List of Cybersecurity for Smart Grid Standards and Guidelines

Collected by Frances Cleveland, Xanthus Consulting International,

Convenor IEC TC57 WG15

May, 2013

1. List of Standards that include Cybersecurity

The following existing work and standards are applicable to the field of Smart Grid information security. This clause contains 3 lists:

1) Smart Grid cybersecurity standards, recommended practices, and guidelines (many reference other standards as well)

2) Smart Grid standards and other Smart Grid documents that include cybersecurity requirements (to greater or lesser extents)

3) Organizations and programs addressing Smart Grid cybersecurity

Cybersecurity for the Smart Grid is a huge and ever-expanding effort, and the items in these lists capture only some of the main standards and efforts. It is expected that these lists could grow significantly as new cybersecurity standards and efforts are recognized.

Many of the cybersecurity standards listed actually consist of many parts. Some of them are based on typical IT standards (e.g. TLS for TCP/IP), but many are unique due to the cyber-physical nature of the Smart Grid, the high importance of availability rather than confidentiality, the wide-spread nature of the power grid, and the criticality of performance (e.g. 4 ms interactions).

Some of these documents are formal standards, while others are still under development or are recommended practices or other informative guidelines. Therefore, some are not freely available, while others may require permission from the developers for access. *(This list does not attempt to provide such contact information.)*

The number of cybersecurity Use Cases for the Smart Grid is very large - in the hundreds if not thousands - although some activities are on-going to categorize them by types of cybersecurity issues. These Use Cases are used to identify cybersecurity requirements and any gaps in standards, but are also used to identify mitigation policies, procedures, and technologies that can minimize cybersecurity risks.

Corrections and suggestions for this list are very welcome. There are certainly additional documents not listed here that are part of the Smart Grid cybersecurity effort – any identification of these additional documents would be very helpful.

1.1 Cybersecurity Standards / Guides Used in the Smart Grid

- ASAP-SG Security Profiles for:
  - Third Party Data Access
  - Advanced Metering Infrastructure (AMI)
  - Distribution Management
  - Wide-Area Monitoring, Protection, and Control (WAMPAC)
  - Substation Automation (*under development*)
- CIGRE B5/D2.46 Application and management of cyber security measures for Protection & Control systems
- CIGRE D2.31 Security architecture principles for digital systems in Electric Power Utilities EPUs
- DHS Catalog of Control Systems Security
- DHS Cyber Security Procurement Language for Control Systems
- DOE / DHS Cybersecurity Capability Maturity Model for the Electricity Subsector
- DOE/NIST/NERC Electricity Subsector Cybersecurity Risk Management Process Guideline
- DOE / DHS Electric Sector Cybersecurity Risk Management Maturity Initiative
- DOE Roadmap to Achieve Energy Delivery Systems Cybersecurity
- IEC 62351 Parts 1-11 Power systems management and associated information exchange – Data and communications security *(Parts 9, 10, & 11 still under development)*
- IEC 62443 series on Security for industrial process measurement and control *(work in process)*
- IEEE 1686 Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities *(being updated)*
- IEEE 802 series
  - IEEE 802.11i Wireless security
  - IEEE 802.1X Port Based Network Access Control
  - IEEE 802.1AE MAC security
- IEEE 802.1AR Secure Device Identity

- IETF Cybersecurity RFCs, including:
  - RFC 5246 Transport Layer Security (TLS)
  - RFC 6407 Group Domain of Interpretation (GDOI)
  - RFC 4101, RFC 4102, RFC 4103 Base standards for IP Security (IPSec)
  - RFC 6347 Datagram Transport Layer Security (DTLS)
  - RFC 3711 Secure Real-time Transport Protocol (SRTP)
  - RFC 4962 Authentication, Authorization, and Accounting
  - RFC 5247 Extensible Authentication Protocol (EAP) Key Management Framework
  - RFC 5746 Transport Layer Security (TLS) Renegotiation Indication Extension
- IETF RFC 6272 Internet Protocols for the Smart Grid (*identifies RFCs used in the Smart Grid)*
- ISA SP99 Cybersecurity mitigation for industrial and bulk power generation stations *(work in process)*
- ISO 27000 Information Security Standards *(many standards)*
- NERC Critical Infrastructure Protection (CIP) 002-009 *(multiple versions)*
- NIST FIPS 140-2 Cryptographic Security
- NIST SP 500-267 Security Profile for IPv6
- NIST SP 800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths *(draft)*
- NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations *(rev 4 as draft)*
- NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards
- NIST Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View
- NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems
- NISTIR 7628 Vol. 1 thru 3 Guidelines for Smart Grid Cyber Security
- NISTIR 7823: Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework *(draft)*
- OASIS WS-Security for web services

