Tom Alrich's Blog

Tuesday, June 21, 2016

Is NERC CIP Hindering Innovation?

Stating the Problem

The CIP standards are always just a small part of the NERC CIPC (CIP Committee) meetings, which focus on many different initiatives and issues regarding cyber security in the electric sector. Usually, the CIP discussion (always led in the past couple years by Scott Mix or Tobias Whitney) is just a summary of what has been going on lately with the standards, and there is nothing too surprising about what is said. However, Tobias Whitney's presentation at the most recent CIPC meeting, in St. Louis on June 7, was quite surprising – to me and a number of others. And it was quite welcome as well.

The title of Tobias presentation (which hasn't been posted as of June 17. I will post the link in a comment below when it is available) was something to the effect of "Is CIP Hindering Innovation?" Tobias explained that what he meant by this question was whether there are new technologies that utilities would like to deploy in their OT environments, but which they aren't deploying for fear they will run afoul of some CIP requirements by doing so.[i] One example of this negative effect is virtualization, as I discussed in this post.

What was probably most surprising about the presentation[ii] was that Tobias wasn't at all disputing the answer to the question in the title. He started out admitting that CIP can restrain innovation, and the example he used of this was the well-known fact that, under CIP versions 1 through 3, some utilities had held off on deploying routable connectivity to their substations – or in at least a few cases literally ripped it out. They did this because CIP v1-3 provided a "get out of jail free" card in cases where there was no external routable connectivity to an asset; the asset automatically was deemed not to have any Critical Cyber Assets. Since the presence of Critical Cyber Assets, like BES Cyber Systems in CIP v5 and v6, was the sole determinant of whether there was a substantial CIP compliance responsibility at an asset, these utilities decided the benefits of deploying routable connectivity to a substation (such as not having to send a technician to the substation to deploy every new patch) were greatly outweighed by the compliance costs of having CCAs and therefore being subject to all the CIP requirements.

While this is certainly an example of CIP inhibiting innovation, I don't think it was the right one for what Tobias was trying to say. The rest of his presentation discussed areas where deployment of particular technologies may be hindered because those technologies aren't addressed at all in CIP currently; this may be leading NERC entities not to want to deploy

those technologies, for fear of running afoul of some CIP requirement or other. But the example he used was one where there was no uncertainty at all: If there was no external routable connectivity, there were no CCAs, period. In other words, the CIP v1 – v3 standards as written provided a direct incentive to utilities not to deploy ERC. I'm sure this wasn't the intent of that provision when it was inserted in CIP v1, but it can't be said that v1-3 ignored the issue of external routable connectivity. Intentionally or not, it directly discouraged its deployment. But that's not the problem with the other technologies Tobias was discussing.

Tobias produced a list of six technologies whose deployment may well be hindered because of uncertainty about how CIP would apply to them; and he made it clear there are almost certainly other technologies in the same boat as well. He listed:

1. The cloud. Of course, the main problem here is that, if CIP is applied literally to data stored in the cloud, every person who has access to any server that might store some of the utility's CIP-protected data will need to be vetted by that utility. This is almost impossible for cloud providers to guarantee.
2. Renewables. Tobias said the main issue here is new GOs (Generation Operators) who manage a lot of "behind the meter" renewables (mainly solar panels, of course). Tobias said that some of these GOs have aggregate capacity approaching 1500 MW, which surprised me. Of course, the bright-line criteria, and especially criterion 2.1, were never written with the idea that there could be anything as recondite as behind-the-meter generation.
3. IEC 61850. Since 61850 uses IP, there isn't much question that it is a routable protocol; thus, uncertainty isn't really the problem here - in theory, 61850 communications should be treated just like any other communications. The problem is that 61850 is inherently a real-time protocol and having to apply controls to it, like encryption, might well make it not worth deploying. The definition of Low impact External Routable Connectivity (LERC) in CIP v6 specifically excludes external communications like 61850 and GOOSE from being considered LERC.[iii] However, there are many areas of application of 61850 (external 61850 communications for Medium impact assets, as well as internal 61850 communications for Medium or High impact assets) that are simply left unaddressed in the current CIP standards. This is where the uncertainty comes in.
4. Virtualization. I wrote about this issue in the post referenced above. However, the v7 SDT is hard at work drafting revisions to the v5/v6 standards and definitions that will take account of virtualization, rather than simply ignoring the technology. So in this one case, it can be said that in a few years CIP will take account of virtualization. That can't be said for any of the other technologies on this list, of course.
5. Wireless. I believe what this means is WiFi within the ESP, where the issue is that it is fairly hard to restrain the signal from crossing the PSP, even if the PSP is well outside of the ESP. What CIP requirements will be violated if that happens? Probably a lot.
6. End of life systems. To be honest, I don't know what Tobias meant by this, and I don't think he talked about it in his presentation (it was listed on a slide).

