DER Cybersecurity Implications

IEEE® P1815.2 (DNP3) vs IEEE Std 2030.5™ vs SunSpec® Modbus®– Friends or Foes?

Tuesday, November 18, 2025, 3:30 - 5:00 PM ET

The workshop notes and recording are offered at no charge to our members and non-members.

Post Event Release

Recording | Slide Deck | Speaker Bios

(See below for Chat Notes and Reference Information)

Description

The DNP Users Group (DNP-UG) has launched a series of informative workshops, open to the public, with industry leaders addressing important topics relevant to our members and the industry. Workshops will generally be followed by related tutorials and training courses for our members.

With the deployment of Distributed Energy Resource (DER) systems on the rise, developing robust solutions to secure their communications infrastructure is becoming increasingly critical. This workshop built on our previous session by focusing on the cybersecurity implications of the three protocols specified in IEEE Std 1547™–2018 for the Local DER Communication Interface: DNP3, IEEE Std 2030.5, and SunSpec Modbus.

Following the panel presentations, the floor was opened for questions and discussion.

Speakers

- John McDonald, Panel Chair, JDM Associates
- Ben Ealey, EPRI
- Grant Gilchrist, Tesco Automation
- Robby Simpson, Enetrics
- Anthony Ciccozzi, Eaton

DNP-UG Information

To receive periodic updates and news, click here: **Enroll**

The DNP-UG is a non-profit group with the mission to actively support measures to improve interoperability and cybersecurity in DNP systems by developing technologies and standards, implementing a conformance program, and providing education to the industry. Utilities and vendors benefit significantly with reduced project and development costs and risks due to a broadly adopted, well managed, highly interoperable and secure protocol (if implemented).

To participate and support our work please join us! Click here: **Membership Guide** or **Join**

For more information click here: **dnp.org home**

Follow us on **LinkedIn**

For assistance or more information, contact Sara at **membership@dnp.org**

Workshop Chat Notes

1. **Does TLS address all cybersecurity aspects of DNP3, or in some cases is TLS not sufficient, and is it necessary to use SAv5 (in addition)?**
    - Transport Layer Security (TLS) is a security control that can be applied at one layer; other security controls can be applied at other layers alongside TLS to develop defense-in-depth. The authentication model built into DNP3 SAv5, which is carried forward into and expanded in DNP3-SL, is applied at a higher layer, closer to the DNP3 application, so that individual critical exchanges can be authenticated between controlling station and outstation, even if security controls at lower layers are circumvented or broken. DNP3 SAv5 and DNP3-SL can both be used over a TLS connection to establish defense-in-depth. Unlike TLS, DNP3 SAv5 and DNP3-SL can both be used over serial connections.
    - There are many possible approaches. Each has strengths and limitations. The benefit of sticking to recommended practices or features embedded in a standard is the expectation of a standardized way of doing things across a wide range of devices, rather than having to bolt on your own solution. A system might have specific requirements that make a particular approach beneficial for it.
2. **Does SunSpec Modbus support timestamping as well?**
    - Modbus and SunSpec Modbus profiles do not have time stamping.
    - In many applications, the Sequence of Events (SoE) or historian capabilities are used to achieve timestamping. This is done by the controller itself (not the protocol). This is usually used for utility and industrial applications (due to cost) and for investigating events/incidents.
    - TLS does prevent repeat attacks through MAC sequence numbers if you are trying to avoid that with time stamping.
3. **Who will own/manage/operate a PKI for IEEE 1815.2 (DNP3)?**
    - The PKI for DNP3-SL can be local to the Utility control center or can connect to corporate PKI.
4. **It has been suggested by some that MACsec might be a better choice than TLS for industrial control / OT because it is more static. Are any of the speakers aware that MACsec is being used instead of TLS?**
    - MACSec is designed for layer 2, while TLS operates higher up in the OSI model. Protecting a high-speed layer 2 protocol, such as IEC 61850-GOOSE, is a good option.

For more distributed applications, TLS should provide sufficient security and support more standard network implementations, such as routing.

5. **Any plans or efforts to consider future PQC options from the DER network protocols? Will it include hybrid or pure PQC?**
    - DNP3 is adding post-quantum crypto algorithms for DNP3-SL.
    - We use standard crypto algorithms, nothing we design ourselves. There is a selection of "must be supported" crypto options, and the protocol is extensible with crypto agility to add new crypto algorithms in the future. You configure the system to use the algorithm that works for your system and the current state of "what is considered secure".
6. I wanted to learn about integrating these protocols with the Common Information Model and other standards. I have worked on CIM-DNP3 integration, but not others.
    - In 1547.2, there is a mapping of the 1547 capabilities to the CIM.
    - The IEEE 2030.5 information model was based on the CIM, so mapping should be relatively straightforward.
    - All the protocols are harmonized to the 1547 functions which has made that mapping easier. Because each has had to implement the functions in 1547 to be included in 1547, IEEE 1547 has encouraged harmonization. They are also all mapped to IEC 61850-7-420.
    - PNNL developed CIM-2030.5 service that does mapping and data exchange. https://github.com/GRIDAPPSD/gridappsd-2030_5
    - Similarly for DNP3: https://github.com/GRIDAPPSD/gridappsd-dnp3/tree/develop

Note: DNP-UG has recently renamed Secure Authentication Version 6 (SAv6) to DNP3 Security Layer (DNP3-SL).

