Substation Physical Security Tiering Practice- Open Distribution

Version 1.0
Document ID: 1775
Approval Date: 03/11/2025

Versioning

Version History

Date	Version	Notes
03/11/2025	1.0	Initial version

Review and Update Requirements

- Review: every 5 years
- Update: as necessary

Contents

1. Purpose

This document is designed to help organizations prioritize physical security for substations using a risk-based approach. This will help organizations evaluate and categorize substations, assigning each substation to a security tier. These tiers, along with a physical security risk assessment of each station, can be used to select human and mechanical physical security measures to protect substation assets.

This document does not create, replace, or change any requirements in the NERC Reliability Standards or other applicable criteria, nor does it create binding norms by which compliance with NERC Reliability Standards is monitored or enforced. Implementation of NATF practices does not ensure compliance with the NERC Reliability Standards. In addition, this document is not intended to take precedence over any company or regional procedure. It is recognized that individual companies may use alternative and/or more specific approaches that they deem more appropriate.

2. Scope

This practice applies to all substations, including CIP-014 substations and distribution substations.

3. Definitions

NATF Practice

A documented method for performing a process, under the same or similar circumstances, in a safe, effective manner where the requisite skills, diligence, prudence, and foresight are those that are reasonably expected from skilled and experienced industry organizations.

NATF Superior Practice

A leading industry practice that can be consistently applied under a range of circumstances and that is a safe, effective, and efficient process or activity for achieving near-optimal industry results in terms of quality, reliability, and maintainability.

Authority Having Jurisdiction (AHJ)

An organization, agency, or individual responsible for enforcing codes, standards, and regulations related to building construction, fire prevention, and life safety. This term is often used in the construction industry, especially for new construction or renovation projects. The AHJ can be different entities, depending on the project's location and type. In general, it could be a local government agency, fire department, or building department. The AHJ's responsibility is to review construction plans, issue permits, conduct inspections, and ensure that the building meets all applicable codes and standards.

4. Substation Tiering

Substation tiering is the process of assigning a numeric ranking to an organization's assets to create a structured asset protection program. This program is conducted continuously by select organizational stakeholders who evaluate key selection considerations to produce an agreed-upon rank. Tier designations are designed to allocate resources effectively by focusing the highest-level security measures on the most critical assets while applying proportionate measures to less critical assets.

Assigning substations to tiers is the first step in an ongoing process. Organizations should then perform security risk assessments to determine substation risk, implement physical security protections at the substations based

on the tier levels and risk assessments, and update substation tiers based on new inputs and periodic reviews. Figure 1 shows the process steps outlined in this document.