I agree with Tobias that there are other technologies you could add to this list. One that I mentioned, in a question after his presentation, was managed security services (managed firewall, managed authentication, etc). I have been told by one auditor that he knows of no NERC entity in the US, which has Critical Cyber Assets or Medium or High impact BES Cyber Systems, that is using a third-party service to monitor or manage their ESP. In fact, the auditor told me that his region had to tell one entity to terminate their use of such a service and that he did this with a heavy heart – since he believed the entity was more secure with the service than without it.

The reason that managed security services don't work under the current CIP regime is the same one that I alluded to for cloud services above. If a NERC entity with High and/or Medium impact assets contracts a third party to monitor and/or manage security information from their ESP, then every employee of that third party, who has any physical or logical access to any server that stores the NERC entity's security information, will have to be vetted by the NERC entity just like any of their own employees who has such access. In practice, this probably means the third party firm will have to segregate servers that house any of the entity's data in a separate room with its own badge reader; only the employees who have been vetted will have access to that room. In practice, of course, this is impossible for most third party service providers to implement.

NERC's Proposed Solution

The above was Tobias' statement of the problem; the 120 or so people in the room seemed to agree that he had done a good job so far. So what was Tobias' proposed solution? I regret to say that the agreement in the room seemed to vanish when he discussed that.

At first glance, you might wonder why there was so much disagreement with Tobias' solution. He proposed something to the effect that the best minds in the NERC community get together and draw up guidelines for – say – using cloud services or WiFi in an ESP. The implication was that, if NERC entities followed those guidelines, they likely would not be judged to have run afoul of the current CIP v5 and v6 requirements. So entities could implement those technologies without fear of suffering the swift hand of judgment by NERC or their region, for violating requirements that make no mention at all of the technology in question in the first place. Many of the people in the room commented, and most of those comments (including mine) were – respectfully – negative.

If you are very new to the NERC CIP world, you might wonder what all the complaints are about. After all, it seemed that Tobias was saying that NERC was willing to be flexible in enforcing the CIP standards, so as not to prevent adoption of any of these new technologies. In other words, the rules would be bent in some way, so that entities could implement these technologies. What's so bad about that?

What's so bad about this – in my opinion - is that we've heard this song before. That is, NERC was previously faced with serious questions regarding how the CIP standards should

be interpreted, and they promised to resolve them in creative ways. Yet after almost two years of trying different approaches to do this, they had to admit there was no way this could be done, other than the two methods that are currently "allowed" by the NERC Rules of Procedure: Requests for Interpretation (RFIs) and Standards Authorization Requests (SARs). Both of these methods literally take years to produce results. Meanwhile, NERC entities are left in exactly the same uncertainty that they were always in, before NERC tried to improve the situation.

To be specific, in early 2014 many NERC entities started spending some quality time trying to understand the CIP v5 standards, since FERC had just approved them in November 2013. As they did this, they started having lots of questions about what the requirements meant.[iv] The question came up of how NERC could provide guidance on these questions – given that the only two "official" ways to do that were RFIs and SARs. NERC's answer to this question was very clear: "Don't worry, we'll take care of it!"

