MESA-DER Workshops: Cybersecurity for MESA-DER (IEEE 1815.2)

June 13, 2023

Frances Cleveland – fcleve@xanthus-consulting.com
Andrew West - andrew.west@ieee.org

Contents

1. Introduction to MESA Alliance and MESA-DER
2. Cybersecurity Concepts
3. NIST Cybersecurity Framework
4. IEEE 1547.3 Cybersecurity Guidelines and Recommendations
5. Cybersecurity for the DNP3 Protocol
6. Questions – *Feel free to use the Chat for Questions during the presentation, but they can only be answered at the end – and Yes, the slides will be shared*

1. Introduction to MESA Alliance, MESA-DER, and Integration into IEEE 1815.2

The **Modular Energy System Architecture (MESA) Standards Alliance** is an industry association comprised of electric utilities and technology suppliers dedicated to providing interoperable communications for DER systems and DER devices.

MESA Membership

AREVON
AVANTUS
AUSTIN ENERGY
CAMUS
DOOSAN
Doosan GridTech
DUKE ENERGY
HYOSUNG
LA DWP
Los Angeles Department of Water & Power
nextracker
NUVATION ENERGY
Pacific Northwest NATIONAL LABORATORY
QualityLogic
RRC
RRC POWER & ENERGY, LLC
Salt River Project
SDGE
A Sempra Energy utility
SMUD
Powering forward. Together.
SNOHOMISH COUNTY PUD PUBLIC UTILITY DISTRICT NO. 1
SOUTHERN CALIFORNIA EDISON
stem
Trimark ASSOCIATES, INC.

MESA Members 2022-23

A full listed of members and partners is available at www.mesastandards.org/members

MESA's Mission

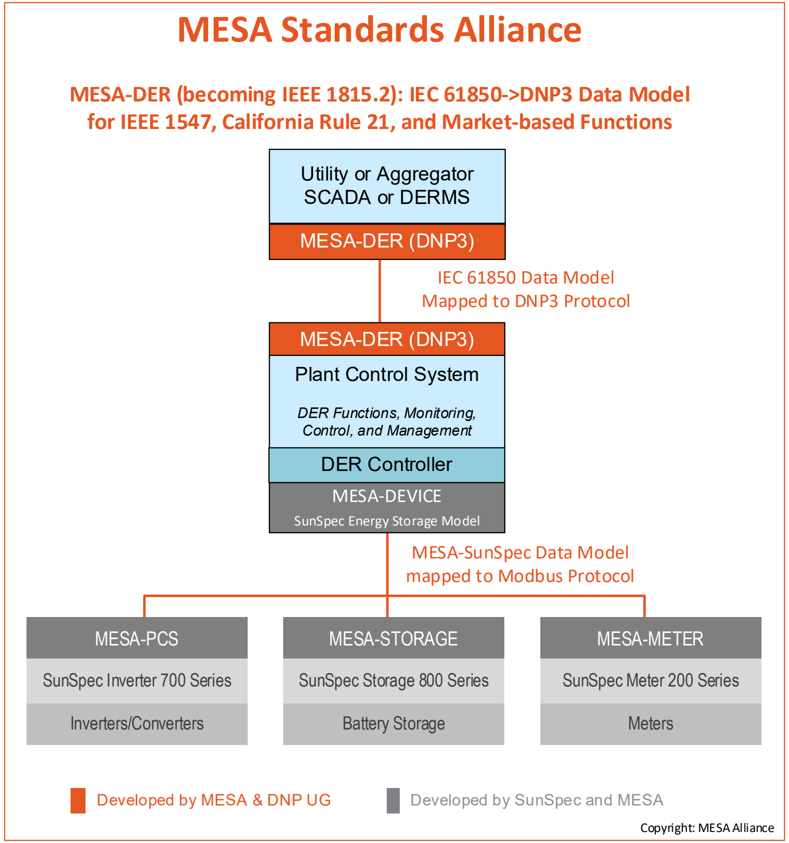
MESA's mission is to accelerate the interconnection of Distributed Energy Resources (DER) through the development of interoperable communication specifications, based on well-established standards that meet the specific needs of utilities and DER integrators.

MESA-DER's focus is on using DNP3 with IEC 61850-7-420 data models for interoperability to meet IEEE 1547, IEEE 2800, and energy storage requirements

MESA specifications support safe, affordable, and scalable DER communications with the following benefits:

	UTILITIES	DEVELOPERS	INDUSTRY
Meet all DER interoperability requirements for IEEE 1547 DER interconnection and interoperability standard	✓	✓	✓
Use international communication standards, including IEEE 1815 (DNP3), IEC 61850, and SunSpec Modbus	✓	✓	✓
Streamline deployments and meet customer timelines	✓	✓	✓
Focus resources on implementing market-based functions for improved efficiency and revenue streams	✓	✓	✓
Reduce costs of technology development and deployment	✓	✓	
Reduce risk by enabling supplier flexibility	✓	✓	
Simplify long-term maintenance and system upgrades	✓	✓	
Efficiently scale DER deployments	✓	✓	
Reduce training and compliance testing costs	✓	✓	✓
Provide products designed for integration with other MESA-compliant products		✓	✓
Increase the array of available partners for projects			✓

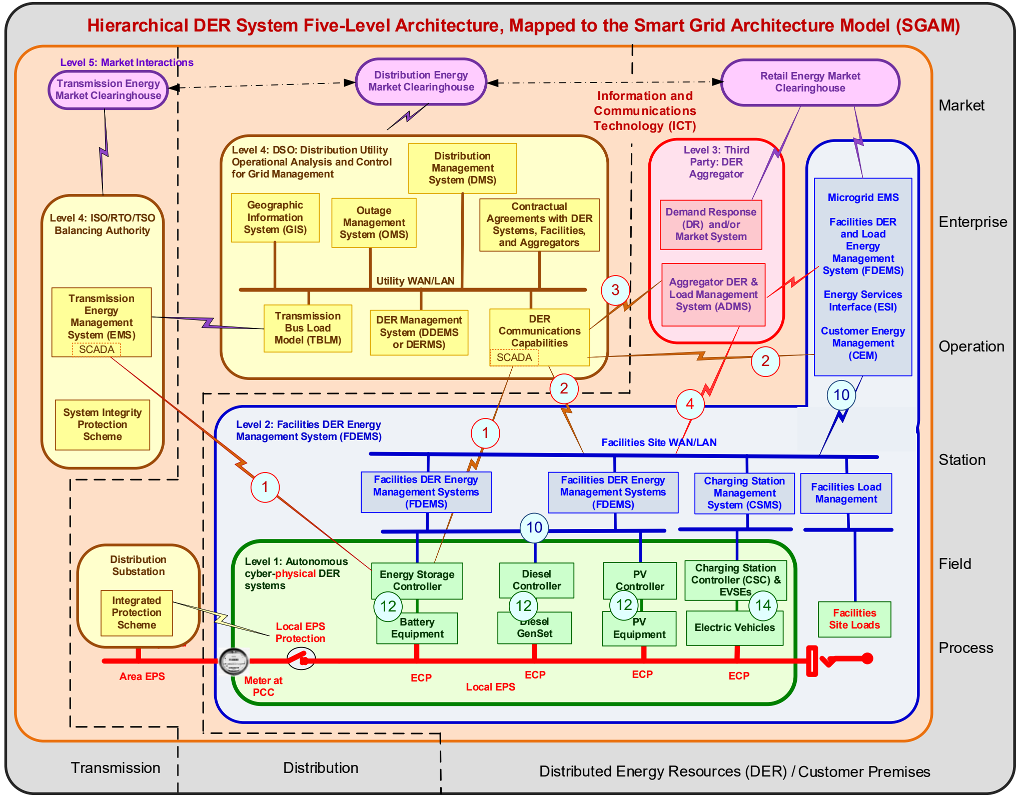
Overview of MESA Specifications


MESA Standards Alliance
MESA-DER (becoming IEEE 1815.2): IEC 61850->DNP3 Data Model for IEEE 1547, California Rule 21, and Market-based Functions
Utility or Aggregator SCADA or DERMS
MESA-DER (DNP3)
IEC 61850 Data Model Mapped to DNP3 Protocol
MESA-DER (DNP3)
Plant Control System
DER Functions, Monitoring, Control, and Management
DER Controller
MESA-DEVICE
SunSpec Energy Storage Model
MESA-SunSpec Data Model mapped to Modbus Protocol
MESA-PCS
SunSpec Inverter 700 Series
Inverters/Converters
MESA-STORAGE
SunSpec Storage 800 Series
Battery Storage
MESA-METER
SunSpec Meter 200 Series
Meters
Developed by MESA & DNP UG
Developed by SunSpec and MESA
Copyright: MESA Alliance

- **MESA-DER Specifications: IEC 61850 Data Model Mapped to DNP3**
  - ❖ IEEE 1547 Mandatory Functions
  - ❖ Operational Management of DER Plant and/or Facility
  - ❖ Monitoring and Control of DER units
  - ❖ Power Market Functions
  - ❖ Scheduling of Functions
  - ❖ Priority Management of Multiple Co-Existing Functions

