacceptable Models	Generator	1,183/6,824	17.33
	Exciter	437/6,496	6.73
	Stabilizer	203/2,746	8.37
	Turbine Governor	699/4,501	15.53
Not Recommended Models	Generator	3,224/6,824	47.25
	Exciter	0/6,496	0.00
	Stabilizer	0/2,746	0.00
	Turbine Governor	508/4,501	11.29
User Written Models*	Generator	353/8,423	4.19
	Exciter	148/7,592	1.95

²⁹ These are not affecting Interconnection performance. This is listed here based on discussions with MOD-032 designees.

Table 3.6: EI Unacceptable and Not Recommended Model Breakdown

Category	Subcategory	Performance	Score (%)
	Stabilizer	169/3,056	5.53
	Turbine Governor	750/5,137	14.60

*Due to how PSS®E distinguishes “user-written” models in their software, this number may be higher and alters based on version of the software

2022 Spring Light Load: 2022SLL

Table 3.7: EI Steady-State Metrics

Metric	Performance	Score (%)
P _{max} Exceedances	0/4,054	0.00
P _{min} Exceedances	0/4,054	0.00
Scheduled Interchange Sum	-0.1	-
Thermal Overloads (LOADING OVER RATE A)	27/99,651	0.04
Thermal Overloads (Severe FLAGRANT LOADING OVER RATE A)	20/99,651	0.03
Low Emergency Rating (RATE A > RATE B)	25/99,651	0.03
High Emergency Rating (RATE B:RATE A RATIO TOO HIGH)	0/99,651	0.00
Voltage Schedule Conflicts	117	-
Tap Step Conflicts	38/21,480	0.18
Tap Step Conflicts (Severe)	14/21,480	0.07
Generator Reactive at Limits	473/2,549	18.56
Generator Reactive Limit Power Factor	138/3,390	4.07
Positive Sequence TX Circulating Current	0/2,622	0.00
Poor Load Power Factor	187/46,161	0.41
Generator Reactive Capability Curve	0/0	0.00
Generator R _{source} :X _{source} Ratio	6/4,054	0.15
X/R Ratio Check	214/93,037	0.23
Generator Terminal Voltage	242/1,722	14.05
Natural Gas Generator Pmax	N/A	N/A
Natural Gas Generator Pmax (Severe)	N/A	N/A

Table 3.8: EI Dynamics Metrics

Metric	Performance	Score (%)	P _{max} (MW)	Q _{max} (MVAR)
Generators without Models	196/6,857	2.86	8,308	2,389
Generators with Classical Models	14/5,209	0.27	6,920	3,805
Netted Generators	65/3,065	2.12	2,666	840
Netted Gens with Models	7/3,065	0.23	246	120
Inconsistent Reactances	40/3,775	1.06	3,878	1,880
Unacceptable Models (total)	1,172/6,661	17.59	-	-
Not Recommended Models (total)	3,197/6,661	48.00	-	-
User-Written Models ³⁰	1,439/25,402	-	-	-
Inconsistent Time Constants	3/4,024	0.07	312	186
Unreasonable Inertia Constants	411/5,024	8.18	29,352	18,959
Unreasonable Saturation Factors	481/4,024	11.95	53,180	27,030
Severe Saturation Factors	41/4,024	1.02	3,808	2,000

³⁰ These are not affecting Interconnection performance. This is listed here based on discussions with MOD-032 designees.

Table 3.8: EI Dynamics Metrics

Metric	Performance	Score (%)	P _{max} (MW)	Q _{max} (MVAR)
PSS but no Excitation	4/6,857	0.06	97	278
Inconsistent Speed Damping	122/4,844	2.52	8,035	3,961
Inconsistent Lead-Lag Time Constant	43/1,939	2.22	10,142	4,552
Erroneous Power Dev Fractions	24/587	4.09	5,027	2,397
DC Exciter Self-Excitation Errors	120/884	13.57	3,661	2,577
Inconsistent Type III Wind Speeds	0/206	0.00	0	0
Suspect PSS2A/2B parameters	359/1,905	18.85	74,665	40,867
Incorrect DER_A Tripping Parameters	0/0	0.00	0	0
Second Generation Renewable Model Parameterization	345/1,595	21.63	-	-

Table 3.9: EI Unacceptable and Not Recommended Model Breakdown

Category	Subcategory	Performance	Score (%)
Unacceptable Models	Generator	1,172/6,661	17.59
	Exciter	425/6,337	6.71
	Stabilizer	203/2,706	7.50
	Turbine Governor	881/4,948	17.81
Not Recommended Models	Generator	3,197/6,661	48.00
	Exciter	0/6,337	0.00
	Stabilizer	0/2,706	0.00
	Turbine Governor	612/4,948	12.37
User Written Models*	Generator	343/8,320	4.12
	Exciter	140/7,482	1.87
	Stabilizer	172/3,046	5.65
	Turbine Governor	784/6,554	11.96

*Due to how PSS[®]E distinguishes “user-written” models in their software, this number may be higher and alters based on version of the software

Texas Interconnection Case Quality Metrics Assessment

The performance and score, evaluated as a percentage, for all of the Texas Interconnection cases are tabulated in [Tables 3.10 to 3.18](#). [Tables 3.10 to 3.12](#) are for the 2023_SP_Final_NonCnv Base Case; [Tables 3.13 to 3.15](#) are for the 2024_HWLL_Final_NonCnv Base Case; [Tables 3.16 to 3.18](#) are for the 2027_SP_Final_NonCnv Base Case.

2024 Summer Peak Case: 2024_SP_Final_NonCnv

Table 3.10: TI Steady-State Metrics

Metric	Performance	Score (%)
P _{max} Exceedances	0/1133	0.00
P _{min} Exceedances	1/1133	0.08
Scheduled Interchange Sum	0	-
Thermal Overloads	28/11,399	0.25
Thermal Overloads (Severe)	28/11,399	0.25
Low Emergency Rating	0/11,399	0.00
High Emergency Rating	2/11,399	0.02
Voltage Schedule Conflicts	47	-
Tap Step Conflicts	66/1,849	3.57

Table 3.10: TI Steady-State Metrics

Metric	Performance	Score (%)
Tap Step Conflicts (Severe)	0/1,849	0.00
Generator Reactive at Limits	102/734	13.90
Generator Reactive Limit Power Factor	98/1054	9.30
Positive Sequence TX Circulating Current	0/46	0.00
Poor Load Power Factor	3/5,645	0.05
Generator $R_{source}:X_{source}$ Ratio	7/1133	0.62
X/R Ratio Check	39/9,300	0.42
Generator Terminal Voltage	0/740	0.00
Generator Reactive Capability Curve	0/0	0.00
Natural Gas Generator Pmax	N/A	N/A
Natural Gas Generator Pmax (Severe)	N/A	N/A

Table 3.11: TI Dynamics Metrics

Metric	Performance	Score (%)	P_{max} (MW)	Q_{max} (MVAR)
Generators without Models	13/1,059	1.23	*4,199	*2,896
Generators with Classical Models	10/915	1.09	4,824	4,492
Netted Generators with Models	3/1,010	0.30	232	58
Netted Generators	3/1,010	0.30	232	58
Inconsistent Reactances	5/444	1.13	333	187
Unacceptable Models (total)	39/2,746	1.42	-	-
Not Recommended Models (total)	469/2,746	17.08	-	-
User-Written Models ³¹	1192/3,087	-	-	-
Inconsistent Time Constants	4/579	0.69	94.4	56.8
Unreasonable Inertia Constants	112/594	18.86	4,517	2,985
Unreasonable Saturation Factors	76/579	13.13	10,135	4,817
Severe Saturation Factors	9/579	1.55	763	371
PSS but no Excitation	0/1,151	0.00	0	0
Inconsistent Speed Damping	17/583	2.92	719	431
Inconsistent Lead-Lag Time Constant	0/244	0.00	0	0
Erroneous Power Dev Fractions	4/51	7.84	2746	827
DC Exciter Self-Excitation Errors	4/38	10.53	491	240
Inconsistent Type III Wind Speeds	0/0	0.00	0	0
Suspect PSS2A/2B parameters	57/319	17.87	3,534	2,171
Incorrect DER_A Tripping Parameters	0/0	0.00	0	0
Second Generation Renewable Model Parameterization	0/382	0.00	-	-

* This total is not indicative of the units identified since the score can be modified by whitelisted units. This sum indicates the total Pmax and Qmax of units that are flagged by the check rather than the subset of remaining units after the exempted models are removed.

³¹ These are not affecting Interconnection performance. This is listed here based on discussions with MOD-032 designees. Further, the MOD-032 designee, TexasRE, allows User Written Models for the TI base cases.

Table 3.12: TI Unacceptable and Not Recommended Model Breakdown

Category	Subcategory	Performance	Score (%)
Unacceptable Models	Generator	29/1,040	2.79
	Exciter	10/890	1.12
	Stabilizer	0/408	0.00
	Turbine Governor	0/408	0.00
Not Recommended Models	Generator	448/1,040	43.08
	Exciter	21/890	2.36
	Stabilizer	0/408	0.00
	Turbine Governor	0/408	0.00
User Written Models*	Generator	481/1,025	-
	Exciter	281/865	-
	Stabilizer	2/413	-
	Turbine Governor	233/784	-

*Due to how PSS[®]E distinguishes “user-written” models in their software, this number may be higher and alters based on version of the software. Further, the MOD-032 designee, TexasRE, allows User Written Models for the TI base cases.

2025 Light Load Case: 2025_HWLL_Final_NonCnv

Table 3.13: TI Steady-State Metrics

Metric	Performance	Score (%)
P _{max} Exceedances	1/842	0.12
P _{min} Exceedances	0/842	0.00
Scheduled Interchange Sum	0	-
Thermal Overloads	30/11,419	0.26
Thermal Overloads (Severe)	27/11,419	0.24
Low Emergency Rating	0/11,419	0.00
High Emergency Rating	2/11,419	0.02
Voltage Schedule Conflicts	79	0.02
Tap Step Conflicts	66/1,850	3.57
Tap Step Conflicts (Severe)	0/1,850	0.00
Generator Reactive at Limits	27/553	4.88
Generator Reactive Limit Power Factor	55/764	7.20
Positive Sequence TX Circulating Current	0/46	0.00
Poor Load Power Factor	5/5,638	0.09
Generator R _{source} :X _{source} Ratio	7/842	0.83
X/R Ratio Check	39/9,321	0.42
Generator Terminal Voltage	5/537	0.93
Generator Reactive Capability Curve	0/0	-
Natural Gas Generator Pmax	N/A	N/A
Natural Gas Generator Pmax (Severe)	N/A	N/A

Table 3.14: TI Dynamics Metrics

Metric	Performance	Score (%)	P _{max} (MW)	Q _{max} (MVAR)
Generators without Models	13/1,059	1.23	*4,199	*2,895
Generators with Classical Models	10/917	1.09	4,824	4,492
Netted Generators with Models	3/727	0.41	232	58
Netted Generators	3/727	0.41	232	58
Inconsistent Reactances	5/444	1.13	335	187
Unacceptable Models (total)	39/2,746	1.42	-	-
Not Recommended Models (total)	469/2,746	17.08	-	-
User-Written Models ³²	1,612/3,503	-	-	-
Inconsistent Time Constants	4/579	0.69	94	57
Unreasonable Inertia Constants	112/594	18.85	4,724	2,984
Unreasonable Saturation Factors	76/579	13.12	10,810	4,817
Severe Saturation Factors	9/579	1.55	781	371
PSS but no Excitation	0/1,152	0.00	0	0
Inconsistent Speed Damping	17/583	2.92	728	431
Inconsistent Lead-Lag Time Constant	0/244	0.00	0	0
Erroneous Power Dev Fractions	4/51	7.84	2795	827
DC Exciter Self-Excitation Errors	4/38	10.52	491	240
Inconsistent Type III Wind Speeds	0/0	0.00	0	0
Suspect PSS2A/2B parameters	57/319	17.87	3,686	2,171
Incorrect DER_A Tripping Parameters	0/0	0.00	0	0
Second Generation Renewable Model Parameterization	0/382	0.00	-	-

* This total is not indicative of the units identified score as the score can be modified by whitelisted units. This sum indicates the total Pmax and Qmax of units that are flagged by the check rather than the subset of remaining units after the exempted models are removed.

