Johan Malmström
ABB Power Grids
– Grid Integration

IEC 61850 Nätverk 2019 - Nätverksträff I
2019-05-24
Stockholm

International Electrotechnical Commission

Agenda

- Arbetsgrupp 15
  - Introduktion, uppdrag, medlemmar
  - Publikationer
  - Pågående arbete och plan
- Hotbild mot ”Digital Substation”
- Vad löser IEC 62351

Uppdrag

- Utveckla standard för att säkra kommunikation för protokoll inom IEC TC57
  - IEC 60870-5, -6
  - IEC 61970, 61968
  - IEC 61850
- Granska och stödja säkerhet för IEC TC57
- Utveckla standarder/tekniska rapporter för at säkra end-to-end kommunikation

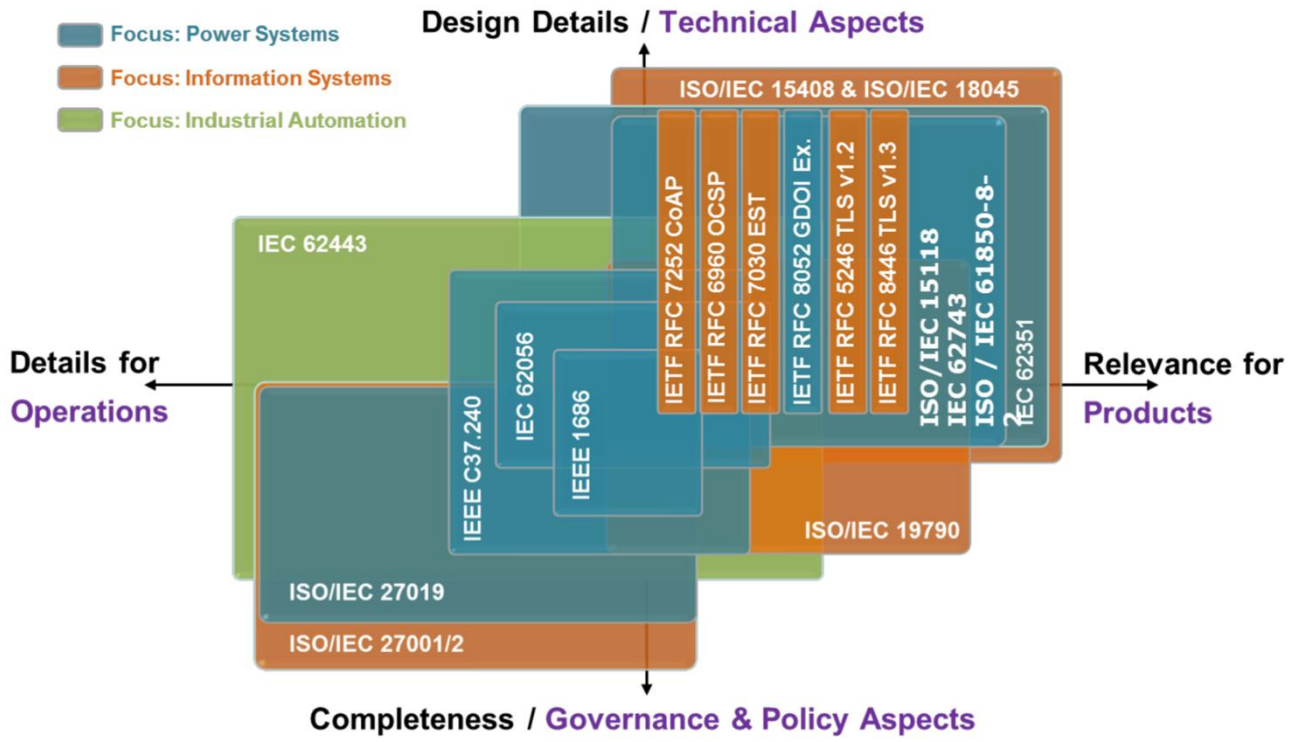
Medlemmar

126 medlemmar från 21 länder

- Argentina
- Austria
- Canada*
- China *
- Croatia
- Denmark*
- Finland
- France*
- Germany*
- Great Britain
- India*
- Italy*
- Japan
- Korea
- Russia
- South Africa
- Spain
- Sweden*
- Switzerland*
- USA *
- South Africa