1.2 Smart Grid Standards that Include or Reference Cybersecurity Requirements

- ANSI C12.1-2008 Standard for Electric Meters Code for Electricity Metering

- ANSI C12.18-2006/IEEE P1701/MC1218 Protocol Specification for ANSI Type 2 Optical Port
- ANSI C12.19-2008/IEEE 1377/MC1219 Utility Industry End Device Data Tables
- ANSI C12.21/IEEE P1702/MC1221 Protocol Specification for Telephone Modem Communication
- ANSI C12.22/IEEE P1703/MC1222 Protocol Spec for Interfacing to Data Comm Networks
- ANSI/ASHRAE 135-2010/ISO 16484-5 BACnet
- ANSI/CEA 709.1-B-2002 Control Network Protocol Specification
- CEA 852.1:2009 Enhanced Tunneling Device Area Network Protocols
- IEC 15118 Road vehicles — Vehicle to grid communication interface
- IEC 60870-5 Telecontrol equipment and systems: Transmission protocols
- IEC 60870-6 Telecontrol Application Service Element 2 (TASE.2) (references IEC 62351)
- IEC 61850 Suite of standards on Communication Networks and Systems for Power Utility Automation (references IEC 62351)
- IEC 61850-90-5 for exchanging synchrophasor information
- IEC 61968 System Interfaces for Distribution Management (references IEC 62351)
- IEC 61970 Energy management system application program interface (EMS-API) (references IEC 62351)
- IEC 62056 COSEM: COmpanion Specification for Energy Metering (COSEM)
- IEC 62541 OPC Unified Architecture
- IEC PAS 62559 Methodology for Requirements Development
- IEEE 1588 Precision Time Protocol in Power System Applications
- IEEE 1815 DNP3 (Distributed Network Protocol)
- IEEE 1901-2010 (Same as ITU-T G.9972) Inter-System Protocol (ISP)-based Broadband Power Line Carrier (PLC)
- IEEE 802 Family, specifically IEEE 802.11i
- IEEE C37.238 Profile of IEEE 1588 for Electric Power Systems
- IEEE C37.239 Standard for Common Format for Event Data Exchange (COMFEDE) for Power Systems
- IEEE P1642 Recommended Practice for Protecting Public Accessible Computer Systems from Intentional EMI
- IEEE P1775/1.9.7, March 2009 IEEE Standard for Power Line Communication Equipment - EMC Requirements - Testing and Measuring Methods
- IEEE P1901 Broadband Communications Over Power Lines MAC and PHY protocols

- IEEE P1901.2 (same as ITU-T G.9955/G.9956) Low frequency communications over power lines
- IEEE P2030 Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation With the Electric Power System (EPS), and End-Use Applications and Loads
- IETF RFC 6272 Internet Protocols for the Smart Grid
- ITU-T G.9955/G.9956 Low frequency communications over power lines
- NEMA SG-AMI 1-2009 Requirements for Smart Meter Upgradeability
- Network Management Standards - including Internet based standards such as DMTF, CIM, WBEM, ANSI INCITS 438-2008, SNMP v3, Netconf, STD 62, and OSI-based standards including CMIP/CMIS
- NISTIR 7761 NISTs Guidelines for Assessing Wireless Standards for Smart Grid Applications
- NRECA MultiSpeak
- OASIS EMIX Energy Market Information eXchange
- SGIP SGTCC Interoperability Process Reference Manual (IPRM)
- UCAIug OpenADE Energy Service Provider Interface
- UCAIug Security Profile for AMI v.1.0 (AMI SEC)
- UL-1741 Static Inverters and Charge Controllers for use in PV Power Systems
- W3C Efficient XML Interchange (EXI)
- W3C Extensible Markup Language (XML)
- W3C Simple Object Access Protocol (SOAP)
- W3C Web Definition Service Language (WSDL)
- W3C XML Service Definition (XSD)
- ZigBee Smart Energy Profile (SEP) 1.0 and 1.1
- ZigBee/HomePlug Smart Energy Profile (SEP) 2.0

1.3 Organizations and Programs Addressing Smart Grid Cybersecurity

- IEC TC57 WG15:
  - Development of the IEC 62351 series of power systems management and associated information exchange – data and communications security
- IEC TC65:
  - IEC 62443 series of industrial automation security standards based on ISA SP99 security standards
  - IEC 62541 OPC UA standards including security