Additional Panelist FAQs

1. **Is cyber security automatically included for DNP, SunSpec Modbus, and IEEE 2030.5?**
    - No, it depends on the protocol. You may need to take an action. When we talk about cybersecurity in DER communications, it's important to recognize that not all protocols include security by default. For example, DNP. While a secure version of DNP3 exists, it must be explicitly specified and implemented. Similarly, SunSpec Modbus builds on the Modbus protocol, which was designed for trusted environments and does not include native encryption or authentication. Cybersecurity for SunSpec Modbus must be layered on externally through network protections and device hardening.

      In contrast, IEEE 2030.5 stands apart by requiring Transport Layer Security and Public Key Infrastructure as part of its core specification.

      So among the three, only IEEE 2030.5 includes cybersecurity automatically when implemented according to the standard. This distinction is critical when considering how to define and test cybersecurity outside of IEEE 1547.
2. **Is there alignment on what security to use for the two protocols that do not automatically implement them?**
    - For the two protocols that do not include cybersecurity by default, DNP3 and SunSpec Modbus, the industry is making steady progress toward alignment, though a universally accepted approach has yet to emerge. There is no one-size-fits-all solution; rather, these protocols offer tools that can be selectively applied to secure communications based on system architecture and operational context.

      In the case of DNP3, several options have been identified by Subgroup 4 of the IEEE 1547 revision effort. Secure Authentication Version 5 (SAV5) is currently available, and DNP3-SL is being reviewed by the IEEE Standards Association. However, many utilities rely on alternative mechanisms such as VPNs or TLS to secure DNP3 traffic, depending on their infrastructure and risk posture.

      For SunSpec Modbus, the SunSpec Alliance has taken a proactive role by developing the SunSpec Modbus TLS Profile, which provides a standardized approach to securing

Modbus communications. That said, compensating controls may also be appropriate in certain deployment scenarios. For example, when Modbus is used between a DER system and a gateway located within a secure facility, and the utility or owner can ensure that traffic remains internal, additional security measures may not be necessary. Conversely, if the DER interface is exposed to public networks, more robust protections must be implemented.

This variability underscores the importance of defining cybersecurity requirements outside of IEEE 1547, allowing for flexibility while ensuring that appropriate safeguards are in place for each protocol and use case.

3. **Why isn't DNP3-SL backward-compatible with SAv5?**
    - SAv5 was integrated into the application layer of DNP3, which turned out to be quite a barrier for vendors to implement. DNP3 is already very state-oriented because it was built with a request-response-confirm structure to ensure reliability. Then to add on another set of state machines for security made things very complex, especially the possible challenge-reply mechanism for each message. The DNP Cyber-Security Task Force felt that to encourage more vendors to implement the protocol, the challenge-reply mechanism should only be used when setting up an association; and the whole mechanism should be pulled out into a separate session layer. Taking these steps also permits this new layer to be implemented with other protocols, if they choose to do so. But adding all of these changes of course makes it non-backward-compatible.
4. **Why do we need a separate protocol for AMP? SAv5 had a method to download keys; wasn't that good enough?**
    - AMP does a lot more than just manage keys, but it also provides a fundamentally different approach to keys than SAv5 used. In SAv5, the authority and controlling station, or a configuration tool, just assigned keys to devices. That meant that usually a human had to type them in somewhere. In DNP3-SL and AMP, the devices generate their own keys and never show them to a human being. This is inherently more secure. The primary job of AMP is then just to authorize or "approve" communications between two devices. This job ends up requiring that the authority manage certificates for the whole network, and do it over the same mixed IP and serial networks as DNP3-SL. So the best way to do that is with an entirely separate protocol. In the meantime, DNP3-SL can still be deployed to secure the DNP3 data stream without waiting for those capabilities.

5. **Why does IEEE 2030.5 not define an access control mechanism?**
    - An example mechanism is given in the standard.
    - Recognize there are many types: role-based, resource-based, policy-based, ACLs, etc.
    - Recognize there are existing IP-based protocols and did not want to reinvent the wheel.
    - Unlike typical power and energy applications where assets are owned by utility, unclear if interoperability is needed for access control when owner, operator, and utility may all be different (and who would define?).
6. **Why are the cybersecurity features of IEEE 2030.5 mandatory?**
    - Default secure principle
    - Defense in depth (can always add more)
    - No longer viewed as burdensome
    - From device perspective, can never guarantee will not be routed, etc. — importance of end-to-end security
    - IEEE 2030.5 is cross-domain by nature and owner, operator, and utility may all be different
7. **What are some challenges when trying to upgrade legacy systems using Modbus?**
    - Legacy devices may not support modern Modbus TCP/IP
    - Legacy devices may have hardware constraints that limits its ability to handle certain types of cryptography.
    - The networks that host legacy devices may not have been setup with a focus on security.
8. **If there are already so many working legacy systems, why do we need to update security standards?**
    - Legacy systems, once isolated or air-gapped, now interact with networked systems to enable real-time operational analytics, predictive maintenance, and remote monitoring.

Workshop Reference Information

1. NIST Common Functions for Smart Inverters, v4, is available here.
2. PNNL GRIDAPPSD CIM-2030.5 service is available here.
3. PNNL GRIDAPPSD CIM-DNP3 service is available here.