INL/RPT-24-77510

Cybersecurity Considerations for Dynamic Line Rating Deployment

November 2024
(Revision 0)

Idaho National Laboratory
Jake Gentle
Zach Priest
Bri Rolston

EnerNex
Jeremy Laundergan
Brian Paul Smith

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

24-GA50457_01_R3

For more information

Jake P. Gentle — Technical Point of Contact

Idaho National Laboratory

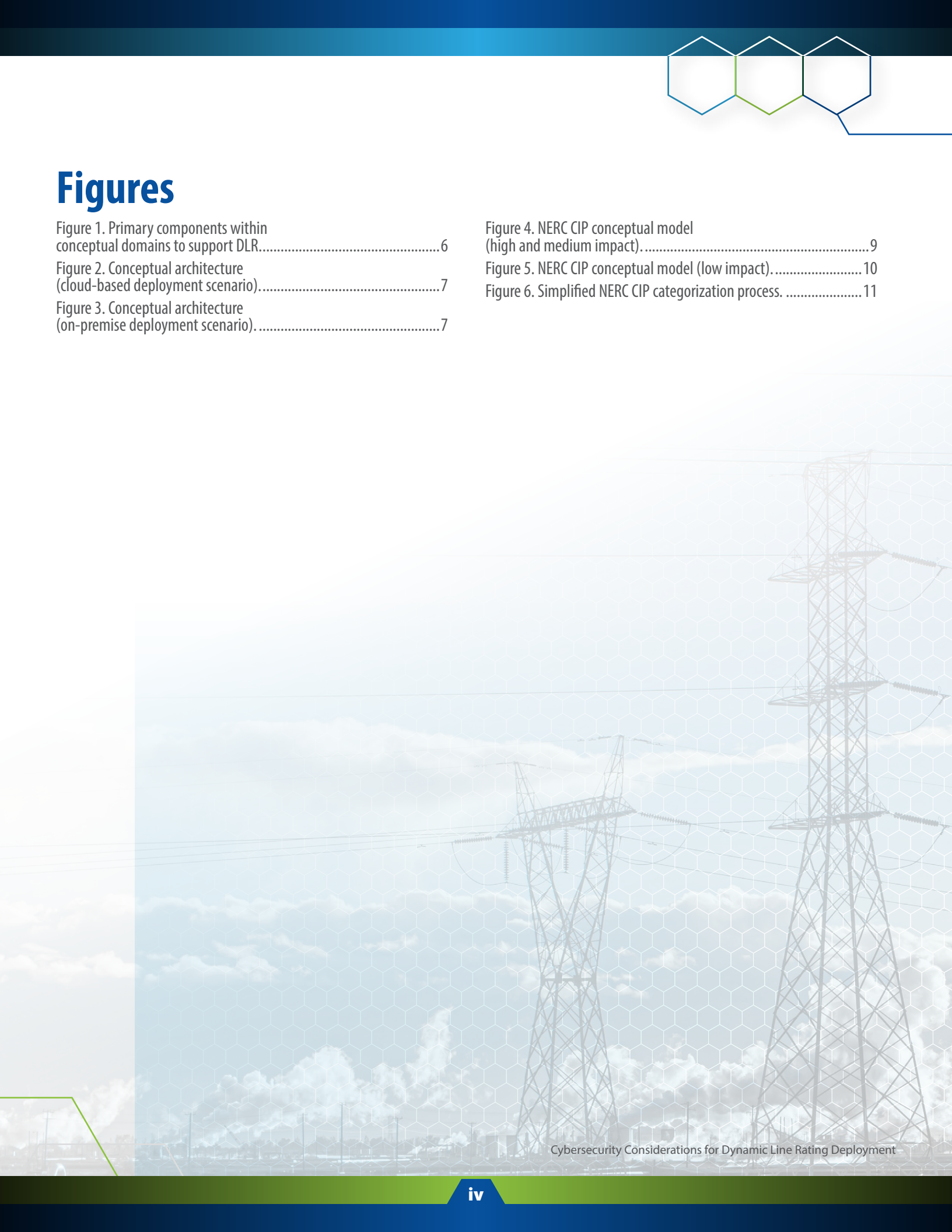
jake.gentle@inl.gov

(208) 526-1753

www.inl.gov

Contents

Figures



Acronyms

AAR	Ambient-adjusted ratings
BCS	BES Cyber Systems
BES	Bulk Electric System
BROS	BES Reliability Operating Services
CIP	Critical Infrastructure Protection
DLR	Dynamic Line Rating
EAP	Electronic Access Point
ERC	External Routable Connectivity
ESP	Electronic Security Perimeter
FERC	Federal Energy Regulatory Commission
IaaS	Infrastructure as a Service
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OT	Operational Technology
PaaS	Platform as a Service
PCA	Protected Cyber Assets
PSP	Physical Security Perimeter
SaaS	Software as a Service
SLR	Static Line Ratings
VLAN	Virtual Local Area Network

Page intentionally left blank

Cybersecurity Considerations for Dynamic Line Rating Deployment

1. FEDERAL ENERGY REGULATORY COMMISSION REQUIREMENTS FOR AMBIENT AND SYSTEM CONDITIONS MONITORING

1.1 FERC Order No. 881

Federal Energy Regulatory Commission (FERC) Order 881, issued in December 2021 and amended in May 2022, requires all transmission lines to have some level of ambient and system conditions monitoring to make better use of existing infrastructure, maintain grid reliability, and keep customer rates as low as possible. This means Transmission Providers—both inside and outside of organized markets—must implement and use ambient-adjusted ratings (AARs) as the basis for evaluating near-term Transmission Service in order to increase the accuracy of near-term line ratings.

AARs can be measured, tracked, and reported in several ways. Though its use is not mandated by Order 881, a dynamic line rating (DLR) method is one option worth considering. In this paper, the DLR method, its associated automation technology, and cybersecurity concerns will be discussed..

