Cybersecurity in Power Systems

A view on connected regulation and standardization

Steffen Fries, Siemens, T CST

May 12, 2023

SIEMENS

Speakers background: Applied industrial research at Siemens Technology

Steffen Fries is working in the area of cybersecurity within Siemens Technology for more than 25 years. As principal engineer he focuses on the analysis, design, and implementation of secure communication solutions for different verticals. This requires collaborating with system architects, implementers, and product management in order to design secure solutions from ground.

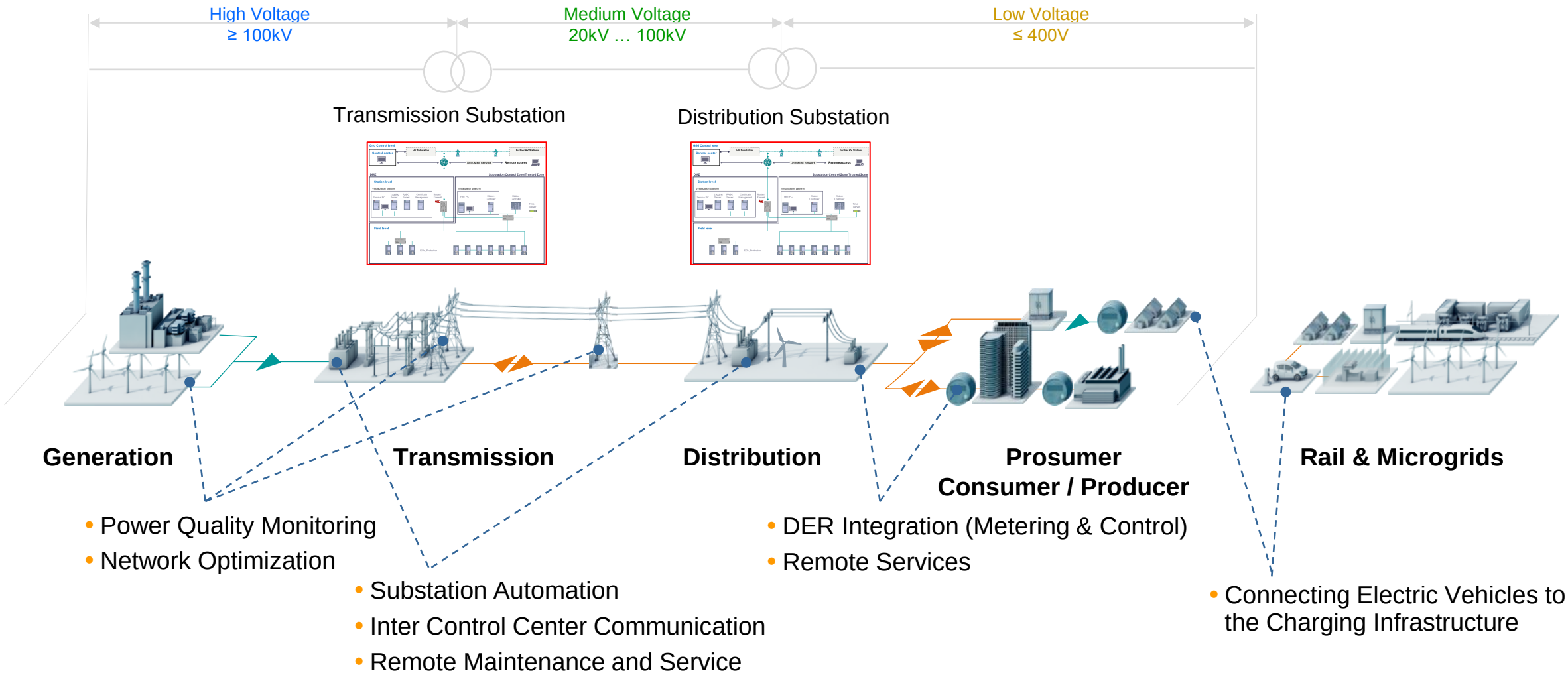
Within standardization, he is editor of and contributor to several IEC 62351 documents in IEC TC 57 for power system automation. Besides this he is active in IEEE on topics related to secure time synchronization for the precision time protocol IEEE 1588. In IETF he contributes to the development of RFCs in the area of device bootstrapping, certificate enrollment and connected protocols and credential formats.

Steffen Fries
Principal Key Expert
Siemens Technology

SIEMENS

Digital Grid – a Critical Infrastructure in Need of Protection

Power system value chain and use case examples



Security must be (continuously) adopted to the changing threat and vulnerability landscape

1950s – 1960s
Military, governments and other organizations implement computer systems

1980s
Computers make their way into schools, homes, business and industry

1999
The globe is connected by the internet

2010s
Cloud computing enters the mainstream

2020s
Internet of Things, Smart and autonomous systems, Artificial Intelligence, Big Data

Digital Information Processing | Digital Connectivity | Digital Automation and Artificial Intelligence