- IEC TC13:
  - Security for metering standards DLMS/COSEM
- National Institute of Standards and Technology (NIST) and the Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG):
  - Development and updating of the NISTIR 7628
  - Review and assessment of standards for cybersecurity specifications and gaps
  - Assessment of privacy Issues
  - Development of a cybersecurity architecture
  - Implementation compliance and testing guidelines
  - Development of AMI security requirements
- European M/490 Smart Grid Information Security (SGIS):
  - Review and assessment of information security standards
  - Recommendations for addressing gaps in cybersecurity standards
  - Enhancement of recommendations on existing standards or need for new ones
  - Recommendations on SGIS security levels and data protection classes
  - SGIS Toolbox for identifying recommended security requirements and associated standards for implementation.
- Department of Energy (DOE) and the Electric Power Research Institute (EPRI) National Electric Sector Cybersecurity Organization (NESCO) and Research (NESCOR)
  - Development of failure scenarios for the Smart Grid
  - Assessment of cybersecurity requirements and standards for specific Smart Grid functions such as wide-area situational awareness and distributed energy resources
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) security standards development:
  - In United States, CIP 002-009 security mandates for the bulk power system
- US White House / DOE sponsored conferences and programs on cyber-physical security
- DOE Smart Grid Projects which require cybersecurity, for example:
  - Cybersecurity Capability Maturity Model for the Electricity Subsector
  - Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline
  - DOE/NIST collaboration on AMI Upgradeability Test bed
  - RDSI Projects (many)
- Cigré D2.22 Information Security for Electric Power Utilities (EPUs)
- DOE and Department of Homeland Security (DHS) Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center
- OpenSG Smart Grid Security Users Group
- ASAP-SG Program to develop security requirements for Smart Grid domains
- Institute of Electrical and Electronic Engineers (IEEE) Power & Energy Society (PES) – various standards development under the different committees
- ZigBee Alliance for the development of SEP 1.x and SEP 2.0

2. Matrix of Cybersecurity Standards Associated with Smart Grid Standards

A (draft) matrix of cybersecurity standards associated with Smart Grid standards is shown in the Excel spreadsheet labeled "*Standards to cybersecurity matrix.xlsx*" (see http://xanthus-consulting.com/Publications/documents/Matrix_of_Standards_with_Cybersecurity.pdf). Some rows and columns still need to be filled in.

While recognizing that matrices are difficult to use, it is expected that this spreadsheet can assist in identifying cybersecurity gaps.

3. Diagrams of Smart Grid Standards

The following diagrams may assist in understanding where some of the Smart Grid standards are used (Figure 1), what OSI Reference Model[1] and GWAC Stack[2] levels they cover (Figure 2 and Figure 3), the IEC 62351 security standards (Figure 4) and, as an example, how cybersecurity standards are applied to one Smart Grid standard, IEC 61850 (Figure 5). Cyber-physical security is shown conceptually in Figure 6.

[1] ISO 7498-1:1994, *Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model.*

[2] The GWAC Stack is available at http://www.gridwiseac.org/ in the *GridWise Interoperability Context-Setting Framework.*

