NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

ERO Enterprise Endorsed Implementation Guidance

NERC Operating Committee Compliance Implementation Guidance
Data Exchange Infrastructure and Testing Requirements

January 8, 2021

RELIABILITY | ACCOUNTABILITY

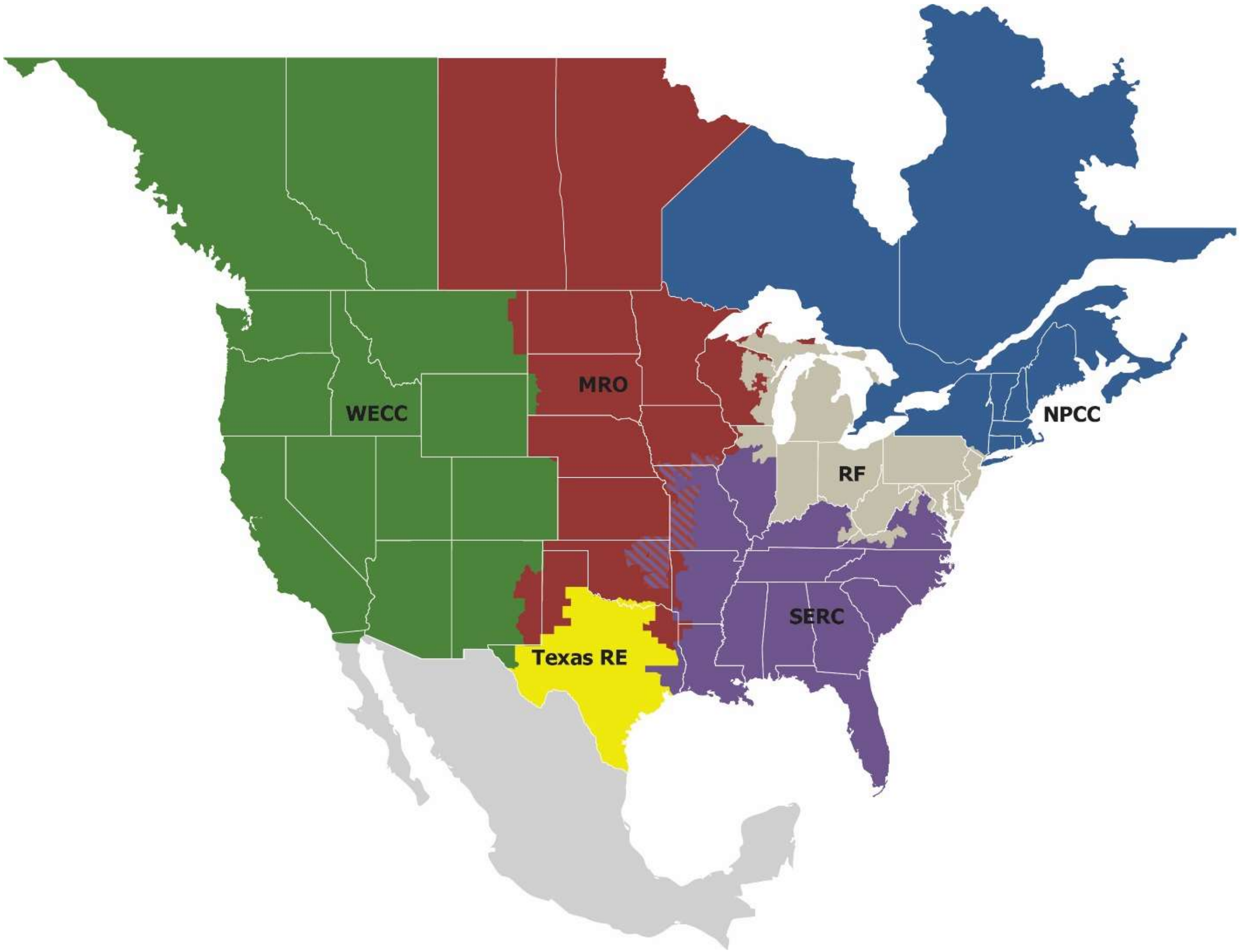
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (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.

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

Chapter 1: Background

1.1 Preamble

Implementation Guidance provides examples or approaches to illustrate how registered entities could comply with standards that are vetted by industry and endorsed by the ERO Enterprise. The examples provided in this Implementation Guidance are not all inclusive, as there are likely other methods for complying with a particular standard requirement. The ERO Enterprise's endorsement of an example means the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) staff will give these examples deference when conducting compliance monitoring activities. Registered entities can rely upon the example and be reasonably assured that compliance with the requirements can be met with the understanding that final compliance determinations will depend on individual facts, circumstances, and system configurations. [1]

- Guidance documents cannot change the scope or purpose of the requirements of a standard.
- The contents of this guidance document are not the only way to comply with a standard.
- Compliance expectations should be made as clear as possible through the standards development process, which should minimize the need for guidance after final ballot approval of a standard.
- Forms of guidance should not conflict.
- Guidance should be developed collaboratively and posted on the NERC website for transparency.

1.2 Purpose

The purpose of this Implementation Guidance is to provide examples or approaches for redundant and diversely routed data exchange infrastructure within the primary Control Center[2] and associated tests for redundant functionality as required by NERC Reliability Standards TOP-001-4, Requirements R20, R21, R23, and R24 and IRO-002-5 Requirements R2 and R3, collectively referred to as "requirements in scope". Registered entities can rely on these examples and/or approaches and be reasonably assured that compliance with the requirements in scope can be met.

This Implementation Guidance provides:

- Examples of data exchange infrastructure reference models, with redundant and diverse routing, within the primary Control Center
- Examples of tests for redundant functionality that test primary Control Center data exchange capabilities

It is noted that the examples or approaches provided in this Implementation Guidance are not exclusive for meeting compliance with the requirements in scope and that, depending on an entity's individual circumstances, other ways, methods, or models exist to demonstrate compliance with the requirements in scope.

1.3 Applicable NERC Reliability Standards

The NERC Data Exchange Infrastructure Requirements Task Force (DEIRTF) developed this Implementation Guidance from the perspective of the Transmission Operator (TOP) for NERC Reliability Standard TOP-001-4 Requirements R20 and R21. The Implementation Guidance is also applicable to Balancing Authorities (BAs) through NERC Reliability Standard TOP-001-4 Requirements R23 and R24, and Reliability Coordinators (RCs) through NERC Reliability Standard IRO-002-5 Requirements R2 and R3, respectively. The NERC Reliability Standards and Requirements applicable to this Implementation Guidance are listed below:

[1] Source: http://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.pdf

[2] Glossary of Terms Used in NERC Reliability Standards https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

TOP-001-4
R20. *Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the TOP's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and Real-time Assessments.*

R21. *Each Transmission Operator shall test its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days. If the test is unsuccessful, the Transmission Operator shall initiate action within two hours to restore redundant functionality.*

R23. *Each Balancing Authority shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Balancing Authority's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Transmission Operator, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and analysis functions.*

R24. *Each Balancing Authority shall test its primary Control Center data exchange capabilities specified in Requirement R23 for redundant functionality at least once every 90 calendar days. If the test is unsuccessful, the Balancing Authority shall initiate action within two hours to restore redundant functionality.*

IRO-002-5
R2. *Each Reliability Coordinator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Reliability Coordinator's primary Control Center, for the exchange of Real-time data with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, for performing its Real-time monitoring and Real-time Assessments.*

R3. *Each Reliability Coordinator shall test its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days. If the test is unsuccessful, the Reliability Coordinator shall initiate action within two hours to restore redundant functionality.*

1.4 Overview

RCs, BAs, and TOPs are responsible for monitoring, conducting several analyses, and taking appropriate action(s) to maintain the reliability of the BPS. Among other things, these activities include Real-time[2] monitoring and Real-time Assessments (RTA)[2].

The requirements in scope were developed to ensure that RCs, BAs, and TOPs do not have single points of failure in their data exchange infrastructure within their respective primary Control Centers that could adversely impact the flow of Real-time data and potentially render Real-time monitoring and RTA unreliable. This Implementation Guidance assists RCs, BAs, and TOPs in assessing which methods, practices, and information may be utilized to achieve compliance with the requirements in scope.

1.5 Commonly Used Terms Within This Implementation Guidance

The following terms used in this Implementation Guidance are not defined within or intended to be included in the NERC Glossary of Terms[2]. These definitions are provided to ensure a common industry understanding of how they are applied solely within this Implementation Guidance. Where available, references to industry standardized definitions have been provided.

Term	Definition
Data Exchange[3]	Project 2009-02: Real-time Monitoring and Analysis Capabilities Concept White Paper refers to data exchange as electronic exchange of data between two computer based control systems and assumes that the data links will utilize ICCP or an equivalent protocol. The concept paper also indicates that "data exchange, in this context, does not include RTUs or other similar types of DCUs. Required data sets to be exchanged are covered in proposed IRO-010-2 and TOP-003-2."
Data Exchange Infrastructure[4]	May include components such as, switches, routers, servers, power supplies, cabling and communication paths between these components in the primary Control Center for exchange of system operating data. Also includes the applicable infrastructure that connects the primary Control Center to its associated data center in the event that the data center is not located within the physical facility as the primary Control Center.
Inter-Control Center Protocol[5]	The Telecontrol Application Service Element (TASE.2) protocol, also known as the Inter-Control Center Communications Protocol (ICCP), allows for data exchange over Wide Area Networks (WANs) between a utility control center and other control centers, other utilities, power pools, regional control centers, and non-utility generators. Data exchange information consists of real-time and historical power system monitoring and control data, including measured values, scheduling data, energy accounting data, and operator messages. This data exchange occurs between one control center's Supervisory Control And Data Acquisition (SCADA)/Energy Management System (EMS)/Distribution Management System (DMS)/Generation Management System (GMS) host and another center's host, often through one or more intervening communications processors.

1.6 Scope

The requirements in scope focus on an entity's exchange of Real-time data with its RC, BA, and the entities it has identified it needs data from to perform its Real-time monitoring and RTA. The requirements in scope need the entity's data exchange capabilities for exchange of Real-time data with entities mentioned previously (RC, BA, and other entities it has identified it needs data from) to have data exchange infrastructure that is redundant and diversely routed within the entity's primary Control Center. The requirements in scope apply to the data exchange infrastructure within an entity's primary Control Center and do not extend to other control centers an entity may have, either to provide for backup functionality (as required by NERC Reliability Standard EOP-008-2[6]) or for other purposes.

While an entity may utilize internal or external sources for data to perform Real-time monitoring and RTA, the requirements in scope focus on the Real-time data the entity exchanges with other entities, namely, the entity's RC,

[3] Project 2009-02: Real-time Monitoring and Analysis Capabilities Concept White Paper https://www.nerc.com/pa/Stand/Project%20200902%20Realtime%20Reliability%20Monitoring%20and/Project_2009-02_rmacsdt_white_paper_021611.pdf

[4] NERC Reliability Standard TOP-001-4, Supplemental Material, Rationale for R20 and R21 https://www.nerc.com/pa/Stand/Reliability%20Standards/TOP-001-4.pdf

[5] International Standard, IEC 60870-6-503 – Telecontrol equipment and systems https://www.sis.se/api/document/preview/559181/

[6] NERC Reliability Standard EOP-008-2: Loss of Control Center Functionality https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-008-2.pdf

BA, and other entities it has identified it needs data from, to perform Real-time monitoring and RTA. This type of data exchange generally occurs through ICCP or an equivalent protocol. This Implementation Guidance does not apply to other types of data an entity may collect and utilize for Real-time monitoring and/or RTA.

Chapter 2: Data Exchange Infrastructure and Testing General Considerations

2.1 Data

As mentioned previously, the requirements in scope focus on the data an entity needs to perform Real-time monitoring and RTA. An entity should determine the data it needs to exchange exchanges with other entities, namely, the entity's RC, BA, and other entities it has identified it needs data from, to perform Real-time monitoring and RTA and the source(s) of such data. NERC Reliability Standards TOP-003-3[7] and IRO-010-2[8] require TOPs, BAs, and RCs to maintain a documented data specification for the data they need to perform Real-time monitoring and RTA. An entity can utilize its data specification from TOP-003-3 or IRO-010-2 to verify the data exchange required to perform Real-time monitoring and RTA. This Implementation Guidance does not apply to other types of data an entity may collect and utilize for Real-time monitoring and/or RTA.

2.2 Data Exchange Infrastructure and Capability

While there is no NERC definition for data exchange infrastructure or capability, NERC Reliability Standard TOP-001-4, Supplemental Material, Rationale[4] for Requirement R20 provides examples of data exchange infrastructure and indicates that data exchange infrastructure may include devices or components, such as, switches, routers, servers, power supplies, and network cabling and communication paths between components in the primary Control Center that are used for data exchange with the entity's RC, BA, and other entities it has identified it needs data from.

In general, data exchange infrastructure in the context of the requirements in scope does not include the following:

- An entity's devices or components (e.g., front end processors, application servers, etc.) that are not associated with ICCP or an equivalent protocol.
- Remote Terminal Units (RTUs) or other similar types of Data Collection Units (DCUs). Entities are not required to have redundant RTUs, DCUs, or similar type of field communication devices utilized for obtaining telemetry information.

Irrespective of whether an entity owns or maintains the equipment that constitutes its data exchange infrastructure within its primary Control Center, the entity should ensure there are no single points of failure within its primary Control Center that could halt the flow of Real-time data.

2.3 Redundancy and Diversity

TOP-001-4, Supplemental Material, Rationale[4] for Requirement R20 states:
"*Redundant and diversely routed data exchange capabilities consist of data exchange infrastructure components (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data) that will provide continued functionality despite failure or malfunction of an individual component within the Transmission Operator's (TOP) primary Control Center. Redundant and diversely routed data exchange capabilities preclude single points of failure in primary Control Center data exchange infrastructure from halting the flow of Real-time data. Requirement R20 does not require automatic or instantaneous fail-over of data exchange capabilities. Redundancy and diverse routing may be achieved in various ways depending on the arrangement of the infrastructure or hardware within the TOP's primary Control Center.*

The reliability objective of redundancy is to provide for continued data exchange functionality during outages, maintenance, or testing of data exchange infrastructure. For periods of planned or unplanned outages of individual

[7] NERC Reliability Standard TOP-003-3 https://www.nerc.com/pa/Stand/Reliability%20Standards/TOP-003-3.pdf
[8] NERC Reliability Standard IRO-010-2 https://www.nerc.com/pa/Stand/Reliability%20Standards/IRO-010-2.pdf

data exchange components, the proposed requirements do not require additional redundant data exchange infrastructure components solely to provide for redundancy.

Infrastructure that is not within the TOP's primary Control Center is not addressed by the proposed requirement."

In general, the requirements in scope focus on component failure or outages that can halt the flow of Real-time data within an entity's primary Control Center. Redundancy and diversity can be achieved by ensuring that no single component failure in the data exchange infrastructure within an entity's primary Control Center can halt the flow of Real-time data.

The requirements in scope do not directly contemplate specific physical criteria or distances to achieve diverse routing. Entities may choose to achieve diverse routing through physical or logical means. An entity applying a risk-based approach may consider the overall strategy of data exchange infrastructure setup within its primary Control Center in determining whether adequate redundancy and diversity in routing has been achieved to avoid single points of failure that could halt the flow of Real-time data.