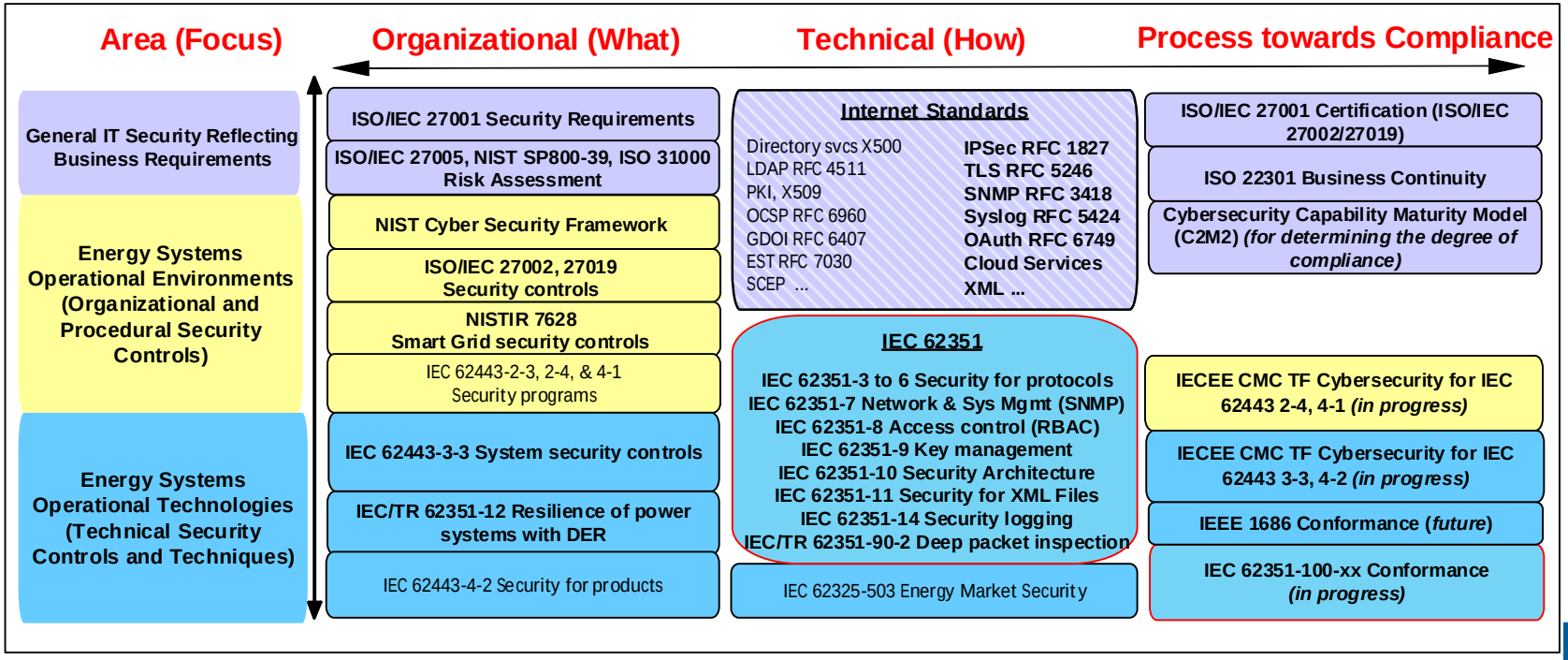
*deltog i möte maj 2019

Cyber security standards



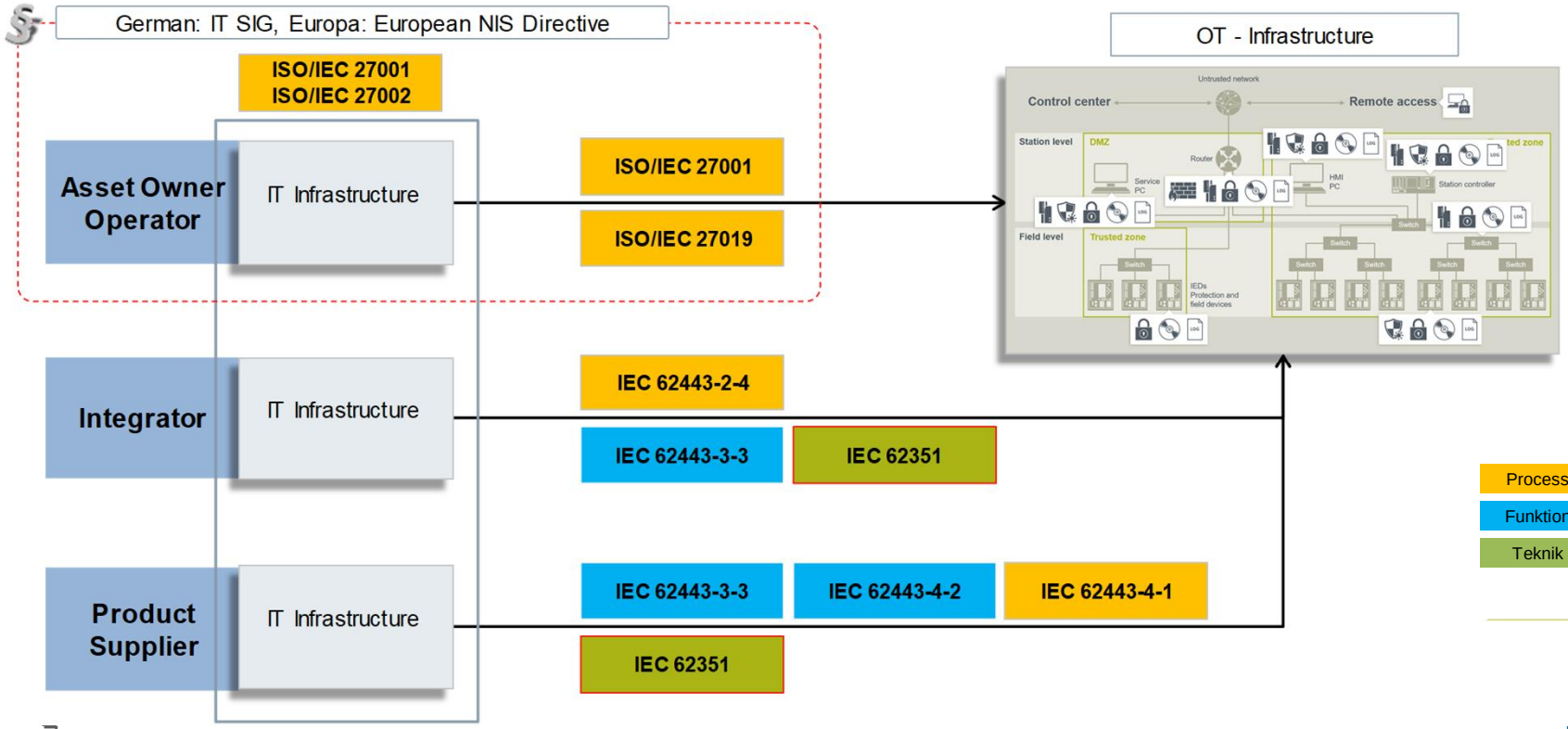
Källa: IEC

CS Standards for Smart Energy

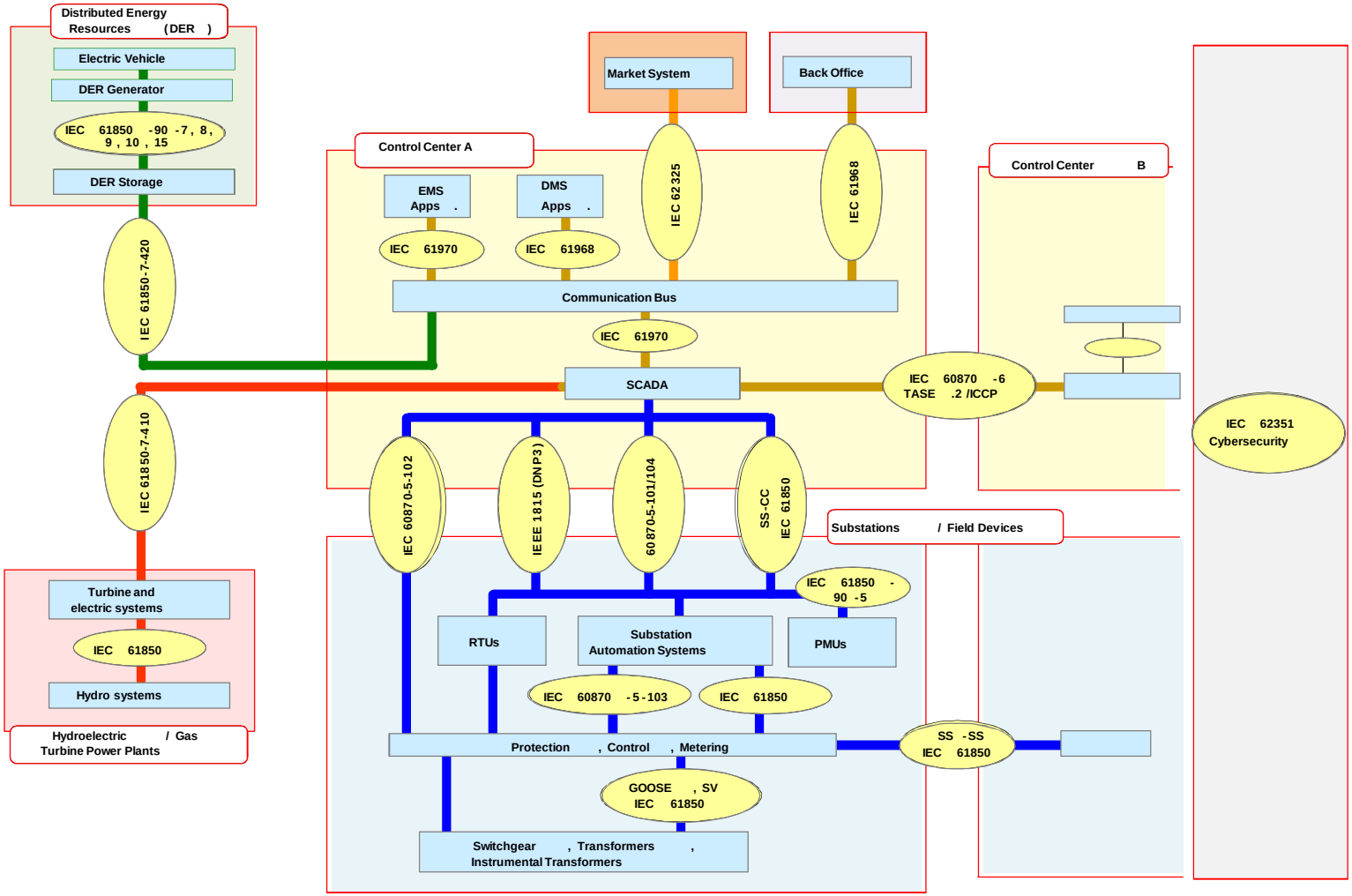


Källa: IEC

Förenklad bild…

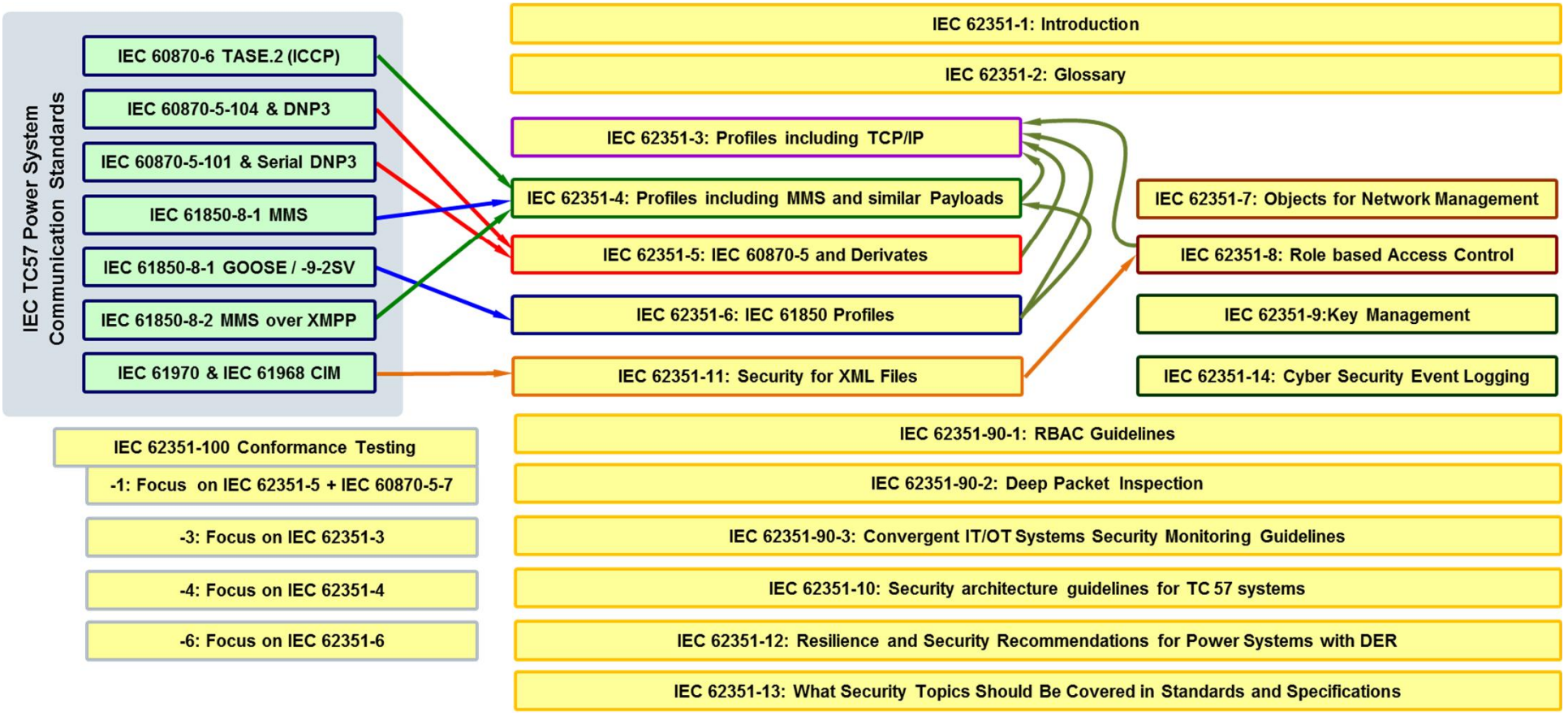


Källa: SIEMENS


Distributed Energy Resources (DER)
Electric Vehicle
DER Generator
IEC 61850-90-7, 8, 9, 10, 15
DER Storage
IEC 61850-7-420
IEC 61850-7-410
Turbine and electric systems
IEC 61850
Hydro systems
Hydroelectric / Gas Turbine Power Plants
Market System
Back Office
Control Center A
EMS Apps
DMS Apps
IEC 61970
IEC 61968
IEC 62325
IEC 61968
Communication Bus
IEC 61970
SCADA
IEC 60870-6 TASE.2 /ICCP
Control Center B
IEC 62351 Cybersecurity
IEC 60870-5-102
IEEE 1815 (DNP3)
60870-5-101/104
SS-CC IEC 61850
Substations / Field Devices
IEC 61850-90-5
RTUs
Substation Automation Systems
PMUs
IEC 60870-5-103
IEC 61850
Protection, Control, Metering
SS-SS IEC 61850
GOOSE, SV IEC 61850
Switchgear, Transformers, Instrumental Transformers

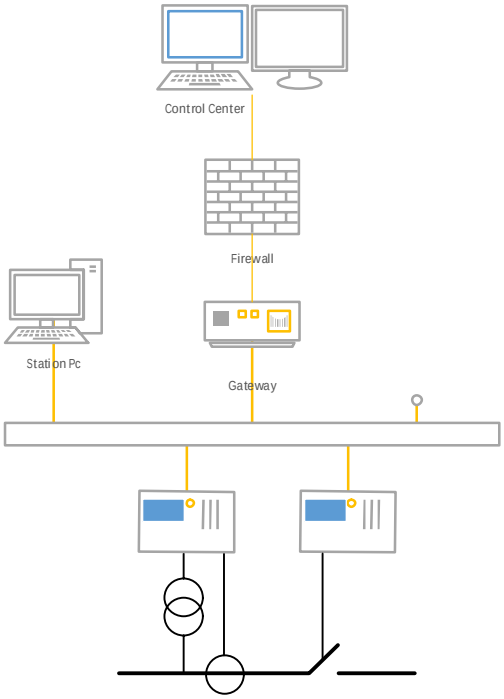
Källa: IEC

Mapping of TC57 Communication Standards to IEC 62351 Security Standards (Update)