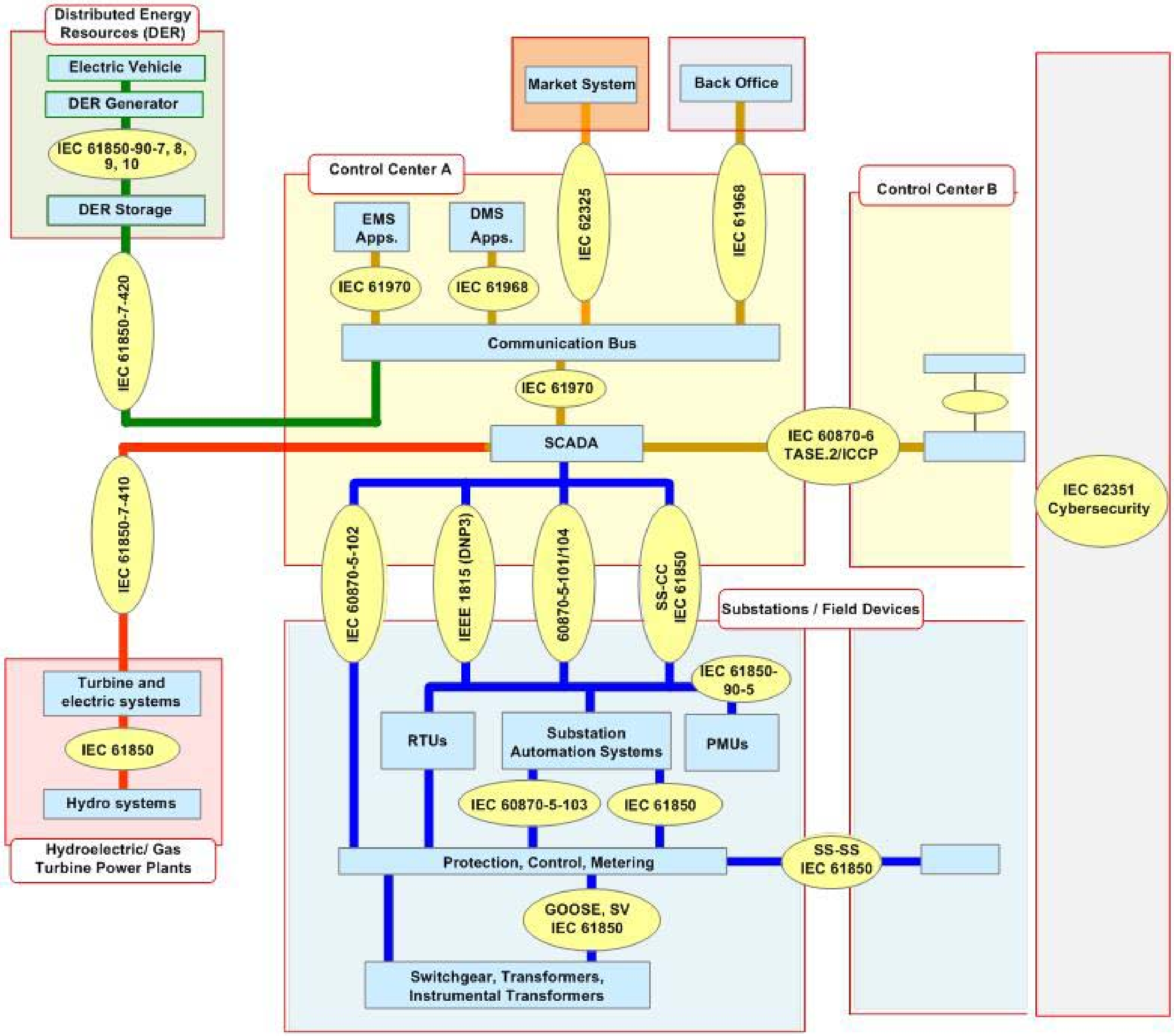


Figure 1: IEC TC57 Smart Grid standards

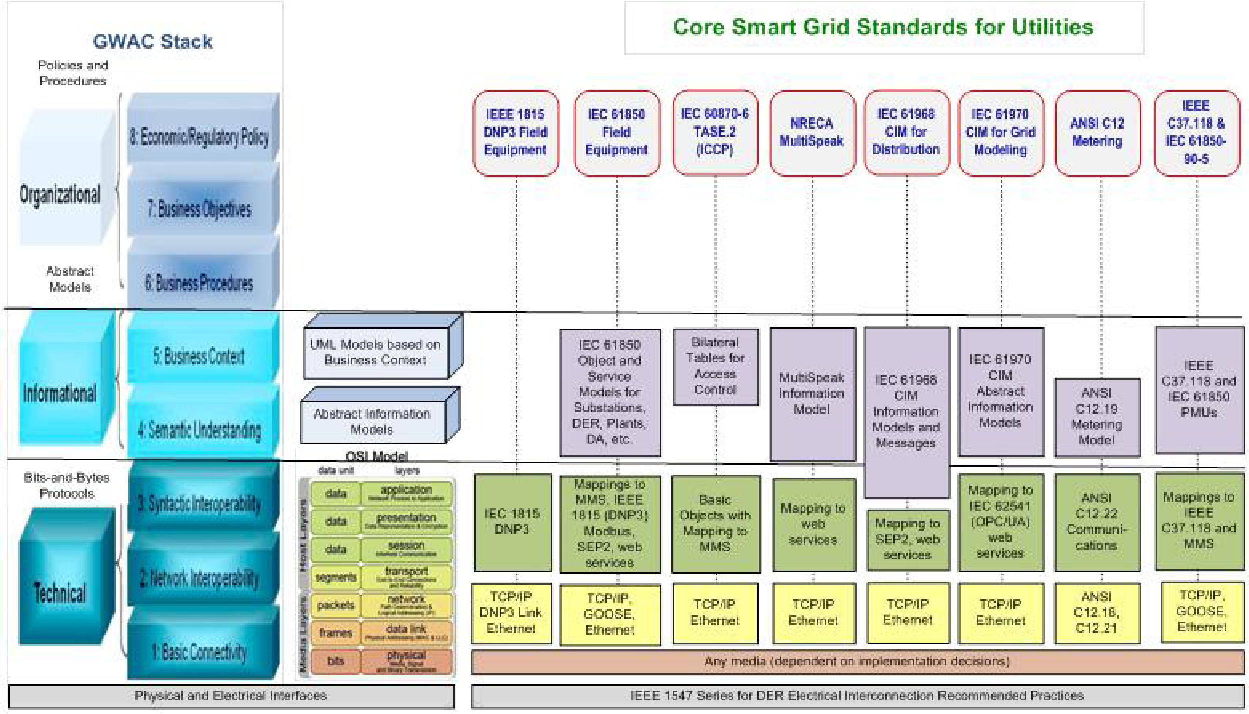

Core Smart Grid Standards for Utilities
GWAC Stack
Policies and Procedures
Organizational
8: Economic/Regulatory Policy
7: Business Objectives
6: Business Procedures
Abstract Models
Informational
5: Business Context
4: Semantic Understanding
Bits-and-Bytes Protocols
Technical
3: Syntactic Interoperability
2: Network Interoperability
1: Basic Connectivity
UML Models based on Business Context
Abstract Information Models
OSI Model
data unit
layers
data
application
data
presentation
data
session
segments
transport
packets
network
frames
data link
bits
physical
Host Layers
Media Layers
IEEE 1815 DNP3 Field Equipment
IEC 61850 Field Equipment
IEC 60870-6 TASE.2 (ICCP)
NRECA MultiSpeak
IEC 61968 CIM for Distribution
IEC 61970 CIM for Grid Modeling
ANSI C12 Metering
IEEE C37.118 & IEC 61850-90-5
IEC 61850 Object and Service Models for Substations, DER, Plants, DA, etc.
Bilateral Tables for Access Control
MultiSpeak Information Model
IEC 61968 CIM Information Models and Messages
IEC 61970 CIM Abstract Information Models
ANSI C12.19 Metering Model
IEEE C37.118 and IEC 61850 PMUs
IEC 1815 DNP3
Mappings to MMS, IEEE 1815 (DNP3) Modbus, SEP2, web services
Basic Objects with Mapping to MMS
Mapping to web services
Mapping to SEP2, web services
Mapping to IEC 62541 (OPC/UA) web services
ANSI C12.22 Communi-cations
Mappings to IEEE C37.118 and MMS
TCP/IP DNP3 Link Ethernet
TCP/IP, GOOSE, Ethernet
TCP/IP Ethernet
TCP/IP Ethernet
TCP/IP Ethernet
TCP/IP Ethernet
ANSI C12.18, C12.21
TCP/IP, GOOSE, Ethernet
