EnergySec
The National Energy Sector Cyber Security Organization

CIP V5
The Top Issues with CIP-002-5.1 and What You Can Do About Them

EnergySec Webinar
May 20, 2015

Agenda

- Introduction and background
- Key Issues – Tom Alrich
- Key Issues – EnergySec
- RFIs and SARs
- Q & A

Meet Your Panelists

Tom Alrich
Manager Cyber Risk Services
Deloitte and Touche LLP

Karl Perman
VP, Services
EnergySec

Steve Parker
President
EnergySec

It's Interactive

Please submit your questions through the control panel to get answers LIVE from our panelists.

It's Hip to Chat

EnergySec is hosting an online chat to accompany this webinar which is open to all registered EnergySec Community participants.

To join the chat as a guest, visit:
https://hipchat.energysec.org/gaWDbbtQT

If you have a HipChat account already, join us in the CIP-002 Webinar Discussion room. Note: Registered users have access to the chat history, file attachments, and links

Webinar Goals

- Provide an independent perspective on key issues with CIP-002-5., including a summary of current guidance
- Offer insights and suggested approaches for dealing with these issues
- Explain formal processes available under the NERC Rules of Procedure for addressing concerns
- Provide a forum for Q&A

Deloitte.

Some top issues with CIP-002-5.1

and what you can do about them

Tom Alrich
Manager
Cyber Risk Services
Deloitte & Touche LLP
May 20, 2015

Agenda

- Introduction
- Identify major interpretation issues in CIP-002-5.1
  - Issue #1: “Facilities” vs. “assets”
  - Issue #2: “Adversely impact”
- Conclusion / key takeaways

Issue #1: “Facilities” vs. “assets”

- CIP-002-5.1 R1 mentions “assets”
  - Attachment 1 mentions “Facilities” in some criteria and never mentions “assets”
- Some of the criteria apply to Facilities – a NERC-defined term
  - Loosely, a “Facility” is operated at high voltage and has terminals.
- Other criteria apply to different types of assets – “Generation”, “SPS”, “RAS”, “Control Center”, etc.

Issue #1: “Facilities” vs. “assets” (continued)

- Criterion 2.1 applies to “Generation”
  - this is an asset (the whole plant)
- Criterion 2.3 applies to “Generation Facilities”
  - The entire plant doesn’t have terminals, only the individual units, so R3 applies to a single unit or multiple units
- Criterion 2.6 says “Generation”, but NERC recently said that means “Generation Facilities”:

  (a unit or units, in other words)
- What about substations? 2.4 through 2.8 apply to substations, however they all read “Facilities” so what does this mean?
  - a “Facility” in a substation is a line, transformer, circuit breaker, bus, etc…it is *not* the whole substation

Issue #1: “Facilities” vs. “assets” (continued)

- Technically, substations don’t have an impact rating, only the “Facilities.”
- In Criterion 2.4, it states “Transmission Facilities operated at 500kV or higher”:
  - For example, you have a substation with two lines, each with associated breakers and relays. One line is 500kV, the other 230 kV. The 500kV line meets 2.4; the 230kV does not. Relays associated with the 500kV line are Medium impact; those associated with the 230kV line are Low impact.

Issue #1: “Facilities” vs. “assets” (continued)

- 2.5 contains two “criteria”
  - The first is Facilities “operating between 200kV and 499kV at a single…substation.”
  - The second “criterion” is for the substation itself. You will need to add up the weightings to see if the substation has 3,000 points.
- The SDT didn’t want to make all lines between 200 and 499kV Medium impact – just those that are at certain critical substations.
- If a substation has 3000 points, it still isn’t technically Medium impact. This means the 200-499kV Facilities at the substation are Medium impact, and the BES Cyber Systems associated with them are Medium impact too. Any lines below 200kV are Lows and their associated BES Cyber Systems are also Lows.

Issue #1: “Facilities” vs. “assets” (continued)

- In criteria 2.3 through 2.8 (also 2.9 and 2.10), it is technically the Facility that is Medium impact, not the asset (i.e. the generating plant or substation). However, in practice everyone refers to Medium impact plants and substations.
- Why is it important to distinguish assets from Facilities? It is definitely important for generation in 2.3 and 2.6, as it will be very expensive to treat an entire plant as Medium vs. just one unit (for example, where a single unit in a plant has been designated Reliability Must Run and therefore is Medium under 2.3).
- For Transmission substations, many entities are treating the entire substation as Medium, since it may be difficult to separate Medium from Low BES Cyber Systems.

