IEEE SCC21 1547 Working Group Meetings, Feb 2021 (virtual)

SAND2021-1781PE

P1547.3 Draft Guide for Cybersecurity Distributed Energy Resources Interconnected with Electric Power Systems

Subgroup 1 Update

Feb 23, 2021

Jay Johnson, Sandia National Laboratories

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

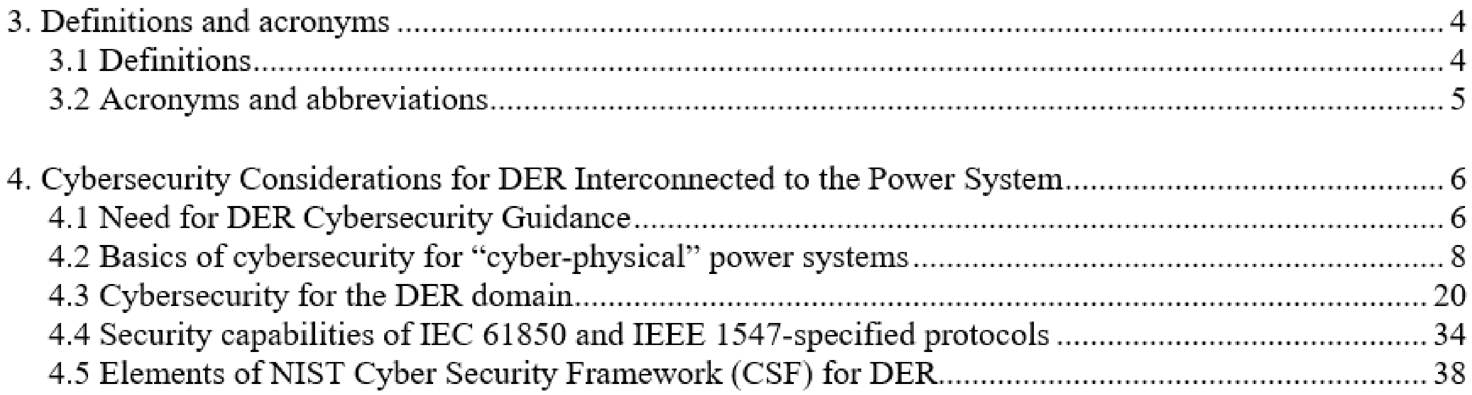
IEEE
Advancing Technology for Humanity

1547.3 “Justification” Subgroup

- IEEE 1547.3 is a Guide:
  - “Standards” when the standard specifies mandatory requirements.
  - “Recommended Practice” when the standard provides recommendations.
  - ***“Guide” when the standard furnishes information.***
- This Subgroup was tasked with providing information through answering the following questions:
  - Why was this guide created?
  - Who should read the guide and why should they care?
  - What are the most important topic areas?
  - What informative material could help non-experts understand the cybersecurity issues for DER?
- In general, this informative content has been reviewed several times.
- The questions now are:
  - What should or could be added?
  - What should be better explained?
  - What might be pared down?

Structure of our discussion today

- Brief overview of proforma sections 1 - 3
- Review of informative contents in Section 4
- Assessment of previous comments
- Additional questions on issues for IEEE 1547.3
- Q&A



1.2 Purpose

Includes an overview of the contents of the guide

- Section 4: Cybersecurity considerations for DER interconnections:
  - Need for cybersecurity guidance
  - Basics of cybersecurity for "cyber-physical" power systems, including cybersecurity resilience, security by design, IT vs OT, risk assessment, and cybersecurity standards and best practices
  - Cybersecurity issues for the DER domain
  - Security for the IEEE 1547 interoperability protocols
  - Elements of the NIST cybersecurity framework
- Section 5: Technical cybersecurity recommendations, including:
  - Engineering and cybersecurity recommendations for different DER stakeholders
  - Risk assessment techniques
  - System engineering of networks and data
  - Access control, including role-based access control of different types of data
  - Security for data in transit and at rest
  - Security management
  - Coping with and recovering from security events
- Section 6: Recommendations for different DER stakeholders, including:
  - Manufacturers of DER systems
  - Integrators and installers of DER systems
  - Testing personnel
  - DER owner/operators
  - DER facility ICT management
  - DER security managers
  - DER maintenance personnel
  - DER operator coping actions during a security event
  - DER recovery actions after a security event
- Section 7: Testing and commissioning of cybersecurity

1.4 Audience

- This Guide is designed to be used by individuals with different areas of expertise and experience with DER and cybersecurity.
- Clause 4 is designed to be informative and provides general background information on DER communications and cybersecurity.
- Clause 5 defines the cybersecurity technical recommendations for DER systems and Clause 6 outlines the roles and responsibilities for stakeholders within this ecosystem.
- Clause 7 lists cybersecurity testing recommendations for equipment and systems. The annexes provide additional information on standards and best practices.