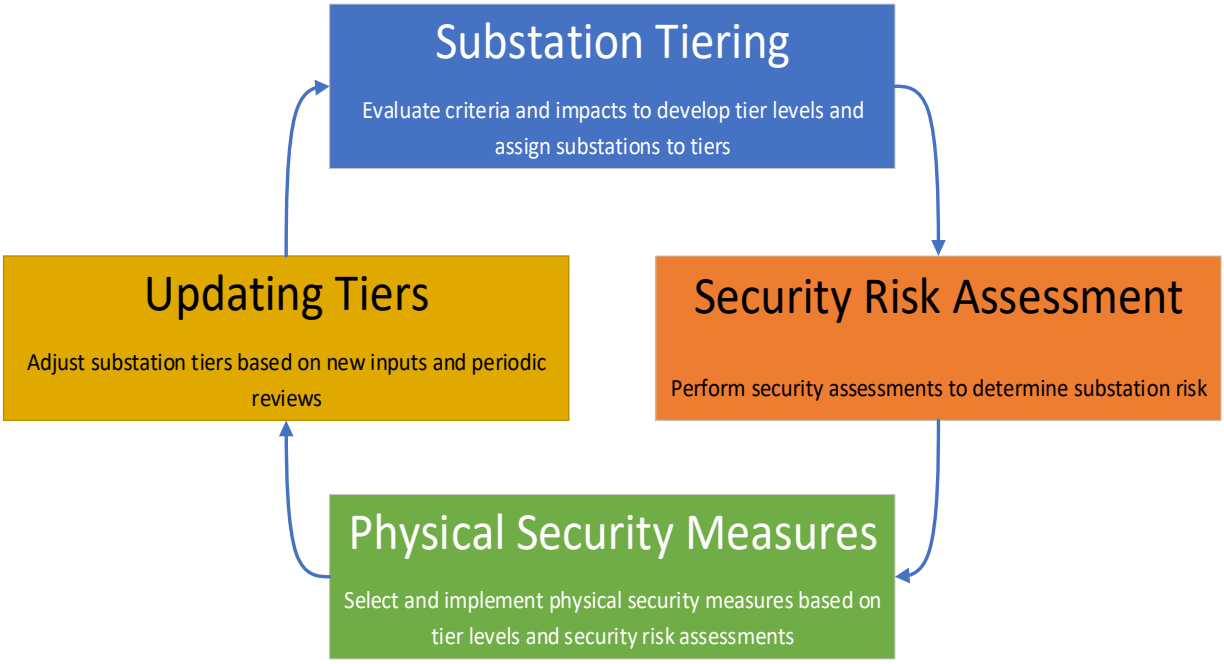

Figure 1: Summary of Steps for Substation Physical Security Tiering

NATF Practices

4.1 Benefits of substation tiering

The process of development, implementation, and maintenance of a substation tiering program can produce numerous benefits for an organization. While the concept of assigning a ranking to a location may sound simple, the benefits can be substantial to an organization and its customers:

- Identification of critical organizational assets
- Cost savings
- Effective resource allocation
- Standardization of security approach
- Coordination of protection efforts across business units
- Justification for financial investments

4.2 Stakeholder selection

Stakeholder selection is a vital component of the substation tiering program. Careful selection ensures that the proper subject matter experts contribute to discussions about the impact of the substation on the organization and the community. While the output of the tiering process will be utilized by security professionals, they should not be the primary influencers of the tier designation.

The following is a list of potential process stakeholders:

- Planning and modeling engineering
- Substation engineering
- Electric system operations
- System protection and control engineering
- Enterprise risk management
- CIP compliance oversight organization
- Key customer business account managers

Different companies may have different names for these groups, or these functions may fall in parts of the organization outside the transmission business unit.

4.3 Selection considerations

The substation tier designation may be based on a wide variety of operational considerations and impacts. There are three key considerations for the selection committee when determining the appropriate designation.

4.3.1 Operational impact

This factor refers to the impact that the loss or functional degradation of the asset would have on the core business functions of the organization. Beyond core functions, this evaluation reviews other aspects, such as the difficulty of restoration, system redundancies, and any other impacts to determine the total operational impact.

4.3.2 Customer and community impact

This factor evaluates the impact on customers and the community due to the loss or functional degradation of a particular asset. Community lifelines, such as hospitals, police stations, etc. are considered to determine the short-term and long-term consequences of activities required to restore the functions of the asset. This factor also includes any impact on the organization's reputation due to public perception of the quality of the utility's protection program for key community resources.

4.3.3 Regulatory or legal impact

This factor considers any legal or regulatory requirements that govern the operation of the asset. While these may be related to the operational impact, there may be additional regulatory issues that result from the failure or functional degradation of the asset (e.g., environmental issues).

4.4 Methodology for ranking

The methodology for ranking substations within the tiering program can follow a quantitative, qualitative, or hybrid model. The quantitative model assigns values based on the operational function of the substation. The qualitative model considers key characteristics of the substation (supports a hospital,

isolated location, etc.) and assigns a value. In many cases, a hybrid model that employs both approaches is used to define the ranking structure. See Appendix 1 for examples of ranking methodologies.

5. Security Risk Assessment

A security risk assessment is a formal process that uses a methodical approach to identify issues or concerns that may pose a security risk to a facility. There may be various levels or types of security risk assessments completed depending upon the specific facility. Security risk assessments are performed at specified intervals and should be an ongoing process as security risks or facilities change.

Overall security risks include industry risks and site-specific risks. The tiering process described in the previous section identifies the criticality of the site, leaving the threat and vulnerability factors to be identified in this portion of the risk assessment. This process may also be referred to as a threat and vulnerability assessment, or TVA. Different methodologies may be used for different tiers, as risk assessments for more critical sites may be more expansive and detailed.