Table 3.15: TI Unacceptable and Not Recommended Model Breakdown

Category	Subcategory	Performance	Score (%)
Unacceptable Models	Generator	29/1,040	2.79
	Exciter	10/890	1.12
	Stabilizer	0/408	0.00
	Turbine Governor	0/408	0.00
Not Recommended Models	Generator	448/1,040	43.08
	Exciter	21/890	2.36
	Stabilizer	0/408	0.00
	Turbine Governor	0/408	0.00
User Written Models*	Generator	642/1,184	-
	Exciter	397/979	-
	Stabilizer	77/434	-
	Turbine Governor	496/906	-

*Due to how PSS®E distinguishes “user-written” models in their software, this number may be higher and alters based on version of the software. Further, the MOD-032 designee, TexasRE, allows User Written Models for the TI base cases.

³² These are not affecting Interconnection performance. This is listed here based on discussions with MOD-032 designees. Further, the MOD-032 designee, TexasRE, allows User Written Models for the TI base cases.

2028 Summer Peak Case: 2028_SP_Final_NonCnv

Table 3.16: TI Steady-State Metrics

Metric	Performance	Score (%)
P _{max} Exceedances	0/1,143	0.00
P _{min} Exceedances	0/1,143	0.00
Scheduled Interchange Sum	0	-
Thermal Overloads	29/11,462	0.25
Thermal Overloads (Severe)	26/11,462	0.23
Low Emergency Rating	0/11,462	0.00
High Emergency Rating	2/11,462	0.02
Voltage Schedule Conflicts	37	-
Tap Step Conflicts	64/1,854	3.45
Tap Step Conflicts (Severe)	0/1,854	0.00
Generator Reactive at Limits	156/746	20.91
Generator Reactive Limit Power Factor	99/1064	9.30
Positive Sequence TX Circulating Current	0/46	0.00
Poor Load Power Factor	3/5,714	0.05
Generator R _{source} :X _{source} Ratio	7/1,143	0.61
X/R Ratio Check	39/9,366	0.42
Generator Terminal Voltage	5/748	0.67
Generator Reactive Capability Curve	0/0	0.00
Natural Gas Generator Pmax	N/A	N/A
Natural Gas Generator Pmax (Severe)	N/A	N/A

Table 3.17: TI Dynamics Metrics

Metric	Performance	Score (%)	P _{max} (MW)	Q _{max} (MVAR)
Generators without Models	13/1,059	1.23	4,199	2,896
Generators with Classical Models	10/916	1.09	4,824	4,492
Netted Generators with Models	3/1,021	0.29	232	58
Netted Generators	3/1,021	0.29	232	58
Inconsistent Reactances	5/436	1.15	333	187
Unacceptable Models (total)	39/2,746	1.42	-	-
Not Recommended Models (total)	461/2,746	16.79	-	-
User-Written Models ³³	1,612/3,503	-	-	-
Inconsistent Time Constants	4/579	0.69	94	57
Unreasonable Inertia Constants	112/594	18.86	4,517	2,985
Unreasonable Saturation Factors	76/579	13.13	10,135	4,817
Severe Saturation Factors	9/579	1.55	763	371
PSS but no Excitation	0/1,151	0.00	0	0
Inconsistent Speed Damping	17/583	2.92	719	431
Inconsistent Lead-Lag Time Constant	0/244	0.00	0	0
Erroneous Power Dev Fractions	4/59	6.78	2,746	827
DC Exciter Self-Excitation Errors	4/38	10.52	491	440
Inconsistent Type III Wind Speeds	0/0	0.00	0	0

³³ These are not affecting Interconnection performance. This is listed here based on discussions with MOD-032 designees. Further, the MOD-032 designee, TexasRE, allows User Written Models for the TI base cases.

Table 3.17: TI Dynamics Metrics

Metric	Performance	Score (%)	P _{max} (MW)	Q _{max} (MVAR)
Suspect PSS2A/2B parameters	65/319	20.38	3,890	2,557
Incorrect DER_A Tripping Parameters	0/0	0.00	0	0
Second Generation Renewable Model Parameterization	0/382	0.00	-	-

* This total is not indicative of the units identified score as the score can be modified by whitelisted units. This sum indicates the total Pmax and Qmax of units that are flagged by the check rather than the subset of remaining units after the exempted models are removed.

Table 3.18: TI Unacceptable and Not Recommended Model Breakdown

Category	Subcategory	Performance	Score (%)
Unacceptable Models	Generator	29/1,040	2.79
	Exciter	10/890	1.12
	Stabilizer	0/408	0.00
	Turbine Governor	0/408	0.00
Not Recommended Models	Generator	440/1,040	42.31
	Exciter	21/890	2.36
	Stabilizer	0/408	0.00
	Turbine Governor	0/408	0.00
User Written Models*	Generator	943/1,978	-
	Exciter	517/1,674	-
	Stabilizer	79/772	-
	Turbine Governor	713/1,549	-

*Due to how PSS[®]E distinguishes “user-written” models in their software, this number may be higher and alters based on version of the software. Further, the MOD-032 designee, TexasRE, allows User Written Models for the TI base cases.

Western Interconnection Case Quality Metrics Assessment

The performance and score, evaluated as a percentage, for all of the Western Interconnection cases are tabulated in [Tables 3.19 to 3.27](#). [Tables 3.19 to 3.21](#) are for the 21HS3a Base Case; [Tables 3.22 to 3.24](#) are for the 22HW2a Base Case; [Tables 3.25 to 3.27](#) are for the 21LS1a Base Case.

2022 Summer Peak Case: 22HS3Sa

Flagrant:

Table 3.19: Steady-State Metrics : 2022 Summer Peak Case: 22HS3Sa

Metric	Performance	Score (%)
P _{max} Exceedances	13/3484	0.37%
P _{min} Exceedances	9/3484	0.26%
Scheduled Interchange Sum	0.0	
Voltage Schedule Conflicts	64/9,987	0.64%
Tap Step Conflicts	6/9,987	0.26%
Tap Step Conflicts (Severe)	6/9,987	0.06%
Low Emergency Rating	5/29,138	0.02%
High Emergency Rating	1/29,138	0.00%
Thermal Overloads	20/31,010	0.06%
Thermal Overloads (Severe)	12/31,010	0.04%
Generator Reactive at Limits	246 of 3699	6.65%
Generator Reactive Limit Power Factor	175 of 3,699	4.73%

Table 3.19: Steady-State Metrics : 2022 Summer Peak Case: 22HS3Sa

Metric	Performance	Score (%)
Positive Sequence TX Circulating Current	350 of 3,699	9.46%
Poor Load Power Factor	3 of 7,553	0.04%
Generator $R_{source}:X_{source}$ Ratio	8 of 4,678	0.17%
Generator Terminal Voltage	0 of 1,874	0.0%
Generator Reactive Capability Curve	63 of 2,393	2.63%
X/R Ratio Check	33 of 2,393	1.38%
Natural Gas Generator Pmax	740 of 977	75.74%
Natural Gas Generator Pmax (Severe)	38 of 977	3.89%

Table 3.20: Dynamics Metrics

Metric	Performance	Score (%)	P _{max} (MW)	Q _{max} (MVAR)
Generators without Models	300 of 3,720	8.06%	27,479.0	13,517.8
Netted Generators with Models	5 of 2,805	0.18%	281.5	18.1
Netted Generators	141 of 2,805	5.03%	9,995.9	3,769.3
Generators with Classical Models	0 of 4,678	0.00%	0.0	0.0
Unacceptable Models (total)	364 of 4,678	7.78%	16,656.3	4,665.1
Not Recommended Models (total)	256 of 4,299	5.95%	16,656.3	4,665.1
User-Written Models[1]	0 of 29,352	0.00%	0.0	0.0
Units with Inconsistent Time Constant	202 of 3,191	6.33%	4,107.7	2,110.3
Inconsistent Inertia Constants	327 of 3,191	10.25%	15,157.0	9,940.6
Inconsistent Saturation factors	540 of 3,191	16.92%	25,392.9	12,279.8
Flagrantly Inconsistent Saturation Factors	174 of 3,191	5.45%	25,392.9	12,279.8
PSS with NO Excitation System model:	36 of 1,818	1.98%	3,518.0	1,601.4
Units with Bad Speed Damping:	215 of 3,191	6.74%	3,408.7	1,516.0
Units with Bad Lead Lag Time Constants	69 of 1,279	5.39%	4,589.1	2,036.4
Erroneous Power Dev Fractions	3 of 159	1.89%	337.2	89.5
DC Exciter Self-Excitation Errors	27 of 469	5.76%	1,221.6	523.4
Inconsistent Type III Wind Speeds	0 of 72	0.00%	0.0	0.0
Incorrect Parameterized Models:	666 of 1,832	36.35%	0.0	0.0
Suspect PSS2A/2B Parameters	52 of 1,653	3.15%	29,128.70	12,679.2
Incorrect DER_A Tripping Parameters	0%	0%		
Second Generation Renewable Model Parameterization	666 of 1,832	36.35%		

* This total is not indicative of the units identified score as the score can be modified by whitelisted units. This sum indicates the total Pmax and Qmax of units that are flagged by the check rather than the subset of remaining units after the exempted models are removed.