1.2 Grid Monitoring Parameters

FERC outlined several parameters for monitoring grid conditions, all of which affect what is measured, what types of equipment are used, and how operational technology (OT) is deployed to automate the process.
The parameters:

- Apply to a time period of not more than 1 hour
- Reflect up-to-date forecast of ambient air temperature across the time period to which the rating applies
- Account for changes of solar heating intensity at night and during the day

- Must be calculated at least once each hour
- Incorporate monthly calculation of changing sunset and sunrise times
- Must be updated every time the temperature changes 5°
- Address how AARs for transmission lines interact with system voltage and stability limits, remedial action schemes, and system operating limits.

1.3 Implementation Timeline

By July 2025, Regional Transmission Organizations and independent system operators must ensure they have procedures and systems that allow Transmission Owners to submit updated transmission line ratings electronically on at least an hourly basis. Public utility Transmission Providers will be required to maintain records of transmission line ratings as well as rating methodologies.

Changes required by the FERC order will possibly necessitate changes to Facility Ratings methodologies, as well as critical infrastructure protection (CIP) cybersecurity controls required by the North American Electric Reliability Corporation (NERC).

2. LINE RATINGS

This section defines different forms of line rating. However, it should be noted that any thermal line rating is determined by the most limiting system element, usually the conductor.

2.1 Static Line Ratings

Static line ratings (SLRs) are calculations regarding the maximum power a transmission line can safely conduct. SLRs are a function of the highest allowed conductor temperature for line operating conditions used by system operators in dispatch decisions to maintain safe operating conditions. SLRs are determined according to Institute of Electrical and Electronics Engineers (IEEE) Standard 738, "Standard for Calculating the Current-Temperature Relationship of Bare Overhead Conductors." [a]

Thermal ratings are calculated using conservative assumptions about the transmission line operating environment, such as static weather conditions, average wind speeds and direction, average ambient temperatures, and solar conditions for summer and winter seasons. While the assumptions used for SLR estimations are not worst-case (e.g., based on absolute maximum ambient temperatures, zero wind speed, or full solar exposure), there can be instances where the real ratings based on actual conditions are lower than SLRs, putting the conductor at risk for thermal damage and greater sag.

The static approach to line rating often leads to underutilization of transmission capacity, an issue that AAR or DLR line ratings can more effectively address.

2.2 AAR Line Ratings

AARs are more dynamic than traditional static rating methodologies. They utilize existing data combined with high-quality weather forecasts to model line conditions more accurately, and have been mandated by FERC in Order 881. They are often adjusted daily or hourly using ambient-temperature weather modeling to manage overhead transmission power lines more effectively.

a IEEE 738, "IEEE Standard for Calculating the Current-Temperature Relationship of Bare Overhead Conductors" https://standards.ieee.org/ieee/738/4997/.

AARs rely on models and data-driven assumptions rather than actual real-time sensor data, making them cheaper to implement than DLR, but more effective than SLRs. As a result, AAR systems can be up and running quickly and offer a reasonable idea of an overhead line's ambient conditions.

They provide a reasonable estimation of performance within the given environmental context, but AARs may not accurately reflect true line capacity if local conditions change suddenly or unexpectedly. In worst-case scenarios, this could lead to overloads or blackouts in the grid.

2.3 Dynamic Line Ratings

According to the U.S. Department of Energy, DLR is a blanket term for the many different technologies and methodologies for determining conductor thermal ratings in a more dynamic fashion using improved, more granular, or real-time data.[b] In principle, DLR uses the same heat balance equations as SLR, but DLR systems include time-varying components.

DLR is a changing transmission line rating based on local conditions, rather than a static rating assumption, and DLR provides additional ampacity capacity to a transmission line. It refers to the ability, in real time, to vary the thermal capacity of an overhead transmission or distribution power line dynamically depending on environmental conditions that directly affect line capacity.

DLR can take various forms and includes dynamic thermal line ratings, AARs, real-time thermal ratings, forecasted dynamic line ratings, and even analysis of existing lines with previously gathered data. DLR technologies have traditionally been bifurcated into weather-based and asset-based systems.[c]

Weather-based systems focus on measurement of the environmental conditions that are direct variables in the heat balance equations. Field data collected includes wind speed and direction, ambient air temperature, solar radiation, and line current. Along with engineering design criteria, these parameters are used to calculate the maximum allowable DLR conductor current.

Asset-based systems focus on measurement of the conductor itself and include local conductor temperature, position or tension, and line current.

b US DOE. (2019). "Dynamic Line Rating," https://www.energy.gov/oe/articles/dynamic-line-rating-report-congress-june-2019.

c Dino, A. and A. Ketley. (2009). Dynamic transmission line rating: technology review, Tech Rep 208478-CR-001, Hydro Tasmania Consulting..

