

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the [NERC Help Desk](#). Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	CIP-002 Communications Protocol Converters SAR		
Date Submitted:	February 3, 2023		
SAR Requester			
Name:	Dr. Trey Melcher CISSP, CISM, CRISC		
Organization:	Burns & McDonnell		
Telephone:	314-391-9648	Email:	tmelcher@burnsmcd.com
SAR Type (Check as many as apply)			
<input type="checkbox"/>	New Standard	<input type="checkbox"/>	Imminent Action/ Confidential Issue (SPM Section 10)
<input checked="" type="checkbox"/>	Revision to Existing Standard	<input type="checkbox"/>	Variance development or revision
<input type="checkbox"/>	Add, Modify or Retire a Glossary Term	<input type="checkbox"/>	Other (Please specify)
<input type="checkbox"/>	Withdraw/retire an Existing Standard		
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
<input type="checkbox"/>	Regulatory Initiation	<input type="checkbox"/>	NERC Standing Committee Identified
<input type="checkbox"/>	Emerging Risk (Reliability Issues Steering Committee) Identified	<input type="checkbox"/>	Enhanced Periodic Review Initiated
<input type="checkbox"/>	Reliability Standard Development Plan	<input checked="" type="checkbox"/>	Industry Stakeholder Identified
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
<p>Section 4.2.3 of CIP-002-5.1a exempts "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." There are situations where Cyber Assets inside of a Control Center's Electronic Security Perimeter require communication to serially connected transmission facilities by using protocol converters. If the transmission facility does not have a defined Electronic Security Perimeter, the exemption of Section 4.2.3 is not applicable as two discrete Electronic Security Perimeters do not exist.</p> <p>There are inconsistencies in interpretations and approaches in categorizing such protocol converters when the Transmission Owner considers the transmission facilities to not have External Routable Connectivity or an Electronic Security Perimeter. This is found in transmission facilities with medium impact Bulk Electric System (BES) Cyber Systems having only serial communications traversing the physical location or transmission facilities with low impact BES Cyber Systems having no applicability for an Electronic Security Perimeter as required by CIP-005 (medium and high impact only).</p>			

Requested information

Additionally, when the protocol converters are physically located within the Transmission Operator’s Control Center, or associated datacenter, and not at the Transmission Owners transmission facility, the Transmission Operator owns and manages the protocol converters as opposed to the Transmission Owner. Other situations may exist where protocol converters are part of a Wide Area Network not owned or managed by either Registered Entity. In such situations, there is not an associated Functional Entity type defined in Appendix 5B of the Rules of Procedure.

This Standard Authorization Request is to consider if such a protocol converter meets the definition of a BES Cyber Asset by having an adverse impact to one or more facilities and the reliable operation on the BES. This includes consideration to the threat of unavailability, degradation, or misuse to a connected BES Cyber System and the aggregation of serial system-to-system communications from substations to Control Center BES Cyber Systems. As such, this project supports reliability by clarifying how these protocol converters should be categorized and if they are to reside within a defined Electronic Security Perimeter.

Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):

This project would provide clarification through revisions to CIP-002 on when a communication protocol converter meets the definition of a BES Cyber Asset

Project Scope (Define the parameters of the proposed project):

This project will make revisions to CIP-002 to clarify if communication protocol converters between a Control Center and a transmission facility meet the definition of a BES Cyber Asset and have a 15-minute impact. Consideration should also be given to generation Control Centers and facilities as protocol converters may also be used in the communication paths.

Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification¹ which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (e.g., research paper) to guide development of the Standard or definition):

Revise CIP-002 to include the identification of communication protocol converters and the relationship to the exception in Section 4.2.3. Specifically, the revisions would be to CIP-002-5.1a Requirement R1, and relevant attachments as necessary, regarding clarification for system-to-system serial communication protocol converters between a Transmission Owner low or medium impact BES Cyber System that connects to a Transmission Operators BES Cyber Systems by either enforcing an authentication break or by residing inside a defined Electronic Security Perimeter.

¹ The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
<p>Consideration should also be giving the security and reliability impacts. Moving the protocol converters inside of an existing Electronic Security Protocol may lower the security posture as the serial traffic is not required to transverse through an Electronic Access Point. Additionally, protocol converters range from capabilities and could lead to technical challenges and limitations when attempting to add authentication breaks on such system-to-system communication links.</p> <p>Consideration should also be given to other types of Cyber Assets used in the communication paths, such as routers and switches, along with ownership and management of the Cyber Assets as applicable to Functional Entity types defined in Appendix 5B of the Rules of Procedure.</p>
<p>Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):</p>
<p>Cost impact is unknown at this time.</p>
<p>Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (e.g., Dispersed Generation Resources):</p>
<p>The physical location of protocol converters is generally inside the Control Center and Physical Security Perimeter, but logically located outside of an Electronic Security Perimeter. This creates a scenario whereby categorizing the protocol converters as a BES Cyber Asset and moving them into an Electronic Security Perimeter bypasses the Electronic Access Point.</p>
<p>To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (e.g., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):</p>
<p>Transmission Operator and Transmission Owner. There is a potential that Generator Operator Control Centers and Generator Owner facilities could have similar architectures and Cyber Assets. The modifications to the Standard should include both transmission and generation architectures.</p>
<p>Do you know of any consensus building activities² in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.</p>
<p>None</p>
<p>Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?</p>
<p>NERC Project 2021-03 CIP-002</p>
<p>Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.</p>

² Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information

None

Reliability Principles

Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
<input type="checkbox"/>	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
<input type="checkbox"/>	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
<input type="checkbox"/>	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
<input type="checkbox"/>	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
<input checked="" type="checkbox"/>	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
<input type="checkbox"/>	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
<input type="checkbox"/>	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
<input checked="" type="checkbox"/>	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles

Does the proposed standard development project comply with all of the following Market Interface Principles ?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances

Region(s)/ Interconnection	Explanation
<i>e.g.</i> , NPCC	None

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).

<input checked="" type="checkbox"/> Draft SAR reviewed by NERC Staff	<input type="checkbox"/> Final SAR endorsed by the SC
<input type="checkbox"/> Draft SAR presented to SC for acceptance	<input type="checkbox"/> SAR assigned a Standards Project by NERC
<input type="checkbox"/> DRAFT SAR approved for posting by the SC	<input type="checkbox"/> SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer