NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Metrics Primers

August, 2019

RELIABILITY | RESILIENCE | SECURITY




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

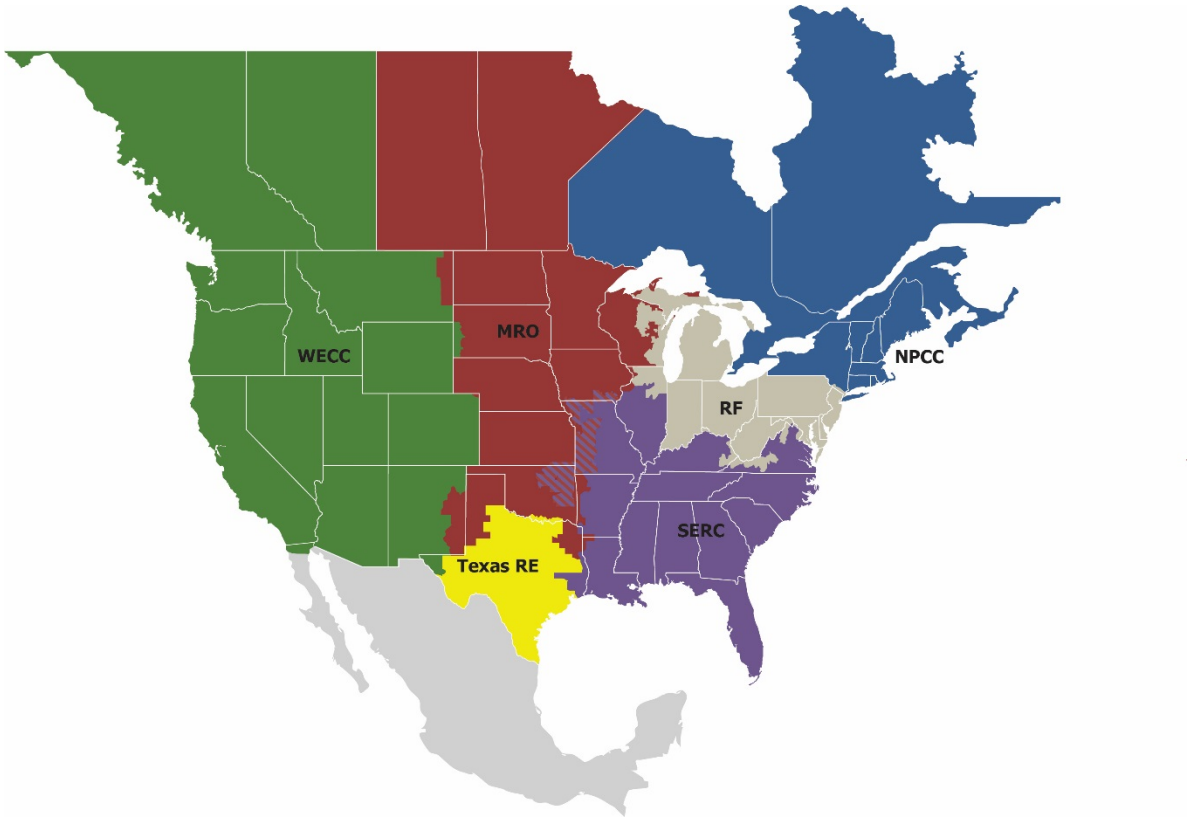
Table of Contents

Preface

*Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. T*he vision for the ERO Enterprise, which is comprised of the NERC and the six Regional Entities, is a highly reliable and secure North American bulk power system. 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 divided into 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 Region 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	Western Electricity Coordinating Council

Metric 1: (Fewer, Less Severe Events) Primer

The ERO Event Analysis Process (EAP) defines certain categories of events that meet a threshold considered significant enough to capture lessons learned that can inform risk monitoring and mitigation of daily operations on the BPS. Quantifying the potential impact of these events improves the global risk picture of BPS operation. This metric is one way to acknowledge proportional contributions from generation and transmission to loss of load.

