GridSME
SUBJECT MATTER EXPERTS

Q1 2020

The Reliable Wire

The Reliable Wire provides updates and insight on recent electric industry developments that may impact your operations or business strategy.

IN THIS ISSUE

- *CAISO Interconnection Cluster Best Practices*
- *Wildfire Mitigation Plan Independent Evaluation Q&A*
- *Transient Cyber Assets and Removable Media Management Tips*
- *EMS Network Applications - Quality Assessment Methods and Benefits*
- *NERC News, Events, and Upcoming Standard Enforcement Dates*

A Note Regarding The Times...

We hope this finds all of you healthy and safe during these strange and challenging times. Along with all of you, we've tried to keep up with all facets of the COVID-19. We are concerned for our staff, families, and clients, just like you are, and are taking steps to modify how we work in this sudden new reality. The health and safety of our people and clients is our top priority. With that said, your business cannot stand still while this thing runs its course, and neither can ours. We are working with this new challenge by using remote work technologies and capabilities already in place.

GridSME is prepared to ensure we continue to provide our clients with uninterrupted services during these challenging circumstances.

Effective March 13th, GridSME implemented a work-from-home plan. In-person meetings are being held virtually until further notice and the GridSecurity team is working from the SOC virtually. As always, GridSME is maintaining close communication regarding the work you've commissioned us to do. For those staff who are working at client sites, their protection and comfort level has been discussed with each of them individually and we will communicate any change in their engagement with you. We've encouraged them to discuss remote capabilities with you as well as best-practice protective measures they can take and follow your company's guidance.

Please let us know if there's any way we can help you during this outbreak and its unique challenges to keep your business moving forward. Working creatively to keep you supported will be our focus for the foreseeable future.

And remember, "this too shall pass." Let's take care of ourselves, families, friends, and communities in the meantime. And now more than ever, thank you to the men and women who work everyday to ensure we have reliable electricity in this country--especially the control center operators, field techs, and other folks who do not have the luxury for working from home during times like these. We all appreciate your hard work and dedication.

John Franzino
Chief Executive Officer

REGULATORY NEWS

Recent NERC News

- In response to the spread of COVID-19, NERC published a **Full Announcement** and a **Level 2 NERC Alert** regarding the associated health concerns. The Electricity Subsector Coordinating Council (ESCC) posted a resource guide call Assessing and Mitigating the Novel Coronavirus (COVID-19) – article **here**.
- NERC posted the presentations from 3/4/20 Reliability and Security Technical Committee Meeting here.
- On 3/3/20, NERC posted February 2020 NERC News (link **here**). The newsletter touched on many subjects including the on-going updates of the Align project, key dates, and the outcomes for the first board meeting of 2020.
- NERC posted the slides and steaming webinar for the Project 2019-03 – Cyber Security Supply Chain Risks webinar from 2/4. Read about this standard below.

Recent FERC News

On 3/18/20, FERC released **FERC, NERC Provide Industry Guidance to Ensure Grid Reliability Amid Potential Coronavirus Impacts**. From March 1, 2020 to December 31, 2020 the coronavirus will be an acceptable basis for non-compliance with personnel certification (PRC-003-2). Registered Entities should notify their Regional Entities of any periodic actions that will be missed from March 1, 2020 to July 31, 2020 this will be taken on a case-by-case basis. Regional Entities will postpone on-site audits, certification and other on-site activities at least until July 31, 2020.

Wildfire Mitigation Plans: Q&A with the Experts

Utility-caused wildfires have received immense scrutiny and attention in recent years. California's legislature has responded with a myriad of bills aimed at enhancing wildfire mitigation efforts and accountability. Today, the state's utilities are focusing their efforts on reviewing, bolstering, implementing, monitoring, and measuring their Wildfire Mitigation Plans (WMP). On one hand, the effort is a compliance exercise in response to California Senate Bill 901. But ultimately, well-managed utilities leverage this regulatory process as a tool to plan for and reduce the probability that their electrical equipment becomes the source of ignition for a catastrophic wildfire.

Given the heightened interest in WMPs and what utilities are doing to reduce risk and protect public safety, we sat down with GridSME's two subject matter experts (SMEs) on the topic, Danny Zaragoza and Tom Watson, for a quick Q&A to learn about the latest events and lessons learned.