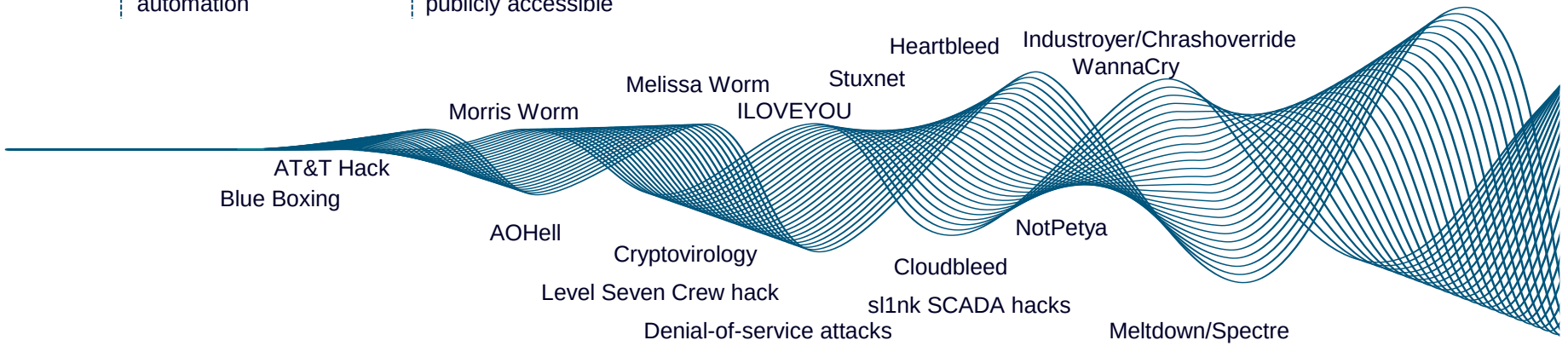
1970s
Home computer is introduced

1990s
Digital enhancement of electrification and automation

1991
The World Wide Web becomes publicly accessible

2000s
Mobile flexibility

2020s
Industry 4.0



Digital Grid as critical infrastructure is addressed through regulative requirements and standards (examples, global view)

Regulative Requirements

- Critical Infrastructure Protection (NERC CIP)
- Executive Order 13636 improving Critical Infrastructure Cyber Security
- Executive Order 14028 improving Nation's Cyber Security

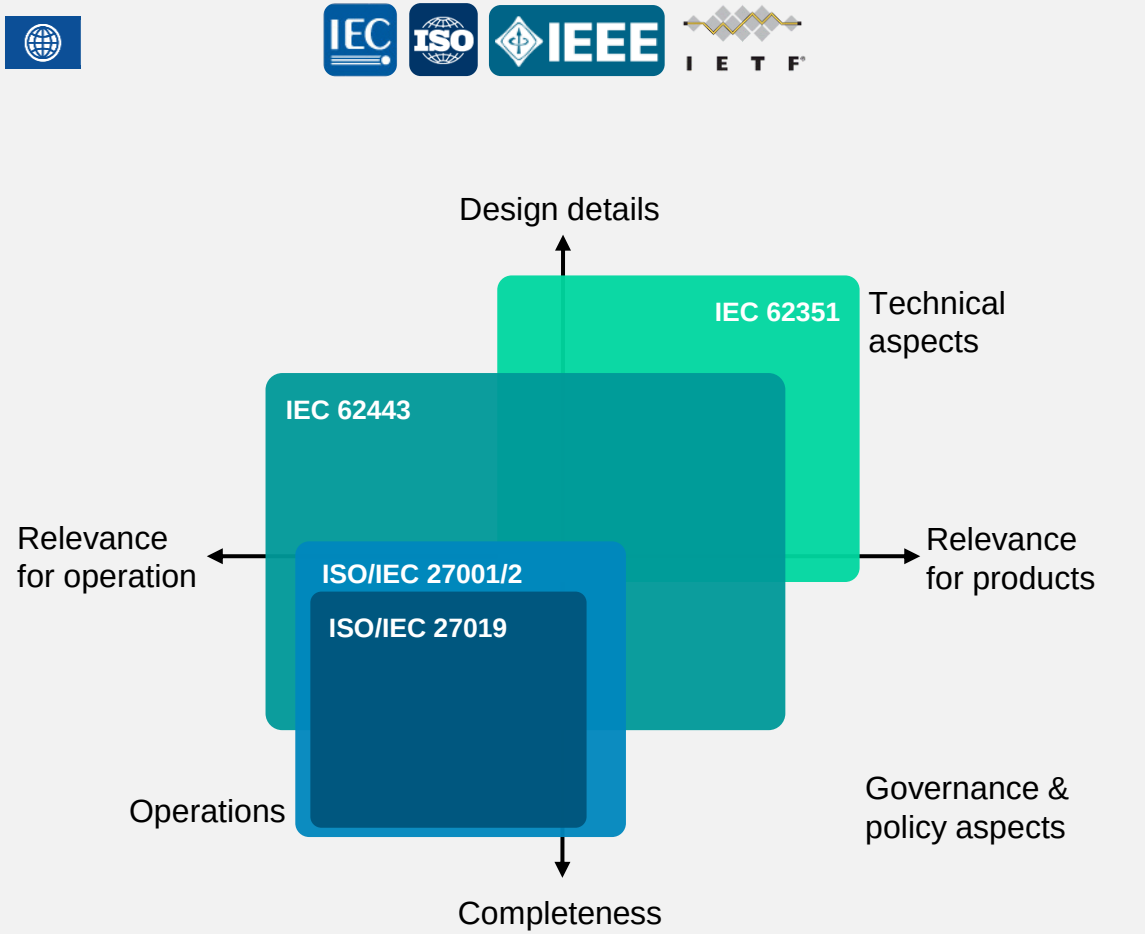
- IT Security Act
- B3S Standards
- BNetzA Security Catalogue
- German Energy Act

- Cyber Security Act (CSA)
- Network Information Security Directive (NIS2)
- Cyber Resilience Act (CRA)