The daily event severity risk index (eSRI) is a composite daily measure of the load loss due to transmission and/or generation resources on the BPS. It is calculated for each event on a given day with a cumulative value of all events assigned to the day. The index uses weighted load loss, transmission loss, and generation loss based on importance to risk. The eSRI equation is as follows:

$$eSRI=1000 * (RPL * w_L * (MW_L) + w_T * (N_T)+ w_G * N_G)$$

Where:
w_L = 60%, weighting factor load loss
w_T = 30%, weighting factor transmission lines lost
w_G = 10%, weighting factor generators lost

MW_L = normalized MW of Load Loss in percent,
N_T = normalized number of transmission lines lost in percent,
N_G = normalized number of generators lost in percent,
RPL = load Restoration Promptness Level:
RPL = 1/3, if restoration < 4 hours,
RPL = 2/3, if 4 <= restoration < 12 hours,
RPL = 3/3, if restoration >=12 hours

A linear regression is performed by using a rolling five-year period of daily eSRI calculations in an effort to describe the correlation of event occurrence with any given day on the operating the system. The regression line provides a means to predict the average value for a chosen date of the eSRI. A lower eSRI is considered more favorable so it follows that it is most favorable to maintain a flat to negative slope of the regression line—fewer events with less overall severity occur. Confidence intervals (95%) are calculated in an effort to provide assurance that event occurrence based on the sample defined by the EAP category definitions statistically characterizes the true population of event occurrences associated with operating the BPS. Statistically significant changes to the sample are identified and evaluated if the regression line and bounding confidence intervals all become positive.

A status modification of the risk indicator is driven by the direction of the regression line as follows:

- Falling slope indicates increasing performance (green).
- Flat slope indicates neutral (white).
- Rising slope indicates decreasing performance (red).

The EAP provides a mechanism to influence improved system performance. The program captures lessons learned for sharing throughout the industry and trending of system performance. Performance trending supports identifying the need for potential action(s) (e.g., a NERC alert), informs reports (e.g., the annual *State of Reliability* report), or may initiate the need for the development/revisions of Reliability Standards. The outcomes from event analysis and cause coding assignment help to inform the BPS industry in a way that facilitates improved reliability of daily operations and thus the maintenance of a falling slope for the eSRI curve.

Metric 1 supports the following RISC identified risk profiles (ERO Reliability Risk Priorities, February 2018):

- Risk Profile #1: Changing Resource Mix
- Risk Profile #2: Bulk-Power System Planning
- Risk Profile #3: Resource Adequacy and Performance
- Risk Profile #5: Human Performance and Skilled Workforce
- RISC Profile #6: Loss of Situational Awareness
- Risk Profile #8: Physical Security Vulnerabilities
- Risk Profile #9: Cybersecurity Vulnerabilities

Data Source: The Event Analysis Management System (TEAMS).

Metric 2: Compliance Violations

Maintaining compliance with the NERC Reliability Standards is one of the key components of risk management. Metric 2: Compliance Violations reflects the registered entities' efforts to maintain compliance with the standards as a means to reduce risk to the BPS reliability. In majority of reported violations, there has been no actual harm to the BPS reliability.

The three subsets of Metric 2 are the following:

- The count of moderate and serious risk noncompliance filed[1]
- The count of violations discovered through self-reports[2]
- The percentage of three-year rolling average of serious risk violations that have been filed compared to the total noncompliance that has been reported[3]

The Compliance Monitoring and Enforcement Program (CMEP) quarterly report provides more insight about these three subsets and includes additional information for clarity and context.

