Congress 2024, June 30, 2024 to July 04, 2024 - Porto, Portugal

Addressing Cybersecurity in Power Systems

From requirements to solutions

Steffen Fries, Siemens, T CST

July 2, 2024

Abstract

Critical infrastructures, taking power systems as one prominent example, are required to obey to specific regulatory requirements regarding their secure reliable and resilient operation. Utilities for instance need to obey the European Network and Information Security Directive (since 2023 the successor, the EU- NIS2 Directive, is in force). In addition, the EU Cyber Resilience Act (EU-CRA) is currently in finalization, posing security requirements to the product manufacturers directly.

To cope with these requirements, different standard (frameworks) have been developed. They address technical and procedural requirements as well as technical specifications to ensure interoperability between different vendors products. Moreover existing standards are renewed or enhanced to address upcoming requirements and advances in cybersecurity.

The presentation provides an overview of regulative requirements and solution standards ensuring secure operation of the electrical infrastructure. Besides this, examples are provided for challenges, requiring further investigation and solution discussion and development.

Businesses and Services of Siemens AG

Industrial Business

Digital Industries

Smart Infrastructure

Mobility

Siemens Healthineers[1]

Portfolio Companies

Siemens Advanta

Services

Siemens Financial Services

Siemens Real Estate

Global Business Services

[1] Publicly listed subsidiary of Siemens; Siemens' share in Siemens Healthineers is 75%

SIEMENS

Charter of Trust
A joint initiative for a secure sustainable digital world

aes Allianz Atos BOSCH

DELL Technologies IBM Infineon

Microsoft MITSUBISHI HEAVY INDUSTRIES, LTD. msc

NXP SIEMENS TotalEnergies TÜV SÜD

Charter of Trust

charteroftrust.com

Associated Partner Forum

Bundesamt für Sicherheit in der Informationstechnik | Canadian Centre for Cyber Security | CEBRI | CCN Centro Criptológico Nacional

certmeg | CR2 | csa cloud security alliance | CSIR

CyberPeace Institute | Cyber Readiness Institute | Global Cyber Alliance | HPI Hasso Plattner Institut

METI | MIC 総務省 | Tecnológico de Monterrey | TU Graz

01

Protect the data of individuals and businesses

02

Prevent damage to people, businesses, and infrastructure

03

Build trust in the digital world

Company Core Technologies

Innovation examples

Simcenter ROM Builder

- Creation of simplified, tool-neutral and reusable models by processing simulation and field data
- Model generation accelerated (up to real-time), interoperable, and deployable from simulation to edge and cloud

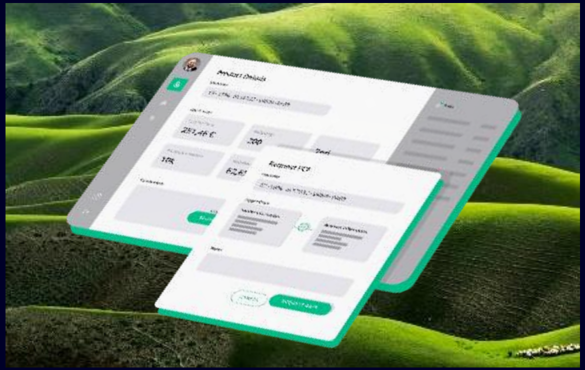
SINEC Security Monitor

- Software for non-intrusive asset and vulnerability detection and AI-based anomaly detection for industrial production networks
- Continuous on-prem securityy monitoring during production
- Supports implementation of NIS2
- Internally developed and used core technology – now available for customers

Reliable power with renewable generation

- Assistant for power system operation with up to 100% renewable peak generation
- Collaborative stabilization and resilience of entire island grids (e.g. Hawaii)
- Capacity can be scaled up to a range between 100 MW and 100 GW

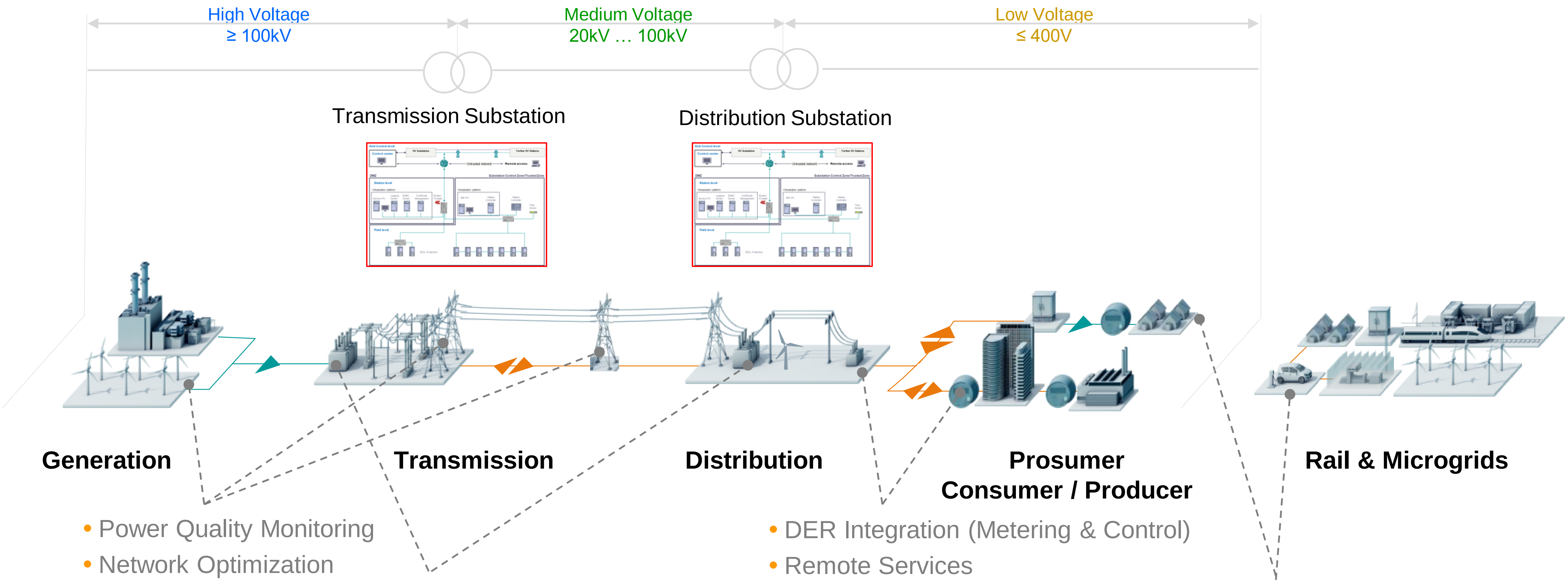
SiGREEN



- Trustworthy exchange of actionable Product Carbon Footprints throughout value chains
- Use of verifiable credentials ensures transparency, confidentiality, and data control in supply chains

Digital Grid – a Critical Infrastructure in Need of Protection

Power system value chain and use case examples



High Voltage
≥ 100kV

Medium Voltage
20kV … 100kV

Low Voltage
≤ 400V

Transmission Substation

Distribution Substation

Generation

Transmission

Distribution

Prosumer Consumer / Producer

Rail & Micr̄ogrids

- Power Quality Monitoring
- Network Optimization

- Substation Automation
- Inter Control Center Communication
- Remote Maintenance and Service

- DER Integration (Metering & Control)
- Remote Services

- Connecting Electric Vehicles to the Charging Infrastructure

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

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

1970s
Home computer is introduced

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

1990s
Digital enhancement of electrification and automation

1991
The World Wide Web becomes publicly accessible

1999
The globe is connected by the internet

2000s
Mobile flexibility

2010s
Cloud computing enters the mainstream

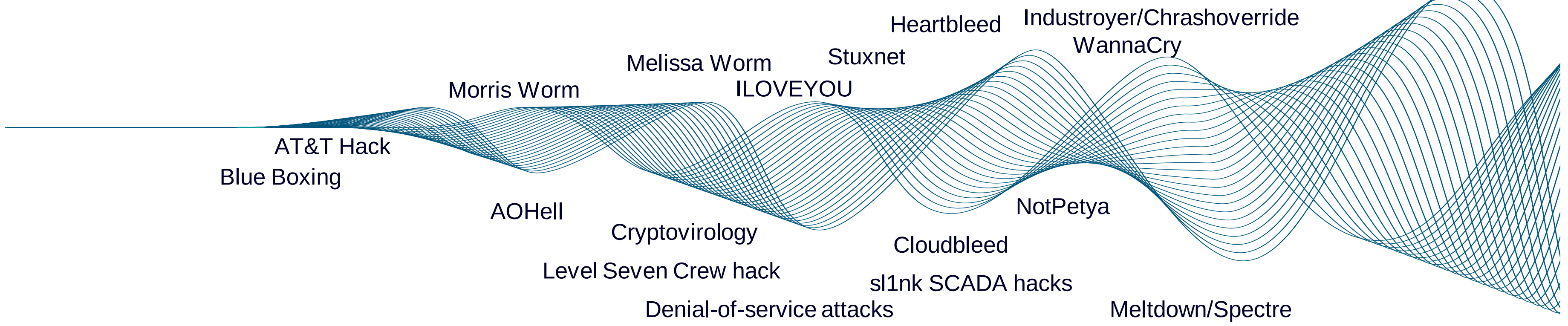
2020s
Internet of Things, Smart and autonomous systems, Artificial Intelligence, Big Data

2020s
Industry 4.0

Digital Information Processing

Digital Connectivity

Digital Automation and Artificial Intelligence



To prevent potential blackouts, a holistic cybersecurity approach is necessary!

How to provide appropriate cybersecurity?

