



PNNL-27062 / NASPI-2017-TR-006

Prepared for the U.S. Department of Energy
Under Contract DE-AC05-76RL01830

Recommended Guidelines for NERC CIP Compliance for Synchrophasor Systems

SR Mix
H Kirkham
A Silverstein

November 2017



Pacific Northwest
NATIONAL LABORATORY

*Proudly Operated by **Battelle** Since 1965*

DISCLAIMER

This documentation was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.** Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401, fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847, fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: <http://www.ntis.gov/ordering.htm>



This document was printed on recycled paper.

Recommended Guidelines for NERC CIP Compliance for Synchrophasor Systems

SR Mix
H Kirkham
A Silverstein

November 2017

Prepared for the North American Synchrophasor Initiative
under an agreement with
U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Executive Summary

Compliance with the NERC requirements for Critical Infrastructure Protection (CIP) for synchrophasor systems in the Version 5 paradigm¹ seems to be a matter of some uncertainty for those in the synchrophasor user community. In the words of the Edison Electric Institute, an organization that represents the investor-owned utilities,²

It is clear that a strong appetite exists for clarifying understandings of the broad range of technical requirements under CIP V5, and several process issues that govern implementation of NERC standards.

This report aims to provide clarification and guidance in the form of case studies based on methods seen in the industry.³

Section 1 is a brief introduction to this report.

Section 2 gives a brief history of the development of the CIP Standards, the entities involved (primarily NERC, NIST and DHS), and briefly discusses considerations for future compliance.

Section 3 deals with the matter of categorization, the topic of CIP-002-5, seemingly one of the most challenging aspects of CIP V5. The section illustrates by example methods for five implementations of a phasor measurement unit (PMU) in a transmission station or generation switchyard, and two for a phasor data concentrator (PDC) at a Control Center.

Section 4 discusses general compliance expectations for BES Cyber Assets identified in the scenarios described in Section 3, and includes some cyber security recommendations beyond those required for strict NERC CIP compliance. The requirements of the other CIP Standards are also discussed.

Section 5 gives some examples of some implementation options, from minimally compliant to fully compliant.

Section 6 draws some conclusions. The CIP standards are seen as establishing a baseline of performance expectations. Compliance does not equal security, and utilities should not fear audit repercussions if they attempt to exceed a particular requirement but fail to meet a more stringent self-imposed requirement in seeking to achieve a more secure synchrophasor system, as long as they continue to meet the baseline requirements.

Section 7 offers some opportunities for further reading on compliance approaches.

¹ The Version 5 paradigm refers to the set of NERC CIP standards approved in 2012. Although standards development on these standards continues with individual standards' version numbers incrementing, the set of standards is still referred to as the "Version 5" family of standards.

² <http://www.nerc.com/pa/CI/Documents/Industry%20Comments%20-%20Transition%20Guidance%20Draft%20for%20CIP%20V5.pdf>, document page 60, accessed 11/1/2017. The words are from "CIP V.5 Implementation Issues / Comments of the Edison Electric Institute and the Electric Power Supply Association on Draft Transition Implementation Guidance"

³ As of the writing of this report (fall 2017) some changes to the standards have been submitted to FERC, but not yet approved, and additional changes are still being developed. This report will include the current status of those changes, and note where they exist. Unless otherwise noted, the discussions will be concerning approved and enforceable requirements.

Acknowledgments

The authors would like to acknowledge the following members of the NERC Synchronized Measurement Subcommittee (SMS) for their suggestions and review of the report:

J Bucciero, Quanta Technology
D Gacek, Commonwealth Edison
AR Goldstein, National Institute of Standards and Technology
D Hislop, PJM Interconnection
A Johnson, Southern California Edison
J Kleitsch, American Transmission Company
A Lee, Nevermore Security
C Parker, Southwest Power Pool
DC Schooley, Commonwealth Edison

Acronyms and Abbreviations

BCA	BES Cyber Asset
BCS	BES Cyber System
BES	Bulk Electric System
BPS	Bulk-Power System
BROS	BES Reliability Operation Services
CIP	Critical Infrastructure Protection
DHS	U.S. Department of Homeland Security
DMZ	demilitarized zone
DOE	U.S. Department of Energy
E-ISAC	Electricity Information Sharing and Analysis Center
EACMS	Electronic Access Control or Monitoring System
EAP	Electronic Access Point
EHV	Extra High Voltage
EMS	Energy Management System
ERO	Electricity Reliability Organization
ESP	Electronic Security Perimeter
FERC	Federal Energy Regulatory Commission
FISMA	Federal Information Security Management Act
FTP	file transfer protocol
GOOSE	Generic Object Oriented Substation Events
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSEC	Internet Protocol Security
IROL	Interconnection Reliability Operating Limit
ISO	Independent System Operator
IT	Information Technology
kV	Kilo Volt
LAN	Local Area Network
MVAR	Mega Volt Ampere Reactive
MW	Mega Watt
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NPIR	Nuclear Plant Interface Requirement
OT	Operations Technology
PACS	Physical Access Control System
PCA	Protected Cyber Asset
PDC	phasor data concentrators
PMU	phasor measurement units
PRA	Personnel Risk Assessment
PSP	Physical Security Perimeter
RAS	Remedial Action Scheme
RBAM	Risk-based Assessment Methodology
RTO	Regional Transmission Organization
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SDT	Standard Drafting Team

SPS	Special Protection Scheme
SSH	secure shell
TCA	Transient Cyber Asset
TCP	Transmission Control Protocol
USB	Universal Serial Bus
UDP	User Datagram Protocol
UFLS	Underfrequency Load Shedding
UVLS	Undervoltage Load Shedding

Table of Contents

<i>Executive Summary</i>	<i>ii</i>
<i>Acknowledgments</i>	<i>iii</i>
<i>Acronyms and Abbreviations</i>	<i>iv</i>
1.0 Introduction	1
2.0 Background	5
<i>Organization and Development History</i>	5
2.1.1 NERC	5
2.1.2 NIST	6
2.1.3 Present Situation	7
<i>Considerations for Future Compliance</i>	8
3.0 CIP V5 Categorization Criteria and Process	10
<i>Scoping and Definitions</i>	10
3.1.1 CIP-002 Version 5 Definitions	11
<i>BES Cyber Asset Determination</i>	14
<i>Impact Level Determination</i>	19
<i>Transmission Station Impact Level Determination</i>	20
3.1.2 Criterion 2.2	21
3.1.3 Criterion 2.4	21
3.1.4 Criterion 2.5	22
3.1.5 Criterion 2.6	23
3.1.6 Criterion 2.7	24
3.1.7 Criterion 2.8	24
3.1.8 Criterion 2.9	24
3.1.9 Criterion 2.10	25
3.1.10 Low Impact Criteria	25
<i>Control Center Impact Level Determination</i>	26
3.1.11 High Impact Control Centers	26
3.1.12 Medium Impact Control Centers	27
3.2 <i>BES Cyber Asset Determination Examples</i>	27
3.2.1 Low Impact, non BES Cyber Asset	27
3.2.2 Low Impact, BES Cyber Asset	29
3.2.3 Medium Impact, non BES Cyber Asset, non-Protected Cyber Asset	30
3.2.4 Medium Impact, non-BES Cyber Asset, Protected Cyber Asset	30
3.2.5 Medium Impact, BES Cyber Asset	31
<i>Control Center Examples</i>	32
3.2.6 PDC at Medium Impact Control Center	32
3.2.7 PDC at High Impact Control Center	33
<i>Communication Networks</i>	33
<i>Applications using Synchrophasor Data</i>	34

<i>Distribution</i>	34
4.0 Synopsis of NERC CIP Requirements	35
<i>Low Impact Requirements</i>	35
<i>Medium Impact with Externally Routable Connectivity Requirements at a Station</i>	37
4.1.1 Requirements from CIP-003 – Security Management Controls	37
4.1.2 Requirements from CIP-004 – Personnel and Training	38
4.1.3 Requirements from CIP-005 – Electronic Security Perimeters	40
4.1.4 Requirements from CIP-006 – Physical Security of BES Cyber Systems	41
4.1.5 Requirements from CIP-007 – Systems Security Management	42
4.1.6 Requirements from CIP-008 – Incident Reporting and Response Planning	43
4.1.7 Requirements from CIP-009 – Recovery Plans for BES Cyber Systems	44
4.1.8 Requirements from CIP-010 – Configuration Change Management and Vulnerability Assessments	44
4.1.9 Requirements from CIP-011 – Information Protection	46
<i>Medium Impact Requirements at a Control Center</i>	46
4.1.10 Additional Requirements from CIP-005 – Electronic Security Perimeters	46
4.1.11 Additional Requirements from CIP-006 – Physical Security of BES Cyber Systems	46
4.1.12 Additional Requirements from CIP-007 – Systems Security Management	47
4.1.13 Additional Requirements from CIP-009 – Recovery Plans for BES Cyber Systems	47
<i>High Impact Requirements</i>	48
4.1.14 Additional Requirements from CIP-005 – Electronic Security Perimeters	48
4.1.15 Additional Requirements from CIP-006 – Physical Security of BES Cyber Systems	48
4.1.16 Additional Requirements from CIP-007 – Systems Security Management	48
4.1.17 Additional Requirements from CIP-009 – Recovery Plans for BES Cyber Systems	48
5.0 Implementation Options	50
5.1.1 Minimal Classification	50
5.1.2 Partial Classification	51
5.1.3 Full Classification	52
5.1.4 Recommended Practices Results	53
6.0 Conclusion	55
7.0 Further Reading	56

Figures

Figure 1: BROS to Entity Registration Mapping	14
Figure 2: Classifying a PMU or PDC in station.....	16
Figure 3: Network Connected PMU and PDC	18
Figure 4: Serially Connected PMU	18
Figure 5: CIP-002 Categorization	19
Figure 6: PMU or PDC operated in substation, not for control	28
Figure 7: PMU or PDC operated in substation, with station LAN, not for control.....	28
Figure 8: PMU data used for real-time decision making	29
Figure 9: PMU data used for real-time decision making, here part of a Relay	29
Figure 10: PMU or PDC operated in substation, without ESP, not for control	30
Figure 11: PMU or PDC operated in substation, with ESP, not for control.....	31
Figure 12: PMU or PDC operated in substation, for control or by operators	31
Figure 13: PMU or PDC operated in substation, shared LAN, for control or by operators	32

Recommended Guidelines for NERC CIP Compliance for Synchrophasor Systems

1.0 Introduction

Many synchrophasor systems now in place appear to have insufficient or inconsistent levels of physical and cyber-security to be compliant as NERC CIP Version 5¹ BES Cyber Assets (or BES Cyber Systems). That makes them unsuitable to support real-time operations.

Synchrophasor systems are geographically dispersed systems comprising phasor measurement units (PMU), phasor data concentrators (PDC), applications that uses data (including processing and presentation or visualization), and communication networks that connect the various components together.

This report is a recommendation guide for synchrophasor systems adopters to use as they develop a NERC CIP-compliant synchrophasor system. It is designed to make the system security measures called for in NERC CIP standards clearer and more accessible.² In particular, CIP-002, which introduces the concept of a BES Cyber Asset, and deals with categorization, can be challenging. The report addresses the CIP Version 5 standards, which are the standards currently being enforced.³

The NERC CIP requirements are generally device-centric, so the majority of the security recommendations in this report focus on applying the NERC CIP requirements to PMU devices and PDC devices. CIP Version 5 introduced the concept of BES Cyber Systems to assist utilities⁴ performing and documenting compliance actions by reducing the amount of required compliance documentation, and in some cases, to allow one BES Cyber Asset in a BES Cyber System to perform required actions on behalf of other BES Cyber Assets in the BES Cyber System. Refer to Section 3.1.1 for additional information.

Applications that use synchrophasor data are contained inside the control system located at either a field location (e.g., a station) or at a Control Center. Security of those applications is applied by securing the BES Cyber Assets that house the data and applications. If an application is not used in real-time decision

¹ The Version 5 paradigm refers to the set of NERC CIP standards approved in 2012. Although standards development on these standards continues with individual standards' version numbers incrementing, the set of standards is still referred to as the "Version 5" family of standards.

² It is fair to observe that as far as readability is concerned, the writing of the Standard documents leaves much to be desired. Often, important requirements are embedded in lists of definitions made up of phrases of sixty or seventy words, the entire structure lacking verbs, and not interpretable as sentences. When we encounter such situations, we will quote the material verbatim, and offer our own clarification.

³ As of the writing of this report (fall 2017) some changes to the standards have been submitted to FERC, but not yet approved, and additional changes are still being developed. This report will include the current status of those changes, and note where they exist. Unless otherwise noted, the discussions will be concerning approved and enforceable requirements.

⁴ This report refers to the companies that must comply with the CIP standards by the term "utilities," even though organizations like Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs) are not utilities in the traditional sense. The standards themselves use the phrase "Responsible Entities" which itself refers to organizations (traditional utilities including investor owned, cooperative and municipal, and other organizations like ISOs and RTOs) which are registered for specific functions under the NERC functional model. In other contexts, the term "registered entities" is also used.

making, or the data is not used in autonomous control applications, its use is considered outside the scope of the NERC CIP requirements.

There are currently no CIP requirements for field communications (i.e., communications from a transmission station to a Control Center, or between transmission stations) so field communications is currently out of scope for NERC CIP compliance; however, security recommendations for these communications are discussed in this report as recommended practices, currently outside the scope of specific NERC CIP requirements or compliance.⁵

Compliance with NERC CIP is mandatory, but will not (indeed, cannot) guarantee security. According to an article in IEEE Spectrum,⁶ the U.S. power system is no less vulnerable to cyber-attack than was the system in Ukraine, which was blacked out by hackers in December 2015, with about 225,000 people disconnected. Our concern in this report is not directly with improving that cybersecurity situation. We are concerned with NERC CIP compliance. NERC CIP requirements are concerned with cybersecurity (among other aspects of infrastructure protection). There is a tension between security and compliance – in the case of security patching, for instance, a compliance mindset seeks to assure that a process is in place to ensure that patches are analyzed within the required 35 days, while a security mindset would focus on the quality and speed of the patch analysis process. Utilities must balance both of these mindsets, and not let either one dominate the organization’s implementation CIP standards.

Extensive investments in infrastructure protection and security technology cannot guarantee complete security. But by complying with the NERC CIP standards, the utility has at least implemented a basic level of security and protection, as well as the security required by regulation, and is by definition following industry good security practices.

Organization

The report is organized as follows.

Section 2 discusses CIP history, including a brief history of the development of the NERC CIP Standards, and parallel activities undertaken by NIST. It also discusses compliance considerations when installing systems that do not yet need to be compliant with the NERC CIP standards.

Section 3 discusses the NERC impact rating criteria, and what computer systems (Cyber Assets in the CIP lexicon) the CIP standards apply to. It further discusses categorization of BES assets, which determine the applicable CIP requirements.

Implementation recommendations of this report are presented starting with a discussion of determining the impact level of a BES Cyber Asset, followed by nine NERC CIP compliance scenarios, five representing the possible scenarios for PMUs or PDCs at field locations such as transmission stations or generation switchyards, two discussing phasor data concentrators (PDC) located at a Control Center, one discussing how the CIP Standards apply to applications, and a brief discussion of synchrophasor systems in other environments.

Section 4 discusses the expectations from the NERC CIP standards for BES Cyber Assets identified in the scenarios discussed in Section 3. Included in the discussion of these scenarios are some suggestions for implementing security beyond the minimum requirements from the NERC CIP Standards.

⁵ See the exclusion clause in section 4.2.3.2 of all the standards, and language in FERC Order No 822 PP 57 stating that the Commission will not require security on communications except between Control Centers.

⁶ Peter Fairley, “Cybersecurity at U.S. utilities due for an upgrade,” IEEE Spectrum, May 2015, pp. 11-13.

Section 5 outlines implementation options including minimal classification, partial classification and full classification options.

Section 6 offers some concluding remarks. The CIP standards establish a minimum floor of performance expectations. Compliance does not equal security, and utilities should not fear audit repercussions if they attempt to exceed a particular requirement but fail to meet a self-imposed more stringent requirement.

Section 7 offers some opportunities for further reading on compliance approaches.

Caveats and explanation

As stated above, compliance with the NERC CIP Standards will not guarantee a secure system, while a secure system may not necessarily meet all the compliance requirements of the NERC CIP standards. Utilities must understand both compliance obligations and security expectations, and strive to be both compliant and secure.

The description of the requirements, and recommendations presented in this report should not be taken as an authoritative statement of the actual NERC CIP standards requirements. In order to maximize this report's usefulness as the CIP standards undergo revision, detailed requirements language, applicability, etc. are not included. Readers should refer to the latest version of the standards on the NERC website⁷ for currently enforceable standards (in the U.S.) for the specific requirements language and applicability statements.

When reading the language of any NERC standard, it is important to understand that certain terms used in the requirements language are terms from the "Glossary of Terms Used in NERC Reliability Standards"⁸. These terms are identified by the use of capital letters in the requirement language. It is important to note that if a term is *not* capitalized in the requirements language, it *does not* refer to a NERC glossary term (even if the term is defined in the glossary).

This report uses the terms "annual" and "monthly"; however, the actual language in the NERC CIP Standards is "15-month" and "35-day." The standards specify actual performance timeframes as the absolute longest time period allowed before the requirement is determined to have not been met, and are intended to provide a grace period to account for holidays, vacations, and system conditions. Utilities are encouraged to perform annual requirements on a 12-month basis, allowing for a three-month grace period to cover unexpected conditions. Similarly, monthly performance is most readily accomplished on a four-week (28-day) or "same day every month" (every 28 to 31 days) approach, allowing for a four to seven day grace period.

This report also uses the term "real-time" as a reference to the "15 minute" threshold contained in the definition of a BES Cyber Asset. The definition uses 15 minutes as a specifically measurable parameter, while the term "real-time" (although not specifically defined) is a well understood concept, separating "real-time" operations performed by a power system operator from "non-real-time" actions performed in a planning department. This is further discussed in the context of the BES Cyber Asset definition in Section 3.1.1

⁷See http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United_States, accessed 11/1/2017

⁸ See http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf, accessed 11/1/2017

While not discussed in this report, there are several cases in the standards requirement language that use the phrase, “where technically feasible.” This wording allows utilities in those specific instances to implement alternatives to the strict reading of the requirement, but still maintain security outcomes as close to the intent of the language as possible. The Technical Feasibility Exception (TFE) process requires that these alternatives be submitted for advance approval, and if approved, will be used for compliance auditing, in lieu of the strict language in the requirement.

There are many ways to be compliant with NERC Standards, and the NERC CIP Standards are no exception. The following sections offer high-level approaches to implementing the standards in what is intended to be a clearer plain-English approach, with some suggestions and examples provided.