2019 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan also describes how identified risks from various resources, such as the Reliability Issues Steering Committee (RISC) identified risk profiles (ERO Reliability Risk Priorities, February 2018), are translated into risk elements that are used in the reshaping of the annual monitoring plan. In that respect, this metric supports all nine risk profiles within the compound of reliability standards, listed here:

- Risk Profile #1: Changing Resource Mix
- Risk Profile #2: Bulk-Power System Planning
- Risk Profile #3: Resource Adequacy and Performance
- Risk Profile #4: Increasing Complexity in Protection and Control Systems
- Risk Profile #5: Human Performance and Skilled Workforce
- Risk Profile #6: Loss of Situational Awareness
- Risk Profile #7: Extreme Natural Events
- Risk Profile #8: Physical Security Vulnerabilities
- Risk Profile #9: Cybersecurity Vulnerabilities

[1] Enforcement filings and postings https://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx
[2] Data source: NERC Compliance Reporting and Tracking System
[3] *Supra fn 1*

Metric 3: Protection System Misoperations Rate Primer

The method used to score the sub metrics below is centered on comparing yearly datasets over a five-year moving period. An appropriate (pooled or unpooled) t-test determines if a statistically significant difference in annual means exists. A status modification of the risk indicator for each sub metric is driven by statistically significant changes in annual means tested at the 0.05 significance level (with 95% confidence) that is determined from a moving year-to-year comparison of the applicable sub metric value during each reporting period/year.

Baseline / Starting Window	
Period	**Reporting Period**
5	2018
4	2017
3	2016
2	2015
1	2014

A score for each pair of compared years is determined as follows. A score of zero indicates no statistically significant change between means for compared years. If a statistically significant difference is established between years, then the difference in means between the current year and the compared year are evaluated, and a score of one or minus one is assigned. A score of one indicates that the current year applicable sub metric is less than the compared year. A score of minus one indicates that the current year applicable sub metric is greater than the compared year. The scores for all compared years within the five-year window of the applicable sub metric are added together (four of the five years) and a value is assigned as a total score. The risk indicator for each sub metric is modified according to the definitions in the table below.

Risk Indicator Scoring		
Total Score	**Definition**	**Risk Indicator**
Positive sum/total	Sum of compared period scores is positive.	Green
0	No statistically significant change to compared periods.	White
Negative sum/total	Sum of compared period scores is negative.	Red

Sub metric 3a: Annual Misoperations Rate

The protection systems misoperations rate metric provides the performance of protection systems (both generator and transmission) on the BPS. The Misoperations Information Data Analysis System (MIDAS) collects counts of protection system operations and details on the misoperation events of protection systems from registered entities.

The data for this metric is reported quarterly (60 days after the end of each quarter) and requires all four quarters to compute. This metric will only be updated in the Q3 dashboard each year.

Calculation: The metric is calculated as the ratio of misoperations to total protection system operations, both at the region level and overall for NERC.

Regional Entities offer interactive webinars and workshops to provide entities with information on protection system operations and misoperations. Additionally, valuable lessons learned are published from events that occur on the system involving misoperations. Detailed data reporting instructions and other reference materials have been developed to improve consistency in reporting and are available on the Misoperations page of the NERC website: https://www.nerc.com/pa/RAPA/Pages/Misoperations.aspx

This metric supports the following RISC identified risk profiles (ERO Reliability Risk Priorities, February 2018):

- Risk Profile #4: Increasing Complexity in Protection and Control Systems
- Risk Profile #5: Human Performance and Skilled Workforce
- Risk Profile #7: Extreme Natural Events

Data Source: Misoperation Information Data Analysis System (MIDAS).

Sub metric 3b: Cumulative Loss of Load for Events with Misoperations

The ERO EAP defines certain categories of events that meet a threshold considered significant enough to capture lessons learned that can inform risk monitoring and mitigation of daily operations on the BPS. Quantifying the potential impact of these events improves the global risk picture of operating the BPS. This metric is one way to acknowledge impactful contributions from unintended or incorrect protective system operations to total load loss for qualified/categorized events on the system.

The baseline/starting window for this sub metric was established using year-to-previous quarter (as of April 1, 2019) datasets that are essentially flat with no statistically significant difference when compared to each other.