Cybersecurity needs a holistic methodology

Recover

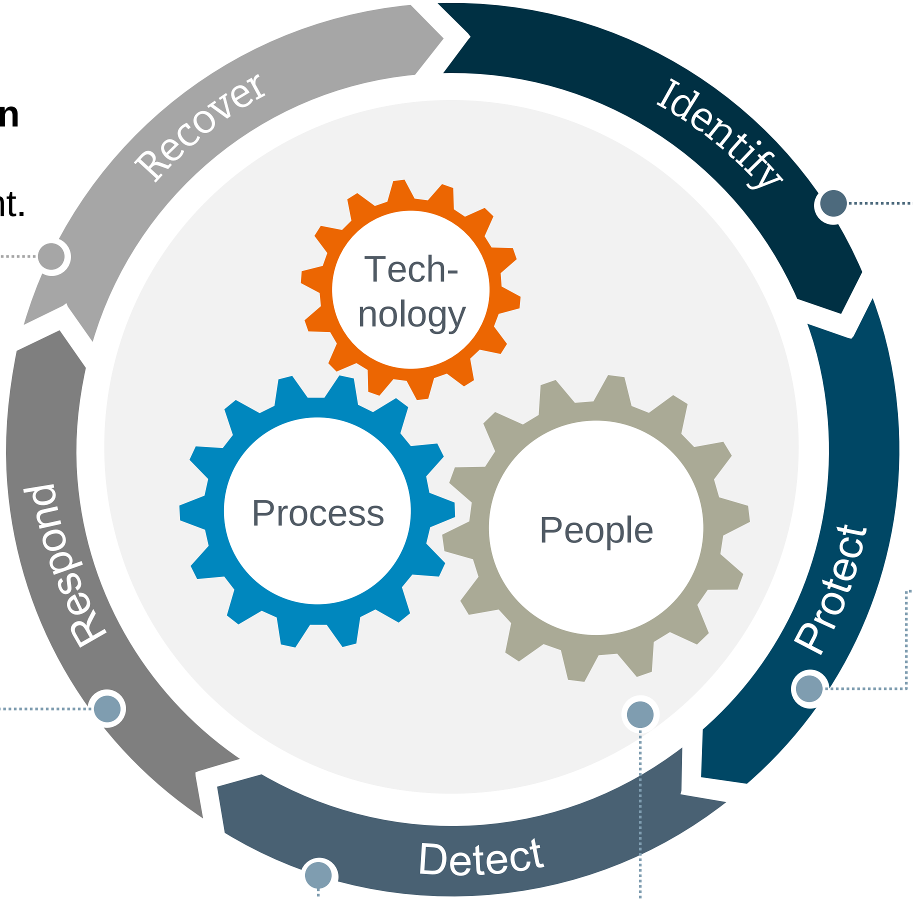
Creating plans for **resilience and restoration** of any capabilities or services that were impaired due to a cyber security related event.

Respond

Taking action against detected cyber security related events. Supports the ability to contain the impact of a potential event.

Detect

Rapid **identification** of the occurrence of a cyber security related event.



Identify

Understanding the business context, the resources that support critical functions and the related cyber security risks.

Protect

Protection of critical infrastructure service, e.g., energy supply by safeguarding the overall system.

Govern

Cybersecurity strategy development and maintenance in the organizational context

Approach aligns with the NIST Cyber Security Framework

Regulative Requirements stipulate Development of Standards to foster Interoperability and to enable Conformity Assessment of Security Features

Regulative Requirements

- Critical Infrastructure Protection (NERC CIP)
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity
- Executive Order 14028: Improving Nation’s Cyber Security

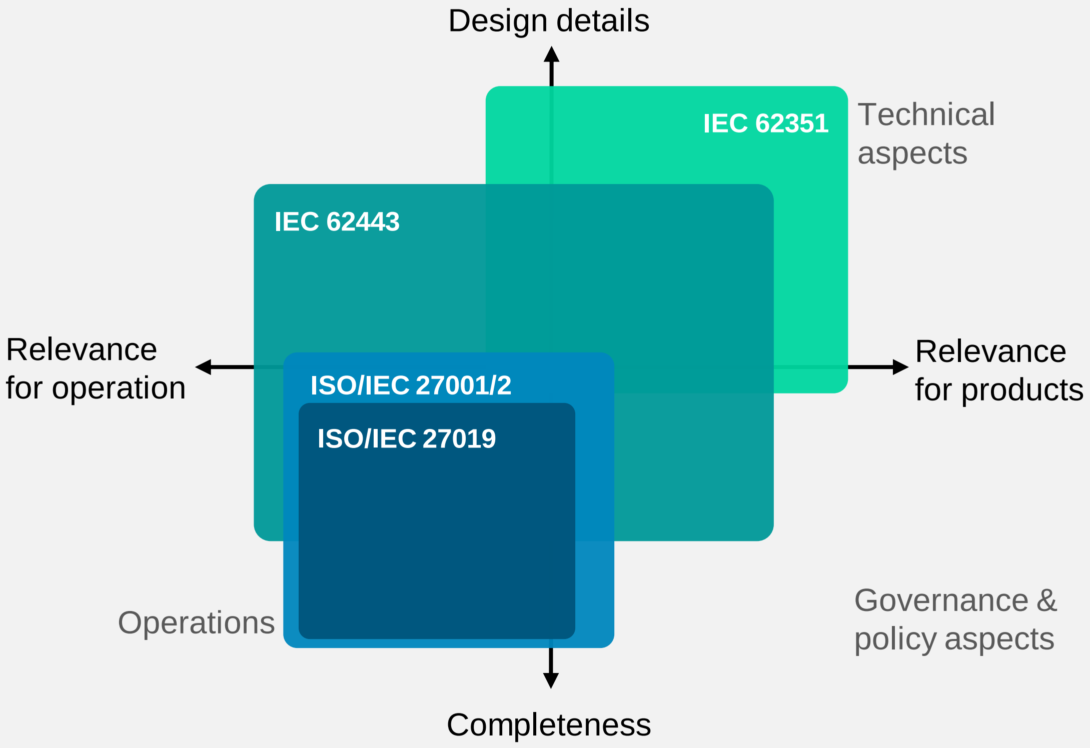
- IT Security Act
- B3S Standards for dedicated critical infrastructure domain
- BNetzA Security Catalogue
- German Energy Act

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

- ANSSI: Critical Infrastructure Protection
- Certification and Key Measures

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

International Standards



Design details

IEC 62351

Technical aspects

IEC 62443

Relevance for operation

Relevance for products

ISO/IEC 27001/2

ISO/IEC 27019

Operations

Governance & policy aspects

Completeness

Note: the stated organizations and standards are considered the most important for power system automation but are not complete

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

Specifies security management requirements for manufacturers, operators, …

ISMS Family of standards

Vocabulary standard

27000
Overview and vocabulary

Requirement standards

27001
ISMS – Requirements

CERTIFICATE

SIEMENS

27006
Requirements for bodies providing audit and certification of ISMS

Guideline standards

27002
Code of practice for information security controls

27005
Information security risk management

27003
ISMS – Implementation guidance

27007
Guideline for ISMS auditing

27004
ISMS – Measurement

Sector-specific guideline Standard (exmples)

27017
Code of practice for information security controls based on ISO/IEC 27002 for cloud services

27019
ISMS – Guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

Addresses specifically

- Security Policies
- Organization and info. security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environ. Security
- Operations Security
- Communications Security
- System and Application
- Supplier Relationship
- Incident Management
- Business Continuity
- Compliance

Domain specific standards augment ISO 27002 according to the target environment

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 🟥				
1-6 Application of IEC 62443 to the Industrial Internet of Things 🟥					

Selected Certificates issued to Siemens

CERTIFICATE
No. IITS1 062845 0004 Rev. 00
Holder of Certificate: Siemens AG SI DG
Certification Mark:
Type: Industrial IT Security
Scope of Certificate: ICS Security Service Provider
Date: 2020-11-04

CERTIFICATE
No. IITS2 062845 0005 Rev. 00
Holder of Certificate: Siemens AG SI DG
Certification Mark:
Product Type: Industrial IT Security
Model(s): Security Program for the "Blueprint Secure Substation"
Date: 2020-11-04

IEC IECEE
Certificate of Conformity – Industrial Cyber Security Capability
TÜVNORD