NATF Practices

5.1 Industry risks

Electrical system infrastructure in general, and substations in particular, have been subject to an increasing number of actual and planned physical attacks using evolving attack methods. Risk assessments should take into account the industry's current understanding of the capabilities and motives of threat actors in general.

5.2 Site-specific security risks

The security risk assessment process should consider the unique threats and vulnerabilities of the various tier levels and each specific site. The criticality identified in the tiering process assists in developing a design basis threat (DBT), which outlines who and what the utility is trying to protect against. Just as a site may have a unique criticality, it may have unique threats and vulnerabilities based on its features, layout, use, location, environmental conditions. The DBT may need to be adjusted as the threat environment changes, and changes in the utility's electrical system, such as expansion, should trigger a reassessment.

5.3 Security assessment considerations

There are several considerations that each utility should review in conducting security risk assessments. Compliance requirements should be reviewed to determine any potential effect they may have. Also, individual utilities' risk tolerance may differ and may change based on other considerations, such as:

- Number of customers served by site
- Customer type (e.g., critical water, hospitals, jails, government facilities)
- Recent events or criminal incidents (local, state, and national)
- Condition of equipment
- Location (e.g., rural or urban)

- Geography (e.g., elevated areas adjacent to site such as mountains or tall structures)
- Physical and environmental hazards (e.g. high fire risk, earthquakes, storms)

5.4 Security risk assessment methodology

Various methodologies may be used to assess a site's overall security risk. Different methodologies may be used for different tiered sites; for example, a more in-depth methodology may be necessary for the most critical tiers. The following are considerations when performing the assessment:

- Who will conduct the assessment?
- Who else is consulted?
- How often will the assessment be reviewed (this may be tier dependent)
- What assessment tools are used (manual or computer-based)
- How are the results of the assessment document?
- Can the method be replicated at various types of sites?

5.5 Identifying security threats

The method of identifying security threats should consider information from local, regional, and national sources both within and outside the utility sector and consider a variety of threat vectors.

5.5.1 Sources of threat intelligence include:

- Electricity Information Sharing and Analysis Center (E-ISAC)
- Joint Regional Intelligence Center (JRIC)/fusion centers
- Local, state, and federal law enforcement
- Internal security incident reports
- Utility partners

5.5.2 Possible threat vectors include:

- Criminal threats, including trespassing, vandalism, sabotage, and shootings (accidental or intentional)
- Unmanned aircraft systems
- Vehicles
- Explosives
- Arson

5.5.3 Temporary or seasonal threats are those that need to be mitigated for a certain time. Large substations or those that appear more prominent may draw or entice a more sophisticated and determined adversary. High-profile events like the Super Bowl, Olympics, or other major events need to be identified, as well as the potential attack methods for each event. Considering such

threats in advance and acting upon the results of the assessment is one of the challenges in conducting assessments.

5.6 Identifying security vulnerabilities

Site criticality and threat information can be used to identify vulnerabilities. Vulnerabilities may be due to a combination of insufficient or inadequate layers of protection when considering the potential capabilities and determination of the adversary. The effectiveness of current mitigations, whether they provide deterrence, create delay, improve detection, deny entry, or enable timely response should be considered. Examples of vulnerabilities include:

- Ineffective perimeter barriers
- Poor detection
- Inadequate deterrence
- Slow response
- Physical and environmental hazards

6. Physical Security Measures

After performing the security risk assessment, physical security measures should be determined for each substation. There is typically a common set of physical security measures for each tier, and specific substations within the tier may be assigned additional measures based on the results of the risk assessments.

Corporate security is responsible for developing and maintaining physical security standards for facilities to protect personnel and assets and meet regulatory requirements. These include, but are not limited to, perimeter fencing, card access, video surveillance, key control, and alarm monitoring. Physical security standards are subject to change based on environmental conditions, threat, risk, vulnerability, and any other factors in the best interest of stakeholders.