Any media (dependent on implementation decisions)
Physical and Electrical Interfaces
IEEE 1547 Series for DER Electrical Interconnection Recommended Practices

Figure 2: Core Smart Grid Standards for Utilities

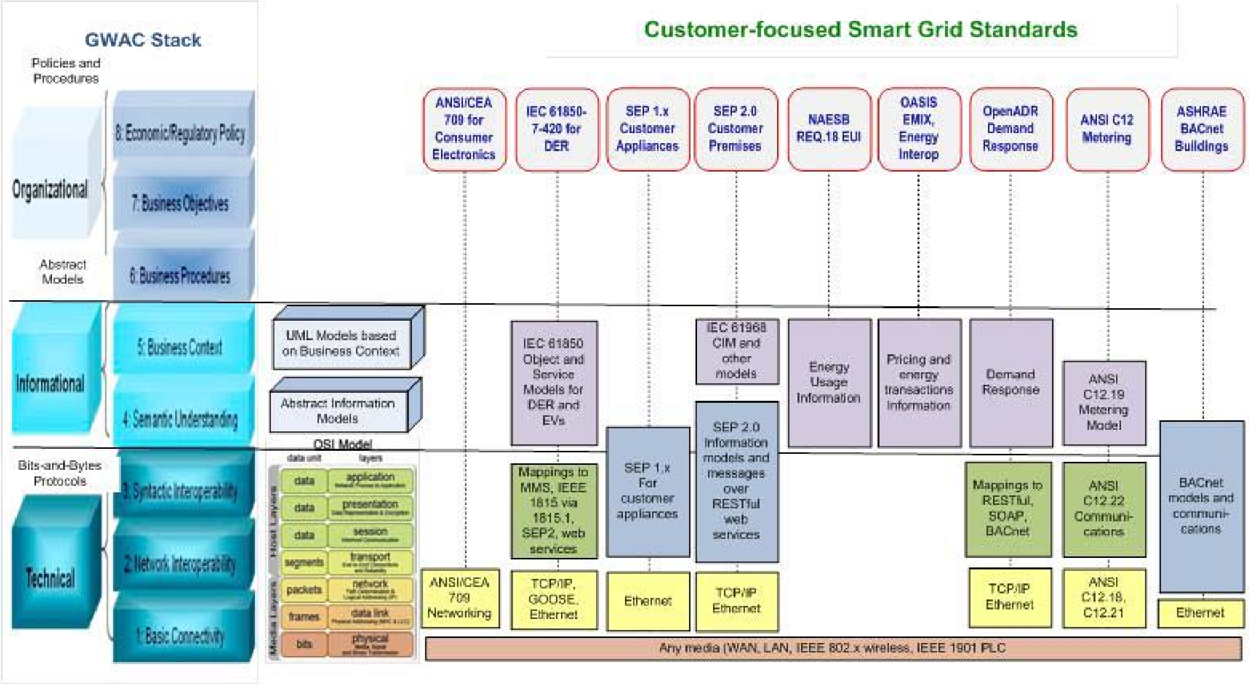

Customer-focused Smart Grid Standards
GWAC Stack
Policies and Procedures
Organizational
8: Economic/Regulatory Policy
7: Business Objectives
6: Business Procedures
Abstract Models
Informational
5: Business Context
4: Semantic Understanding
Bits-and-Bytes Protocols
Technical
3: Syntactic Interoperability
2: Network Interoperability
1: Basic Connectivity
UML Models based on Business Context
Abstract Information Models
OSI Model
data unit
layers
data
application
data
presentation
data
session
segments
transport
packets
network
frames
data link
bits
physical
Host Layers
Media Layers
ANSI/CEA 709 for Consumer Electronics
IEC 61850-7-420 for DER
SEP 1.x Customer Appliances
SEP 2.0 Customer Premises
NAESB REQ.18 EUI
OASIS EMIX, Energy Interop
OpenADR Demand Response
ANSI C12 Metering
ASHRAE BACnet Buildings
IEC 61850 Object and Service Models for DER and EVs
IEC 61968 CIM and other models
Energy Usage Information
Pricing and energy transactions information
Demand Response
ANSI C12.19 Metering Model
SEP 1.x For customer appliances
SEP 2.0 Information models and messages over RESTful web services
Mappings to MMS, IEEE 1815 via 1815.1, SEP2, web services
Mappings to RESTful, SOAP, BACnet
ANSI C12.22 Communi-cations
BACnet models and communi-cations
ANSI/CEA 709 Networking
TCP/IP, GOOSE, Ethernet
Ethernet
TCP/IP Ethernet
TCP/IP Ethernet
ANSI C12.18, C12.21
Ethernet
Any media (WAN, LAN, IEEE 802.x wireless, IEEE 1901 PLC

