NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Considerations High - Impact Control Centers

December 12, 2018

RELIABILITY | ACCOUNTABILITY




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

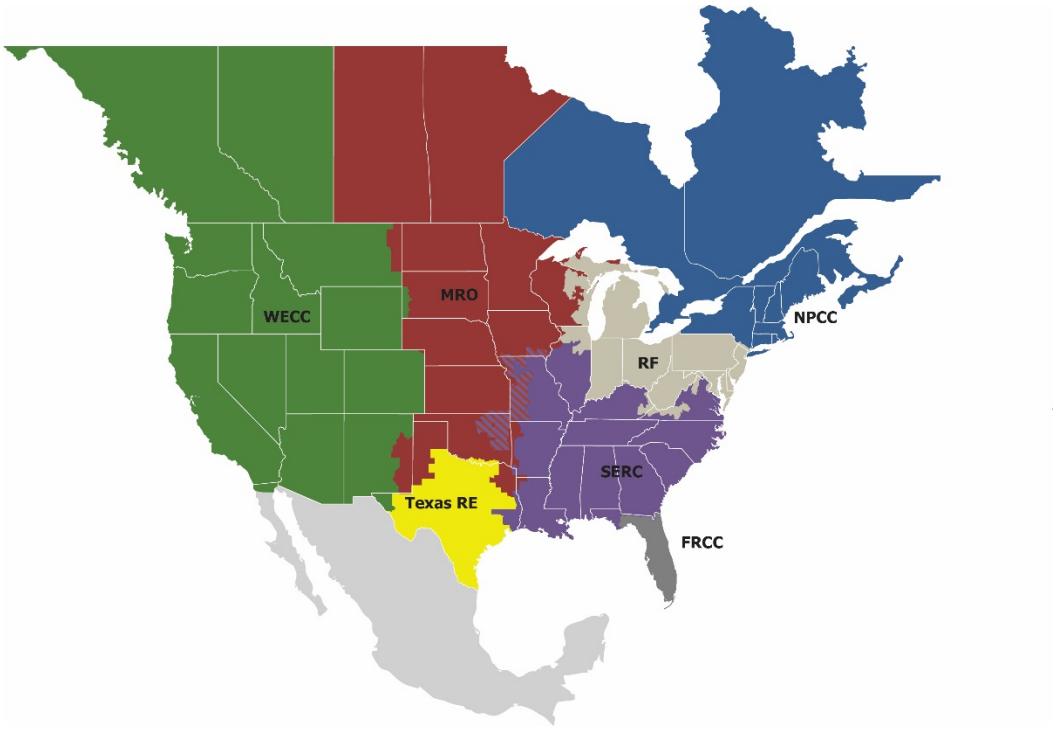
Table of Contents

Preface

This Guideline provides information for organizations to use if they wish to improve security at high-impact control centers. It is a menu of ideas; many of the measures in this document could be used in the design of a new facility, but a few also could be used to enhance security at an existing site. The decision on how much of this Guideline to use rests entirely with the owner/operator of the control center(s).

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven 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 seven 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.



FRCC	Florida Reliability Coordinating Council
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

References

A. CIP-014 Report Physical Security Protection for High Impact Control Centers, 2 Oct 2017
B. Government of Ontario IT Standard Number 25.18 Physical Security Requirements for Data Centres Version #1.2 dated 18 March 2015
C. CIP-004-006 – Cyber Security – Personnel & Training
D. CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
E. Royal Canadian Mounted Police G1-026 Guide to the Application of Physical Security Zones
F. Security Management in the North American Electricity Subsector: A Guideline (available from the E-ISAC)
G. CIP-014-2 Physical Security

NERC Definitions

Control Center: One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

High Impact Control Center: Please see Section 2 of Reference A.

Chapter 1: Threat Assessment

In Reference A, NERC offers the following threat assessment:

> "There are two basic threats to consider relating to the physical security of Control Centers: (1) a physical attack designed to damage, destroy, or otherwise render the Control Center inoperable; or (2) a physical attack designed to gain physical access to the Control Center to operate BES assets in a manner that would adversely affect reliable BES operations.
>
> In the first type of threat, the assailant's objective is to affect the availability or operability of the Control Center. For instance, threat actors could approach the facility housing the Control Center in a vehicle filled with explosives and detonate it close enough to the facility to destroy or damage the facility to render the Control Center inoperable. Similarly, a threat actor could seek to render a Control Center inoperable by cutting off its power sources, including its backup power supplies. Additionally, this type of threat scenario also includes threat actors seeking to gain entry into the facility housing the Control Center to damage or destroy the equipment and systems in the Control Center used to operate the grid.
>
> The second type of threat involves threat actors that seek to gain physical access to the Control Center with the intent to operate the grid in an unreliable manner, by directly operating or directing others to operate the system in a manner that would adversely affect reliable operations, including damaging BES equipment. This type of physical attack may require the threat actors to have a sophisticated knowledge of grid operations and the BES Cyber Systems that control BES Facilities. This type of attack could have a greater impact on BES operations as compared to the first type of attack."