Table 3.21: Unacceptable and Not Recommended Model Breakdown

Category	Subcategory	Performance	Score (%)
Unacceptable Models	Generator	108 of 4,678	2.31%
	Exciter	106 of 4,299	2.47%
	Stabilizer	65 of 1,893	3.43%
	Turbine Governor	85 of 2,418	3.52%
Not Recommended Models	Generator	231 of 4,678	4.94%
	Exciter	152 of 4,299	3.54%
	Stabilizer	0 of 1,893	0.00%
	Turbine Governor	56 of 2,418	2.32%

Table 3.21: Unacceptable and Not Recommended Model Breakdown

Category	Subcategory	Performance	Score (%)
User Written Models	None	0 of 29,352	0.0%

2021–2022 Winter Peak Case: 22HW2a**Table 3.22: Steady-State Metrics**

Metric	Score (%)	Performance
P _{max} Exceedances	0.44%	12 out of 2,717
P _{min} Exceedances	0.33%	9 out of 2,717
Scheduled Interchange Sum	0.0%	0
Voltage Schedule Conflicts	0.65%	64 out of 9,860
Tap Step Conflicts	0.34%	34 out of 9,860
Tap Step Conflicts (Severe)	0.08%	8 out of 9,860
Low Emergency Rating	0.35%	100 out of 28,878
High Emergency Rating	0.02%	7 out of 28,878
Thermal Overloads	0.04%	11 out of 30,699
Thermal Overloads (Severe)	0.01%	3 out of 30,699
Generator Reactive at Limits	6.97%	253 out of 3,631
Generator Reactive Limit Power Factor	3.72%	135 out of 3,631
Positive Sequence TX Circulating Current	9.58%	348 out of 3,631
Poor Load Power Factor	0.04%	3 out of 6,914
Generator R _{source} :X _{source} Ratio	0.20%	9 out of 4,584
Generator Terminal Voltage	0.00%	9 out of 1,882
Generator Reactive Capability Curve	2.56%	48 out of 1,878
X/R Ratio Check	2.50%	47 out of 1,878
Natural Gas Generator Pmax	N/A	N/A
Natural Gas Generator Pmax (Severe)	N/A	N/A

Table 3.23: Dynamics Metrics

Metric	Performance	Score (%)	P _{max} (MW)	Q _{max} (MVAR)
Generators without Models	286 of 3632	7.87%	3,7731	8,,748.3
Netted Generators with Models	5 of 2184	0.23%	107.5	47.4
Netted Generators	72 of 2184	3.30%	2,419.8	823.6
Generators with Classical Models	0 of 4584	0.00%	0	0
Unacceptable Models (total)	120 of 4584	2.62%	18,326.4	5,396.4
Not Recommended Models (total)	119 of 4253	2.80%	18,326.4	5,396.4
User-Written Models[1]	4 of 20654	0.30%	0.0	0.0
Units with Inconsistent Time Constant	207 of 3188	6.49%	5,638.0	2,659.2
Inconsistent Inertia Constants	315 of 3188	9.88%	17,055.2	10,506.1
Inconsistent Saturation factors	531 of 3188	16.66%	2,419.8	823.6
Flagrantly Inconsistent Saturation Factors	179 of 3188	5.61%	5,205.6	2,495.0
PSS with NO Excitation System model:	120 of 4584	16.66%	18,326.4	5,396.4
Units with Bad Speed Damping:	119 of 4253	2.80%	18,326.4	5,396.4
Units with Bad Lead Lag Time Constants	42 of 1284	3.27%	2,970.2	1,680.8
Erroneous Power Dev Fractions	5 of 186	2.69%	552.2	219.5
DC Exciter Self-Excitation Errors	26 of 512	5.80%	1194.1	508.4

Table 3.23: Dynamics Metrics

Metric	Performance	Score (%)	P _{max} (MW)	Q _{max} (MVAR)
Inconsistent Type III Wind Speeds	0 of 76	0%	0	0
Incorrect Parameterized Models:	540 of 1,560	34.62%	0.0	0.0
Suspect PSS2A/2B Parameters	61 of 1,642	3.71%	32,701.70	14,218.2
Incorrect DER_A Tripping Parameters	0 of 0%	0%	N/A	N/A
Second Generation Renewable Model Parameterization	540 of 1,560	34.62%	N/A	N/A

* This total is not indicative of the units identified score as the score can be modified by whitelisted units. This sum indicates the total P_{max} and Q_{max} of units that are flagged by the check rather than the subset of remaining units after the exempted models are removed.

Table 3.24: Unacceptable and Not Recommended Model Breakdown; Case: 22HW2a

Category	Subcategory	Performance	Score (%)
Unacceptable Models	Generator	120 of 4,584	2.62%
	Exciter	119 of 4,523	2.8%
	Stabilizer	68 of 0	3.55%
	Turbine Governor	95 of 2,428	3.91%
Not Recommended Models	Generator	259 of 4,584	5.65%
	Exciter	179 of 4,253	3.54%
	Stabilizer	0 of 1,917	0.00%
	Turbine Governor	56 of 2,428	2.31%
User Written Models	DC Lines	4 of 20,654	0.30%

2022 Summer Light Load Case: 22LS2a

Table 3.25: Steady-State Metrics

Metric	Performance	Score (%)
P _{max} Exceedances	0.42%	10 out of 2,397
P _{min} Exceedances	1.34%	32 out of 2,397
Scheduled Interchange Sum	0%	0
Voltage Schedule Conflicts	0.61%	61 out of 9,957
Tap Step Conflicts	0.33%	33 out of 9,957
Tap Step Conflicts (Severe)	0.07%	7 out of 9,957
Low Emergency Rating	0.12%	34 out of 29,107
High Emergency Rating	0.01%	2 out of 29,107
Thermal Overloads	0.05%	14 out of 30,974
Thermal Overloads (Severe)	0.01%	2 out of 30,974
Generator Reactive at Limits	7.01%	259 out of 3,694
Generator Reactive Limit Power Factor	4.74%	175 out of 3,694
Positive Sequence TX Circulating Current	9.94%	367 out of 3,694
Poor Load Power Factor	0.06%	4 out of 6440
Generator R _{source} :X _{source} Ratio	0.22%	10 out of 4,550
Generator Terminal Voltage	0.00%	0 out of 1,876
Generator Reactive Capability Curve	2.39%	37 out of 1,550
X/R Ratio Check	4.52%	70 out of 1,550
Natural Gas Generator Pmax	80.79%	782 out of 968
Natural Gas Generator Pmax (Severe)	1.65%	16 out of 968

Table 3.26: Dynamics Metrics

Metric	Performance	Score (%)	P _{max} (MW)	Q _{max} (MVAR)
Generators without Models	313 of 3,698	8.46%	19,564.7	9,202.3
Netted Generators with Models	14 of 1,890	0.74%	130.7	133.4
Netted Generators	115 of 1,890	6.08%	5,434.6	1,673.8
Generators with Classical Models	0 of ,650	0.00%	0	0
Unacceptable Models (total)	108 of 4,678	2.31%	16,656.3	4,665.1
Not Recommended Models (total)	106 of 4,299	2.47%	16,656.3	4,665.1
User-Written Models[1]	2 of 26,003	0.21%	0.0	0.0
Units with Inconsistent Time Constant	202 of 3,191	6.33%	4,107.7	2,110.3
Inconsistent Inertia Constants	314 of 3,191	9.84%	15,157.0	9,940.6
Inconsistent Saturation factors	637 of 3,191	19.96%	25,392.9	12,279.8
Flagrantly Inconsistent Saturation Factors	174 of 3,191	5.45%	25,392.9	12,279.8
PSS with NO Excitation System model:	36 of 1,818	1.98%	3,518.0	1,601.4
Units with Bad Speed Damping:	215 of 3,191	6.74%	3,408.7	1,516.0
Units with Bad Lead Lag Time Constants	69 of 1,279	5.39%	4,589.1	2,036.4
Erroneous Power Dev Fractions	3 of 1,59	1.89%	337.2	89.5
DC Exciter Self-Excitation Errors	27 of 469	5.76%	1,221.6	523.4
Inconsistent Type III Wind Speeds	0 of 72	0%	0.0	0.0
Incorrect Parameterized Models:	620 of 1,747	35%	0.0	0.0
Suspect PSS2A/2B Parameters	54 of 1,654	3.26%	32,510.10	14,159.60
Incorrect DER_A Tripping Parameters	0 of 0%	0%		
Second Generation Renewable Model Parameterization	620 of 1,747	35.49%		

* This total is not indicative of the units identified score as the score can be modified by whitelisted units. This sum indicates the total Pmax and Qmax of units that are flagged by the check rather than the subset of remaining units after the exempted models are removed.

Table 3.27: Unacceptable and Not Recommended Model Breakdown : Case: 22LS2a

Category	Subcategory	Performance	Score (%)
Unacceptable Models	Generator	110 of 4,650	2.37%
	Exciter	107 of 4,323	2.48%
	Stabilizer	66 of 0	3.45%
	Turbine Governor	86 of 2,422	3.55%
Not Recommended Models	Generator	247 of 4,650	5.31%
	Exciter	168 of 4,323	3.89%
	Stabilizer	0 of 1,912	0.0%
	Turbine Governor	56 of 2,422	2.31%
User Written Models	DC Lines	2 of 26,003	0.21%

Chapter 4: Observations and Recommendations

For the summer peak cases, [Table 4.1](#) demonstrates the number of metrics above 5% according to the categories identified in [Table 1.1](#). Additional trending information between past NERC case quality metrics assessments and this year's version can be found in [Appendix A](#).

Interconnection	Number of Bad Data Metrics above 5%	Number of Suspect Data Metrics above 5%	Number of Case Setup Issues above 5%
East	2	5	2
Texas	1	5	1
West	4	6	3

Observations

Based on the results of the case quality metrics assessment, the following observations are made:

- Generators dispatched at reactive limits remains an issue across the Interconnections even though this metric has improved since the *2017 Case Quality Metrics: Annual Interconnection-Wide Model Assessment* when it was first implemented. These generators in the Base Case are dispatched in a suspect manner.
- Generators with reactive limits that have relatively low power factor (i.e., large reactive limits relative to active power limits) are still an issue for the TI and WI Interconnections. The flagged data is suspect.
- Unreasonable inertia constants are still an issue for all Interconnections even when widening the range of reasonable data. The trend for this data either contains a degradation of performance or a constant elevated performance across all Interconnections. The flagged data is suspect.
- Unreasonable saturation factors are still an issue for all Interconnections, but the severe version of this metric has seen improvement. The saturation factors with severe inaccuracies should be a priority for the WI; however, both severe and non-severe metrics are consistently high score. In general, this metric is trending towards improvement. For those generators flagged, their modeled saturation factor values are suspect.
- Generator speed damping parameters with values other than zero are still an issue in the WI but not in the EI or TI. Furthermore, a general trend towards improvement was made in the EI and TI. These generator models contain bad data.
- The dc exciter self-excitation errors are still an issue for all Interconnections with only the TI showing improvements in the score. These generator models contain bad data.
- A general decline in performance regarding generators above the modeling threshold not having generator models have been observed. Generators flagged are indicative of a case setup issue in addition to being a suspect condition for such generators.
- A slight increasing score for inclusion of netted generation in the EI and WI has been observed; however, the trend has historically stayed below a score of 5%. The EI has only demonstrated this increase in the light load case.
- In the unacceptable or not recommended model metrics, all Interconnections demonstrate either a consistent performance or worsening score. Of special note is that the TI and WI have maintained the unacceptable model score below 5% while the EI has increased its score significantly.
- The TI corrected the large increase of Generator Reactive Limit Power Factor metric in the summer case from 2020.