- **MESA-Device Specifications:**
  SunSpec Models providing Modbus for inverters and battery storage devices
  - ❖ MESA-PCS: Power Conversion Systems
  - ❖ MESA-Storage: Batteries
  - ❖ MESA-Meter: Meters

MESA-DER Focus on Interface #1, #2, #4, & #10 (DNP3 for SCADA) and MESA-Device/SunSpec on Interface #12 (Modbus for Storage Devices)



Hierarchical DER System Five-Level Architecture, Mapped to the Smart Grid Architecture Model (SGAM)
Level 5: Market Interactions
Transmission Energy Market Clearinghouse
Distribution Energy Market Clearinghouse
Retail Energy Market Clearinghouse
Information and Communications Technology (ICT)
Market
Level 4: DSO: Distribution Utility Operational Analysis and Control for Grid Management
Distribution Management System (DMS)
Geographic Information System (GIS)
Outage Management System (OMS)
Contractual Agreements with DER Systems, Facilities, and Aggregators
Utility WAN/LAN
Transmission Bus Load Model (TBLM)
DER Management System (DDEMS or DERMS)
DER Communications Capabilities
SCADA
Level 4: ISO/RTO/TSO Balancing Authority
Transmission Energy Management System (EMS)
SCADA
System Integrity Protection Scheme
Level 3: Third Party: DER Aggregator
Demand Response (DR) and/or Market System
Aggregator DER & Load Management System (ADMS)
Microgrid EMS
Facilities DER and Load Energy Management System (FDEMS)
Energy Services Interface (ESI)
Customer Energy Management (CEM)
Enterprise
Operation
3
2
2
4
10
1
1
Level 2: Facilities DER Energy Management System (FDEMS)
Facilities Site WAN/LAN
Facilities DER Energy Management Systems (FDEMS)
Facilities DER Energy Management Systems (FDEMS)
Charging Station Management System (CSMS)
Facilities Load Management
Station
10
Level 1: Autonomous cyber-physical DER systems
Energy Storage Controller
Diesel Controller
PV Controller
Charging Station Controller (CSC) & EVSEs
12
12
12
14
Battery Equipment
Diesel GenSet
PV Equipment
Electric Vehicles
Facilities Site Loads
Field
Distribution Substation
Integrated Protection Scheme
Local EPS Protection
Area EPS
Meter at PCC
ECP
ECP
ECP
ECP
Local EPS
Process
Transmission
Distribution
Distributed Energy Resources (DER) / Customer Premises

Copyright Xanthus Consulting International

MESA-DER Specification

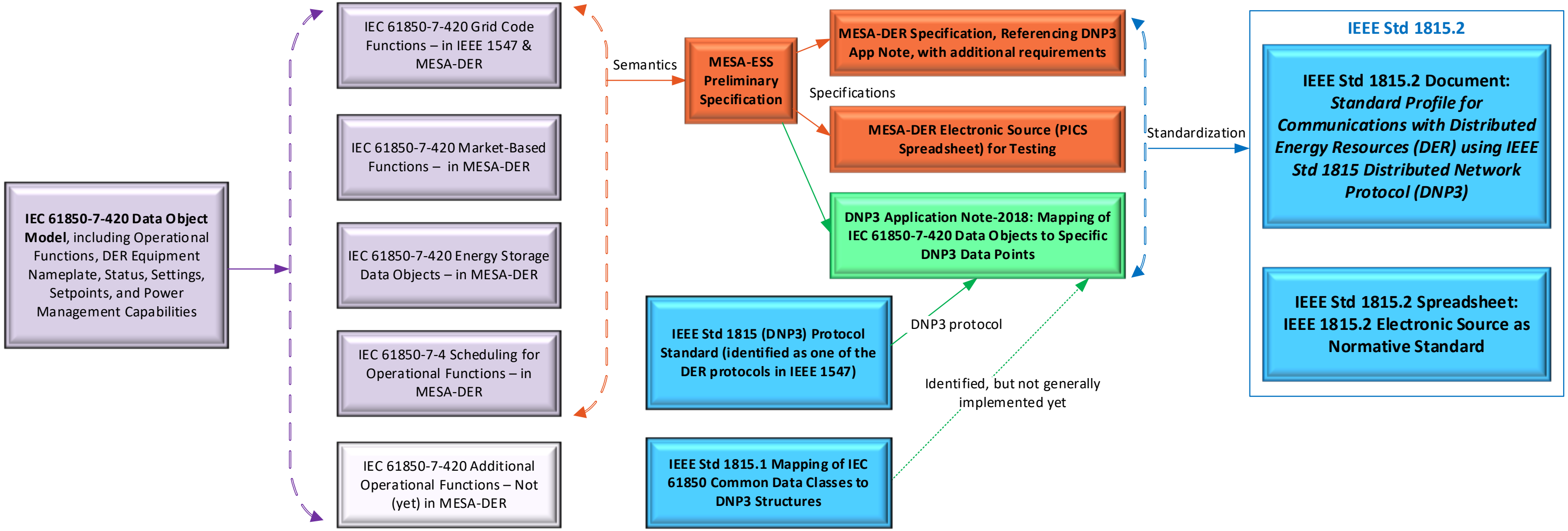
The MESA-DER Specification provides *standardized* and *interoperable* communications language using the IEC 61850 information Model mapped to specific DNP3 (IEEE 1815) data points, thus ensuring both utilities and DER vendors have precisely the same understanding of the meaning of these data points.

This MESA-DER Specification meets the IEEE 1547 functional and interoperability requirements and is specified in IEEE 1547.1 for the interoperability testing of DNP3. MESA-DER also supports many additional functions, such as AGC, Generation Following, Load Following, Set Active Power (base load), Peak Power Limiting, Operational Reserve, and Coordinated Charge/Discharge for storage.

MESA-DER can be used for interactions among the various "stakeholders", including the SCADA system (distribution and/or transmission) operator, the balancing authority, DER facility energy management systems, interactions between DERs within a facility, response to power market requirements, inter-DER markets (e.g., generation following of a PV plant by a storage plant), virtual DER plants, microgrids, etc.).

Status 2023: Integration into IEEE 1815.2

IEC 61850-7-420 Semantics, MESA-DER Specification, MESA-DER Spreadsheet, and DNP3 Application Note Integration into IEEE 1815.2



IEC 61850-7-420 Data Object Model, including Operational Functions, DER Equipment Nameplate, Status, Settings, Setpoints, and Power Management Capabilities

IEC 61850-7-420 Grid Code Functions – in IEEE 1547 & MESA-DER

IEC 61850-7-420 Market-Based Functions – in MESA-DER

IEC 61850-7-420 Energy Storage Data Objects – in MESA-DER

IEC 61850-7-4 Scheduling for Operational Functions – in MESA-DER

IEC 61850-7-420 Additional Operational Functions – Not (yet) in MESA-DER

Semantics

MESA-ESS Preliminary Specification

Specifications

MESA-DER Specification, Referencing DNP3 App Note, with additional requirements

MESA-DER Electronic Source (PICS Spreadsheet) for Testing

DNP3 Application Note-2018: Mapping of IEC 61850-7-420 Data Objects to Specific DNP3 Data Points

IEEE Std 1815 (DNP3) Protocol Standard (identified as one of the DER protocols in IEEE 1547)

DNP3 protocol

Identified, but not generally implemented yet

IEEE Std 1815.1 Mapping of IEC 61850 Common Data Classes to DNP3 Structures

Standardization

IEEE Std 1815.2

IEEE Std 1815.2 Document: *Standard Profile for Communications with Distributed Energy Resources (DER) using IEEE Std 1815 Distributed Network Protocol (DNP3)*

IEEE Std 1815.2 Spreadsheet: IEEE 1815.2 Electronic Source as Normative Standard

- IEEE PSCC P15 WG, with major support by MESA and the DNP User Group is developing the draft IEEE 1815.2
- Draft is being reviewed by the P15 WG
- Next Step is Balloting – probably around September 2023

MESA-DER: 21 Functions

IEEE 1547.1 Functions (Via NRTL Test Tools)

- Low/High Voltage Ride-Through
- Low/High Frequency Ride-Through
- Dynamic Volt-Watt Function
- Frequency-Watt Function (Droop)
- Limit Active Power Function
- Volt-Watt Function
- Constant VArs Function
- Fixed Power Factor Function
- Volt-VAr Control Function
- Watt-VAr Function
- Dynamic Reactive Current Support