Reference A offers guidance on the threat and vulnerability assessment process for specific facilities, suggesting that the following may be considered when siting the facility:

- Terrain/elevation of surrounding ground or structures providing line of sight.
- Line-of-sight distance from approach avenues (distance and direction that armament can be utilized).
- Proximity to and speed of adjacent vehicular traffic for vehicle-induced damage.
- Proximity to traffic for easy vehicular access and egress (e.g., "drive-by" access).
- Proximity to other targets of interest or critical load (e.g., number of customers affected, densely populated area, high-profile commercial or governmental entities served, etc.).
- Number of operational targets, electrical component assets, etc. at a single site.
- Proximity to company or other response personnel may impact target selection and restoration response.
- Proximity to law enforcement or emergency personnel may impact target selection and restoration response.
- The risk resulting from historical events that have occurred at this location as well as similar facilities nationwide and the proximity of these events to the facility being assessed.
- Location of the Control Center (collocated in a company headquarters, standalone secured facility, collocated in company headquarters with other tenants, located in a multi-tenant facility owned by someone else, etc.).

Chapter 2: Security Planning Considerations

Regulatory

CIP-004-6 Cyber Security – Personnel & Training impose several requirements which must be accounted for in High Impact Control Center security planning as follows:

> "… the registered entity must take the following actions for any individual granted unescorted physical access to High Impact BES Cyber Systems and associated Electronic Access Control and Monitoring Systems (EACMS) and Protected Cyber Assets (PCAs), and Medium Impact BES Cyber Systems with External Routable Connectivity (ERC) and associated EACMS and PCAs:
>
> - Provide the individual training on physical access controls, among other things (Requirement R2).
> - Perform a personnel risk assessment (or background check) of the individual (Requirement R3).
> - Implement an access management program to authorize, based on need, individuals that may have unescorted physical access into a Physical Security Perimeter (PSP), which houses BES Cyber Systems (Requirement R4).
> - Implement an access revocation program to revoke an individual's access authorization (Requirement R5). The requirements in CIP-004-6 are designed to reduce the risk of physical security events at Control Centers and other types of facilities by training individuals on physical access controls (i.e., how they work, what to look for, etc.) and taking steps to eliminate insider threats by ensuring that only individuals with a need for unauthorized physical access have and can be trusted with such access.

CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems impose additional requirements related to access control, visitor control, and maintenance and testing of physical access control systems.

Zone System

Security planners may want to consider dividing the control center complex into distinct zones. Each zone should have its own threat and vulnerability assessment conducted to ensure that specific threats are adequately addressed.[1] The suggested zones are as follows:

- ***Public Zone***: This zone may include parking lots, grounds surrounding the facility, public corridors or concourses, elevator lobbies (if in a shared facility), and any areas that the public enjoys unimpeded access to during normal business hours.
- ***Reception Zone***: This zone is where the public and facility staff meet, or where staff enter the facility. These areas include the main entrance to the facility, visitor receiving or waiting areas, and public services desks or kiosks.
- ***Support Zone***: This zone is the area of the facility where access is limited to authorized personnel and visitors and does not include the control room floor. Typically, this zone would include hallways, storage closets, employee offices, maintenance, supply, etc.
- ***Operations Zone***: Monitored continuously, this is the main control center floor. It must: have a recognizable perimeter; employ robust and reliable physical barriers to access; be constructed in such a way that all barriers and doors remain closed and locked when not in use; employ active monitoring with immediate response; enjoy positive access control at all times and be located within the support zone.
- ***High Security Zone***: This zone or zones are where sensitive computer equipment, communications equipment, and any other technologies or systems deemed critical to the operation of the center

[1] For further information on the zone system please see References B and E.

technology resides. Contained with the Operations zone, it has an additional layer of access control and monitoring to minimize the number of personnel who have access.