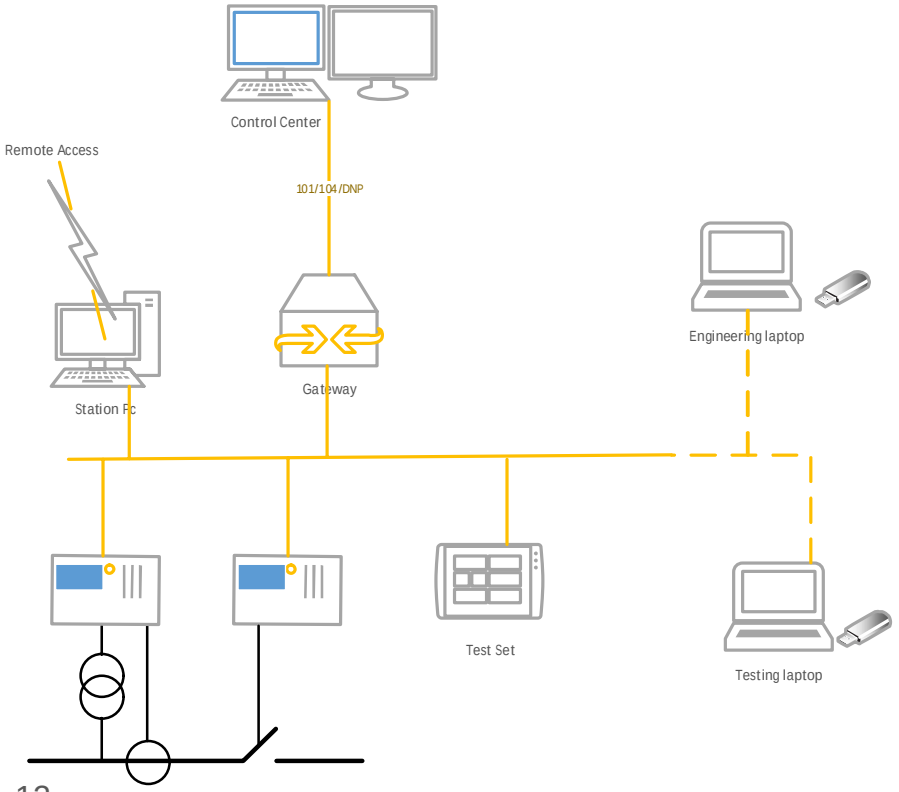
IEC 62351 Part	Release	Editor	Notes and Activities	Re
IEC/TS 62351-1: Introduction	2007	Cleveland	May need to be updated eventually – Assessment started	No re
IEC/TS 62351-2: Glossary of terms	2008	Formea	http://std.iec.ch/terms/terms.nsf/ByPub?OpenView&Count=-1&RestrictToCategory=IEC%2062351-2	Pending – r Curr
IEC/IS 62351-3: Security for profiles including TCP/IP	Ed 1.1 05/2018	Fries	IS Ed. 1 in 2014, updated to IS Ed.1.1 in 2018, currently in AMD2 phase. Revision to Ed.2 in discussion	AMD2 C
IEC/IS 62351-4: Security for profiles including MMS and derivatives	IS 11/2018	Andersen	IS in 11/2018, COR #1, AMD #1	CC
IEC/IS 62351-5: Security for IEC 60870-5 and derivatives	DC, CD	Grechi	TS Ed2 Released April 2013, IS underway	TS to IS 5/
IEC/IS 62351-6: Security for IEC 61850 profiles	CDV	Falk	Updates underway	CDV 08/201
IEC/IS 62351-7: Network and System Management (NSM) data object models	2017	Pugni	Eventual mapping to 61850, as IEC 61850-90-24 – but on hold	
IEC/IS 62351-8: Role-Based Access Control	CDV	Fries	Finalization of CDV and conversion to IS	RR 10/201 3
IEC/IS 62351-9: Key Management	2017	Fries		
IEC/TR 62351-10: Security Architecture	2012	Fries		
IEC/IS 62351-11: Security for XML Files	2016	Falk		
IEC/TR 62351-12: Resilience and Security Recommendations for Power Systems with DER	2016	Cleveland		
IEC/TR 62351-13: Guidelines on What Security Topics Should Be Covered in Standards and Specifications	2016	Cleveland		
IEC/IS 62351-14 Cyber Security Event Logging	NWIP	Kumar	Based on existing security logging	NWIP by 6/ IS 12/2020
IEC/TR 62351-90-1: Guidelines for Using Part 8 Roles	2018	Fries	Submitted to IEC as TR in 11/2017	WD 3/
IEC/TR 62351-90-2 Deep Packet Inspection	2018	Carullo	TR to discuss the issues around deep packet inspection	
IEC/TR 62351-90-3 Guidelines for Network Management	DC	Carullo	Ready to submit DC	
IEC/TS 62351-100-1: Conformance test cases for IEC 62351-5 and IEC 60870-5-7	2018	Grechi	Conformance testing of 62351-5 and 60870-5-7	
IEC/TS 62351-100-3: Conformance test cases for IEC 62351-3	CD	Grechi	Separated Part 3 from this TS to 100-3 as CD	NWIP 7/
IEC/TS 62351-100-4: Conformance testing for 62351-4 with IEC 61850	NWIP	Lacroix	Conformance testing for IEC 61850	
IEC/TS 62351-100-6-1: Conformance testing for 62351-6 with IEC 61850-8-1 and 61850-9-2	NWIP	Lacroix	Conformance testing for IEC 61850	
IEC/TR 61850-90-19: Using Role Based Access Control (RBAC) and IEC 61850 (joint with WG10)	WG10 Effort	Falk	Joint effort with WG10	
IEC/TR 62351-90-4 or White Paper? Use cases for how best to use the IEC 62351 series	Starting on DC	Fries	Use cases for how best to use the IEC 62351 series	Under

Digital substation – Ideal bild



- IEDs
- Isolerad PC
- Korrekt inställd gateway och brandväg

Verkligheten



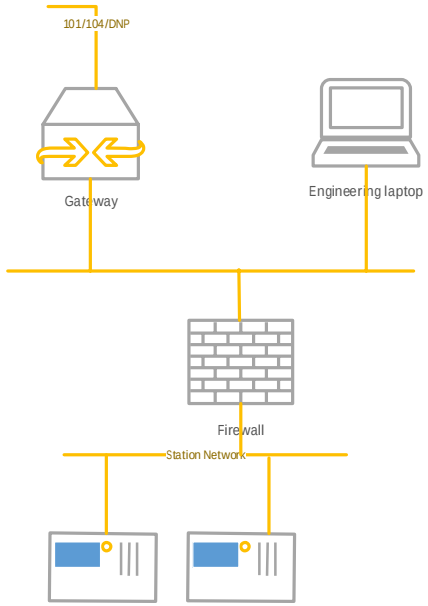
- Odokumenterade uppkopplingar
  - Support
  - Leverantörer
- Bärbara datorer
- USB minnen etc

Största risker

- Människor
- Enheter som har *relationer* med omvärlden

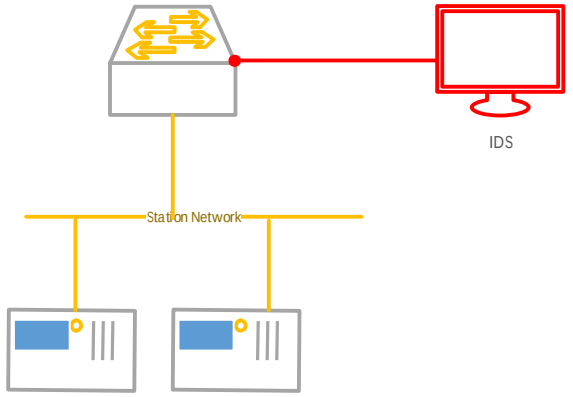
Minska risken

- Patchning
- Extra brandväggar
  - Fördelar
  - Problem
- Nätverksövervakning



Nätverksövervakning

- SNMP
- IEC 62351-7
- Syslog

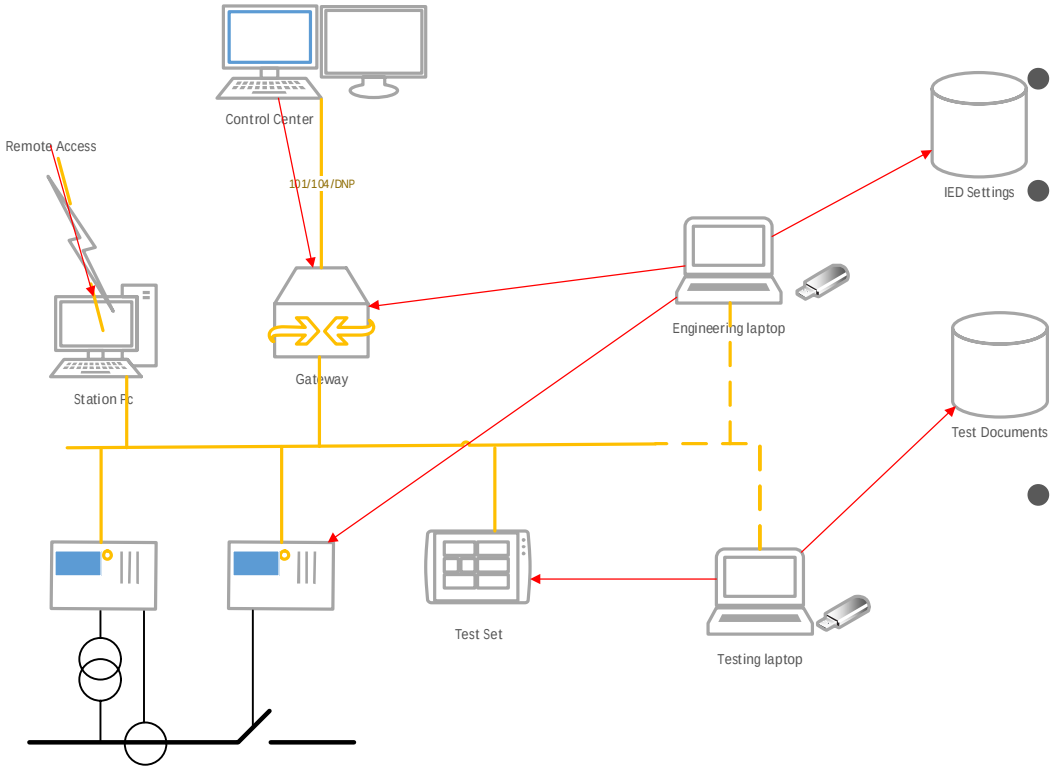


- SIEM

IEC 62351-7

- **IEC 62351 Part 7 (IS 2017) specifies data object models to monitor the health and the condition of the power system components/communications**