2.4 Redundant Functionality Testing

TOP-001-4, Supplemental Material, Rationale[4] of Requirement R21 states:

"*A test for redundant functionality demonstrates that data exchange capabilities will continue to operate despite the malfunction or failure of an individual component (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center for the exchange of system operating data). An entity's testing practices should, over time, examine the various failure modes of its data exchange capabilities. When an actual event successfully exercises the redundant functionality, it can be considered a test for the purposes of the proposed requirement.*"

The requirements in scope do not identify specific components of an entity's data exchange infrastructure that need testing for redundant functionality. The tests for redundant functionality are highly dependent on an entity's data exchange infrastructure configuration. An entity applying a risk-based approach may evaluate whether simulating the failure or malfunction of a single component results in continued data exchange. In such situations (for example Figure 3), simulating the failure or malfunction of an individual component in one data exchange path will have tested the functionality of other components in the remaining available data exchange path(s). An entity applying a risk-based approach may assess and minimize risks associated with conducting redundant functionality tests, ensuring that adverse impacts to operations are minimized.

2.5 Testing Frequency and Schedule

The requirements in scope require entities to test primary Control Center data exchange capabilities for redundant functionality at least once every 90 calendar days. An entity must conduct a redundant functionality test within 90 calendar days of its most recent test (no more than 90 calendar days between tests).

To develop a testing plan that would examine various failure modes over time, an entity may identify different test scenarios and develop a schedule to conduct a redundant functionality test using one such scenario every 90 calendar days. An entity may repeat the same redundant functionality test every 90 calendar days if the entity can test several failure modes through a single test.

Chapter 3: Compliance Implementation Examples

This section provides a few data exchange infrastructure reference models that an entity can rely on and be reasonably assured that compliance with the requirements in scope can be achieved. These reference models do not contain all the complexities of a primary Control Center data exchange infrastructure setup and do not represent all methods or ways of achieving redundant and diversely routed data exchange infrastructure. It is noted that these reference models are not exclusive for meeting compliance with the requirements in scope and that, depending on an entity's individual circumstances, other ways, methods, or models exist to demonstrate compliance with the requirements in scope.

To help entities compare and contrast, this section also provides two data exchange infrastructure reference models that are not recommended. These reference models are clearly labelled "Not-Recommended" and identify the single point(s) of failure within the primary Control Center, as appropriate. The reference models are discussed in increasing order of complexity of the data exchange infrastructure configuration within an entity's primary Control Center.

3.1 Not-Recommended Data Exchange Infrastructure Reference Models

This section provides two examples of data exchange infrastructure reference models that are not recommended because these reference models contain single points of failure within the entity's primary Control Center that could halt the flow of Real-time data. The data exchange reference models shown in this section assume the following:

1. The provider/entity network(s) shown do not fall under the requirements in scope because they are not within the primary Control Center.
2. The entity need not have two different provider networks from two different vendors.
3. The entity may achieve diverse routing through physical or logical means.
4. The entity may not need specific physical criteria or distances to achieve diverse routing. For example, while it may not be a best practice, depending on the entity's individual circumstances, the entity may run multiple cables through the same tray or conduit as long as the cables are different components.
5. The entity may have redundant equipment located in the same rack or cabinet, as long as the equipment is powered by different power supplies.
6. The entity need not have redundancy at each internal component of the data exchange infrastructure within its primary Control Center. If a power supply to a server fails, the entity fails over to another server which has its own power supply.

Reference Model 1 – Simple Single Port Router (Not-Recommended)

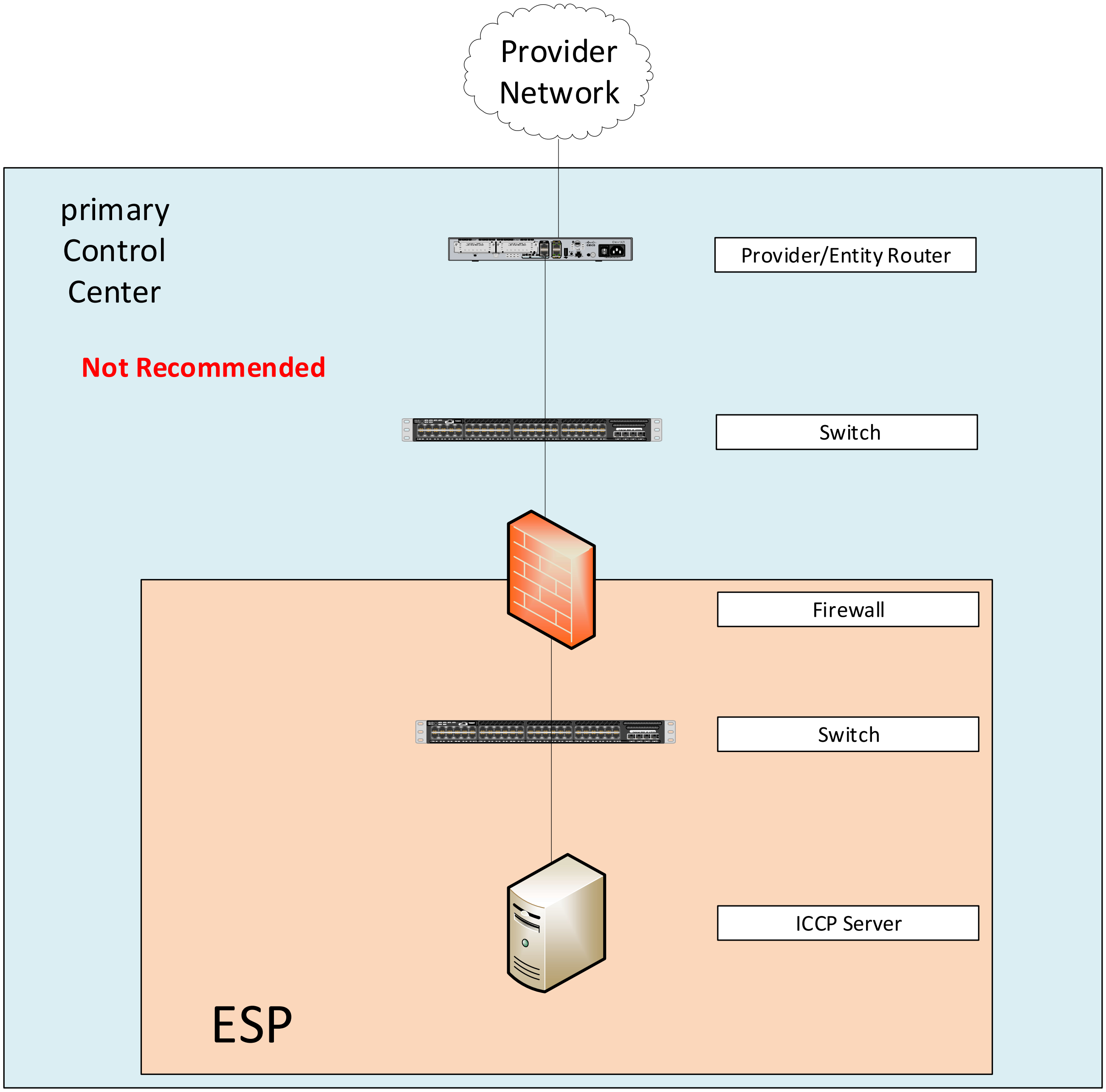


Figure 1: Simple Single Port Router Reference Model (Not-Recommended)

Figure 1 shows a basic reference model of data exchange infrastructure setup within an entity's primary Control Center. This reference model is not recommended because there are several single points of failure within the entity's primary Control Center that could halt the flow of Real-time data. The single points of failure in Figure 1 are:

- Provider/Entity Router
- Switch(es)
- Firewall
- ICCP Server

Reference Model 2 – Redundant Element (Not-Recommended)