2.0 Background

2.1 Organization and Development History

2.1.1 NERC

The NERC (North American Electric Reliability Corporation) CIP (for Critical Infrastructure Protection) Standards have evolved over time. NERC was formed (originally as the National Electric Reliability Council) in 1968 in response to the major blackout of 1965. The name was changed in 1981 to “North American” to acknowledge the participation of Canada. Over the years, NERC developed reliability-oriented guidelines and practices that were voluntary in nature, with no incentives for compliance, nor penalties for non-compliance other than industry peer pressure.

In 2004, following the 2003 U.S.-Canada blackout and under pressure from the Federal Energy Regulatory Commission (FERC), NERC created a permanent committee on Critical Infrastructure Protection, and issued a set of 90 measurable standards known as the “Version 0 Reliability Standards” (based on prior industry-developed reliability infrastructure guidelines). Voluntary compliance with the Version 0 standards (as a set of guidelines) was expected as a matter of good practice, effective in April 2005. At the same time, NERC submitted the Version 0 standards (including 90 measurable standards, and 12 “fill-in-the-blank” standards which specified that each reliability region specify applicable requirements) to FERC as an informational filing.

Following the enactment of the Energy Policy Act in August 2005, NERC applied to FERC to become the US “Electric Reliability Organization,” or ERO, and formally filed the Version 0 standards for approval in 2006.

Following certification by FERC as the ERO,⁹ on January 1, 2007 NERC was re-organized with an independent board, and renamed the North American Electric Reliability Corporation. Later in that year, FERC approved 83 NERC Reliability Standards (of the 102 standards filed in 2006). In June 2007, compliance with those standards became mandatory and enforceable, with penalties and sanctions associated with non-compliance. Version 1 of the CIP standards was approved in January 2008, with phased-in implementation.

FERC Order No. 706, the order approving the initial set of CIP standards, directed NERC to modify various aspects of the standards, including some that FERC wanted complete before the implementation date. To meet these FERC directives, NERC formed a Standards Drafting Team (SDT) of industry members to undertake the rapid development, submission, and approval of “Version 2” and “Version 3” of the standards. Version 3 remained the enforceable version until FERC approved “Version 5” of the standards in late 2013 under FERC Order No. 791. (Version 4 was developed and approved, but never implemented.) Compliance with Version 5 was required of all applicable utilities by April 1, 2016 (later delayed to July 1, 2016).

Version 5 implements all of the directives issued in FERC Order No. 706 (the FERC order approving Version 1), and incorporates various lessons learned from implementation of Versions 1 through 3.

⁹ NERC also signed MOUs with the Canadian provinces to enable performance as the ERO within Canada as well as in the U.S.

Version 5 represents a complete re-write of the standards, dramatically changing the scope of applicability of the requirements, and the format in which they are written.

The fundamental defining concepts of Version 5 are:

- The elimination of the “risk-based assessment methodology” (RBAM) used in Versions 1-3 to determine which “Cyber Assets”¹⁰ (i.e., computer systems, relays, RTUs, etc.) should be classified as “Critical Cyber Assets,” and therefore require the protections described in the remainder of the CIP standards; replacing the RBAM with an “impact rating criteria” applied consistently across all utilities, coupled with additional specificity in the definition of “BES Cyber Asset” (the new term that replaces “Critical Cyber Asset”) replacing, expanding, and clarifying the subjective phrase “essential to the reliable operation” used in previous versions; and,
- The introduction of an impact-based approach to categorizing the “BES Cyber Assets” and “BES Cyber Systems” into high impact, medium impact, and low impact, and adding additional qualifiers (primarily whether the BES Cyber Assets can be accessed remotely using routable protocols, and whether the BES Cyber Assets are located at Control Centers) to specify exactly which requirements or requirement parts¹¹ apply to a specific BES Cyber Asset.

These two changes addressed many implementation issues encountered during the implementation of Version 1-3, chiefly, the ability of two neighboring utilities to make inconsistent judgments of whether a particular Cyber Asset is a Critical Cyber Asset, based on their internally developed RBAM, and the inclusion of a set of requirements for all Cyber Assets that play a “real-time” role in reliable operation of the Bulk Power System.

Development of modifications to the CIP standards continues, but the changes to date are incremental in nature and do not alter the fundamental shift represented in the migration from Version 3 to Version 5. While development of revisions to the CIP Standards continues, and the version numbers of individual standards continue to increase, they are still informally referred to as the “Version 5 family of CIP standards,” or, more simply, “CIP V5.”

2.1.2 NIST

At the same time that NERC began developing cyber security standards for the electric industry, NIST began developing cyber security guidance primarily targeted at US federal government organizations. Acting under the Federal Information Security Management Act (FISMA), signed into law as part of the Electronic Government Act of 2002, NIST developed guidance for both traditional information technology (IT) systems, as well as operational technology (OT) and industrial control systems (ICS) environments. This guidance has been documented in a number of NIST Special Publications, primarily in the SP 800 series. Since 2003, NIST has issued and since updated a number of Special Publications (SPs) on cybersecurity topics, including SP-800-37 (revised in 2014, undergoing further revision in 2017), the Guide for Applying the Risk Management Framework to Federal Information Systems: A

¹⁰ Note that the language adopts the NERC practice of using capital letters to denote terms used in the NERC Glossary of Terms Used in Reliability Standards. See

http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf, accessed 11/1/2017

¹¹ CIP V5 standards use the newer concept of “requirement parts” rather than the original concept “sub-requirements”

Security Life Cycle Approach. NIST has also published several papers and guidelines on how to secure information systems and industrial control systems.¹²

In 2014, Congress adopted the Federal Information Security Modernization Act, authorizing the Department of Homeland Security (DHS) to administer the implementation of security policies. NIST continues to maintain the Risk Management Framework on its website.¹³

FERC continues to refer to the NIST Risk Management Framework. In the July 2015 Notice of Proposed Rulemaking (152 FERC ¶ 61,054 (Revised Critical Infrastructure Protection Reliability Standards)), FERC proposed approving “CIP Version 6,” directing staff to, “examine the technical issues concerning communication security, remote access, and the National Institute of Standards and Technology (NIST) Risk Management Framework.”¹⁴

Cybersecurity threats and challenges are changing rapidly, and the technologies and methods to secure critical systems are trying to keep pace; NERC CIP standards and the FERC approval process follow along in their wake. DHS has taken over cybersecurity work from NIST. NIST is seemingly not involved with NERC CIP standards development, but FERC continues to refer to them. As EEI observes,¹⁵ “it is clear that a strong appetite exists for clarifying understandings of the broad range of technical requirements under CIP V5, and several process issues that govern implementation of NERC standards.”

2.1.3 Present Situation

The NERC CIP requirements represent a minimum framework that must be implemented in its entirety for all applicable BES Cyber Assets, including synchrophasor system components, as specified in the requirements language, with little latitude for deviation from the expected outcome. Compliance with that framework and requirements necessitates both actions and technologies to be undertaken to achieve security, and documentation of the relevant actions and technologies and the processes and rationales behind them.

The CIP standards contain elements of both cyber security and of auditing or compliance. The standards are written to be specifically measureable for audit, and the audit aspect of the standards often gets more attention from utilities. For example, CIP-002 Requirement R2 specifies that security patches are expected to be assessed for applicability at intervals not greater than 35 calendar days, providing a metric against which execution of a periodic patch analysis process can be measured.

The CIP V5 requirements are written to specify a functional or performance-based outcome, allowing the owner some discretion to determine how best to achieve the outcome in the requirement. Version 5 has attempted to reduce technology-specific prescriptions, without eliminating the ultimate security goal. An example of this is in malware protection. Under Version 3, the malware protection requirement specified use of “anti-virus software and other malicious software (“malware”) prevention tools” which were not available for many Cyber Assets (e.g., protective relays). The revised language in Version 5 requires that

¹² See the full set of current NIST Cybersecurity guidelines at: <https://csrc.nist.gov/publications/search?requestserieslist=1&requeststatuslist=1,3&requestdisplayoption=brief&itemsperpage=all&requestsortorder=5>, accessed 11/1/2017.

¹³ <https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-Quick-Start-Guides>, accessed 11/1/2017

¹⁴ From the NOPR at <http://www.ferc.gov/whats-new/comm-meet/2015/071615/E-1.pdf>, accessed 11/1/2017

¹⁵ <http://www.nerc.com/pa/CI/Documents/Industry%20Comments%20-%20Transition%20Guidance%20Draft%20for%20CIP%20V5.pdf>, document page 60, accessed 11/1/2017

utilities “deploy method(s) to deter, detect, or prevent malicious code” and “mitigate the threat of detected malicious code.” These are the actions commonly performed by anti-virus software, but the revised language offers flexibility in how to achieve the desired outcome without prescribing a specific technology or implementation.

Individual utilities can go beyond the strict Version 5 requirements language in pursuit of good security. Utilities should not fear audit repercussions for going beyond the strict requirements, whether doing more than is strictly required, or implementing additional CIP requirements where they are not required (e.g., applying medium impact requirements at a low impact location).

The current NERC CIP cybersecurity¹⁶ standards address:

- CIP-002 Identifies and categorizes BES Cyber Assets and their BES Cyber Systems. This is where an impact rating is specified.
- CIP-003 Specifies consistent and sustainable security management controls that establish responsibility and accountability
- CIP-004 Requires an appropriate level of personnel risk assessment, training, and security awareness
- CIP-005 Specifies a controlled Electronic Security Perimeter with border protections
- CIP-006 Specifies a physical security plan with a defined Physical Security Perimeter
- CIP-007 Specifies select technical, operational, and procedural requirements for the BES Cyber Assets and BES Cyber Systems
- CIP-008 Specifies incident response requirements
- CIP-009 Specifies recovery plan requirements
- CIP-010 Specifies configuration change management and vulnerability assessment requirements
- CIP-011 Specifies information protection requirements

Though concepts from NIST Framework can be seen in most of the NERC CIP standards, the wording indicates that the NIST contribution has been reviewed and incorporated into the requirement language and structure, and the NERC document is self-contained.

The expectations of the NERC CIP standards are not entirely clear. This report is aimed to help the reader understand the intent of the standards, to clarify what can and should be done to achieve compliance and be secure. These clarifications are not intended to change or misrepresent the meaning of the CIP V5 standards.

2.2 Considerations for Future Compliance

When implementing either a security program or a compliance program, utilities should also consider future conditions, and plan and implement accordingly. For example, a utility that is installing a PMU or PDC today at a station, where the data will be used initially for research and non-decision making roles has no obligation to implement the CIP standards, since the PMU or PDC will not be considered a BES Cyber Asset when installed (see Section 3.2). However, if in the future, the PMU or PDC data is used as a primary input into a Remedial Action Scheme (RAS) or other autonomous control system (which would

¹⁶ The NERC CIP family of standards also includes a supply chain standard (CIP-013, not yet approved by FERC), and a standard dealing with physical security of transmission stations and control centers beyond protecting the BES Cyber Assets (CIP-014). Neither of those standards are discussed in this report. Also under development is a standard dealing with communications between Control Centers (CIP-012), which will be discussed briefly.

cause the PMU or PDC to be considered a BES Cyber Asset) the PMU or PDC will need to be fully compliant prior to being used for that purpose (the CIP implementation plan considers this a “planned” action, requiring full compliance with all NERC CIP non-periodic requirements activation of the RAS).

While individual utility practices may vary, a general rule of thumb is, if the PMU or PDC will be used such that it will be considered a BES Cyber Asset within one to two years, it should be treated as if it were a BES Cyber Asset when installed. This minimizes the disruption to existing systems and the amount of re-work required to change networks, establish ESPs and EAPs, etc., and develop procedures prior to commissioning of the new application of the synchrophasor data, when the PMU or PDC is required to be compliant.

In the meantime, if the PMU or PDC can exist outside of an otherwise existing ESP, the full set of processes and procedures will not be required, since there will be no compliance audits until the PMU or PDC is determined to be a BES Cyber Asset, giving the utility time to develop and test any periodic procedures. Development and verification that procedures work (e.g., for patch analysis or baselining) can be completed, but the periodic requirements associated with them will not need to be performed, nor evidence collected to demonstrate compliance, until the PMU or PDC is used in a real-time application. (If the PMU or PDC is within an existing medium impact ESP, it is considered a Protected Cyber Asset, and must be compliant with the majority of the requirements regardless of its designation.)

On the other hand, if the PMU or PDC will not be used for autonomous or real-time information for a longer period, the likely change in technology (both of the PMU or PDC, and of its supporting and surrounding equipment), engineering practices, and even the language of the NERC standards themselves may not warrant implementing the CIP requirements until closer to the actual use of the PMU or PDC for real-time operations. However, in this case, the change would likely still be considered a “planned” change, and the PMU or PDC would need to be fully compliant with the requirements prior to its use for real-time control.

3.0 CIP V5 Categorization Criteria and Process

The NERC CIP standards include a “scoping” or “categorization” process used to determine which Cyber Assets are subject to the requirements of the NERC CIP standards. This categorization process is contained in Standard CIP-002. Key factors in asset categorization for V5 security purposes include the function or use of the asset or system, the impact of that function on BES reliability, and the asset or system’s physical and/or cyber-accessible location relative to other assets.

3.1 Scoping and Definitions

The NERC Version 1-3 standards used the risk-based asset method (RBAM) approach. This allowed each individual utility to develop a set of criteria which they used to ascertain whether a particular Bulk Electric System (BES) “asset” (i.e., transmission station, generating unit, or control center) was a “Critical Asset” (i.e., critical to the reliable operation of the BES) and then determine which Cyber Assets (i.e., “computer systems”, relays, RTUs, etc.) at that Critical Asset were “Critical Cyber Assets” (i.e., they were “essential to the reliable operation of” the associated Critical Asset). This analysis was largely inward-facing, and was not required to account for external impacts to the BES, nor to consider how partner organizations use the utility’s Cyber Assets or data contained in them.

Version 5 still uses a risk-based approach, but modified it by using a consistent, common set of criteria for which Cyber Assets are required to have protections. The CIP V5 standards apply the largest number and most stringent controls to those environments with the largest impact, and greatest assumed threat. The CIP-002 process results in BES Cyber Assets or BES Cyber Systems being categorized as having a high impact, a medium impact, or a low impact.

Version 5 adopts the terms, “BES Cyber Assets” and “BES Cyber Systems” (where a BES Cyber System is one or more BES Cyber Assets). Version 5 eliminates the subjectivity of the RBAM, adopting impact rating criteria which define the BES characteristics of high-, medium- and low-impact BES Cyber Systems respectively. Version 5 establishes individual protection and documentation requirements for each of the three impact categories, with some additional qualifiers, such as whether the BES Cyber Systems is reachable from outside of its border by a routable protocol (i.e., it has “External Routable Connectivity”). The most stringent requirements apply to high-impact BES Cyber Systems, followed by medium-impact BES Cyber Systems with External Routable Connectivity or BES Cyber Systems at Control Centers, then the remaining medium-impact BES Cyber Systems, and finally low-impact BES Cyber Systems. Additional qualifiers are also attached to medium-impact BES Cyber System, and some ancillary and support systems found in BES Cyber System environments such as electronic or physical access control systems.

Since the NERC CIP standard’s requirements are generally device-centric, in the context of this report the analysis and implementation of the various requirements is based on applying them to the synchrophasor system devices, that is, the PMU or PDC. For purposes of the following discussions, the categorization of a PMU or PDC device is discussed, or to the Cyber Asset that executes a synchrophasor application.

3.1.1 CIP-002 Version 5 Definitions

The categorization process in CIP V5 is designed to address the issue of which assets are essential to the reliable operation of the bulk electric system. It no longer requires the formal identification of a Critical Asset as was required in Version 3 (although informally, many utilities still perform this identification), and there is additional clarity around the Version 3 concepts of “associated with” and “essential to the reliable operation of” clauses in the definition of a Critical Cyber Asset. Further, the ability for a utility to self-select its risk tolerance or other subjective elements of the RBAM has been removed, and replaced with a set of “impact rating criteria” that are used to determine the magnitude component of the impact analysis.

There are three new defined terms associated with the CIP-002 evaluation process. The new terms are “BES Cyber Asset,” “BES Cyber System,” and “Protected Cyber Asset” while the definition of “Cyber Asset” was modified from Version 3.

Scoping definitions

Cyber Assets are:

Programmable electronic devices, including hardware, software and data in those devices.¹⁷

Cyber Assets are essentially computer systems – devices containing a microprocessor running firmware or software. Examples of Cyber Assets include traditional computer system (servers, desktops, and laptops), microprocessor-based relays, microprocessor-based RTUs, network infrastructure (routers, switches, and firewalls), PMUs and PDCs. Whether a particular Cyber Asset is subject to the CIP Standards depends on whether it meets the characteristics in the definition of a BES Cyber Asset. Note that the definition dropped the communication network clause from Version 3.

BES Cyber Assets are those, which:

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 of 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.¹⁸

CIP-002 further clarifies:

This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.¹⁹

The BES Cyber Asset is expected to perform as designed, when it is needed, so the CIP V5 standards must address an action that does not only affect current operations, but could be triggered at a later date.

¹⁷ See http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf, accessed 11/1/2017

¹⁸ *idem*

¹⁹ See [http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber Security ___ BES Cyber System Categorization&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber_Security___BES_Cyber_System_Categorization&jurisdiction=United%20States), Section 6, Background, paragraph on Real-time operations, accessed 11/1/2017

The 15 minute parameter is intended to capture the “real-time” nature of the expected operation of the BES Cyber Asset. The 15 minute value was selected based on operational concerns (several Operations and Planning requirements have a 15 minute threshold to return to expected operating conditions), and is largely based on the amount of time that it takes a human operator to determine that an action needs to take place, determine what action is most appropriate to initiate, initiate the action, and allow the system to implement the action.²⁰

A **BES Cyber System**, which is:

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.²¹

In this definition, “responsible entity” refers to the utility or company that is responsible for complying with the standards, and “functional entity” refers to the utility that is registered with NERC (according to its role in the NERC Functional Model²²) to perform a specific function such as transmission operations. In the context of this definition, both phrases refer to the same company.

The BES Cyber System concept was introduced to allow functional groupings as a way to: 1) minimize the compliance burden to allow common audit evidence to be applied to all BES Cyber Assets which belong to a common BES Cyber System; and 2) to allow the BES Cyber System to be treated as a single entity, allowing some BES Cyber Asset members of the group to perform functions on behalf of the entire group, even for those BES Cyber Assets which cannot perform the function. For example, a group of protection relays in a station may not be able to perform malware detection and remediation (e.g., they can’t run an anti-virus product), but a separate Cyber Asset that is capable of monitoring traffic for malicious code (e.g., an intrusion detection system (IDS) with deep packet inspection) can perform that function for the entire system. A BES Cyber System could be composed of the protection relays and the IDS in order to meet the malware detection or defense requirements of the CIP V5 standards.