1. What is a Wildfire Mitigation Plan and why is it so important for utilities to develop Wildfire Mitigation Plans?

Danny: Wildfire Mitigation Plans describe the programs and measures that utilities have developed to build a more reliable and resilient power grid to protect public safety, comply with the above stated goals, as applicable, and meet the requirements of the numerous elements as outlined in SB901.

SB 901 (Dodd. Wildfires.), which was signed by the Governor of California on September 21, 2018, requires electrical corporations, local publicly owned electric utilities, and electrical cooperatives to develop and submit Wildfire Mitigation Plans.

SB 901 amended Public Utilities Code section 8386(a) to read: Each electrical corporation shall construct, maintain, and operate its electrical lines and equipment in a manner that will minimize the risk of catastrophic wildfire posed by those electrical lines and equipment.

In addition, SB 901 amended Public Utilities Code section 8387(a) to read: Each local publicly owned electric utility and electrical cooperative shall construct, maintain, and operate its electrical lines and equipment in a manner that will minimize the risk of wildfire posed by those electrical lines and equipment.

The WMPs are the utilities telling all stakeholders how they are going to do that.

2. What are the most important components of a Wildfire Mitigation Plan?

Danny: There is no one single element of a Wildfire Mitigation Plan that I can say is the most important. There are about 19 different elements to PUC section 8386 or 8387 that utilities must address in their plans and all elements build upon each other to create a comprehensive and successful program. Each utility has different challenges, so each utility has to identify its highest risk(s) and prioritize where they begin or what mitigation measures to address first.

Just as important is the development of your plan to ensure it meets the regulatory compliance requirements and address all elements of PUC section 8386 (IOUs) or 8387 (POUs).

In my experience, the foundational program should be built on situational awareness tools such as the weather network, cameras, sensors, etc. A utility's weather network provides the ability to forecast upcoming critical fire weather events, monitor real-time operating conditions in order to execute any type of safety work practices, up to and including a Public Safety Power Shutoff (PSPS), and forecast when the critical weather conditions will subside in order to return to normal operations. A robust weather network provides the ability to monitor microclimates to predict high risk situations (e.g., localized wind events) impacting the power grid. To effectively do this, utilities need to install a sufficient number of weather stations to have the ability to monitor system conditions in areas where their electrical facilities are at risk during high fire risk conditions.

3. In California, is it accurate to say Senate Bill 901 and Public Utilities Code section 8386 (IOUs) and 8387 (specific to the POUs) are the key regulatory drivers requiring IOUs and POUs to develop and implement a WMP?

Tom: Yes, SB 901 amended 8386 and 8387 and it is the applicable code section the state's utilities are focused on right now.

3(a). What parts of SB 901 and PUC 8386/8387 are most challenging to comply with? What are the common gaps you see in utilities' WMPs relative to the regulatory requirements?

Tom: As Danny mentioned, each utility has its own unique challenges. So, this will vary. Certainly, proper vegetation and tree management are paramount and because living vegetation is constantly growing, this represents an ongoing, continuous effort.

One key piece of the WMP activities that we haven't mentioned yet is records management. So that is one gap I see that is potentially underappreciated. I think the utilities are finding this to be a huge effort. Certainly, a bigger challenge than initially thought and in some senses is an evolving target as lessons are learned through actual events. It's one thing to have a great program and comply with the code, but to be able to comprehensively demonstrate it to an outside party after-the-fact, that's a whole other undertaking.

Danny: I wouldn't say that any particular area is more challenging than another. Making one requirement a higher priority than another discredits the importance and challenge in meeting all of the requirements. All are important and all are essential to the success of your program.

4. Can you share some WMP best practices and ways utilities can foster a culture of safety, compliance, and proactive risk management?

Tom: A culture of safety and compliance must start at the top – with the company's executive leadership providing clear direction and expectations, as well as support.

Danny: I agree, Tom. Public and employee safety and, in particular, wildfire safety, must be a top priority set by the executive leadership and must be a year-round priority. A corporate culture must exist where people are always thinking, "safety first and how do I mitigate the risk for a catastrophic wildfire?" For example, when a wire comes down in the middle of winter, the question has to be asked, "Why did that wire come down? And what happens if it comes down during a red flag warning?" The mindset should always be to minimize the risk of system failures and the culture must be top-to-bottom throughout an organization.

5. Dwight Eisenhower once said, "Plans are useless, but planning is indispensable." How applicable is that idea to WMPs? Is it really the planning process that is key to a successful Wildfire Mitigation program? What can utilities do to plan and proactively mitigate wildfire risks?