Figure 3: Customer-focused Smart Grid Standards

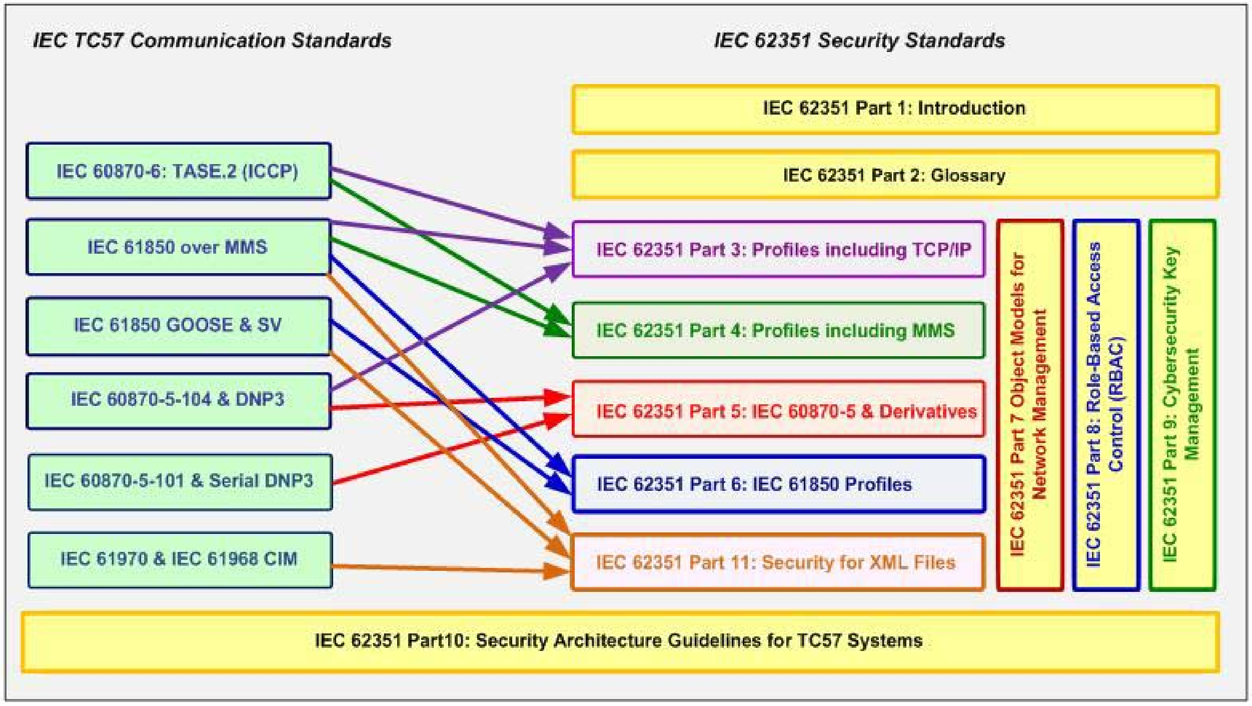
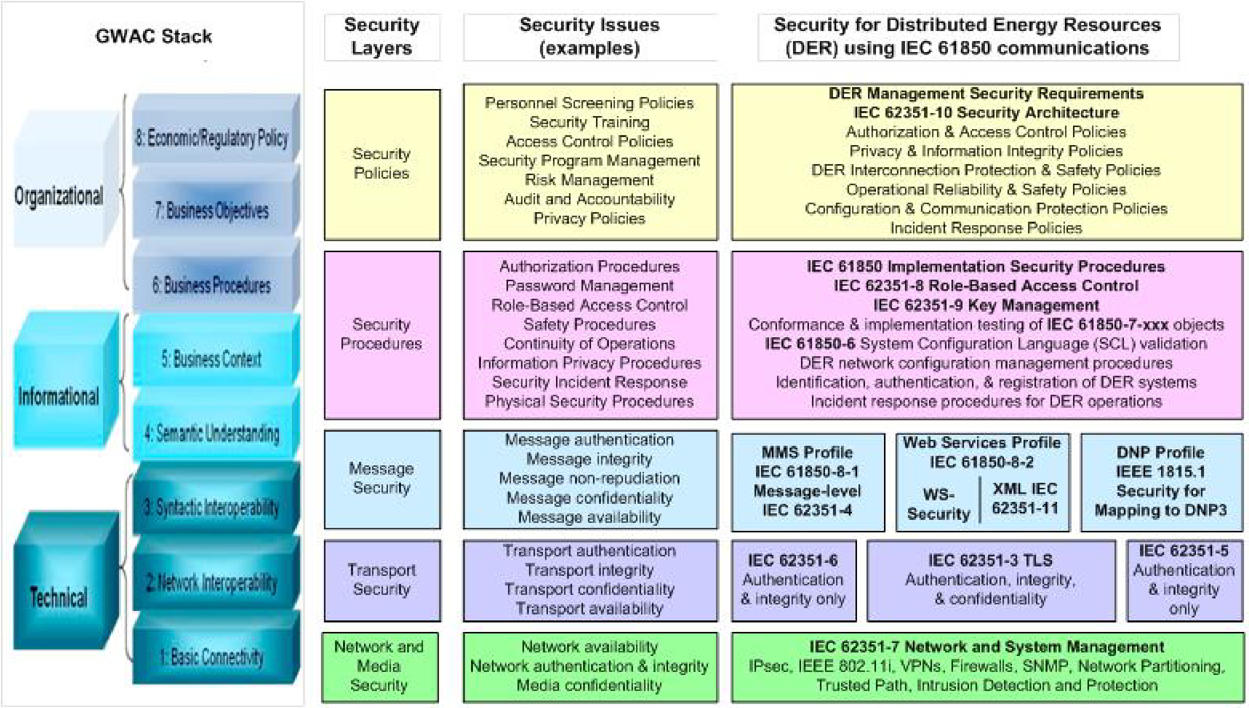