Some requirements lend themselves to the “system” approach, while others lend themselves to the “asset” approach. For example, treating all PMUs or PDCs from the same manufacturer, of the same model, with the same software/firmware installed, and with the same set of network and performance options as a single BES Cyber System, allows the patch analysis and vulnerability assessment requirements to be performed once for the system, rather than repeated for each individual PMU or PDC. On the other hand, if a patch or new version of software needs to be applied, it must be individually applied and verified, with supporting compliance documentation, on each individual PMU or PDC. Each utility is free to determine how it applies and documents the system vs. asset approach to each requirement. While it was not the intent of the drafting team, it is acceptable to treat each individual BES Cyber Asset as its own BES Cyber System, effectively nullifying the system approach.

While most of the CIP requirements are written at the BES Cyber System level to allow for flexibility, the terms are often used interchangeably when discussing specific requirements. This report uses the term BES Cyber Asset when discussing requirements, since the direct application is to the PMU and PDC devices, although those devices may also be components of a BES Cyber System (e.g., a PMU may be

²⁰ For example, if a transmission line is overloaded, it gets hot, expands and sags. The operator has 15 minutes to take actions to return the power flows on the line to within expected ranges, and let the line cool down and contract. If a Cyber Asset that senses or controls the flow on the line prevents the operator from being alerted and take action, the line could continue to be overloaded longer than the 15 minute threshold, causing it to sag further and potentially trip or cause physical damage, due to a vegetation or ground contact.

²¹ See http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf, accessed 11/1/2017

²² See <http://www.nerc.com/pa/Stand/Pages/FunctionalModel.aspx>, accessed 11/1/2017

included in a BES Cyber System at a station containing a stand-alone PMU (with or without a PDC) as well as protection relays and primary instrumentation sensors).

A Protected Cyber Asset, which is:

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 Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. ²³

Under Version 5, the Protected Cyber Asset concept, formal definition, and use, ensures that all Cyber Assets on the same Local Area Network (LAN) as a high-impact or medium-impact BES Cyber Asset (i.e., within the same Electronic Security Perimeter, or ESP) are categorized and treated consistently.

While not a formal definition, the Guidelines and Technical Basis section of CIP-002-5²⁴ contains a discussion of a set of “**BES reliability operating services**,” also referred to as the BROS. These services include:

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints
- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

This list of services represents a view of reliability services expressed from a functional or application viewpoint, rather than a registration viewpoint as organized in the NERC Functional Model.²⁵ Since obligation and responsibility for performing these services is often spread across different functional registrations, the CIP-002 guideline section contains a cross-map of BROS function to functional registrations, reproduced here:

²³ See http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf, accessed 11/1/2017

²⁴ See <http://www.nerc.com/ layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber Security — BES Cyber System Categorization&jurisdiction=United States>, Guidelines and Technical Basis section, accessed 11/1/2017

²⁵ See <http://www.nerc.com/pa/Stand/Pages/FunctionalModel.aspx>, accessed 11/1/2017

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Figure 1: BROS to Entity Registration Mapping

The guidance section in CIP-002 provide further information on what is included in each of the BROS. The BROS approach is useful when assessing the function or purpose of an individual Cyber Asset when determining if it meets the qualification of as BES Cyber Asset.

3.2 BES Cyber Asset Determination

The following sections describes the categorization process in the Version 5 standards, which determines which Cyber Assets (in the context of this discussion, PMUs and PDCs) meet the threshold of being BES Cyber Assets, and must therefore meet the appropriate requirements in the remaining CIP Standards. This process requires two, often parallel, processes be performed: 1) determining where the PMUs or PDCs are located, and 2) determining what function(s) are performed by the PMU or PDC or its data. A useful process may be broken down into the following components:

1. Create a list of all the installed PMUs and PDCs and their locations (i.e., the substation or control center where the PMU or PDC resides).
2. Using the list, document the function or functions performed by each PMU or PDC, or which use the data produced by the PMU or PDC.
3. Analyze the functions and data use to determine whether the PMU or PDC meets the definition of a BES Cyber Asset.
4. Using the location of each PMU or PDC, determine the impact level of the PMU or PDC.
5. If the PMU or PDC does not meet the definition of a BES Cyber Asset, but is connected to the same computer network as medium impact or high impact BES Cyber Assets, it is treated as a Protected Cyber Asset.

Cyber Assets must be assessed to determine if they support reliable operations of the Bulk Electric System (BES, which the Energy Policy Act of 2005 calls the Bulk Power System, or BPS) by determining if their impact plays a significant enough role in order to be covered. The impact analysis looks at both time-based impacts and magnitude-based impacts, and the analysis is heavily dependent on how a

particular Cyber Asset is used at a specific utility. For example, a market operations system at one utility may not play a reliability role, while at another, it is tightly integrated into BES operational specifications. Even within a utility, a data from PMU at one station may be used as part of a RAS scheme, while data from a PMU at another station may be used to record fault data for after-the-fact analysis. The criteria for analysis are contained in the definition for a BES Cyber Asset.

Recall that the definition of a BES Cyber Asset states that “[r]edundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.” In the context of PMU data, this can be interpreted to mean that if the PMU data is used in an application that supports real-time operations decisions, such as a linear state estimator, even if the PMU data is only used as a “backup” for other telemetered data, the PMU or PDC and its data meets the criteria for being classified as a BES Cyber Asset.

This analysis is the same one that would be performed for any Cyber Asset such as a relay or RTU in a station supplying SCADA data to a Control Center. There is nothing inherently special about PMUs or PDCs, or data derived from them that would cause them to be automatically considered BES Cyber Assets. The analysis focuses on the function(s) they perform, or applications and processes that use the data they produce. Just like any data source, analysis of the use of the data must include all reliability-based uses regardless of ownership of a particular system or dataset. If data from a PMU or PDC owned by one organization is used in an application owned by another organization, it is incumbent on both parties to agree on the classification of the PMU and PDC, and its data, and to implement the requirements accordingly.²⁶

The high-level process for determining whether a Cyber Asset meets the threshold for being categorized as a BES Cyber Asset is shown in Figure 2.

²⁶ A number of questions concerning use of PMU or PDC data by one organization obtained from PMUs or PDCs owned by another organization, and the impact of the CIP-002 classification on those PMUs or PDCs. The NERC standards are silent concerning ownership of particular Cyber Assets, and rather, focus on the function, application, or use of data for “real-time” reliable operations. In these cases, both parties must acknowledge and agree to the function, application and use of the PMU or PDC data. The format and content of those agreements is beyond the scope of this report.

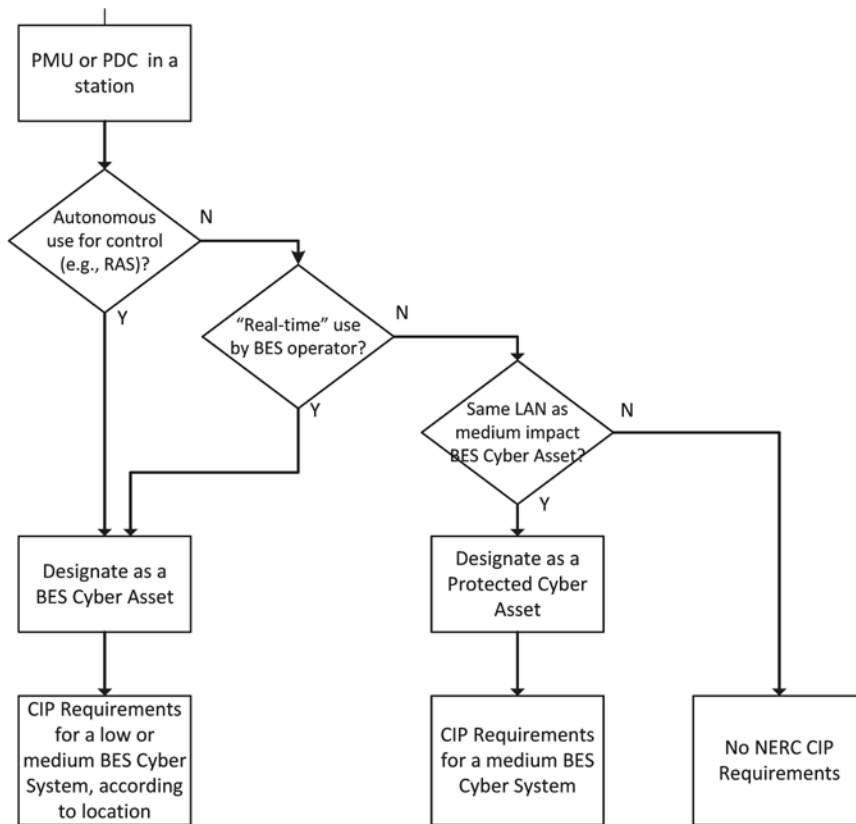


Figure 2: Classifying a PMU or PDC in station

A useful way to start the V5 categorization process is to create a list of PMUs and PDCs, and document where each PMU or PDC is *located*. At the BES level, PMUs and field PDCs are generally located in transmission stations or generation switchyards (both considered transmission locations), so the transmission station or the generation switchyard is evaluated based on the transmission and generation impact rating criteria in CIP-002 V5. This process will determine whether the PMU or PDC is potentially a medium-impact or a low-impact BES Cyber Asset. Note that V5 specifies that high-impact BES Cyber Systems are only located at Control Centers.

Once the list of PMUs and PDCs is complete, the analysis of the function or functions performed or supported by the PMU or PDC must be done to determine whether the PMU or PDC is considered a BES Cyber Asset. It is important to capture all the functions performed or supported by the PMU or PDC, since not all of them could be in support of real-time reliability operations. Some functions may not currently support reliable operations, but could in the future. Capturing the functions now could save time and re-work in the future.

The definition of a BES Cyber Asset is discussed in Section 3.1.1. In order to meet the definition of a BES Cyber Asset, the Cyber Asset must have an impact to real-time (i.e., within 15 minutes) reliable operations. If the Cyber Asset's performance or non-performance for any reason within 15 minutes could have an adverse reliability impact to BES operation, the Cyber Asset should be characterized as a BES Cyber Asset. Similarly, if the data from the PMU or PDC could be maliciously modified causing an improper operational decision to be made in the 15 minute window, the Cyber Asset should be characterized as a BES Cyber Asset.

In the case of a PMU or PDC, this analysis can be performed by asking whether the data from the PMU or PDC is used either autonomously (e.g., input to a Remedial Action Scheme) or by operators to make “real-time” (i.e., sub-15 minute) decisions in support of reliable operations of the BES, and if so, then the PMU or PDC is a BES Cyber Asset. Further components of the analysis include assessing whether misuse of the PMU or PDC, or its data could lead to unreliable actions taken, or decisions made either leading to wrong actions taken, or correct actions not taken, or if any actions or decisions would be delayed causing to reliability problems from the data being not available or misleading.

Redundant or backup Cyber Assets *cannot* be used to lessen the impact level of a BES Cyber Asset, since backups are generally included to allow one of the Cyber Assets to be removed from service for maintenance (e.g., to install a software patch), or for expected mechanical failure of a particular Cyber Asset (e.g., a disk head crash). A cyber issue impacting one Cyber Asset (i.e., a malicious attack against it or an inadvertent misconfiguration) would likely affect both Cyber Assets in a redundant configuration, therefore having a backup (that has an equal chance of being corrupted along with the primary) cannot guarantee that the function performed by the Cyber Asset will continue to perform as expected or designed.

Once the Cyber Assets have been determined to be BES Cyber Assets by performing this analysis, they become the targets for implementing the CIP Standards, at the appropriate impact levels (and subject to connectivity and other characteristics) as discussed in the following sections.

If the PMU or PDC does not meet the requirements to be considered a BES Cyber Asset, but is on the same LAN as other medium impact BES Cyber Assets, then it is defined as a “Protected Cyber Asset,” and must meet essentially all the same requirements as if it were a medium impact BES Cyber Asset (note that there are no Protected Cyber Assets at low impact). If the PMU or PDC does not meet the requirements as a BES Cyber Asset, and is not on the same LAN segment as BES Cyber Assets, then no NERC CIP requirements apply. However, if a PMU or PDC at a medium impact station does meet the requirements of a BES Cyber Asset, and is not on the same LAN as other medium impact BES Cyber Assets, and does not have External Routable Connectivity, it still must comply with a subset of the NERC CIP requirements (i.e., those that apply to medium impact BES Cyber Assets, but not those that specify “with External Routable Connectivity”).

We assume that the PMUs or PDCs typically communicate outside the station using a routable protocol (which PMUs or PDCs connected to a NASPInet or similar wide area synchrophasor data network would use), so the set of standard requirements that apply would be either those associated with a medium impact BES Cyber System with External Routable Connectivity, or those associated with a low impact BES Cyber System (with external routable connections), depending on the location of the PMU or PDC, see Figure 3.

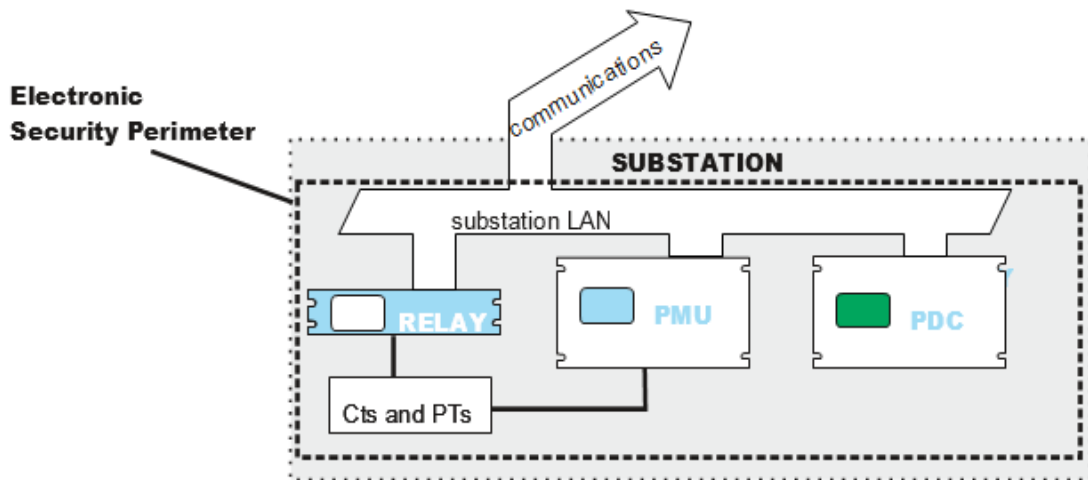


Figure 3: Network Connected PMU and PDC

The condition exists where the PMUs themselves in a station do not communicate using a routable protocol, but rather using a “serial” protocol to a local PDC, which then uses a routable protocol to communicate to systems outside the station, see, for example, Figure 4. In this case, at a medium impact station, the PDC would have External Routable Connectivity, while the PMUs would not. However, both the PMUs and the PDC would need to be assessed to determine if they would be considered BES Cyber Assets depending on how they or their data is being used. If they are considered BES Cyber Assets, the PDC would need to comply with the requirements of a medium impact BES Cyber Asset with External Routable Connectivity, but the PMU would need to comply with a smaller set of requirements than to the PDC. This report will not provide details on which requirements only are applicable to the PMUs in this case – but they are the ones that apply to medium impact BES Cyber Systems but do not specify “with External Routable Connectivity” in the applicability column of the standard.

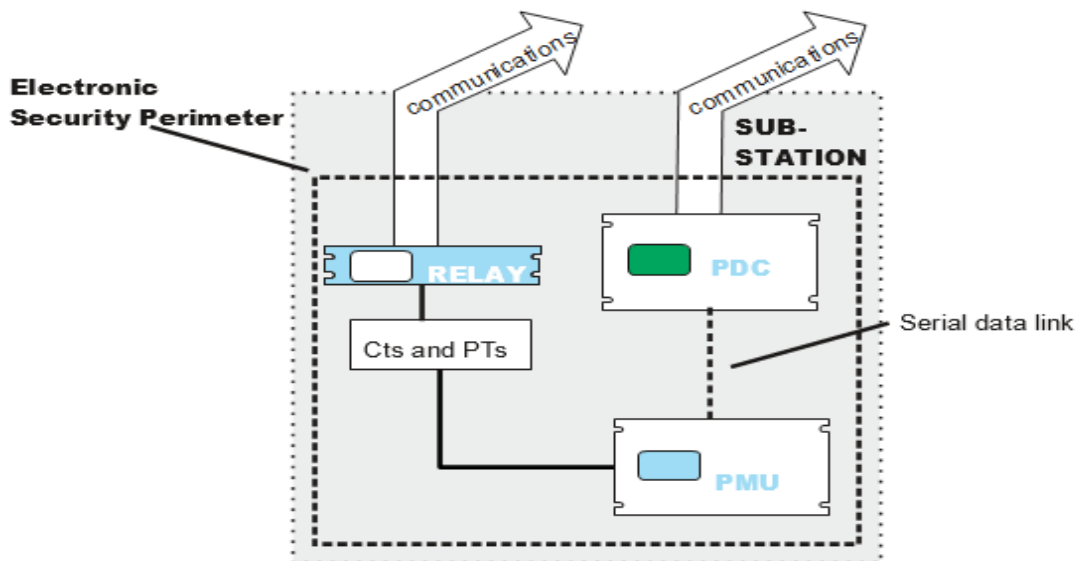


Figure 4: Serially Connected PMU

As shown in Figure 5, V5 CIP-002 categorization considers an asset or system’s reliability impact (which is often closely related to its location on the system) and whether it has routable connectivity.

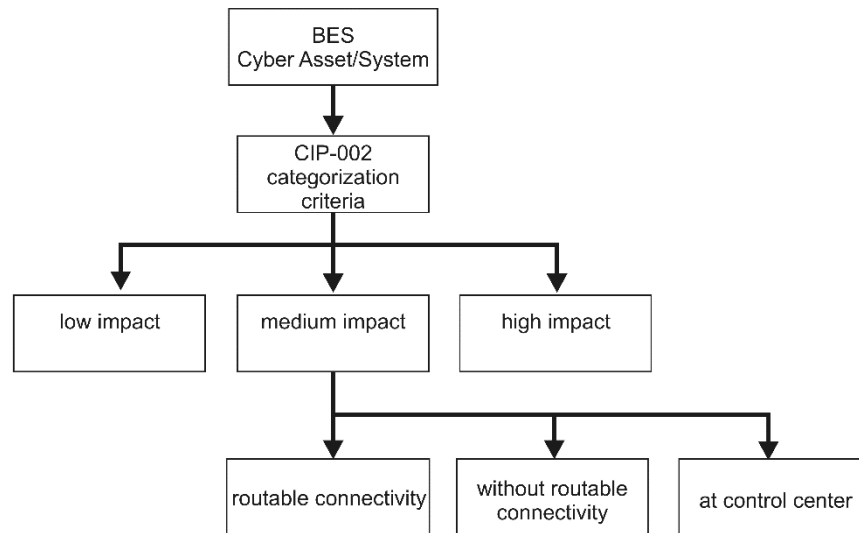


Figure 5: CIP-002 Categorization

The CIP-002 criteria are used to determine whether a particular BES Cyber Asset has a low impact, a medium impact, or a high impact. Detailed criteria for high, medium and low impact assets are detailed in Attachment 1 of CIP-002-5. The additional qualifiers for routable connectivity (or lack thereof) or medium impact BES Cyber Assets at Control Centers is contained within the language of the requirements themselves in the remainder of the standards.