The cause coding assignment process (CCAP) provides a mechanism to influence improved system performance based on reporting from the EAP. The CCAP is designed to identify contributing causes and root causes for use in trending BPS performance if possible. The outcomes from the CCAP help the ERO inform industry in a way that facilitates improved reliability of daily operations and by extension improve operating conditions such that the potential for having a load loss event as a result of a misoperation(s) is reduced. The ERO informs industry through a variety of communications, including reports, alerts, messages, lessons learned, and webinars.

This sub metric supports the following RISC identified risk profiles (ERO Reliability Risk Priorities, February 2018):

- RISC Profile #4: Increasing Complexity in Protection and Control Systems (ERO Reliability Risk Priorities, February 2018).

Data Source: The Event Analysis Management System (TEAMS).

Metric 4: Events Caused by Natural-Gas-Fired Unit Forced Outages Due to Cold Weather or Natural Gas Unavailability

Sub Metric 4a: No Firm Load Loss Due to Natural-Gas-Fired Unit Outages during Cold Weather
The annual measurement for no firm load loss due to natural-gas-fired unit outages during cold weather will be captured for immediate forced outages occurring during the months of January, February, March, and December of the same calendar year.

This metric captures immediate firm load loss on forced unit outages for natural-gas-fired units during cold weather months. It will be captured using energy emergency alerts (EEA3), OE-417 and EOP-004 reports and will be reported on a quarterly basis for the annual report.

Sub metric 4b: No Firm Load Loss Due to Natural Gas Unavailability
The annual measurement for no firm load loss on natural-gas-fired generation units due to natural gas unavailability metric. This metric will be capture natural-gas-fired unit unavailability for the entire calendar year.

This metric captures immediate firm load loss on forced natural gas units due to natural gas unavailability across the entire year. This metric will be captured with EEA3s, OE-417, and EOP-004 reports and will be reported on a quarterly basis for the annual report.

Situation Awareness (SA) allows for an opportunity to analyze information on system disturbances and other incidents that impact the North American BPS. SA also allows for dissemination of information to internal departments, registered entities, regional organizations, and other stakeholders within the industry as necessary. Trending and early detection of events within the first 24–48 hours allows for sustained events to be shared with the events analysis team for further monitoring and analysis as needed to ensure the safe, reliable operation of the BES. Early detection of events is also shared with the RA group for input into the *State of Reliability* report and NERC alerts if deemed necessary. The outcome of increased situation awareness helps inform the industry of potential trends and impacts on the BES and provides improved reliability of the daily operation of the BES during extreme weather and other impactful events maintaining the Green status on the indicator.

Sub metric 4c: Percentage of Winter Period Net MWh of Potential Production Lost Due to Natural-Gas-Fired Unit Outages during Cold Weather
This metric calculates the amount of potential production loss due to the immediate forced outages and derates of natural gas units due to cold weather. The data for this metric is reported quarterly, 45 days after the end of each quarter. Due to the seasonal nature of this metric, it will only be updated in the Q1 and Q2 dashboards each year.[4]

Calculation: The Net Available Capacity of each gas unit is multiplied by the duration of the immediate forced outage or derate event for the unit and compared to total potential production of available gas units for the months of January, February, March, and December of the same calendar year. The current year is compared to the five-year rolling average of the same months.

Training materials and data reporting instructions provide details to increase quality of the causes of forced outages due to cold weather. The ERO Enterprise conducts training, outreach, and education annually to support generating in combating cold weather outages.

[4] In the Q1 dashboard, all cold weather months of the previous calendar year data will be reported. In the Q2 dashboard, only the cold weather months of January through March of the current year will be reported.