NATF Practices

6.1 Closed-circuit television (CCTV) cameras

Cameras are effective for identifying events in substation yards as they occur. CCTV cameras improve physical security by providing proactive monitoring. Additionally, cameras can be enhanced through integration with the access control system (card readers) and the implementation of software analytics that improve investigation efficiency and image quality. These systems can also improve coordination with local law enforcement.

An aerial survey may be conducted to determine placement of the cameras. In many instances, cameras can be installed on dedicated structures in the substation yard; however, there may be instances where spatial or time constraints dictate the need to use existing structures, such as the control house.

Internet protocol (IP) based cameras are typically used. Cameras may use infrared for thermal imaging and may be fixed view or a mix of pan, tilt, and zoom (PTZ). Security should determine which of these features is needed at each specific location.

Not all facilities are fitted/or retrofitted with all types of cameras. The installation of this equipment is based on size, location, environment, threat, likelihood of criminal activity, and risk.

6.2 Perimeter lighting

Perimeter lighting should be used to improve visibility at night and to improve detection of animals and people. Perimeter lighting consists of downcast lighting (lights pointed downwards, illuminating the fence line) around the perimeter fence of the substation. This provides deterrence as well as improving detection, helping to distinguish between animal, person, and vehicles. It also enhances the safety and security of employees who work at these facilities.

Design engineers should check local ordinances to ensure that downcast lighting is permitted. The illumination level at the fence perimeter should be set to provide a minimum illumination level (e.g. 0.5 foot-candles at the base of the fence) while not exceeding the maximum level dictated by local ordinance.

6.3 Perimeter fencing

Perimeter fence design depends on the size of the facility and the location. Fences should be of height and construction to deter climbing, cutting, and wildlife intrusion. Access may include a wide-swing vehicle access gate as well as pedestrian gates. When designing the perimeter fencing, design engineers coordinate with security and the AHJ to determine the best type of material.

All fencing should be maintained for proper upkeep and integrity. Conditions such as holes in mesh, excessive repairs to mesh, undermining due to water run-off or poor drainage, and the condition of gates should be noted and repairs made as needed.

Prefabricated concrete or special fence materials, such as dual mesh anti-cut, or anti-climb fencing, may be appropriate for higher tier substations.

6.4 Perimeter barriers

Barriers for substations should be based on size and asset location (e.g., transformers, other critical assets, environment). Jersey barriers may be used to control access and prevent the substation from being rammed by a vehicle. Crash barriers may be implemented and should be crash-certified and minimally intrusive.

Temporary barriers may be installed as a foundation along the perimeter fencing near facilities that have multiple avenues of approach, busy roads, or a history of vehicular accidents, or around assets within the perimeter fence. Security should determine the proper placement and size of barriers.

Crash-rated barriers or cable are expensive and may be considered as a physical security enhancement for higher tier substations.

6.5 Ballistic walls

Security and substation engineers should determine whether a wall is needed at a substation and where the wall should be placed. The engineers should also determine if equipment access and airflow will be

adequate after installation of ballistic walls. Building the wall with removable panels and making the columns supporting the panels removable (e.g., with anchor bolts securing the columns to the foundation) can improve access. A sound study may be considered when installing ballistic walls around equipment to ensure noise levels are mitigated if required. Organizations should specify a minimum ballistic standards rating.

6.6 Facility access control

Card readers may be used to control access to substation yards with automated gates and to the control house inside the yard. A gate intercom system is a secondary control measure that may be placed alongside the card readers anywhere motor-operated gates are installed.

Control houses may be supplied with a standard off-the-shelf (OTS) key and cylinder. The key system should be controlled by a documented process that ensures that keys are issued only to those who have the need to have them. A better practice is to use electronic keys, as they offer usage tracking and timely de-authorization as the need arises. Bluetooth padlocks and smart keys are also good access control measures.

6.7 Signage

Signage for the main access gate may include “Stop,” “No Trespassing,” “Electric Hazard,” and “Site Under Surveillance.” “Stop” signage should be affixed to manual or automated gates. “No Trespassing” and “Electric Hazard” signs should be affixed to the perimeter in a conspicuous manner and on all manual or automated gates. If the site has active surveillance, a “Site Under Surveillance” sign should be located at each gate and in other locations as required by local laws and regulations. This allows local, state, or federal law enforcement to press charges against those who trespass onto critical Infrastructure substations.