Issue #1: “Facilities” vs. “assets” (continued)

- What should an entity do about this issue?
- If you have a generating unit subject to 2.3 or 2.6, you should definitely consider just treating the unit as Medium, not the whole plant. That is what you’re required to do.
- If, like most NERC entities, you plan to treat all BCS at “Medium” substations as Medium impact, then you need to document this decision.
- Regardless of your decision in this matter, it is still a good idea to identify, in Medium substations, the Facility (line, etc.) that each Cyber Asset is associated with:
  - This will be very helpful when you try to determine whether the Cyber Asset can have “adverse impact”, the next topic.
  - Also, you may decide later that you do want to classify BCS by the Facility.

Issue #2: “Adversely impact”

- The meaning of “adversely impact” is one of the most important issues in CIP v5. It is required for applying the BES Cyber Asset definition.
- This isn’t a case – like “programmable” – where a simple definition is required. Rather, a *procedure* is required to determine whether a Cyber Asset can adversely impact the BES.
- The BES Cyber Asset definition can be thought of as three criteria, applied to a Cyber Asset:
  1. Its unavailability or misuse would “adversely impact” one or more “Facilities, systems or equipment” (FSE).
  2. This impact has to occur within 15 minutes.
  3. If the above adverse impact causes the FSE to be “destroyed, degraded or otherwise rendered unavailable *when needed*”, this will “affect the reliable operation of the (BES).”

Issue #2: “Adversely impact”

- There are two levels of impact in question:
  1. Does the Cyber Asset impact the asset or Facility it’s associated with?
  2. Does this *necessarily* translate into an impact of the asset or Facility on the BES itself?
- If the answer to either of these questions is “no”, the Cyber Asset isn’t a BES Cyber Asset.
- If the answer to both is “yes”, and if there is also a 15-minute impact, then the Cyber Asset is a BCA.

Issue #2: “Adversely impact”

There are two questions:

1. Does the Cyber Asset impact the asset or Facility it’s associated with?
   - Since it is a control system, it’s very hard to argue it doesn’t have an impact on the asset/Facility (the impact may not be in 15 minutes – then it still wouldn’t be a BCA).
2. If the answer to the above is “yes”, does this *necessarily* translate into an impact of the asset or Facility on the BES itself?
   - Not every impact on a BES asset/Facility results in an impact on the BES.
   - How do we know whether or not it has this impact?

Issue #2: “Adversely impact”

- This is where the BES Reliability Operating Services (BROS) can help.
  - These provide a “Cliff’s Notes” version of how an asset/Facility can impact the BES.
- If an asset/Facility normally fulfills one or more BROS, but can no longer *completely* fulfill all of them due to the impact of the misuse or loss of a Cyber Asset, then the answer to the second question is “Yes”.
  - In other words, “Yes” means the loss/misuse of the Cyber Asset does impact the asset/Facility in a way that results in an impact on the BES. If the impact is within 15 minutes, the Cyber Asset is a BCA.
  - If this isn’t the case, the answer to the second question is “No”, and the Cyber Asset isn’t a BCA.

Issue #2: “Adversely impact”

- Note that we’re not talking about the impact of the Cyber Asset itself on the BES. In the majority of cases, Cyber Assets don’t by themselves impact the BES.
- Two examples:
  1. SEMS system – impacts the plant (by shutting it down). The plant shutting down can cause a BES impact (through the BROS) in 15 minutes. Therefore SEMS is a BCA.
  2. Phone system – impacts the asset (e.g., plant or control center), but that doesn’t *necessarily* cause a BES impact (through BROS) in 15 minutes. So it’s not a BCA.

Conclusions / Key takeaways

- Unfortunately, there are many interpretation issues in CIP-002-5.1 that haven’t been definitively addressed.
- In these cases, responsible entities have no choice but to develop and document their own interpretations.
- You must show you considered all the available guidance – at the time you needed to address this issue.