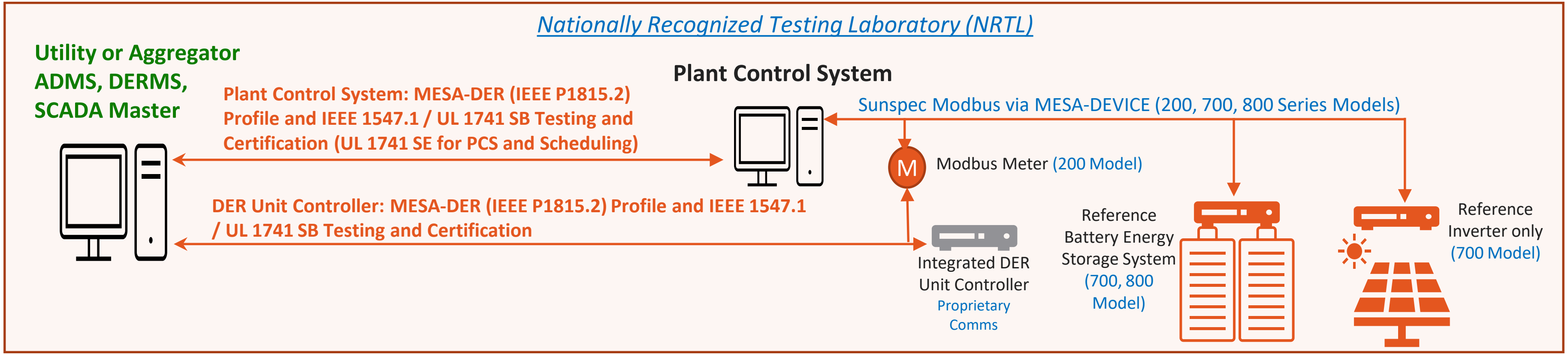
Additional MESA Functions

- Charge/Discharge Function (Set Active Power)
- Coordinated Charge/Discharge Function
- Active Power Response Function #1 (Peak Power Limiting)
- Active Power Response Function #2 (Generation Following)
- Active Power Response Function #3 (Load Following)
- Automatic Generation Control (AGC) Function
- Active Power Smoothing Function
- Frequency-Watt “Curve” Function (Artificial Inertia, Fast Frequency Response, etc.)
- Power Factor Correction Function
- Pricing Function
- Scheduling

MESA-DER (IEEE P1815.2): UL Managed Testing of Communications plus Functions for Plant Control Systems & DER Unit Controllers

Plant Control Systems will use lab specified “Reference” Battery Energy Storage System, Inverter, and Meter which are MESA-Device compliant

DER Unit Controller is tested at the NRTL or at the facility



Nationally Recognized Testing Laboratory (NRTL)
Utility or Aggregator ADMS, DERMS, SCADA Master
Plant Control System: MESA-DER (IEEE P1815.2) Profile and IEEE 1547.1 / UL 1741 SB Testing and Certification (UL 1741 SE for PCS and Scheduling)
Plant Control System
Sunspec Modbus via MESA-DEVICE (200, 700, 800 Series Models)
M
Modbus Meter (200 Model)
DER Unit Controller: MESA-DER (IEEE P1815.2) Profile and IEEE 1547.1 / UL 1741 SB Testing and Certification
Integrated DER Unit Controller
Proprietary Comms
Reference Battery Energy Storage System (700, 800 Model)
Reference Inverter only (700 Model)

- Triangle Microworks, Inc. (TMW)
- QualityLogic, Inc. (QL)
- Nationally Recognized Testing Laboratory (NRTL)
- Underwriters Laboratories (UL)

- *Note: Reference BESS, inverter, and meter will be MESA DEVICE Compliant. Translation may be used if SunSpec Modbus 200, 700 & 800 Models are not currently available for the device at the time of testing.*
- *Since Plant Control Systems may communicate with many inverter types with different protocols, we require they at minimum communicate via SunSpec Modbus/MESA-Device internal to the “plant”.*

Section 2

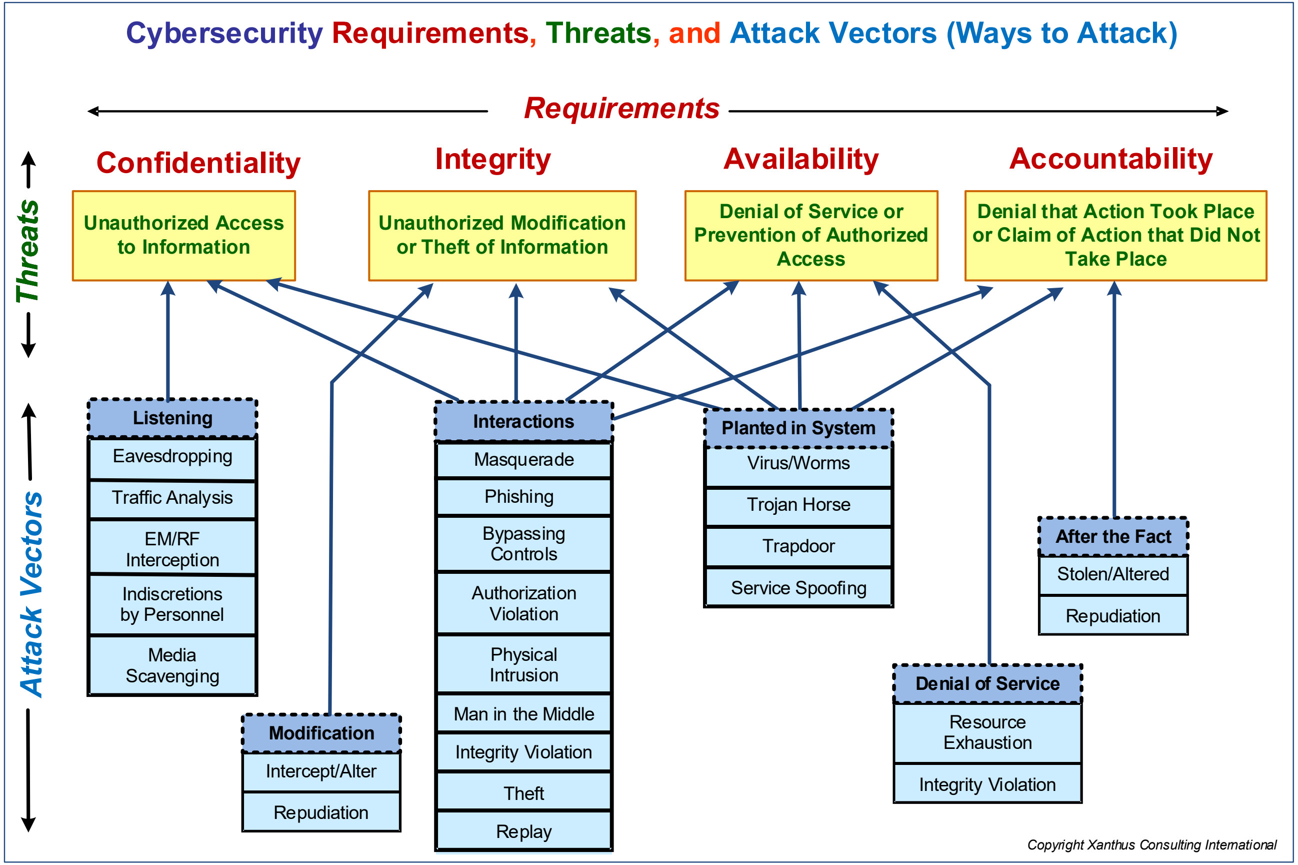
Cybersecurity Concepts

Security Requirements, Threats to those Requirements, Types of Attacks, and Mitigations of the Possible Threats

Five Key Cybersecurity Concepts

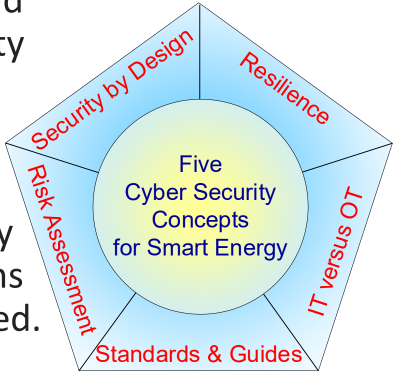
Cybersecurity Standards for Cyber-Physical Systems, including DER