Sub metric 4d: Percentage of Annual Net MWh of Potential Production Lost Due to Natural Gas Unavailability Compared to a Five-Year Rolling Average

This metric calculates the amount of potential production loss due to the immediate forced outages or derates of natural gas units due to lack of fuel for an operating year. The operating year for this metric is defined as Q3 of the previous year through Q2 of the current year. The data for this metric is reported quarterly, 45 days after the end of each quarter, and requires all four quarters to compute. This metric will only be updated in the Q3 dashboard each year.

Calculation: The Net Available Capacity of each gas unit is multiplied by the duration of the immediate forced outage or derate event for the unit and compared to total potential production of gas units for the period. The current operating year is compared to the five-year rolling average.

Improved descriptions and examples of cause codes associated with fuel availability are being added to the data reporting instructions to provide clarification on appropriate use of these cause codes.

This metric supports the following RISC identified risk profiles (ERO Reliability Risk Priorities, February 2018):

- Risk Profile #1: Changing Resource Mix
- Risk Profile #2: Bulk Power System Planning
- Risk Profile #3: Resource Adequacy and Performance
- Risk Profile #7: Extreme Natural Events

Data Source: EOP-004, OE-417 and Energy Emergency Alerts (EEA3) (4a, b).

Data Source: Generating Availability Data System (GADS) (4c,d).

Metric 5a/b: Reduce AC Transmission Line Forced Outages

Sub Metric 5a: Operator or Other Human Performance Issues

Calculations:

Outages per circuit: This metric is calculated as the number of transmission line outages caused by Human Error divided by the total inventory of circuits, resulting in the number of outages per circuit. The metric year number of outages per circuit is compared to a five-year rolling average.

Statistical significance: Changes over the five-year period will be evaluated for statistical significance.

The data for this metric is reported quarterly, 45 days after the end of each quarter, and requires a complete year of data. This metric will only be updated on the Q3 dashboard each year.

Improved descriptions and scenarios associated with human performance are included in the data reporting instructions and training materials to provide clarification on appropriate use of these cause codes. The ERO Enterprise conducts training, outreach, and education annually to support the industry in the area of human performance and human and organizational error reduction.

This sub metric supports the following RISC identified risk profiles (ERO Reliability Risk Priorities, February 2018):

- Risk Profile #5: Human Performance and Skilled Workforce
- Risk Profile #7: Extreme Natural Events

Data Source: Transmission Availability Data System (TADS).

Sub Metric 5b: Substation Equipment Failures or Failed AC Circuit Equipment

Calculations:

Outages per circuit: This metric is calculated as the number of transmission line outages caused by AC substation equipment failures (such as transformers) and failed AC circuit equipment divided by the total inventory of circuits, resulting in the number of outages per circuit. The number of outages per circuit for the metric year is compared to a three-year rolling average.

Statistical significance: Changes over the three-year period will be evaluated for statistical significance.

The data for this metric is reported quarterly, 45 days after the end of each quarter, and requires a complete year of data. This metric will only be updated on the Q3 dashboard each year.

Improved descriptions and scenarios associated with equipment failures are included in the data reporting instructions and training materials to provide clarification on appropriate use of these cause codes. Additionally, valuable lessons learned are published from events that occur on the system involving equipment failure and associated shortcomings.

This sub metric supports the following RISC identified risk profiles (ERO Reliability Risk Priorities, February 2018):

- Risk Profile #4: Increasing Complexity in Protection and Control Systems

- Risk Profile #5: Human Performance and Skilled Workforce
- Risk Profile #7: Extreme Natural Events

Data Source: Transmission Availability Data System (TADS).

Metric 5c: Vegetation Encroachment

Ineffective vegetation management was identified as a major cause of the August 14, 2003, blackout and was also cited as a major causal factor in other large-scale North American outages. The ERO Enterprise has observed an increase in FAC-003-3 R2 violations that result in vegetation contacts. These violations result from vegetation management programs that have less than adequate procedures to address identified problems or that fail to adapt to changing conditions (e.g., increased precipitation that accelerates vegetation growth).

Metric 5c monitors the number of sustained outages from vegetation fall-ins into the transmission right-of-way (not a violation of standard but required periodic data reporting per FAC-003) and vegetation encroachments into the minimum vegetation clearance distance (MVCD) observed, including those in real time, absent a sustained outage (violation of reliability standards)[5].

FAC-003 is one of the standards included in ERO's current and past CMEP annual implementation plan that also is related to several risk profiles, such as Risk Profile #7: Extreme Natural Events, Risk Profile #5: Human Performance and Skilled Workforce, and Risk Profile #2: Bulk Power System Planning.

The CMEP quarterly report also includes a section that discusses reported vegetation-related sustained outages.

The number of vegetation-related outages from encroachments into the MVCD has been very small, and the outage duration has been very short in all cases. While the goal is to have no vegetation encroachments into the MVCD, NERC monitors the potential issues that reported for FAC-003 to ensure that both vegetation-related sustained outages from inside and outside of the right-of-way remain within one standard deviation.

[5] Vegetation Management Reports https://www.nerc.com/pa/comp/CE/Pages/vegetation-management-reports.aspx

Metric 6: (Unauthorized Physical or Electronic Access) Primer

2019 ERO Enterprise dashboard Metric 6: Unauthorized Physical or Electronic Access "measures risk and impact to the BPS from cyber or physical security attacks." The measurement is based on industry submissions of the mandatory NERC Event Reporting (EOP-004) and Department of Energy Electric Emergency Incident and Disturbance Report (OE-417) forms. The measurement variable is the number of disruptions of BES facilities due to cyber attacks or physical attacks. For the purposes of this metric, "disruption means that a BES Facility was removed from service as a result of the cyber or physical incident."

The term "cyber and physical attacks" is not defined for the purpose of this metric, but it is understood to broadly include any reported occurrences generally involving physical security or cyber security. The metric's clarification of the term "disruption" still leaves room for interpretation, and it is understood here to be limited to a BES facility removed from service by automatic or manual means either as a direct result of the attack or as an immediate operational mitigation of the attack's effects. Future controlled or planned outages for inspection or repairs are not considered to be a disruption for the purpose of this metric, since by definition the system can be operated appropriately around constraints imposed by planned outages.

While the metric's understanding is inconsistent with how many security professionals define "attack," this larger aperture allows the E-ISAC to review all submissions of the two reports to understand the reported issue and the impact to the BES while working in close coordination with NERC's BPS Awareness (BPSA) group. The E-ISAC also receives and reviews voluntary event reports, but these voluntary reports are not included in this metric.

This metric supports the following RISC identified risk profiles (ERO Reliability Risk Priorities, February 2018):

- Risk Profile #8: Physical Security Vulnerabilities
- Risk Profile #9: Cybersecurity Vulnerabilities

Metric 7: Disturbance Control Standard Events

The purpose of Metric 7, Disturbance Control Standard (DCS) Events, is to measure risk to the BPS by monitoring the trend in the number of DCS events that are greater than the most severe single contingency (MSSC). DCS events are "Balancing Contingency Events" as defined in the *NERC Glossary of Terms* and the BAL-002-3 Reliability Standard. The MSSC for a Balancing Authority (BA) or reserve sharing group (RSG) is also defined in the *NERC Glossary of Terms* and the BAL-002-3 standard. DCS events occur at the BA or RSG level. MSSCs are also specific to and determined by the BA or RSG annually in accordance with BAL-002-3. The magnitude in which the DCS Event exceeded the BA's (or RSG's) MSSC is unknown.

The Metric performance is determined by the statistical significance of the slope of a linear regression line, tested at the significance level of 5% for quarterly DCS events > MSSC for a rolling 28 quarters (seven years).