🏅 Certification relevance

▨ Functional

▦ Procedural

🟩 Published

🟧 Under revision

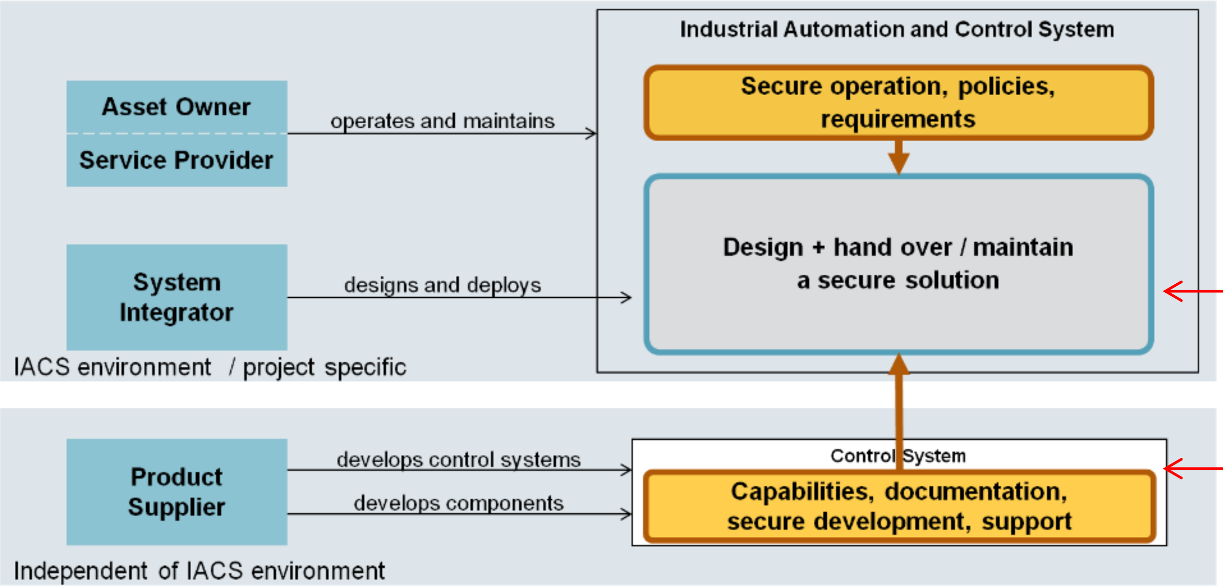
🟥 In development / planned

SIEMENS

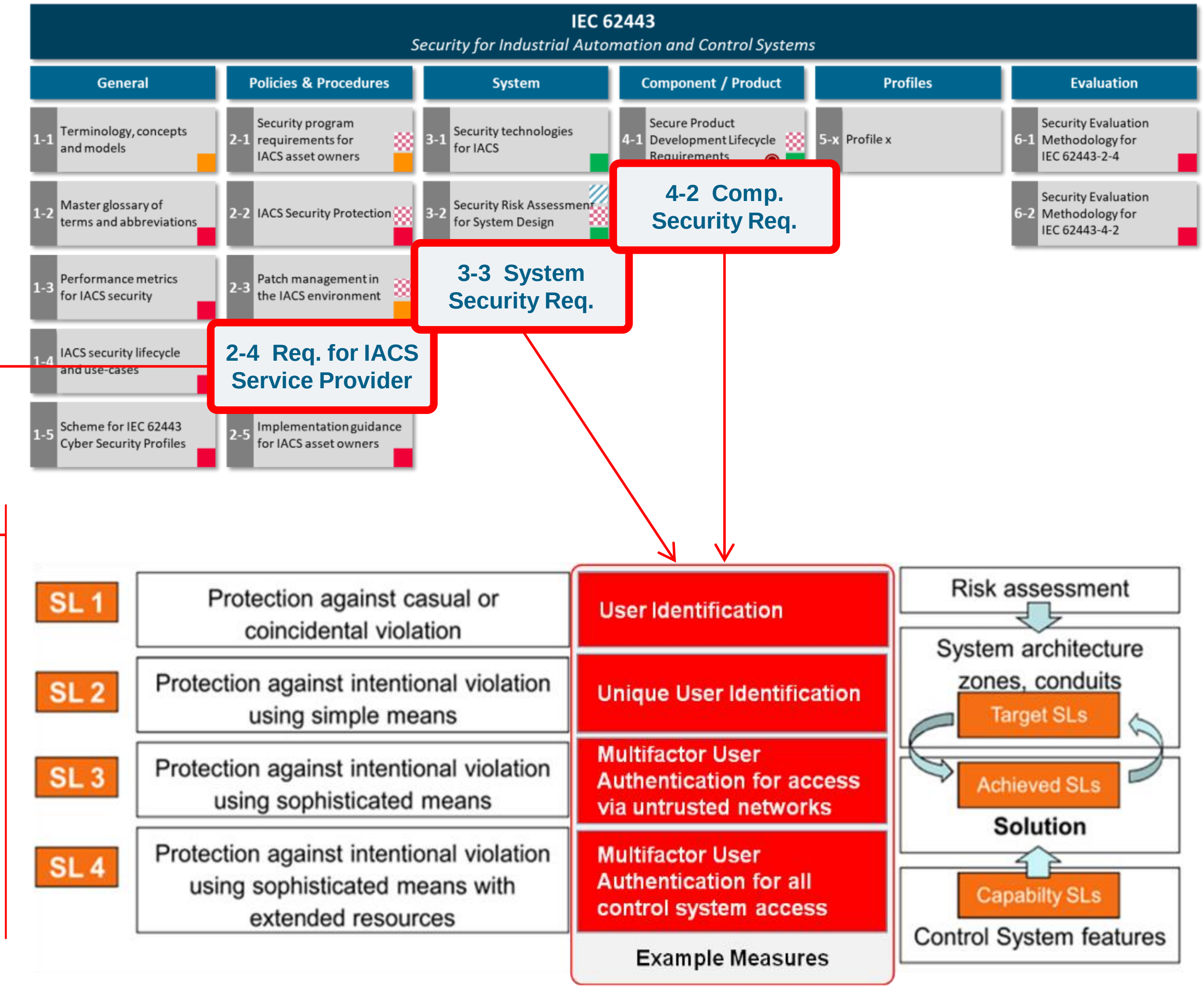
IEC 62443 – Security for Industrial Automation and Control Systems

Enables a graded security approach to achieve appropriate protection

example



Industrial Automation and Control System
Asset Owner
Service Provider
operates and maintains
Secure operation, policies, requirements
System Integrator
designs and deploys
Design + hand over / maintain a secure solution
IACS environment / project specific
Product Supplier
develops control systems
develops components
Control System
Capabilities, documentation, secure development, support
Independent of IACS environment



IEC 62443
Security for Industrial Automation and Control Systems

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 Comp. Security Req.		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 Req.			
1-4 IACS security lifecycle and use-cases	2-4 Req. for IACS Service Provider				
1-5 Scheme for IEC 62443 Cyber Security Profiles	2-5 Implementation guidance for IACS asset owners				

		Example Measures
SL 1	Protection against casual or coincidental violation	User Identification
SL 2	Protection against intentional violation using simple means	Unique User Identification
SL 3	Protection against intentional violation using sophisticated means	Multifactor User Authentication for access via untrusted networks
SL 4	Protection against intentional violation using sophisticated means with extended resources	Multifactor User Authentication for all control system access

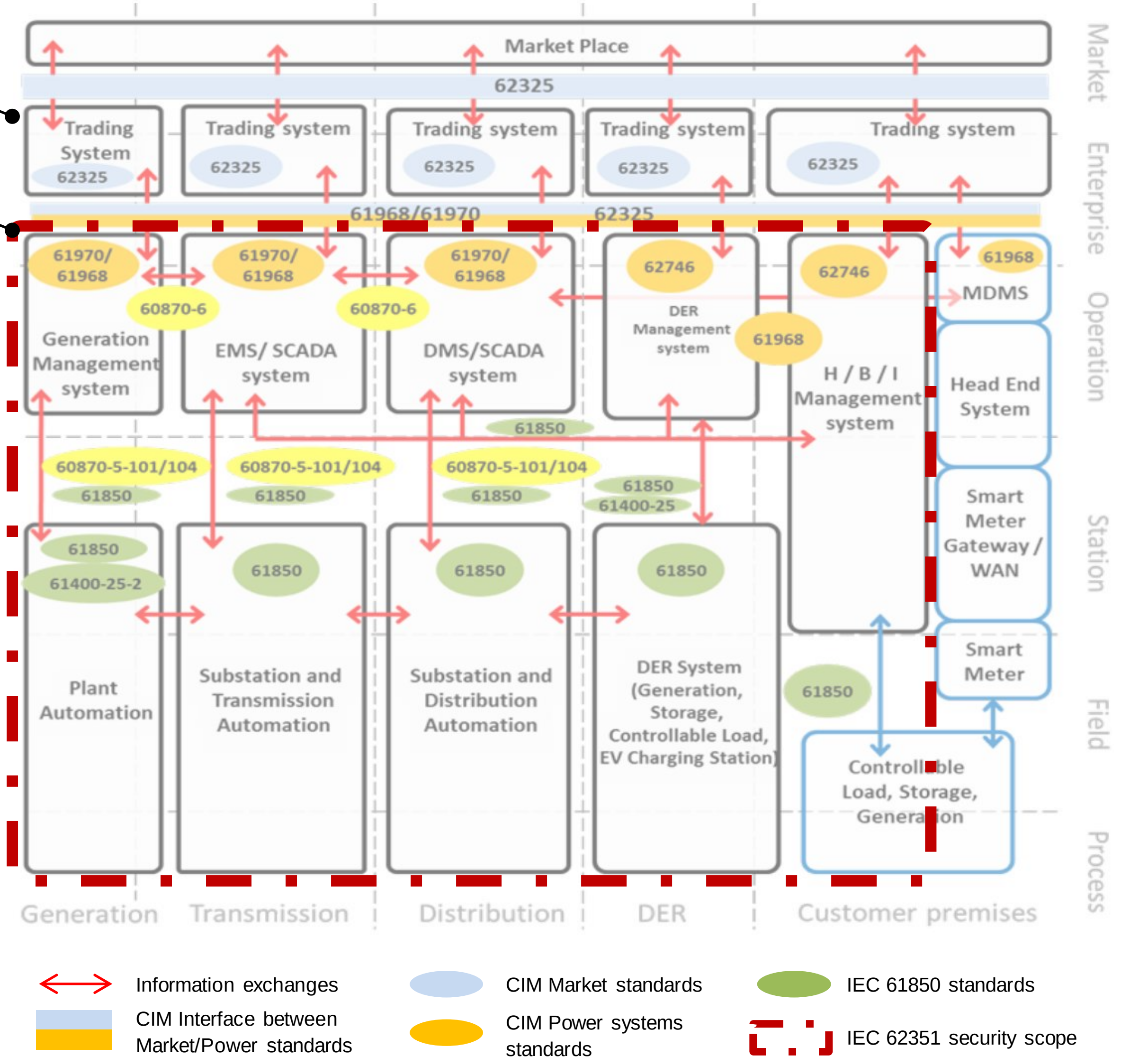
SIEMENS

Core Communication Standards for Digital Grids

IEC TC57 defines the reference architecture including domain-specific cybersecurity

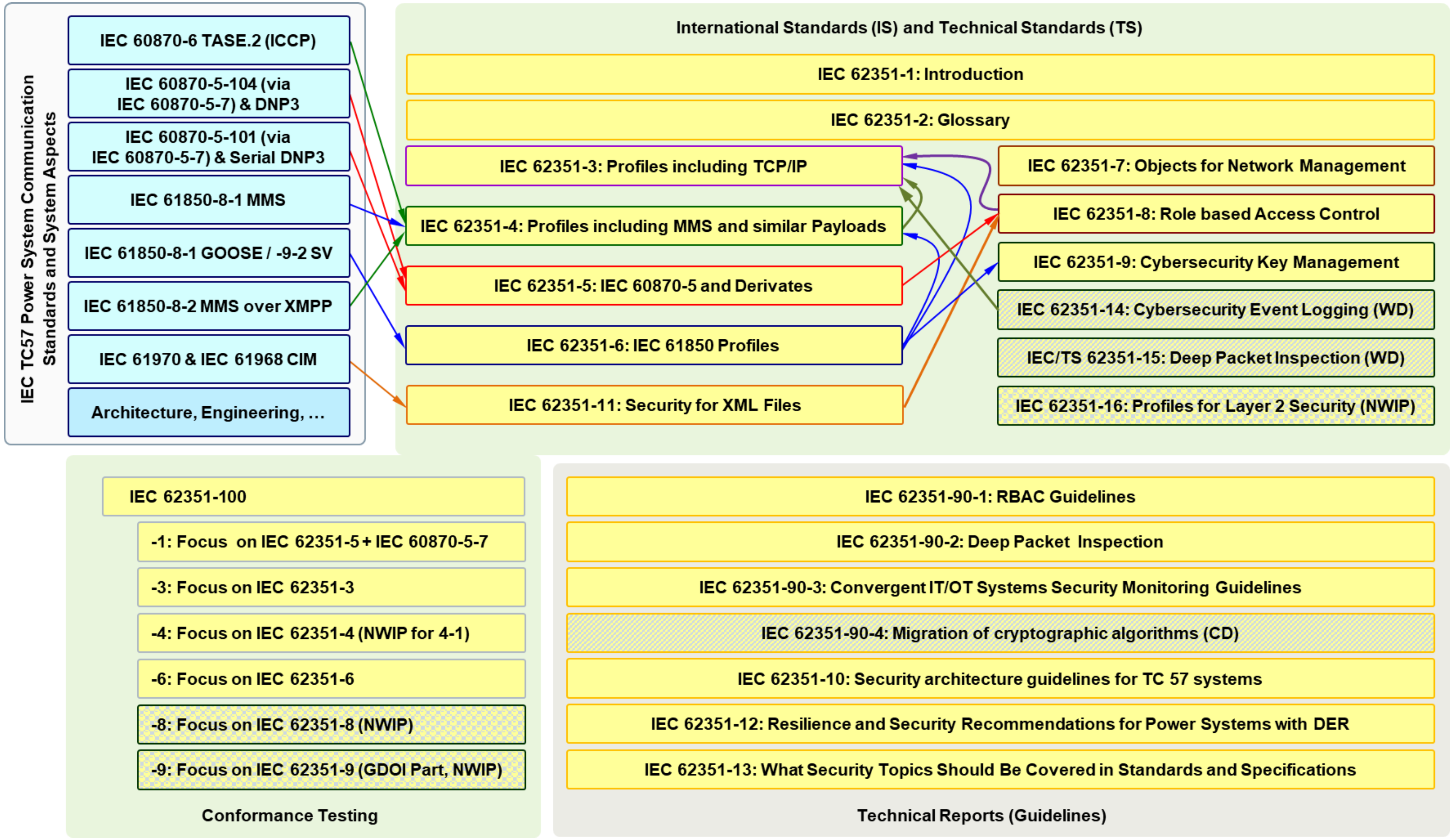
- IEC 62357 defines power system management reference architecture
- Incorporates security to protect communication protocols defined by IEC TC 57, specifically
  - IEC 60870-5 and IEC 60870-6 series,
  - IEC 61850 series,
  - IEC 61968 & IEC 61970 series.
- Undertake the development of standards and/or technical reports on end-to-end security issues.