Since the NERC CIP requirements are generally device-centric, this section of the report focuses on applying the NERC CIP requirements just to PMU devices and PDC devices. (A brief discussion of how to apply the requirements to applications and how the requirements might be applied to communication networks is also included toward the end of this section.)

Since PMUs or PDCs often communicate to external systems using a routable protocol (e.g., using a synchrophasor data network), this paper does not address compliance for BES Cyber Assets that *do not* use a routable protocol for external communications.

3.3 Impact Level Determination

As noted above, the first step in implementing a CIP compliance program is to determine *where* each BES Cyber Asset is located. While there is no auditable result to the location determination process, CIP-002-5 refers to *locations* as if they were the *criteria*. CIP V5 lists the impact rating criteria (essentially a list of locations) in Attachment 1 of CIP-002. (Criteria 2.1 and 2.3 have been left out of this report only because they deal with generation control systems, and the authors of this report regard that as out of scope. Generation interconnections are discussed in Criterion 2.8.)

Since PMUs and PDCs are generally located on the transmission grid, this report addresses the specific criteria associated with transmission stations and generation switchyards. This report does not directly address PMUs or PDCs considered part of the distribution system, since distribution assets are typically

not jurisdictionally subject to NERC and FERC regulation. The BES definition process²⁷ describes how distribution-level assets can be included in the BES.

If a utility has an existing CIP compliance program, most of the analysis work required by CIP-002 should have already been performed. If the analysis has not already been performed (for example, although unlikely, if there are no Cyber Assets located in field locations (e.g., all the protection systems are implemented using electromechanical relays)), the entity should apply these criteria to the PMUs and PDCs.

This section of the report will discuss five scenarios for a PMU or PDC in a field location such as a transmission station or generator switchyard. These scenarios are presented starting with the minimum level requirements and progressing towards the most stringent requirements. There are two scenarios for PMUs or PDCs in low impact situations, and three for medium impact situations.

Since high impact BES Cyber Systems can exist only at Control Centers, and PMUs are primarily located in field locations (i.e., not at Control Centers) compliance with the CIP Standards for PMUs at high impact will not be discussed in this report. However, Phasor Data Concentrators (PDC) do exist at Control Centers, so a discussion of CIP compliance for PDCs at a high impact Control Center is included as the final scenario.

3.4 Transmission Station Impact Level Determination

There are medium impact criteria for generation control systems, transmission systems, and Control Centers. The language in the criteria use the phrase “transmission stations or substations” to include cases where some utilities refer to all their transmission stations as “substations,” while others only refer to stations that include transformers as “substations” – all others are referred to as “switching stations” or simply “stations.” The wording was used to ensure that all transmission stations are included in the analysis, regardless of what terms are used locally in a utility.

The CIP standards use a series of criteria, associated with different types of transmission assets, to determine the impact level of each specific asset. A PMU, and perhaps a PDC, that are associated with a particular type of asset (e.g., monitoring a transformer) will take on the BES Cyber Asset impact level of that asset. As noted previously, if the PMU or PDC is located within a station that has a specific impact level rating, the BES Cyber Assets should be assigned the impact level associated with that rating.

Currently, transmission Control Centers are only defined for high impact and medium impact. While there is some ongoing discussion concerning low impact transmission Control Centers, it is unlikely that they will contain PDCs due to proposed threshold criteria being very low (e.g., less impact than two medium impact transmission stations). Once the actual thresholds for low impact transmission stations are determined, this section of the report should be revisited.

In the following sections, individual transmission impact level criteria are discussed. By the time this level of assessment is started, an individual PMU or PDC should have already been assessed to determine whether it is a BES Cyber Asset. If a PMU or PDC is not a BES Cyber Asset (or is not a Protected Cyber Asset on the same network as an other BES Cyber Asset), it is not assessed by these criteria.

²⁷ See <http://www.nerc.com/pa/RAPA/Pages/BES.aspx>, accessed 11/1/2017

3.4.1 Criterion 2.2

Criterion 2.2 deals with large reactive resources. While this category may include generation facilities, it also includes large capacitor or reactor (inductor) installations which are generally considered transmission. The criterion specifies that a medium impact rating applies to a BES Cyber System associated with:

Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.²⁸

The *single location* is where the reactive power resource is. The *criterion* that is applied there is whether the BES Cyber System could, within 15 minutes, adversely impact the operation of that reactive power resource.

Note that the “shared system” qualifier would depend on the specifics of the installation. In order for a PMU or PDC to meet shared systems “exemption,” it would need to have a view of only a portion of the installed reactive resource, as discussed below.

Imagine a station that contains two independent 600 MVAR capacitor banks, each with separate control systems, but connected to the same transmission element (the same or normally interconnected bus). The capacitor control system only has scope of control of 600 MVAR, so it does not meet the “shared system” qualifier, and therefore would not meet the criterion. However, if only one PMU or PDC is located at the station, and has observability of the interconnected bus, it would have a scope of 1200 MVAR, and therefore it *would* meet the criteria.

On the other hand, if the capacitor banks are electrically isolated from each other (i.e., on separate busses with no tie breakers, connected to separate transmission lines leaving the station), then a single PMU or PDC would only see 600 MVAR (on the bus or line it is connected to). In this scenario, there are likely two PMUs, each having a scope of 600 MVAR, however a single PDC connected to both PMUs would a scope of 1200 MVAR. In this case, a further review of the intra-station network (LAN) architecture would also need to be performed to determine if there could be any interaction from one PMU to another which could cause the PMUs to be considered “shared.”

It is not completely clear from the criterion language whether a synchronous condenser (a generator unit that is configured to only produce MVARs, not MWs) is considered a “generation Facility” for this criterion. However, since a synchronous condenser has no turbine and generates no power, but is performing a transmission function, the authors of this report consider it equivalent to a capacitor.

3.4.2 Criterion 2.4

Criterion 2.4 deals with EHV (extra high voltage) transmission. The criterion applies a medium impact rating to a BES Cyber System associated with:

²⁸ See <http://www.nerc.com/ layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber%20Security%20-%20BES%20Cyber%20System%20Categorization&jurisdiction=United%20States%20>, Attachment 1, accessed 11/1/2017

Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.²⁹

The “generation interconnection Facility” clause in the criterion excludes a topology scenario where the lines leading from a single generator out to the rest of the transmission system are considered a “radial” line.

Therefore, a PMU connected to a 500-kV or higher transmission line or bus, and its associated PDC (if it exists at the transmission station) meets this criterion.

3.4.3 Criterion 2.5

Criterion 2.5 otherwise deals with large network interconnection points in the transmission network, representing the greatest possibility of concentrated power flows at a single point. It is also the most complicated criterion. The criterion states that a medium impact rating is applied to a BES Cyber System associated with:

Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.³⁰

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0 ³¹

In this criterion, the specific transmission network topology must be analyzed, along with the voltage ratings of individual lines. The first step is to determine the number of lines greater than 200 kV that leave the station. If the number is less than 3, the criterion does not apply.

If any lines are single-path radial connections to generation Facilities they are eliminated from the count. If two parallel lines go to a generation switchyard, then a network flow could go through the lines even if the generator is not on-line, so parallel lines to a generation switch yard do not automatically qualify to be

²⁹ *idem*

³⁰ *idem*

³¹ This level of voltage is addressed by Criterion 2.4, above.

excluded from the count – the configuration of the generation Facility switchyard would need to be assessed to determine if such a network flow was possible.

Finally, the number of “other” transmission stations is counted. If the number of other transmission stations is three or greater, then the criterion applies. If one of the stations is a generator radial line, it is not considered a “Transmission” station, and does not count. When counting the number of stations, consider the example of a transmission corridor consisting of two parallel lines that connect a series of transmission stations along the path. Any given station along that corridor has four lines connecting to it, but the lines only go to two other stations, so the network configuration criteria is not met. However, if one of those stations has a fifth line connecting to a third station, it meets the connection criterion.

Once the network configuration component is met, the weighted value for each line that is above 200kV, and not a single-path radial line to a generator is accumulated to determine whether the sum is 3000 or greater. Individual lines are counted even if they go to the same station at the other end, and include parallel connections to generation facilities. If the aggregated weighted value is 3000 or greater, the station meets the criteria.

Note that a large generation switchyard may also meet this criterion, since it operates as a transmission station that just happens to be co-located at a generation plant. Generation switchyards that connect to multiple other transmission stations can be energized and operate even if the generator is off line.

3.4.4 Criterion 2.6

Criterion 2.6 deals with transmission and generation facilities that have been determined by a planning analysis to be necessary to avoid wide-scale adverse reliability conditions. In operation, these will be associated with Interconnection Reliability Operating Limits, or IROLs. The criterion applies a medium impact rating to a BES Cyber System associated with:

Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.³²

IROL limits are determined by planning studies. Limit violations could lead to adverse reliability conditions, such as instabilities. The criterion states that any generation plant or transmission Facility, regardless of size or voltage level, could be designated (as a result of a transmission study) for monitoring for an IROL limit violation.

PMUs or PDCs located at these locations could be beneficial in monitoring flows to help ensure that the limits are not violated. It is presumed that generation facilities will have been previously identified that should be included under this criterion.

³² See <http://www.nerc.com/ layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber%20Security%20-%20BES%20Cyber%20System%20Categorization&jurisdiction=United%20States%20>, Attachment 1, accessed 11/1/2017

3.4.5 Criterion 2.7

Criterion 2.7 deals with transmission stations identified as critical to the continued operation of nuclear power plants. The criterion applies a medium impact rating to a BES Cyber System associated with:

Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.³³

Nuclear Plant Interface Requirements (NPIRs) are determined using standard NUC-001, and are the facilities outside of a nuclear plant switchyard that have been determined to be necessary to supply off-site power to continue to operate the nuclear plant safety systems in the event the nuclear generation goes off line. Nuclear plant and transmission operators follow the requirements of Standard NUC-001 to determine and mutually agree which external facilities meet this requirement.

Any PMU or PDC located at a Transmission station identified as part of an NPIR meets this criterion. NPIRs may include distribution facilities (e.g., blackstart generation and cranking path lines), but this criterion is restricted to only Transmission Facilities.

3.4.6 Criterion 2.8

Criterion 2.8 deals with the interconnection of large or required generation covered under criterion 2.1 (generation plant locations producing 1500 MW or more) and criterion 2.3 (generation that has been determined by an engineering analysis to be necessary to avoid an Adverse Reliability Impact). The criterion states that a medium impact rating is applied to a BES Cyber System associated with:

Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.³⁴

All transmission facilities, including radial generation interconnection lines, are included in the criterion for generation that has been identified under either criterion 2.1 or 2.3. It is presumed that it is already determined which generation facilities meet either of these criteria, and would therefore be included in criterion 2.8.

3.4.7 Criterion 2.9

Criterion 2.9 deals with Remedial Action Schemes (also called “Special Protection Systems”³⁵). The criterion states that a medium impact rating is applied to a BES Cyber System associated with:

Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs)

³³ *Idem*

³⁴ *Idem*

³⁵ Note that the term “Special Protection Scheme” was been deprecated after CIP-002-5 was approved. It will be removed from the criterion language in a future revision.

violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.³⁶

The specific RAS referenced are those used to avoid exceeding operation limits associated with IROLs, similar to the studies used in criterion 2.6. PMUs or PDCs located at these locations could be beneficial in monitoring flows, and could provide operational information to the Remedial Action Scheme processing. There are already PMU data-driven RAS in operation, and research is underway to develop autonomous RAS triggered by PMU data. If the RAS data stream includes use of a PDC, the PDC would be categorized at the same level as the PMU.

3.4.8 Criterion 2.10

Criterion 2.10 deals with Systems that perform large load-shedding operations. While not often seen in operations, a large load shedding system could be misused, leading to operational and reliability issues. The criterion applies a medium impact rating to a BES Cyber System associated with:

Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.³⁷

Since PMUs are installed to monitor transmission and generation assets, it is unlikely that this criterion would be the sole reason why a PMU or PDC would be classified as a medium impact cyber asset.

3.4.9 Low Impact Criteria

The low impact criteria represent a “catch-all” set of criteria used to ensure that BES Cyber Assets that are not already captured by either a high impact or medium impact criterion are captured and included within the CIP requirements. In other words, Cyber Assets that are associated with the reliable operation of the BES and meet the qualifications of a BES Cyber Asset, but have a lesser impact to BES reliable operations than those associated with a high impact or medium impact.

For the purposes of this report, PMUs or PDCs meet the low impact criteria if they are included into scope by the qualifications of Section 4.2³⁸ of CIP-002, but are not included in Attachment 1 Section 1 (high impact rating) or Attachment 1 Section 2 (medium impact rating.) That means that the PMU or PDC could be associated with any of the assets in the following list, from CIP-002-5.1a Attachment 1, low impact criteria:

³⁶ See <http://www.nerc.com/ layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber%20Security%20—%20BES%20Cyber%20System%20Categorization&jurisdiction=United%20States%20>, Attachment 1, accessed 11/1/2017

³⁷ *idem*

³⁸ This is a reference to Section 4.2 of CIP-002 (a normative section), containing an expanded list of applicable distribution facilities. Section 4.2 “Facilities” is further discussed in the Guidelines and Technical Basis (an informative section of the standard)

- 3.2 Transmission stations and substations
- 3.4 Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.
- 3.5 Special Protection Systems that support the reliable operation of the Bulk Electric System.
- 3.6 For Distribution Providers, Protection Systems specified in Applicability section 4.2.1³⁹ above.

Criteria 3.2 is a category aimed at capturing all remaining BES transmission stations not already captured by a medium impact criterion (a Section 2 criterion).

Criteria 3.3 is a category aimed at capturing system restoration facilities. Blackstart Resources are typically small “self-starting” generation units (often hydroelectric plants), which do not need external power in order to start and operate. Their purpose is to provide enough power to run the ancillary systems at larger plants (often coal or oil-fired plants) necessary to start the plants (e.g., coal handling and pulverizing systems, or oil fuel pumps). Cranking Paths are lines that move power from the Blackstart Resources to the larger generating plants to get them started. These may include some distribution voltage lines. PMUs or PDCs located at Blackstart Resources or along Cranking Paths could be beneficial in resynchronizing the grid or re-connecting islands that are formed during a blackstart operation.

Criteria 3.5 captures all remaining RAS (here referred to as Special Protection Systems) which are not implemented to remedy IROL conditions.

Criteria 3.6 captures distribution-level systems that are implemented for the purpose of ensuring the Transmission system remains reliable and stable. Examples include underfrequency and undervoltage load shedding systems not captured in criterion 2.10, or other required transmission protection systems that are implemented on the distribution network.

3.5 Control Center Impact Level Determination

While there may be a PDC in transmission stations with PMUs,⁴⁰ higher-level PDC aggregators (Super PDCs) and historians reside within Control Centers.

The language for Control Centers contains the phrase, “performs the functional obligation of,” to describe the functions performed at the Control Center. This language was selected to include Control Centers that performed specific functions, such as transmission operations, regardless of their formal NERC registration status. There is ongoing debate about how this language should be applied, and whether modifications to the language or registration process should be made to address the underlying issues.

3.5.1 High Impact Control Centers

There are two transmission-related criteria for high-impact Control Centers. They state that all Reliability Coordinator Control Centers, and any Transmission Operations Control Centers which operate one or more stations categorized as medium impact are considered high impact. The rationale is that since Reliability Coordinators have a wide-area view of the grid, they should be held to the highest level of cyber security. For Transmission Operations, since Control Center manages more than one transmission

³⁹ This is a reference to Section 4.2.1 of CIP-002

⁴⁰ A PDC within a transmission station is classified according to the impact level of the transmission station.

station, if at least one of them is categorized as medium, then the Control Center should be held to a higher level of cybersecurity than the transmission stations that it controls.

Since PMUs are more likely installed at medium transmission stations than low impact transmission stations, there will most likely be PDCs at both the Transmission Operations Control Center for that station, and the associated Reliability Coordinator Control Center. These Control Center PDCs will be categorized as high impact (since a Transmission Control Center with operational control of one or more medium impact transmission locations is categorized as high impact) while the field PDCs will be categorized as medium impact.

3.5.2 Medium Impact Control Centers

All Transmission Operations Control Centers that do not meet the above criteria for high impact are categorized as medium impact. In order for a Transmission Operator Control Center to be medium impact, it must not serve any medium impact transmission stations.⁴¹

3.6 BES Cyber Asset Determination Examples

This section offers several examples of how to classify PMUs and PDCs on the basis of functionality and impact.

3.6.1 Low Impact, non BES Cyber Asset

In this scenario, the PMU or PDC is installed for research or non-real-time engineering purposes (e.g., next-day fault analysis). Since the PMU or PDC is not used for autonomous control, nor is it used by power system operators to make real-time decisions, the PMU or PDC does not meet the threshold in the definition of a BES Cyber Asset, and is therefore not categorized as a BES Cyber Asset. There may be a relay nearby that meets the definition of a BES Cyber Asset, nevertheless. See Figure 6.

⁴¹ NERC is currently developing criteria for low impact Transmission Control Centers, but as of the writing of this report, that effort is still in the early development stage.