Cybersecurity Requirements, Threats, and Attacks



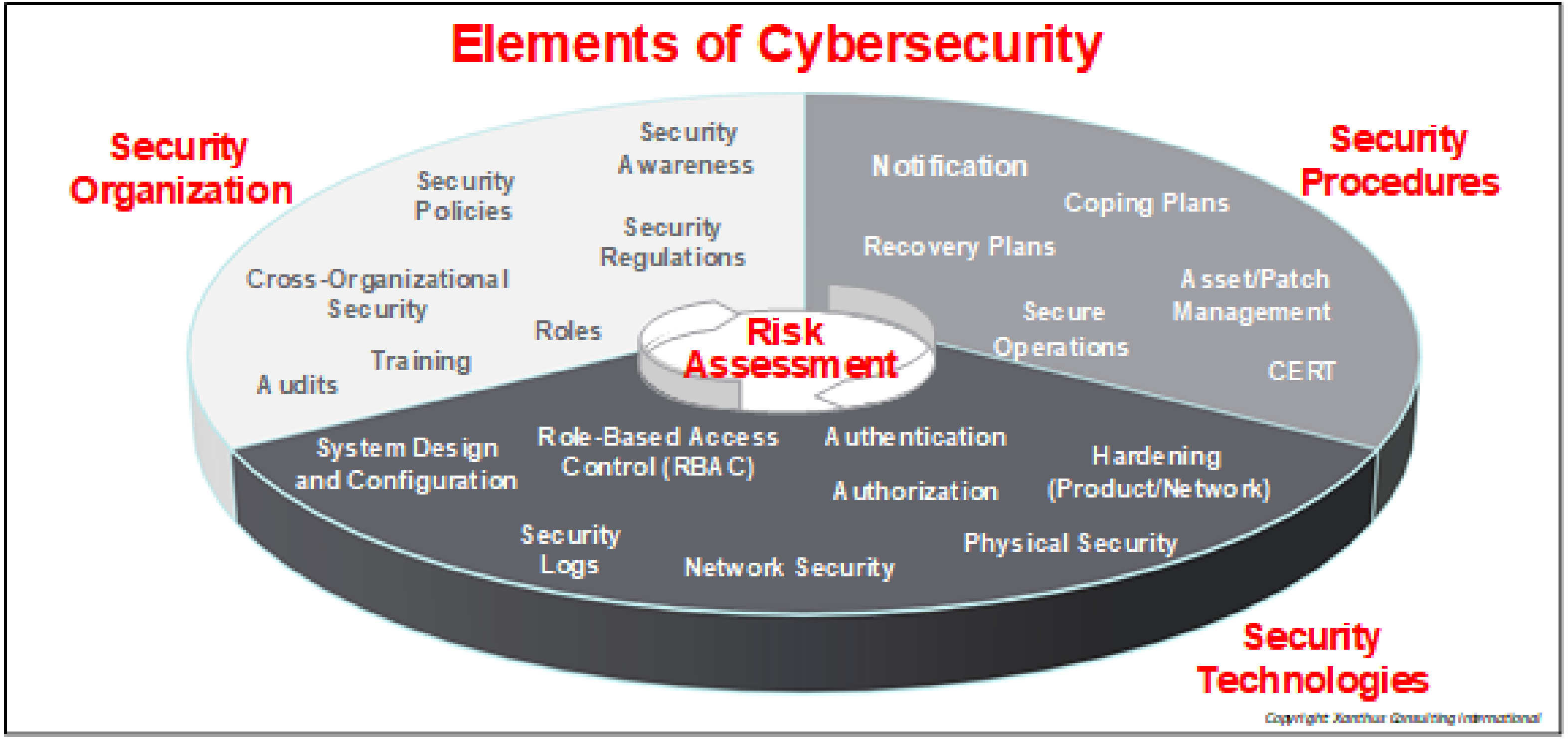
Five Key Concepts for DER Cybersecurity

- **Concept #1.** **Resilience** should be the overall strategy for ensuring business continuity: When focusing on resilience in general, organizations must consider safety, security, and reliability of the processes and the delivery of their services. Resilience includes security measures that can mitigate impacts, not only before incidents (identify & prevent), but also during such incidents (detect & respond) and after incidents have been resolved (recover).
- **Concept #2.** **Security by Design** is the most cost-effective approach to security: Security is vital for all critical infrastructures and should be designed into systems and operations from the beginning, rather than being applied after the systems have been implemented.
- **Concept #3.** **IT and OT are Similar but Different**: Technologies in Operational environments (called OT in this document) have many differing security constraints and requirements from Informational Technologies (IT) environments.
- **Concept #4.** **Risk Assessment, Risk Mitigation, and Continuous Update of Processes** are fundamental to improving security: Based on an organization’s business requirements, its security risk exposure must be determined (human safety, physical, functional, environmental, financial, societal, reputational) for all its business processes.
- **Concept #5.** **Cyber Security Standards and Best Practice Guidelines** for energy OT environments should be used to support the risk management process and establish security programs and policies: at the right time.



Copyright: Xanthus Consulting International

Risk Assessment as Key Cybersecurity Requirement



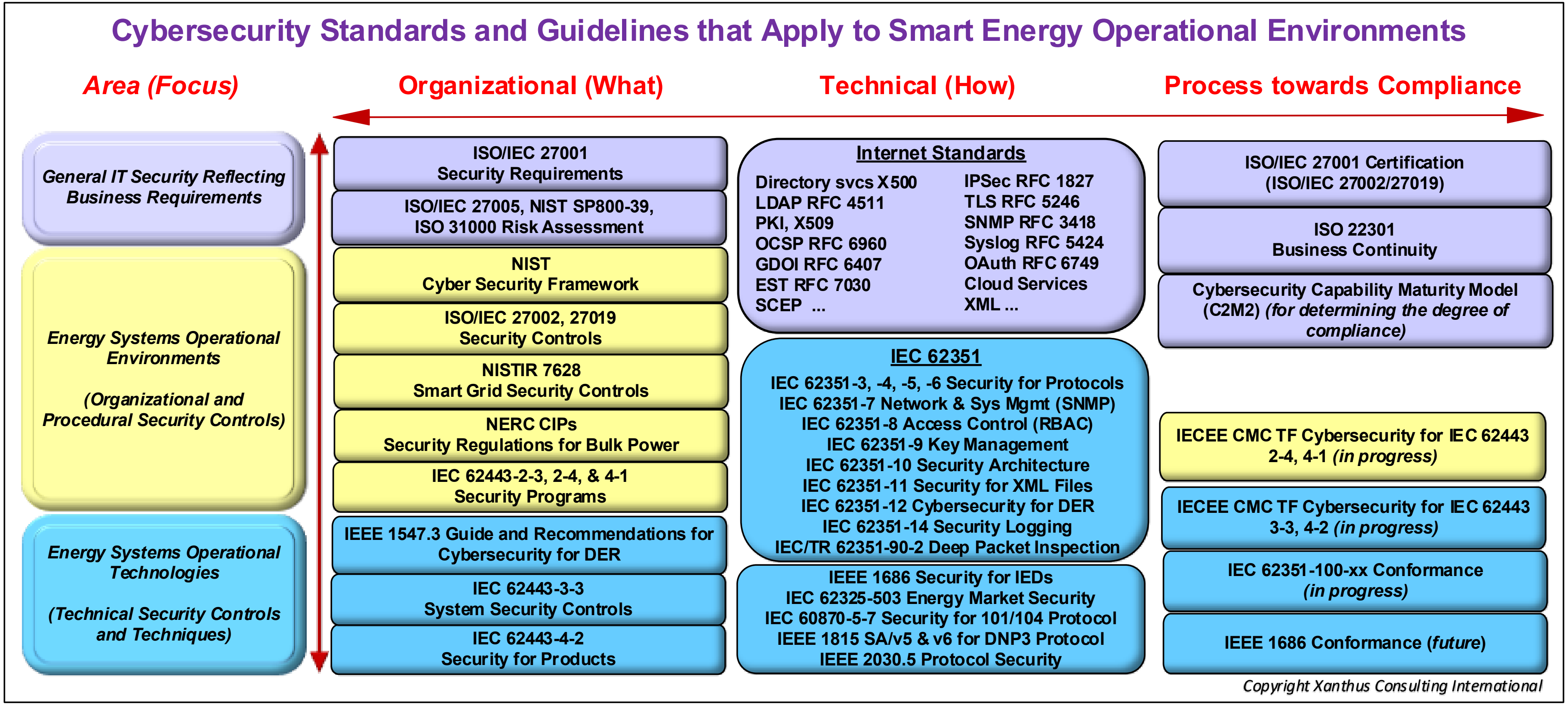
Section 3

Cybersecurity Standards and Guidelines

“What” standards and “How” standards

Who’s doing what

Cybersecurity Standards: What and How



Cybersecurity Standards and Guidelines that Apply to Smart Energy Operational Environments

Area (Focus)

Organizational (What)

Technical (How)

Process towards Compliance

General IT Security Reflecting Business Requirements

Energy Systems Operational Environments

(Organizational and Procedural Security Controls)

Energy Systems Operational Technologies

(Technical Security Controls and Techniques)

ISO/IEC 27001
Security Requirements

ISO/IEC 27005, NIST SP800-39,
ISO 31000 Risk Assessment

NIST
Cyber Security Framework

ISO/IEC 27002, 27019
Security Controls

NISTIR 7628
Smart Grid Security Controls

NERC CIPs
Security Regulations for Bulk Power

IEC 62443-2-3, 2-4, & 4-1
Security Programs

IEEE 1547.3 Guide and Recommendations for Cybersecurity for DER

IEC 62443-3-3
System Security Controls

IEC 62443-4-2
Security for Products

Internet Standards

Directory svcs X500	IPSec RFC 1827
LDAP RFC 4511	TLS RFC 5246
PKI, X509	SNMP RFC 3418
OCSP RFC 6960	Syslog RFC 5424
GDOI RFC 6407	OAuth RFC 6749
EST RFC 7030	Cloud Services
SCEP ...	XML ...