- Critical Infrastructure Protection
- Certification and Key Measures

- Cyber Essential Scheme
- Direct adaptation of European NIS Directive and GDPR

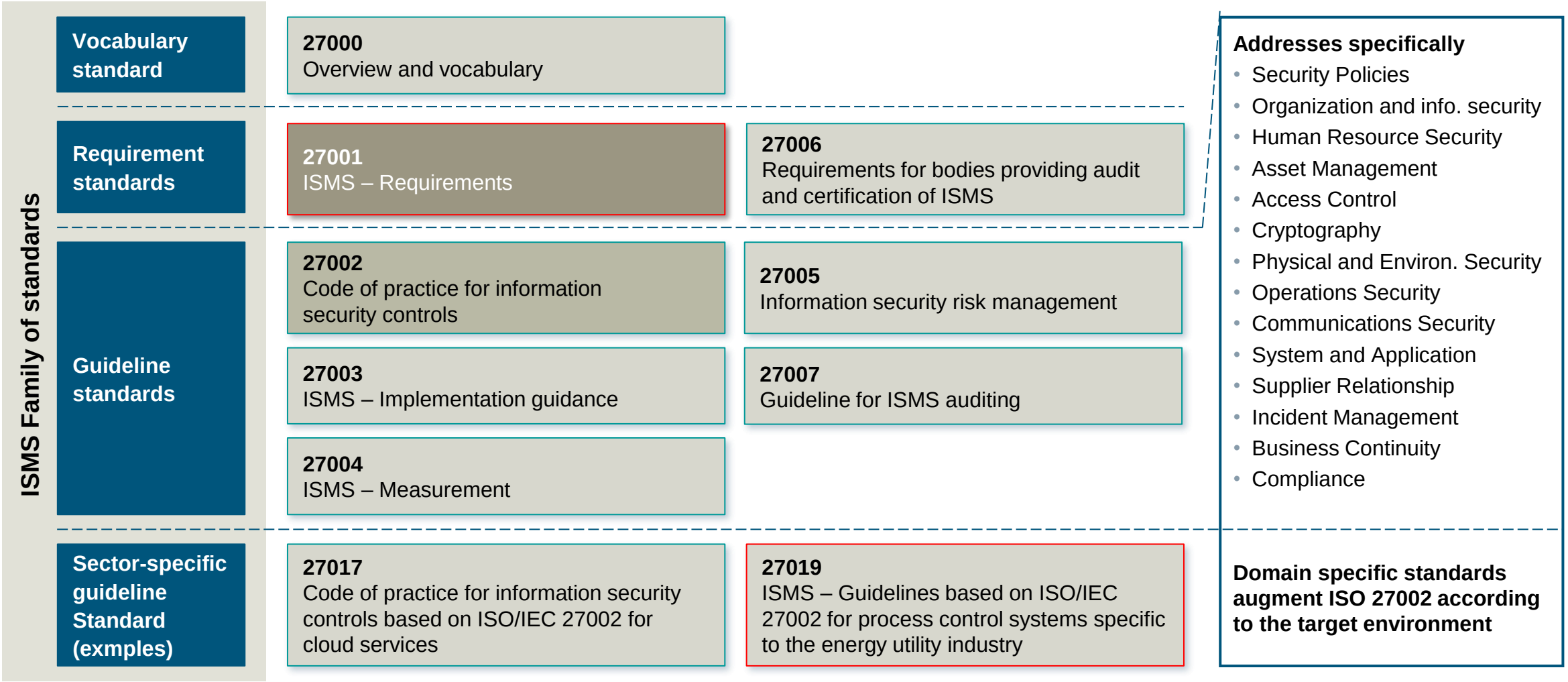
International Standards



Note: the stated organizations and standards are just examples and are not complete

ISO/IEC 270xx Series – Information Security Management System (ISMS)

Specifies security management requirements for manufacturers, operators, …

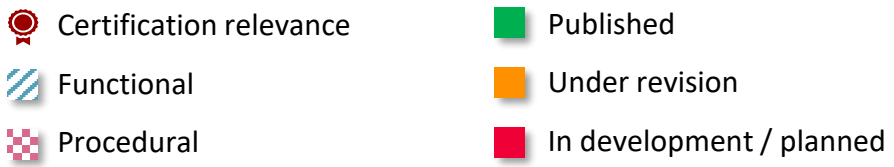


IEC 62443 – Security for Industrial Automation and Control Systems

Addresses the complete value chain from product manufacturing to operation

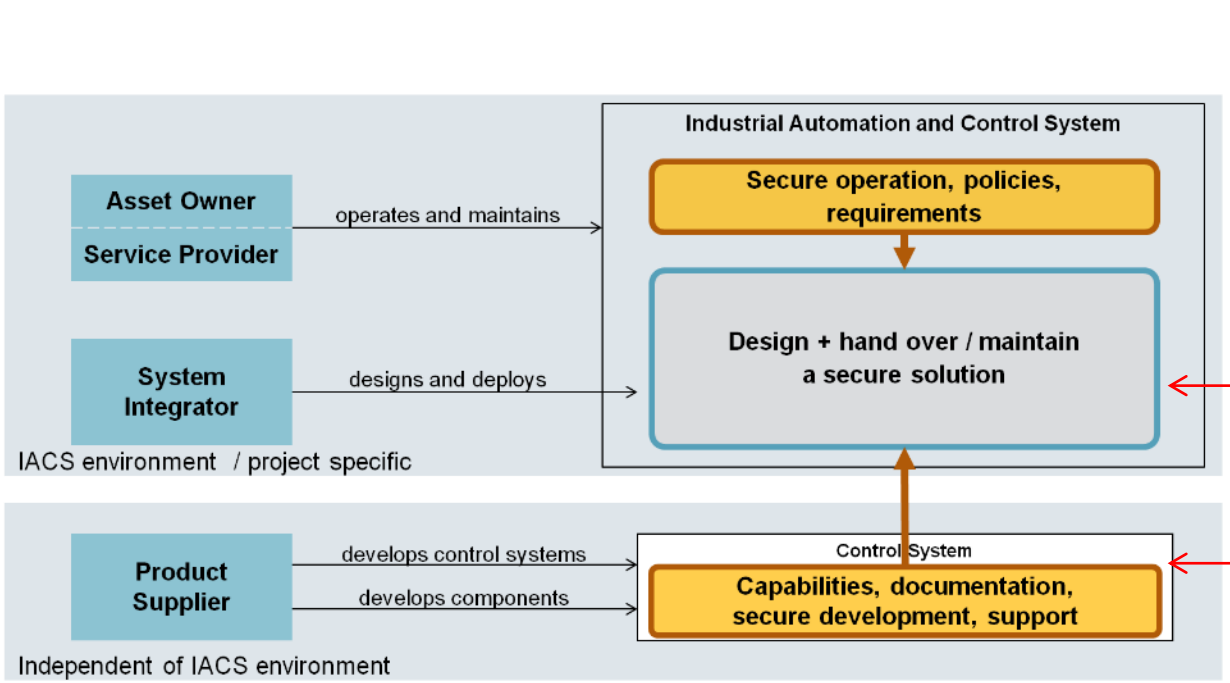
- Targets operator, integrator, and product supplier in terms of processes and security capabilities and allows for certification