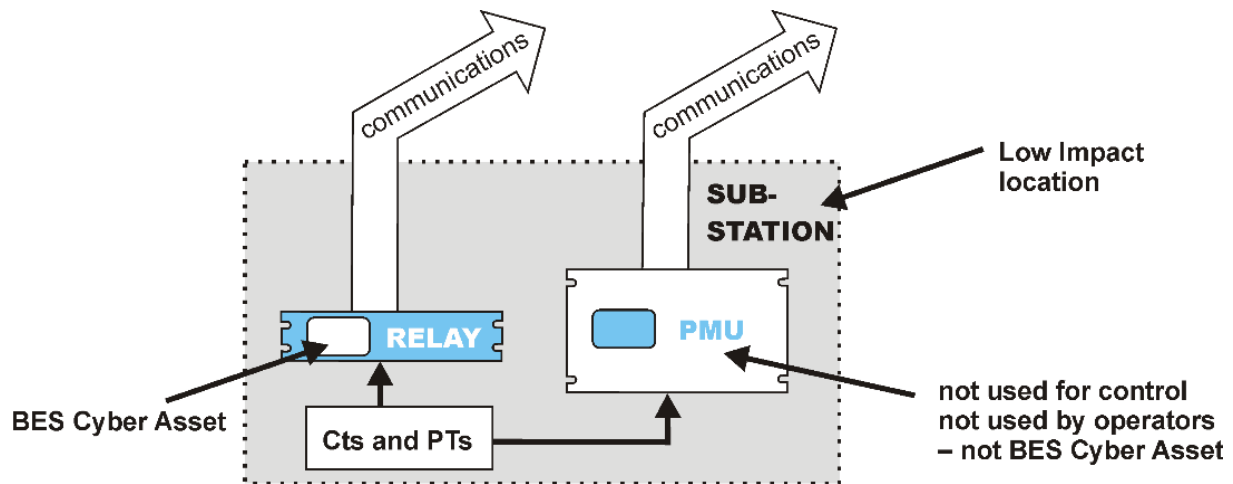


Figure 6: PMU or PDC operated in substation, not for control

From a CIP V5 standpoint, low impact categorizations represent the least impact to reliability, and therefore have the least stringent requirements. Keeping with the risk-based approach to defining requirements, there are no electronic perimeter requirements designated for low impact (i.e., there is no ESP requirement). Since there is no ESP (Electronic Security Perimeter), there are no PCAs (Protected Cyber Assets) at low impact locations, and therefore no requirements to be placed on PCAs. There are no auditable CIP V5 requirements for this PMU or PDC.

However, if the PMU or PDC is placed on the same LAN as low impact BES Cyber Assets, it is prudent from a security standpoint to treat the PMU or PDC as if it was a “low impact PCA” (i.e., treat it as if it were a BES Cyber Asset as described in section 3.6.2), since it does represent a potential attack vector into the BES Cyber Asset(s). See Figure 7.

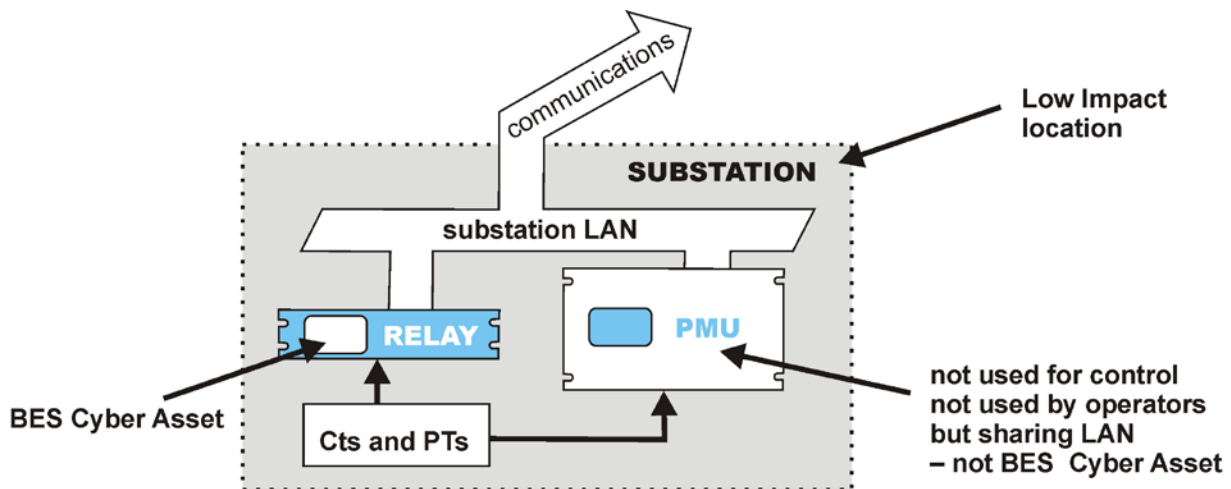


Figure 7: PMU or PDC operated in substation, with station LAN, not for control

3.6.2 Low Impact, BES Cyber Asset

In the second scenario, the PMU or PDC is installed at a low impact location and either provides real-time information to an autonomous control system, or supplies data used by a power system operator to make real-time decisions about reliable operations of the BES. It therefore meets the threshold to be designated as a BES Cyber Asset. It may be the PMU is a separate device, see Figure 8, or it could be part of a relay, see Figure 9.

Refer to Section 4.1 for the details of the NERC CIP requirements for low impact BES Cyber Assets.

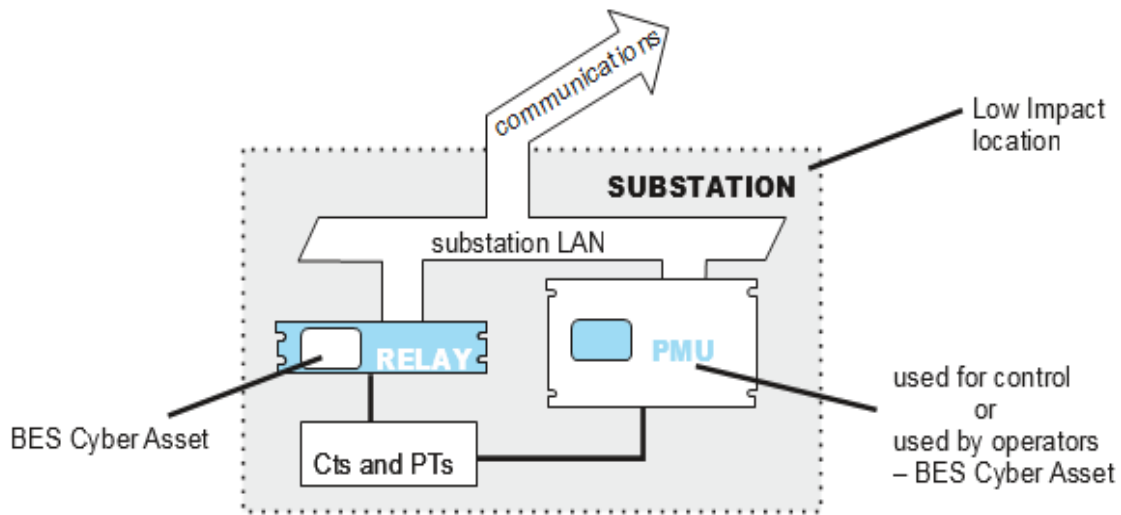


Figure 8: PMU data used for real-time decision making

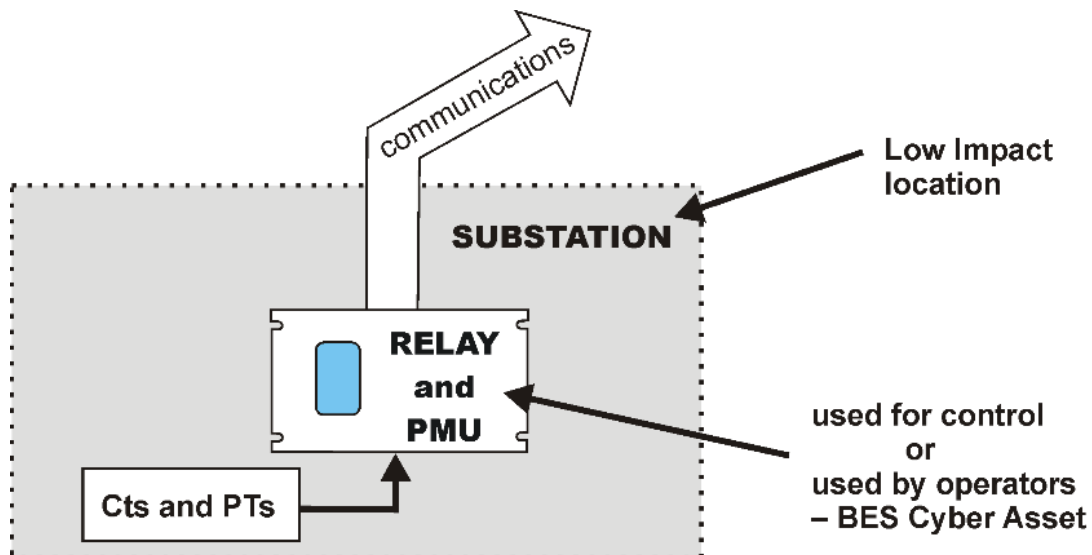


Figure 9: PMU data used for real-time decision making, here part of a Relay

3.6.3 Medium Impact, non BES Cyber Asset, non-Protected Cyber Asset

In the third scenario, the PMU or PDC is installed at a medium impact location for research or non-real-time engineering purposes (e.g., next-day fault analysis). Since the PMU or PDC is not used for autonomous control, nor is it used by power system operators to make real-time decisions, the PMU or PDC does not meet the threshold in the definition of a BES Cyber Asset, and is therefore not categorized as a BES Cyber Asset. Furthermore, it is not located on the same LAN as other BES Cyber Assets at the station, see Figure 10. This could be the result of the PMU or PDC being on a different LAN than the BES Cyber Assets, or the station where the PMU or PDC is located may have “legacy” BES Cyber Assets which do not communicate with each other using a routable protocol over a LAN.

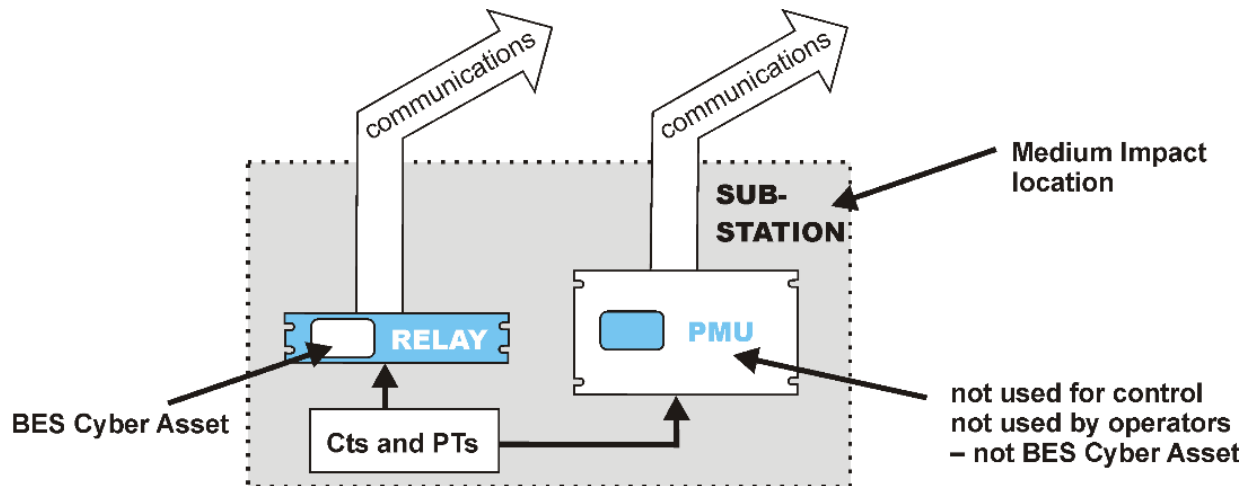


Figure 10: PMU or PDC operated in substation, without ESP, not for control

In this case, the PMU or PDC is neither a BES Cyber Asset, nor a Protected Cyber Asset, and there are no auditable CIP V5 requirements for the PMU or PDC. However, good security practice for the PMU or PDC would be to protect it as if it were a BES Cyber Asset as discussed in section 3.6.5. Since there are no mandatory requirements, the utility is not required to maintain any audit records, and may choose to implement less than a complete set of medium impact requirements.

3.6.4 Medium Impact, non-BES Cyber Asset, Protected Cyber Asset

In the fourth scenario, the PMU or PDC is installed at a medium impact location for research or non-real-time engineering purposes (e.g., next-day fault analysis). Since the PMU or PDC is not used for autonomous control, nor is it used by power system operators to make real-time decisions, the PMU or PDC does not meet the threshold in the definition of a BES Cyber Asset, and is therefore not categorized as a BES Cyber Asset. However, in this scenario, the PMU or PDC is co-located on the same LAN as BES Cyber Assets, and is therefore characterized as a Protected Cyber Asset, see Figure 11. There are few requirement differences between those for a BES Cyber Asset and a Protected Cyber Asset. The specific recommendations for this environment are discussed in section 3.6.5; any actions which are not required for Protected Cyber Assets will be noted there. However, good security practice for the PMU or PDC would be to protect it as if it were a BES Cyber Asset as discussed in section 4.2.

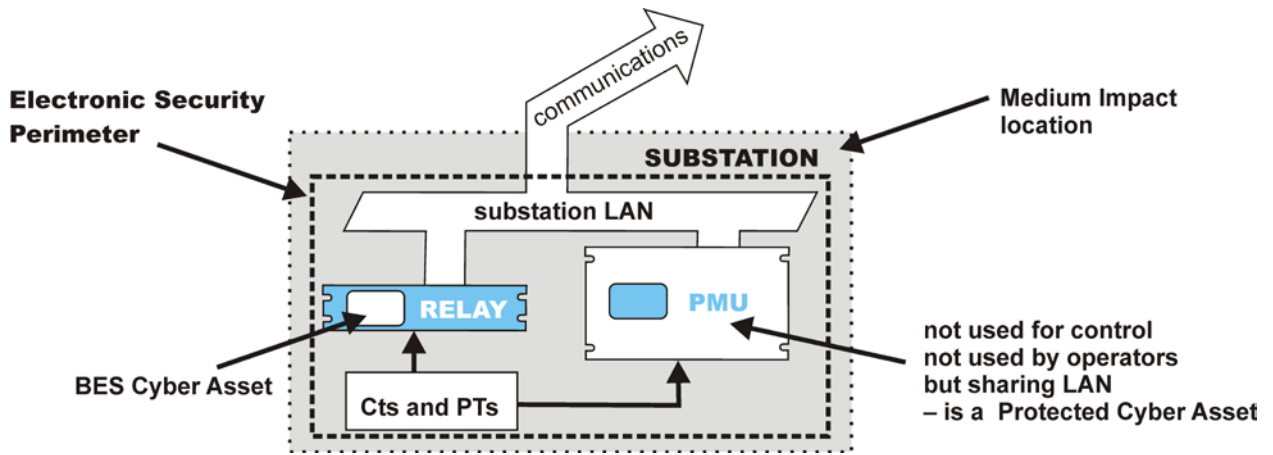


Figure 11: PMU or PDC operated in substation, with ESP, not for control

3.6.5 Medium Impact, BES Cyber Asset

In the fifth scenario, the PMU or PDC is installed at a medium impact location, and either provides real-time information to an autonomous control system, or the data is used by a power system operator to make real-time decisions about reliable operations of the BES. It therefore meets the threshold to be designated as a BES Cyber Asset.

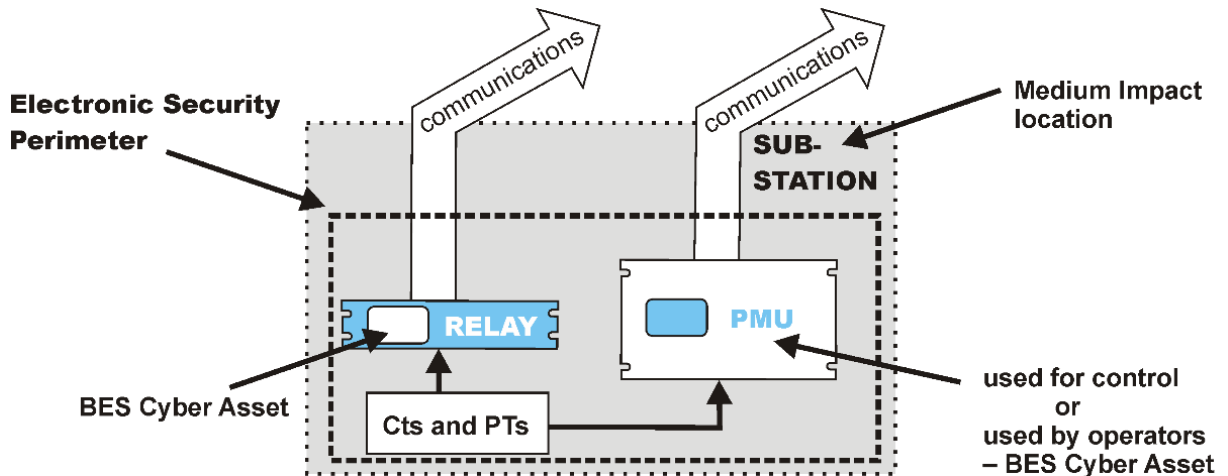


Figure 12: PMU or PDC operated in substation, for control or by operators

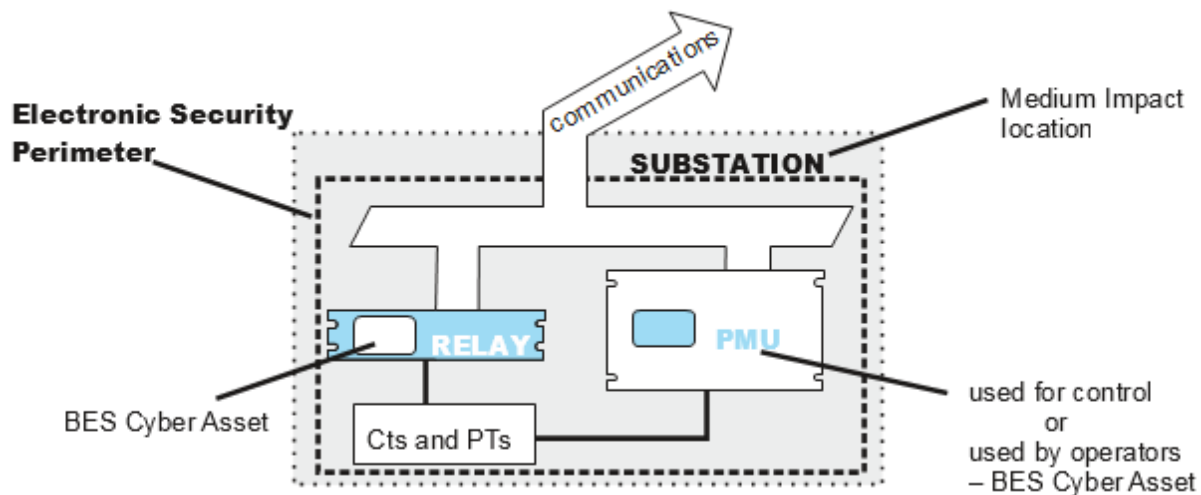


Figure 13: PMU or PDC operated in substation, shared LAN, for control or by operators

The PMU could use its own external connection, as in Figure 12, or could be on a shared substation LAN and use a common external connection as in Figure 13. In both cases, we assume that the communication uses a routable protocol, and therefore qualifies as External Routable Communication.