NERC talked about various ways in which they could provide guidance. One of the first was to embed guidance in the RSAWs; after one try at this it became clear this approach wouldn't work. Another approach was the CIP v5 Implementation Study. But when the study came out, it was clear that – while it did provide a lot of good ideas for how to implement CIP v5 compliance – it didn't (indeed, it couldn't) address any interpretation questions.

Probably NERC's most promising idea for providing guidance was the Lessons Learned. They drafted a large number of these, some addressing some difficult guidance issues including "Programmable" and virtualization. But in the end, only ten LL's were finalized. As with the Implementation Study, these ten documents provided very good tips on how to implement compliance, but none of them provided guidance on interpretation questions. All of the draft LLs that did address such questions (along with the late, unlamented Memoranda) were withdrawn.

These interpretation questions were then turned over to the new Standards Drafting Team (as described in this white paper from the NERC CIP v5 Transition Advisory Group). Some of these questions[v] will be resolved in the next CIP version, but that is unlikely to be in effect before 2018 at the very earliest. So it turns out that there *was* no other way for NERC to provide CIP v5 guidance, except through RFIs and SARs. Meanwhile, NERC entities are still on their own as far as interpretation of these v5 issues goes – just as they were in early 2014.

So I hope that I – as well as others in the room at the CIPC meeting – can be excused for our skepticism when Tobias once again told us that the problem of CIP hindering innovation could be addressed by some sort of creative thinking on NERC's part. While Tobias' (and NERC's) intention is certainly good, there is simply no way that NERC entities can ever feel completely safe in implementing these new technologies until they are actually directly incorporated into the standards (i.e. the SAR process), even though that will take years. Trying to once again figure out a way to circumvent this long process is bound to fail.

The Real Solution

So what is the real solution to this problem of CIP hindering deployment of new technologies? I can see two options. The first is to simply go through the SAR process for each of these areas. That is, NERC should start working today (well, tomorrow is OK) on SARs for every technology discussed above (except virtualization, since that has already been included in a SAR). For each of these technologies, they will have to appoint a Standards Drafting Team (they certainly don't want to dump all this on the current SDT![vii]). Some of these SARs might be combined, so that each one wouldn't require its own SDT.

Of course, it will probably take six months for each new SDT to be appointed and have their first meeting. Then it will take at least 6-9 months for them to come up with their first draft. That will then be submitted to a NERC ballot, and – if the past is any guide – will almost certainly fail to pass. So a new draft will be developed in say three or four months, submitted for a new ballot – and probably also voted down. After at least 3-4 ballots, there will be a final version of the new (or revised) standards. This will be submitted to FERC and approved by them in probably no less than six months. So each of these new technologies will take at a bare minimum three years to be actually "built in" to the CIP standards. At that point, NERC entities can safely implement them.

Incorporating each of these new technologies will require an expansion of the CIP standards, so that they may be - say - twice as large once all of the above technologies are accounted for.

And of course, as new technologies come around that NERC entities would like to take advantage of, the same process will need to be repeated for each one. So there will be an ongoing need for CIP drafting team members! In fact, I can see this becoming a career option in itself, with courses being taught in colleges on NERC CIP SDT Membership. Is this great or what? Meanwhile, the NERC CIP standards will approach the length of the Bible, and some utilities will start dedicating a majority of their staff to CIP compliance!

I don't know about you, but I find Option 1 to be profoundly depressing. It will provide ironclad assurance that the electric utility industry will always be behind all other industries in taking advantage of new technologies (how long ago did virtualization first appear? And how long will it be before CIP v7 finally makes it safe to implement in your ESP? My guess is there is at least a 15 year gap between the two dates). And it will also assure that an ever-increasing share of utilities' budgets will go to CIP compliance. What's Option 2?