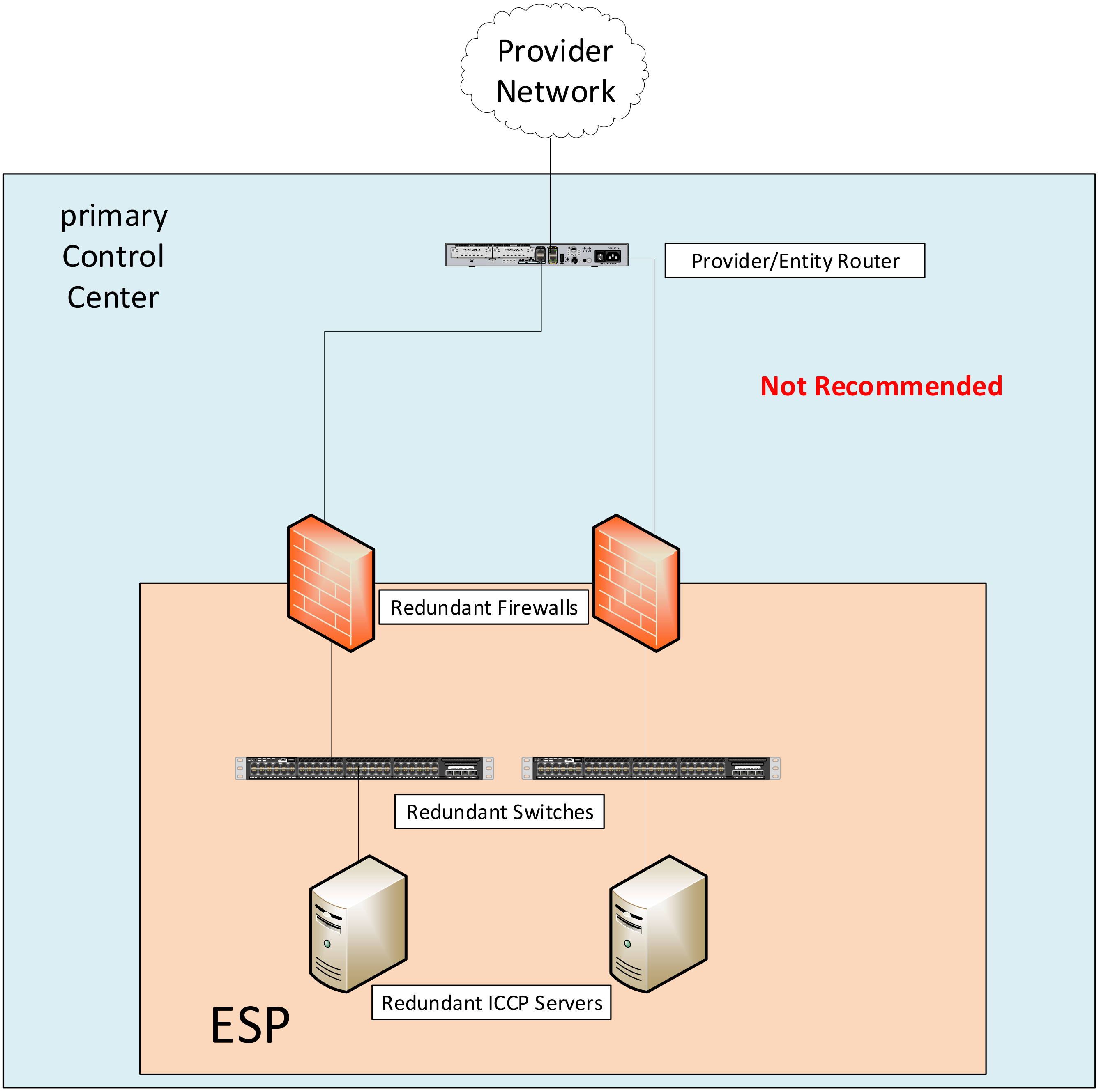


Figure 2: Redundant Element Reference Model (Not-Recommended)

Figure 2 shows a reference model of data exchange infrastructure setup within an entity's primary Control Center with a provider/entity router, redundant firewalls, redundant switches, and redundant ICCP servers. This reference model is not recommended because there are several single points of failure within the entity's primary Control Center that could halt the flow of Real-time data. The single points of failure in Figure 2 are:

- Provider/Entity Router
- Communication path between the Provider/Entity Router and Provider Network

3.2 Recommended Data Exchange Infrastructure Reference Models

This section provides three recommended examples of data exchange infrastructure reference models that do not contain single points of failure within the entity's primary Control Center that could halt the flow of Real-time data. The recommended data exchange reference models shown in this section assume the following:

1. The provider/entity network(s) shown do not fall under the requirements in scope because they are not within the primary Control Center.
2. The entity need not have two different networks from two different vendors.
3. The entity may achieve diverse routing through physical or logical means.
4. The entity may not need specific physical criteria or distances to achieve diverse routing. For example, while it may not be a best practice, depending on the entity's individual circumstances, the entity may run multiple cables through the same tray or conduit as long as the cables are different components.
5. The entity may have redundant equipment located in the same rack or cabinet, as long as the equipment is powered by different power supplies.
6. The entity need not have redundancy at each internal component of the data exchange infrastructure within its primary Control Center. If a power supply to a server fails, the entity fails over to another server which has its own power supply.