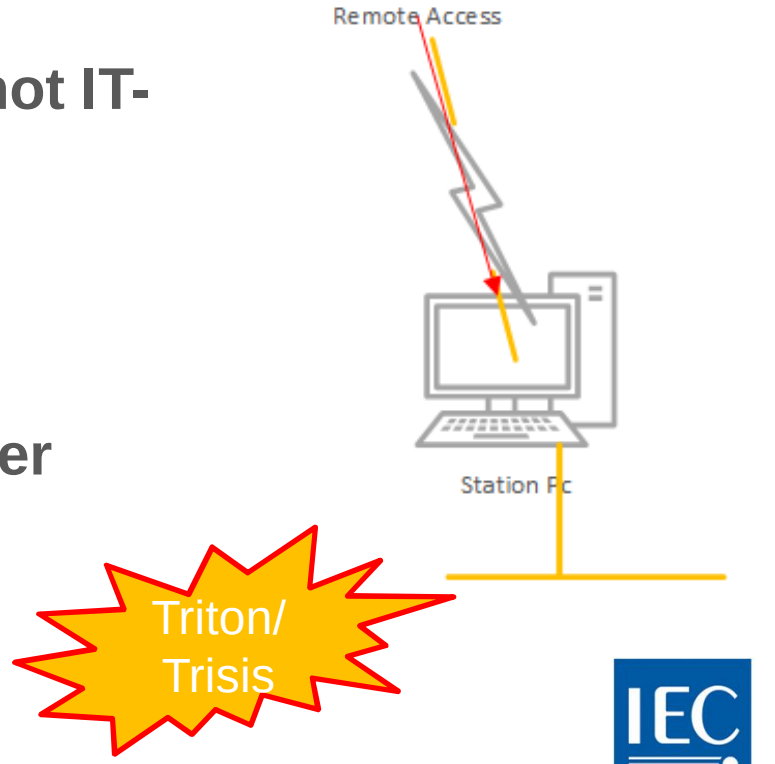
Attack vektorer



- Fjärråtkomst
- Direkt uppkopplade laptops
- USB-minnen

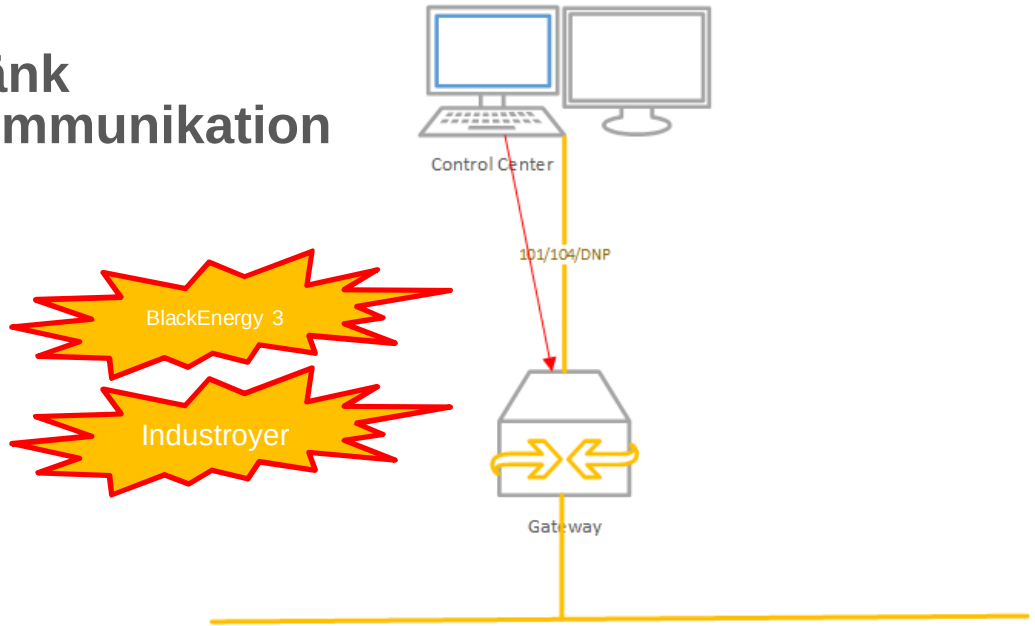
Hot: Fjärråtkomst

- Hot
  - Odokumenterade kopplingar mot IT-system
    - Direkt
    - VPN
  - Remote desktop
- Motmedel
  - Styr koppling från kontrollcenter
  - 2-faktor
  - Process
  - Nätverksövervakning



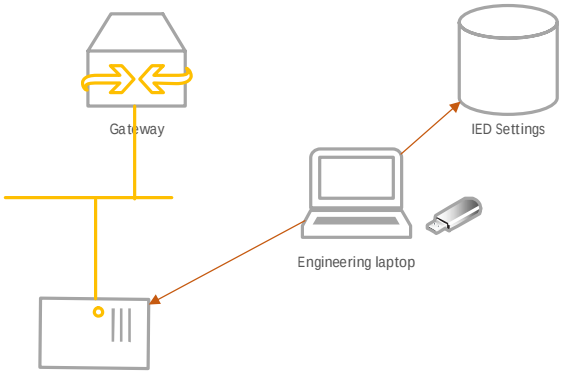
Hot: Kontrollcenter/Gateways

- Hot
  - Kommunikations länk
  - Icke autoriserad kommunikation
- Exempel
  - Ukraina 2015
  - Ukraina 2016
- Motmedel
  - Begränsa protokoll
  - Inre brandvägg
  - Övervaka gateway

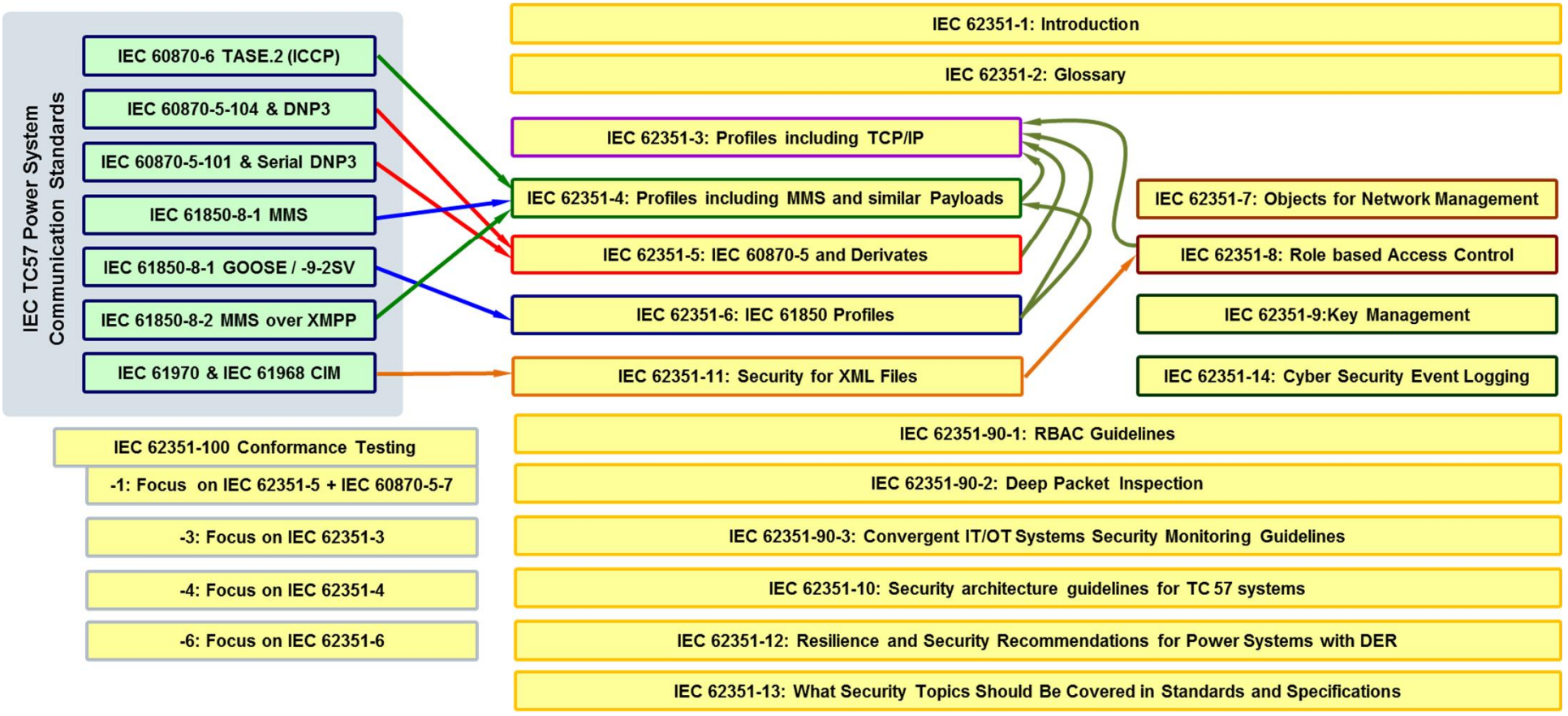


Hot: Engineering pc

- Hot
  - Laptop kopplas mot nätverk
- Motmedel
  - Definierad process hur överföring av dokument ska göras
  - Dedikerad pc



Mapping of TC57 Communication Standards to IEC 62351 Security Standards (Update)



IEC TS 62351-1: Introduction

- Released 2007
  - Ingen planerad revision
- Bakgrund till CS
- Översikt över delarna


TECHNICAL SPECIFICATION

IEC TS 62351-1

First edition
2007-05

Power systems management and associated information exchange – Data and communications security

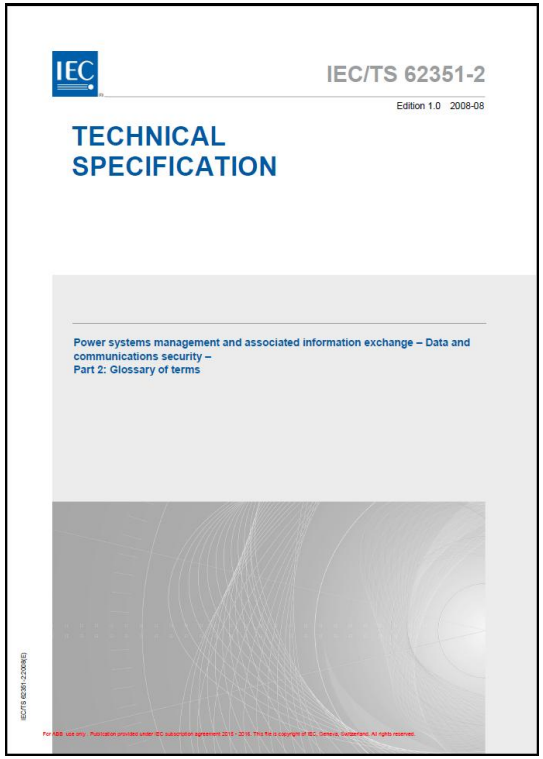
Part 1:
Communication network and system security – Introduction to security issues