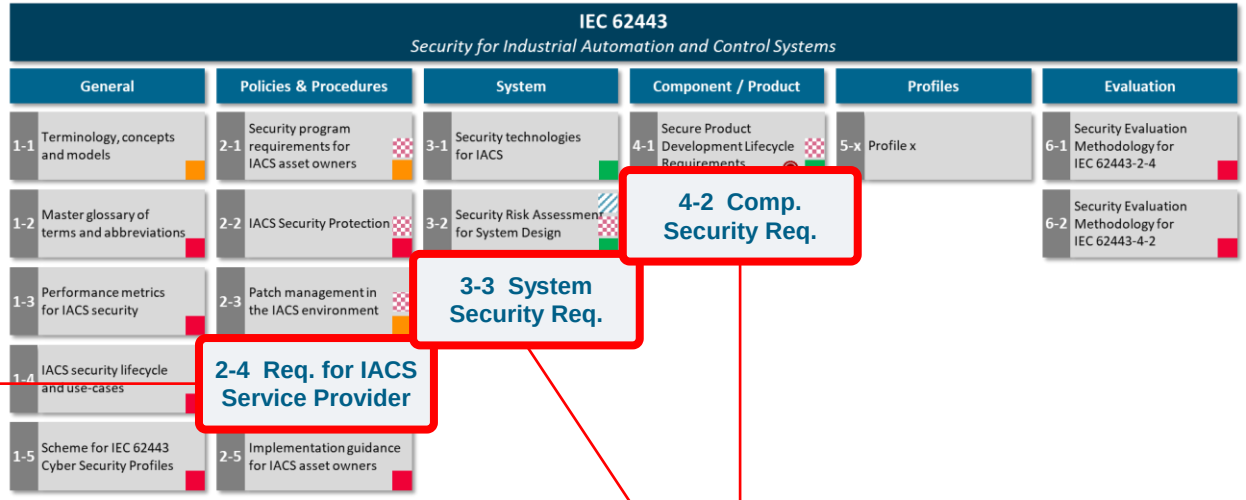
General	Policies & Procedures	System	Component / Product	Profiles	Evaluation
1-1 Terminology, concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Secure Product Development Lifecycle Requirements	5-x Profile x	6-1 Security Evaluation Methodology for IEC 62443-2-4
1-2 Master glossary of terms and abbreviations	2-2 IACS Security Protection	3-2 Security Risk Assessment for System Design	4-2 Technical security requirements for IACS components		6-2 Security Evaluation Methodology for IEC 62443-4-2
1-3 Performance metrics for IACS security	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels			
1-4 IACS security lifecycle and use-cases	2-4 Security program requirements for IACS service providers				
1-5 Scheme for IEC 62443 Cyber Security Profiles	2-5 Implementation guidance for IACS asset owners				