Reference Model 3 – Redundant Element Reference Model

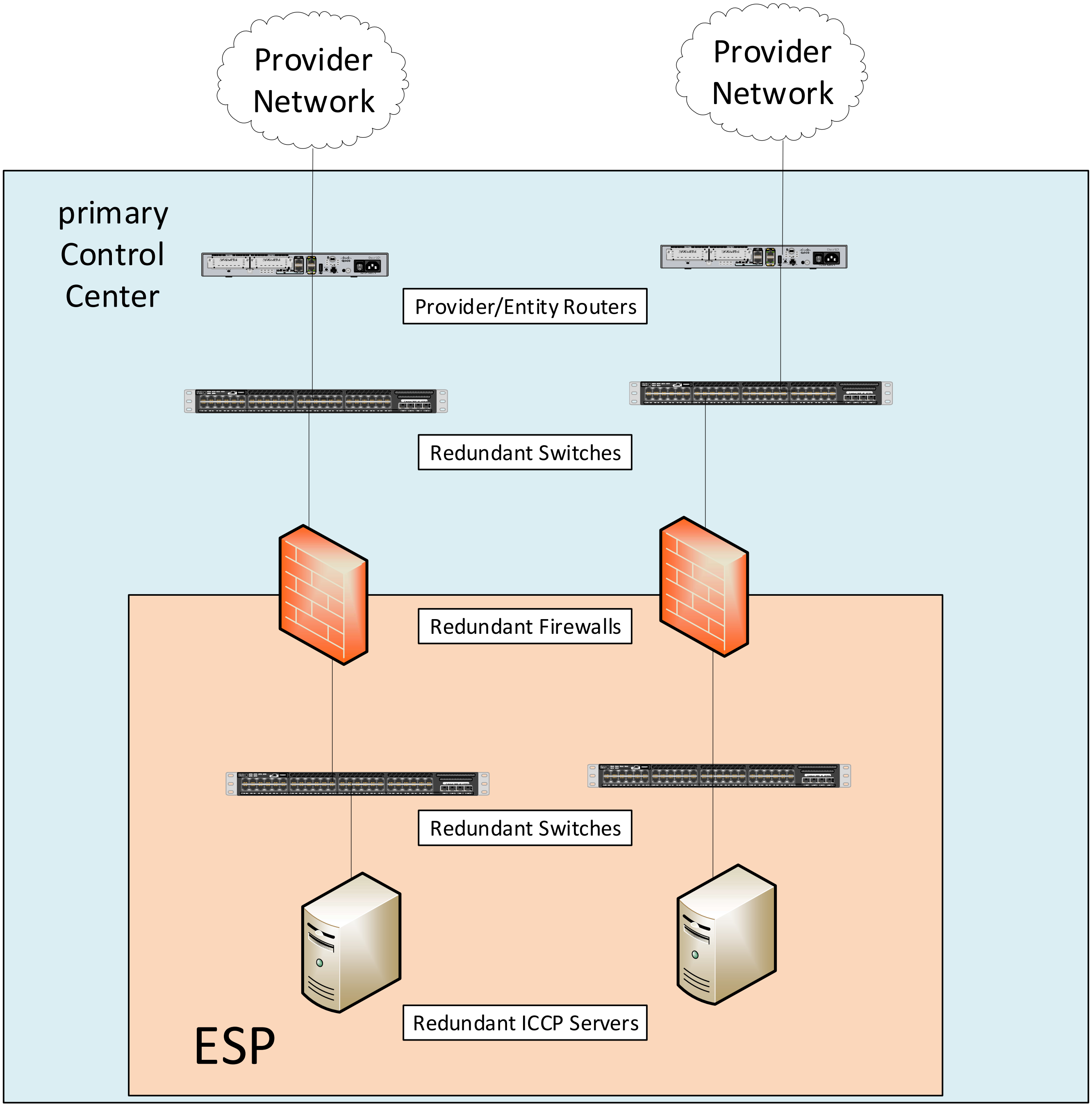
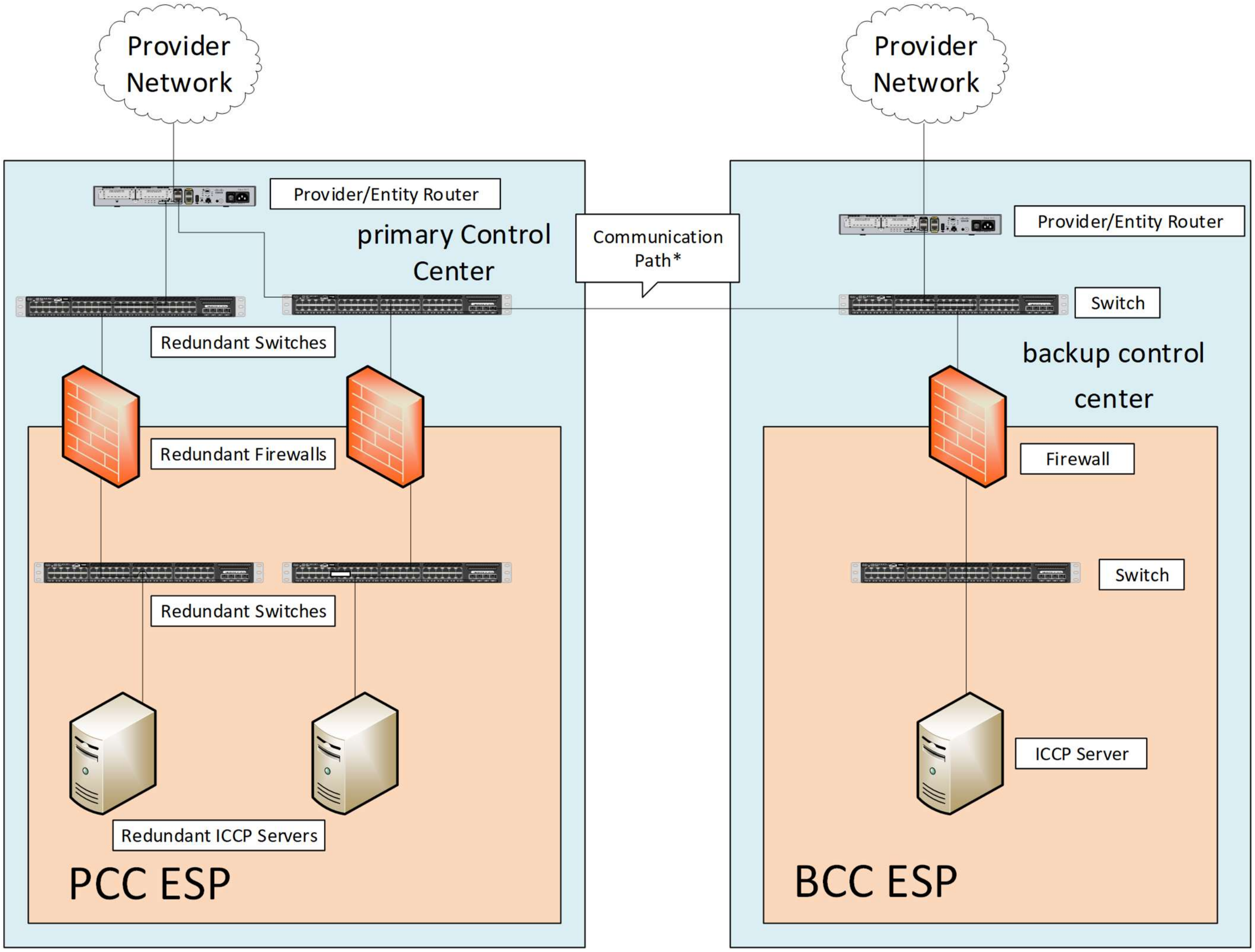


Figure 3: Redundant Element Reference Model

Figure 3 shows a basic reference model of data exchange infrastructure setup within an entity's primary Control Center with redundant provider/entity routers, redundant firewalls, redundant switches, and redundant ICCP servers. This data exchange infrastructure reference model is recommended because there are no single points of failure within the entity's primary Control Center that could halt the flow of Real-time data.

In this example, the entity may also have communication paths between the redundant "Provider/Entity Routers", "Redundant Switches", or the "Redundant Firewalls", thus adding additional layers of diversity and redundancy for flow of Real-time data. Such variations would also constitute a recommended approach.

Reference Model 4 – Redundant Element Backhaul Reference Model



*Communication path architecture shown in Figure 4 may contain additional network equipment including routers, firewalls, encryptors, switches, etc.

Figure 4: Redundant Element Backhaul Reference Model

Figure 4 shows a reference model of data exchange infrastructure setup within an entity's primary Control Center with a provider/entity router, redundant firewalls, redundant switches, redundant ICCP servers, and a communication path for exchange of Real-time data from an alternate location.

This data exchange infrastructure reference model is recommended because there are no single points of failure within the entity's primary Control Center that could halt the flow of Real-time data. At any given time if a data exchange path becomes unreliable because of the malfunction or failure of an individual component or a combination of components in a particular data exchange path, the remaining available data exchange path(s) would support continued flow of Real-time data.

In this example, the entity may also have communication paths between the "Redundant Switches" and "Redundant ICCP Servers" in the ESP of the primary Control Center, thus adding additional layers of diversity and redundancy for flow of Real-time data. Such variations would also constitute a recommended approach.

The alternate location could be the entity's backup control center as long as the entity can demonstrate that the primary Control Center is not dependent on the alternate location for control center functionality. There could be several approaches and designs the entity could choose to setup the data exchange infrastructure within the primary Control Center using the communication path from the alternate location. The entity should ensure that it is not solely relying on the alternate location, which is serving as the backup control center, for achieving redundancy and/or diversity required within the entity's primary Control Center. The entity should also note that the NERC Glossary definition of "Control Center" includes the associated data center(s). Depending on how the entity has setup its data exchange infrastructure to achieve redundancy and/or diversity within its primary Control Center, the alternate location could constitute an associated data center of its primary Control Center.