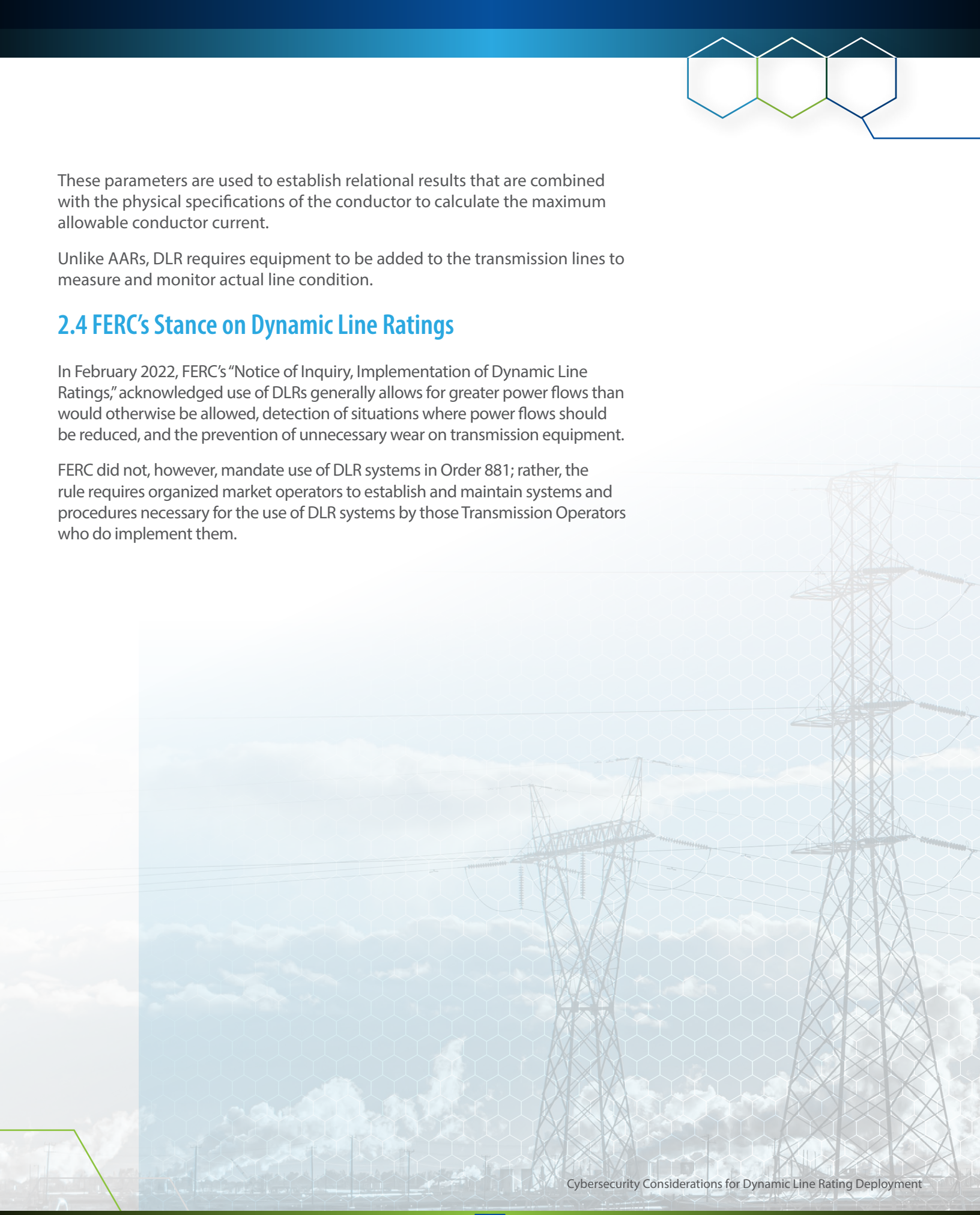
These parameters are used to establish relational results that are combined with the physical specifications of the conductor to calculate the maximum allowable conductor current.

Unlike AARs, DLR requires equipment to be added to the transmission lines to measure and monitor actual line condition.

2.4 FERC's Stance on Dynamic Line Ratings

In February 2022, FERC's "Notice of Inquiry, Implementation of Dynamic Line Ratings," acknowledged use of DLRs generally allows for greater power flows than would otherwise be allowed, detection of situations where power flows should be reduced, and the prevention of unnecessary wear on transmission equipment.

FERC did not, however, mandate use of DLR systems in Order 881; rather, the rule requires organized market operators to establish and maintain systems and procedures necessary for the use of DLR systems by those Transmission Operators who do implement them.



3. BASIC SYSTEM ARCHITECTURES

From a conceptual point of view, a DLR deployment can be represented as three primary groupings of components within the domains described in the National Institute of Standards and Technology (NIST) Smart Grid Framework conceptual architecture and as adapted in Figure 1 and Figure 2.
These include:

- (Utility) Transmission
  - » Field-deployed DLR Sensors
- (Third-Party) **Service Provider** or (Utility Back Office) **Operations**
  - » DLR Calculation Engine
- (Utility Back Office Systems) for **Operations**
  - » Service Integration
  - » Energy Management System

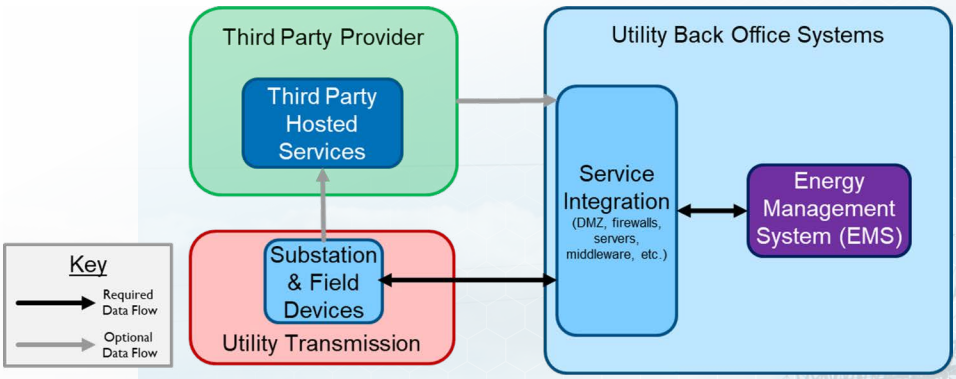


Figure 1. Primary components within conceptual domains to support DLR.

3.1 Deployment Scenarios

The basic DLR system architecture outlined in the previous section can be realized by various deployment scenarios. Certain characteristics of specific DLR system deployment scenarios may present challenges to a Responsible Entity's efforts to comply with relevant NERC CIP requirements. These scenarios represent areas that might not be compatible with Responsible Entity's existing processes and solutions for systems and devices that are

categorized as NERC CIP Bulk Electric System (BES) Cyber Systems (BCS) or Protected Cyber Assets (PCA) and include:

- Field-deployed DLR sensors that reside outside the physical substation perimeter
- Field-deployed DLR sensors that use telecommunications services not owned by the Responsible Entity, such as the commercial cellular carrier or public Internet to provide an interface for the centralized components
- A DLR calculation engine that is owned and managed by the Responsible Entity, but is hosted off-premises using computing resources supplied by a cloud service provider (infrastructure as a service [IaaS])
- A DLR calculation engine that is owned by the Responsible Entity but is managed and hosted by a third party as a cloud-based application (platform as a service [PaaS])
- A DLR calculation engine that is owned, managed, and hosted by a third party as a cloud-based application (software as a service [SaaS]).