IEC 62351

IEC 62351-3, -4, -5, -6 Security for Protocols
IEC 62351-7 Network & Sys Mgmt (SNMP)
IEC 62351-8 Access Control (RBAC)
IEC 62351-9 Key Management
IEC 62351-10 Security Architecture
IEC 62351-11 Security for XML Files
IEC 62351-12 Cybersecurity for DER
IEC 62351-14 Security Logging
IEC/TR 62351-90-2 Deep Packet Inspection

IEEE 1686 Security for IEDs
IEC 62325-503 Energy Market Security
IEC 60870-5-7 Security for 101/104 Protocol
IEEE 1815 SA/v5 & v6 for DNP3 Protocol
IEEE 2030.5 Protocol Security

ISO/IEC 27001 Certification
(ISO/IEC 27002/27019)

ISO 22301
Business Continuity

Cybersecurity Capability Maturity Model (C2M2) *(for determining the degree of compliance)*

IECEE CMC TF Cybersecurity for IEC 62443 2-4, 4-1 *(in progress)*

IECEE CMC TF Cybersecurity for IEC 62443 3-3, 4-2 *(in progress)*

IEC 62351-100-xx Conformance *(in progress)*

IEEE 1686 Conformance *(future)*

Copyright Xanthus Consulting International

Federal and State Cybersecurity

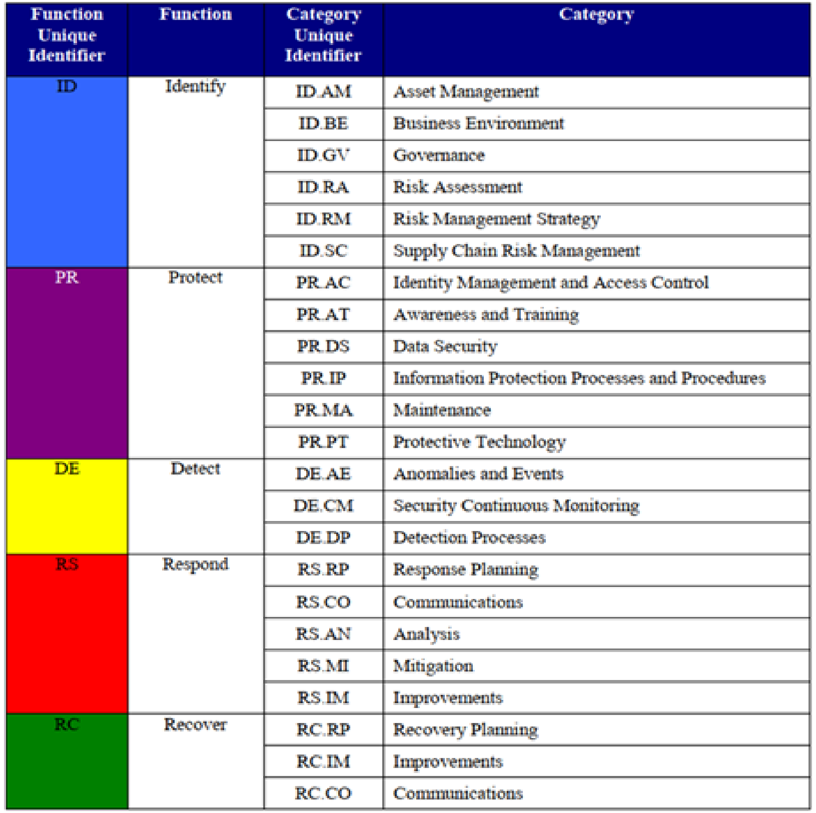
- National Cybersecurity Strategy
  - Defend Critical Infrastructure – We will give the American people confidence in the availability and resilience of our critical infrastructure and the essential services it provides, including by:
    - ✓ Expanding the use of minimum cybersecurity requirements in critical sectors to ensure national security and public safety and harmonizing regulations to reduce the burden of compliance;
    - ✓ Enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services; and,
    - ✓ Defending and modernizing Federal networks and updating Federal incident response policy
- DOE and NARUC
  - The National Association of Regulatory Utility Commissioners, with support from U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response, is developing a Cybersecurity Baseline(s) which would be applicable to distribution utilities and to the distributed energy resources (DER) that interconnect with the distribution grid. Once the baselines are completed, additional efforts will include the development of implementation and compliance guidance for states who decide to adopt the baselines as requirements.
- California Laws SB 327 on Privacy
  - A manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.

Cybersecurity Testing and Certification

- **CPUC Smart Inverter Operationalization Cybersecurity Subgroup**
  - Development of phased cybersecurity requirements for California DER interconnected to the grid, based on the NIST Cybersecurity Framework and IEEE 1547.3 with input from California stakeholders including the utilities, SunSpec, UL, etc.
  - Still determining the Phase 1 Basic Cybersecurity Requirements – expected Q3 2023
- **SunSpec Cybersecurity Certification**
  - The mission of the SunSpec / Sandia DER Cybersecurity Work Group is to support the deployment of Distributed Energy Resources (DER) by defining best practices in cybersecurity for DER and driving the concepts that emerge from these best practices into relevant national and international standards.
- **UL 2941 Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources**
  - Contains mandatory, conditional, and optional cybersecurity requirements applies to cyber security evaluation for network connected inverter-based resources and parts of IBR systems that provide software-based and firmware-based controls, including, but not limited to such devices as inverters, monitoring, and controller devices. It describes the minimum cybersecurity requirements that IBR equipment shall support.
- **IEC 62351-100-x – Testing requirements for the IEC 62351 series of standards**
- **DNP Users Group – Testing for DNP3 SAv5 and soon SAv6**

NIST Cybersecurity Framework (CSF)

Establishes a Common Language



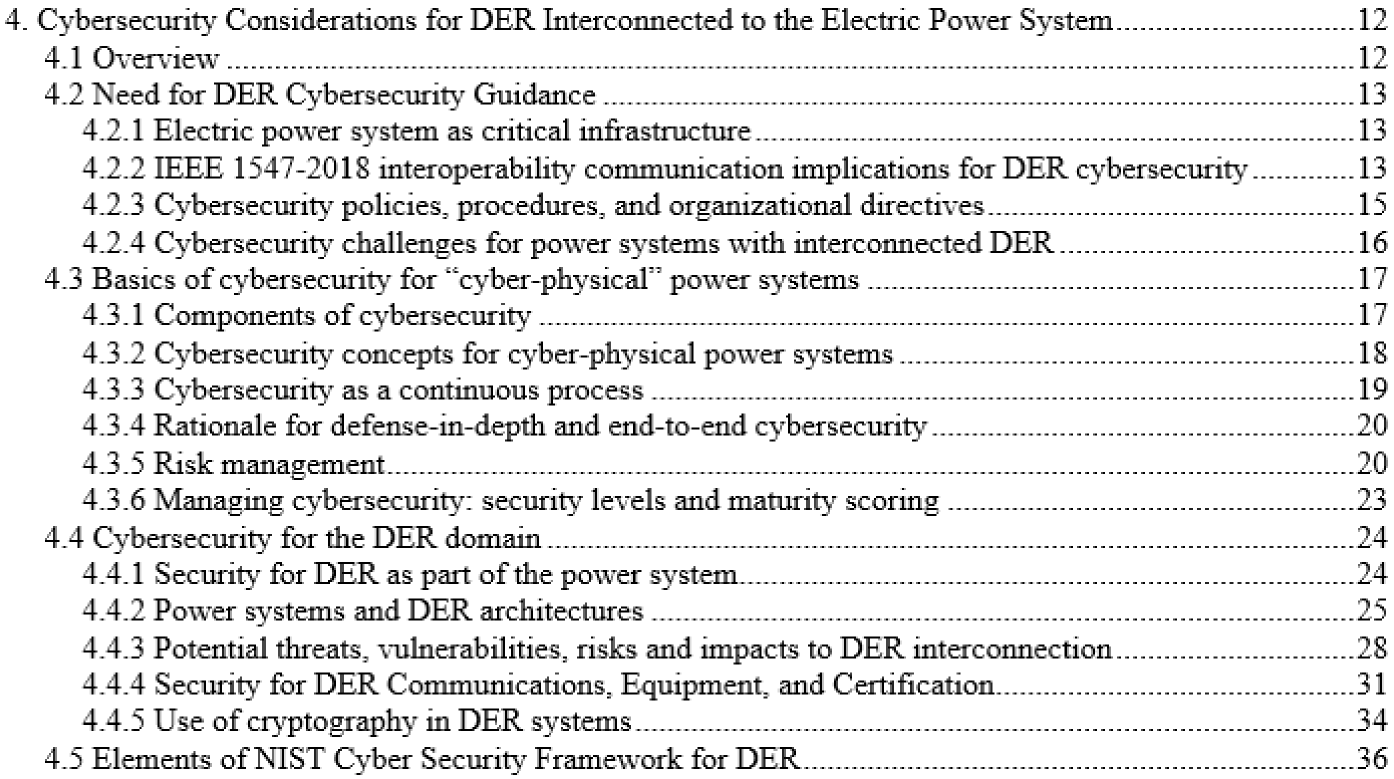
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

- Defines the entire breadth of cybersecurity – excellent as a checklist
- In addition to addressing “prevention of cyber attacks”, it includes planning, detection of possible attacks, and reactions to cope and recover
- Includes “cross-walks” to key cybersecurity standards

Section 4

IEEE 1547.3 Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems

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

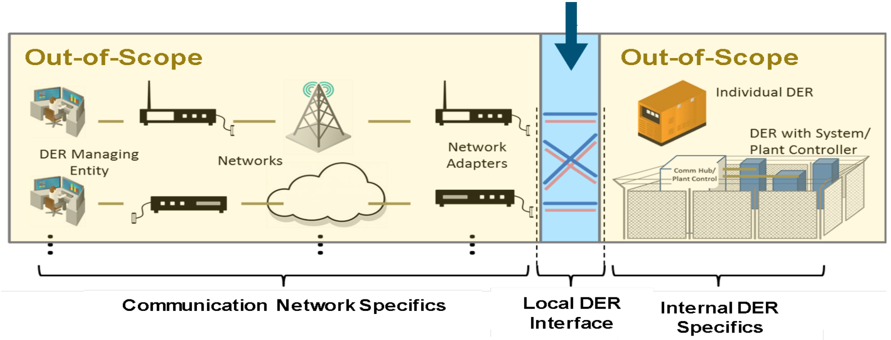


Cybersecurity for DER IEEE 1547.3 Scope – Beyond IEEE 1547-2018 Because Security must be "End-to-End"