  End-to-End Security = a set of security policies, procedures, and technologies that provides a high degree of assurance that data exchanged between a source (sender) and a sink (receiver) is protected from unauthorized access and/or modifications, while being transferred from one end to the other through intermediate nodes.



Cybersecurity in Digital Grids is defined in IEC 62351 (IEC TC57 WG15)

Specification of technical security measures / guidelines to cope with given security requirements



IEC TC57 Power System Communication Standards and System Aspects

- IEC 60870-6 TASE.2 (ICCP)
- IEC 60870-5-104 (via IEC 60870-5-7) & DNP3
- IEC 60870-5-101 (via IEC 60870-5-7) & Serial DNP3
- IEC 61850-8-1 MMS
- IEC 61850-8-1 GOOSE / -9-2 SV
- IEC 61850-8-2 MMS over XMPP
- IEC 61970 & IEC 61968 CIM
- Architecture, Engineering, …

International Standards (IS) and Technical Standards (TS)

- IEC 62351-1: Introduction
- IEC 62351-2: Glossary
- IEC 62351-3: Profiles including TCP/IP
- IEC 62351-4: Profiles including MMS and similar Payloads
- IEC 62351-5: IEC 60870-5 and Derivates
- IEC 62351-6: IEC 61850 Profiles
- IEC 62351-11: Security for XML Files
- IEC 62351-7: Objects for Network Management
- IEC 62351-8: Role based Access Control
- IEC 62351-9: Cybersecurity Key Management
- IEC 62351-14: Cybersecurity Event Logging (WD)
- IEC/TS 62351-15: Deep Packet Inspection (WD)
- IEC 62351-16: Profiles for Layer 2 Security (NWIP)

Conformance Testing

- IEC 62351-100
  - -1: Focus on IEC 62351-5 + IEC 60870-5-7
  - -3: Focus on IEC 62351-3
  - -4: Focus on IEC 62351-4 (NWIP for 4-1)
  - -6: Focus on IEC 62351-6
  - -8: Focus on IEC 62351-8 (NWIP)
  - -9: Focus on IEC 62351-9 (GDOI Part, NWIP)

Technical Reports (Guidelines)

- IEC 62351-90-1: RBAC Guidelines
- IEC 62351-90-2: Deep Packet Inspection
- IEC 62351-90-3: Convergent IT/OT Systems Security Monitoring Guidelines
- IEC 62351-90-4: Migration of cryptographic algorithms (CD)
- IEC 62351-10: Security architecture guidelines for TC 57 systems
- IEC 62351-12: Resilience and Security Recommendations for Power Systems with DER
- IEC 62351-13: What Security Topics Should Be Covered in Standards and Specifications

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

by utilizing or profiling

- existing standards and recommendations

SIEMENS

Cybersecurity for Power System Automation

Interplay of ISO/IEC 27k / IEC 62443 / IEC 62351

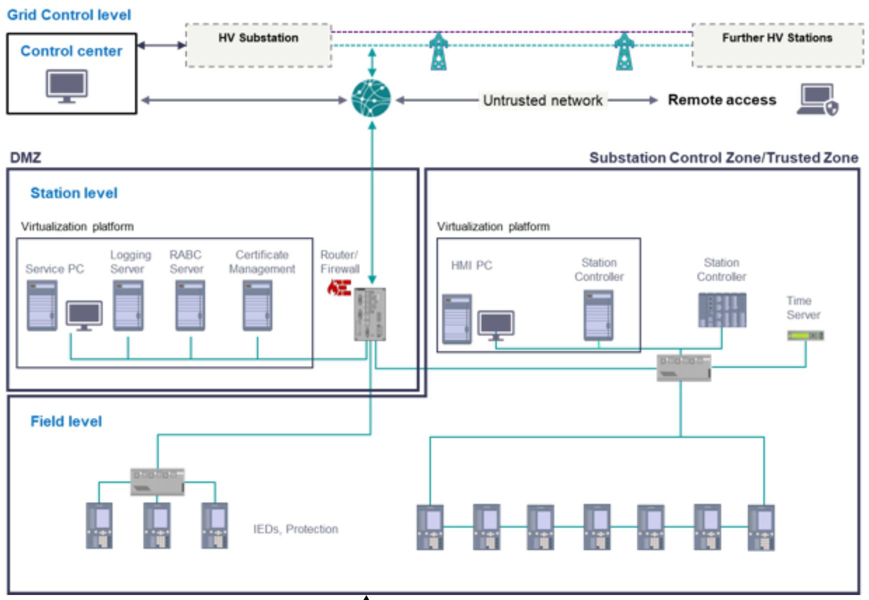
§ Cyber Security regulations are provided for instance by
- European NIS/NIS2 Directive and derived country specific laws
- US FERC for North America

ISO/IEC 27001

Asset Owner Operator – IT Infrastructure → ISO/IEC 27001, ISO/IEC 27019, IEC 62351

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

SIEMENS

Cybersecurity is addressed in power system automation through IEC 62351

Several parts of the series are likely applicable also in other domains

A

Authorization of Users/Devices

- Application of X.509 framework with enhancements
- Usage of deployed technologies like RADIUS, LDAP, and OAUTH

B

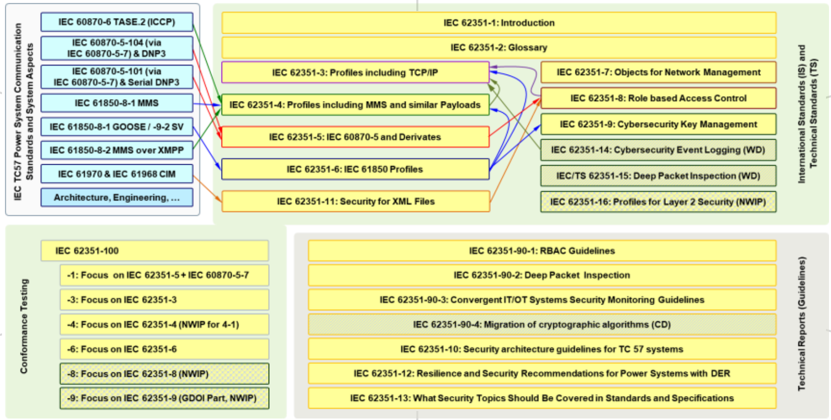
Secure communication
(Ethernet, IP, serial, application)

- Profiling existing standards (e.g., TLS)
- Definition of specific security enhancements if necessary

C

Key management (asym/sym)

- Application / profiling of established certificate management (EST, SCEP)
- Application and enhancement of key management (GDOI) functions



IEC TC57 Power System Communication Standards and System Aspects

IEC 60870-6 TASE.2 (ICCP)

IEC 60870-5-104 (via IEC 60870-5-7) & DNP3

IEC 60870-5-101 (via IEC 60870-5-7) & Serial DNP3

IEC 61850-8-1 MMS

IEC 61850-8-1 GOOSE / -9-2 SV

IEC 61850-8-2 MMS over XMPP

IEC 61970 & IEC 61968 CIM

Architecture, Engineering, …

International Standards (IS) and Technical Standards (TS)

IEC 62351-1: Introduction

IEC 62351-2: Glossary

IEC 62351-3: Profiles including TCP/IP

IEC 62351-4: Profiles including MMS and similar Payloads

IEC 62351-5: IEC 60870-5 and Derivates

IEC 62351-6: IEC 61850 Profiles

IEC 62351-11: Security for XML Files

IEC 62351-7: Objects for Network Management

IEC 62351-8: Role based Access Control

IEC 62351-9: Cybersecurity Key Management

IEC 62351-14: Cybersecurity Event Logging (WD)

IEC/TS 62351-15: Deep Packet Inspection (WD)

IEC 62351-16: Profiles for Layer 2 Security (NWIP)

Conformance Testing

IEC 62351-100

-1: Focus on IEC 62351-5 + IEC 60870-5-7

-3: Focus on IEC 62351-3

-4: Focus on IEC 62351-4 (NWIP for 4-1)

-6: Focus on IEC 62351-6

-8: Focus on IEC 62351-8 (NWIP)

-9: Focus on IEC 62351-9 (GDOI Part, NWIP)

Technical Reports (Guidelines)

IEC 62351-90-1: RBAC Guidelines

IEC 62351-90-2: Deep Packet Inspection

IEC 62351-90-3: Convergent IT/OT Systems Security Monitoring Guidelines

IEC 62351-90-4: Migration of cryptographic algorithms (CD)

IEC 62351-10: Security architecture guidelines for TC 57 systems

IEC 62351-12: Resilience and Security Recommendations for Power Systems with DER

IEC 62351-13: What Security Topics Should Be Covered in Standards and Specifications

D

Monitor and audit of relevant events

- Definition of power system specific events and counters
- Usage of established standards like syslog and SNMP

- **Guidance and support** for securing power system architectures
  - Examples for network design, and key management, role-based access control (RBAC), monitoring, …

- **Test case description** for specified security measures in system context
  - Specification of conformity test cases