Contact Us

Sharon Chand
Director
Deloitte & Touche LLP
+312 486 4878
shchand@deloitte.com

Eric Bowman
Senior Manager
Deloitte & Touche LLP
+1 206 716 7839
ebowman@deloitte.com

Tom Alrich
Manager
Deloitte & Touche LLP
+1 312 515 8996
talrich@deloitte.com

Deloitte.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Two More Key Issues

- Criterion 2.1 – Shared BES Cyber Systems at large generation plants
  - What are shared systems?
  - Can you "split" a plant to lower impact levels?
  - What are common mode vulnerabilities?
- The meaning of "Programmable Electronic Devices"
  - What is programmable?
  - Is the draft Lessons Learned still valid?
  - Is NERC's memorandum final?

What are Shared Systems?

Criterion 2.1

For each group of generating units, 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 units that in aggregate equal or exceed 1500 MW in a single Interconnection.

SDT Guidance

By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

What are common mode vulnerabilities?

FAQ 50

Any systems that can affect two or more BES Facilities, such as multiple generation units. A substation could affect the entire generation location if it were disabled and power was not able to be transmitted on the grid. Protection systems, fuel-handling systems, cooling water, and air systems are also examples that should be evaluated as common mode vulnerabilities.

- Appears to refer to plant systems that are shared between units
- Substation reference seems out of place

SDT Guidance

ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

- Appears to refer to BES Cyber Systems that can be compromised via the same vulnerability

Can you "split" a plant to lower the impact level?

NERC Lessons Learned

Segment the Generating Units and Their Associated Shared BES Cyber Systems. Responsible Entities may choose to segment generating units … and their associated BES Cyber Systems such that each segmented unit, or group of units, and their associated BES Cyber Systems do not meet the 1500 MW criteria…

… provide evidence that shared BES Cyber Systems … are segmented effectively such that there are no shared BES Cyber Systems that could result in the loss of 1500 MW or more of generation

What about electronic connectivity?

NERC Lessons Learned:

Identifying shared BES Cyber Systems involves detailed analysis that considers shared generating plant operational processes (e.g., air, water, steam, environmental, and fuel handling processes) and electronic connectivity.

evidence that could demonstrate effective segmentation includes:

- BES Cyber Systems protected by the segmented unit network(s)
- Access restrictions on network interfaces between each generating unit or group of units and external networks (e.g., firewall rules)

The implication is that BES Cyber Systems on a common network might be considered "shared"

Programmable Electronic Devices

Cyber Asset Definition (V5)

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

Programmable (Dictionary.com)

capable of being programmed.

Programmable (Thefreedictionary.com)

capable of being programmed for automatic operation or computer processing

NERC Memorandum

April 22, 2015 “any device that is electronic and capable of executing a set of instructions.”

<u>Differs from NERC Lessons Learned</u>

January 9, 2015

“whether the device has a microprocessor and filed-updateable firmware or software”

Standards Authorization Request Process

1. Project Identified in Reliability Standards Development Plan or initiated by the Standards Committee
2. Draft SAR
3. Post SAR for 30-day informal comment period
4. Develop Draft of Standard, Implementation Plan and VRFs and VSLs
5. Obtain Standards Committee Approval to post for comment and ballot
6. Comment period and ballot
7. Revise Draft Reliability Standard, if needed
8. Post Response to Comments
9. Conduct final ballot
10. Submit Reliability Standard and Implementation Plan to BOT for Adoption and Approval
11. Submit all BOT-approved documents to Applicable Governmental Authorities for approval

Request for Interpretation Process

- "When a requirement of an approved Reliability Standard is unclear, and the lack of clarity or an incorrect interpretation could result in a direct, material reliability impact to the requesting entity."

1. Any entity that is directly and materially affected by the reliability of the North American Bulk Power Systems may request an Interpretation
2. NERC Reliability Standards and Legal Staff review and accept, reject or ask to have Request modified and resubmitted
3. If accepted, then form a ballot pool and assemble an Interpretations Drafting Team
4. IDT may submit a SAR if they identify that an Interpretation is not the appropriate remedy
5. IDT creates the Interpretation, which will be balloted, similar to a Standard
6. If approved by ballot pool, then the Interpretation is forwarded to NERC Board of Trustees

Questions

Thank You

Deloitte.

Tom Alrich
talrich@deloitte.com
312.515.8996
www.deloitte.com

EnergySec
The National Energy Sector Cyber Security Organization

Karl Perman
karl@energysec.org
503.905.2000
www.energysec.org