2. Normative References

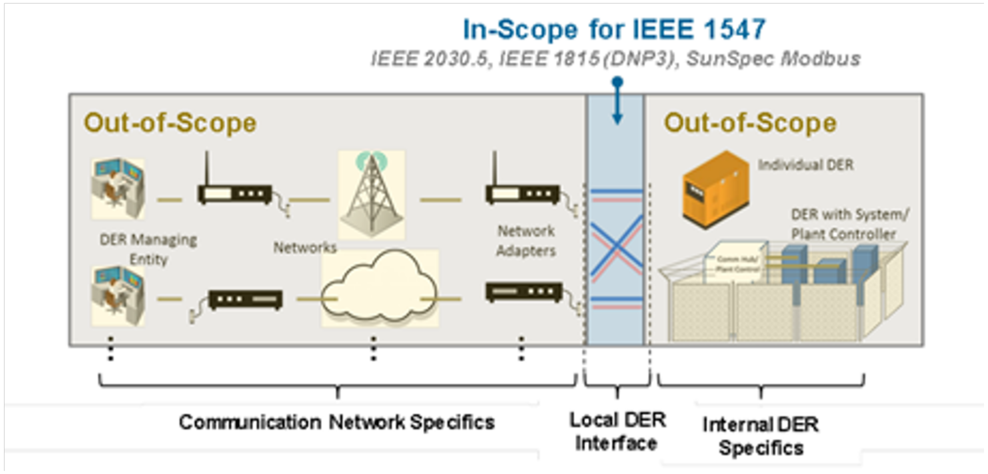
- Only documents referenced in the Guide should be added.
  - IEEE Std 1547.2™, IEEE xxx.
  - IEC 62351 series,
  - ISO/IEC 27000 series,
  - IEC 62443 series,
  - UL 2900-2 series,
  - NISTIR 7628
  - NIST cybersecurity framework and other cybersecurity guidelines
  - IEEE 1686 revision
  - IEEE C37.240 revision
  - IETF, Internet cybersecurity standards

3. Definitions and acronyms

- Definitions
  - **gateway**: A network entity (software or hardware) that interfaces between networks that use different protocols, or are of different, potentially incompatible, technology.
  - **production test**: A test conducted on every unit of equipment prior to shipment.
  - **type test:** Test of one or more devices made to a certain design to demonstrate that the design meets certain specifications. Syn: **design test**.
  - …
- Acronyms and abbreviations
  - 1.5 pages included currently.
  - Please add to the list as new acronyms are added to the document.

Clause 4: Cybersecurity Considerations for DER Interconnected to the Power System

- **4.1 Need for DER cybersecurity guidance**
  - Why did we create the IEEE 1574.3 guide?
    - Short answer, IEEE 1547-2018 requires interoperability but includes no guidance on cybersecurity. IEEE 1547.3 is intended to fill that gap.
  - Argument for end-to-end cybersecurity requirements beyond the scope of IEEE 1547-2018.
  - **4.1.1 Cybersecurity policies, procedures, and technologies**
    - Importance of having good policies and clear procedures, in addition to cybersecurity technologies.