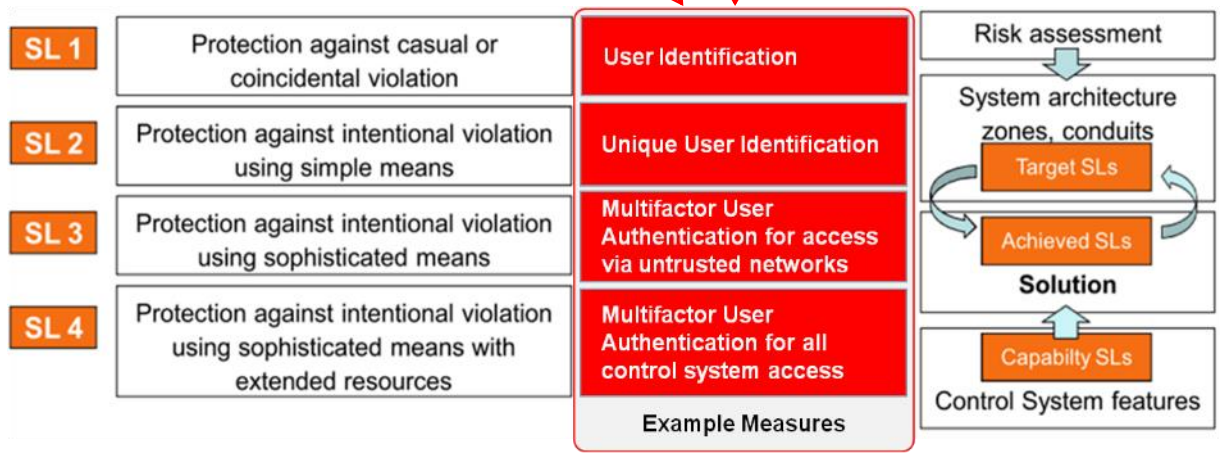


IEC 62443 – Security for Industrial Automation and Control Systems

Enables a graded security approach to achieve appropriate protection





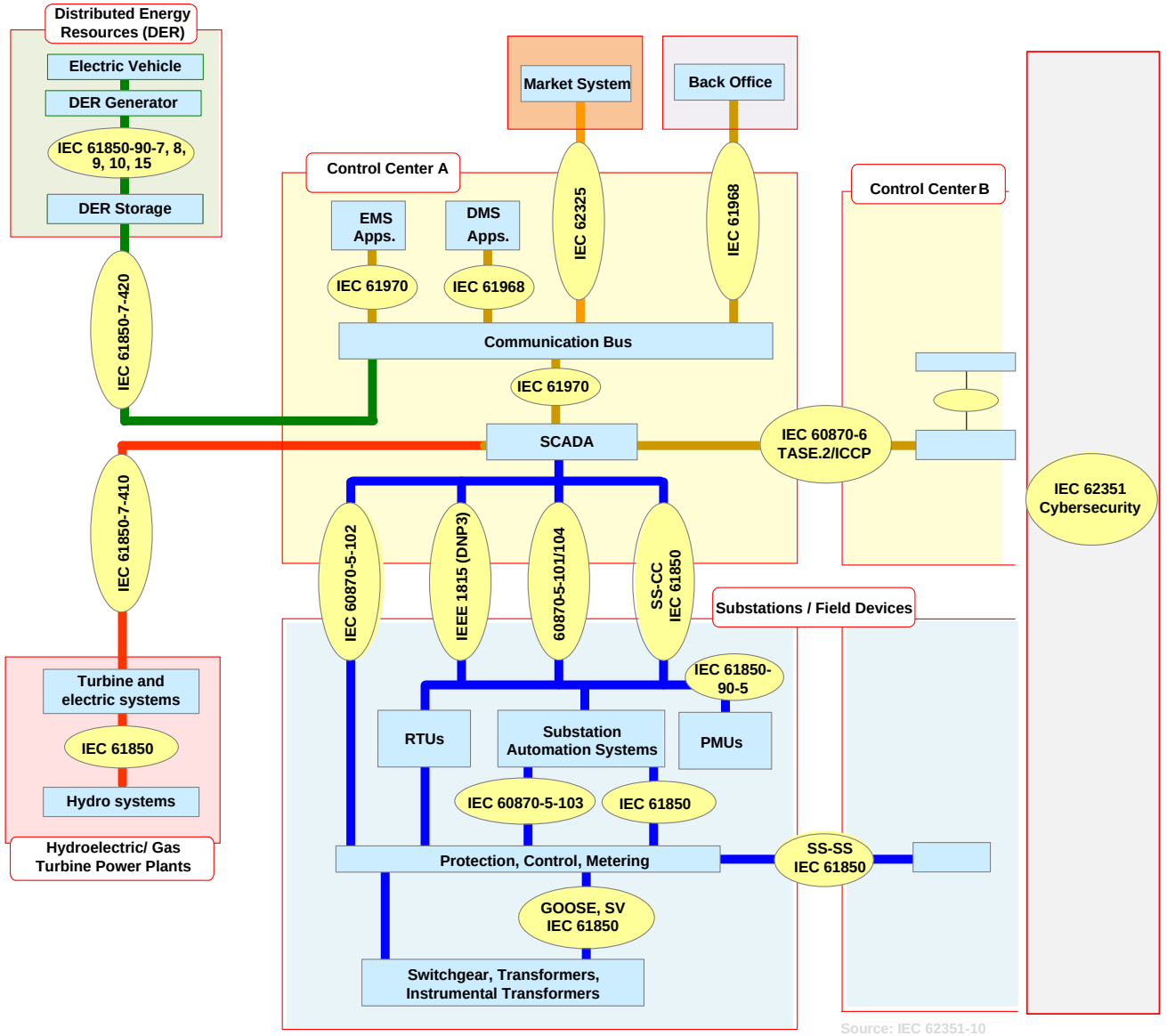


Core Communication Standards for Digital Grids

IEC TC57 defines the reference architecture with domain-specific cybersecurity

IEC TC57 WG15 Scope

- Development of IEC 62351 to secure communication protocols defined by IEC TC 57, specifically
  - IEC 60870-5 and IEC 60870-6 series,
  - IEC 61850 series,
  - IEC 61968 & IEC 61970 series.
- Focus on end-to-end security to ensure that data exchanged between a source (sender) and a sink (receiver) is protected from unauthorized access and/or modifications.
- Further parts address architecture and system aspects and support engineering and operation.
- Addressed in currently 18+ parts of IEC 62351 of different status



Cybersecurity provided with IEC 62351

Building blocks to address technical security requirements in Power Systems

Identity and Access Management

Identification, Authentication, Authorization (RBAC) of Users/Devices

Focus: Usage of X.509 certificates

Secure Communication

Between different actors on different layers (Ethernet, IP, serial)

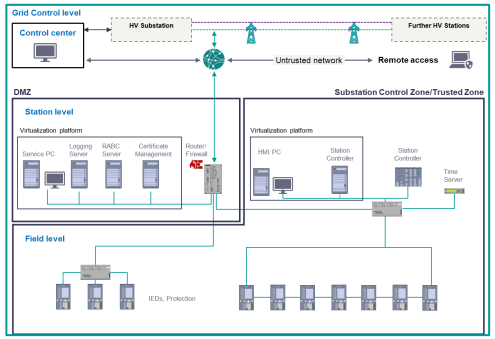
Focus: Profiling of existing standards (e.g., TLS) and definition of security enhancements if necessary

Monitoring and Audit

Logging and processing of security relevant events

Focus: Application of established standards like syslog and SNMP

IEC 62351



Key Management

Management of long term and session keys

Focus: Application of established certificate management (EST, SCEP) and key management (GDOI) protocols

Conformity Tests

Test case description for specified security measures in the different parts of IEC 62351 based on PICS statements