IEC

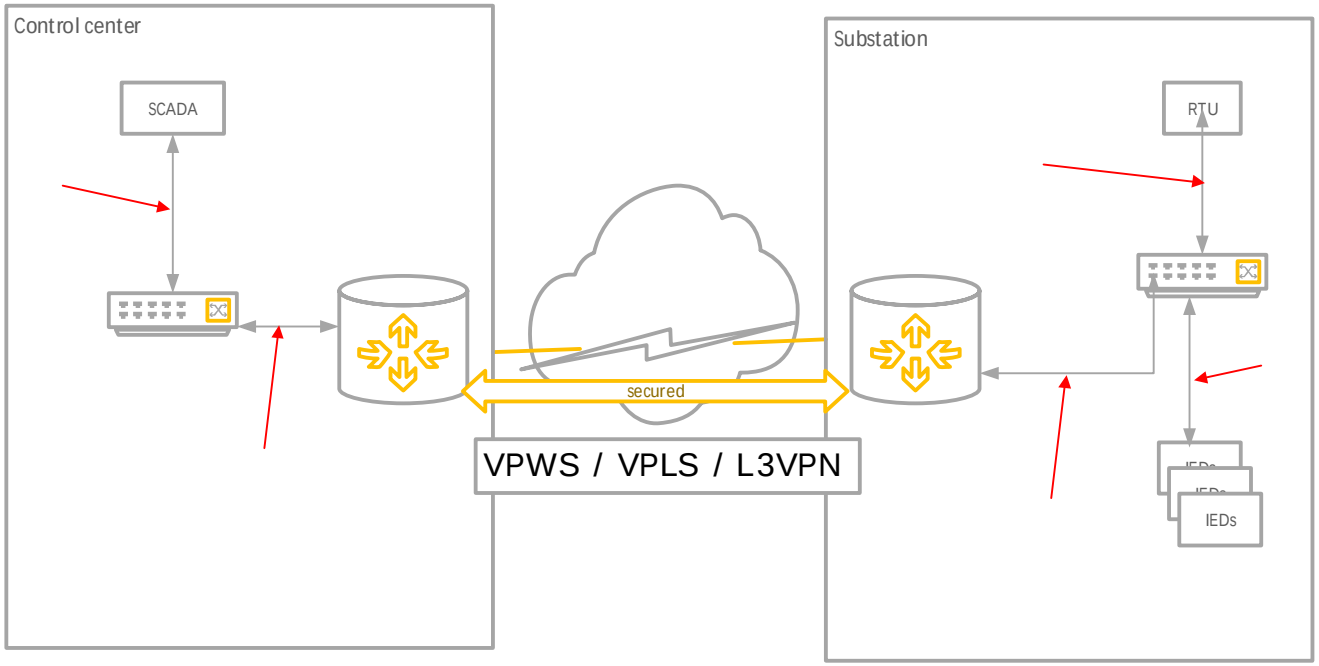
Reference number
IEC/TS 62351-1:2007(E)

IEC TS 62351-2: Glossary of terms

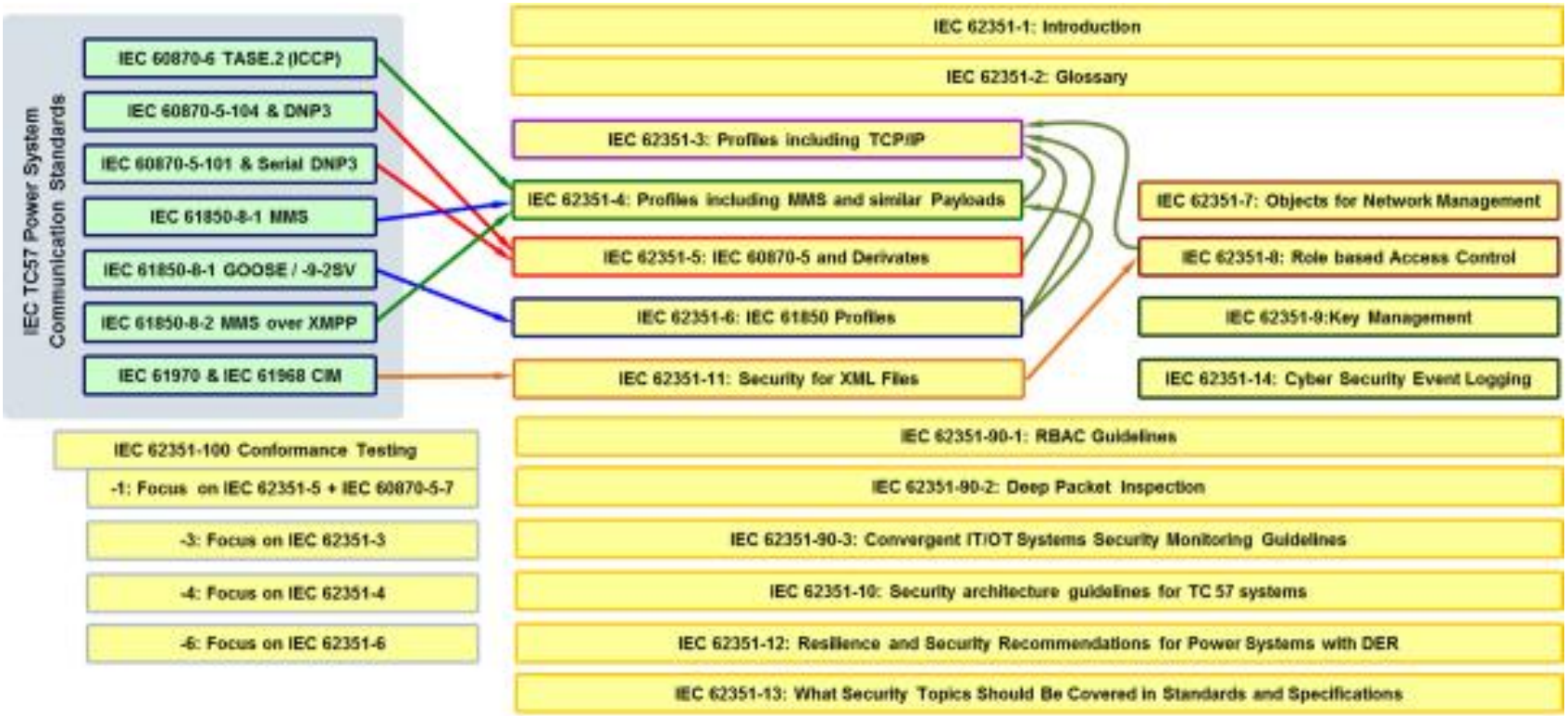
- **Released 2008**
  - **Revidering pågår**



Säkra WAN-kommunikaitonen IEC 61850-90-12

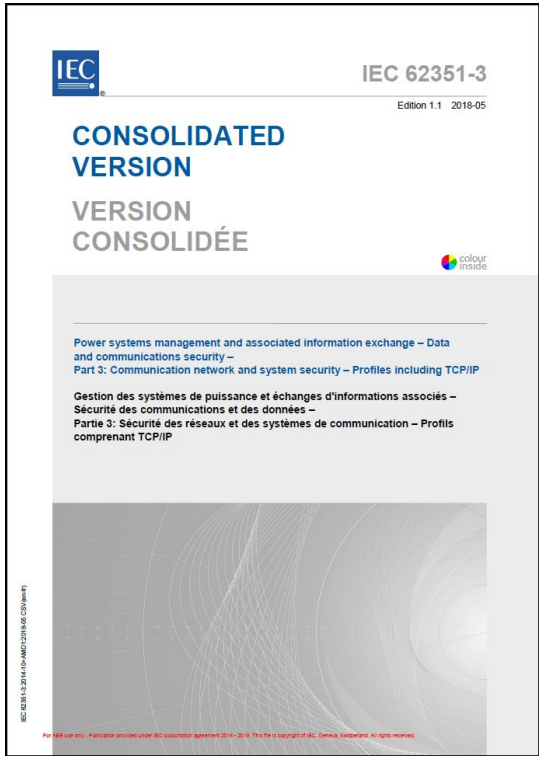


3,4,5 & 6


IEC TC-57 Power System Communication Standards
IEC 60870-6 TASE.2 (ICCP)
IEC 60870-5-104 & DNP3
IEC 60870-5-101 & Serial DNP3
IEC 61850-8-1 MMS
IEC 61850-8-1 GOOSE / -9-2SV
IEC 61850-8-2 MMS over XMPP
IEC 61970 & IEC 61968 CIM
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:Key Management
IEC 62351-14: Cyber Security Event Logging
IEC 62351-100 Conformance Testing
-1: Focus on IEC 62351-5 + IEC 60870-5-7
-3: Focus on IEC 62351-3
-4: Focus on IEC 62351-4
-5: Focus on IEC 62351-6
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 62351-10: 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

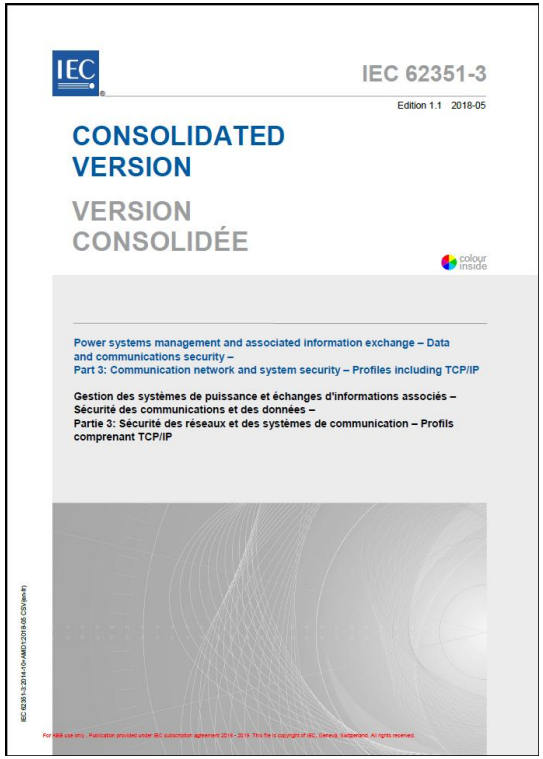
IEC/IS 62351-3: Security for profiles including TCP/IP

- *"how to provide confidentiality, integrity protection, and message level authentication for SCADA and telecontrol protocols that make use of TCP/IP as a message transport layer when cyber-security is required"*

