All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Powerful security

I have been spending time lately with more and more up to date standards documents that are more and more confusing. This weekend I spent a few dozen hours looking at NERC-CIP[1] to try to figure out an easy way to explain it to people who actually have to implement it. I am pretty much certain at this point that it is not that hard to understand, if you have a Ph.D., 40+ years of experience, and several days to read it. In fact, it is a really sensible approach with reasonably defined metrics that can be measured and used to make decent decisions.

It's not the substance – it's the form

I cannot believe I am saying this. I have spent years decrying the "form over substance" problem in that people seem to put form over substance, starting with the MacDocuments we saw when people started using Macintosh computers and their WYSIWYG[2] interface to produce documents that look great but have less flavor… OK it wasn't the flavor. It's the use of end of page to determine what words you use that was the problem. And these days, I hate the user interfaces that put a few things on a page and make you scroll up and down to see what should be readily visible in a single screen. Bad UI[3], though, is a different issue than my present point.

In reading standards, and NERC-CIP is the flavor of the month in this case, I find it is often nearly impossible to disentangle the real situation. Here's a sample:

- Each BES Cyber System used by and located at any of the following:
  - 1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.
  - 1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.
  - 1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.
  - 1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.
  - …
  - 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. 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.

1 North American Electrical Reliability Corporation – Critical Infrastructure Protection – the standard for North American electrical power providers being adopted increasingly around the world
2 What You See Is What You Get
3 User Interface

It's not the substance

Just to be clear, the substance of this is great. If you look carefully, what is really says is that, for example, (1.4) if you have a control center (or backup control center) that acts as the General Operator for anything (2.1) that has generated (over the last year) or could cause loss of more than 1.5 Billion Watts[4] of power within 15 minutes (all in a single connection) it gets a "High" impact rating. Sort of… there are lots of other conditions for getting this rating, but the concept is right… if a failure can have a consequence over a threshold, it has "High impact".

It's the form

I agree – power loss to millions of homes should be considered high impact. Of course that's not what the standards say. And the reason, it seems to me, is that the people writing these standards are dealing with rules that engineers can try to apply by doing calculations. We engineers (I count myself among them by training, education, and experience) unfortunately tend to have a hard time understanding things like "power loss to millions of homes". We start to ask questions like:

- How many homes exactly? What happens when I design my system then they build more homes? If there is a fire that burns some of the homes does the fire make my control center lower impact?[5] What kind of homes? Some generate their own electricity most of the time using solar power… and so forth.

The problem here is not that the specifications are in terms of measurable phenomena like Watts and Volts and Amps. That's a good thing. The problem is that for some reason somebody somewhere probably said something like this:

- We can generate 1500MW of power, but usually only generate 1480MW of power. Why should we have to do all that extra stuff for 1500MW?

No doubt once that started, the food fight began, the lawyers got involved, and we got things like "12 calendar months" (is there some other sort of month?) and "that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed" (Who does the calculation to determine it was 15 minutes and 8 seconds so we aren't "High" impact?)

And the volume

Of course I only chose one example. If you look at the big picture, it's a big picture! That was Section 1 of Attachment 1 of CIP-002-5.1a. That attachment is 23 pages long, or about 30 times the size of the part I quoted. And that's one of 14 different currently active CIP components that apply to CIP version 6.

The producers of NERC-CIP provide helpful tools to get the job done. In fact, they provide a spreadsheet that has these things codified so implementers don't have to copy and paste sentences from the PDF files into their own spreadsheet to make the information usable. That's a good thing and it reduces the effort for compliance. That's not the problem.

---

4 That's 15 million 100 Watt light bulbs, or 750,000 homes with 200 amp 110V connection (20KW) using 100% of their capacity. More typically 1.5M homes or more affected.

5 Ask PG&E which apparently caused the fire in Paradise, CA destroying thousands of homes by knowingly failing to maintain a safe condition. I'm pretty sure it wasn't engineers trying to lower the NERC-CIP threshold.

And the definitions

Of course we wouldn't want anybody to be confused about what constitutes a "Control Center" or a "backup Control Center". Otherwise some clever person out there will decide they don't have a "Control Center" - rather they have two "Control Points", neither of which is at the "Center". So it doesn't apply to us – right? The "Glossary of Terms" is a 57-page small font document that is truly beautiful. Here is what constitutes a "Control Center":

- One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Note that there is no definition of a "backup Control Center" provided.

Like any good dictionary, the terms within other terms are also defined. For example:

- **Balancing Authority:** The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
- **Balancing Authority (as of 2019-01-01):** The responsible entity that integrates resource plans ahead of time, maintains Demand and resource balance within a Balancing Authority Area, and supports Interconnection frequency in real time.

Note that definitions change over time, and thus the dictionary identifies the effective date of new definitions, in advance, so that planning can be done for such changes. However, you might also note that changing definitions may have a wide range of effects on the 14 components and their many different sections, subsections, subsubsections, and so forth.

How is a power engineer supposed to do all of this?

They are not! Running a critical infrastructure is a team sport. It takes more than a village to run a power infrastructure supporting millions of homes. It takes executive management, teams of engineers and line workers, specialists, control center operators, engineering firms that supply lots of different equipment and systems, lawyers, accountants, maintenance people, workers who do day-to-day "paperwork" tasks, and so forth.

Still, a bit of authorship would help

None of this excuses the unnecessary complexity of the wording and structure of documents. And I take blame where blame is due. Ultimately, anything that is enforced with fines or other legal penalties will be bandied about at great length, producing lots of special cases, and lots of wording issues that are ultimately meaningful in financial terms. I do expert witness work, and I plea guilty to contributing to the complexity of documents and wording. NERC-CIP looks like a document I had a hand in writing, and even though I didn't, and wish I did, I take blame.

Conclusions

I pledge to try to write more readably, especially in technical documents others may have to read and follow. And I pledge to try to help others do the same, in a reasonably friendly way, which I hope is the spirit this article will be taken in by those who wrote and continue to improve NERC-CIP and other similar things that help keep us all safe, alive, and well.