- For the WI and EI, there is a consistent high performance or worsening score for the Generator Reactive at Limits, Generator Terminal Voltage, Natural Gas Generator, and Reactive Capability Curve metrics. The TI is an exception that has generally improved in these metrics since last year. All of these metrics are related to case dispatch or suspect data that involve reactive capability of generators. Additionally, the WI’s natural gas generation in the case does not reflect the ambient thermal impact to changes in steady-state active power limits for natural gas generators due to the effect of ambient temperature differences between the seasonal cases; all such data is suspect.

Table 4.2 gives a “scorecard” for performance based on the overall assessment of cases for each Interconnection. This performance is based on highlights from the specific observations above and the performance tables identified in Appendix A.

Table 4.2: Interconnection Scorecard		
Interconnection	Metrics	Evaluation
Eastern	Powerflow	Most metrics below 5% 2 metrics worsening, or consistent high score Voltage schedule conflicts major increase
	Dynamics	Most metrics below 5% 6 metrics consistent high score 1 metric worsening
Texas	Powerflow	Most metrics below 5% 1 metric worsening 1 metric consistent worsening or improving 1 metric consistent high score
	Dynamics	Most metrics below 5% 3 metrics consistent high score 2 metrics worsening 1 metric improving
Western	Powerflow	Most metrics below 5% 5 metrics improving, 4 metrics worsening
	Dynamics	Most metrics below 5% 3 metrics improving, 8 metrics worsening

Recommendations

Based on the previously listed observations, NERC recommends the following:

- NERC should continue performing the NERC case quality metrics assessment each year to assess the overall performance of case quality for the Interconnection-wide planning cases developed. NERC should then provide such feedback to the MOD-032 designees for year-over-year improvement.
- NERC should continue working with subject matter experts to improve both the Powerflow and Dynamics metrics.
- The MOD-032 designees for the EI and TI should focus on verifying the saturation factor curves and provide exceptions for verified generator parameters via a whitelist. The WI should focus on the severe saturation factor generators as a priority. Each MOD-032 designee should review the listed units with unreasonable saturation factors and work with their respective Generator Owners (GOs) to review model validation test reports to ensure accuracy.
- Generators above the modeling threshold for each Interconnection should have a model, one that conforms to the MOD-032 designees modeling practices (and all models should adhere to the NERC Acceptable Model List). The MOD-032 designees should review their model building process and enforce their modeling thresholds. The large majority of not recommended models is the generator model GENROU. MOD-032 designees are encouraged to read the *Modeling Notification: Use of GENTPJ Generator Model*³⁴ for recommended models to better represent the effect of stator current on saturation.
- The MOD-032 designees for each Interconnection should review the generators identified in the Generator Reactive Limit Power Factor to determine if the power factor is correct and provide verified exceptions via a whitelist.
- The MOD-032 designee for the WI should actively work with its GOs to correct units with inconsistent time constants. The metric is flagging generator model parameters that are not physically realistic.
- The MOD-032 designee for the WI should work with its respective GOs to correct the use of speed damping coefficients on units that are not modeled as classical machines. These values should be zero for generation units flagged.
- Each MOD-032 designee should work with their respective GOs to correct issues associated with the dc exciter self-excitation errors. This report provides some information in the description of the metric on how to correct these issues.
- The MOD-032 designees should ensure their natural gas generator thermal rates are represented in the Interconnection wide base cases. When software inputs exist to determine fuel type, such fields should be filled out accordingly. Where such fields do not exist, supplemental data or requests to software vendors should be made to encourage identification of generators with possibly large capacity changes due to ambient temperature. The MOD-032 designee for the WI should determine how feasible it is to request seasonal thermal limits in their ratings for natural gas generation facilities. The MOD-032 designees for the EI and TI should determine how to best include seasonal natural gas generator capacities into their base case packages.
- The MOD-032 designees should utilize the unacceptable and not recommended model generators adjusted for GENROU as flagged in those metrics to begin targeting efforts for model improvement and replacement.
- The MOD-032 designee for the WI should review their case cases to ensure that generator reactive capability curves are entered properly, that generator bus voltages stay within 0.95 and 1.05 p.u. and that generators are not dispatched to their reactive maximum capability.

³⁴ A link to the notification is provided [here](#).

- The MOD-032 designees for the WI and EI should ensure that the parameterization for second-generation renewable models is reflective of plant specific parameters. Generators flagged in the check have one or more model with parameters that are suspect.
- The MOD-032 designee for the WI should review their light summer cases to correct suspect generation data as more generation (as a percentage of all generators online) with suspect data seems to be used year-over-year.

Appendix A: Yearly Comparison

The metrics for each case were assessed to compare this year’s performance against prior years’ performance. The results of this assessment are shown in [Tables A.1 to A.9](#). The color coding used in the tables denotes the following.

	Consistent performance under 5% performance score, or performance score moved from greater than 5% to less than 5%
	Positive performance improvements (decrease in score of 2% or more from previous year)
	Continued performance above 5% performance score with no noticeable improvement
	Noticeable performance degradation (increase of 1% or more from previous year), or performance score moved from less than 5% to greater than 5%

Many of the metrics are below 5 percent (dark green) signifying that the overall case quality of the Interconnection-wide base cases are consistently of good quality. Similar in Chapter 3, scores in **red** indicate a higher than 5 percent score for that year. A few metrics obtained light green scores indicating an improvement of case quality and the few scores that had the orange score, indicating a stable, but high score. It is good to note that the EI Base Case Creation Process has a series number associated with the Base Case that will not line up with the year listed in the tables. Thus, there is a year difference between the series number and the case quality metrics assessment year. To further clarify, the case quality metrics assessment year is X, and the EI builds their models for year X in year X-1.

Eastern Interconnection

Table A.1: EI Heavy Summer Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
Powerflow	P _{max} Exceedances	0.15	0.10	0.05	0.06	0.06	
	P _{min} Exceedances	0.10	0.1	0.02	0.01	0.01	
	Scheduled Interchange Sum	0	0.01	0	0	0	
	Thermal Overloads	0.17	0.19	0.13	0.15	0.19	
	Thermal Overloads (Severe)	0.13	0.15	0.11	0.12	0.15	
	Low Emergency Rating	0.00	0.00	0.02	0.02	0.03	
	High Emergency Rating	0.03	0.00	0.00	0.00	0.09	
	Voltage Schedule Conflicts	27	14	29	102	118	
	Tap Step Conflicts	0.07	0.07	0.16	0.17	0.18	
	Tap Step Conflicts (Severe)	0.03	0.01	0.09	0.09	0.06	
	Generator Reactive at Limits	18.82	18.88	16.52	15.70	16.42	
	Generator Reactive Limit Power Factor	13.16	12.14	10.30	2.38	8.09	
	Positive Sequence TX Circulating Current	0.00	0.00	0.00	0.00	0.00	
	Poor Load Power Factor	0.35	0.29	0.30	0.33	0.44	
	Generator Reactive Capability Curve	N/A	0.00	0.00	0.00	0	
	Generator R _{source} ·X _{source} Ratio	0.00	0.00	0.06	0.04	0.11	
	X/R Ratio Check	N/A	0.25	0.25	0.23	0.23	
	Generator Terminal Voltage	N/A	6.33	5.53	4.15	4.07	
Natural Gas Generator Pmax	N/A	N/A	N/A	N/A	N/A		

Table A.1: EI Heavy Summer Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Natural Gas Generator Pmax (Severe)	N/A	N/A	N/A	N/A	N/A	
Dynamics	Generators without Models	1.62	1.96	2.26	2.37	2.98	
	Generators with Classical Models	0.26	0.25	0.28	0.27	0.27	
	Netted Generators with Models	0.26	0.64	0.47	0.37	2.51	
	Netted Generators	3.58	2.65	2.79	2.48	0.18	
	Inconsistent Reactance	0.23	0.24	0.82	1.05	1.06	
	Unacceptable Models	N/A	11.83	11.81	13.17	12.36	
	Not Recommended Models	N/A	23.56	21.09	19.87	18.29	
	User-Written Models ³⁵	N/A	N/A	-	-	-	
	Inconsistent Time Constants	0.11	0.11	0.13	0.09	0.07	
	Unreasonable Inertia Constants	8.04	8.44	8.06	7.77	8.18	
	Unreasonable Saturation Factors	22.22	10.76	11.00	11.09	12.00	
	Severe Saturation Factors	0.94	0.81	0.90	0.90	1.02	
	PSS but no Excitation	0.11	0.06	0.10	0.06	0.06	
	Inconsistent Speed Damping	3.33	3.13	2.22	2.28	2.52	
	Inconsistent Lead-Lag Time Constant	1.64	2.06	1.82	1.90	1.94	
	Erroneous Power Dev Fractions	1.02	1.27	1.20	3.48	3.81	
	DC Exciter Self-Excitation Errors	10.34	10.58	12.83	13.40	13.56	
	Inconsistent Type III Wind Speeds	0.00	0.00	0.00	0.00	0.00	
	Suspect PSS2A/2B parameters	16.41	16.69	17.01	18.54	17.56	
	Incorrect DER_A Tripping Parameters	N/A	0.00	0.00	0.00	0.00	
Second Generation Renewable Model Parameterization	N/A	N/A	N/A	17.57	21.87		

³⁵ Performance not tracked

Table A.2: EI Heavy Winter Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
Powerflow	P _{max} Exceedances	0.31	0.10	0.02	0.03	0.02	
	P _{min} Exceedances	0.08	0.16	0.02	0.00	0.00	
	Scheduled Interchange Sum	0	0	0	0	0	
	Thermal Overloads	0.13	0.18	0.15	0.14	0.14	
	Thermal Overloads (Severe)	0.11	0.14	0.12	0.11	0.11	
	Low Emergency Rating	0.00	0.00	0.03	0.02	0.02	
	High Emergency Rating	0.03	0.00	0.00	0.00	0.00	
	Voltage Schedule Conflicts	31	16	36	107	118	
	Tap Step Conflicts	0.07	0.07	0.16	0.17	0.18	
	Tap Step Conflicts (Severe)	0.02	0.00	0.09	0.09	0.06	
	Generator Reactive at Limits	18.35	17.99	14.48	17.01	16.77	
	Generator Reactive Limit Power Factor	11.28	11.14	8.54	2.46	7.17	
	Positive Sequence TX Circulating Current	0.00	0.00	0.00	0.00	0.00	
	Poor Load Power Factor	0.27	0.24	0.25	0.27	0.43	
	Generator Reactive Capability Curve	N/A	0.00	0.00	0.00	0.05	
	Generator R _{source} :X _{source} Ratio	0.00	0.00	0.05	0.05	0.16	
	X/R Ratio Check	N/A	0.26	0.24	0.23	0.00	
	Generator Terminal Voltage	N/A	7.75	4.50	5.28	4.13	
	Natural Gas Generator Pmax	N/A	N/A	N/A	N/A	N/A	
Natural Gas Generator Pmax (Severe)	N/A	N/A	N/A	N/A	N/A		
Dynamics	Gens without Models	1.72	2.07	2.39	2.59	3.21	
	Gens with Classical Models	0.25	0.27	0.28	0.27	0.28	
	Netted Generators	4.07	2.45	2.17	2.09	1.81	
	Netted Generators with Models	0.23	0.71	0.26	0.34	0.21	
	Inconsistent Reactance	0.23	0.27	0.64	1.10	1.05	
	Unacceptable Models	N/A	13.87	10.33	13.15	12.26	
	Not Recommended Models	N/A	23.48	20.94	19.69	18.15	
	User-Written Models ³⁶	N/A	N/A	-	-	-	
Inconsistent Time Constants	0.11	0.11	0.13	0.09	0.12		