Refer to Section 4.2 for the details of the NERC CIP requirements for medium impact BES Cyber Assets with External Routable Connectivity, and their associated PCAs, EACMS, and PACS.

3.7 Control Center Examples

The final two scenarios are not for a PMU or PDC located at a field location, but rather for a PDC located at a Control Center.

3.7.1 PDC at Medium Impact Control Center

While PMUs are unlikely located at a Control Center, while it is much more likely that a PDC is located at a Control Center. If the utility has implemented distributed PDCs in its stations, or if the Control Center is a large Transmission Operations Control Center, the PDC at a Control Center may receive its data feed from other PDCs rather than PMUs themselves (or it may receive its data feed from a combination of PMUs and other PDCs). In this case, the PDC at the Control Center is sometimes called a “Super PDC.”

PDCs are integral to the use of PMU data in applications, performing functions including data aggregation, data conversion, time alignment, etc. that are necessary for a synchrophasor data application to properly function. If the PDC is disabled or maliciously used, the PMU data is either lost to the application, or improper data is presented to the application. For this reason, if any synchrophasor data applications are used to make real-time operational decisions, the PDC must be considered a BES Cyber Asset, and protected accordingly.

Note that if the PMU data is not used for real-time decision making at a medium impact Transmission Owner or Transmission Operator Control Center, but the data is passed to a high impact Reliability Coordinator Control Center where it is used to make real-time decisions, both the Reliability Coordinator

and the Transmission Owner or Transmission Operator must mutually agree on the proper characterization of the PDC at the Control Center (and the PMUs and PDCs feeding it data), as well as the use of the data. If the Reliability Coordinator uses PMU data to make real-time decisions, then in order to protect the data from malicious manipulation, the entire set of PMUs and PDC feeding the Reliability Coordinator's application likely meets the criteria to be considered BES Cyber Assets. If agreements cannot be reached on how to protect all the PMUs and intermediate PDCs in the data channel, the Reliability Coordinator should not be using the resultant PMU data for real-time decision making.

If the PDC at the Control Center is on the same network (i.e., inside of the ESP) containing other medium impact BES Cyber Assets (such as an EMS or SCADA system), it is considered a Protected Cyber Asset, and is subject to essentially the same set of requirements as a medium impact BES Cyber Asset at a Control Center, regardless of the use of the PDC or PMU data that it contains.

Refer to Section 4.3 for the details of the NERC CIP requirements for medium impact BES Cyber Assets at Control Centers, and their associated PCAs, EACMS, and PACS.

3.7.2 PDC at High Impact Control Center

Like a PDC at a medium impact Control Center, the PDC at a high impact Control Center will likely receive PMU data from other PDCs, and be classified as a Super PDC. This is especially true for a Reliability Coordinator Control Center.

The same discussion and rationale for PDCs at medium impact Control Centers can be made for PDCs at high impact Control Centers.

Refer to Section 4.4 for the details of the NERC CIP requirements for high impact BES Cyber Assets, and their associated PCAs, EACMS, and PACS.

3.8 Communication Networks

While out of scope for NERC CIP compliance, except in the case of ongoing development for security of Control Center to Control Center communications, the security of synchrophasor data is nonetheless important. Synchrophasor data networks are modern routable communication networks that do not inherently have legacy restrictions often found in the telemetry networks used for SCADA communications. As such, these networks can be implemented using more state-of-the-art security techniques, such as site-to-site encryption, and IPSEC security. If these modern security measures are designed and implemented early in the development phase of a synchrophasor system installation, any performance issues introduced by the security measures can be worked out prior to the network "going live" for use. This is often not the case for a legacy network that cannot tolerate simultaneous testing of new security features while carrying live data.

Standard CIP-012 [still under development] deals with communications between Control Centers. Requirements in this standard may apply to communications from one PDC to another PDC (assuming the PDCs are located at Control Centers), but not between a PMU or a PDC located in a transmission station and a PDC located at a Control Center. Since the requirements are still under development, the specific details cannot be discussed here. The reader is encouraged to review the requirements in CIP-012 once they are complete to determine what actions need to be implemented for PDC communications.

3.9 Applications using Synchrophasor Data

Applications that use synchrophasor data reside generally in one of three environments, either: 1) at a transmission or generation station, and likely as part of the control system network at that location or sharing information between multiple stations, such as in the case of a Remedial Action Scheme; 2) as part of the analytical and control systems located at a Control Center such as real-time oscillation detection and control or linear state estimation; or, 3) in a research environment outside of the real-time control environment.

In the first two cases, the Cyber Assets hosting application execution and information presentation should be assessed to determine if they are BES Cyber Assets. If the applications and presentation are used to make real-time decisions, or perform autonomous control, they meet the definitional threshold of being BES Cyber Assets, and the Cyber Assets hosting the applications should be protected based on the impact rating determined for the location.

If the Cyber Assets hosting the application are not determined to be BES Cyber Assets, but are on the same LAN as medium or high impact BES Cyber Assets at that location, they are Protected Cyber Assets, and need to be protected as if they were BES Cyber Assets at that location.

If the Cyber Assets hosting the application are not determined to be BES Cyber Assets, and they are not located on the same LAN as BES Cyber Assets, which would also be the case for research applications, then there are no NERC CIP requirements that apply to the Cyber Assets.

In the case where the PDC hosting the data is located inside of an ESP, perhaps with some application uses used for real-time decision making, and other applications used for research purposes, the PDC and the Cyber Assets hosting applications used for decision making would be considered BES Cyber Assets, and protected as such, including residing inside of an Electronic Security Perimeter (ESP). The Cyber Assets hosting the research application are not themselves BES Cyber Assets, but need to obtain data from the PDC which is inside the ESP, so an EAP would need to be configured to allow the data to be passed from the PDC to the research application⁴². This may also require that user accounts be established on the PDC for the research application users, requiring those users to comply with the requirements in standard CIP-004, and the PDC's accounts to be managed as required in standards CIP-004 and CIP-007.

3.10 Distribution

PMUs or PDCs located on the distribution network (unless they have been classified as part of the BES using the BES definition process, or they meet Standard CIP-002 Attachment 1 criterion 3.6 as described above) are not within the jurisdiction of NERC, and therefore are not subject to the CIP standards.

However, prudent security practice would be to treat them at least as if they were low impact BES Cyber Systems, particularly if they communicate with other PMUs or PDCs that are subject to the CIP standards or the information from them is used to inform real-time distribution system actions.

⁴² Note that An EAP must be configured whenever data (including TCP "ACK" packets) is sent from Cyber Assets outside an ESP to Cyber Assets inside an ESP. Even if the two Cyber Assets are both inside separate ESPs, the data must still cross the ESP boundary, and the communication be managed to ensure that data does not end up in a Cyber Asset outside an ESP.

4.0 Synopsis of NERC CIP Requirements

This section of the report provides a high-level overview of the NERC CIP requirements for the indicated impact levels. The specific details of the requirements are contained in the NERC CIP Standards themselves, and are not reproduced in this report, in order that the report will remain relevant and correct even if the specific language of the standards is modified slightly through revisions.

In call cases, the reader is encouraged to refer to the exact language of the most current applicable version of the NERC CIP standards, available on the NERC web site⁴³.

4.1 Low Impact Requirements

There are eight requirements for low impact BES Cyber Assets, all contained in NERC Standard CIP-003-7, including all technical and governance requirements for field-located low impact BES Cyber Assets. This means that if a utility only has low impact BES Cyber Assets it need not look at any CIP Standards other than CIP-002 (to develop the list of locations containing low impact BES Cyber Systems) and CIP-003 (which contains all the requirements which must be applied to the low impact BES Cyber Systems). A more realistic scenario might be one where all of the utility's field-located BES Cyber Assets are low impact, but its Control Center could be medium impact. In that case, the Control Center-hosted BES Cyber Assets would be the only BES Cyber Assets which must comply with the remainder of the CIP Standards.

The first requirement is a set of six required policy statements that is intended to apply generically to all low impact BES Cyber Assets, and can be a subset of a policy document written for high or medium impact BES Cyber Assets:

1. Cyber security awareness;
2. Physical security controls;
3. Electronic access controls;
4. Cyber Security Incident response;
5. Transient Cyber Assets and Removable Media malicious code risk mitigation [submitted but not approved]⁴⁴; and
6. Declaring and responding to CIP Exceptional Circumstances [submitted but not approved]⁴⁵.

The first five policy statements directly correlate to the “technical requirements” for low impact BES Cyber Assets, while the sixth deals with a process for determining and declaring an “exceptional circumstance” (e.g., a fire, or storm restoration) where strict compliance with a requirement cannot be completed without jeopardizing health or service restoration. The CIP Exceptional Circumstance policy should describe the process for determining when it must be invoked, provide a documentation trail of when and how it was declared and when it ended, and the process for ensuring that the intent of the CIP Standard's requirements were met after the event was over. The process should be consistent with a similar process for high and medium impact.

⁴³ See http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United_States for the most current set of NERC standards for the United States jurisdiction, accessed 11/1/2017.

⁴⁴ See http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition_CIP-003-7.pdf, accessed 11/1/2017. As of the writing of this report, FERC has not taken final action on this petition.

⁴⁵ *idem*

Policy documents are written at a high level, and are intended to be company-wide, or at least division wide. Since most utilities will have a mixture of different impact levels, the NERC CIP standards allow that the low impact policy statements can be stand-alone, or can be integrated into policies written for the high or medium environment.

The second requirement deals with the designation of a “CIP Senior Manager” who must approve the policy documents described above. The third requirement deals with a delegation process for the CIP Senior Manager. However, since there are no delegable requirements for a utility who only has low impact BES Cyber Assets, a simple statement that “no delegations will be made” will suffice. If the utility also has high or medium impact BES Cyber Assets, the CIP Senior Manager designation and delegation should be consistent across all impact levels.

The remaining five requirements are technical, and consist of: 1) a security awareness program, 2) physical security, 3) electronic security, 4) incident response, and 5) Transient Cyber Asset and Removable Media protections [submitted but not approved]⁴⁶. These requirements are contained in Attachment 1 of NERC Standard CIP-003.

The security awareness requirement is similar to that for high and medium, except for the refresh period (15 months for low vs. 3 months for high and medium). This is an awareness program, so no formal attendance records are required. Examples of an awareness program materials include posters, emails, and “security minutes” at tailgate or employee meetings (similar to “safety minute” presentations).

The physical security requirement specifies a minimum physical protection of the BES Cyber Asset (but not specifically the BES electrical components). Since PMUs or PDCs generally reside inside the control house at a transmission station or generator switchyard, the physical security controls are generally implemented by locking the control house door, and implementing either a proximity key card, or some method of hard-key (sometimes called “brass key”) control to prevent unauthorized personnel from gaining access to the interior of the control house.

No formal authorization process exists at the low impact level, nor is a formal list of authorized users required. Restrictions based on work location assignment, or job title (e.g., relay technicians assigned to the north region) should be acceptable.

The electronic security requirement specifies that routable protocol communications between (in this case) the PMU or PDC and any Cyber Asset outside the station are restricted to only those necessary. It is up to each utility to determine what is “necessary,”⁴⁷ and to document the rationale for their decision. Electronic protections only apply to routable communications that are not used for “time-sensitive protection or control functions between intelligent electronic devices,” which excludes legacy serial protocols (if they are non-routable), as well as GOOSE messaging (which is time sensitive). Dial-up connectivity also needs to be authenticated, but it is unlikely that PMUs or PDCs will have much use of dial-up.

There is greater flexibility for electronic security for low impact BES Cyber Assets than there is for high and medium BES Cyber Assets. The Guidelines and Technical Basis section of CIP-003 describes several alternative implementations for electronic security, including a host-based firewall option that is not specifically available in high and medium environments. The reader is encouraged to review the specific drawings and explanations contained in CIP-003 for additional information.

⁴⁶ *idem*

⁴⁷ The concept of “necessary” communication is also included in the CIP-003-7 petition, which FERC has not yet approved.

The incident response requirement specifies that plans must be developed and tested for responding to Cyber Security Incidents. The requirements are very similar to those for medium and high (there are only so many ways to do incident response), except the timing of tests and plan updates is longer.

The Transient Cyber Asset and Removable Media requirement [submitted to FERC but not approved] specifies actions that need to be taken to mitigate the risk of introducing malicious code from either a Transient Cyber Asset (e.g., a computerized test harness) or Removable Media (e.g., a USB memory stick). Several suggested implementations are presented, with a different set specified for whether the Transient Cyber Asset is managed by the utility, or managed by someone else (e.g., a service vendor), or for Removable Media. The expected performance for Transient Cyber Assets and Removable Media is very similar to the same requirements for high and medium impact, allowing a common program to be implemented across all impact levels

4.2 Medium Impact with Externally Routable Connectivity Requirements at a Station

The CIP standard requirements for a medium impact BES Cyber Asset with routable connectivity are the most stringent for a BES Cyber Asset located at a field location, and requires implementation for nearly all requirements in standards CIP-003 through CIP-011⁴⁸. The performance expectations will be discussed below, standard by standard and requirement by requirement. Unless otherwise noted, the requirements apply to the BES Cyber Assets: BCA (or BES Cyber Systems - BCS), Protected Cyber Assets – PCA, as well as the Electronic Access Control or Monitoring Systems – EACMS (e.g., firewalls, logging systems), and Physical Access Control Systems – PACS (e.g., key card systems, card readers, camera, physical logging).

4.2.1 Requirements from CIP-003 – Security Management Controls

NERC Standard CIP-003 – Security Management Controls deals with governance issues, and applies to utilities with BES Cyber Assets at all impact levels.

Requirement R1 specifies the topics for a set of required policy statements that is intended to apply generically to all high and medium impact BES Cyber Assets, and can be selectively applied to the policy requirement for low impact BES Cyber Assets. There are nine required policy statement subject areas which must be included:

1. Personnel and training (CIP-004);
2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
3. Physical security of BES Cyber Systems (CIP-006);
4. System security management (CIP-007);
5. Incident reporting and response planning (CIP-008);
6. Recovery plans for BES Cyber Systems (CIP-009);
7. Configuration change management and vulnerability assessments (CIP- 010);

⁴⁸ This report does not reference specific versions of the CIP standards, but rather to the CIP standard numbers (e.g., rather than CIP-003-5, it will refer to CIP-003). The reader is encouraged to refer to the latest version of the standards if there are any question. For the level of detail in this report, the specific version number matters little, and there are few significant revisions underway that would cause a misinterpretation of the recommendations in this report.

8. Information protection (CIP-011); and
9. Declaring and responding to CIP Exceptional Circumstances.

The first eight policy statements directly correlate to the remaining CIP cyber security standards (CIP-004 through CIP-011), while the ninth deals with a process for determining and declaring a “CIP Exceptional Circumstance” (e.g., a fire, or storm restoration) where strict compliance with a requirement cannot be completed without jeopardizing health or service restoration. The CIP Exceptional Circumstance policy should describe the process for determining when and how it must be invoked, provide a documentation trail of when it was declared and when it ended, and the process for ensuring that the intent of the CIP Standard’s requirements were met after the event was over. The process should be consistent with a similar process for low impact, if one exists.

Policy documents are written at a high level, and are intended to be company-wide, or at least division wide. Since most utilities will have a mixture of different impact levels, the standards allow that the policy statements can be written only for high and medium impact BES Cyber Assets (allowing low impact policy statements, if they exist, to be stand-alone), or an integrated policy set for all impact levels can be written.

Requirement R2 contains the technical requirements for low impact BES Cyber Systems, so it does not apply in this case.

Requirement R3 specifies that a CIP Senior Manager must be designated. The CIP Senior Manager is a corporate official (or equivalent) with authority to ensure that the CIP Standards are being adequately applied to the BES Cyber Assets. The CIP Senior Manager is required to approve various actions and lists generated during the implementation of the CIP standards, in order to provide senior management oversight into the program, and to ensure that attention is paid to implementing the CIP Standards at high levels in the utility, and ensuring that appropriate resources are given to implementing the standards.

Requirement R4 specifies the creation of a delegation process that allows the CIP Senior Manager to designate some authority (generally approval of specific actions or reviews of required lists) to lower levels in the company. The only obligation that cannot be delegated is the annual approval of the policy documents from Requirement R1. A delegation process is not required, and if not used, a simple statement that “no delegations will be made” will suffice. If delegations are used, this process specifies the minimum expectations for the delegation process.

4.2.2 Requirements from CIP-004 – Personnel and Training

NERC Standard CIP-004 – Personnel and Training deals with training and personnel issues, and applies to utilities with high and medium impact BES Cyber Assets.

Requirement R1 specifies the development of a security awareness program, which must be refreshed at least once a calendar quarter (as compared with a similar program for low impact BES Cyber Assets which must be refreshed at least once every 15 calendar months). This requirement only applies to users of the BES Cyber Assets, not PCAs, EACMS or PACS. This is an awareness program, so no formal attendance records are required. The intent of a quarterly refresh is to keep the security awareness program “fresh” in employee’s minds. A common approach is to hang different posters in locations frequented by employees (e.g., break rooms, hallways), and on a quarterly basis, rotate the posters so that there is a visual change (color, shape, etc.) which causes employees to notice something different, and take a moment to see what the change was. Other examples of an awareness program materials include

emails, and “security minutes” at tailgate or employee meetings (similar to “safety minute” presentations). Many utilities with a mixture of high and medium as well as low impact BES Cyber Assets use a common program to reach all their employees, and follow the quarterly refresh cycle.

Requirement R2 specifies the development of a formal security training program. Completion of the training program is required prior to being granted unescorted physical access or electronic access to BES Cyber Systems, PCAs, EACMS, and PACS, and the training must be re-completed annually. The following specific topic areas that must be covered by the training program:

1. Cyber security policies;
2. Physical access controls;
3. Electronic access controls;
4. The visitor control program;
5. Handling of BES Cyber System Information and its storage;
6. Identification of a Cyber Security Incident and initial notifications in accordance with the incident response plan;
7. Recovery plans for BES Cyber Systems;
8. Response to Cyber Security Incidents; and
9. Cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.

The training program should be updated whenever significant technology or process changes (which are mentioned in the training program) are implemented. The annual refresher will ensure that all required employees eventually trained on any modified material. Formal training attendance records are required; and, while not required, good training programs generally include quizzes to ensure that the employees have reviewed and captured the material.

Requirement R3 specifies the development of a “personal risk assessment” – PRA (more commonly referred to as a background check) be performed prior to granting unescorted physical access or any electronic access to a BES Cyber Asset. The PRA includes an initial identity check, as well as a seven-year lookback criminal records check with specific details on the minimum records to be checked, specifies that the utility must develop a set of criteria which constitutes “passing” the PRA, ensuring that vendors and contractors undergo a similar PRA process, and ensuring that the PRA process (but not necessarily the identity verification) process is repeated at least once every seven years.