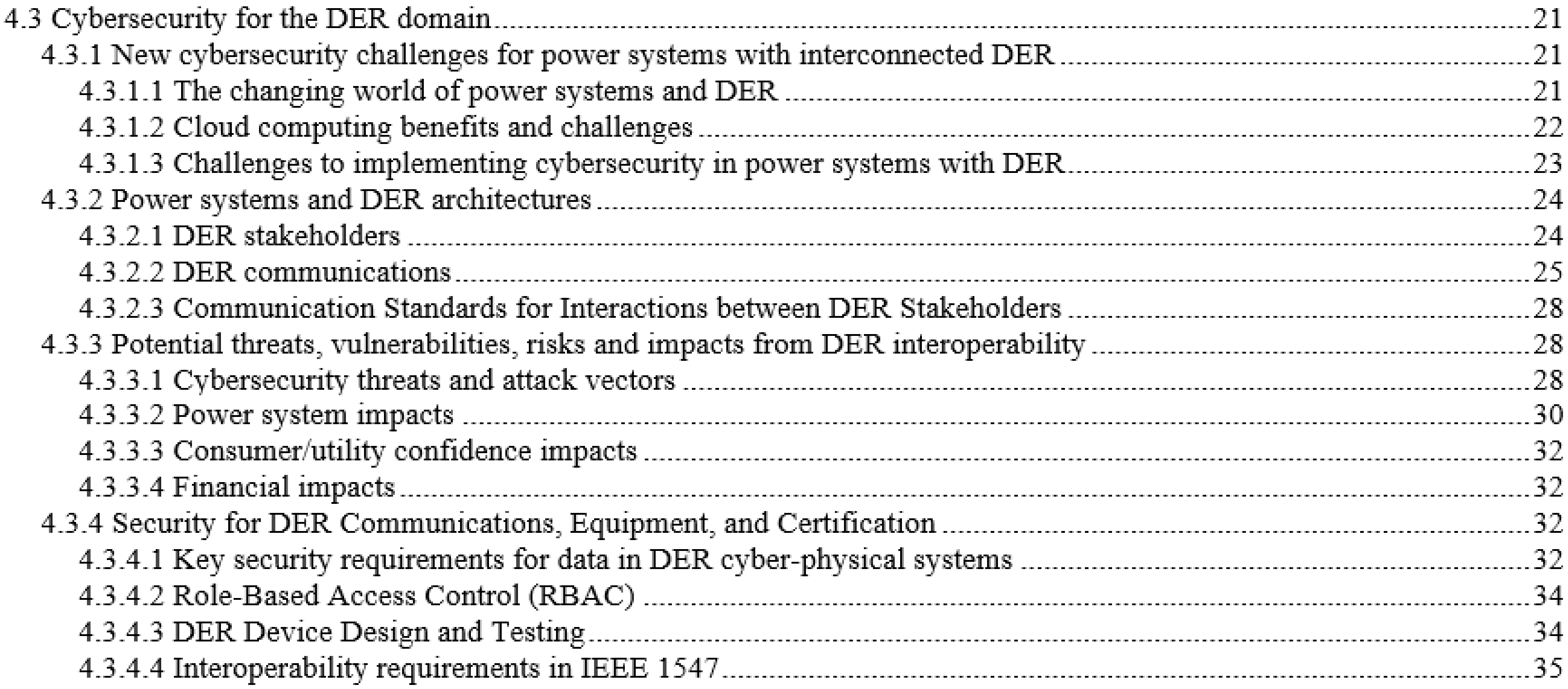


IEEE 1547 Scope for Interoperability Requirements.