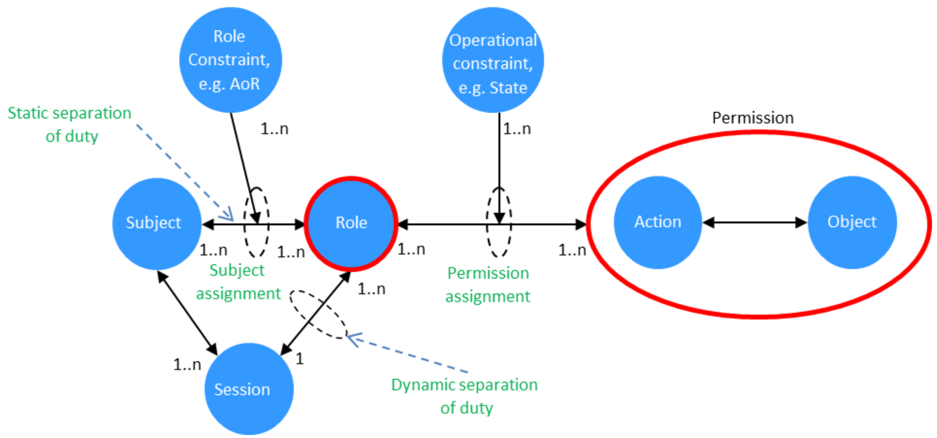
IEC 62351-8 Role-based access control (RBAC) for power system management

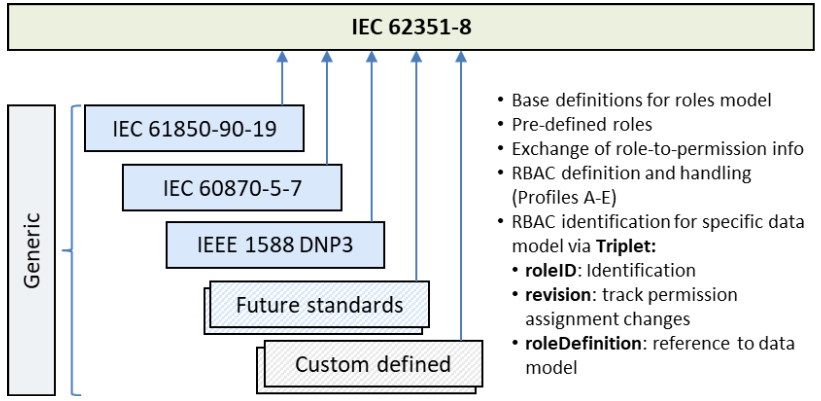
Support of fine-grained authorization

deep dive

A

- **RBAC:** ease access control configuration and decisions based on distinction of
  - subjects and roles; subjects = {humans; devices; SW processes}
  - roles and associated permissions (action on object, e.g., read/write of files)
- IEC 62351-8 adds and defines
  - Pre-defined roles and mechanisms for defining custom based roles (XACML)
  - **Handling of constraints** to restrict the applicability of a role (based on geographical or organizational constraints) using "area of responsibility"
  - Common approach for binding RBAC information to a **target data model**
  - Interaction with repositories for RBAC information, either as **PULL or PUSH**
  - Different profiles to provide RBAC information using
    - **New extensions in X.509 public key and attribute certificates**
    - **JSON Web Tokens** in OAUTH environments
    - **RADIUS** via vendor specific attributes
    - **LDAP** via an own schema or group mapping



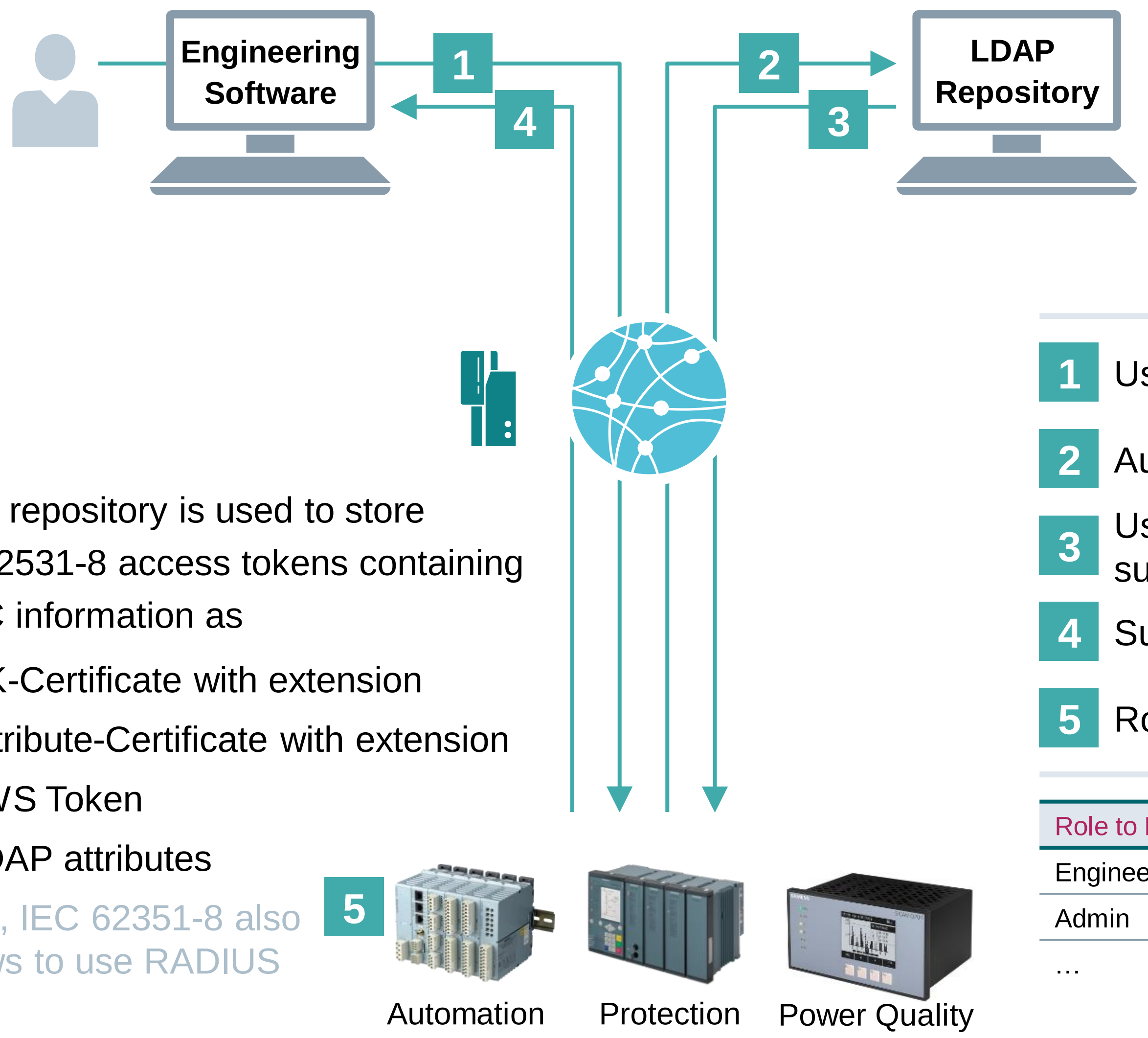


- Base definitions for roles model
- Pre-defined roles
- Exchange of role-to-permission info
- RBAC definition and handling (Profiles A-E)
- RBAC identification for specific data model via **Triplet:**
  - **roleID**: Identification
  - **revision**: track permission assignment changes
  - **roleDefinition**: reference to data model

IEC 62351 Application Examples

Role-based access control to power systems and services

deep dive



Roles <-> Users	Role
User 1	Engineer
User 2	Admin
…	

1 User requests access to IED with username and password

2 Authentication request with username, password via LDAP

3 Users access token as response from LDAP repository after successful authentication

4 Success/Fail Response from device to user

5 Role-based user session initiated/denied

Role to Permission mapping	Operation A	Operation B	Operation C	Operation …
Engineer	X	X		
Admin		X	X	
…				

LDAP repository is used to store IEC 62531-8 access tokens containing RBAC information as

- PK-Certificate with extension
- Attribute-Certificate with extension
- JWS Token
- LDAP attributes

Note, IEC 62351-8 also allows to use RADIUS

IEC 62351-3 Profiles including TCP/IP

Profiling of TLS to utilize state-of-the-art TCP/IP security measures

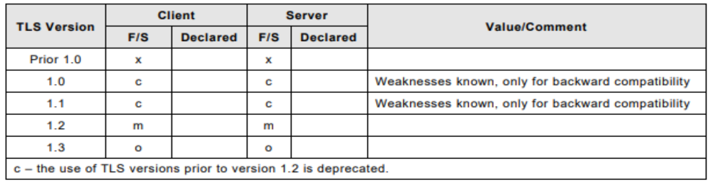
deep dive

B

- Power system protocols like IEC 61850 MMS, IEC 60870-5-104, or IEEE 1815 (DNP3) rely on TCP/IP using **Transport Layer Security (TLS)** for protection.
- TLS = very feature rich → requires profiling to limit misconfiguration, ease interoperability and keep the security on a desired level.
- IEC 62351-3 defines a **profile for TLS 1.2 and TLS 1.3** addressing specifically
  - **Mutual authentication** using X.509 certificates
  - **Certificate verification** (specifically for long lasting connections)
  - **Selection of cipher suites** (mandatory, optional). Also considers integrity-only (non-encrypting) cipher suites to allow traffic monitoring.
  - **Session security parameter handling** (key update strategies using session resumption / session renegotiation / post handshake key update)
  - **Security event definition** to enable identification of potential error situations.
- IEC 62351-3 Edition 2 published 06/2023 is a self-contained document and is likely applicable also in other domains.

Example profiling items

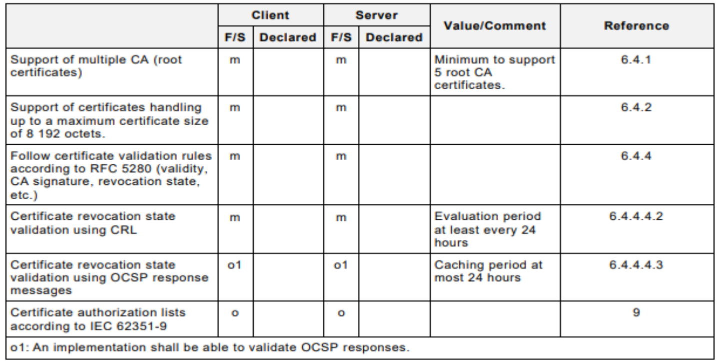
Table 7 – Conformance to TLS versions



TLS Version	Client		Server		Value/Comment
	F/S	Declared	F/S	Declared	
Prior 1.0	x		x		
1.0	c		c		Weaknesses known, only for backward compatibility
1.1	c		c		Weaknesses known, only for backward compatibility
1.2	m		m		
1.3	o		o		

c – the use of TLS versions prior to version 1.2 is deprecated.