Scope Statement for **IEEE 1547**

Yellow areas are out-of-scope for communication protocols

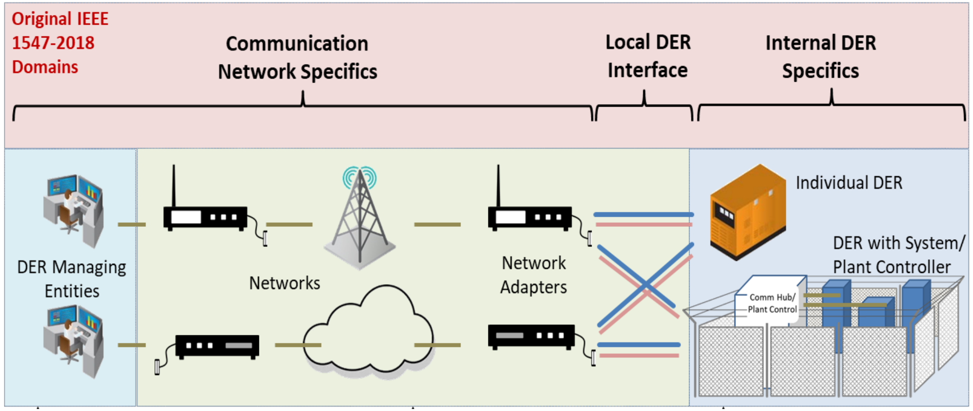
IEEE 1547-2018 scope, which requires SunSpec Modbus, IEEE 1815 (DNP3), or IEEE 2030.5 communications.



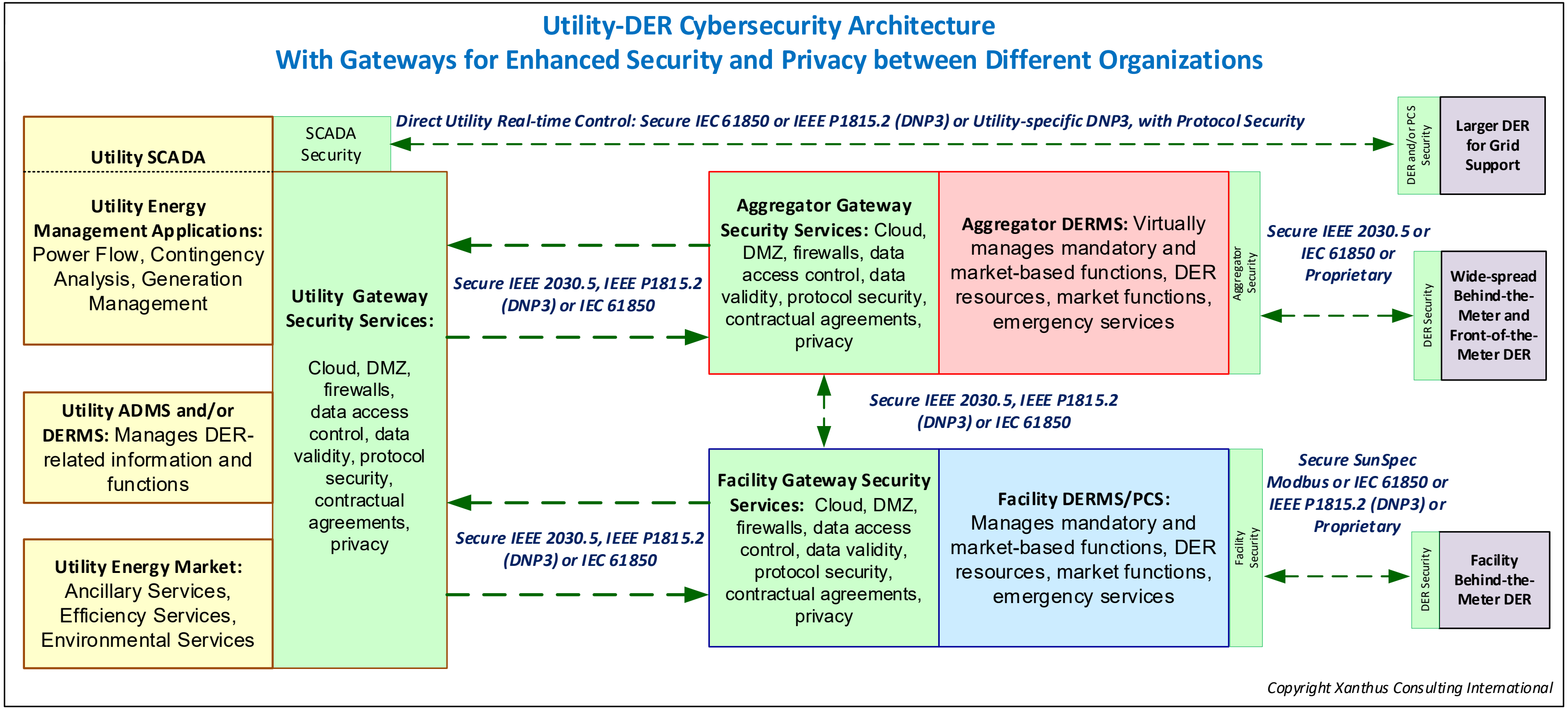
Scope Statement for **IEEE 1547.3**

Pink area is in-scope

On-going debate on scope of **IEEE 1547.10 on Gateways which include Cybersecurity requirements**



Cybersecurity Architecture for Data Exchanges between Utilities, Aggregators, IBR Plants, DER Facilities, and DER Units



Utility-DER Cybersecurity Architecture
With Gateways for Enhanced Security and Privacy between Different Organizations

Utility SCADA

SCADA Security

Direct Utility Real-time Control: Secure IEC 61850 or IEEE P1815.2 (DNP3) or Utility-specific DNP3, with Protocol Security

DER and/or PCS Security

Larger DER for Grid Support

Utility Energy Management Applications: Power Flow, Contingency Analysis, Generation Management

Utility ADMS and/or DERMS: Manages DER-related information and functions

Utility Energy Market: Ancillary Services, Efficiency Services, Environmental Services

Utility Gateway Security Services:

Cloud, DMZ, firewalls, data access control, data validity, protocol security, contractual agreements, privacy

Secure IEEE 2030.5, IEEE P1815.2 (DNP3) or IEC 61850

Aggregator Gateway Security Services: Cloud, DMZ, firewalls, data access control, data validity, protocol security, contractual agreements, privacy

Aggregator DERMS: Virtually manages mandatory and market-based functions, DER resources, market functions, emergency services

Aggregator Security

Secure IEEE 2030.5 or IEC 61850 or Proprietary

DER Security

Wide-spread Behind-the-Meter and Front-of-the-Meter DER

Secure IEEE 2030.5, IEEE P1815.2 (DNP3) or IEC 61850

Secure IEEE 2030.5, IEEE P1815.2 (DNP3) or IEC 61850

Facility Gateway Security Services: Cloud, DMZ, firewalls, data access control, data validity, protocol security, contractual agreements, privacy

Facility DERMS/PCS: Manages mandatory and market-based functions, DER resources, market functions, emergency services

Facility Security

Secure SunSpec Modbus or IEC 61850 or IEEE P1815.2 (DNP3) or Proprietary

DER Security

Facility Behind-the-Meter DER

Copyright Xanthus Consulting International

Clause 5 Technical Cybersecurity Recommendations for DER Operations

- 5.1 Overview of the Structure of this Section
- 5.2 Risk Assessment and Management (RA) Recommendations
  - 5.2.1 General
  - 5.2.2 Risk Assessment Across Organizations (Inter-organizational)
  - 5.2.3 Risk Management Across Organizations (Inter-organizational)
  - 5.2.4 Intra-organizational Risk Issues
- 5.3 Communication Network Engineering (NE) Recommendations
  - 5.3.1 General
  - 5.3.2 Network Segmentation and Defining Security Boundaries
  - 5.3.3 Managing Security Boundary
  - 5.3.4 Network Traffic Monitoring
  - 5.3.5 Network Security Equipment
  - 5.3.6 Physical Access to Networks
  - 5.3.7 Cloud Computing
- 5.4 Access Control (AC) Recommendations
  - 5.4.1 General
  - 5.4.2 User Access Recommendations
  - 5.4.3 System Access Recommendations
  - 5.4.4 Access Management Recommendations
  - 5.4.5 Role-Based Access Control (RBAC) Recommendations
- 5.5 Data Security (DS) Recommendations
  - 5.5.1 General
  - 5.5.2 Security for Data-at-Rest
  - 5.5.3 Security for Data-in-Transit
  - 5.5.4 Comparison of DER Protocol Security
- 5.6 Security Management (SM) Recommendations
  - 5.6.1 General
  - 5.6.2 Lifecycle Management
  - 5.6.3 Supply Chain Management
  - 5.6.4 Patch Management
  - 5.6.5 Security Event Logging
  - 5.6.6 Data Backups
  - 5.6.7 Software Operating Systems and Application Security
- 5.7 Coping with and Recovering from (CM) Security Events Recommendations
  - 5.7.1 General
  - 5.7.2 Pre-Event Coordination Planning and Cross-Organization Security Studies
  - 5.7.3 During-Event Security Event Notification, Coping, and Coordination with Stakeholders
  - 5.7.4 Post-Event Cross-Organization Review of Impact of Security Situation

Example of NIST CSF Items for Section 5.4 Access Control (AC) Recommendations

- ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
- ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
- PR.AC-1: Identities and credentials are managed for authorized devices and users
- PR.AC-3: Remote access is managed
- PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties
- PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
- PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
- PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality
- DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
- DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors

5.4.2 User Access Recommendations

This section provides recommendations for access control for human users, while a more detailed discuss of role-based access control is found in “*Recommendations for Distributed Energy Resource Access Control.*”

Necessary means applicable to all DER; ***Optional*** means applicable to larger or more critical groups of DER.