Requirement R4 specifies that the utility must have an “access management program” to manage all unescorted physical access, all electronic access, and all access to storage locations containing BES Cyber Systems Information (i.e., information about BES Cyber Systems that could be used to compromise their operation), whether the locations are physical or electronic. The access management program must include the process used by the utility to determine whether access by individuals is “needed.” It also specifies that once a calendar quarter, access is reviewed to ensure it is authorized, and an annual review to ensure that authorizations are still valid.

Requirement R5 specifies actions to be taken to revoke access once it has been determined to be no longer needed by an individual. For “reassignments and transfers” (i.e., the individual is still an employee), access must be revoked on the calendar day following a determination that access is no longer required. Note that there is no specific timeframe associated with what constitutes “no longer needed.” This allows utilities to make business decisions about when access is no longer “required.” For example, if an employee is transferred or promoted, there will be a period of training for the employee taking over the job. The specific time associated with this training will be heavily dependent on the job and the

individual. Additionally, there may be infrequent periodic processing (e.g., year-end processing) which may occur long after the promotion or transfer. There may also be requirements for back-up of the task in the event that the new employee is unable to perform.

On the other hand, if the employee has been terminated for any reason (i.e., the employee is no longer an employee), access must be revoked as soon as possible, but no later than the end of the next calendar day. The standard specifically states that revocation of external remote access and physical access is sufficient to “revoke access” to the BES Cyber Assets in this timeframe, and allows for 30 days to clean up and revoke (or disable) individual accounts on BES Cyber Assets.

4.2.3 Requirements from CIP-005 – Electronic Security Perimeters

NERC Standard CIP-005 – Electronic Security Perimeters deals with electronic (or logical) border protection surrounding BES Cyber Assets and establishing an “Electronic Security Perimeter.” It applies to utilities with high and medium impact BES Cyber Assets. Standard CIP-005 only applies to BES Cyber Assets and PCAs (i.e., all the systems inside of an Electronic Security Perimeter – ESP). ESPs are not required around PACS, and the requirements in CIP-005 deal with establishing and configuring firewall EACMS, so the requirements (except for the inbound and outbound traffic filtering) do not apply to the firewall EACMS computers. (They should, however, be applied to EACMS computers inside the ESP that perform logging or authentication functions.)

Requirement R1 specifies that utilities establish and document an “Electronic Security Perimeter” – ESP surrounding all networks to which BES Cyber Assets are connected using a routable protocol (e.g., TCP/IP). Since PMUs or PDCs most likely communicate using a routable protocol when sending data to PDCs at Control Centers or other data repositories outside of the station, they require an ESP, even if they get their data from field instrumentation using a non-routable protocol (e.g., IEC 61850 sample value running on a layer 2 network). Additionally, even if there are no other BES Cyber Assets with routable network connections, an ESP is still required around the PMU or PDC if there are routable communications between them, or to connect the PMU or PDC to a wide-area network router.

Requirement R1 also specifies that all routable connections must pass through an Electronic Access Point – EAP, which is defined as a network interface on a firewall EACMS, and the routable communication passing through the EAP must be filtered in both inbound and outbound directions, with a documented reason for allowing the traffic, and a specific denial of all other traffic by default. This filtering is generally accomplished using a network firewall device, and the reason specified for allowing the traffic is often included in the firewall rule comments. There also needs to be a process or method for detecting known or suspected malicious inbound and outbound communication. This includes both connection requests and data flows on unexpected ports in either direction (generally performed by the filtering feature of the EACMS), and possibly unexpected data flows across authorized ports. Finally, authentication of dial-up connections must be performed (although this is unlikely for a PMU or PDC).

Requirement R2 specifies that a process for managing interactive remote users must be implemented. In the context of the CIP standards, “remote” access is any access that originates from outside the ESP, regardless of “how far” outside the ESP. An “Intermediate System” (also known as a proxy server or a jump host) must be used to manage all interactive access coming from outside the ESP. The Intermediate System must not be located inside the ESP (it can be outside or “on” the ESP as part of the EACMS), since it is used to authenticate the interactive remote users. All Interactive Remote Access must pass through the Intermediate System and must use both encryption and multi-factor authentication that terminate on the Intermediate System. If the Intermediate System was inside the ESP, then unauthenticated and unauthorized interactive users would have access to the network inside the ESP, and

could potentially have unauthorized interactions with the BES Cyber Assets prior to the authentication being performed. Communications that pass through the ESP into the ESP must be inspected for malicious traffic (see Requirement R1) prior to entering the ESP, but encrypted communications that terminate on Cyber Assets inside the ESP can't meet the inspection requirement.

Note that this requirement applies to “interactive” access, not “machine-to-machine” or “system-to-system” access. Interactive access refers to access initiated by a (human) user using a protocol that is typically associated with human interactions, such as ad-hoc file transfer (e.g., ftp) or command line access (e.g., telnet or secure shell – SSH). This has raised issues in cases where a management console automated process uses a traditionally interactive protocol (e.g., telnet) in order to perform its management functions. Since the firewall EACMS performing the filtering cannot determine from the protocol used or the command structures sent whether the commands are coming from an automated process in the management console, which would normally be thought of as a machine-to-machine interaction, it is recommended that these interactions be passed through the Intermediate System, and the management console be programmed to perform the authentication as if it were coming from a human user.

The encryption obligation has placed some architecture restrictions on communication paths that require encrypted paths. For example, some network equipment located inside an ESP can only be managed using an SSH command stream, which is an inherently encrypted protocol. The solution proposed is to establish an SSH connection to the Intermediate System, decrypt and inspect the traffic on the Intermediate System, then re-encrypt it and send it through to the end device. This is allowed since the intermediate Systems is considered to be part of the EACMS, and the EACMS is where the traffic inspection needs to take place. From a security standpoint, if the traffic inspection and decryption are not done on the same computer, the two computers should be located in a demilitarized zone (DMZ) network, sometimes referred to as a perimeter network, to prevent traffic snooping and spoofing from unauthorized sources.

4.2.4 Requirements from CIP-006 – Physical Security of BES Cyber Systems

NERC Standard CIP-006 – Physical Security of BES Cyber Assets deals with physically protecting BES Cyber Assets and establishing a “Physical Security Perimeter.” It applies to utilities with high and medium impact BES Cyber Assets. Note that this standard does not apply to the physical security of the BPS elements themselves (e.g., lines, breakers, transformers), but rather to the BES Cyber Assets used to monitor and control them. BES Cyber Assets are typically located in the control house of a transmission station. However, in some cases, the BES Cyber Assets may be contained inside the BPS element cabinets (e.g., breaker control cabinets, transformer load tap changer cabinets), in which case CIP-006 requirements would apply to those control cabinets containing the BES Cyber Assets. In a Control Center, the BES Cyber Assets are typically located in data centers or operations theaters.

Requirement R1 requires the development of a security plan that contains the designation of a “Physical Security Perimeter” – PSP and at least one physical access control used to control unescorted physical access to only those personnel who have been granted unescorted physical access. If the PMU or PDC is located in the control house of a transmission station or switchyard, a locked door on the control house with key-card access is generally used. If the PMU or PDC is located outside the control house, generally, the PSP encompasses more than the control house, and could possibly contain the entire switchyard. (This is a significant change from the CIP Version 3 requirements.) Procedures must be in place to monitor and alert for unauthorized access attempts to gain access to the PSP, or to access the Physical Access Control System. Logging is required for individual personnel access, including date and time of access. Logs must be maintained for at least 90 days to support after-the-fact investigations.

If cabling inside of an ESP, but outside of a control house or cabinet, it is generally accepted to declare the station fence to be the PSP, since all cabling inside the ESP in a station must be also enclosed inside of a PSP. If the entire switchyard is declared to be the PSP, the fence access gate(s) become the physical access points, while cameras and motion sensors become components of the required physical access monitoring.

Requirement R2 specifies that a visitor control program must be implemented for anyone who enters the PSP, but has not been granted unescorted access to the PSP. The visitor control program should specify how employees manage visitors, including provisions for visitor hand-off from one escort to another escort, and observation of visitor behavior while in the PSP. Automatic or manual logging of all visitors is required, including time of initial entry and final exit for the day, and the point of contact (often the escort). Visitor logs are to be maintained for 90 days.

Requirement R3 specifies that a testing program must be developed and implemented to test all aspects of the Physical Access Control System, including card readers, door and window sensors, cameras, provisioning, and logging systems. All aspects of the PACS must be tested at least once every 24 calendar months, but this can be an on-going process which continually tests portions of the PACS, as long as each component test is within the testing period.

4.2.5 Requirements from CIP-007 – Systems Security Management

NERC Standard CIP-007 – Systems Security Management deals with securing the BES Cyber Assets themselves, and applies to utilities with high and medium impact BES Cyber Assets.

Requirement R1 specifies that network and physical ports that are not used, and that can be disabled, should be disabled. The language for logical ports allows for keeping an unused or unnecessary port enabled if there is no means of disabling the port (e.g., a firmware-based system that does not provide a configuration option to disable a logical port).

Requirement R2 specifies that a security patch management program must be developed and implemented to assess each BES Cyber Asset (individually or by group or class) every month to determine if security patches have been released that are applicable to the BES Cyber Asset's software configuration have been released, and if so, within another month, either install the patch (to mitigate the vulnerability), or to determine a vulnerability mitigation, and to document an action plan to implement the mitigation and eventually install the patch. Since BES Cyber Assets are real-time systems with limited capability to take them down to install patches, the mitigation and action plan allows the vulnerability to be temporarily addressed without installing the patch, mitigating the vulnerability until the patch can be installed. Due to operational concerns and maintenance schedules, patch installation could be deferred, in some cases, several years until an available maintenance window allow the BES Cyber Asset to be taken out of service for patch installation. The temporary mitigations will serve as a mitigation until the patch is installed, and can then be removed if desired (or left in-place as a defense-in-depth against future vulnerabilities).

Requirement R3 specifies that the utility must have in place a procedure to deter, detect, or prevent the introduction of malicious code onto the BES Cyber Assets, or into the BES Cyber System. If malicious code is detected, but not prevented from entering the BES Cyber Asset, the procedure must address how the malicious code's actions will be mitigated. Note that preventing the malicious code from entering or impacting the BES Cyber Assets is itself a form of mitigation. This is a case where the BES Cyber System concept can assist in mitigating or preventing the introduction of malicious code, if an individual BES Cyber Asset is incapable of detecting or mitigating the malicious code (e.g., a firmware-based BES

Cyber Asset that cannot run anti-malware software). In this case, a border device (which could be an EACMS firewall or IDS) could detect or deter the code from entering the BES Cyber System, or it could mitigate an exfiltration attack by blocking malicious or suspicious outbound traffic. The requirements also specify that if the mitigation method is “signature based” (i.e., a traditional consumer-style anti-virus product), a process for updating and testing signature updates must be implemented.

Requirement R4 specifies that a process must be in place to generate, analyze and respond to security events. At a minimum, successful and unsuccessful login attempts and malicious code detection must be logged. The process must include an analysis and escalation process for generating a response alert for an alert event that requires further response activities, and the procedure must generate a response alert in the event of a failure of the logging system. Logs must be kept for a minimum of 90 days to aid in after-the-fact investigations.

Requirement R5 specifies that a process for enforcing authentication of interactive access is implemented. This is in addition to the requirement in CIP-005 for authorizing and authenticating interactive Remote Access, and applies to all local and remote interactive access (the CIP-005 process only authorized interactive “entry” into the ESP – the CIP-007 authenticates access to individual BES Cyber Assets).

Requirement R5 also specifies that an inventory of all known generic or default accounts be performed, and a list of individuals who have access to those shared accounts is maintained. All known default passwords must be changed.

Requirement R5 also specifies minimum password construction restrictions, and allows for implementing something less than the minimum if the BES Cyber Asset does not support the minimums (i.e., complex passwords cannot be used if the password character set is restricted to only numeric characters). If the minimum password construction requirements cannot be met, the utility must implement the maximum supported by the device, and demonstrate using vendor documentation the password construction supported. Passwords must be changed annually, with enforcement either technical (preferred) or procedural (if the device does not support a forced password change). A minimum number of password attempts before locking the account (permanently or temporarily) or generating a repeated failed access attempt log event must be implemented.

4.2.6 Requirements from CIP-008 – Incident Reporting and Response Planning

NERC Standard CIP-008 – Incident Reporting and Response Planning deals with recognizing and responding to cyber security incident issues, and applies to utilities with high and medium impact BES Cyber Assets.

Requirement R1 specifies that the utility must have a procedure in place to identify, classify and respond to Cyber Security Incidents. This must include a process for determining whether the incident is a Reportable Cyber Security Incident, and if so, include the process for generating and submitting the report to the appropriate entity(s) (e.g., E-ISAC, DOE). The response procedures should include identification of roles and responsibilities of responders, and procedures for handling the incident (e.g., containment, eradication, recovery, resolution).

Requirement R2 specifies that the incident response procedures must be tested annually. The test can be response to an actual incident, a “paper drill” (or “table top”) exercise, or an “operational exercise.” The documented response plan and procedures from requirement R1 must be used in the test, and records of actions taken during the test must be maintained.

Requirement R3 specifies that lessons learned (if any) from the test must be documented, and of the lessons learned indicate that the procedure must be modified, the procedure must be updated within 90 days following the test, and the updated plan must be communicated to all persons with a role in the plan. Within 60 days of a change in responder roles, or a technology (e.g., a replacement system from a different vendor) mentioned in the plan, the plan must be updated and communicated to all persons with a role in the plan.

4.2.7 Requirements from CIP-009 – Recovery Plans for BES Cyber Systems

NERC Standard CIP-009 – Recovery Plans for BES Cyber Systems deals with procedures for returning BES Cyber Asset functionality following an incident that interrupts those functions, and applies to utilities with high and medium impact BES Cyber Assets.

The requirements in CIP-009 specify a parallel process to that in CIP-008, but for recovery following response actions in CIP-008.

Requirement R1 specifies that a recover plan be developed, that includes specific conditions for activating the recovery plan, and identifies roles and responsibilities for responders. It also requires that processes be implemented for backup and storage of all information needed to recover the BES Cyber Systems. This includes installation media for operating systems, installed products, applications, and data, as well as instructions on how to restore the system to a functioning state. For a firmware-based PMU or PDC, this could include firmware chips or equipment used to “flash” (install) updated firmware. The procedures must include a process for verifying that backups of running systems (e.g., current data and configurations) have completed successfully, and that any discrepancies are investigated and remediated. Finally, if the actions do not impede restoration to service, have procedures to preserve data for post-event analysis.

4.2.8 Requirements from CIP-010 – Configuration Change Management and Vulnerability Assessments

NERC Standard CIP-010 – Configuration Change Management and Vulnerability Assessments deals with understanding what software and configurations are running on BES Cyber Assets and managing vulnerabilities on them, and applies to utilities with high and medium impact BES Cyber Assets.

Requirement R1 specifies that a software and configuration baseline be created and maintained for each BES Cyber Asset. The baseline includes software & operating system (including name, version, and patch level) or firmware (including version and patch level) as well as any customized software or configurations, and network accessible logical port configurations. Any deviations from the baseline for installed software must be authorized and documented. Undocumented deviations must be investigated, and if found to be legitimate, the baseline must be updated. For planned changes to the baseline, an assessment of the security controls from CIP-005 and CIP-007 must be performed and verified, and the baseline documentation updated after the change has been made.

Requirement R2 applies only to high impact BES Cyber Assets

Requirement R3 specifies that vulnerability assessments must be conducted annually. Vulnerability assessments may be automated scans (e.g., using a commercial tool), or may be conducted manually via a table-top exercise (e.g., gathering configuration and version information from the BES Cyber Asset, and

reviewing vulnerability sites from NIST⁴⁹ or MITRE⁵⁰, and reviewing uninstalled patches to manually determine whether known vulnerabilities exist with the running configuration). The results of the vulnerability assessment must be documented, and a plan developed and implemented to address any vulnerabilities found.

Requirement R4 specifies that a plan for managing vulnerabilities from Transient Cyber Assets (e.g., computer test equipment) and Removable Media (e.g., USB memory) based on introduction of malicious code from those devices. The requirements are broken into three areas: 1) Transient Cyber Assets managed by the utility; 2) Transient Cyber Assets managed by third parties (e.g., vendors or contractors); and 3) Removable Media. Since there is greater control over mitigations that can be placed on Transient Cyber Assets managed by the utility, the requirements are more stringent and more straightforward. The specific performance expectations are:

- 1) For Transient Cyber Assets (TCA) managed by the utility:
 - a. Manage the TCAs either in an ongoing (e.g., the TCA is normally connected to a network and periodically scanned and receives antivirus and patch updates automatically) or on-demand (e.g., the TCA is scanned and patches applied before each use) basis
 - b. Authorize the use of the TCA by users, locations, and uses
 - c. Implement some form of software vulnerability mitigation, such as patch installation, read-only boot media, or system hardening
 - d. Manage introduction of malicious code using antivirus software or application whitelisting, and
 - e. Manage unauthorized use by restricting physical access to the TCA, utilizing full-disk encryption with authentication on the TCA, or use multi-factor authentication to access the TCA
- 2) For Transient Cyber Assets (TCA) managed by third parties:
 - a. Review software vulnerability mitigation actions by the third party, including review of installed patches, review of patching process, and review of other software vulnerability mitigation actions
 - b. Review procedures to prevent the introduction of malicious software, including review of antivirus software used, update level and update procedures, review of read-only media, and review of system hardening procedures and actions
 - c. Determine whether the reviewed actions are acceptable, and require additional actions if not
- 3) For Removable Media:
 - a. Authorize the use of the Removable Media by users and locations
 - b. Mitigate malicious code on the Removable Media by scanning it before connecting it to the BES Cyber Asset

⁴⁹ See the NIST National Vulnerability Database at <https://nvd.nist.gov/>, accessed 11/1/2017

⁵⁰ See the MITRE Common Vulnerabilities and Exposures Database at <https://cve.mitre.org/>, accessed 11/1/2017

4.2.9 Requirements from CIP-011 – Information Protection

NERC Standard CIP-011 – Information Protection deals with protecting information about BES Cyber Assets which could be used to compromise their functionality (such information is called BES Cyber Systems Information), and applies to utilities with high and medium impact BES Cyber Assets. BES Cyber Systems Information such as IP address, and PMU or PDC model can be contained in configuration files or data files extracted from PMUs and PDCs.

Requirement R1 specifies that methods must be developed and implemented to identify information that meets the definition of BES Cyber System Information, and procedures for handling and protecting BES Cyber System Information, including marking of information and media containing BES Cyber System information, as well as procedures used during transit and storage must be developed and implemented.