Reference Model 5 – Redundant primary Control Centers Reference Model

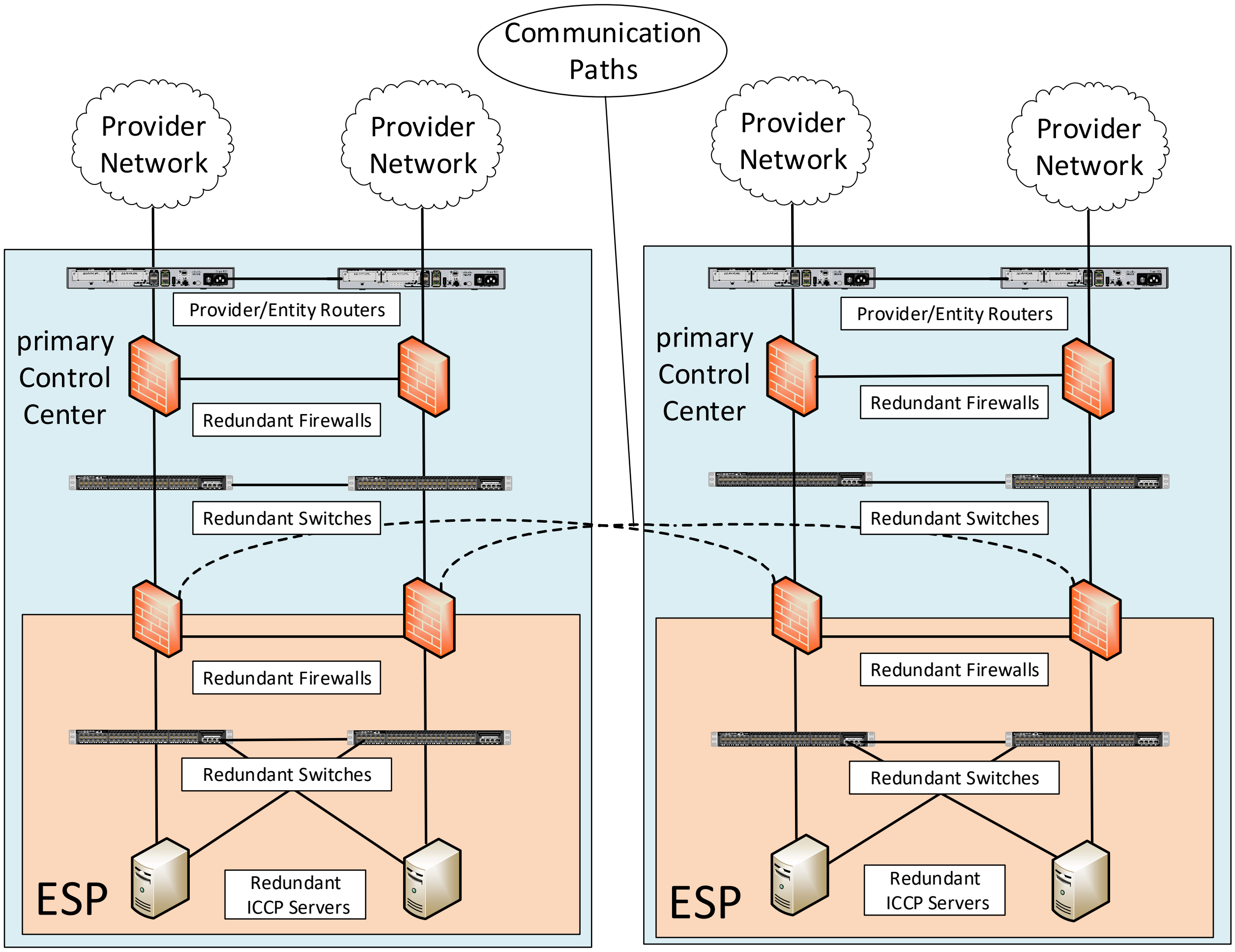


Figure 5: Redundant primary Control Centers Reference Model

Figure 5 shows a reference model of an entity that operates from two redundant primary Control Centers that are staffed with System Operators 24 X 7. In this reference model, both primary Control Centers exchange data for normal Real-time operations independently with other entities and are able to operate the BPS without relying on the other Control Center for Control Center functionality. In this setup, each primary Control Center has redundant provider/entity routers, redundant firewalls, redundant switches, and redundant ICCP servers.

This data exchange infrastructure reference model is recommended because there are no single points of failure within each primary Control Center that could halt the flow of Real-time data. At any given time if an individual component or a combination of individual components malfunction or fail to operate data exchange continues to occur because of the redundant components described above. While the "Communication Paths (dotted lines)" between the two primary Control Centers of the entity are not required to achieve redundant and diversely routed data exchange infrastructure, they serve as additional layers of redundancy and diversity that enable the entity to use data exchange infrastructure located in either primary Control Center irrespective of the primary Control Center the entity's System Operators are operating from.

In this example, the entity may also have communication paths between the redundant "Provider/Entity Routers", redundant "Switches", or the redundant "Firewalls" within each primary Control Center to create additional data exchange path(s) for further improvement in diversity and redundancy for flow of Real-time data. Such variations would also constitute a recommended approach.

3.3 Example Tests of Redundant Functionality

This section provides a few approaches an entity can utilize to conduct redundant functionality tests for the recommended reference models discussed in Section 3.2. It is noted that the testing approaches provided in this Implementation Guidance are not exclusive for achieving compliance with the requirements in scope and that, depending on an entity's circumstances, other suitable methods or ways to conduct such tests exist that can demonstrate compliance with the requirements in scope. It is also noted that some example tests for redundant functionality provided in this Implementation Guidance may be beyond the simplest test an entity can conduct to test its primary Control Center data exchange capabilities for redundant functionality.

The redundant functionality testing examples shown in this section assume the following:

1. The provider/entity network(s) shown do not fall under the requirements in scope because they are not within the primary Control Center.
2. The entity need not have two different networks from two different vendors.
3. The entity may achieve diverse routing through physical or logical means.
4. The entity may not need specific physical criteria or distances to achieve diverse routing. For example, while it may not be a best practice, depending on the entity's individual circumstances, the entity may run multiple cables through the same tray or conduit as long as the cables are different components.
5. The entity may have redundant equipment located in the same rack or cabinet, as long as the equipment is powered by different power supplies.
6. The entity need not have redundancy at each internal component of the data exchange infrastructure within its primary Control Center. If a power supply to a server fails, the entity fails over to another server which has its own power supply.

TOP-001-4, Supplemental Material, Rationale[4] for Requirement R21 focuses on testing individual components for failure or malfunction; however, an entity applying a risk-based approach may choose to test a data exchange path within its primary Control Center. To test a data exchange path for redundant functionality the entity may have to remove multiple components or combinations of components from service to force the data exchange to occur through remaining available data exchange path(s) within its primary Control Center. In some instances (e.g., Figures 7 and 8) the entity may have to determine which individual components or combinations of components when removed from service will test the redundant functionality of the remaining available data exchange path(s).

To develop a testing plan that would examine various failure modes over time, an entity applying a risk-based approach may identify different test scenarios, which may involve removing or simulating the failure of individual components or combinations of components. Once such possible testing scenarios are identified, the entity may develop a testing schedule and conduct a test using one such scenario every 90 calendar days. An entity may repeat the same test every 90 calendar days if the entity can test several failure modes through a single test.