Tom: While the process is certainly key, having a documented, comprehensive plan is critical to successful wildfire mitigation efforts, particularly with such wide-ranging compliance requirements. In this case, that Plan document is very valuable.

Danny: The planning process is key to the WMP as it establishes a roadmap for how a utility will execute their plans. Additionally, it will hold the entities accountable for executing on their plans as described within the WMP in order to achieve the goal of, "constructing, maintaining, and operating its electrical lines and equipment in a manner that minimizes the risk of catastrophic wildfires posed by its electrical lines and equipment".

GRIDSECURITY NEWS

It's 2020, Have You Verified Your TCAs and RM Yet?

Now that CIP-003-7 is enforceable, we just wanted to take a moment to issue a friendly public service announcement (PSA) to ensure that all field techs, vendors, and O&M providers are following Generator Owner (GO) approved CIP-003 Transient Cyber Assets and Removeable Media (TCA/RM) policies and procedures. If I had a crystal ball, I would bet that the vast majority of CIP self-reports in 2020 are due to TCA/RM plan violations. After all, the Regional Entities have already established that they expect self-reports each and every time a TCA or RM is used without following the documented CIP-003 plans.

This PSA focuses on what evidence Responsible Entities need to have—if you need help Understanding & Managing Transient Cyber Assets, check out **this webinar**.

In accordance with NERC's **CIP Evidence Request Tool v4.0**, as part of the initial Level 1 evidence request process for CIP low impact facilities, in addition to applicable policies and plans, Responsible Entities will need to provide the following evidence for TCAs.

Transient Cyber Assets Managed by the Responsible Entity or by a Party Other Than the Responsible Entity						
TCA ID	TCA Management Type	Description of Use	Managed by	Asset ID Where Used	For on-demand, Cyber Asset ID of BCA/PCA or Low Impact BES Cyber System ID Accessed	For on-demand Date and Time of Access

Then, according to the Level 2 data request, a sampling of technical TCA evidence is required.

For TCAs managed in an ongoing, on-demand, or combination of both fashion, provide evidence that each TCA has:

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

For TCAs managed in an on-demand fashion, provide evidence that each TCA has performed:

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.
- Review to determine whether additional mitigation was necessary and was implemented prior to connecting.

For RM, the Level 1 request is a little less detailed:

Removable Media		
Removable Media ID	Asset ID Where Used	Description of Use

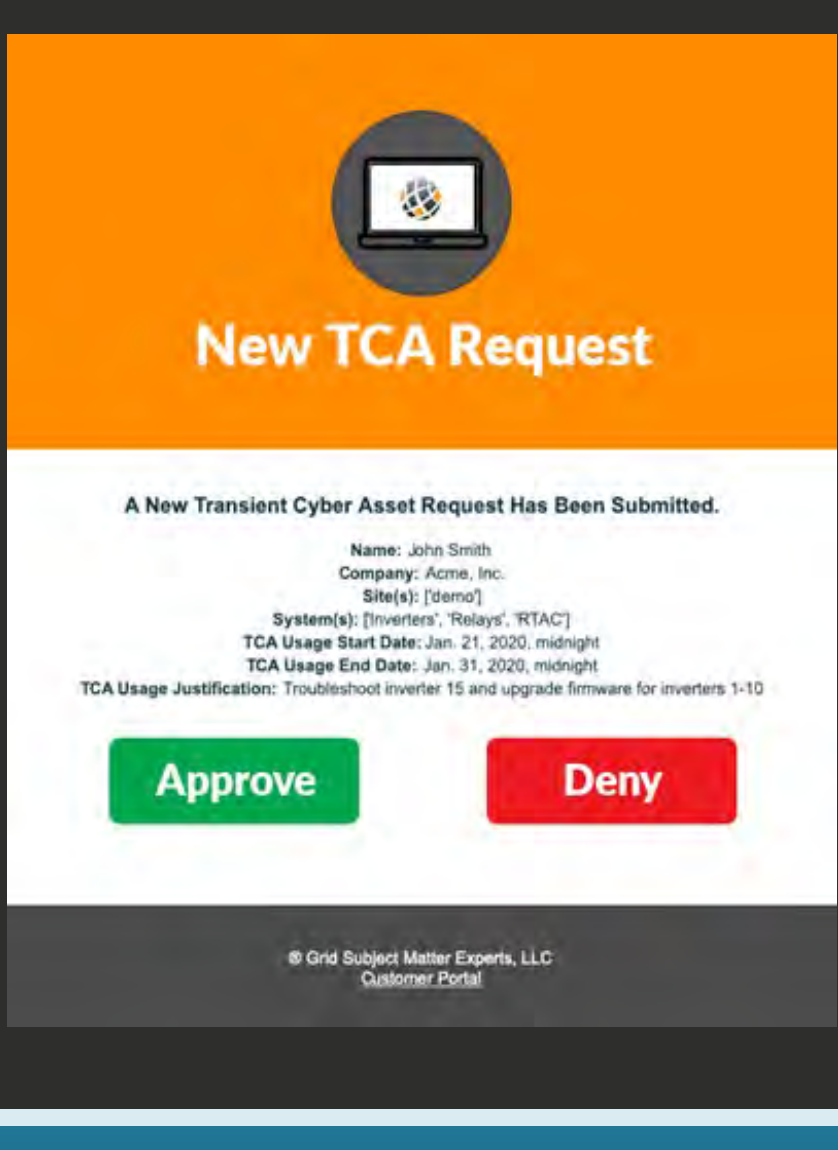
For each location where Removable Media is utilized, Responsible Entities will need to provide the following as part of the Level 2 request:

1. Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and
2. Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

When it comes to the new TCA and RM requirements for CIP low impact facilities, no news is not good news—if you haven't had any requests to use TCAs or RM yet, I wouldn't assume that means no one has used them. Be proactive and ask your personnel the question explicitly.

And remember, if you use GridSME for managed compliance services (MCS) and/or managed security services (MSS), your field techs, vendors, and operators must coordinate and communicate TCA/RM usage with us. If you do not, we have no way to help you ensure compliance with the CIP-003-7/8 requirements!

For MSS clients, you have been provided SOPs to share with your field techs, vendors, and operators. Once the request is submitted, those designated as approvers will receive the email below. You can review all past, pending, and active TCA/RM requests via the GridSME Customer Portal, as well as the associated evidence for retention.



ENGINEERING AND INTERCONNECTION NEWS

CAISO QC13 Application Window - Tips and Best Practices

Attention New Resource Developers! The 2020 CAISO Cluster 13 Application Window for Generator Interconnection Request Applications starts April 1st and ends April 15th. Please keep in mind that this application window may change in light of COVID-19. GridSME will share any changes to the timing of this application window as soon as it is announced.

As the Cluster Application Window approaches, we want to share the lessons GridSME has learned over the years. In helping our clients navigate the CAISO Cluster process, our consultants have accumulated countless scars, bumps, and bruises along the way – lessons in what not to do as much as what to do.

This topic reminds us of the cynical definition of an "expert." Someone once defined an expert as the person that learned all the wrong ways to do something. This topic also reminds us of the Thomas Edison quote, "I haven't failed -- I've just found 10,000 ways that won't work." Such is the case with the CAISO Cluster process.

First, here are a couple of basics about the CAISO Cluster 13 request window:

- For a project to move to the validation phase, all elements of the application request must be submitted and deemed complete by April 15, 2020.
- If the application request does not meet all elements of the criteria by the close of April 15th, it will be deemed incomplete with NO opportunity to cure and the application request will not be included in the cluster study.

So, what are the do's and don'ts of the annual CAISO Cluster Application Window? Here are some best practices, tips, and tricks GridSME has learned along the way.

1. We highly recommend making your first project submission early in the 15-day window (e.g., April 1st to the 3rd). Do not wait until April 15th, or even the 13th, to make your first submission. Get your submission in early in the window. This gives you a chance to cure any deficient elements before April 15th. We cannot stress this enough. You must have a complete submittal to CAISO by close of business April 15th.
2. We cannot stress enough the importance of a thorough quality assurance/quality control (QA/QC) review in the interconnection submission package review process.
   a. Many deficiencies requiring a "cure" are simple form and file data variances. So be sure all data matches across the various forms. We recommend someone other than the preparer "reconcilie" the information on all the various forms and technical data to make sure it is consistent.
   b. The facility modeling files and data require close attention and oversight, as well.
3. Firm up the idea of your project early and complement missing information that is not required for the Cluster Application Window acceptance during the scoping meeting, which usually takes place in May or June.
4. Make sure your project names will be acceptable to CAISO. Some project names are not allowed so get your name approved early on before you start populating forms and preparing files with a name that will not be accepted by CAISO.
5. Acquire the Secretary of State Certificate and Proof of Signatory Authorization for the entity entering the CAISO Cluster 13 Application Window.