Zone Security Measures and Control Matrix

Functionality and Security Controls[2]	Public Zone	Reception Zone	Support Zone	Operations Zone	High Security Zone
Access Control	N/A	No	Yes	Yes	Yes
Authorized Personnel Only	N/A	No	Yes	Yes	Yes
Barriers (Basic)	Yes	Yes	Yes	No	No
Contractors (Unescorted)	Yes	Yes	Yes	Yes	No
Electronic Access Controls	Consider	Consider	Yes	Yes	Yes
Exterior Barriers (Robust)[3]	Consider	N/A	N/A	N/A	N/A
Exterior Entrances	Yes	Yes	No	No	No
Garbage bins, large/outdoor	Yes	No	No	No	No
Glass or glazed doors	N/A	Yes	Avoid	No	No
Guard	N/A	Yes	No	Consider	No
Interior Barriers (Robust)[4]	N/A	No	No	Yes	Yes
Key Management and Control	N/A	Yes	Yes	Yes	Yes
Locked Door Environment	N/A	No	Consider	Yes	Yes
Lighting	Yes	Yes	Yes	Yes	Yes
Lobby/Greeting Area	Yes	Yes	Avoid	No	No
Maintenance Staff (Security Cleared)	N/A	Yes	Yes	Yes	No
Maintenance Staff (Uncleared)	N/A	No	No	Consider	No
Monitoring (Periodic)[5]	Yes	Yes	Yes	No	No
Monitoring (Continuous)[6]	N/A	Consider	Consider	Yes	Yes
Monitoring (Audited)[7]	N/A	No	No	Consider	Yes
Parking Areas Access	Yes	No	No	No	No
Public Access	Yes	Yes	No	No	No
Recognizable Perimeter	N/A	Consider	Yes	Yes	Yes
Recycled Paper Storage	No	No	Yes	No	No
Roof Hatch	N/A	Yes	Yes	Yes	No
Secure Doors/Locksets	N/A	Yes	Consider	Yes	Yes
Slab-to-Slab Walls	N/A	Yes	Consider	Yes	Yes
Two-Factor Authentication	N/A	No	No	Yes	Yes
Visible ID Required	N/A	Yes	Yes	Yes	Yes
Visitors Escorted	N/A	No	Yes	Yes	Yes
Visitors Reception	N/A	Yes	No	No	No
Windows/Glazing Permissible	N/A	Yes	No	No	No

[2] Adapted from Government of Ontario IT Standard Number 25.18 Physical Security Requirements for Data Centres Version #1.2 dated 18 March 2015 (Reference B) page 12

[3] An example of a robust exterior barrier would be a crash-rated gate at the road entrance to the facility or a bollard

[4] An example of a robust interior barrier would be a man-trap gate or sally port

[5] From Reference D: "**Monitored periodically** - to confirm on a regular basis that there has not been a breach of security. The frequency and diligence of monitoring is based on the recommendations of a Threat and Risk Assessment. Examples include a guard patrol or employees working at the location."

[6] From Reference D: "**Monitored continuously** - to confirm on a continuous basis that there has not been a breach of security. Examples include electronic intrusion detection systems or someone guarding a particular point on a constant basis."

[7] 24/7/365 monitoring where details of access are recorded, stored, and audited.

Facility Location

The location of the control center should not be:

- In an area where there is a history of natural disasters, such as floods, wildfires, or earthquakes;
- Within three miles / five kilometers of an area or a facility with the potential for an industrial disaster, such as truck or rail transportation routes; oil or gas facilities, chemical plants, or airports;
- Within ten miles / sixteen kilometers of a nuclear power plant to ensure that the facility will not be within the evacuation zone in the event of an emergency[8]; and
- In proximity to high profile or high-risk locations, such as military offices, financial districts, or political or symbolic targets.

The control center should be at a location that is serviced by:

- good roads, including local truck routes;
- multiple routes in, and no choke points, such as at a single bridge;
- easily available fire, police, and emergency medical services; and
- redundant supplies of utilities such as water, power, and telecommunications

Construction

Because facility security is central to the operation of a high-impact control center, a threat and risk assessment should be conducted prior to the commencement of the design and construction. Borrowing from the language of CIP-014-2 *Physical Security*, the TRA should consider the following:

> *"4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);*
>
> *4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and*
>
> *4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors."*[9]

The design team should include a security engineer, and the final design of the facility should be informed by the results of the threat and risk assessment.