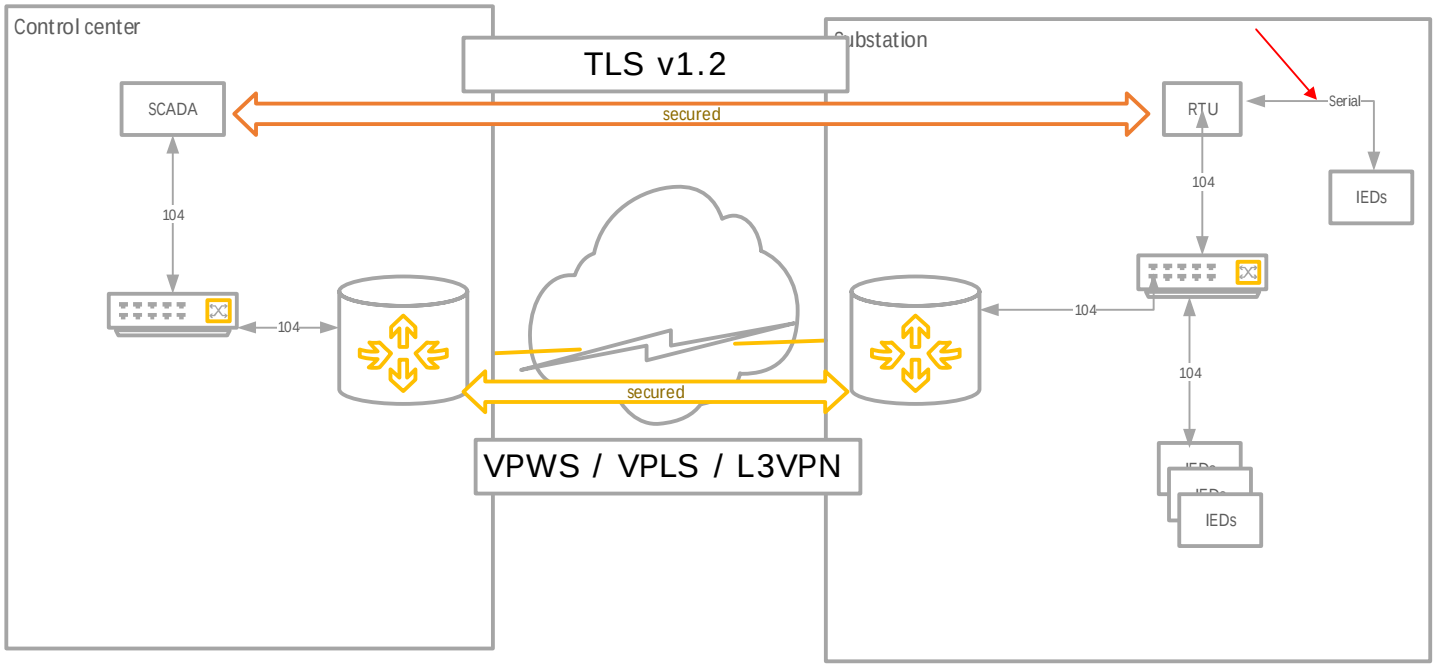


IEC/IS 62351-3: Security for profiles including TCP/IP

- Ed 1.1 Released 2018
  - Revidering pågår AMD2 (Ed 1.2) (2019-07)
  - Även Ed 2 diskuteras

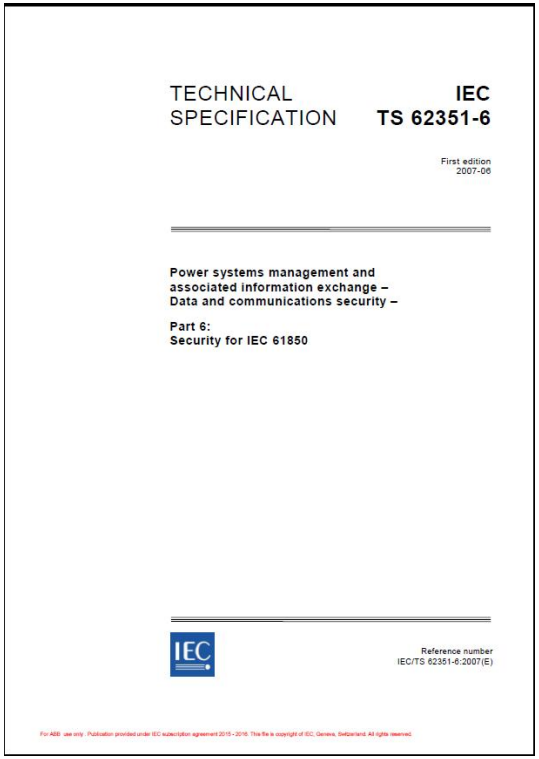


IEC 62351-3
Lägg till transportlagersäkerhet till slutenhet



IEC/IS 62351-5: Security for IEC 60870-5 and derivatives

- **Specifies messages, procedures and algorithms for securing the operation of all protocols based on or derived from IEC 60870-5**
  - IEC 60870-5-101
  - IEC 60870-5-102
  - IEC 60870-5-103
  - IEC 60870-5-104
  - DNP3 Distributed Network Protocol


TECHNICAL SPECIFICATION

IEC TS 62351-6

First edition
2007-06

Power systems management and associated information exchange – Data and communications security –

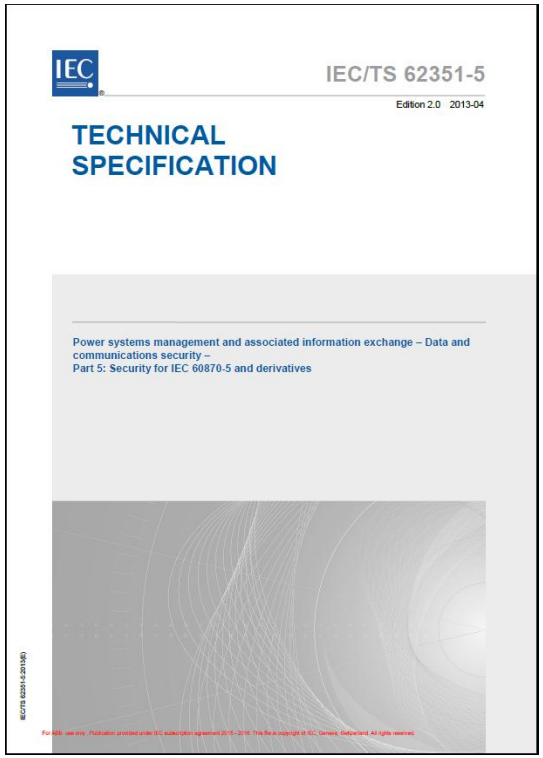
Part 6:
Security for IEC 61850

IEC

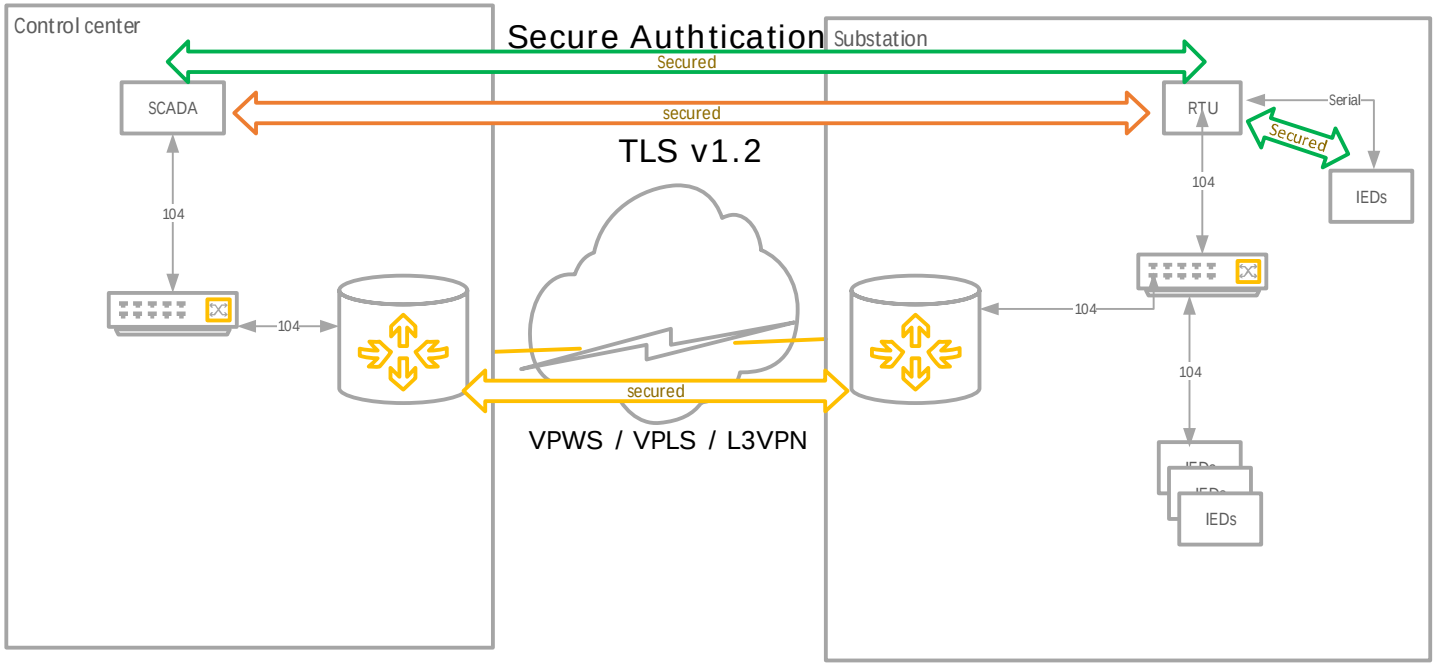
Reference number
IEC/TS 62351-6:2007(E)

IEC/IS 62351-5: Security for IEC 60870-5 and derivatives

- TS Ed2 Released April 2013,
- IS under utveckling, slutet av 2019
- Resolve the issues identified by the DNP 3SA and IEC 60870-5 implementors
- Integrate the new functional requirements currently being defined in the DNP 3SA WG and WG 15 to improve the standard.
- Provide common solutions for both DNP 3 and 60870 -5 protocols security extension