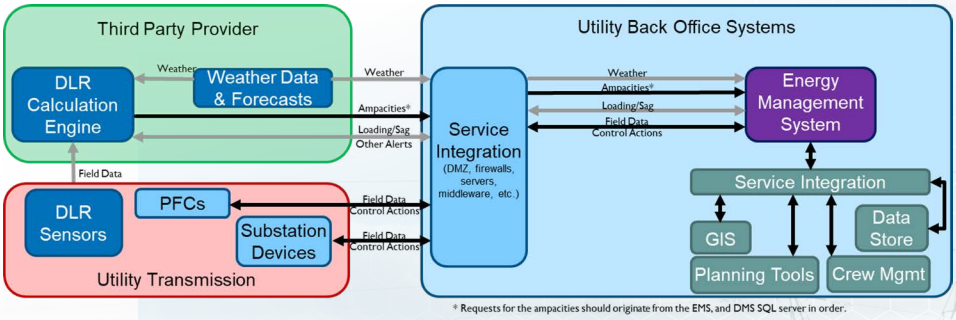


Figure 2. Conceptual architecture (cloud-based deployment scenario).

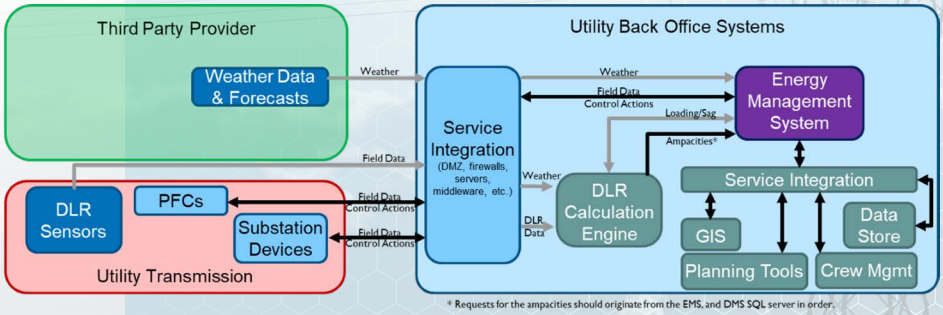


Figure 3. Conceptual architecture (on-premises deployment scenario).

4. NERC CIP IMPLICATIONS FOR DLR SYSTEMS

As many of the Responsible Entities considering implementing DLR systems are covered by NERC Reliability Standards, it is important to note a few basic facts relating to the CIP standards:

1. *Compliance with the NERC CIP Reliability Standards is achieved when the Responsible Entity builds a security program covering BCS and demonstrates that they have been operating in accordance with this program.*
2. *A system that has been designed and deployed based on cybersecurity best practices is not guaranteed to be compliant to the NERC CIP Reliability Standards.*
3. *A product or service itself cannot be NERC CIP compliant, instead that label only applies to Responsible Entities as they use products and services.*

Many Responsible Entities that are covered by the NERC CIP Reliability Standards will have established and mature compliance programs. These programs have evolved based on a classic view of the compliance model, in which the Responsible Entity physically hosts and controls all assets within the compliance footprint, as illustrated in Figure 4 (for high- and medium-impact BCS) and Figure 5 (for low-impact BCS).

The implications of NERC CIP Reliability Standards to a potential DLR system deployment are those of applicability and compatibility. The extent of the NERC CIP implications relating to a potential DLR system's deployment are primarily driven by first determining the applicability of the NERC CIP standards as per NERC CIP-002-5.1a. The compatibility of the potential DLR deployment with the Responsible Entity's existing NERC CIP compliance program is driven by the specific deployment scenario selected, as noted in Section 1.3.

Physical Security Perimeter: The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Physical Access Control Systems: Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanism, and badge readers.

Electronic Security Perimeter: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol

Electronic Access Control or Monitoring Systems: Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems

Electronic Access Point: A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside and Electronic Security Perimeter

BES Cyber System: One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity

BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy or affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Transient Cyber Asset: A Cyber Asset that is:
1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communications) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset
   - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - PCA associated with high or medium impact BES Cyber Systems.

Protected Cyber Assets: One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of the Protected Cyber Asset is equal to the highest rated BES Cyber System in the same ESP.

Cyber Assets: Programmable electronic devices, including the hardware, software, and data in those devices.

BES Cyber System Information: Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