- ***Necessary Recommendations***

- AC-1. Authentication – All electronic access to systems and devices, whether locally through a control panel or diagnostic port, or remotely through communications media, are protected with an authentication mechanism that identifies a user with a unique user identification (ID) and password combination.
- AC-2. User authorization – Users are assigned permissions to access data, services, resources, or objects granted by the security policy. These permissions are also constrained to one or more of the following: viewing (seeing), reading (downloading), writing (uploading), issuing control commands, creating new items, or deleting items.
- AC-3. User accountability and non-repudiation – User actions are logged so events can be traced, time-synchronized with other events, and/or audited.

Optional Recommendations

AC-4. User authentication – Users provide one or more proofs of identity to help ensure they are who they claim to be. Legitimate users are either required to know something (username/password, key code, etc.), have something (access card), be something (fingerprints, biometric scans, etc.), or—in the case of multifactor authentication—use a combination of these items to prove their identity. Recent implementations are also incorporating geolocation techniques to authenticate legitimate users based on where they are.

AC-5. User-created passwords follow a set of rules that are adhered to in the creation of each password. Passwords are at least eight characters in length and are case sensitive. They do not use common dictionary words and/or consecutive and repeatable characters. When encoding passwords in plain text, the password characters contain the following as a minimum:

AC-6. Any attempt to create a password that violates these rules is captured at the time of attempted creation, and the user is notified and prompted to choose another password that conforms to the rules.

AC-7. Access failures support adjustable account lockout thresholds and durations.

AC-8. Passwords and other security tokens are never displayed through any means, including local display panel, configuration software (local or remote; offline or online), web browser, and terminal access.

AC-9. User access capabilities include a timeout feature that automatically logs out a user who has logged in after a period of user inactivity.

AC-10. For user access to critical devices, applications, or systems, multifactor authentication is used.

CPUC Phase 1 Basic Cybersecurity Requirements: Selecting key items to make "Shall" requirements

- ***Necessary Recommendations***

- AC-1. Authentication – All electronic access to systems and devices, whether locally through a control panel or diagnostic port, or remotely through communications media, **shall be protected** with an authentication mechanism that identifies a user with a unique user identification (ID) and password combination.
- AC-2. User authorization – Users **shall be assigned** permissions to access data, services, resources, or objects granted by the security policy. These permissions are also constrained to one or more of the following: viewing (seeing), reading (downloading), writing (uploading), issuing control commands, creating new items, or deleting items.
- AC-3. User accountability and non-repudiation – User actions **shall be logged** so events can be traced, time-synchronized with other events, and/or audited.

Annexes A - H

Annex E: Recommendations Based on NIST Cybersecurity Framework, Expanded to Identify Key Stakeholders

Subcategory	Justification for Recommendations	Security for Grid Operators for their Interconnected DER	Security for DER Facility Owner/Operators	Security for DER Aggregators/Energy Service Providers	Security for Vendors/Implementors of DER Systems	References to Security Standards
PR.DS-1: Data-at-rest is protected	In the case of power grid systems, protecting data-at-rest applies to protecting the integrity of device settings. If tampered with, device settings may cause a safety or reliability issue.	Grid operators protect data-at-rest from unauthorized viewing, downloading, or modification, and detect, record, and report any unauthorized changes to software, firmware, and data-at-rest. All data updates be validated with roll-back capabilities if applicable. All patches to applications and system software be validated. If cloud computing is used, RBAC is used to help ensure each user has only authorized permissions.	DER facility owner/operators protect data-at-rest from unauthorized viewing, downloading, or modification, and detect, record, and report any unauthorized changes to software, firmware, and data-at-rest. All data updates be validated with roll-back capabilities if applicable. All patches to applications and system software be validated. If cloud computing is used, RBAC is used to help ensure each user has only authorized permissions.	Aggregators protect data-at-rest from unauthorized viewing, downloading, or modification, and detect, record, and report any unauthorized changes to software, firmware, and data-at-rest. All data updates be validated with roll-back capabilities if applicable. All patches to applications and system software be validated. If cloud computing is used, RBAC is used to help ensure each user has only authorized permissions.	Vendors provide methods to protect data-at-rest from unauthorized viewing, downloading, or modification, and provide methods to detect, record, and report any unauthorized changes to software, firmware, and data-at-rest. All data updates have the capability to be validated with roll-back capabilities if applicable. All vendor patches to applications and system software be validated.	**IEC 62443-3-3:2013 SR 3.4, SR 4.1** **ISO/IEC 27001:2013 A.8.2.3** **NIST SP 800-53 Rev. 4 SC-28** **NERC CIP-004-6-R4, CIP-004-6-R5, CIP-011-2-R1, CIP-011-2-R2** ***IEEE 1686 (section TBD)***
PR.DS-2: Data-in-transit is protected	In the case of power grid systems, protecting data in-transit is an important tool to help protect the integrity of control information and device settings. Loss of integrity of control information may cause a safety or reliability issue. Power system owners/operators consider the potential for resource-intensive cryptographic mechanisms to interfere with the functional performance of control systems and use additional methods to protect data in transit when less resource intensive cryptographic mechanisms are used.	Grid operators protect data-in-transit from unauthorized viewing, reading, or modification, and detect, record, and report any unauthorized access. Loss or unavailability of expected or time-sensitive data be detected, and measures taken to compensate.	DER facility owner/operators protect data-in-transit from unauthorized viewing, reading, or modification, and detect, record, and report any unauthorized access. Loss or unavailability of expected or time-sensitive data be detected, and measures taken to compensate.	Aggregators protect data-in-transit from unauthorized viewing, reading, or modification, and detect, record, and report any unauthorized access. Loss or unavailability of expected or time-sensitive data be detected, and measures taken to compensate.	Vendors provide methods to protect data-in-transit from unauthorized viewing, reading, or modification, and provide methods to detect, record, and report any unauthorized access. Loss or unavailability of expected or time-sensitive data be capable of being detected, and measures be provided to compensate.	**IEC 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2** **ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3** **NIST SP 800-53 Rev. 4 SC-8** **NERC CIP-003-7-R2, CIP-004-6-R4, CIP-004-6-R5, CIP-005-5-R1, CIP-005-5-R2, CIP-011-2-R1** ***IEC 62351-3, -4, -5, -6***

Annex F: DER Stakeholder Roles and Responsibilities

❖ Manufacturer DER *design engineering strategies*

1. Manufacturers design the hardware or firmware to prevent software applications or settings from harming these hardware/firmware components. For instance, hardware switches or sensors prevent the software from running the equipment if it would overheat the equipment or while critical self-check operations are taking place. *(e.g., avoid vulnerability of overheating equipment to cause failure)*
2. Manufacturers design the DER system to include setting limits to help ensure that no setting changes can exceed these limits and harm the equipment.
3. Manufacturers include sensors to monitor critical status and measurements, such as switch status, component temperature, speed, vibration, flow, pressure, etc. *(e.g., avoid vulnerability of harming equipment)*
4. Manufacturers design the DER system to provide feedback for actions and commands, including success or failure as well as resulting status or measurement values.
5. Manufacturers harden the DER system such that only essential software and applications are installed in the product and default configuration settings are installed.
6. Manufacturers constrain remote access to the DER hardware/firmware settings that could cause safety or physical damage, such as the use of two-factor authentication and role-based access control.
7. Manufacturers limit even local access to settings that may impact the safety of the DER system or the grid.

❖ Manufacturer DER *design cybersecurity recommendations*

1. Manufacturers provide all DER components with unique cryptographic device identifications by the manufacturer, such as a permanent, global, and unique MRID which is created and stored in its secure element (SE) (e.g. TPM chip).
2. Manufacturers design all DER systems with the default that all access be authenticated.
3. Manufacturers include in DER systems the pre-defined roles for DER owner, DER operator, aggregator, utility normal operations, and utility emergency operations, as a minimum, with pre-defined default permissions for each role. These default permissions could be updated by implementation-specific profiles for rights.
4. Manufacturers test all purchased components for their security capabilities, whether there are any holes in their security through fuzzing and other security assessment methods, and the presence of any malware.
5. Manufacturers use penetration type-testing to help ensure the DER systems are well-protected against cyber attacks.
6. Manufacturers design DER systems with secure firmware or hardware memory for passwords and other embedded private or confidential information that is encrypted or otherwise secured against unauthorized access.
7. Manufacturers design DER systems to permit only non-sensitive data to be accessed by non-authenticated requests.