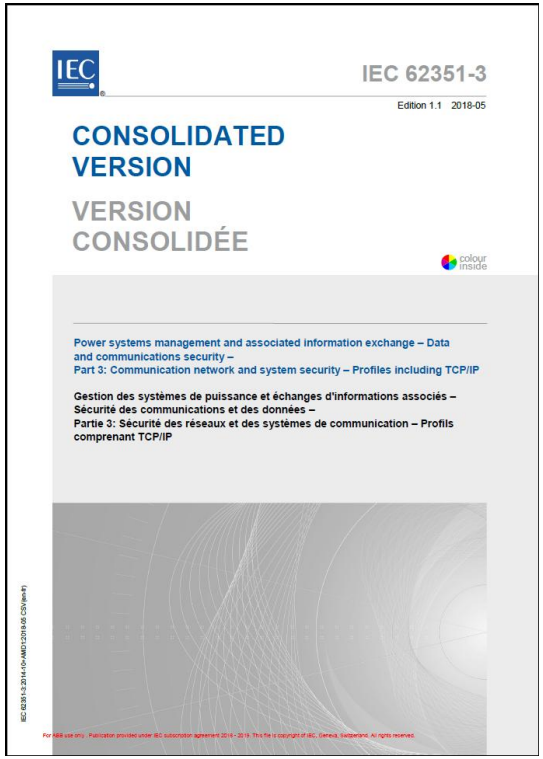


IEC 62351-5
Säkra applikationslagret



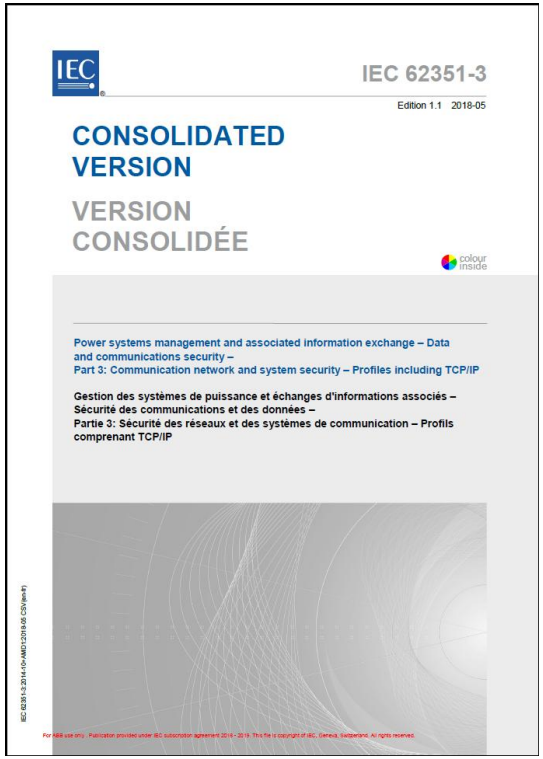
IEC/IS 62351-4: Security for profiles including MMS and derivatives

- MMS
  - Autentisering handskakning, data överföring
  - Nyckelhantering och kryptering av data överföring
  - End-to-end säkerhet
- OSI och XMPP



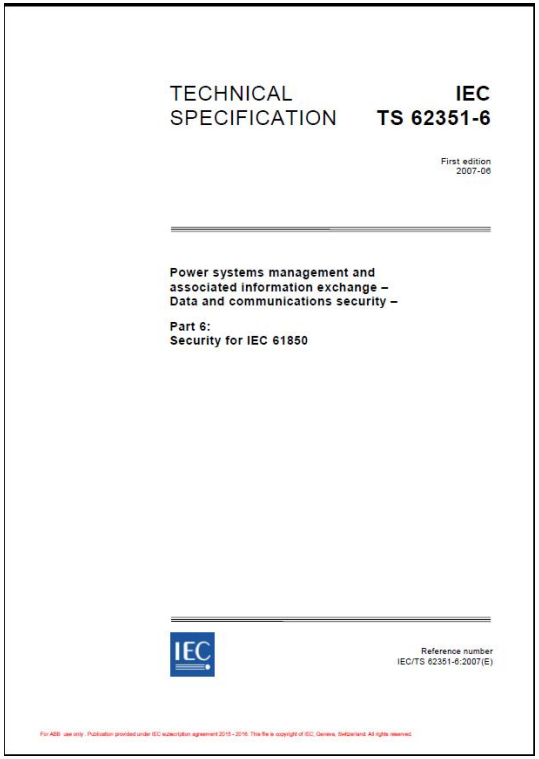
IEC/IS 62351-4: Security for profiles including MMS and derivatives

- Ed 1.0 Released 2018
  - Revidering pågår AMD1 (Ed 1.1)
  - Rättning av felaktigheter
  - Väntar på stabil -3



IEC/TS 62351-6: Security for IEC 61850 profiles

- 2007
- specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the standard IEC 61850
  - IEC 61850-8-1
  - IEC 61850-9-2
  - IEC 61850-6



TECHNICAL SPECIFICATION

IEC TS 62351-6

First edition
2007-06

Power systems management and associated information exchange – Data and communications security –

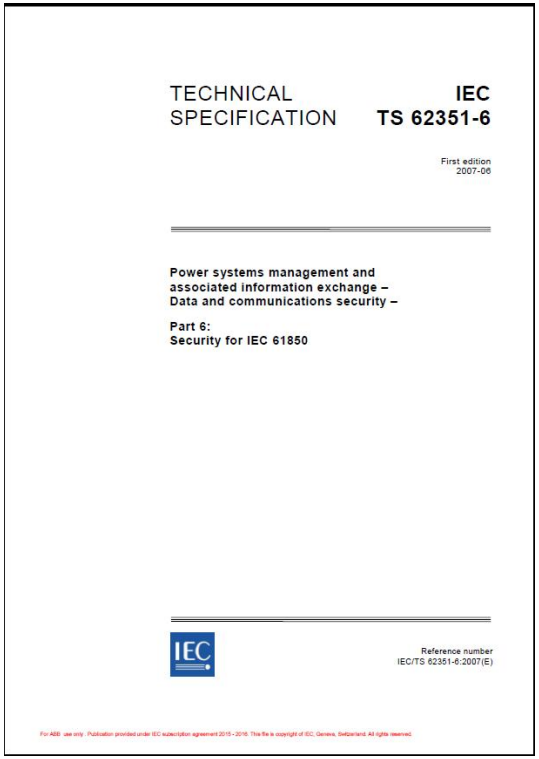
Part 6:
Security for IEC 61850

IEC

Reference number
IEC/TS 62351-6:2007(E)

IEC/TS 62351-6: Security for IEC 61850 profiles

- Pågående revison, TS 1.0 till IS 1.0. Planerad slutet av 2019
- Väntar på del 3 & 4
- Inkluderar ändringar i
  - IEC 62351-4
  - IEC 62351-8
  - IEC 61850-8-1
  - IEC 61850-8-2 (XMPP)



TECHNICAL SPECIFICATION

IEC TS 62351-6

First edition
2007-06

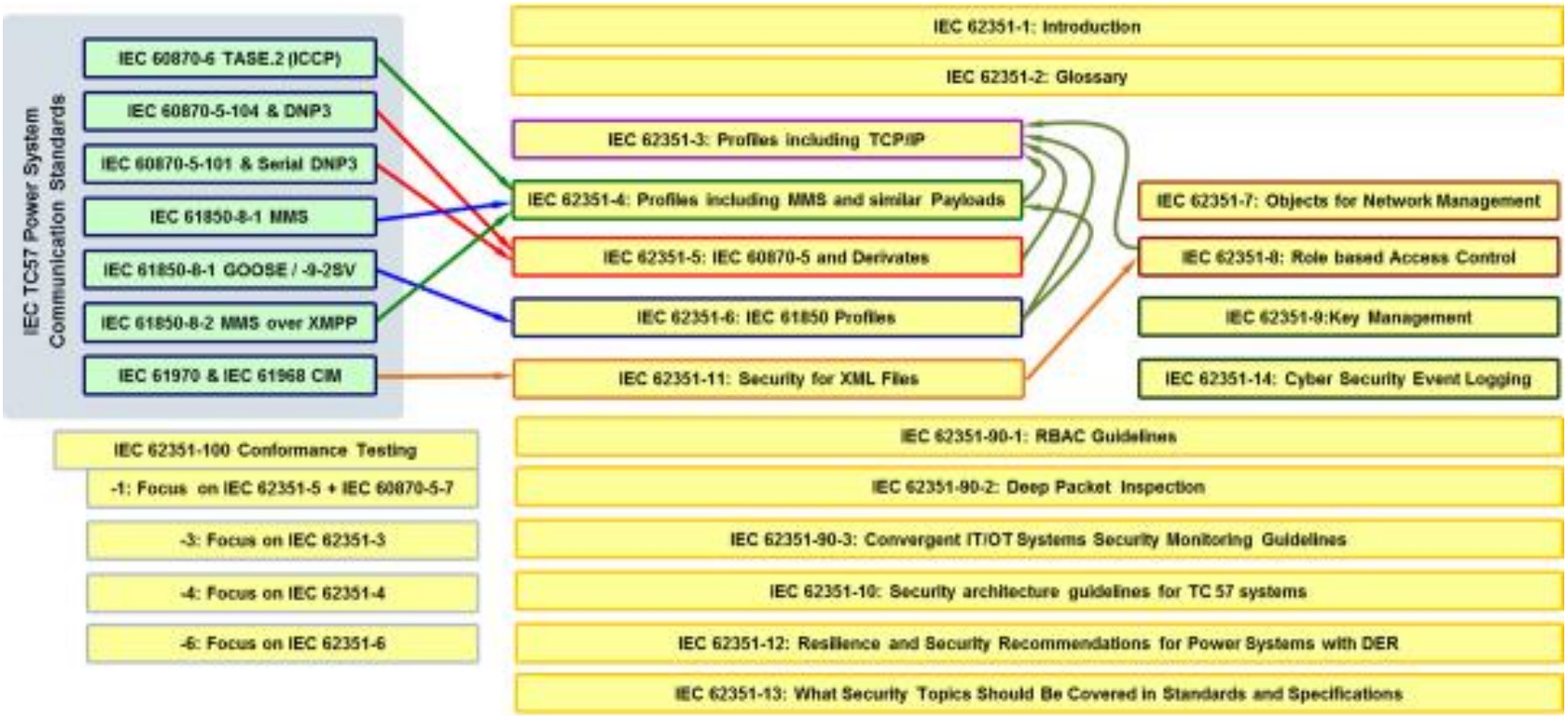
Power systems management and associated information exchange – Data and communications security –

Part 6:
Security for IEC 61850

IEC

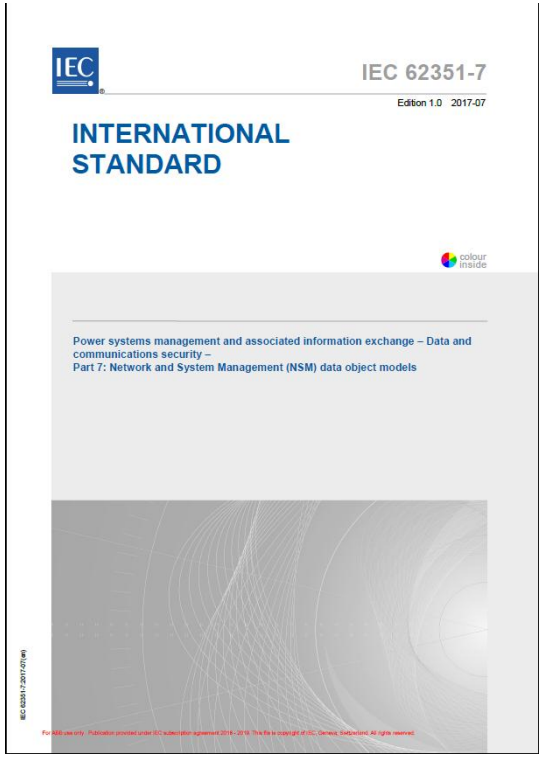
Reference number
IEC/TS 62351-6:2007(E)