³⁶ Performance not tracked

Table A.2: EI Heavy Winter Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Unreasonable Inertia Constants	8.11	8.49	8.07	7.76	8.12	
	Unreasonable Saturation Factors	22.19	10.75	10.99	11.12	11.95	
	Severe Saturation Factors	0.94	0.81	0.91	0.90	1.01	
	PSS but no Excitation	0.11	0.06	0.10	0.06	0.06	
	Inconsistent Speed Damping	3.33	3.12	2.22	2.28	2.51	
	Inconsistent Lead-Lag Time Constant	1.63	2.16	1.81	1.88	1.93	
	Erroneous Power Dev Fractions	1.36	1.27	1.20	3.48	3.77	
	DC Exciter Self-Excitation Errors	10.54	10.77	12.59	13.43	13.40	
	Inconsistent Type III Wind Speeds	0.00	0.00	0.00	0.00	0.00	
	Suspect PSS2A/2B parameters	16.51	16.67	17.32	18.63	17.60	
	Incorrect DER_A Tripping Parameters	N/A	0.00	0.00	0.00	0.00	
	Second Generation Renewable Model Parameterization	N/A	N/A	N/A	18.57	24.22	

Table A.3: EI Light Spring Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
Powerflow	P _{max} Exceedances	0.11	0.06	0.17	0.00	0.00	
	P _{min} Exceedances	0.06	0.21	0.11	0.05	0.00	
	Scheduled Interchange Sum	0	0	0.001	0	0	
	Thermal Overloads	0.06	0.07	0.05	0.04	0.04	
	Thermal Overloads (Severe)	0.05	0.06	0.05	0.03	0.03	
	Low Emergency Rating	0.00	0.00	0.02	0.02	0.03	
	High Emergency Rating	0.03	0.00	0.00	0.00	0.00	
	Voltage Schedule Conflicts	32	13	38	70	117	
	Tap Step Conflicts	0.06	0.06	0.16	0.17	0.18	
	Tap Step Conflicts (Severe)	0.02	0.00	0.09	0.09	0.07	
	Generator Reactive at Limits	23.62	20.87	19.64	16.98	18.56	
	Generator Reactive Limit Power Factor	13.65	13.65	9.29	2.44	8.32	

Table A.3: EI Light Spring Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Positive Sequence TX Circulating Current	0.00	0.00	0.00	0.00	0.00	
	Poor Load Power Factor	0.38	0.38	0.35	0.28	0.41	
	Generator Reactive Capability Curve	N/A	0.00	0.00	0.00	0.00	
	Generator $R_{source} \cdot X_{source}$ Ratio	0.00	0.00	0.08	0.08	0.15	
	X/R Ratio Check	N/A	0.25	0.24	0.23	0.23	
	Generator Terminal Voltage	N/A	13.51	6.07	6.09	14.05	
	Natural Gas Generator Pmax	N/A	N/A	N/A	N/A	N/A	
	Natural Gas Generator Pmax (Severe)	N/A	N/A	N/A	N/A	N/A	
Dynamics	Generators without Models	1.68	1.81	2.36	2.62	2.86	
	Generators with Classical Models	0.26	0.23	0.28	0.26	0.27	
	Netted Generators	5.40	2.75	2.06	2.21	2.12	
	Netted Gens with Models	0.24	1.05	0.31	0.73	0.23	
	Inconsistent Reactances	0.24	0.25	0.82	1.06	1.06	
	Unacceptable Models	N/A	13.95	11.86	13.23	17.59	
	Not Recommended Models	N/A	23.79	21.15	19.95	48.00	
	User-Written Models ³⁷	N/A	N/A	-	-	-	
	Inconsistent Time Constants	0.11	0.11	0.13	0.09	0.07	
	Unreasonable Inertia Constants	8.01	8.32	8.01	7.80	8.18	
	Unreasonable Saturation Factors	22.12	10.78	11.04	10.99	11.95	
	Severe Saturation Factors	0.94	0.81	0.91	0.91	1.02	
	PSS but no Excitation	0.11	0.06	0.11	0.07	0.06	
	Inconsistent Speed Damping	3.35	3.12	2.23	2.29	2.52	
	Inconsistent Lead-Lag Time Constant	1.64	2.08	1.83	1.92	2.22	
	Erroneous Power Dev Fractions	1.02	1.09	1.21	3.49	4.09	
	DC Exciter Self-Excitation Errors	10.27	10.58	12.84	13.45	13.57	
Inconsistent Type III Wind Speeds	0.00	0.00	0.00	0.00	0.00		

³⁷ Performance not tracked

Table A.3: EI Light Spring Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Suspect PSS2A/2B parameters	17.85	17.73	18.09	19.55	18.85	
	Incorrect DER_A Tripping Parameters	N/A	0.00	0.00	0.00	0.00	
	Second Generation Renewable Model Parameterization	N/A	N/A	N/A	17.31	21.63	

Texas Interconnection

Table A.4: TI Heavy Summer Peak Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
Powerflow	P _{max} Exceedances	0.00	0.00	0.00	0.11	0.00	
	P _{min} Exceedances	0.00	0.00	0.00	0.00	0.08	
	Scheduled Interchange Sum	0	0	0	0	-	
	Thermal Overloads	0.13	0.06	0.10	0.24	0.25	
	Thermal Overloads (Severe)	0.10	0.04	0.04	0.23	0.25	
	Low Emergency Rating	0.00	0.00	0.00	0.00	0.00	
	High Emergency Rating	0.02	0.03	0.00	0.02	0.02	
	Voltage Schedule Conflicts	0	5	47	31	47	
	Tap Step Conflicts	3.21	0.07	1.33	3.66	3.57	
	Tap Step Conflicts (Severe)	0.00	0.00	0.00	0.00	0.00	
	Generator Reactive at Limits	14.11	6.37	6.78	8.52	13.90	
	Generator Reactive Limit Power Factor	11.11	13.73	31.83	9.36	9.30	
	Positive Sequence TX Circulating Current	0.00	0.00	0.00	0.00	0.00	
	Poor Load Power Factor	0.11	0.13	0.06	0.02	0.05	
	Generator R _{source} ·X _{source} Ratio	0.00	0.13	0.00	0.42	0.62	
	X/R Ratio Check	N/A	0.43	0.44	0.34	0.42	
	Generator Terminal Voltage	N/A	1.92	0.30	0.58	0.00	
	Generator Reactive Capability Curve	N/A	0.00	0.00	0.00	0.00	
	Natural Gas Generator P _{max}	N/A	N/A	N/A	N/A	N/A	
	Natural Gas Generator P _{max} (Severe)	N/A	N/A	N/A	N/A	N/A	

Table A.4: TI Heavy Summer Peak Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
Dynamics	Generators without Models	4.07	5.20	2.52	2.88	1.79	
	Generators with Classical Models	1.55	2.15	0.00	1.22	1.09	
	Netted Gens with Models	0.00	0.00	0.00	0.00	0.30	
	Netted Generators	0.14	0.00	0.00	0.00	0.30	
	Inconsistent Reactances	1.25	0.62	1.07	1.31	1.13	
	Unacceptable Models	N/A	2.96	2.10	1.85	1.42	
	Not Recommended Models	N/A	24.37	21.77	20.09	17.08	
	User-Written Models ³⁸	N/A	N/A	-	-	-	
	Inconsistent Time Constants	0.42	0.40	0.79	0.73	0.69	
	Unreasonable Inertia Constants	11.30	14.01	15.31	16.40	18.86	
	Unreasonable Saturation Factors	20.12	13.17	12.82	13.55	13.13	
	Severe Saturation Factors	1.45	1.20	1.18	1.65	1.55	
	PSS but no Excitation	0.00	0.00	0.00	0.00	0.00	
	Inconsistent Speed Damping	3.78	3.10	2.82	2.91	2.92	
	Inconsistent Lead-Lag Time Constant	0.00	0.00	0.00	0.00	0.00	
	Erroneous Power Dev Fractions	0.00	0.00	0.00	2.44	7.84	
	DC Exciter Self-Excitation Errors	11.67	12.50	13.46	11.31	10.53	
	Inconsistent Type III Wind Speeds	0.00	0.00	0.00	0.00	0.00	
	Suspect PSS2A/2B parameters	12.5	16.92	14.07	16.21	17.87	
	Incorrect DER_A Tripping Parameters	N/A	0.00	0.00	0.00	0.00	
Second Generation Renewable Model Parameterization	N/A	N/A	N/A	N/A	N/A		

Table A.5: TI Heavy Wind Light Load Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
Powerflow	P _{max} Exceedances	0.00	0.00	0.00	0.17	0.12	
	P _{min} Exceedances	0.00	0.00	0.37	0.00	0.00	

³⁸ Performance not tracked.

Table A.5: TI Heavy Wind Light Load Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Scheduled Interchange Sum	0	0	0	0	0	
	Thermal Overloads	0.25	0.05	0.03	0.17	0.26	
	Thermal Overloads (Severe)	0.18	0.04	0.01	0.13	0.24	
	Low Emergency Rating	0.00	0.00	0.00	0.00	0.00	
	High Emergency Rating	0.02	0.03	0.00	0.02	0.18	
	Voltage Schedule Conflicts	0	12	62	43	79	
	Tap Step Conflicts	3.21	0.00	1.60	3.01	3.57	
	Tap Step Conflicts (Severe)	0.00	0.00	0.00	0.00	0.00	
	Generator Reactive at Limits	17.34	12.59	14.01	9.16	4.88	
	Generator Reactive Limit Power Factor	12.39	7.82	7.84	6.53	7.20	
	Positive Sequence TX Circulating Current	0.00	0.00	0.00	0.00	0.00	
	Poor Load Power Factor	0.20	0.19	0.06	0.05	0.09	
	Generator $R_{source} \cdot X_{source}$ Ratio	0.00	0.21	0.00	0.68	0.83	
	X/R Ratio Check	N/A	0.43	0.43	0.34	0.42	
	Generator Terminal Voltage	N/A	0.00	0.00	0.76	0.93	
	Generator Reactive Capability Curve	N/A	0.00	0.00	0.00	0.00	
	Natural Gas Generator Pmax	N/A	N/A	N/A	N/A	N/A	
	Natural Gas Generator Pmax (Severe)	N/A	N/A	N/A	N/A	N/A	
Dynamics	Generators without Models	6.62	8.55	2.93	3.08	1.79	
	Generators with Classical Models	1.55	1.43	0.00	1.22	1.09	
	Netted Gens with Models	0.00	0.00	0.38	0.00	0.41	
	Netted Generators	0.22	0.00	0.38	0.00	0.41	
	Inconsistent Reactances	1.25	1.23	1.07	1.31	1.13	
	Unacceptable Models	N/A	2.79	2.11	1.85	1.42	
	Not Recommended Models	N/A	24.68	21.67	20.09	17.08	
	User-Written Models ³⁹	N/A	N/A	N/A	N/A	N/A	
	Inconsistent Time Constants	0.41	0.39	0.79	0.73	0.69	
	Unreasonable Inertia Constants	11.30	13.98	15.31	16.40	18.85	

³⁹ Performance not tracked.