4.2 Basics of cybersecurity for power systems applications

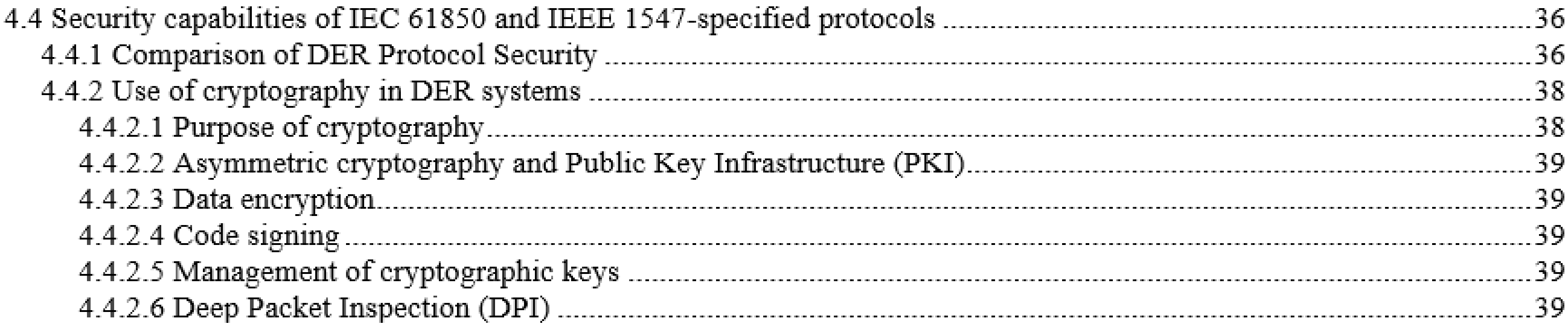
- 4.2 Basics of cybersecurity for power systems applications
  - 4.2.1 Five cybersecurity concepts for smart grid resilience
    - 4.2.1.1 **Resilience** should be the overall strategy for ensuring business continuity
    - 4.2.1.2 **Security by Design** is the most effective approach to security
    - 4.2.1.3 **IT and OT** are similar but different
    - 4.2.1.4 **Risk assessment**, risk mitigation, and continuous update of processes are fundamental to improving security
    - 4.2.1.5 **Cybersecurity standards and best practice guidelines** for energy OT environments should be used to support the risk management process and establish security programs and policies
  - 4.2.2 Cybersecurity as a continuous process
  - 4.2.3 Rationale for defense-in-depth and end-to-end cybersecurity
  - 4.2.4 Risk assessment and mitigation
    - 4.2.4.1 General
    - 4.2.4.2 Risk assessment
  - 4.2.5 Managing cybersecurity: security levels and maturity scoring
- *Should Section 4.2.4 Risk Assessment become a higher-level section? There is a proposal to make the risk assessment section its own Clause. It’s 6 pages long now.*

Section 4.3 – Application of the cybersecurity principles to DER



- *Should Role-Based Access Control (RBAC) be expanded since it is critical to even normal operations of DER?*
- *Section 4.3.4.4 seems out of place – any suggestions?*

Section 4.4 – Security Capabilities of IEEE 1547 and IEC 61850 Protocols



- *Should the protocol security comparison table be modified? If so, how?*
- *Should Section 4.4.2 be moved to section 4.3 since it is not specific to the DER protocols? Or should it have its own section?*
- *Should more on cryptographic key management be added, rather than just a reference to IEC 62351-9?*

4.4.1 Comparison of DER Protocol Security

DER Communications	IEC 61850	IEEE 1815 (DNP3)	IEEE 2030.5	SunSpec Modbus
Associated Protocol Cybersecurity Requirements	IEC 62351 series	IEEE 1815 Secure Authentication v5 (being update to v6) (based on IEC 62351-5) available for both DNP serial and DNP LAN/WAN	IEEE 2030.5 + CSIP	Modbus TCP via a TLS wrapper. No security available for Modbus serial.
Application Layer Security (Authentication)	Authentication by IEC 62351-4 (MMS, XMPP), IEC 62351-6 (GOOSE)	Authentication, based on IEC 62351-5	Authenticated encryption of client identity in client/server framework. No authentication of individual users within client facilities.	No
Transport Layer Security (Authentication)	Authentication by IEC 62351-3 with specific requirements for TLS 1.2 or 1.3	Authentication via TLS 1.2 for TCP	Authentication via TLS 1.2 for TCP	Authentication only for Modbus TCP, TLS 1.2/1.3 for Modbus TCP
Authorization Supported (See guidance in Section 5.4)	Authorization by Role-based access control by type of service and by specific data objects, as defined in IEC 61850-90-19, based on IEC 62351-8.	Authorization in v6 by AMP which provides an optional centralized authorization mechanism in which the connectivity and RBAC roles permitted for each pair of devices in the system is approved via a centralized system called an Authority. Optionally, Access Control Lists (ACLs) may be configured on the outstation to enforce permissions at a per-point level.	Yes, access control of clients by white-listing in servers. Access control by type of service (read, write, control).	No
Confidentiality	Yes, IEC 62351-4: Available at both Application Layer and Transport Layer	Available at Application Layer in SAv6 and at Transport Layer	Mandatory encryption of client identity	Only at Transport Layer with TLS wrapper.
Integrity Protection and Tamper Detection	Yes, via IEC 62351-3 (TLS) and IEC 62351-4 (hash)	Yes, by v5 or v6 (hashes)	Yes, How?	No
Non-Repudiation	Not natively but through logging and security event management, e.g. Syslog and IEC 62351-14.			
Availability	Primarily through engineering means, e.g. IEC 62351-7 and comm loss notification			
Man-in-the-Middle Protection	Yes, via IEC 62351-3 and IEC 62351-4	Yes, by TLS	If TLS is end-to-end	If TLS is end-to-end
Masquerade Protection	Yes, via IEC 62351-3 and IEC 62351-4	Yes, by SAv5 or SAv6	Using white listing in server	No
Replay Protection	Yes, via IEC 62351-3 and IEC 62351-4	Yes, by SAv5 or SAv6	Yes	No
Cryptographic Key Management and Distribution	IEC 62351-9: Public Key Infrastructure (PKI). Use X.509 digital certificates for authentication.	Public Key Infrastructure (PKI). Use X.509 digital certificates for authentication	CSIP document, Public Key Infrastructure (PKI). Use X.509 digital certificates for authentication	Public Key Infrastructure (PKI). Use X.509 digital certificates for authentication for Modbus-TCP
Symmetric Keys	IEC 62351-9: Secret keys, Group Domain of Interpretation (GDOI) for groups of devices	Secret keys, pre-shared keys in v5 (v6 uses a Low-Entropy Shared Secret (LESS) for enrollment)	Secret keys	No
Certificate Revocation Management	IEC 62351-9: Certificate Revocation List (CRL), Online Certificate Status Protocol (OCSP)	Certificate revocation handled at Master Station.	Certificates do not expire. CRLs and OCSP are prohibited in IEEE 2030.5/CSIP.	No
Encryption Technologies	TLS_DH_DSS_WITH_AES_256_SHA as mandatory, but others are permitted	Multiple TLS cipher suites are permitted, but TLS_RSA_WITH_AES_128_SHA shall be supported at minimum	TLS_ECDHE_ECDSA with AES_128_CCM_8	None
Security Management	IEC 62351-9: Enrolment of devices. Encryption technologies can be renegotiated	IEEE 1815 update (in process)	Encryption technologies fixed for devices	None
Testing and Certification of Cybersecurity	IEC 62351-100-1 for IEC 62351-3; IEC 62351-100-6 for IEC 62351-6 (in process)	DNP Users Group and authorized test labs	Yes, SunSpec certifies the results from authorized Test Labs	Yes, SunSpec certifies devices.