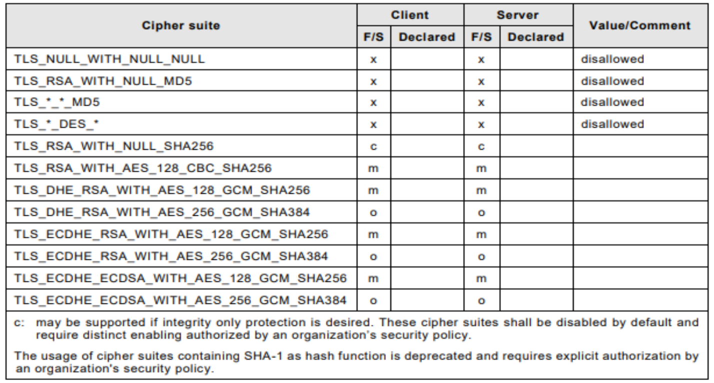
Table 8 – Conformance to certificate support



	Client		Server		Value/Comment	Reference
	F/S	Declared	F/S	Declared		
Support of multiple CA (root certificates)	m		m		Minimum to support 5 root CA certificates.	6.4.1
Support of certificates handling up to a maximum certificate size of 8 192 octets.	m		m			6.4.2
Follow certificate validation rules according to RFC 5280 (validity, CA signature, revocation state, etc.)	m		m			6.4.4
Certificate revocation state validation using CRL	m		m		Evaluation period at least every 24 hours	6.4.4.4.2
Certificate revocation state validation using OCSP response messages	o1		o1		Caching period at most 24 hours	6.4.4.4.3
Certificate authorization lists according to IEC 62351-9	o		o			9

o1: An implementation shall be able to validate OCSP responses.

Table 9 – Conformance to TLSv1.2 usable cipher suites



Cipher suite	Client		Server		Value/Comment
	F/S	Declared	F/S	Declared	
TLS_NULL_WITH_NULL_NULL	x		x		disallowed
TLS_RSA_WITH_NULL_MD5	x		x		disallowed
TLS_*_*_MD5	x		x		disallowed
TLS_*_DES_*	x		x		disallowed
TLS_RSA_WITH_NULL_SHA256	c		c		
TLS_RSA_WITH_AES_128_CBC_SHA256	m		m		
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	m		m		
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	o		o		
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	m		m		
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	o		o		
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	m		m		
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	o		o		

c: may be supported if integrity only protection is desired. These cipher suites shall be disabled by default and require distinct enabling authorized by an organization's security policy.

The usage of cipher suites containing SHA-1 as hash function is deprecated and requires explicit authorization by an organization's security policy.

IEC 62351-9 – Cyber security key management for power system equipment

Handling the prerequisite: symmetric and asymmetric keys

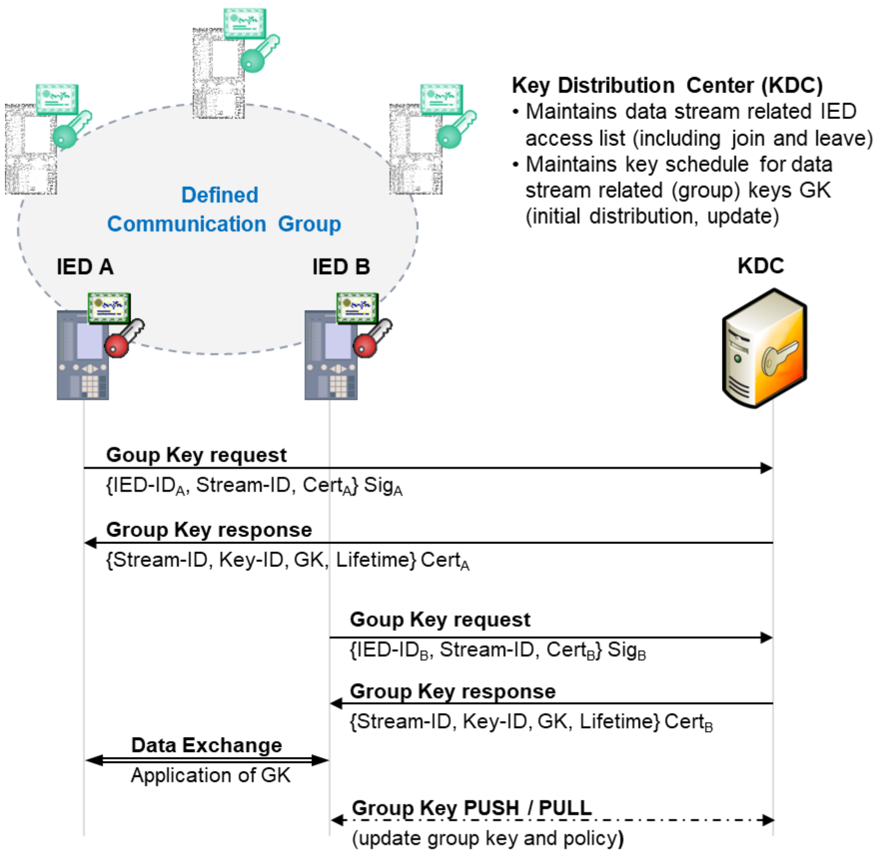
deep dive

C

- IEC 62351-9 defines management of X.509 credentials as well as group keys and associated security policies, specifically:
  - **Management of X.509 certificates (PKI)**
    - Selection of standardized **enrollment protocols**: EST (RFC 7030), SCEP (RFC 8894)
    - **X.509 certificate profiles** to support operation
    - **Certificate verification** of public-key and attribute certificates, including revocation status checking using CRLs and OCSP
    - Optional support of trust anchor management: TAMP (RFC 5934)
  - **Management of symmetric group keys**
    - **Group key management** applying GDOI (RFC 6407) utilizing certificate based group member authentication and support of pull/push for group-key update
    - **Enhancements** to distribute group keys and group security policy for different protocols, i.e., GOOSE, SV, and PTP

PKI – Public Key Infrastructure
OCSP – Online Certificate Status Protocol
SCEP – Simple Certificate Enrollment Protocol
TAMP – Trust Anchor Management Protocol
EST – Enrollment over Secure Transport
GDOI – Group Domain of Interpretation
CRL – Certificate Revocation List

Group based key management (centralized approach)



Defined Communication Group
IED A
IED B
KDC
Key Distribution Center (KDC)
• Maintains data stream related IED access list (including join and leave)
• Maintains key schedule for data stream related (group) keys GK (initial distribution, update)
Goup Key request
{IED-ID$_A$, Stream-ID, Cert$_A$} Sig$_A$
Group Key response
{Stream-ID, Key-ID, GK, Lifetime} Cert$_A$
Goup Key request
{IED-ID$_B$, Stream-ID, Cert$_B$} Sig$_B$
Group Key response
{Stream-ID, Key-ID, GK, Lifetime} Cert$_B$
Data Exchange
Application of GK
Group Key PUSH / PULL
(update group key and policy)

SIEMENS

IEC 62351-14 – Cyber security event logging

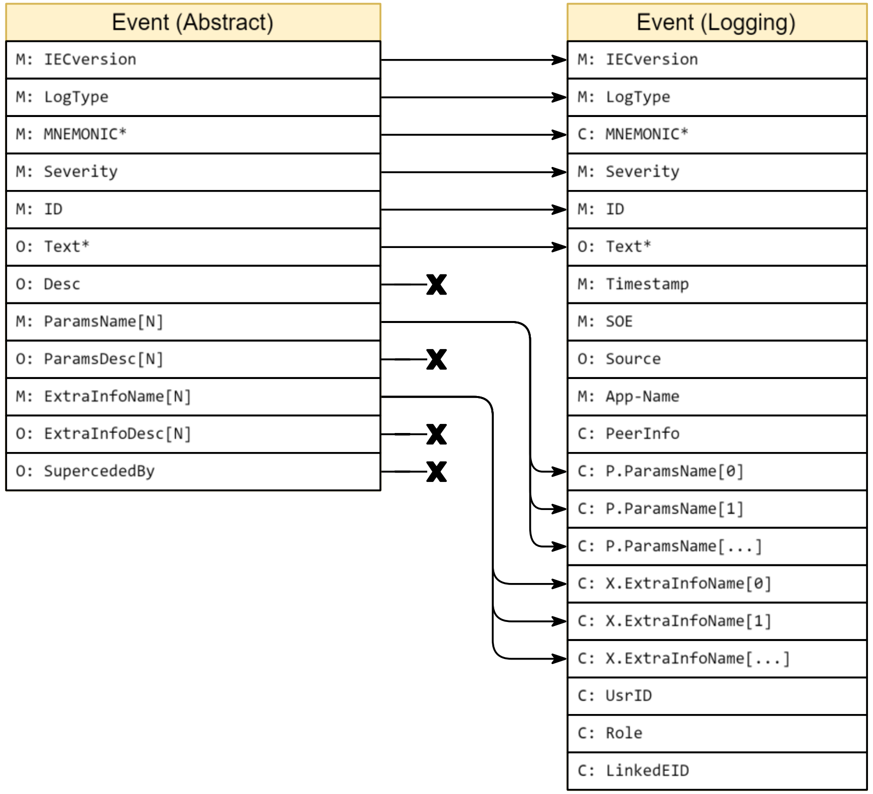
Cybersecurity events are supporting forensic analysis and auditing

deep dive

D

- IEC 62351-14 defines
  - an **abstract security event format** to be used for reporting success and failure cases locally and to a SIEM system
  - mapping of the abstract events to **structured syslog** messages
  - allowing use of unstructured syslog message, e.g., for vendor specific use
  - protection of syslog is by relying on **syslog over TLS**. For this the TLS profile specified in IEC 62351-3:2023 has to be used, which is also aligned with an ongoing update of the ciphersuites in IETF RFC 5424).
- IEC 62351-14 currently defines security events for IEC 62351 parts, which have not be recently updated and involve an own definition. The events will be incorporated into the respective parts during the next maintenance cycle and will take precedence.
- Current approach is incorporate already into
  - IEC 62351-3:2023
  - IEC 62351-5:2023
  - IEC 62351-9:2023
  - IEC 62351-8:Ed.2 (currently being done)