6.8 Communications

Security engineers should check with communications teams to determine where there is adequate bandwidth for security needs. In some areas, limited bandwidth may delay alarms and reduce the quality of video. If bandwidth is limited, security engineers should work with communications teams to determine how to improve bandwidth to support security needs.

6.9 Assess effectiveness

Periodic assessments ensure that security equipment is functioning optimally and providing the intended level of protection. Assessments should include penetration testing, performance testing, incident reviews, and documentation of maintenance and upgrades. Once the assessment is complete, an action plan should be developed and executed to address any findings.

7. Updating Tiers

As changes occur, individual substations may move to a higher or lower tier according to the utility’s method for determining tier levels. A tier review and update process helps ensure that substations continue to receive an appropriate level of physical security protection based on risk.

NATF Practices

7.1 Tiers should periodically be adjusted based on new inputs.

7.2 Individual substations should undergo a periodic (e.g., annual) review as outlined in Section 4, and tier levels should be updated appropriately.

7.3 Evaluations should look at future plans, including load increases and new construction.

7.4 Tier changes should be discussed and evaluated by the affected stakeholders.

7.5 Tier changes should be provided to the physical security team as part of a process to establish expectations for the timeliness of revised risk assessments and updates to security measures.

Appendix 1: Examples of Ranking Methodologies

The following are examples of models for determining substation tier levels. See Section 4 for more information about ranking methodologies.

Quantitative Model

In a quantitative model, values are assigned based on counts of equipment and lines, the voltage level, amount of generation, number of customers, or other important factors. These scores are added, and a tier is assigned based on where the total score falls relative to established ranges.

Value	Category
x	Number of distribution circuits
x	Number of transmission lines
x	Number of tie-lines
x	Number of transformers
x	Number of auto-transformers
x	Score for highest voltage
x	Score for amount of connected generation
x	Score for number of customers supplied by station
x	Score for number of community lifelines supplied by station
Total	

Qualitative Model

In a qualitative model, values are assigned based on qualities or features of a station.

Value	Category
x	CIP-014 applicable
x	Transmission station
x	Generation station
x	Distribution station
x	No grid redundancy
x	Limited grid redundancy
x	Multiple community lifelines supplied by station
x	Limited number of community lifelines supplied by station
Total	

Range of Total	Tier
xx-xx	1
xx-xx	2
xx-xx	3
xx-xx	4

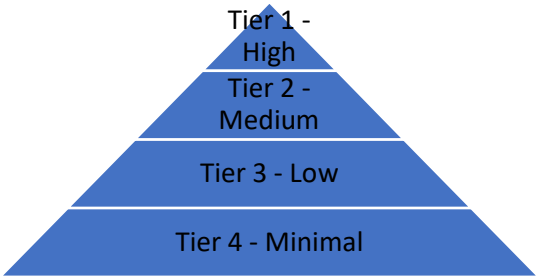

Figure 2: Example Tier Levels

Appendix 2: Example of Physical Security Measures

The following is one example of physical security measures for each substation tier. It is not intended to be a prescriptive list of physical security measures.

Tier I (High)

CCTV Cameras

- Cameras shall be installed to provide maximize perimeter detection. Cameras shall be installed to monitor the interior yard, the control house, and entry gates.
- Radar or a similar product is required. The radar shall be able to detect movement and enable cameras and lighting while tripping an alarm.
- Thermal cameras, PTZ, or fixed cameras should be utilized depending upon the location of the facility.
- The cameras shall have live stream capabilities (see below for communication bandwidth).

Gates and Signage

- An automated drive gate is required (may not be required for jointly-owned substations).
- An additional manual pedestrian entry gate is required at the facility to allow ingress or egress in case of power loss events.
- If seldom-used gates are required for substation and/or transmission line construction, removable fencing or jersey barriers shall be installed as necessary.
- Warning signage (e.g. “STOP”, “No Trespassing”, and “Electric Hazard”) shall be affixed to the perimeter in a conspicuous manner and prominently on all manual or automated gates.