Section 4.5 – Elements of NIST Cyber Security Framework (CSF) for DER

- Stakeholder groups
  - Grid Operators
  - DER Facility Owners
  - DER Aggregators/Energy Service Providers
  - DER Vendors/Service Provider
- NIST CSF Elements
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- Links to Annex E

- *Should this section be expanded to include the CSF aspects, such as Trustworthiness?*

IEEE Advancing Technology for Humanity

Previous Feedback to Justification Group

- Too long (*currently 35 pages – is that too long?*)
- Too detailed (*now most "gory" details are in annexes*)
- Too many standards references; sea of acronyms
- Can Clause 4 become multiple clauses?
- Must link Clause 4 items to Clause 5/6 recommendations (*Difficult since Clause 4 is informative, and Clauses 5/6 are recommendations*).
- What can/should be cut? (*Or added or clarified.*)
- Table 2 is massive… (*2 pages out of 35?? See previous pages*)
- Plus many detailed comments (*currently resolved – pending more comments)*
- Need to "trim the fat" from the document and then polish the content (*What is "fat" and what is useful information for someone?)*
- ***So, should we revisit the purpose of this section as informative about cybersecurity for DER? – This is a Guide document, after all.***

Specific Questions for IEEE 1547.3

- In addition to discussing the previous feedback issues, the following issues need discussion:
  - IEEE 1547.3 is a Guide. However, it currently includes both Informative material (Section 4) and Recommendations (Sections 5, 6, and probably 7). **Should the PAR be revised to make this a Recommended Practices document?**
  - Cybersecurity technologies and probably regulatory requirements will change over the next few years (e.g. block chain, 5G networks, cloud computing, NERC CIPs reaching down to aggregated DER, Bulk power IBR plants, etc.) **Should these futuristic issues be addressed, and if so, how?**
  - Although this document now 85 pages long, plus 100 pages of Annexes, only a small number of people have been actively involved. **How do we get additional cybersecurity experts and DER experts involved? Can we ask other SDOs, such as the IEC, to actively support this effort?**

Current Feedback??

Need an interim Subgroup 1 leader

- I’ll be on paternity leave from the end of May through mid-July.
- Volunteers?