MESA

Section 5

Focus on DNP3 Cybersecurity

Andrew West

DNP3 Secure Authentication

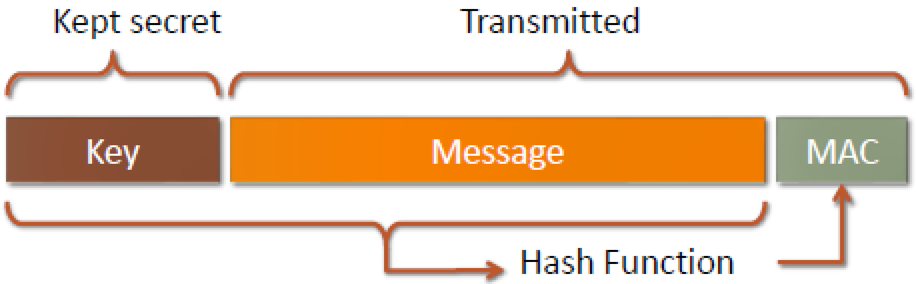
- Areas of Focus
- Availability
- Integrity
  - Message comes from a known, trusted source (not an impersonator)
  - Message not tampered with
  - Message not recorded and replayed
- Execution efficiency

- Developed in parallel with and based on IEC 62351-5

DNP3 Secure Authentication

- Special characteristics for SCADA environment
- Works with any transport media: Serial, Ethernet or mixed media (e.g. Ethernet to a gateway, serial from gateway to IED)
- Suitable for isolated networks
  - Does not require corporate IT access for network management
- Application-to-application authentication
  - Not just site-to-site tunnelling (VPN routers) or “comm port-to-comm port” verification

DNP3-SA



- Core concepts
- Authenticate message with a Hashed Message Authentication Code (HMAC)
  - Adds the MAC to the message being sent
  - Uses secret symmetric “Session Keys” that update frequently
  - Relatively low computational overhead
  - Based on existing standard cryptographic hashing algorithms
- Symmetric “Update Keys” used in periodically updating the Session Keys using cryptographic key-change algorithms

DNP3-SA History

- Initial release: 2007
- SAv2 included in IEEE 1815-2010
  - Pre-shared symmetric Update Keys
- SAv5 included in IEEE 1815-2012
  - Added functions supporting remote distribution of Update Keys
- SAv6 in development for next release of IEEE 1815 (~2025)
  - Removes key management issues
  - Simplifies establishment of trust
  - Adds option for Confidentiality (encryption)

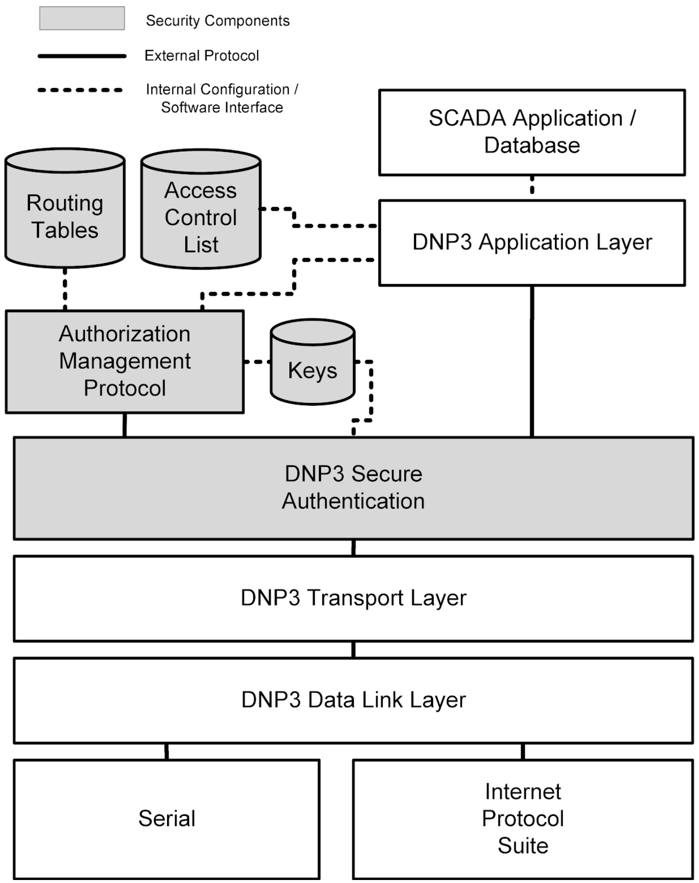
DNP3-SAv6 & AMP

DNP3-SAv6

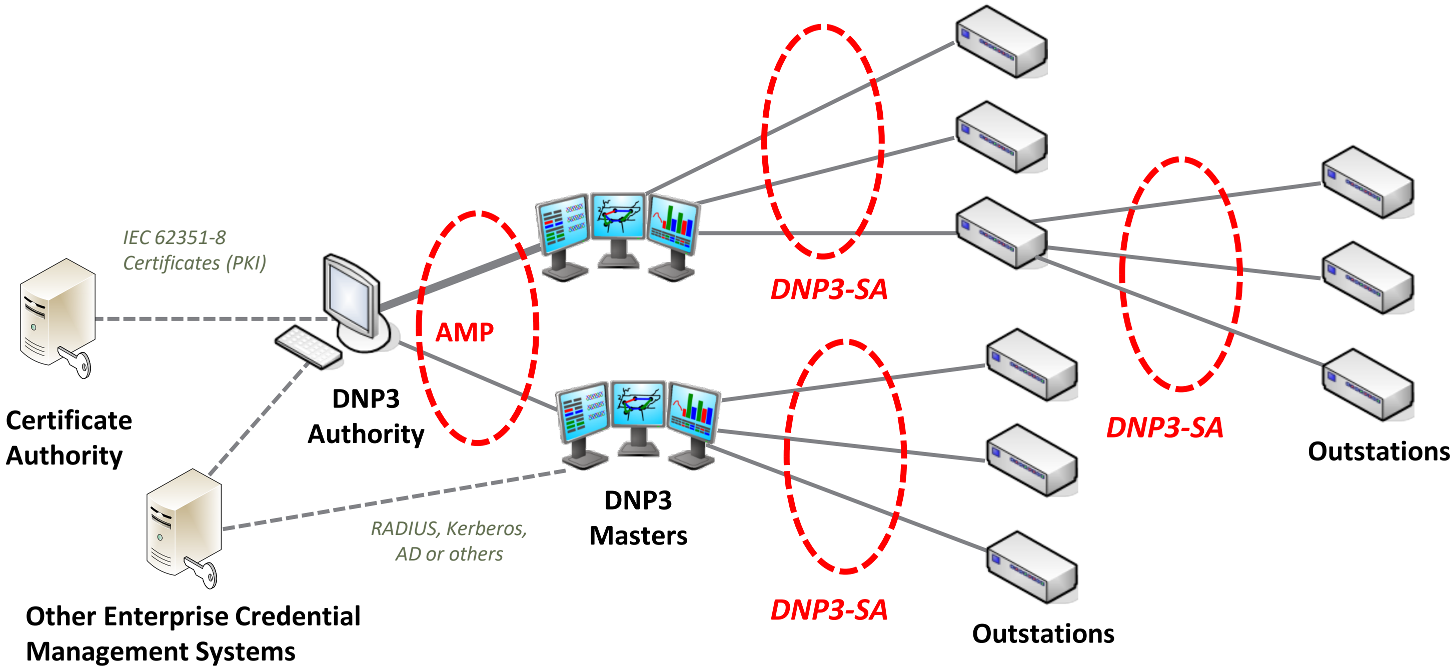
- Protocol between master and outstation
- Provides secure session
- Device enrolment with limited human interaction and no pre-configured keys

Authorization Management Protocol

- Protocol between authority and devices
- Authorizes which devices communicate
- Supports RBAC management



Enterprise Integration



DNP3-SA

- Basic authentication capability unchanged since 2007
- SAv6 will simplify device deployment
  - Eliminating key management
- AMP will provide enhanced management features
  - Remotely manage authorization of communication and RBAC
- SAv2 and SAv5 available now
  - Can be used with pre-configured Update Keys

MESA Membership

MESA Membership

Membership Fee:

- ✓ Offers entry into working groups and committees
- ✓ Members can be elected to the Board of Directors

Discretionary Allocation to Technical Priorities:

- ✓ Variable depending on organizational technical priorities
- ✓ Fees can be directed toward a specific project

2023 Membership Options:

Standard (Companies with revenue > $1M): $5,000

Small Business (Companies with revenue ≤ $1M): $3,000

MESA/SunSpec Joint Modbus Membership: $9,000

Individual/Strategic Partner: $1,000

Student: $350

2023 Technical Allocation:

A min $5,000 per company (depends on available funds) focused on MESA-DER certification program development

Read more about MESA's membership options at **http://mesastandards.org/membership/**

Questions?