Abstract security events are mapped to syslog



SIEMENS

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

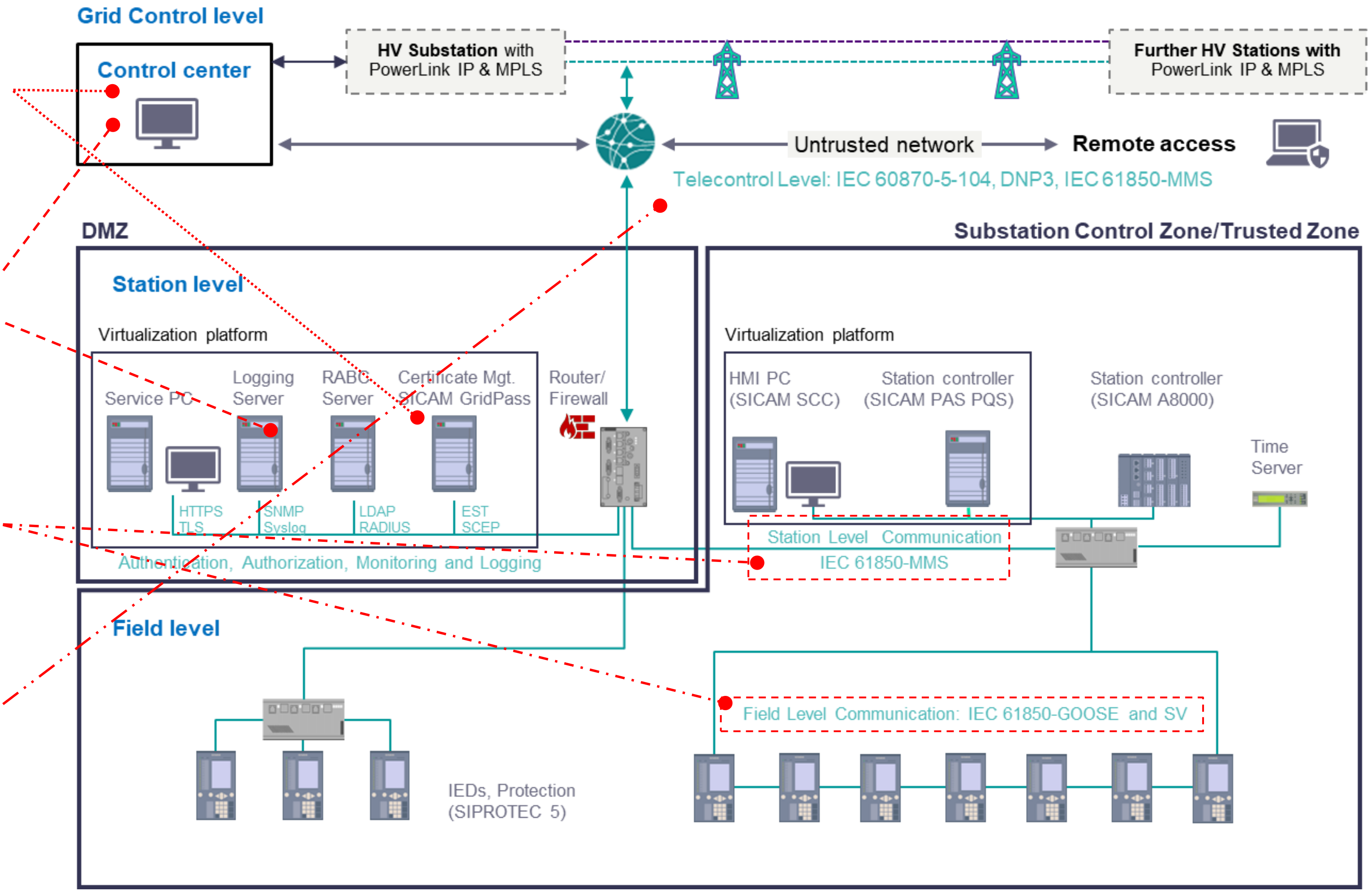
IEC 62351-7/14

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

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

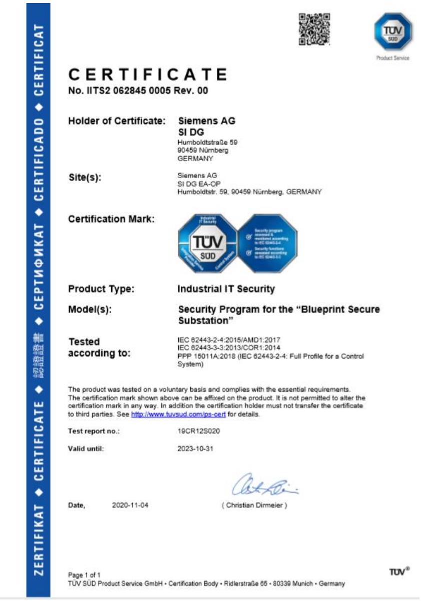
Securing telecontrol and control center communication using TLS and / or security measures on application level

IEC 62351-3/4/5/9


Grid Control level
Control center
HV Substation with PowerLink IP & MPLS
Further HV Stations with PowerLink IP & MPLS
Untrusted network
Remote access
Telecontrol Level: IEC 60870-5-104, DNP3, IEC 61850-MMS
DMZ
Substation Control Zone/Trusted Zone
Station level
Virtualization platform
Service PC
Logging Server
RABC Server
Certificate Mgt. SICAM GridPass
Router/ Firewall
HTTPS TLS
SNMP Syslog
LDAP RADIUS
EST SCEP
Authentication, Authorization, Monitoring and Logging
Virtualization platform
HMI PC (SICAM SCC)
Station controller (SICAM PAS PQS)
Station controller (SICAM A8000)
Time Server
Station Level Communication IEC 61850-MMS
Field level
IEDs, Protection (SIPROTEC 5)
Field Level Communication: IEC 61850-GOOSE and SV

Additionally, certification of security functionalities is possible to underline a security aware development and integration process as well as support of technical security means (e.g., using IEC 62351).

Certification possible according to IEC 62443



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE
No. IITS2 062845 0005 Rev. 00

Holder of Certificate:	**Siemens AG** **SI DG** Humboldtstraße 59 90459 Nürnberg GERMANY
Site(s):	Siemens AG SI DG EA-OP Humboldtstr. 59, 90459 Nürnberg, GERMANY
Certification Mark:	
Product Type:	**Industrial IT Security**
Model(s):	**Security Program for the "Blueprint Secure Substation"**
Tested according to:	IEC 62443-2-4:2015/AMD1:2017 IEC 62443-3-3:2013/COR1:2014 PPP 15011A:2018 (IEC 62443-2-4: Full Profile for a Control System)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

Test report no.:	19CR12S020
Valid until:	2023-10-31

Date, 2020-11-04

(Christian Dirmeier)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

SIEMENS

Security Requirement Consideration

Development and feature set definition on the example of a protection device

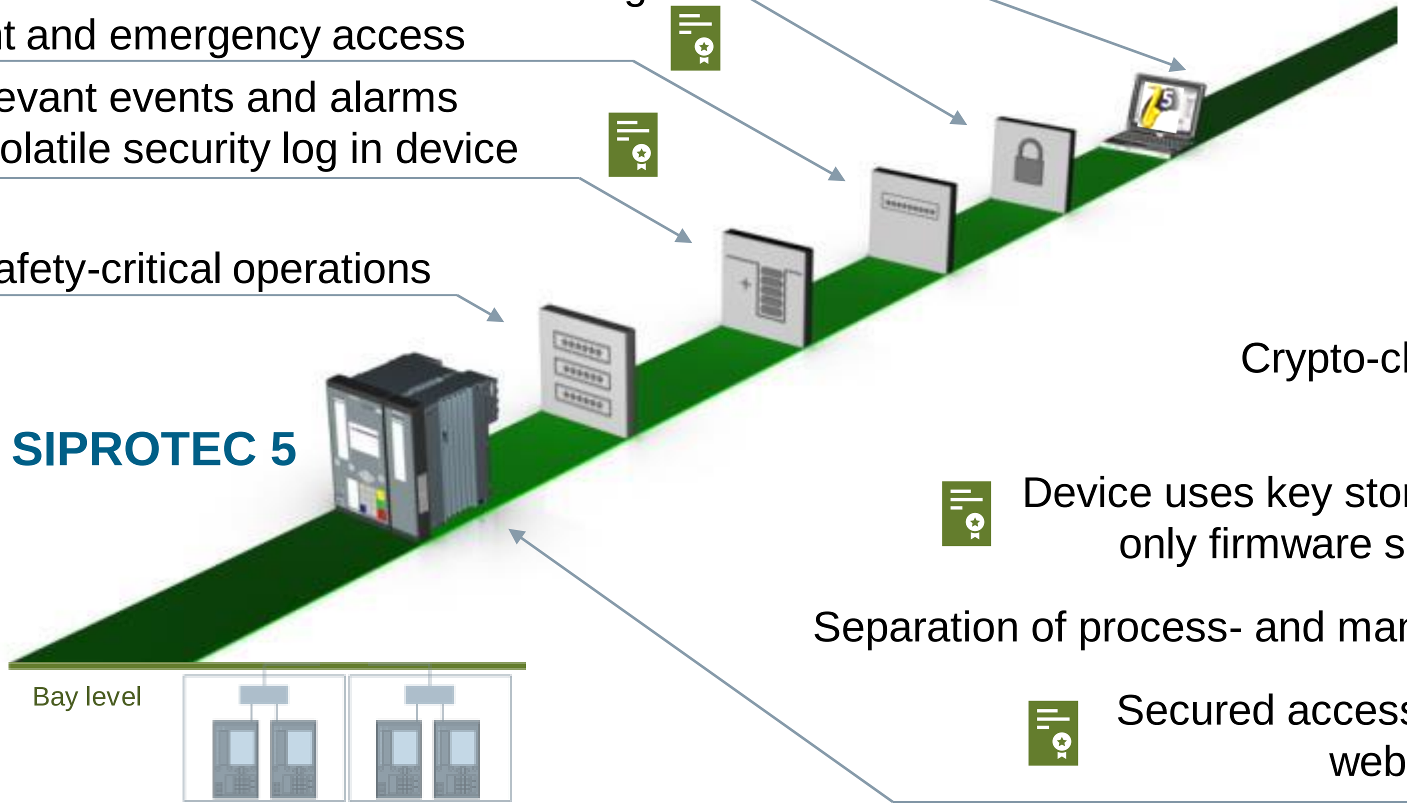
Technical Measures according to IEC 62351

Mutually authenticated and encrypted communication line for operational protocols and engineering

Device-side support for role-based access control including central user management and emergency access

Recording of security-relevant events and alarms over Syslog and in non-volatile security log in device

Confirmation codes for safety-critical operations



Secure development
Patch management
Virus protection

Product hardening

Independent testing

Crypto-chip for secure information storage and transmission

Device uses key stored in crypto-chip to allow only firmware signed by Siemens to load

Separation of process- and management communication

Secured access for HMI interactions and web-based device monitoring

Measures for product lifecycle supported by requirements from IEC 62443

X.509 Certificates applied

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 TLS Syslog (as of IEC 62351-14)

RBAC for engineering and operation

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

X.509 certificate management with SICAM GridPass (IEC 62351-9)

Communication Security

- TLS security (based on IEC 62351-3)
- Application layer security for IEC 80670-5-104, IEC 61850, DNP3i according to IEC 62351-5
- Intrusion Detection

All good?
Well, there are still Security Challenges!