Perimeter Fencing and Lighting

- All fencing shall be of height and construction to deter climbing, cutting, and wildlife intrusion.
- Fencing shall be dual mesh, anti-cut, and anti-climb.
- Perimeter downcast lighting shall be installed.

Perimeter Barriers

- Reinforced Jersey barriers or other means of access protection such as properly rated barrier wire are installed for perimeter fences and gates.
- Jersey barriers shall be installed as needed around external transmission or distribution structures, communications equipment, or other structures (e.g. microwave towers, communication buildings).

Ballistic Protection

- Security engineering may require ballistic walls or fencing upgrades to protect equipment.
- Security engineering may require interior protection materials (e.g. additional sheet metal, bulletproof wall panels) and exterior protection (e.g. barriers) to protect the control house and key interior components (e.g. relays, communication, batteries). This may include concrete barriers or a reinforced outer shell that is ballistic rated.

Facility Access Control

- An access control system is installed at the main access gate to control access into the facility. This includes card readers to enter and exit the facility.
- Card readers shall be affixed next to each door of all control houses inside the substation.
- In the event of power loss, a controlled key system with a lock box code is affixed near the control house door and at the entry gate card reader.
- Equipment for physical security shall be installed on the designated wall space inside the control house.

Communications

- Communications systems shall be installed with a minimum bandwidth to facilitate multiple users accessing the camera system from a remote site.

Tier II (Medium)

CCTV Cameras

- Cameras shall be installed to provide maximize perimeter detection. Cameras shall be installed to monitor the interior yard, the control house, and entry gates.
- Radar or a similar product is required. The radar shall be able to detect movement and enable cameras and lighting while tripping an alarm.
- Thermal cameras, PTZ, or fixed cameras should be utilized depending upon the location of the facility.
- The cameras shall have live stream capabilities.

Gates and Signage

- An automated drive gate is required.

- If seldom used gates are required for substation construction, removable fencing or jersey barriers shall be installed as necessary.
- Warning signage shall be affixed to the perimeter in a conspicuous manner and prominently on all manual or automated gates.

Perimeter Fencing and Lighting

- All fencing shall be of height and construction to deter climbing, cutting, and wildlife intrusion.
- Perimeter downcast lighting shall be installed.

Perimeter Barriers

- Jersey barriers shall be installed as needed around external transmission or distribution structures, communications equipment, or other structures.

Ballistic Protection

- Security engineering may require ballistic walls or fencing upgrades to protect equipment.

Facility Access Control

- Card readers shall be affixed next to each door of all control houses inside the substation.
- In the event of power loss, a controlled key system with a lock box code is affixed near the control house door and at the entry gate card reader.
- Equipment for physical security shall be installed on the designated wall space inside the control house.

Communications

- Communications systems shall be installed with a minimum bandwidth to facilitate multiple users accessing the camera system from a remote site.

Tier III (Low)

CCTV Cameras

- Cameras shall be installed inside the control house (if the structure is onsite) and on the outside of the control house.

Gates and Signage

- A man gate is required.
- An additional vehicle entry gate shall be installed if available.
- Warning signage shall be affixed to the perimeter in a conspicuous manner and prominently on all manual or automated gates.

Perimeter Fencing and Lighting

- All fencing shall be of height and construction to deter climbing, cutting, and wildlife intrusion.
- Perimeter downcast lighting shall be installed.

Perimeter Barriers

- Barriers are not required to be on site but should be available and centrally located in the event of heightened National Terrorism Advisory System (NTAS) security level.

Facility Access Control

- Card readers shall be affixed near each door of the control house.
- In the event of power loss, there should be a controlled key system with lock box code affixed near the control house door.

Communications

- Communications systems shall be installed with a minimum bandwidth to facilitate multiple users accessing the camera system from a remote site.

Tier IV (Minimal)

Gates and Signage

- A man gate is required.
- An additional vehicle entry gate shall be installed if available.
- Warning signage shall be affixed to the perimeter in a conspicuous manner and prominently on all manual or automated gates.

Perimeter Fencing and Lighting

- All fencing should be of height and construction to deter climbing, cutting, and wildlife intrusion.
- Perimeter downcast lighting shall be installed.

Facility Access Control

- Locks and keys are used to control access.