The DCS data used for evaluation of Metric 7 is obtained from BAs and RSGs via voluntary quarterly submittals that are requested by the fifteenth day following the end of each quarter. The data is reviewed and compiled by the NERC Resources Subcommittee (RS) and presented at their quarterly meetings that occur in the third week following the end of each quarter. When BAs fail to submit data on time, the RS representatives perform outreach to those BAs. Due to the timing in BA data submittals and compilation by the RS, the metric is updated one quarter in arrears.

Metric 7 is evaluated on a quarterly basis to determine an annual result using the aforementioned measurement method.

Success **(green)** is achieved when the linear regression line of the most recent seven years of quarterly DCS events > MSSC has a statistically significant negative slope. The neutral grade (white) occurs when the slope of the time trend is statistically neither increasing nor decreasing. Failure **(red)** occurs if slope of the time trend is increasing with statistical significance.

Metric 8: Interconnection Frequency Response

Metric 8, Interconnection Frequency Response, measures risk and impact to the BPS by evaluating interconnection frequency response measure (IFRM) performance for each frequency event selected for BAL-003-1 compliance as compared to the interconnection frequency response obligation (IFRO).

IFROs are calculated for each Interconnection and recommended in the *Frequency Response Annual Analysis* (FRAA) report for Reliability Standard BAL-003-1.1 implementation. The *FRAA* report is presented each year to the NERC RS for approval and then to the NERC Operating Committee for endorsement. IFRM performance is measured for each BAL-003 frequency event by comparing the resource (or load) MW loss to the frequency deviation using the method below. The unit for frequency response is MW / 0.1 Hz.

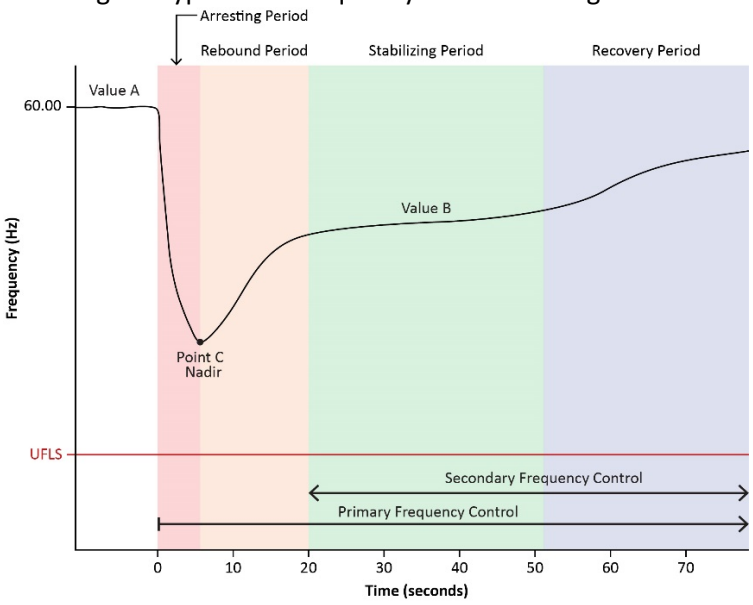
$$IFRM(A-B) = \frac{MW\ Loss}{10\ x\ \Delta f(A-B)}$$

Where: MW Loss = Loss of generating resource (or load)

f_A *= Starting frequency*

f_B *= Average frequency from 20 to 52 seconds after the start of the event*

Below is a frequency graph showing the typical low frequency event resulting from the loss of a generation resource.



Candidate frequency events are reviewed quarterly by the NERC Frequency Working Group (FWG) and events are selected based on Interconnection-specific criteria defined in the BAL-003-1.1 standard and supporting documents.

Metric 8 is evaluated on a quarterly basis to determine an annual result. The IFRM for each BAL-003-1 frequency event is compared to the respective Interconnection's IFRO.

Success **(green)** is achieved when no Interconnection experienced a BAL-003-1 event where IFRM performance was less than their respective IFRO. Failure **(red)** occurs if IFRM performance for any single event is below the respective IFRO. Due to the timing in selection of events the metric is updated one quarter in arrears.