Redundant Functionality Testing Example 1

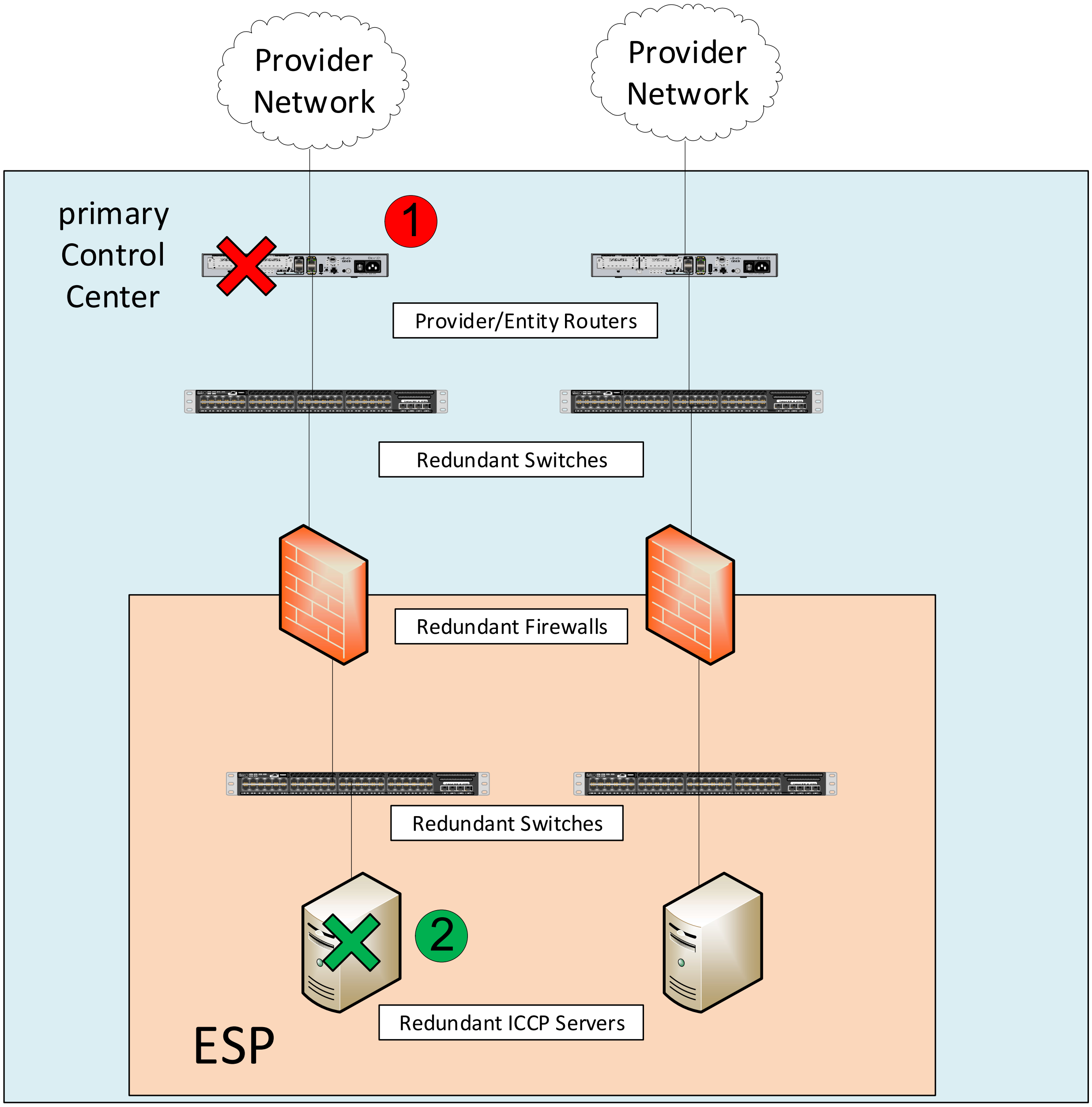


Figure 6: Redundant Functionality Testing Example 1

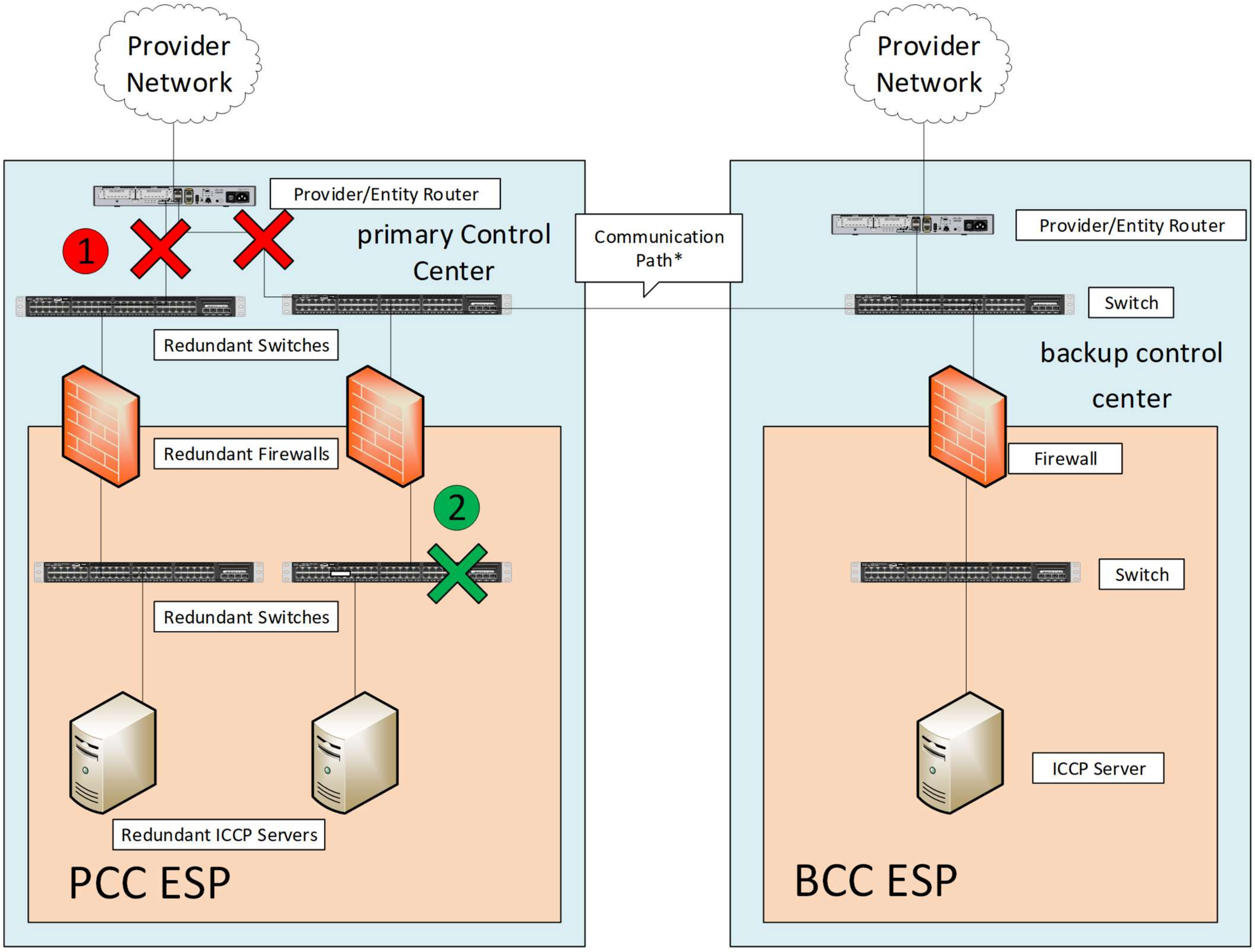
Figure 6 shows two different example tests for redundant functionality (marked in red X and green X and numbered 1 and 2, respectively) an entity can utilize to test its data exchange capabilities in Reference Model 3. These are two different tests for redundant functionality the entity conducts in two different 90-day calendar periods. In this example, removing any single component (e.g., provider/entity router, switch, firewall, etc.) from service in a single data exchange path would force the data exchange to occur through the remaining available data exchange path, thus testing all the components in that data exchange path.