Focus: Specification of conformity test cases

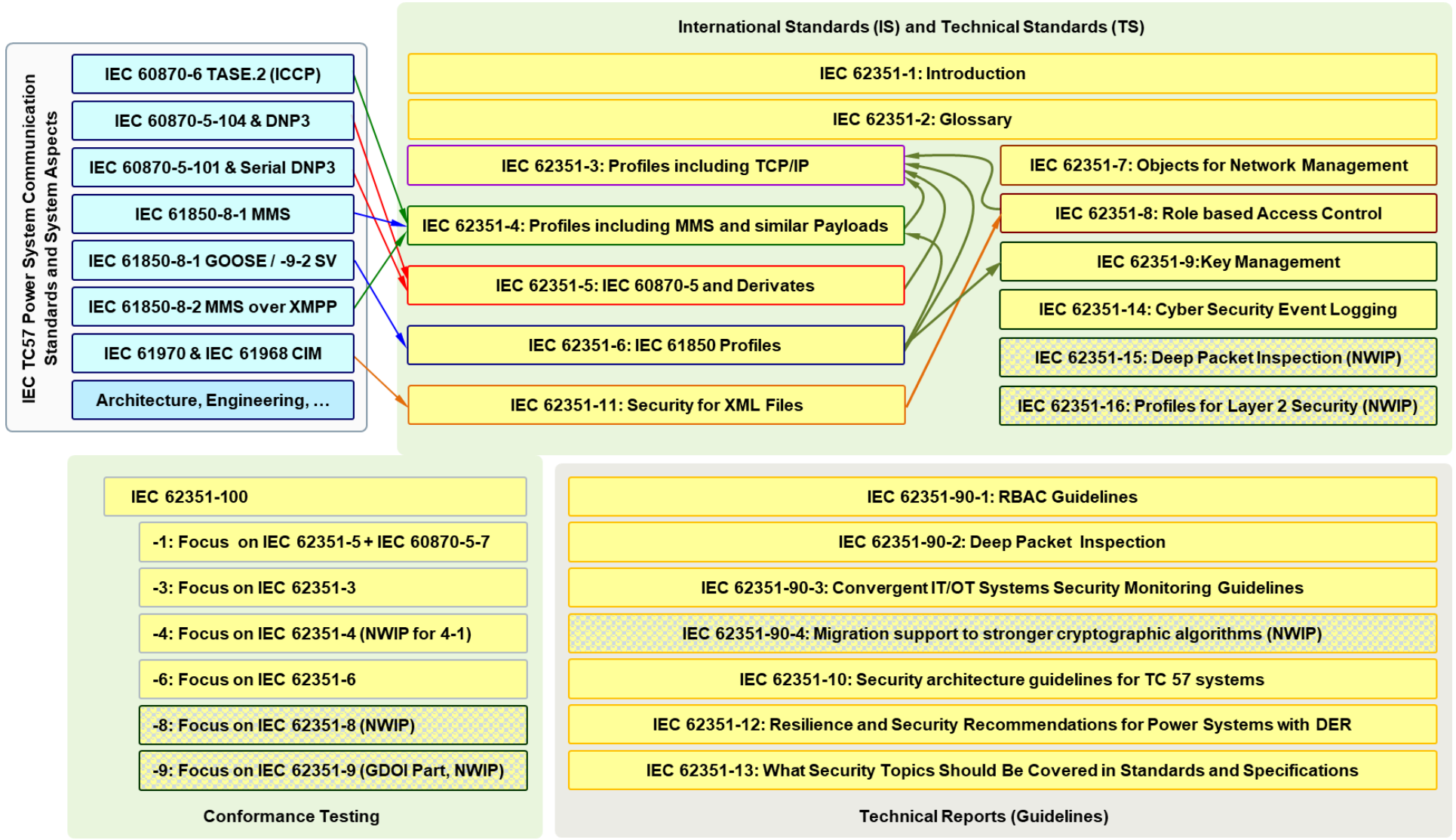
Guidelines

Guidance and support for securing power system

Focus: Examples for architectures, RBAC, monitoring, …

Cyber security in Digital Grids

IEC 62351 provides technical security measures and guidelines



Security means defined for

- Authentication and authorization (RBAC)
- Secure IP- based and serial communication
- Secure application level exchanges
- Security monitoring and event logging
- Test case definition
- Guidelines for applying specific security measures in power system architectures

by utilizing or profiling

- existing standards and recommendations

Different Security Standards meet in the Operational Environment

Application of IEC 62351 in a digital substation

Specification of technical solutions for an infrastructure supporting certificate based authentication and authorization (PKI, RBAC)

IEC 62351-8/9

Monitoring & Audit Adaptation and enhancement of existing infra-structures and technologies for network management using SNMP and syslog