[8] The radius of the evacuation zone should be confirmed with any nuclear power plant within fifty miles or 80 kilometers
[9] Reference G

Chapter 3: Security Measures

Security measures are used to eliminate or reduce the vulnerability articulated in the Threat and Vulnerability Assessment. Taken together, the security measures used should cover the following functions:

- **Access control**
- **Deterrence**
- **Detection**
- **Assessment**
- **Delay**
- **Response**
- **Evidence collection**

The following table shows many of the more common security measures, and the functions that they perform:

Type	Access	Deter	Detect	Delay	Assess	Respond	Evidence
Guards	x	x	x	x	x	x	x
Mobile Patrols		x	x	x	x	x	x
CCTV	x	x	x		x		x
FIDS[10]		x	x				
IDS[11]		x	x				
Locks	x	x		x			
Lights		x	x		x	x	x
Alarms		x				x	
LIDAR[12]			x		x		x
Barrier: Fence/Wall/Door/Man Trap/Bollard	x	x		x			

Security Measure Functions

There should be redundancy for each function. For example, Access Control is achieved through more than just locks: it should include CCTV and a barrier, such as a man-trap.

In the threat assessment provided by Reference A, the two basic threats are:

1. a physical attack designed to damage, destroy, or otherwise render the Control Center inoperable; or
2. a physical attack designed to gain physical access to the Control Center to operate BES assets in a manner that would adversely affect reliable BES operations.

The first threat is external to the control center, and the most likely vector would be an explosives attack of some sort. The security measures would most likely include bollards, crash-rated gates, and fencing. The purpose would be to keep vehicles that potentially could carry improvised explosive devices well back from the exterior of the building and away from the entrances and exits.

[10] Fence Line Intrusion Detection System
[11] Intrusion Detection System
[12] Light Detection and Ranging

The second threat requires that the security plan ensure that an adversary cannot gain access to the control center. This requires a much larger set of security measures, both technical and procedural. Doors, man traps, electronic card access control systems, CCTV cameras, background checks, visitor management programs, key management programs, etc. are all components of a comprehensive plan to ensure that the only people who get into the Operations zone and the High Security zone have proper authorization.

The combination of security measures selected would, as a whole: control access to the control center; deter, detect, and delay adversaries; assist security officers in assessing the nature of an apparent incursion; provide for a response to the attack; and collect and preserve evidence for use in any subsequent legal action.

Security Plans and Threat Response

A security plan is vital to the effective protection of the facility. As a high-impact facility may be one that is regulated by NERC CIP-014-2 *Physical Security*, the plan should incorporate the requirements of R5.

> *"…The physical security plan(s) shall include the following attributes:*
>
> *5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.*
>
> *5.2. Law enforcement contact and coordination information.*
>
> *5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.*
>
> *5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

Security plans should include measures that would allow a control center to increase or decrease security measures in consonance with changes in the threat level. If the threat level goes from low to high, then additional security measures should be brought into play to increase the protection of the facility and to send a message to any adversary who may be conducting pre-attack surveillance that the facility has a robust security plan and that they are exercising it.

Resilience

The control center should be able to support BES operations without external support (power, water, regular telephone and Internet connections, food, or staff changes) as long as required for full services to be restored. The period of self-sufficiency is flexible and depends on the nature of the disaster. For example:

- flooding of the surrounding area could isolate the control center, but supplies and staff can be brought in by boat or helicopter;
- an ice storm can cut off power for days or weeks, but the backup generator can run for as long as it has fuel; and
- a disease pandemic may leave all services available, but operators are in short supply.

The key to self-sufficiency lies in good all-hazards threat and vulnerability assessments, strong business continuity plans, and realistic exercises. As plan execution may require time to assemble transport and other resources, it is recommended that the control center be able to operate entirely on its own for at least 72 hours.

Security Management

Managing the security of a High-Impact Control Center is a challenging and complex task. Organizations should consider recruiting professional security managers to lead the security function at the facility. Professional security managers are usually certified by a professional society. Applicable certifications include:

- ASIS International's Certified Protection Professional (CPP)
- ASIS International's Physical Security Professional (PSP)
- The Security Institute (UK) Chartered Security Professional (CSyP) or Fellow (FSyl)

For further information on security leadership skills and experience please see Reference F.

Change Management and Review

The security plan of the facility should be reviewed as follows:

- As required by regulation;
- Annually:
- Upon an increase in the threat level:
- Upon a change in the security leadership of the organization; or
- After a security incident at the facility or at a similar facility elsewhere in the bulk power system.

The review of the security plan should be documented, and include:

- All information as required by applicable regulation;
- The date of the review;
- The reason for the review;
- An updated threat and risk assessment;
- An update on the completion of security changes required by the previous review;
- All changes required to the security plan; and
- The timeline for the completion of the changes.