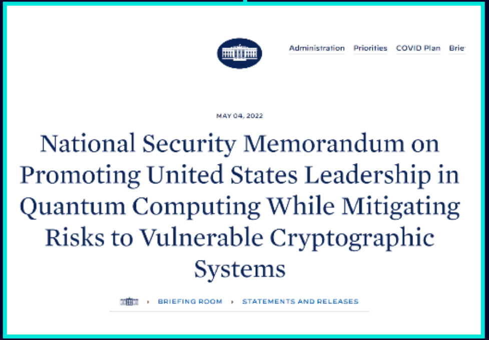
- **Operational challenge** to migrate existing systems to utilize specified security standards and BCPs
- Observation of **System Integrity** to identify unauthorized (and also unintended) changes in system configuration. This may be connected with response handling upon detection.
- Ensuring **Resilience** to allow a system to stay operational with a degraded performance or functionality even when it has been attacked successfully.
- Performing **Monitoring** of industrial communication to ensure reliance with the intended operational environment even if the communication is encrypted. Influences on network design and privacy to be obeyed.
- Address **Supply Chain Security** requirements to enable verification of the system integrity along the product value chain and also after commissioning during operation.
- Support of **Crypto Agility** to enable migration to stronger cryptographic algorithms. Advances in quantum computing endangers specifically asymmetric cryptographic algorithms like RSA or Elliptic Curve Cryptosystems (ECC) used for authentication, authorization, and key agreement in devices and infrastructure.

Crypto Agility: Transition to PQC must be prepared to meet upcoming requirements and customer demands for long lived critical infrastructures

- US administration is pushing for the transition to post-quantum cryptography
- Initial focus on US NSS systems starting by 2025, e.g., armed forces, intelligence
- Private sector expected to follow soon afterwards
- Similar recommendations seen also in other regions, e.g., Europe, China, …

May 2022

National Security Memorandum



Administration Priorities COVID Plan Brie

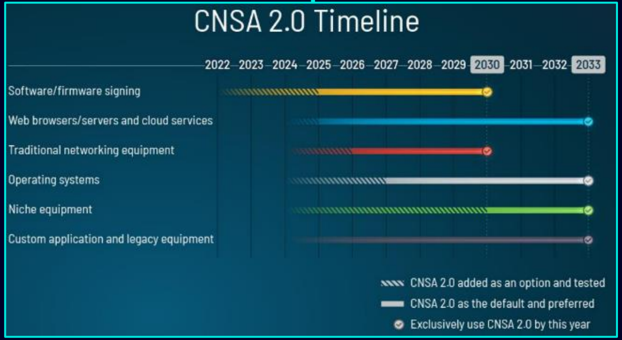
MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

› BRIEFING ROOM › STATEMENTS AND RELEASES

Sep 2022

NSA releases CNSA 2.0 for NSS



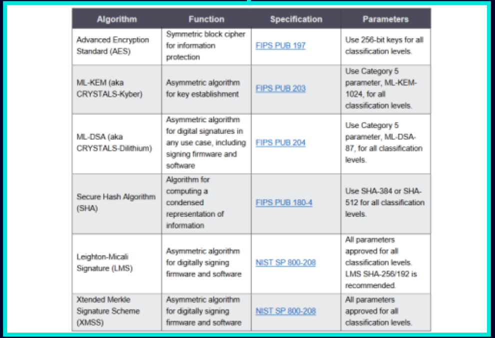
Mar 2023

US National Cybersecurity Strategy

"… Federal Government will prioritize the transition of vulnerable public networks and systems to quantum-resistant cryptography [...] The ***private sector should follow the government's model*** *in preparing its own networks and systems for our post-quantum future"*

Apr 2024

CNSA 2.0 Suite FAQ Update



Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
ML-KEM (aka CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	Use Category 5 parameter, ML-KEM-1024, for all classification levels.
ML-DSA (aka CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software	FIPS PUB 204	Use Category 5 parameter, ML-DSA-87, for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. LMS SHA-256/192 is recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.

SIEMENS

Related activities for standards and guidelines are ongoing

Examples: ISO/IEC, IETF, ETSI, NIST, German BSI, EU Commission

- ISO/IEC JTC 1 SC27 engaged in PQC standardization of PWC algorithms (FrodoKEM, Kyber, and Classic McEliece)
- IEC TC57 WG15 ongoing work on migration to stronger cryptographic algorithms in IEC 62351-90-4

- Several working groups at IETF (CFRG, LAMPS, SUIT, PQUIP, …) started specifying the usage of post-quantum algorithms in cryptographic protocols and data formats
- Stateful Hash-based signatures standardized (XMSS, HSS-LMS)

- ETSI Quantum Safe WG provides recommendations and guidelines for the application of post-quantum algorithms in different use cases (TR 103 619, 2020).

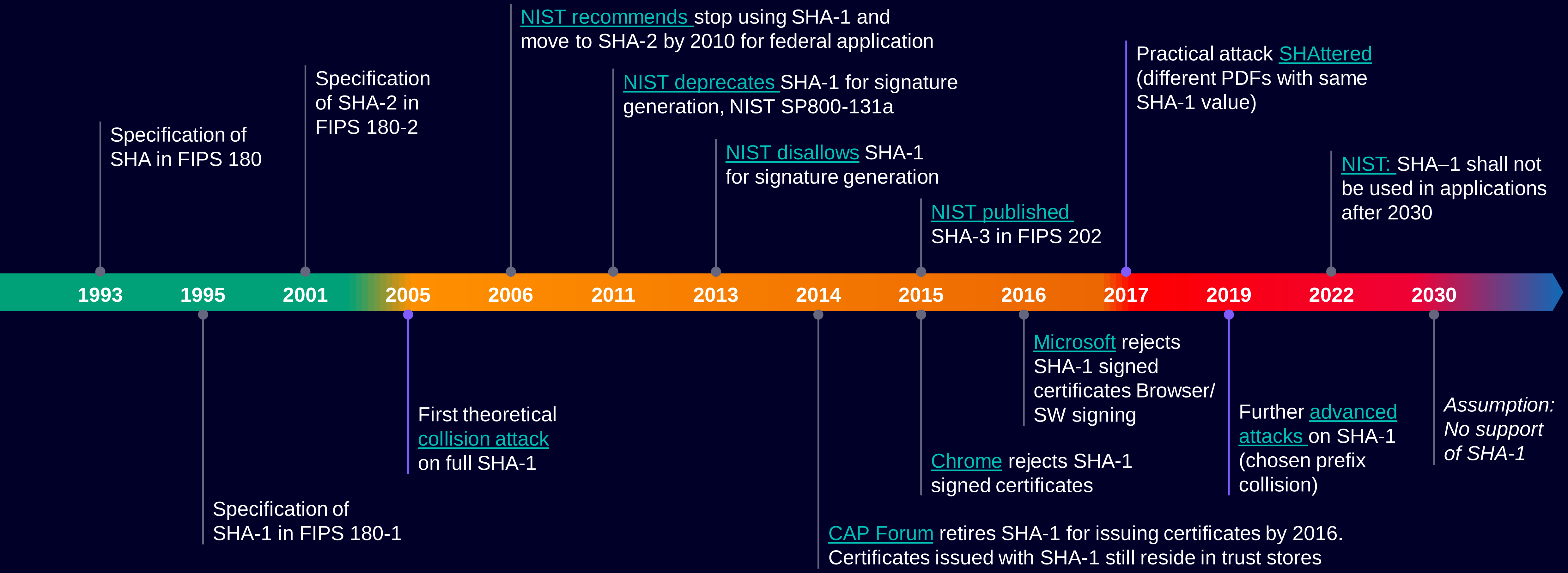
- NIST SP1800-38B: Migration to Post Quantum Cryptography
- Standardization of PQC algorithms ongoing (CRYSTALS-Kyber (ML-KEM, FIPS 203), CRYSTALS-Dilithium (ML-DSA, FIPS 204), SPHINCS+ (SLH-DSA, FIPS 205), FALCON)

- German BSI provides recommendations and key length also for PQC algorithms in TR 02102-1 (yearly updated) as well as general guidelines for the migration.

- European Commission: Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography (April 2024)

Experiences from ongoing cryptographic algorithm migration

The rise and fall of SHA–1



- 1993 – Specification of SHA in FIPS 180
- 1995 – Specification of SHA-1 in FIPS 180-1
- 2001 – Specification of SHA-2 in FIPS 180-2
- 2005 – First theoretical collision attack on full SHA-1
- 2006 – NIST recommends stop using SHA-1 and move to SHA-2 by 2010 for federal application
- 2011 – NIST deprecates SHA-1 for signature generation, NIST SP800-131a
- 2013 – NIST disallows SHA-1 for signature generation
- 2014 – CAP Forum retires SHA-1 for issuing certificates by 2016. Certificates issued with SHA-1 still reside in trust stores
- 2015 – NIST published SHA-3 in FIPS 202
- 2015 – Chrome rejects SHA-1 signed certificates
- 2016 – Microsoft rejects SHA-1 signed certificates Browser/ SW signing
- 2017 – Practical attack SHAttered (different PDFs with same SHA-1 value)
- 2019 – Further advanced attacks on SHA-1 (chosen prefix collision)
- 2022 – NIST: SHA–1 shall not be used in applications after 2030
- 2030 – *Assumption: No support of SHA-1*

Migration towards new cryptographic algorithm support takes its time. Disallowing application of outdated cryptographic algorithm takes even **longer.**

Summary & Outlook

- Cybersecurity has been acknowledged as prerequisite for limiting risks in critical infrastructures.
- Cyber security needs a holistic approach – collaboration between vendors, integrators and operators; taking into account people, processes, and products in the specific domain.
- Regulation increasingly requires to address technical and organizational cybersecurity measures to ensure reliable operation of critical infrastructures and beyond.
- Security-by-Design using a risk-based approach is essential to provide appropriate security features from the ground and addresses functional and procedural security requirements during product manufacturing and operation.
- Standardization and guideline activities support the alignment of approaches and interoperability of different vendor’s products and need to adopt upcoming new requirements.

- Still, some challenges as shown remain and are already addressed, e.g., in the related standardization groups … and provide further food for thoughts.

[redacted]

Contact

Steffen Fries
Principal Key Expert Engineer

T CST
Otto-Hahn-Ring 6
81739 Munich
Germany

Phone: +48 89 780522928

E-mail steffen.fries@siemens.com

Siemens Grid Security

Siemens Cyber Security

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.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.

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