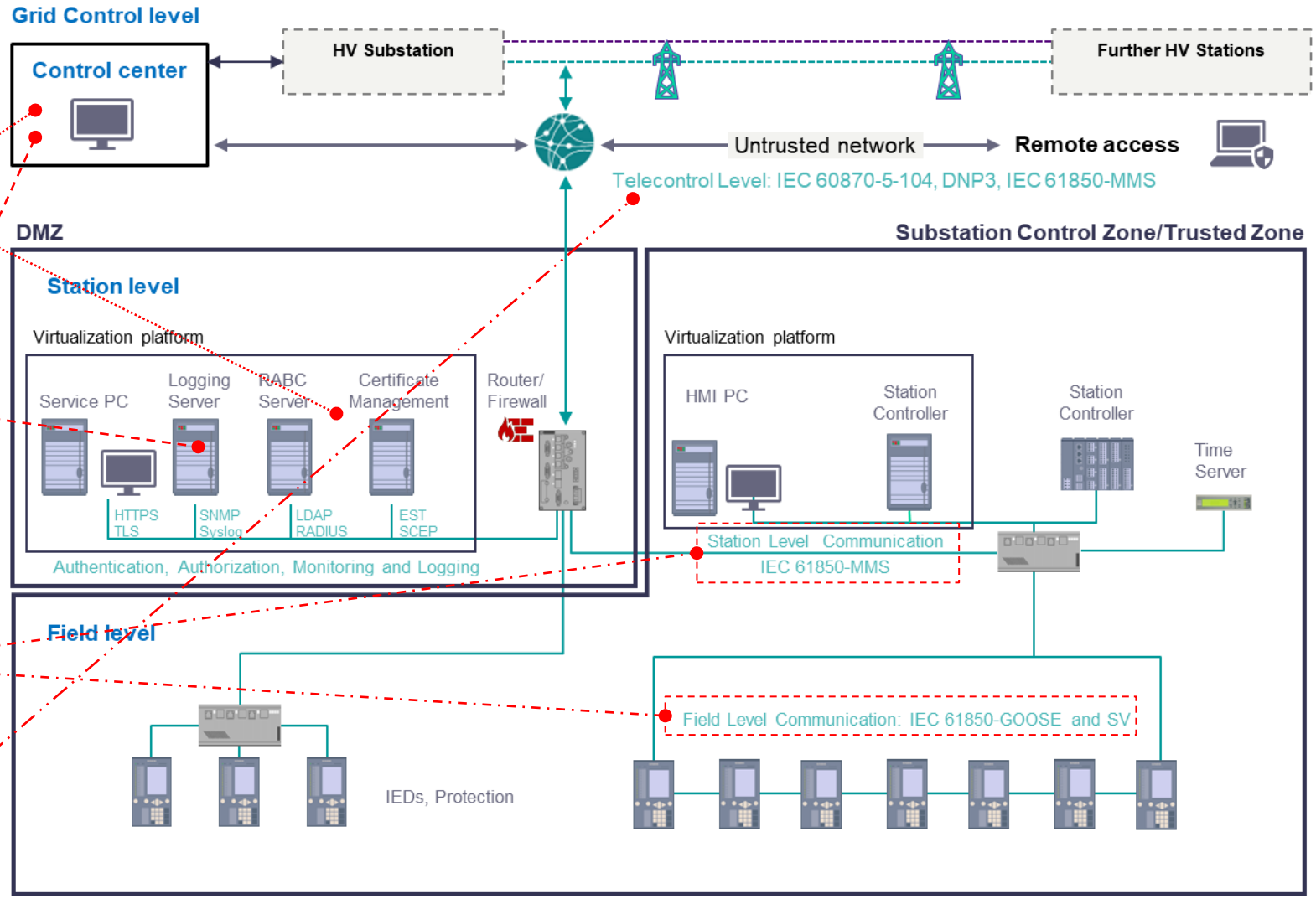
IEC 62351-7/14

Protection of process level and field level communication with real-time constraints using appropriate security measures

IEC 62351-3/4/5/6/9

Securing telecontrol and control center communication using TLS and / or security measures on application level

IEC 62351-3/4/5/9



Summary: Cybersecurity for Power System Automation

Interplay of ISO/IEC 27001 / IEC 62443 / IEC 62351

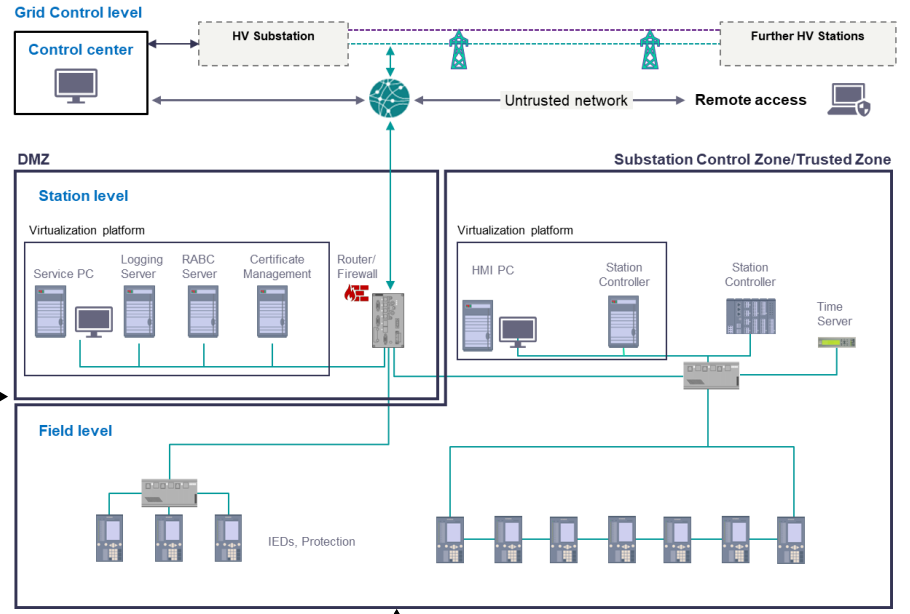
Cyber Security regulation are provided for instance by
- European NIS Directive and derived country specific laws
- US FERC for North America

ISO/IEC 27001

Asset Owner Operator — IT Infrastructure — **ISO/IEC 27001**, **ISO/IEC 27019**

Integrator — IT Infrastructure — **IEC 62443-2-4**, **IEC 62443-3-3**, **IEC 62351**

Product Supplier — IT Infrastructure — **IEC 62443-3-3**, **IEC 62443-4-2**, **IEC 62443-4-1**, **IEC 62351**



OT - Infrastructure

Procedural: e.g.: ISMS for operator, or requirements for the development process for integrators and manufacturers

Functional: e.g., security levels, strength of security measures

Technical: e.g., security measures implementation, support interoperability

Contact

Steffen Fries
Principal Key Expert

T CST
Otto-Hahn-Ring 6
81739 Munich
Germany

E-mail steffen.fries@siemens.com

Siemens Grid Security

Siemens Cyber Security

SIEMENS

Information

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Security note

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic Industrial Security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art Industrial Security concept. Third-party products that may be in use should also be considered. For more information on Industrial Security, visit:

siemens.com/industrial-security

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit

support.automation.siemens.com

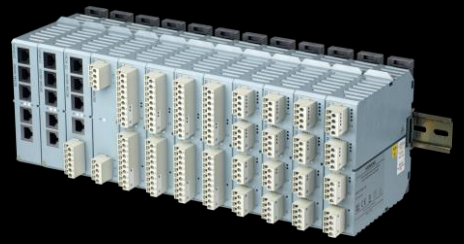
Cybersecurity in the Power Grid
Security by Design in Products

Signed software/firmware

Protection against firmware/software manipulation

Firewall & VLAN

Separation of Ethernet traffic over integrated firewall & VLAN

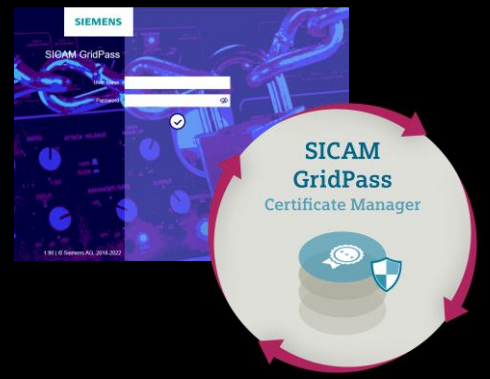


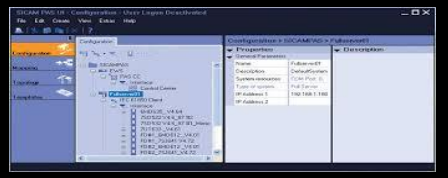
Security Logging

Non-volatile persistence of security audit trail and transfer over Syslog

RBAC with central user management

Centrally manage users and assign roles for authorization (based on IEC 62351-8)