Table A.5: TI Heavy Wind Light Load Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Unreasonable Saturation Factors	20.12	13.19	12.85	13.55	13.12	
	Severe Saturation Factors	1.45	1.18	1.19	1.65	1.55	
	PSS but no Excitation	0.00	0.00	0.00	0.00	0.00	
	Inconsistent Speed Damping	3.78	3.07	2.82	2.91	2.92	
	Inconsistent Lead-Lag Time Constant	0.00	0.00	0.00	0.00	0.00	
	Erroneous Power Dev Fractions	0.00	0.00	0.00	2.44	7.84	
	DC Exciter Self-Excitation Errors	11.67	12.5	13.46	11.32	10.52	
	Inconsistent Type III Wind Speeds	0.00	0.00	0.00	0.00	0.00	
	Suspect PSS2A/2B parameters	12.5	16.92	14.07	16.21	17.87	
	Incorrect DER_A Tripping Parameters	N/A	0.00	0.00	0.00	0.00	
	Second Generation Renewable Model Parameterization	N/A	N/A	N/A	0.00	0.00	

Table A.6: TI Second Summer Peak Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
Powerflow	P _{max} Exceedances	0.00	0.00	0.00	0.11	0.00	
	P _{min} Exceedances	0.00	0.00	0.00	0.00	0.00	
	Scheduled Interchange Sum	0	0	0	0	0	
	Thermal Overloads	0.22	0.04	0.05	0.29	0.25	
	Thermal Overloads (Severe)	0.15	0.04	0.04	0.25	0.23	
	Low Emergency Rating	0.00	0.00	0.00	0.00	0.00	
	High Emergency Rating	0.02	0.03	0.00	0.02	0.02	
	Voltage Schedule Conflicts	0	23	37	39	37	
	Tap Step Conflicts	3.35	0.94	1.40	3.60	3.45	
	Tap Step Conflicts (Severe)	0.00	0.80	0.00	0.00	0.00	
	Generator Reactive at Limits	16.24	9.14	16.28	13.37	20.91	
	Generator Reactive Limit Power Factor	10.97	13.35	12.59	9.15	9.30	
	Positive Sequence TX Circulating Current	0.00	0.00	0.00	0.00	0.00	
	Poor Load Power Factor	0.11	0.13	0.04	0.02	0.05	

Table A.6: TI Second Summer Peak Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Generator $R_{source} \cdot X_{source}$ Ratio	0.00	0.13	0.00	0.43	0.61	
	X/R Ratio Check	N/A	0.43	0.44	0.34	0.42	
	Generator Terminal Voltage	N/A	0.00	0.30	0.29	0.67	
	Generator Reactive Capability Curve	N/A	0.00	0.00	0.00	0.00	
	Natural Gas Generator Pmax	N/A	N/A	N/A	N/A	N/A	
	Natural Gas Generator Pmax (Severe)	N/A	N/A	N/A	N/A	N/A	
Dynamics	Generators without Models	3.94	5.19	3.35	3.26	1.79	
	Gens with Classical Models	1.55	1.43	0.00	1.21	1.09	
	Netted Gens with Models	0.00	0.00	0.24	0.00	0.29	
	Netted Generators	0.14	0.00	0.24	0.00	0.29	
	Inconsistent Reactances	1.25	1.23	1.07	1.31	1.15	
	Unacceptable Models	N/A	2.72	2.10	1.85	1.42	
	Not Recommended Models	N/A	24.57	21.76	20.09	16.79	
	User-Written Models ⁴⁰	N/A	N/A	-	-	-	
	Inconsistent Time Constants	0.41	0.39	0.79	0.73	0.69	
	Unreasonable Inertia Constants	11.30	13.98	15.31	16.40	18.86	
	Unreasonable Saturation Factors	20.12	13.21	12.85	13.55	13.13	
	Severe Saturation Factors	1.45	1.18	1.19	1.65	1.55	
	PSS but no Excitation	0.00	0.00	0.00	0.00	0.00	
	Inconsistent Speed Damping	3.78	3.07	2.82	2.91	2.92	
	Inconsistent Lead-Lag Time Constant	0.00	0.00	0.00	0.00	0.00	
	Erroneous Power Dev Fractions	0.00	0.00	0.00	2.44	6.78	
	DC Exciter Self-Excitation Errors	11.67	12.50	13.46	11.32	10.52	
	Inconsistent Type III Wind Speeds	0.00	0.00	0.00	0.00	0.00	
	Suspect PSS2A/2B parameters	12.5	16.92	14.07	16.21	20.38	
	Incorrect DER_A Tripping Parameters	N/A	0.00	0.00	0.00	0.00	

⁴⁰ Performance not tracked.

Table A.6: TI Second Summer Peak Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Second Generation Renewable Model Parameterization	N/A	N/A	N/A	0.00	0.00	

Western Interconnection

Table A.7: WI Heavy Summer Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
Powerflow	P _{max} Exceedances	0.03	0.00	0.23	0.28	0.37	
	P _{min} Exceedances	0.03	0.03	0.32	0.21	0.26	
	Scheduled Interchange Sum	0	0.0	-0.0	0.0	0.0	
	Voltage Schedule Conflicts	80	63	55	58	64	
	Tap Step Conflicts	0.66	0.72	0.62	0.54	0.26	
	Tap Step Conflicts (Severe)	0.10	0.45	0.05	0.07	0.06	
	Low Emergency Rating	0.13	0.40	0.37	0.03	0.02	
	High Emergency Rating	0.02	0.01	0.01	0.01	0.00	
	Thermal Overloads	0.01	0.01	0.05	0.07	0.06	
	Thermal Overloads (Severe)	0.00	0.00	0.04	0.05	0.04	
	Generator Reactive at Limits	6.53	4.84	5.50	5.19	6.65	
	Generator Reactive Limit Power Factor	25.11	28.35	10.06	9.78	4.73	
	Positive Sequence TX Circulating Current	0.00	0.00	0.00	0.00	9.46	
	Poor Load Power Factor	0.04	0.07	0.05	0.05	0.04	
	Generator R _{source} :X _{source} Ratio	0.21	0.05	0.05	0.09	0.17	
	Generator Terminal Voltage	N/A	3.90	6.03	7.24	0.0	
	Generator Reactive Capability Curve	N/A	0.00	3.47	0.00	2.63	
	X/R Ratio Check	N/A	0.18	0.19	0.19	1.38	
	Natural Gas Generator Pmax	N/A	72.30	84.13	79.67	75.74	
Natural Gas Generator Pmax (Severe)	N/A	5.94	4.35	6.41	3.89		
Dynamics	Generators without Models	4.73	4.89	6.69	7.16	8.06	
	Netted Gens with Models	0.20	1.07	0.16	0.34	0.18	
	Netted Generators	2.01	3.57	3.22	3.98	5.03	

Table A.7: WI Heavy Summer Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Generators with Classical Models	0.00	0.00	0.00	0.00	0.00%	
	Unacceptable Models	N/A	4.19	3.73	3.23	7.78%	
	Not Recommended Models	N/A	11.93	10.88	9.13	5.95%	
	User-Written Models ⁴¹	N/A	N/A	-	-	0.01%	
	Inconsistent Reactances	3.34	3.54	3.24	3.35	0%	
	Inconsistent Time Constants	5.96	5.87	5.74	6.16	6.33%	
	Unreasonable Inertia Constants	13.03	13.06	11.90	11.69	10.25%	
	Unreasonable Saturation Factors	27.08	19.74	19.00	19.14	16.92%	
	Severe Saturation Factors	6.86	6.65	6.12	5.91	5.45%	
	PSS but no Excitation	0.39	0.00	0.72	0.76	1.98%	
	Inconsistent Speed Damping	8.23	7.22	7.24	7.04	6.74%	
	Inconsistent Lead-Lag Time Constant	1.86	2.49	2.48	3.11	5.39%	
	Erroneous Power Dev Fractions	3.74	2.91	2.69	2.73	1.89%	
	DC Exciter Self-Excitation Errors	5.78	4.98	5.34	5.75	5.76%	
	Inconsistent Type III Wind Speeds	0.00	1.27	1.32	0.00	0%	
	Suspect PSS2A/2B parameters	4.19	3.52	3.16	3.74	3.15%	
	Incorrect DER_A Tripping Parameters	N/A	0.00	0.00	0.00	0.0%	
	Second Generation Renewable Model Parameterization	N/A	N/A	N/A	31.13	36.35%	

Table A.8: WI Heavy Winter Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
Powerflow	P _{max} Exceedances	0.08	0.08	0.55	0.44	0.44	
	P _{min} Exceedances	0.35	0.41	0.59	0.33	0.33	
	Scheduled Interchange Sum	0.0	0	-0.0	0.0	0.0	
	Voltage Schedule Conflicts	77	63	54	64	64	
	Tap Step Conflicts	0.62	0.61	0.57	0.34	-0.34	

⁴¹ Performance not tracked.

Table A.8: WI Heavy Winter Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Tap Step Conflicts (Severe)	0.06	0.06	0.06	0.08	-0.08	
	Low Emergency Rating	0.27	0.14	0.35	0.35	-0.35	
	High Emergency Rating	0.04	0.02	0.03	0.02	-0.02	
	Thermal Overloads	0.00	0.01	0.02	0.04	-0.04	
	Thermal Overloads (Severe)	0.00	0.00	0.02	0.01	-0.01	
	Generator Reactive at Limits	5.82	3.81	4.69	5.06	6.97	
	Generator Reactive Limit Power Factor	12.31	27.41	10.28	9.58	3.72	
	Positive Sequence TX Circulating Current	0.00	0.00	0.00	0.00	9.58	
	Poor Load Power Factor	0.06	0.06	0.13	0.04	0.04	
	Generator $R_{source} \cdot X_{source}$ Ratio	0.28	0.16	0.11	0.20	0.20	
	Generator Terminal Voltage	N/A	3.90	6.18	10.15	N/A	
	Generator Reactive Capability Curve	N/A	0.00	3.37	0.00	2.56	
	X/R Ratio Check	N/A	0.18	0.19	0.20	2.50	
	Natural Gas Generator Pmax	N/A	N/A	N/A	N/A	N/A	
	Natural Gas Generator Pmax (Severe)	N/A	N/A	N/A	N/A	N/A	
Dynamics	Gens without Models	5.15	4.38	8.26	7.87	7.87	
	Netted Gens with Models	0.20	0.40	0.20	0.23	0.23	
	Netted Generators	1.43	2.00	2.93	3.30	3.30	
	Generators with Classical Models	0.00	0.00	0.00	0.00	0.00	
	Unacceptable Models	N/A	4.66	3.38	2.48	2.62	
	Not Recommended Models	N/A	12.36	10.18	6.59	2.80	
	User-Written Models ⁴²	N/A	N/A	-	-	0.30	
	Inconsistent Reactances	3.35	3.32	3.52	3.45	0	
	Inconsistent Time Constants	5.84	6.02	6.15	6.49	7.87	
	Unreasonable Inertia Constants	13.10	13.32	12.48	11.86	9.88	
	Unreasonable Saturation Factors	27.09	19.75	19.85	19.13	16.66	
	Severe Saturation Factors	6.97	6.70	6.39	5.83	5.61	
	PSS but no Excitation	0.34	0.11	0.66	0.98	2.62	

⁴² Performance not tracked.