IEC TC57 Communication Standards
IEC 62351 Security Standards
IEC 62351 Part 1: Introduction
IEC 62351 Part 2: Glossary
IEC 60870-6: TASE.2 (ICCP)
IEC 61850 over MMS
IEC 61850 GOOSE & SV
IEC 60870-5-104 & DNP3
IEC 60870-5-101 & Serial DNP3
IEC 61970 & IEC 61968 CIM
IEC 62351 Part 3: Profiles including TCP/IP
IEC 62351 Part 4: Profiles including MMS
IEC 62351 Part 5: IEC 60870-5 & Derivatives
IEC 62351 Part 6: IEC 61850 Profiles
IEC 62351 Part 11: Security for XML Files
IEC 62351 Part 7 Object Models for Network Management
IEC 62351 Part 8: Role-Based Access Control (RBAC)
IEC 62351 Part 9: Cybersecurity Key Management
IEC 62351 Part10: Security Architecture Guidelines for TC57 Systems

Figure 4: Mapping of IEC TC57 Communication Standards to IEC 62351 Cybersecurity Standards



Security Layers	Security Issues (examples)	Security for Distributed Energy Resources (DER) using IEC 61850 communications		
Security Policies	Personnel Screening Policies Security Training Access Control Policies Security Program Management Risk Management Audit and Accountability Privacy Policies	**DER Management Security Requirements** **IEC 62351-10 Security Architecture** Authorization & Access Control Policies Privacy & Information Integrity Policies DER Interconnection Protection & Safety Policies Operational Reliability & Safety Policies Configuration & Communication Protection Policies Incident Response Policies		
Security Procedures	Authorization Procedures Password Management Role-Based Access Control Safety Procedures Continuity of Operations Information Privacy Procedures Security Incident Response Physical Security Procedures	**IEC 61850 Implementation Security Procedures** **IEC 62351-8 Role-Based Access Control** **IEC 62351-9 Key Management** Conformance & implementation testing of **IEC 61850-7-xxx** objects **IEC 61850-6** System Configuration Language (SCL) validation DER network configuration management procedures Identification, authentication, & registration of DER systems Incident response procedures for DER operations		
Message Security	Message authentication Message integrity Message non-repudiation Message confidentiality Message availability	**MMS Profile** **IEC 61850-8-1** **Message-level** **IEC 62351-4**	**Web Services Profile** **IEC 61850-8-2** **WS-Security** | **XML IEC 62351-11**	**DNP Profile** **IEEE 1815.1** **Security for Mapping to DNP3**
Transport Security	Transport authentication Transport integrity Transport confidentiality Transport availability	**IEC 62351-6** Authentication & integrity only	**IEC 62351-3 TLS** Authentication, integrity, & confidentiality	**IEC 62351-5** Authentication & integrity only
Network and Media Security	Network availability Network authentication & integrity Media confidentiality	**IEC 62351-7 Network and System Management** IPsec, IEEE 802.11i, VPNs, Firewalls, SNMP, Network Partitioning, Trusted Path, Intrusion Detection and Protection		

Figure 5: Security Requirements and Standards used with IEC 61850 Profiles for Distributed Energy Resources (DER)