BDEW Whitepaper and IEC 62443 conformity

Fulfils recommendations for control and communication systems security

Certificate Management

Easy X.509 certificate management with SICAM GridPass

Gateway Features in SICAM A8000 & PAS

- VPN & TLS security
- Secure IEC 80670-5-104, IEC 61850, DNP3i
- Hardware-based application layer firewall in SICAM A8000
- Intrusion Detection

IEC 62351 – Overview and Status

04/2023

IEC 62351 Part	Release	Notes and Activities	Status as of January 2023 (Completed, Pending, submission date)
IEC/TS 62351-1: Introduction	05/2007	May need to be updated – Assessment started	No revision planned, but assessment started
IEC/TS 62351-2: Glossary of terms	08/2008	Link to document	Pending – no specific date – additions assessed.
IEC/IS 62351-3: Security for profiles including TCP/IP	Ed.1.2: 02/2020 Ed.2:	FDIS edition 2 provided to IEC	RR Ed.2 IS 11/2020, CD 07/2021, CDV 03/2022, FDIS 12/2022, IS 05/2023
IEC/IS 62351-4: Security for profiles including MMS and derivatives	Ed.1.1: 07/2020	IS in 11/2018, AMD #1 (Ed 1.1)	IS Ed1.1 07/2020 with code components
IEC/IS 62351-5: Security for IEC 60870-5 and derivatives	TS: 2013 Ed.1: 01/2023	Note that IS Ed.1 is not backward compatible to TS	IS 01/2023
IEC/IS 62351-6: Security for IEC 61850 profiles	TS: 01/2007 Ed. 1: 10/2020		IS 10/2020
IEC/IS 62351-7: Network and System Management data object models	Ed.1: 07/2017	Revision to edition 2 ongoing	Ed.2 RR 03/2022, CD 02/2023, CDV 09/2023
IEC/IS 62351-8: Role-Based Access Control	Ed.1: 04/2020	RR for edition 2 in preparation	CD 02/2024
IEC/IS 62351-9: Key Management	Ed.1: 05/2017 Ed.2:	FDIS edition 2 provided to IEC	RR Ed.2 IS 02/2020, CD 12/2020, CDV 12/2021, FDIS 11/2022, IS 05/2023
IEC/TR 62351-10: Security Architecture	10/2012		TR 10/2012
IEC/IS 62351-11: Security for XML Files	09/2016		IS 9/2016
IEC/TR 62351-12: Resilience + Security Rec. for Power Systems with DER	04/2016		TR 4/2016
IEC/TR 62351-13: Guidelines on Security Topics in Standards and Specs	08/2016		TR 8/2016
IEC/IS 62351-14 Cyber Security Event Logging	CD	CDV in preparation	NWIP 06/16, CD 10/2019, CD2 02/2021, CD3 12/2021, CDV 07/2023, FDIS 10/2023, IS 06/2024
IEC/IS 62351-15 Deep Packet Inspection	NWIP	will be based on IEC 62351-90-2, NWIP sent to IEC	NWIP 10/2022, TS 10/2024
IEC/IS 62351-16 Profiles for Layer 2 Security, MACsec	NWIP	NWIP sent to IEC	NWIP 12/2022
IEC/TR 62351-90-1: Guidelines for Using Part 8 Roles	01/2018	contained in Part 8	TR 1/2018
IEC/TR 62351-90-2 Deep Packet Inspection	09/2018		TR 9/2018
IEC/TR 62351-90-3 Guidelines for Network Management	03/2021		TR 03/2021
IEC/TR 62351-90-4: Migration support to stronger cryptographic algorithms	WD	PWI and CD in preparation	
IEC/TS 62351-100-1: Conformance testing IEC 62351-5 and IEC 60870-5-7	11/2018	RR in preparation	RR 02/2023, TS 06/2024
IEC/TS 62351-100-3: Conformance testing IEC 62351-3	01/2020	Preparation of Ed. 2 following Ed.2 of IEC 62351-3	RR 11/2022, TS 03/2024
IEC/TS 62351-100-4: Conformance testing for 62351-4 with IEC 61850	DTS	Conformance testing for IEC 61850 client-server	NWIP 5/2018, CD 03/2021, CD2 10/2021, DTS 12/2022, TS 07/2023
IEC/TS 62351-100-4-1: Conformance testing for 62351-4 A-Profile	NWIP	NWIP being prepared	NWIP 12/2022
IEC/TS 62351-100-6: Conformance testing for 62351-6 with IEC 61850-8-1 and 61850-9-2	08/2022	Conformance testing for IEC 61850 GOOSE, SV	TS 06/2022
IEC/TS 62351-100-8: Conformance testing for IEC 62351-8	NWIP	NWIP in preparation	
IEC/TS 62351-100-9: Conformance testing for IEC 62351-9	NWIP	In Preparation, Clarification if one/multiple documents	
Application Note: Vol 1 General security and IEC 62351 descriptions, Vol 2 "What" to "How" using 62351, Vol 3 Application examples for how best to use the IEC 62351 series	White Paper	Motivation and application use cases for IEC 62351 series, development ongoing	Multi-Volume Application Note
Related secifications			
IEC/TR 61850-90-19: Using RBAC and IEC 61850 (joint with WG10)	DC2	Joint effort with WG10, discussion to convert to IS	Up to WG10: DC1 3/2020, DC2 5/2021, CD ??/2023
IEC/TR 60870-5-7: Security for IEC 60870-5-101/104 (WG3)	WD	Joint effort with WG10, discussion to convert to IS	CD 07/2023, DTS 07/2024