Table A.8: WI Heavy Winter Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Inconsistent Speed Damping	8.51	7.03	7.19	6.87	2.80	
	Inconsistent Lead-Lag Time Constant	1.82	2.59	2.39	3.27	3.27	
	Erroneous Power Dev Fractions	3.67	2.86	3.26	2.69	2.69	
	DC Exciter Self-Excitation Errors	6.98	5.86	5.88	5.08	5.80	
	Inconsistent Type III Wind Speeds	0.00	0.00	1.52	0.00	0	
	Suspect PSS2A/2B parameters	4.01	3.95	4.05	3.71	3.71	
	Incorrect DER_A Tripping Parameters	N/A	0.00	0.00	0.00	0	
	Second Generation Renewable Model Parameterization	N/A	N/A	N/A	34.66	34.62	

Table A.9: WI Light Summer Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
Powerflow	P_{max} Exceedances	0.00	0.19	0.14	0.08	0.42	
	P_{min} Exceedances	0.00	0.05	0.87	0.25	1.34	
	Scheduled Interchange Sum	0	0.0	-0.0	0.0	0.0	
	Voltage Schedule Conflicts	75	62	56	58	0.61	
	Tap Step Conflicts	0.61	0.45	0.60	0.53	0.33	
	Tap Step Conflicts (Severe)	0.07	0.06	0.07	0.07	0.07	
	Low Emergency Rating	0.14	0.39	0.37	0.03	0.12	
	High Emergency Rating	0.03	0.02	0.01	0.01	0.01	
	Thermal Overloads	0.01	0.01	0.01	0.04	0.05	
	Thermal Overloads (Severe)	0.00	0.00	0.01	0.01	0.01	
	Generator Reactive at Limits	6.76	5.99	5.67	5.43	7.01	
	Generator Reactive Limit Power Factor	25.24	28.43	10.60	9.94	4.74	
	Positive Sequence TX Circulating Current	0.00	0.00	0.00	0.00	9.94	
	Poor Load Power Factor	0.03	0.06	0.08	0.08	0.06	
	Generator $R_{source}:X_{source}$ Ratio	0.21	0.05	0.05	0.09	.22	

Table A.9: WI Light Summer Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Generator Terminal Voltage	N/A	7.30	4.74	5.20	0.00	
	Generator Reactive Capability Curve	N/A	0.00	2.18	0.00	2.39	
	X/R Ratio Check	N/A	0.17	0.19	0.19	4.52	
	Natural Gas Generator Pmax	N/A	N/A	N/A	N/A	N/A	
	Natural Gas Generator Pmax (Severe)	N/A	N/A	N/A	N/A	N/A	
Dynamics	Generators without Models	4.79	4.96	6.84	7.30	8.46	
	Netted Gens with Models	0.12	0.40	0.29	0.32	0.74	
	Netted Generators	1.76	2.94	2.83	3.46	6.08	
	Generators with Classical Models	0.00	0.00	0.00	0.00	0.00	
	Unacceptable Models	N/A	4.17	3.79	3.41	2.37	
	Not Recommended Models	N/A	11.85	10.82	9.11	2.48	
	User-Written Models ⁴³	N/A	N/A	-	-	0.21	
	Inconsistent Reactances	3.33	3.55	3.24	3.44		
	Inconsistent Time Constants	5.95	5.88	5.74	2.86	6.33	
	Unreasonable Inertia Constants	13.16	13.01	12.00	10.95	9.84	
	Unreasonable Saturation Factors	27.15	19.72	19.39	13.57	19.96	
	Severe Saturation Factors	6.85	6.68	6.35	1.67	5.45	
	PSS but no Excitation	0.45	0.28	0.55	0.00	0.54	
	Inconsistent Speed Damping	8.22	7.19	7.24	10.12	6.74	
	Inconsistent Lead-Lag Time Constant	1.85	2.48	2.47	3.55	3.47	
	Erroneous Power Dev Fractions	3.74	2.90	3.21	1.49	1.89	
	DC Exciter Self-Excitation Errors	5.83	5.22	5.53	7.08	5.76	
	Inconsistent Type III Wind Speeds	0.00	1.28	1.27	0.00	0	
	Suspect PSS2A/2B parameters	4.19	3.76	3.17	3.75	3.26	
Incorrect DER_A Tripping Parameters	N/A	0.00	0.00	0.00	0		

⁴³ Performance not tracked.

Table A.9: WI Light Summer Cases

Type of Metric	Metric	2018 Score (%)	2019 Score (%)	2020 Score (%)	2021 Score (%)	2022 Score (%)	Performance
	Second Generation Renewable Model Parameterization	N/A	N/A	N/A	30.72	35.49	

Standing Committee Coordination Group (SCCG) Update

Action

Information

Summary

Per the SCCG scope document, the SCCG is to “provide quarterly reports to the standing committees for inclusion in their public Agenda posting on cross-cutting initiatives addressing risks to the reliability, security, and resilience of the BPS. This report shall be prepared in advance and voted on by the SCCG at the SCCG’s quarterly meetings.”

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standing Committees Coordinating Group (SCCG) Quarterly Report

July 29, 2022

Third Quarter Update

RELIABILITY | RESILIENCE | SECURITY



Compliance and Certification Committee (CCC)

Chair: Scott Tomashefsky Vice-Chair: Silvia Parada Mitchell

Purpose: The CCC will engage, support, and advise the NERC Board and NERC Management regarding all facets of the NERC Compliance Monitoring and Enforcement Program, and Organization Registration and Certification Programs and specific elements of the Reliability Standards Development Process.

Top Priorities for SCCG Discussion:

- Evaluating Success of Triage Process
- Incorporating Agility into CMEP Efforts
- Optimizing CMEP Tools
- Maximizing Value of Stakeholder Feedback for ERO Enterprise

What information/guidance/support is needed from another committee?

- RSTC (Risk Tool Selection ((Guideline, SAR, White Papers, etc.)))
- SC (Joint Standards Grading Task Force, SER collaboration)
- All Committees (Stakeholder Perception Feedback input)
- RISC (Feedback loops for risk reliability priorities)

Recent Risk Identification, Mitigation, Monitoring Activity

- Continued support of ERO Program Alignment topics, including
 - Implementation Guidance
 - CMEP Practice Guide Reviews
 - Align Tool
- Inform development of risk-based standards and shape compliance oversight
- Stakeholder Perception Feedback
 - Q2 Focused Discussion
 - Compliance Guidance Policy

Upcoming Risk Identification, Mitigation, Monitoring Activity

- Stakeholder Perception Feedback Plan
 - Q3 Focused Discussion
 - Compliance Oversight Plans
 - COVID-19 Lessons Learned
- Internal Audits / CCC engagement
- CMEP Practice Guide Review
- Align User Group Meeting
- ORCS Collaboration on Development of ERO 102 and focus group participation related to Functional Mapping
- Understanding Federal/Provincial Governance within ERO Enterprise

Personnel Certification Governance Committee (PCGC)

Chair: Cory Danson Vice-Chair: Michael B. Hoke

Purpose: The PCGC shall be to provide oversight to the policies and processes used to implement and maintain the integrity and independence of NERC's System Operator Certification Program.

Top Priorities for SCCG Discussion:

- Credential Maintenance Research Project in progress with final presentation August 2022
- Review findings to determine what changes to incorporate into the certification and credential maintenance programs

What information/guidance/support is needed from another committee?

- N/A

Recent Risk Identification, Mitigation, Monitoring Activity

- N/A

Upcoming Risk Identification, Mitigation, Monitoring Activity

- N/A

Reliability Issues Steering Committee (RISC)

Chair: Brian Slocum Vice-Chair: Adrienne Collins

Purpose: The RISC is an advisory committee that triages and provides front-end, high-level leadership and accountability for nominated issues of strategic importance to bulk power system reliability.

Top Priorities for SCCG Discussion: Will begin looking at options for the January 2023 Leadership Summit. The agenda will be discussed on July 28, and the survey for next year will also be discussed as an item that will be sent out in the 4th quarter this year.

What information/guidance/support is needed from another committee?

- RSTC and RISC may need to review the status of the cold weather inquiry items as some of the sub teams may have taken a different direction from what was initially discussed in the tiger teams.
- As the Leadership Summit preparation unfolds, we will probably need input on executive panelists to speak on each of the topics.

Recent Risk Identification, Mitigation, Monitoring Activity

- The RISC will begin working with MRO on their risk prioritization model for input.

Upcoming Risk Identification, Mitigation, Monitoring Activity

- RISC will be releasing an industry survey later this year, and will begin preparing for the Leadership Summit.
- RISC will collaborate with RSTC
- Smaller teams are beginning to meet with NERC staff on the risk prioritization and the reliability indicators.

Reliability and Security Technical Committee (RSTC)

Chair: Greg Ford Vice-Chair: Rich Hydzik

Purpose: The RSTC strives to advance the reliability and security of the BPS by creating a forum for ideas and interests to support the ERO's mission, and leveraging such expertise to identify solutions to study, mitigate, and/or eliminate emerging risks.

Top Priorities for SCCG Discussion:

- Continue to monitor progress on RSTC work plan
- Prioritize and incorporate RISC Report and Cold Weather Report recommendations into RSTC work plan
- Incorporate metrics into Reliability Guidelines

What information/guidance/support is needed from another committee?

- **CCC** – Participate in the SCTF as needed.
- **PCGC** – N/A
- **RISC** – Evaluated RISC Report recommendations for risk mitigation activities by the RSTC subgroups. Will continue to monitor work plan progress and reassess progress in early 2023.
- **SC** - IRPS will revise a proposed SAR on EOP-004 revisions for RSTC endorsement in September. For the TOCC Field Test plan, we will continue coordination of the field test with the Standard Drafting Team.

Recent Risk Identification, Mitigation, Monitoring Activity

- Approved *GMD Monitoring Reference Document, Reliability Coordinator Reliability Plan Reference Document* and three *White Papers: BPS Reliability Perspectives for Distributed Energy Resource Aggregators, Recommendations for Simulation Improvement and Techniques Related to DER Planning AND FERC RM22-3: Internal Network Security Monitoring - NERC Security Working Group Whitepaper*
- Endorsed two SARs from the ERATF and one SAR from the IRPS

Upcoming Risk Identification, Mitigation, Monitoring Activity

- Facility Ratings Task Force will schedule a kick-off meeting in July
- Tranche 1 of revised Reliability/Security Guidelines (including effectiveness metrics) are due in September for approval.
- EGWG will request approval of *Design Basis Criteria for a Natural Gas Study* at the September meeting
- RSTC will initiate annual review of subgroups at the September meeting
- Gathering comments on GADS Section 1600 data request for subsequent RSTC approval.