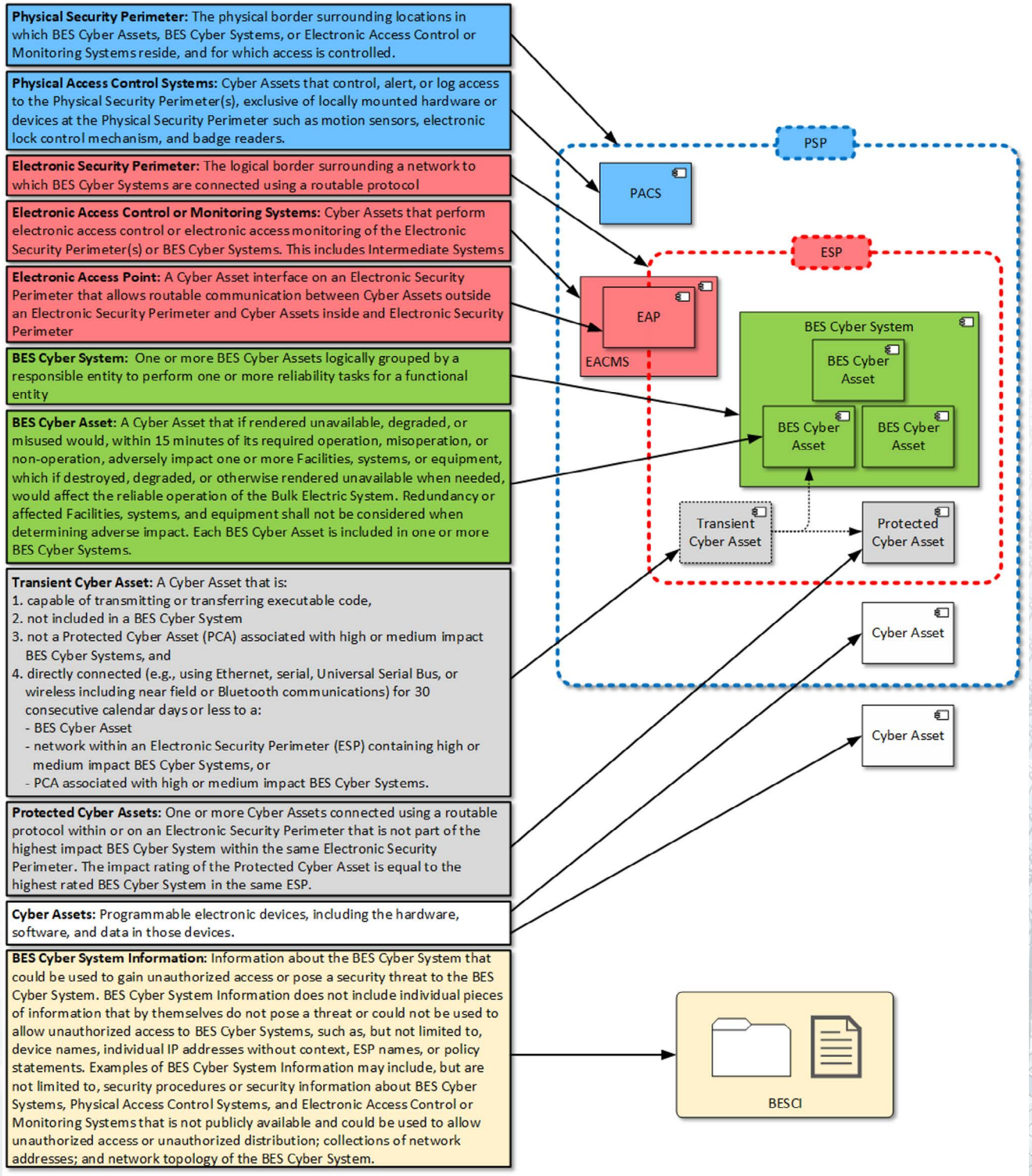


Figure 4. NERC CIP conceptual model (high and medium impact).

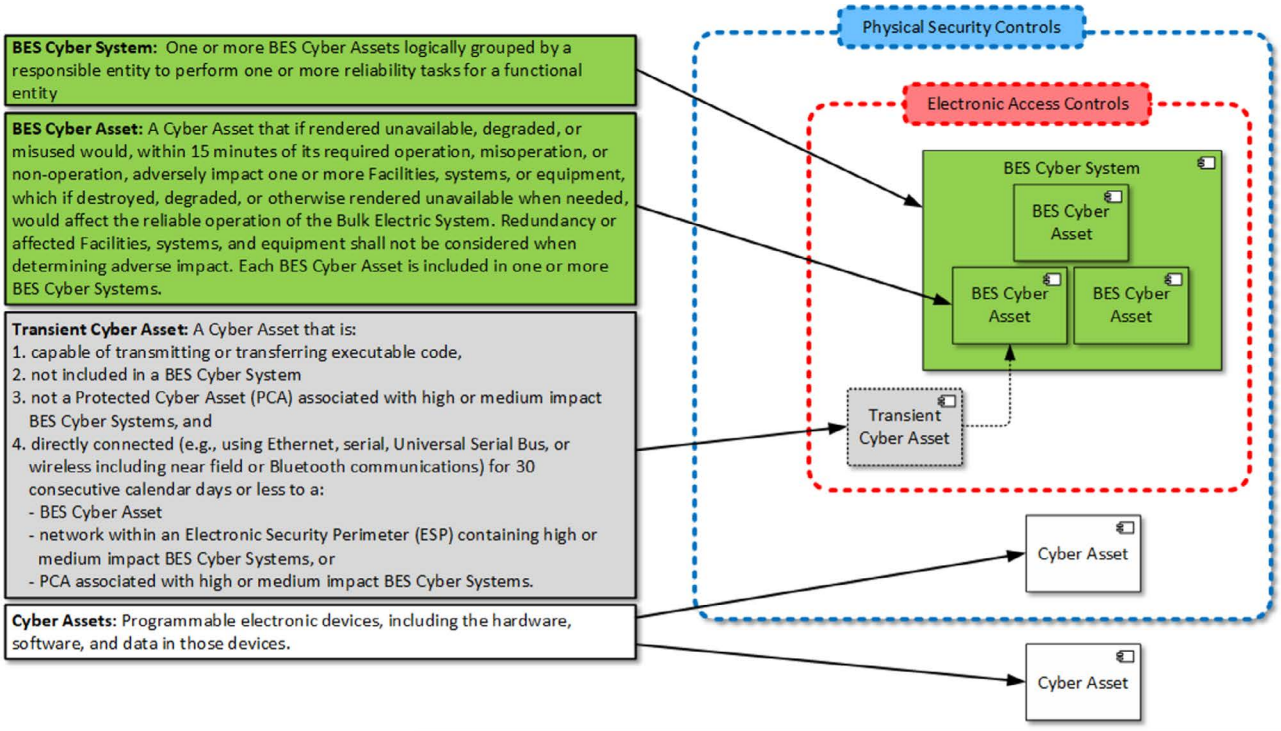


Figure 5. NERC CIP conceptual model (low impact).