In the first example test (red X and numbered 1), removing the "Provider/Entity Router" from service in the left data exchange path would force data exchange to occur through the right data exchange path. A second test (green X and numbered 2) will also force data exchange to occur through the right data exchange path. These are two different tests for redundant functionality the entity conducts in two different 90-day calendar periods.

The entity also conducts a batch of similar redundant functionality tests by removing components from service in the right data exchange path, forcing the data exchange to occur through the left data exchange path. Thus the entity demonstrates that data exchange capabilities continue to operate despite the malfunction or failure of an individual component in Reference Model 3 over a period of time (several 90-day calendar periods).

To develop a plan/schedule for redundant functionality testing for examining various failure modes over time, the entity creates an inventory of various testing scenarios (some identified above) that may involve removing from service individual components or combinations of components and utilizes one such scenario to conduct a redundant functionality test every 90 calendar days.

Redundant Functionality Testing Example 2



*Communication path architecture shown in Figure 7 may contain additional network equipment including routers, firewalls, encryptors, switches, etc.

Figure 7: Redundant Functionality Testing Example 2

Figure 7 shows two different examples tests for redundant functionality (marked in red X and green X and numbered 1 and 2, respectively) an entity utilizes to test its data exchange capabilities in Reference Model 4. These are two different example tests for redundant functionality the entity conducts in two different 90-day calendar periods.

In the first test (red X and numbered 1), the entity removes from service the data connections between the "Provider/Entity Router" and the "Redundant Switches" and shows that data exchange continues to occur through the "Communication Path" between the primary Control Center and the alternate location. This test is useful for instances where the entity does not own the "Provider" router. In the second test (green X and numbered 2), the entity removes the "Redundant Switch" in the right data exchange path within the primary Control Center and shows that data exchange continues to occur through the remaining available data exchange path on the left.

To develop a plan/schedule for redundant functionality testing for examining various failure modes over time, the entity creates an inventory of various testing scenarios that may involve removing from service components or combinations of components and utilize one such scenario to conduct a redundant functionality test every 90 calendar days.

Redundant Functionality Testing Example 3

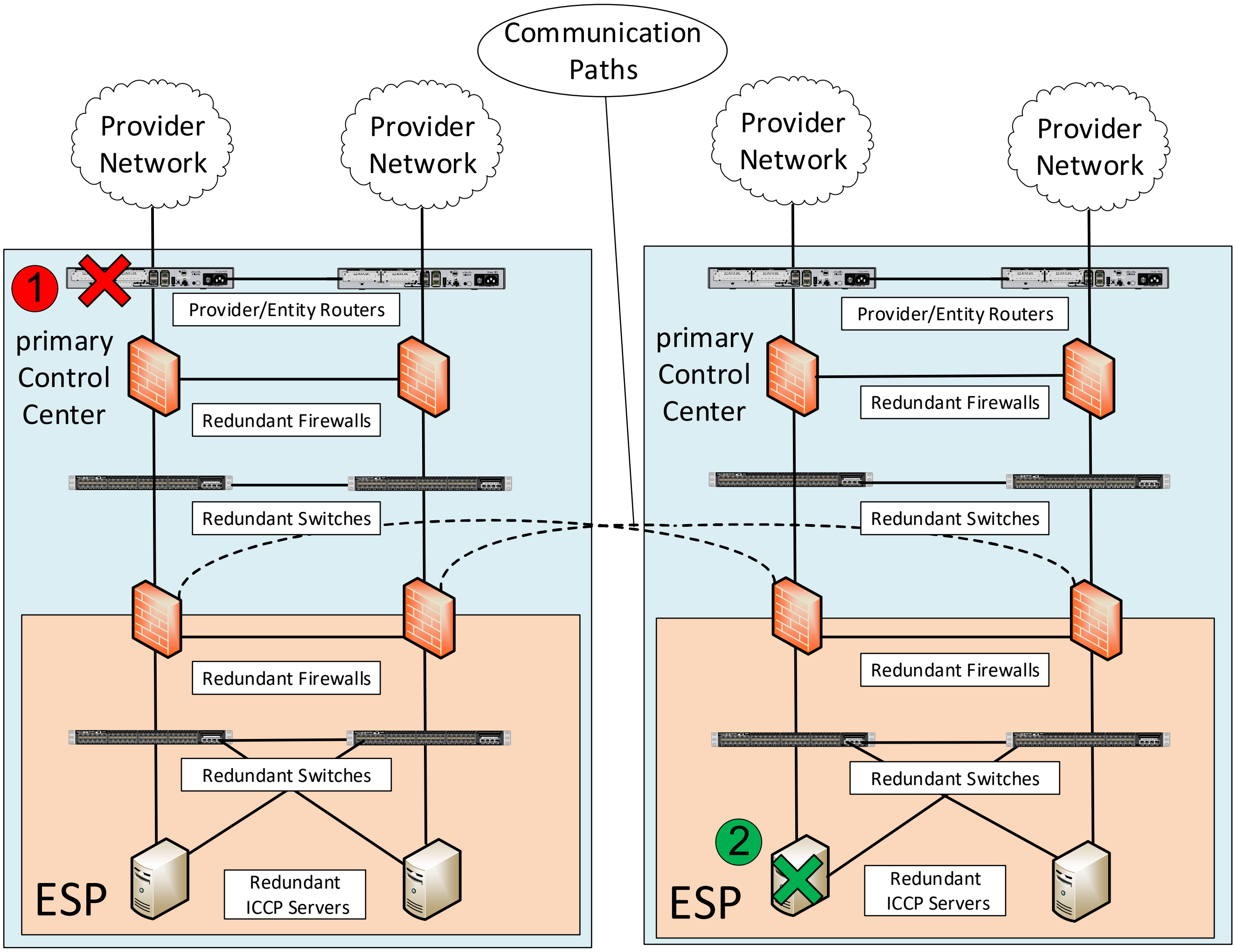


Figure 8: Redundant Functionality Testing Example 3

Figure 8 shows two different examples of tests for redundant functionality (marked in red X and green X and numbered 1 and 2, respectively) an entity utilizes to test its data exchange capabilities in Reference Model 5. These are two different example tests for redundant functionality the entity can conduct in two different 90-day calendar periods.

In the first example test (red X and numbered 1), an entity may remove from service the "Provider/Entity Router" marked in red X and show that data exchange continues to occur. In the second example test (green X and numbered 2) an entity may remove from service the "ICCP Server" in the left data exchange path within the primary Control Center on the right and show that data exchange continues to occur.

It is noted that in Reference Model 5, the entity needs to conduct a redundant functionality test within each primary Control Center to test the data exchange capabilities of both primary Control Centers. The entity, applying a risk-based approach, may conduct a redundant functionality test within a primary Control Center every 90 calendar days to minimize adverse impacts to reliable operation of the BPS. One redundant functionality test in one of the primary Control Centers every 90 calendar days is sufficient. The entity does not simply rely on its capability to operate from either primary Control Center independently of the other primary Control Center to achieve compliance with the requirements in scope. The entity tests the data exchange capabilities of each primary Control Center separately.

To develop a plan/schedule for redundant functionality testing for examining various failure modes over time, the entity creates an inventory of various testing scenarios within each primary Control Center that may involve removing from service components or combinations of components and utilizes one such scenario to conduct a redundant functionality test within a primary Control Center every 90 calendar days.

3.4 Actions in the Event a Redundant Functionality Test Fails

In the event a redundant functionality test is unsuccessful, the entity needs to initiate action to restore the redundant functionality within two hours; the requirements in scope do not expect that the entity restore the redundant functionality within two hours.

Some example actions the entity can initiate to restore the redundant functionality within two hours include the following:

- Notifying support personnel who are available 24/7 to troubleshoot such issues
- Requesting vendor support for certain hardware or software issues as appropriate