Requirement R2 specifies that procedures must be in place to protect against the inadvertent release of BES Cyber Systems Information on storage media, by ensuring that the information cannot be legibly retrieved from the media. If the media is to be re-used inside of an ESP of the same or higher impact level, a simple erasure of the media may be performed. If the media will be re-used outside of an ESP (e.g., used in a corporate environment), a more complete secure erasure may be used. If the media is to be disposed of, a more permanent erasure process, likely media destructions, is required. If whole-disk encryption has been used, destruction of the encryption key and a re-format is likely an acceptable information destruction process.

4.3 Medium Impact Requirements at a Control Center

The requirements for BES Cyber Assets located at a medium impact Control Center include all the provisions as a medium impact BES Cyber System with External Routable Connectivity described above (i.e., the same as are being assumed for a PMU or PDC at a medium impact field location), but with additional requirements. For a PDC at a medium impact Control Center location, all the medium impact BES Cyber Asset requirements from Section 4.2 of this report will apply, with the following additions.

4.3.1 Additional Requirements from CIP-005 – Electronic Security Perimeters

Requirement R1 specifies that inspection of data and traffic crossing the ESP must be performed, looking for malicious traffic, including malware, entering or exiting the ESP. Malicious traffic could include looking for unexpected protocols, unexpected command sequences, or unexpected code in the data stream.

4.3.2 Additional Requirements from CIP-006 – Physical Security of BES Cyber Systems

Requirement R1 specifies that cabling that exits a Physical Security Perimeter (PSP), but does not exit an Electronic Security Perimeter (e.g., cabling that runs from a data center PSP to a control room PSP but passes through the ceiling of an unsecured hallway) must be either physically or logically protected. Physical protection could be accomplished by encasing the cabling in conduit. Logical protection could be accomplished by encrypting the data prior to its exit from one PSP, and decrypting it after it enters the other PSP.

4.3.3 Additional Requirements from CIP-007 – Systems Security Management

Requirement R1 specifies that the use of unnecessary physical I/O ports, such as network ports, console ports, USB ports, etc. must be protected against. This is often accomplished by physically disabling them by removing internal jumpers or installing port blocking locks in the ports to prevent them from being used. Software disabling them (via configuration settings or by not starting software modules) is not recommended since the software could be compromised rendering the ports available for use.

Requirement R4 specifies that event logs be retained for at least 90 calendar days, if technically feasible, and except for CIP Exceptional Circumstances.

Requirement R5 specifies that unsuccessful login attempts be either monitored or managed by either locking the account after a number of unsuccessful attempts, or generate an alert after a number of unsuccessful attempts. The standard is silent on the number of unsuccessful attempts to be used before locking or generating the alert, but five is generally considered to be a reasonable number, balancing the practicality of authorized users forgetting or mis-typing passwords against the security of a password being guessed by a brute-force attack. Similarly, the standard doesn't address how locked accounts can be unlocked. They can be unlocked manually by an administrator, or it may be possible to automatically unlock them after a sufficiently long time period, say 15 minutes to an hour, depending on the sensitivity of the BES Cyber Asset being protected, and the typical urgency of the need to access the BES Cyber Asset after the account has been inadvertently locked.

4.3.4 Additional Requirements from CIP-009 – Recovery Plans for BES Cyber Systems

Requirement R1 specifies that a process be implemented for verifying that backups made for purposes of recovery or restoration will be usable when needed, and any verification failures are addressed. Backup failures could be either media failures, in which case, the backup media should be replaced, or procedural errors (e.g., not everything that should be backed up is included in the backup process). In the event of a process failure, the process must be updated, and the backup re-created. If the process has been in use for a period of time, and the failure is just noted, all previous backups should be examined to determine whether they are usable for recovery purposes, and if not, they should be marked so they are not inadvertently used for disaster recovery purposes.

Requirement R2 specifies that the recovery plan be tested annually. The test can be response to an actual incident, a “paper drill” (or “table top”) exercise, or an “operational exercise.” The documented response plan and procedures from requirement R1 must be used in the test, and records of actions taken during the test must be maintained. The test should include a sample of all information that could be used in the recovery to ensure that it is usable in the recovery process

Requirement R3 specifies that any lessons learned from the test be documented, and if the lessons learned indicate that the procedure must be modified, update the procedure within 90 days following the test, and communicate the updated plan to all persons with a role in the plan. Within 60 days of a change in responder roles, or a technology (e.g., a replacement system from a different vendor) mentioned in the plan, the plan must be updated, and communicated to all persons with a role in the plan.

4.4 High Impact Requirements

In general, requirements for BES Cyber Assets located at high impact Control Centers include all the provisions as a medium impact BES Cyber System with External Routable Connectivity (i.e., the same as are being assumed for a PDC at a medium impact Control Center), but with additional requirements. In a few cases, there are alternate requirements. For a PDC at a high impact Control Center location, all the medium impact BES Cyber Asset requirements from sections 4.2 and 4.3 of this report will apply, with the following additions and substitutions:

4.4.1 Additional Requirements from CIP-005 – Electronic Security Perimeters

Requirement R5 specifies that when dealing with account revocation, passwords for shared accounts (e.g., “admin” or “root” accounts) must be changed within 30 days, but allows for an extension if there is an extenuating operation circumstance (e.g., heat wave resulting in high power demands, or a storm restoration) of 10 days following the conclusion of the extenuating circumstance.

4.4.2 Additional Requirements from CIP-006 – Physical Security of BES Cyber Systems

Requirement R1 specifies that at least two different physical access controls are required. A keycard and pin or keycard and biometric, are often used.

4.4.3 Additional Requirements from CIP-007 – Systems Security Management

Requirement R4 specifies that at least every 15 calendar days, a review of logged events must be performed to ensure that all significant and actionable events are being processed and appropriate alerts being generated.

4.4.4 Additional Requirements from CIP-009 – Recovery Plans for BES Cyber Systems

Requirement R2 specifies that a full operational recovery test must be performed at least every three years.

4.4.4.1 Additional Requirements from CIP-010 – Configuration Change Management and Vulnerability Assessments

Requirement R1 specifies that changes that affect the baseline must be tested in a test environment prior to be installed in the operational environment (or at least tested in a manner that minimized adverse effects to the operational system), with the test results being documented.

Requirement R2 specifies that monitoring for changes or deviations in the baseline must be performed on a monthly cycle, with a process to investigate any deviations from the baseline configuration.

Requirement R3 specifies that, prior to adding a new Cyber Asset (that is not a direct replacement or addition of an existing Cyber Asset with the same configuration) into the environment (i.e., connecting it to a network inside the ESP), an active vulnerability assessment must be performed, and any issues found in the assessment must be remediated before the new Cyber Asset can be installed into the environment.

5.0 Implementation Options

There is no single way to implement the CIP Standards. The utilities that contributed to this review of implementation practices⁵¹ adopt one of three different synchrophasor use and CIP application postures.

- (1) A utility can determine that **none** of their PMUs or PDCs meet the threshold to be considered a BES Cyber Asset, because the synchrophasor system's functionality is not considered critical to operation or decision making in real time. This allows the owner to avoid the need to comply with the NERC CIP standards. (But the utility must still consider a number of other factors.)
- (2) A utility can decide that essentially **all** their PMUs and PDCs are either used to provide, or are capable of providing, information critical to their system operation or to real-time decision making. In this situation, it will need to adopt classifications and practices that make the synchrophasor system fully compliant with the CIP requirements.
- (3) An intermediate position is possible. Some PMUs or PDCs and their uses meet the BES Cyber Asset criteria, while others do not. There is more than one way to deal with this condition -- a dual-PMU or PDC scheme could be employed in which some important locations are served by one PMU or PDC that is considered a BES Cyber Asset and one PMU or PDC that is not.

We will examine practices in all these categories.

Bear in mind that while the following comments are intended to apply only to the PMU, PDC and their associated applications, there is some blurring of functionality between PMUs and relays, so both are considered.

Also note that there is a wide variety of possible options between the option to classify no PMUs or PDCs as BES Cyber Assets, and the option to classify all PMUs and PDCs as BES Cyber Assets. We will examine one of those options as an intermediate solution.

5.1.1 Minimal Classification

If a utility decides that none of its PMUs or PDCs are critical to its operations, it may effectively disconnect them from any real-time system by removing all communication access between the PMUs or PDCs and applications that could use data from the PMU or PDC for making real-time decisions. Provided the equipment "disconnected" in this way is not part of a decision chain, such disconnection ensures security and compliance (although it may create inconvenience).

Disconnection from real-time uses could allow remote access to the PMU or PDC for maintenance purposes or data retrieval, and may even include streaming data to a research or maintenance function, but the communication is still isolated from that used for providing data used to make real-time decisions. The utility will need to ensure that use of the PMU or PDC data does not cause the PMU or PDC to meet the conditions for being a BES Cyber Asset. The data from the PMU or PDC are still transmitted to the user, but they must be kept out of the regime of application that would consider them BES Cyber Assets. PMUs or PDCs used in this manner would fall into a category of use similar to a digital fault recorder,

⁵¹ Note – the utilities were contacted early in the Version 5 transition process while NERC was working with select industry participants to develop effective practices for Version 5 compliance. These three compliance examples are how common Version 3 compliance activities could be transitioned to the Version 5 paradigm.

used by maintenance and engineering department personnel (but not operators) for after-the-fact analysis of faults and transients on the power system.

The viewpoint behind this decision is that PMUs or PDCs are not BES Cyber Assets, because no operator will ever do anything based solely on data from a PMU or PDC. PMU data could be available in a control room for informational purposes, or as a trial application, as long as it is not relied on for operational decisions. In the control room, the parallel for this argument is the Weather Channel. Operators often use it as a guide, but it is never the only data considered. The utility would need to demonstrate that no operational procedures or instructions require the use of the PMU-based data or application for decision making purposes.

Disconnection is thus not regarded as an abandonment of the value and usefulness of PMU or PDC data. Rather, it represents a risk-averse approach to the introduction of new technology.

5.1.2 Partial Classification

A utility that has installed PMUs and PDCs might decide that while the information they furnish is always useful, only *some* of it is ever used for operational decisions. For example, if the data from one or two PMUs or PDCs is being used in the State Estimator, then those PMUs and PDCs should be identified as BES Cyber Assets, and be compliant with the NERC CIP standards. If for some reason one particular PMU or PDC cannot readily be brought up to compliance, its data must be removed from the State Estimator.

According to a NASPI presentation of survey results in 2015,⁵² “50% of the TOs have deployed PMUs or PDCs within a NERC-defined electronic security perimeter; most consider the synchrophasor technology a critical cyber asset” (which for CIP V5, roughly translates to a medium impact BES Cyber Asset). That means that the minimal classification approach of the previous section does not apply to them. This approach is a form of risk management that is acceptable to NERC, though it may not be simple to implement.

If a utility adopts this approach, it must determine the impact level *for each individual PMU and PDC* used to make real-time decisions, using the impact rating criteria described in Attachment 1 of CIP-002-5. For example, PMUs or PDCs used to help make real-time decisions at the point of interconnection with a 1,500 MW generator, and those monitoring transmission facilities at the 500 kV levels would be classified as medium impact and protected accordingly, while other PMUs or PDCs used to help make real-time decisions might be classified as low impact and given less stringent CIP protection.


Once the PMU or PDC at a particular location has been designated as having a high or medium or low impact rating, the appropriate compliance monitoring, physical requirements, electronic perimeter, and the records that have to be retained are fixed, according to the level of impact. There is a lot to be categorized and kept track of.⁵³ One way to keep track of the process of managing site-dependent data is

⁵² See https://www.naspi.org/sites/default/files/reference_documents/17.pdf, accessed 11/1/2017

⁵³ For example, all PMUs or PDCs categorized as medium impact *and* use what CIP calls “External Routable Connectivity” (which in practice will likely mean any that are connected any significant distance, or are connected to a synchrophasor data network) must have a defined Electronic Security Perimeter (ESP). (Even stand-alone networks for these devices must also have a defined ESP). The ESP defines a zone of protection around the PMUs or PDCs. Access *through* the ESP means taking certain security steps. These are based on the NIST Risk Management Framework and required by the CIP standards. Connectivity through the Electronic Security Perimeter is required to be via an identified Electronic Access Point, controlling both inbound and outbound traffic and

to collect information such as that shown here as Table I. This can be managed (for example, sorted by impact rating), and kept updated regularly as changes are made.

Table I: Example of Site Information Collected

CIP Sites					
Site name 	Impact Rating	Notes	Switchyard Cyber Assets	Compliance	Compliance Date
Church	High	Includes data center at Lulworth Lake	None	Y	March 9, 2016
Grange	Low			Y	April 4, 2015
Hennel	Low			Y	April 4, 2015
Holmrook Plains	Med	Multiple 345 kV lines		Y	April 4, 2017
Lulworth Lake	Med			N	August 25, 2017
Winckley Knoll	Low	Will be decommissioned in 2017		N	N/A

Since the utility will have to inventory every grid-connected Cyber Asset to determine how and why to classify it for CIP purposes, such a list could include every PMU and PDC and a device-specific explanation for its classification.

Even a utility that wants to treat all PMUs and PDCs as BES cyber assets may decide that some don't merit that treatment. Some PMUs or PDCs just cannot be made to comply, and that has to be accepted; the asset owner then needs to be sure those PMUs or PDCs are not used in for real-time operational decision-making. Implementing a partial protection solution requires threading through both physical and cyber access issues, which interact. The solution requires a good deal of planning and design, and the support of management. But it is possible to do it.

5.1.3 Full Classification

Even a utility that decides to make compliance of the maximum number of PMUs or PDCs a goal may, in the end, decide that not all PMUs or PDCs are going to be initially within the purview of the effort. So in a way, this part of the Recommended Practices report is not labelled with perfect accuracy (at least at the start). If a PMU or PDC just cannot be made to comply, and if the utility wants all of its PMUs and PDCs to be compliant, it should determine why that PMU or PDC cannot be made compliant, and propose a remedy to bring it into compliance. In the extreme case, the PMU or PDC may need to be replaced with a different (probably newer) model that can be made to be compliant.

The compliance tasks often have to do with both physical and cyber access, and these two aspects interact. The solution requires a good deal of planning and design, and the support of management. But it is possible to do it. For example, a PMU or PDC that was located —on the premises of a customer of the utility, say, or attached to a remote DER—a managed physical boundary may have a straightforward meaning if the DER is not large. A weather-tight cabinet with a key may suffice for physical security, and a router with access list capability implemented may suffice for logical security.

inspecting it for maliciousness. This is discussed in detail in previous sections (ref medium impact BES Cyber Assets).

Consider the business of getting data from a PMU or PDC, and perhaps changing its settings. Data, both to and from the PMU or PDC, may be encrypted.⁵⁴ In this case, measured results from the PMU or PDC are encrypted at the PMU or PDC location and decrypted in the control center. The process of sending data may be automatic via a UDP multicast (that is, it does not require a command from the control room) and the data stream is supplemented with a C37.118 Config2 frame every minute. This aspect of the cyber access issue is straightforward enough (and is considered to require an ESP, as described in the footnote on the previous page), but it is only part of the greater whole. What about the physical access issue?

Physical access to BES cyber assets must be restricted to only trusted employees. PMUs or PDCs at some locations may have different owners. For these locations, the matter of trusted employees requires some extra work.

Even then, access by someone visiting the PMU or PDC location is not done directly with the PMU or PDC, it is done via a connection through the control center and back. Instead of getting a direct connection to a PMU or PDC, the visiting employee would connect to a port on the equipment rack, and thereby would get access back to the control center via a secure network management system. Encryption is also used, and data coming from the control center are not allowed access to the PMU's or PDC's network interface. The network system is responsible for authentication by passwords, and (as appropriate) would send information to the PMU or PDC via a terminal server located in the rack. This system, of course, ultimately handles all the CIP rules⁵⁵

With this kind of operation, the password used in the PMU or PDC need not be known to the employee gaining access to it, and can be changed independently of the employee's password. Thus, when an employee leaves the company payroll, his/her password can be removed from the list. (This is a CIP-004 requirement.) Other employees do not have to be given new passwords, and do not need to be notified when a PMU or PDC key is changed.

Altogether, the solution requires a good deal of planning and design, support by vendor products, and the support of management. But it is possible to do it.

5.1.4 Recommended Practices Results

Table I compares the results of following the practices discussed above. It can be seen that PMU or PDC measurements are visible in all approaches.

⁵⁴ Encryption of data is a matter that seems to invite reconsideration by the NERC CIP standards development process, because at present CIP-005 requires traffic inspection capability.

⁵⁵ Note that not all systems are presently capable of this kind of operation, and some unexpected failure modes may exist.

Table I Results of following different levels of CIP adoption

	Solution Adopted		
	Minimal Classification	Partial Classification	Full Classification
PMUs or PDCs classified as BES Cyber Asset	None	Some	All at utility-owned locations
PMU or PDC data visible	Yes, but not for real-time use	Yes, for those PMUs or PDCs that are treated as medium and high impact	Yes, all PMU or PDC data available in real-time
Local access capability	Yes	Yes, subject to stringent physical and electronic security provisions for those PMUs or PDCs that are treated as medium and high impact	Yes, subject to stringent physical and electronic security provisions
Remote access capability	Some	Some, but only via secure communications	Yes, but only via secure communications
Documentation	least	intermediate	most
Ensure operator and field personnel training reflects this approach	Yes	Yes	Yes

6.0 Conclusion

The CIP Standards are an evolving set of requirements. The CIP V5 approach is attempts to make asset classification clear, objective and risk-informed. CIP V5 creates several levels of security classifications with associated levels of protection and compliance expectations. As applied to synchrophasor systems, security classifications are based on the impact rating of the location containing the synchrophasor system components and the function(s) performed by those components.

The CIP Standards (and in fact, all NERC standards) are intended to be performance or outcome based. The requirements describe the expected performance or outcome without prescribing the solution, to allow the utility flexibility and freedom to implement a solution that achieves the expected outcome.

The CIP standards establish a minimum set of performance expectations which utilities are allowed and encouraged to exceed. Compliance with the CIP standards does not guarantee security. Utilities that attempt to exceed a particular requirement should not fear audit repercussions if they fail to meet the higher goal, as long as their performance continues to meet the CIP standard requirement.

7.0 Further Reading

During the transition period leading up to full compliance with the CIP V5 standards, NERC and the NERC Regions developed and published numerous guidance documents to assist industry in the transition from CIP V3 to CIP V5. While none of this guidance is specifically targeted at synchrophasor systems, it is nonetheless a useful source of information pertaining to compliance with the new requirements, as well as offering guidance on compliance and implementation issues in supporting areas, such as communications.

The central repository for documents and presentation from NERC's "CIP Version 5 Transition Program" is located at <http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx> (accessed 11/1/2017). This web page contains links to supporting materials, including "Implementation Study, Lessons Learned, and FAQs" located at <http://www.nerc.com/pa/CI/Pages/Transition-Program-V5-Implementation-Study.aspx> (accessed 11/1/2017) in addition to other documents and web references.