5. KEY NERC CIP CONSIDERATION FOR DLR DEPLOYMENTS

5.1 Categorization of DLR System Components

NERC CIP-002-5.1a, Requirement R1, requires Responsible Entities to identify and categorize BCS.[d] The steps to appropriately apply the relevant NERC CIP standards to a DLR system are similar to those of other digital devices in a BES facility. A Responsible Entity must first identify whether the system meets the threshold of being categorized as a BCS and, if so, what impact rating would be assigned to the system. Attachment 1 of NERC CIP-002-5.1a provides guidance for these categorizations and impact ratings, and the high-level overview of this categorization process is shown in Figure 6. If the Responsible Entity determines that the DLR system or its components would not be categorized as a BCS, then a secondary categorization is performed based on the logical proximity to any BCS to determine whether they meet the definition of PCA.

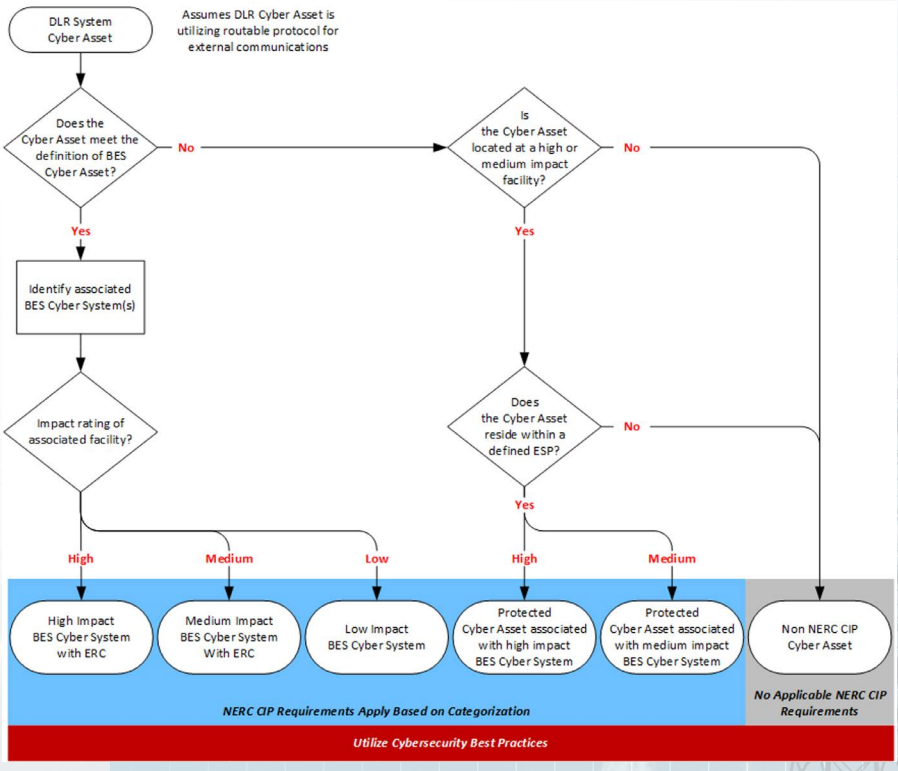


Figure 6. Simplified NERC CIP categorization process.

d See NERC CIP-002-5.1a: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf.

For DLR systems, categorization should be performed independently for the DLR calculation engine and field-deployed DLR sensors, with each having different categorization criteria for BCS determination.

5.1.1 DLR-Calculation Engine Categorization

For a DLR calculation engine, the criteria for BCS determination are based on how these components support the Responsible Entity's NERC registration and the BES Reliability Operating Services (BROS) that support these functions. If these components are identified as BCS, then the impact rating of these components is determined by the impact rating of the associated control center (i.e., High, Medium, or Low).

- Does the DLR calculation engine meet the definition of BCS? This needs to be traceable to the Responsible Entity's functional registration (e.g., Transmission Owner) and the BROS that support these functions.
  - » Does the system provide any control capabilities?
  - » How does data from the system affect operational decisions?
- The DLR calculation engine might not be owned or managed by the Responsible Entity.
  - » Is there a scenario where it can be argued that these components meet the threshold of being considered a BCS, but are owned and managed by a third-party provider?
  - » In this case, the Responsible Entity is responsible for NERC CIP compliance.
- Document a clear Responsible Entity position and justification of its categorization of the DLR calculation engine.

5.1.2 Field-Deployed DLR Sensor Categorization

For field-deployed DLR sensors, the primary criteria for BCS determination are based on potential adverse impacts to the reliable operation of the BES. If these components are identified as BCS, then they would more than likely fall into the low-impact category unless they are specifically attached to one of the Responsible Entity's medium-impact facilities.

- Do the field-deployed components of the DLR system meet the definition of BCS? How can they (or how can they not) impact the reliable operation of the BES?
  - » It is likely that field-deployed elements of a DLR system would not be considered BCS if the associated field devices are

only measuring or monitoring and do not provide control or automation capabilities.

- The field components of a DLR system might not be owned or managed by the Responsible Entity.
- Document a clear Responsible Entity position and justification of its categorization of the field-deployed components of a DLR system.

5.2 Applying NERC CIP Requirements to Cloud-Based Solutions

If it has been determined that the DLR calculation engine would meet the threshold of being categorized as a BCS, applying the appropriate NERC CIP requirements may not be feasible for deployment scenarios where the DLR calculation engine is hosted off-premises from the Responsible Entity's facilities (such as using an IaaS, PaaS, or SaaS model). It should be noted that this potential difficulty is present in any cloud-based solution for a BCS, and is not particular to DLR.

5.2.1 Low-Impact BCS

NERC CIP-003-8, Requirement R2, requires Responsible Entities to document a plan and to implement technical controls to meet the cyber and physical security objectives which have been outlined in Attachment 1 for low-impact BCS.

As many Responsible Entities have the required cybersecurity plans documented, these have typically been created for scenarios where low-impact BCS are owned by the Responsible Entity and located within its substation or control center. In cases where a Responsible Entity has determined that the DLR calculation engine meets the threshold of being categorized as a low-impact BCS, certain aspects of the Responsible Entity's existing cybersecurity plans may be difficult to apply for specific DLR system architectures where some or all these components are provided by a vendor or third party. Furthermore, providing evidence of a third-part's compliance with the Responsible Entity's documented plans, when the Responsible Entity does not own or control these elements, may present significant additional challenges.