If you have any questions during the process or need any assistance in preparing your request package, do not hesitate to contact us. We're happy to help.

GRID TECHNOLOGY NEWS

EMS Network Applications - Quality Assessment Methods and Benefits

Understanding how to get the most value and highest quality data from your EMS Network Applications is critical to system reliability and market performance. GridSME's VP of Grid Technology Services, Brett Wangen, wrote a whitepaper detailing ideas and best practices on how to get the most from these analytical tools. The following is a high-level summary – you can find **Brett's entire whitepaper on our website (link here)**.

So how do you know how well your EMS applications measure up? How do you know if you are doing enough to ensure they are providing your organization with strong reliability and market performance? In a nutshell, it is critical that you establish metrics that define "strong performance" and measure the quality of your EMS Network Applications. At a minimum, these metrics must address model accuracy, application availability, and application accuracy.

Model Accuracy
The network model is the foundation of all EMS network applications. Key considerations include how to establish the "right" sized external network model, how to properly represent load so that the model can be used for studies, and finally how to validate the model by comparing model performance with actual system events.

Application Solution Availability
Application solution availability simply measures what percentage of time the EMS network application solutions and data are available to end users. These suggestions include methods for tracking solution availability and ways to promote operator and engineer awareness of solution quality and status.

Application Accuracy
Application solution availability metrics help show that solutions are available to end users. But how do you know if those solutions have a high degree of accuracy? The full white paper presents ideas to promote awareness of errors that exist in Real-time and study network application solutions and gives specific ideas that can be easily implemented in any control center.

What's Next?
Building appropriate metrics for your organization takes some thought and planning but can provide a great degree of value in the long run. Getting leadership, operations, EMS teams, and end users all on the same page with a common vision for use of EMS Network Applications will remove obstacles that otherwise may impede progress. The whitepaper lays out practical steps that can be taken to begin taking steps to improving your organization's use of EMS Network Applications.

If GridSME can be of any value to your organization as you go down this path, please let us know.

UPCOMING EVENTS

Due to COVID-19, these events are subject to change. Check host website to confirm.

April

April 8, 2020
Texas RE Spring Standards and Compliance Workshop
(Webinar registration **here**)

April 16, 2020
FERC Commission Meeting
(Webinar registration **here**)

April 21, 2020
ReliabilityFirst Open Compliance Call
(Webinar information **here**)

May

May 21, 2020
WECC Compliance Open Webinar
(Webinar information **here**)

May 28, 2020
Texas RE NERC Standards Review Forum
(Webinar registration **here**)

UPCOMING EFFECTIVE DATES

Reliability Standard	Title	Effective Date
CIP-003-7	Cyber Security - Security Management Controls	January 1, 2020 (Newly Effective)
PRC-026-1 (R2-R4)	Relay Performance During Stable Power Swings	January 1, 2020 (Newly Effective)
CIP-003-8	Cyber Security - Security Management Controls	April 1, 2020
CIP-005-6	Cyber Security - Electronic Security Perimeter(s)	July 1, 2020
CIP-010-3	Cyber Security - Configuration Change Management	July 1, 2020
CIP-013-1	Cyber Security - Supply Chain Risk Management	July 1, 2020
PER-006-1	Specific Training for Personnel	October 1, 2020
PRC-027-1	Coordination of Protection Systems for Performing During Faults	October 1, 2020

ABOUT GRIDSME

GridSME is a results-focused consulting firm, representing a diverse group of talented electric industry experts ready to help guide our clients through the fast-changing landscape of the industry.

Our clients make up a very diverse group, ranging from small renewable energy companies to large regional utilities and everything in-between—our subject matter experts (SME) provide pragmatic solutions on a wide range of operational, technical, and business challenges, leveraging industry best-practice knowledge gleaned over the many decades of collective experience amassed by our team. While GridSME's core competencies lie in NERC compliance, cybersecurity, electrical engineering, and grid technology, we provide a number of additional grid support services to our clients, such as electricity market expertise, operations training, and IT services.

**Please let us know if you want more information on anything contained in this issue.
We appreciate your feedback on The Reliable Wire.**
customerservice@gridsme.com