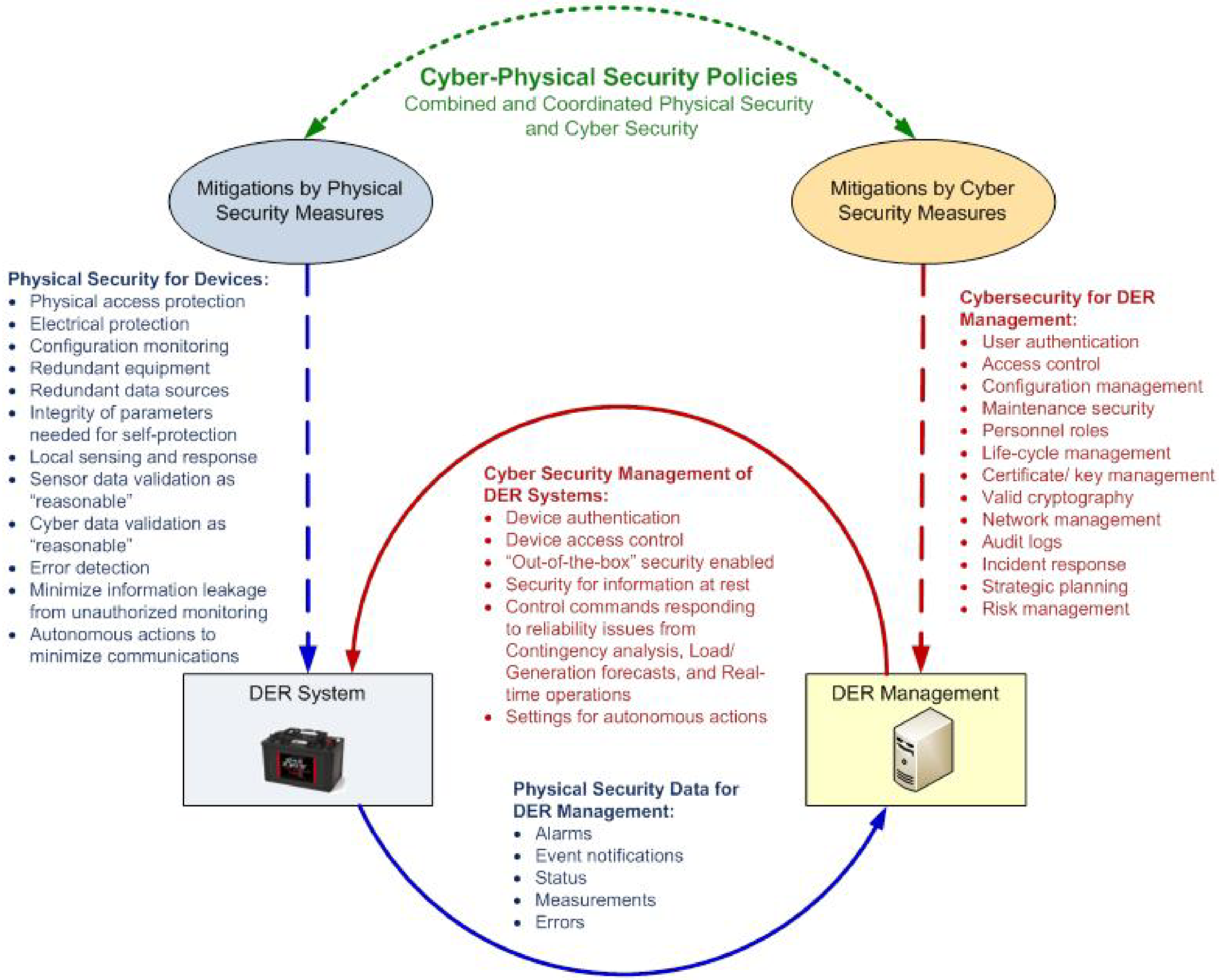

Cyber-Physical Security Policies
Combined and Coordinated Physical Security and Cyber Security
Mitigations by Physical Security Measures
Mitigations by Cyber Security Measures
Physical Security for Devices:
• Physical access protection
• Electrical protection
• Configuration monitoring
• Redundant equipment
• Redundant data sources
• Integrity of parameters needed for self-protection
• Local sensing and response
• Sensor data validation as "reasonable"
• Cyber data validation as "reasonable"
• Error detection
• Minimize information leakage from unauthorized monitoring
• Autonomous actions to minimize communications
Cybersecurity for DER Management:
• User authentication
• Access control
• Configuration management
• Maintenance security
• Personnel roles
• Life-cycle management
• Certificate/ key management
• Valid cryptography
• Network management
• Audit logs
• Incident response
• Strategic planning
• Risk management
Cyber Security Management of DER Systems:
• Device authentication
• Device access control
• "Out-of-the-box" security enabled
• Security for information at rest
• Control commands responding to reliability issues from Contingency analysis, Load/ Generation forecasts, and Real-time operations
• Settings for autonomous actions
DER System
DER Management
Physical Security Data for DER Management:
• Alarms
• Event notifications
• Status
• Measurements
• Errors

Figure 6: Cyber-Physical Security – Combined & coordinated physical security and cyber security