5.2.2 Electronic Security Perimeter

NERC CIP-005-7, Requirement R1 addresses establishing an Electronic Security Perimeter (ESP) around applicable high- and medium-impact BCS as well as monitoring and controlling communications into and out of this boundary.

Responsible Entities have typically established ESPs based on the physical interface of a firewall that is owned and controlled by the Responsible Entity. The network infrastructure and anything connected to it downstream from this interface would then be considered in scope of the NERC CIP standards as either a BCS or PCA.

For deployment scenarios where a DLR calculation engine is hosted off-premises from the Responsible Entity's facilities (using an IaaS, PaaS, or SaaS model), the hyperconverged infrastructure used by the cloud service provider represents a significant challenge when applying the ESP requirements within the NERC CIP standards. Although virtualization technology allows for logical segregation, it has typically not been embraced as an acceptable method for establishing an ESP under the current version of the NERC CIP standards.

For instance, in many environments, it is common practice to segregate systems using multiple virtual local area networks (VLANs) configured on the same Ethernet switch. In NERC CIP environments, all VLANs on this Ethernet switch would typically be considered within the ESP defined by the associated firewall interface. Any assets that the Responsible Entity desires to keep outside of the scope of the NERC CIP standards would then use a separate network infrastructure connected to a physically separate firewall interface. For this reason, demonstrating that the Responsible Entity has established, controls, and monitors an ESP around a DLR calculation engine that is hosted off-premises and has been categorized as a BCS would be difficult

5.2.3 Remote Access

NERC CIP-005-7, Requirement R2, addresses managing remote interactive access to high- and medium-impact BCS. Responsible Entities must ensure that the system initiating the remote access request does not directly access an applicable cyber asset, instead using an intermediate system (i.e., a jump host). Responsible Entities must also ensure encryption is employed and terminates at an intermediate system, as well as set up multifactor authentication for the initial remote access session. Additionally, Responsible Entities must be able to both determine active remote access sessions and disable them.

5.2.4 Physical Security of Cyber Systems

NERC CIP-006-6 addresses physical security of high- and medium-impact BCS and associated PCA. In cases where a third party provides the DLR calculation engine, the Responsible Entity may not be provided the capability to manage physical security of the systems used for DLR calculation.

5.2.5 Patch Management and Malicious-Code Prevention

NERC CIP-007-6, Requirement R2, addresses security patch management and Requirement R3 addresses malicious code prevention for high- and medium-impact BCS and PCA.

As many Responsible Entities have the required patch management and malicious code prevention processes documented, these have typically been created for scenarios where BCS and PCA are owned by the Responsible Entity and located within its substation or control center. In cases where the Responsible Entity has determined that the DLR calculation engine meets the threshold of being categorized as high- or medium-impact BCS or PCA, certain aspects of the Responsible Entity's existing patch management and malicious code prevention processes may be difficult to apply to specific DLR system architectures when some or all these components are provided by a vendor or third party. Furthermore, providing evidence of a third party complying to the Responsible Entity's patch management or malicious code prevention processes when the Responsible Entity does not own or control these elements may present additional challenges.

For example, a Responsible Entity's patch management or malicious code prevention processes may have been developed based on solutions using specific on-premises management tools owned by the Responsible Entity, such as Microsoft Configuration Manager for the Microsoft Windows operating system or Red Hat Satellite for Red Hat Enterprise Linux hosts. Extending these tools to manage components provided by a third party may not be feasible or pose a significant risk to the Responsible Entity.

5.2.6 Security Event Monitoring

NERC CIP-007-6, Requirement R4, addresses security event monitoring for high- and medium-impact BCS and PCA.

In cases where a third party provides a DLR calculation engine as a SaaS, the Responsible Entity may not be provided the capability to collect cybersecurity logs from these components to generate the required alerts.

5.2.7 System Access Controls

NERC CIP-007-6, Requirement R5, addresses system access controls for high- and medium-impact BCS and PCA.

In cases where a third party provides the DLR calculation engine, the Responsible Entity may not be provided the capability to manage and enforce the associated access controls.

5.3 Applying NERC CIP Requirements to DLR Sensors

5.3.1 Low-Impact BCS

NERC CIP-003-8, Requirement R2, requires Responsible Entities to document a plan and to implement controls to meet the security objectives that have been outlined in Attachment 1 for low-impact BCS. Unlike the more prescriptive requirements for high- and medium-impact BCS, CIP-003-8 provides some flexibility for Responsible Entities to determine the appropriate controls to meet these objectives.

As most Responsible Entities have documented the required cybersecurity plans, these have typically been created for scenarios where low-impact BCS, deployed in the field, are owned by the Responsible Entity and located within its substation. In cases where the Responsible Entity has determined that the DLR sensors meet the threshold of being categorized as low-impact BCS, certain aspects of the Responsible Entity's existing cybersecurity plans may be difficult to apply to DLR system architectures where any of the following are true:

- Components are located outside the substation perimeter
- Components are managed by a third party
- Components use wireless communications technology.