Standards Committee (SC)

Chair: Amy Casuscelli Vice-Chair: Todd Bennett

Purpose: The SC oversees the development of NERC Reliability Standards as its members review actions to ensure the standards development process is being followed.

Top Priorities for SCCG Discussion:

- 2022 Periodic Reviews - Standards Efficiency Review
- Standards Process Improvements

What information/guidance/support is needed from another committee?

- CCC – Participate and support standards efficiency review as needed in tandem with the SCPS SER project.
- PCGC – N/A
- RISC – N/A
- RSTC – Increased awareness of SAR development process through standing agenda item on SC agenda. Fuel Assurance SAR outreach and discussion.

Recent Risk Identification, Mitigation, Monitoring Activity

- Low Impact project posted for ballot and comment
- Many projects posting related to IRPTF standard revisions recommendations
- Accepted two ERATF SARs to address energy assurance with energy-constrained resources
- Accepted the Generator Ride-Through Standard (PRC-024-3 Replacement) SAR

Upcoming Risk Identification, Mitigation, Monitoring Activity

- Cold Weather upcoming project posting
- Virtualization upcoming project posting
- Standards process improvements



North American Generator Forum RSTC Update

Wayne Sipperly
Executive Director - North American Generator Forum
wsipperly@generatorforum.org
December 7, 2022

NAGF Mission



The NAGF mission is to promote the safe, reliable operation of the generator segment of the bulk electric system through generator owner and operator collaboration with grid operators and regulators.

Agenda



- **NERC Standard Projects**
- **Areas of Focus**
- **Participation and Coordination**
- **NAGF 2022 Annual Meeting**

➤ NERC Standard Projects



➤ NERC Standards Projects

- The NAGF is actively engaged in the following NERC Projects to help ensure the generator sector perspective is heard and understood:
 - NERC Project 2017-01: Modifications to BAL-003
 - NERC Project 2019-04: Modifications to PRC-005
 - NERC Project 2020-02: Modifications to PRC-024
 - NERC Project 2020-06: Verifications of Models and Data for Generators
 - NERC Project 2021-02: Modifications to VAR-002
 - NERC Project 2021-04: Modifications to PRC-002
 - NERC Project 2021-07: Extreme Cold Weather Ops
 - NERC Project 2021-08: Modifications to FAC-008
 - NERC Project 2022-02: Modifications to TPL-001 and MOD-032
 - NERC Project 2022-03: Energy Assurance w Energy-Constrained Resources

Areas of Focus



- NERC Project 2021-07 – Phase II
- Facility Ratings
- 2022 Reliability Issues Steering Committee (RISC) Emerging Risks Survey
- Generator CIP Low Impact Procedures update

Participation and Collaboration



- NERC Quarterly MRC/BOT Meeting November 2022
 - NAGF Policy Input
 - NAGF 2022 Fall Activities Summary

- DOE funding declined for development of Hydro Generation focused Resilience Maturity Model (HY-RMM) with Pacific Northwest National Laboratory (PNNL). The NAGF continues to explore future collaboration opportunities with PNNL.

NAGF 2022 Annual Meeting



➤ NAGF Annual Meeting

- Held October 11th (1/2 day pm), 12th (full day) and 13th (1/2 day am) at the NERC offices in Atlanta, GA
 - Format: In-Person w remote attendance option
- Conference focus: Generator Reliability and Resiliency
- Keynote Speakers:
 - NERC Senior Vice President and E-ISAC CEO Manny Cancel
 - TexasRE President/CEO Jim Albright
 - Topics:
 - ✓ Generator Modeling Standards
 - ✓ Future Energy Mix
 - ✓ Facility Ratings Best Practices
 - ✓ Cold Weather Standards
 - ✓ Low Impact Criteria Review White Paper

Q & A



Thank you!

www.GeneratorForum.org



Community

Confidentiality

Candor

Commitment

NATF Report to NERC RSTC December 7, 2022

Roman Carter, NATF

Open Distribution

Copyright © 2022 North American Transmission Forum. Not for sale or commercial use. All rights reserved.

NATF Interfaces with the ERO

On reliability, resiliency, security and safety topics

- Promote improvement in these areas
- Reduce duplication of effort - limited industry resources

Meet periodically with ERO leadership to discuss topics and activities.

- Most recently held coordination call on November 3rd
- Topics included: supply chain, Facility Ratings, Resilience Summit and NERC RSTC Strategic Plan

Facility Ratings Risk Construct

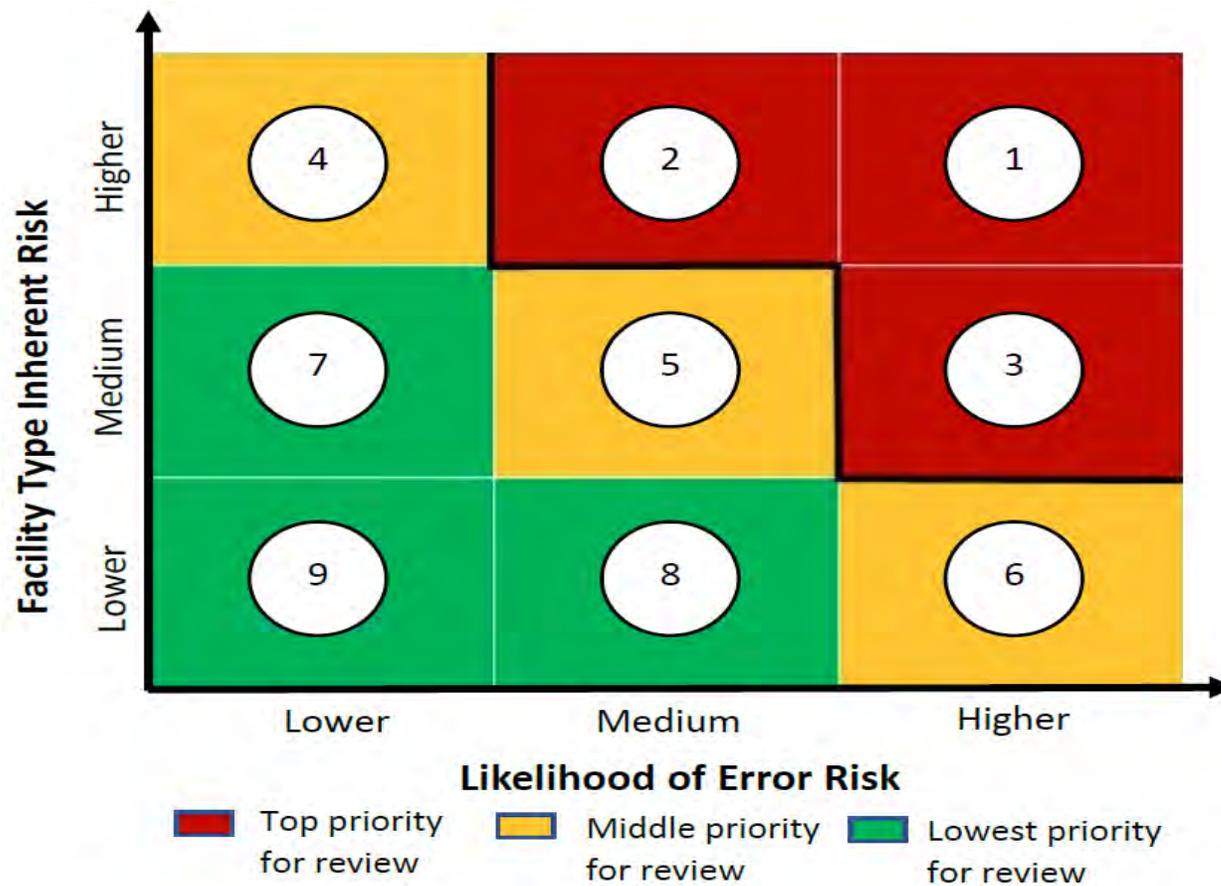
NATF members developed NATF Facility Ratings Practices Document

- Being implemented by membership (84% of total N. American transmission mileage at 100kV and above)

Recently developed a Facility Ratings “risk construct” that prioritizes implementation of practices

- Approved by NATF Board for industry use
- Establishes a baseline to inform the FR Task Force and the FAC-008 SAR drafting team of risk-focused efforts

Likelihood of Error Risk



Public Operating Experience Report

Recently posted a new operating experience (OE) report of our public website to help improve industry safety, reliability, and resilience; Most recent report covered:

- Improper Guy Anchor Installations
- Correlates to locations with difficult conditions like rock, hard soil, or steep terrain
- Project management team will work with identified contractors to assess the scope/extent of condition and develop/implement mitigation plans
- New metrics developed to assist in identifying high-risk structures

FERC 881 Ambient-Adjusted Ratings

The NATF continues to work with its members to prepare for the implementation of FERC Order 881 (“Managing Transmission Line Ratings”)

- Requires the use of ambient-adjusted ratings for most transmission lines by July 11, 2025.
- NATF’s FERC Order 881 Working Group is
 - Defining the problems that need to be solved
 - Assessing ongoing efforts in the industry, and, where appropriate,
 - Initiating projects to allow members to share information and develop solutions



North American Transmission Forum External Newsletter

October 2022

Facility Ratings Risk Construct

The “NATF Risk Construct for Prioritizing Facility Ratings Reviews” document has been posted for industry use on the [NATF public website](#). This document supplements the publicly posted “Key NATF Practices for Facility Ratings” document¹ by providing a risk-based approach for prioritizing implementation of the practices, specifically baseline and periodic reviews to confirm ongoing accuracy of ratings and effective operation of controls.

Given the magnitude of performing comprehensive reviews of all facilities, Transmission Owners likely need to implement via a phased, prioritized approach. A good starting point is to conduct a review of a limited sample of facilities, evaluate the results, and, if necessary, expand the sample for review. This is best accomplished by initially targeting facilities with higher risk to BES reliability or higher likelihood for facility ratings error and continuing until all facilities have been reviewed. The NATF risk construct aids that approach.

FERC Order 881 (Ambient-Adjusted Ratings)

The NATF continues to work with its members to prepare for the implementation of FERC Order 881 (“Managing Transmission Line Ratings”), which requires the use of ambient-adjusted ratings for most transmission lines by July 11, 2025.

As the order will have a significant impact on NATF members and other industry utilities, the NATF has formed a multidisciplinary group to help members make the technical and process changes that are necessary to implement the order. The NATF’s FERC Order 881 Working Group is defining the problems that need to be solved, assessing ongoing efforts in the industry, and, where appropriate, initiating projects to allow members to share information and develop solutions.

Recently, NATF staff briefed FERC staff from the Office of Energy Policy Innovation and Office of Electric Reliability on the NATF’s approach to assisting our members through the FERC Order 881 response project.

Redacted Operating Experience Reports

We recently posted a new operating experience report to the “[Documents](#)” section of our public site for members and other utilities to use internally and share with their contractors to help improve safety, reliability, and resilience.

For more information about the NATF, please visit <https://www.natf.net/>.

¹ a summary of the NATF member-confidential practices for facility ratings and how the practices address the issues and align with the controls identified by the ERO Enterprise in the November 1, 2019, ERO Facility Ratings Problem Statement