Option 2 is something I have been talking about for a while, and I can promise you there's a lot more to come. In fact, I and two co-authors are starting work on a book on this topic. The fact is, I believe NERC CIP is now on a completely unsustainable course. In the post just referenced, I focus on the idea that it is economically unsustainable, and what I've just discussed simply reinforces that. CIP compliance costs mushroomed under CIP v5, and they will continue to expand as CIP is expanded to include new areas (virtualization, supply chain,

the cloud, etc). Further expanding CIP to accommodate each of the technologies I've been discussing will simply assure that expansion will continue, until total NERC CIP compliance costs approach the level of the national GDP.

And what I've just been writing about adds a whole new level of unsustainability to CIP. Not only are the direct costs of CIP compliance going to continue to expand rapidly as time goes on, but the indirect costs are as well. These indirect costs include the "costs" that utilities incur by not being able to take advantage of new technologies (in their ESPs) like virtualization and the cloud. I heard today of a major utility whose control center server room used to be chock full of boxes in every nook and cranny. Now all those boxes have been compressed into less than three racks, saving lots of money as well as greatly simplifying server administration. Any utility that isn't doing virtualization in their control centers is probably forgoing (proportionately) similar cost savings. And just think of the savings a utility might reap if there were some way to use cloud services within ESPs (currently I believe that is impossible under CIP, although I'd love to hear if you are doing it and are comfortable with the compliance aspect).

Why are the CIP standards so unsustainable and so unfriendly to innovation? It is because they are prescriptive. Prescriptive security standards address a certain pre-determined set of threats and are based on a pre-determined set of technologies (and if you think that CIP is becoming less prescriptive, please read this post). That would be fine if both the threats and the technologies didn't change, but that simply isn't the case; in fact, one could make the case that these are both changing faster than ever.

What is needed are non-prescriptive standards – of which a good example is CIP-014. With non-prescriptive standards (I used to call these "risk-based", but I and my co-authors have decided that isn't the right term. We're currently trying to figure out what is the right term - perhaps "threat-based"), regular assessments identify the threats the utility faces, as well as the technologies in place that need protection; the outcome of these assessments yields the set of steps the utility must take to address cyber security. The threats and technologies in scope will be as up-to-date as the last assessment; if a utility decides it needs to deploy cloud technologies, it will get a new assessment that addresses the threats appropriate to the cloud. Most importantly, the security measures the utility takes will be to address the threats it faces, as well as the technologies it employs – not a one-size-fits-all set of measures that applies to all utilities in North America.

This is why, while I support the current SDT's efforts to draft CIP v7 and I am enjoying participating in some of their meetings, I don't want to see any further prescriptive versions of CIP, whether to address the cloud, wireless, renewables, or whatever. The next CIP version needs to be non-prescriptive. Otherwise, CIP will become the Monster that ate the North American Electric Utility Industry.

The views and opinions expressed here are my own and don't necessarily represent the views or opinions of Deloitte Advisory.

---

[i] "Innovation" is probably not the correct word here. I think of innovation as what led to these technologies being developed in the first place. A more appropriate title might have been "Is CIP Hindering Deployment of New Technologies?"

[ii] I believe it will be posted by NERC, but I don't think it is up yet. When it is posted, I will publish a link to it in the comment section below.

[iii] FERC ordered this definition be rewritten in Order 822, although their objections had nothing to do with the wording about 61850. The v7 SDT is now feverishly working on drafting the new definition, and I am finding the online discussions to be very interesting.

[iv] In addition, there was at least one blogger who was inflaming the situation by himself asking a lot of questions about what the standards meant, for example in this post.

[v] But certainly not all of them! See this post.

[vi] NERC has said that, once FERC issues their long-awaited Order to develop supply chain security standards, a new SDT will be appointed for that task. This is partly because the current team already has enough on their plate, and also because there will be somewhat different skills needed for this new task.

Tom Alrich at 9:16 PM

1 comment:

michaljohn July 13, 2016 at 5:18 AM

Thank you for posting the great content...I was looking for something like this...I found it quiet interesting, hopefully you will keep posting such blogs....Keep sharing.
Supply chain management services

Reply

Enter your comment...

‹ Home ›

View web version

About Me

Tom Alrich

View my complete profile