5.3.2 Electronic Security Perimeter

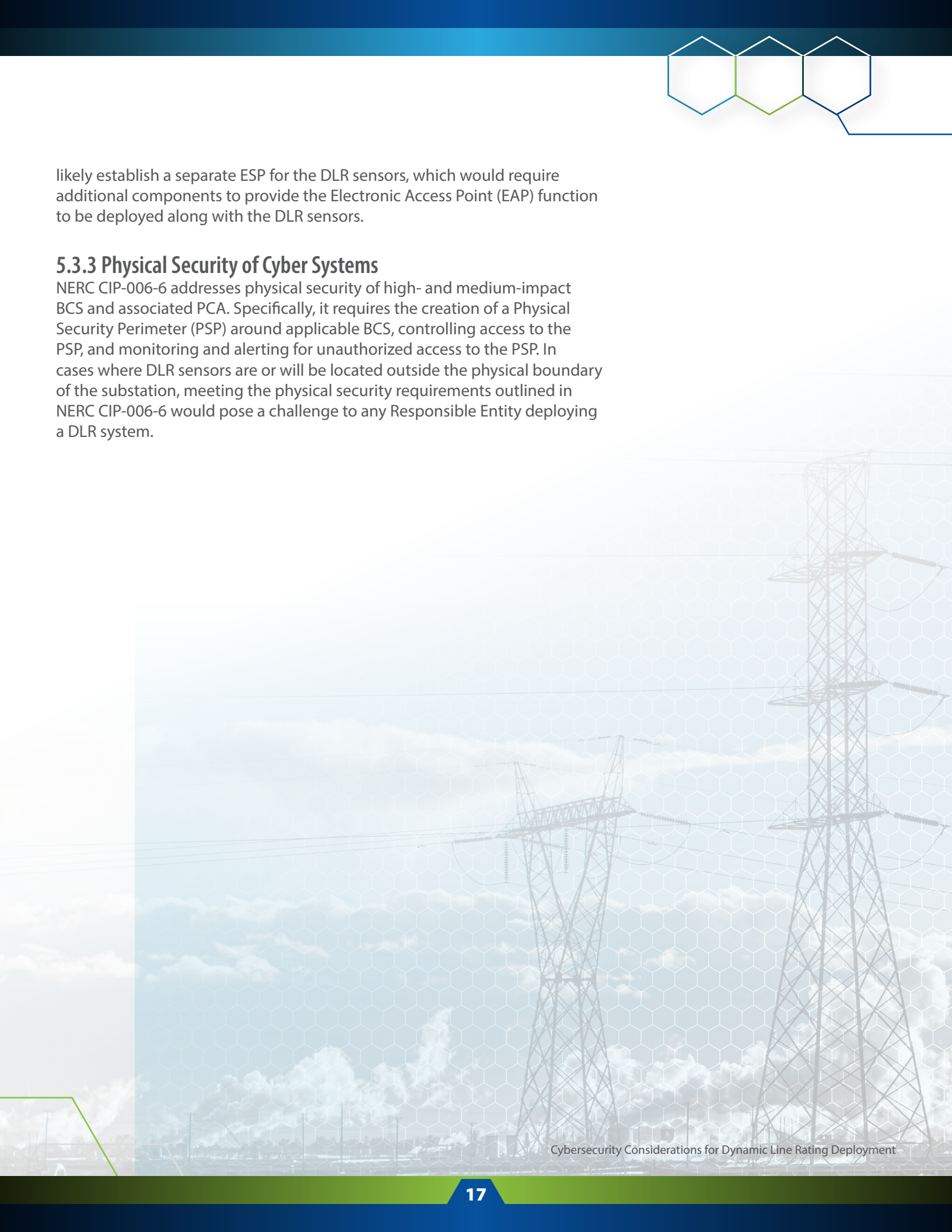
NERC CIP-005-7, Requirement R1, addresses the establishment of an ESP around applicable high- and medium-impact BCS as well as monitoring and controlling communications into and out of this boundary. Responsible Entities have typically established ESPs based on the physical interface of a firewall that is owned and controlled by the Responsible Entity. The network infrastructure and anything connected to it downstream from this interface would then be considered in scope of the NERC CIP Standards as a BCS or PCA.

In many deployments, DLR sensors are located outside of the traditional boundaries of the Responsible Entity substation on specific structures or spans of the transmission line. High-impact ratings are limited to only specific control centers; thus, the DLR sensors would never fall into a high-impact categorization under the current construct. If, however, the DLR sensors are determined to be BCS and associated with one of the Responsible Entity's medium-impact substations, then these systems would be required to reside within a defined ESP. While possible to do so while remaining compliant, extending the ESP from the associated substation would introduce difficulty and complexity. Therefore, in this case, the Responsible Entity would more

likely establish a separate ESP for the DLR sensors, which would require additional components to provide the Electronic Access Point (EAP) function to be deployed along with the DLR sensors.

5.3.3 Physical Security of Cyber Systems

NERC CIP-006-6 addresses physical security of high- and medium-impact BCS and associated PCA. Specifically, it requires the creation of a Physical Security Perimeter (PSP) around applicable BCS, controlling access to the PSP, and monitoring and alerting for unauthorized access to the PSP. In cases where DLR sensors are or will be located outside the physical boundary of the substation, meeting the physical security requirements outlined in NERC CIP-006-6 would pose a challenge to any Responsible Entity deploying a DLR system.



6. CONCLUSIONS

6.1 Deployment Scenarios

Currently, a deployment scenario where the DLR calculation engine is hosted as IaaS, PaaS, or SaaS using a cloud service provider will be difficult to implement in a NERC CIP compliant manner. If a DLR calculation engine is determined to be a BCS, then the Responsible Entity should consider a deployment scenario where the DLR calculation engine is hosted on-premises. This would not preclude an arrangement where the DLR vendor operates and maintains the DLR calculation engine. The Responsible Entity should work with their respective Regional Entity to evaluate any DLR system deployment plan for CIP compliance purposes.

6.2 Reference Architecture Scenarios

Ideally, Responsible Entities considering deployments of DLR systems would benefit from a set of reference architectures and implementation guidance customized for various deployment scenarios that are compliant with NERC CIP and a Responsible Entity's respective Regional Entity. Unfortunately, such resources are currently unavailable. In the absence of these resources, it's essential for each Responsible Entity that has implemented or is considering the implementation of a DLR system to develop its own reference architecture. This reference architecture should align with the capabilities of the DLR system and adhere to comprehensive cybersecurity best practices. Additionally, it should clearly define critical deployment details, such as the categorization of each system component, system boundaries, and the applicable NERC CIP requirements. The ultimate goal of this reference architecture is to ensure cohesive alignment among the information technology (IT), OT, and compliance groups involved in both the deployment and ongoing operation of the DLR system.