7,8,9 & 11


IEC TC-57 Power System Communication Standards
IEC 60870-6 TASE.2 (ICCP)
IEC 60870-5-104 & DNP3
IEC 60870-5-101 & Serial DNP3
IEC 61850-8-1 MMS
IEC 61850-8-1 GOOSE / -9-2SV
IEC 61850-8-2 MMS over XMPP
IEC 61970 & IEC 61968 CIM
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:Key Management
IEC 62351-14: Cyber Security Event Logging
IEC 62351-100 Conformance Testing
-1: Focus on IEC 62351-5 + IEC 60870-5-7
-3: Focus on IEC 62351-3
-4: Focus on IEC 62351-4
-6: Focus on IEC 62351-6
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 62351-10: 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

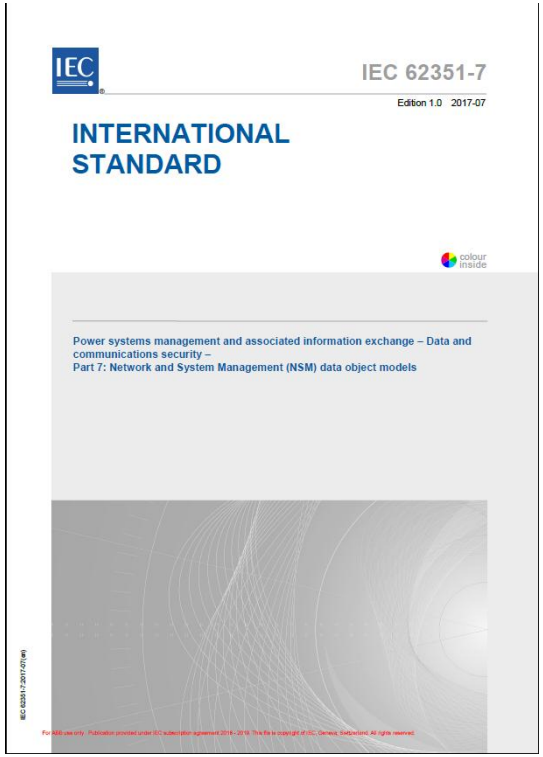
IEC/IS 62351-7: Network and System Management (NSM) data object models

- monitor the health of networks and systems, to detect possible security intrusions
- to manage the performance and reliability of the information infrastructure.
- Abstract data model
- Adaption to SNMP MIBs



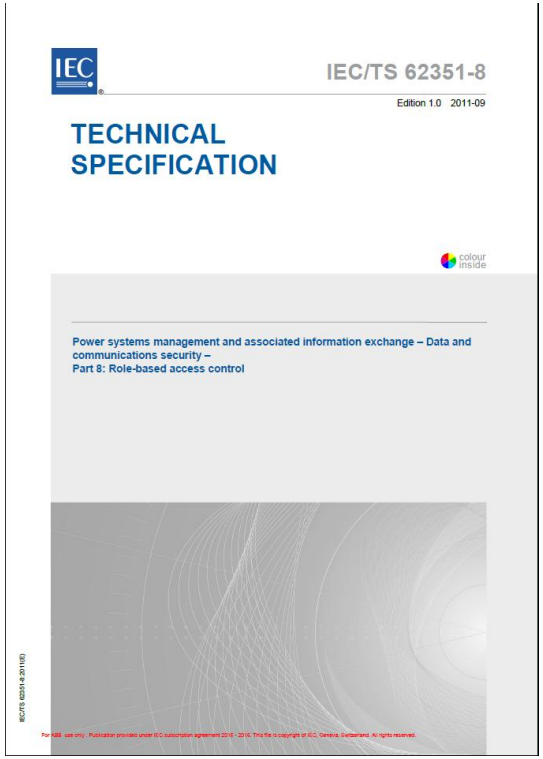
IEC/IS 62351-7: Network and System Management (NSM) data object models

- **Reviderad (TS till IS) 2017**
  - **SNMP MIBs**



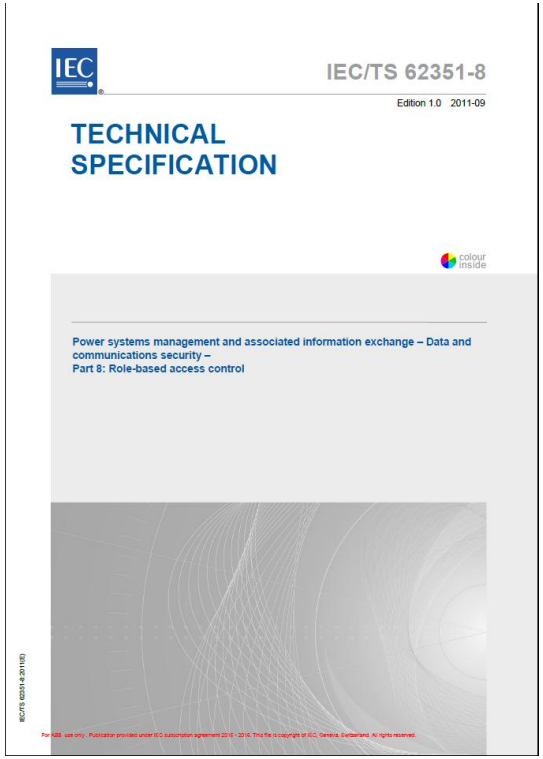
IEC/TS 62351-8: Role-Based Access Control

- covers the access control of users and automated agents to data objects in power systems by means of role-based access control

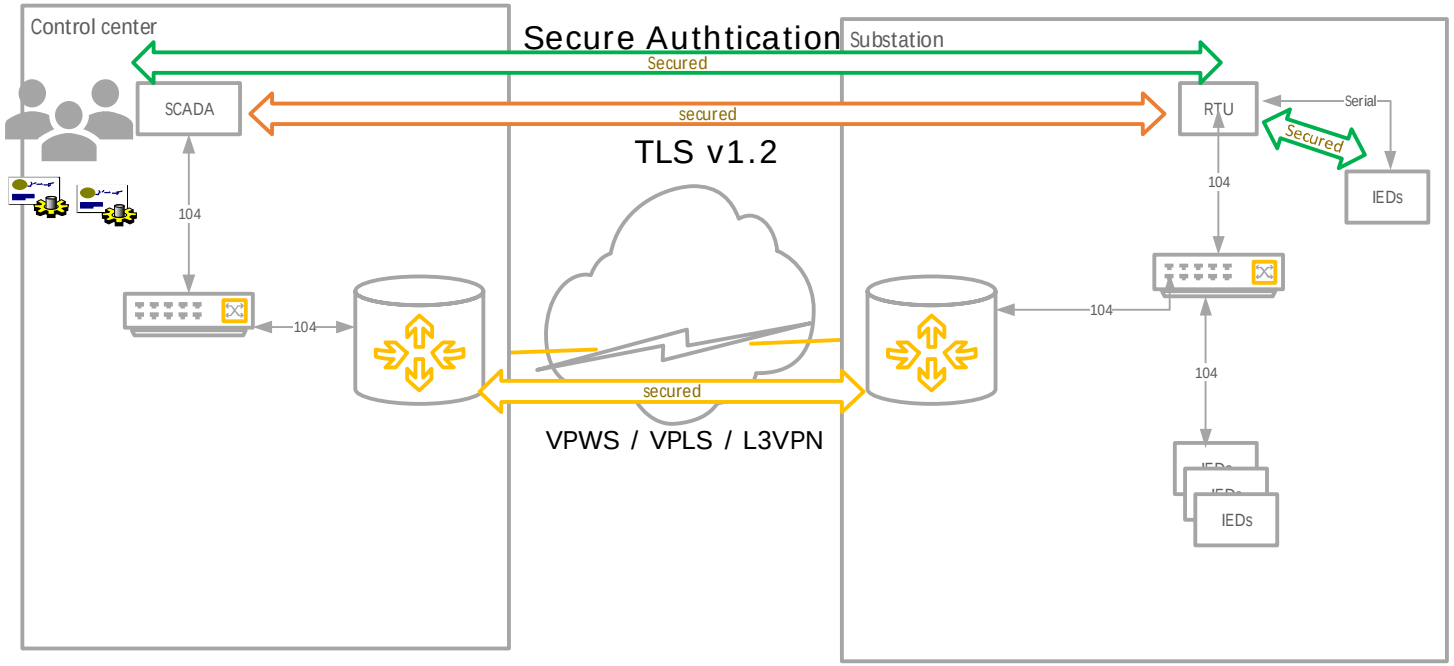


IEC/TS 62351-8: Role-Based Access Control

- Revidering pågår
  - TS till IS
  - Början av 2020
- Scope
  - Ytterligare profiler
  - Funktionella förbättringar
  - Specifikation av ”custom roles”
  - Utökat scope (utanför 61850)

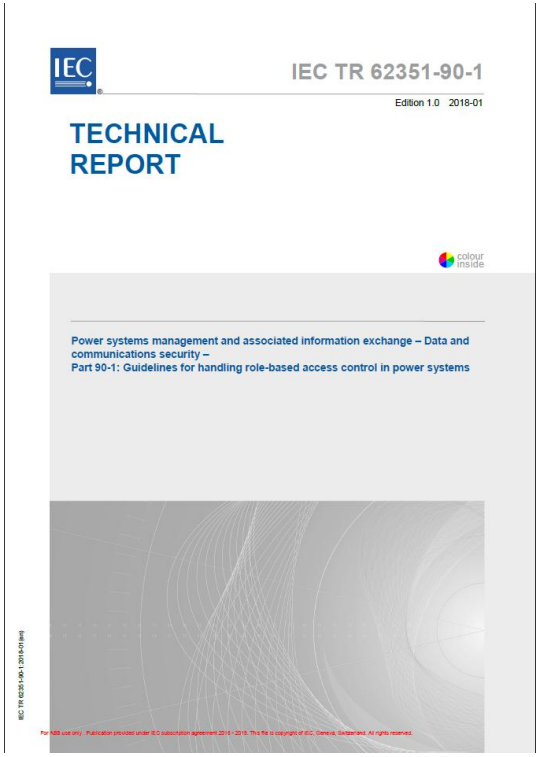


Användare och roller



IEC/TR 62351-90-1: Guidelines for handling role-based access control in power systems

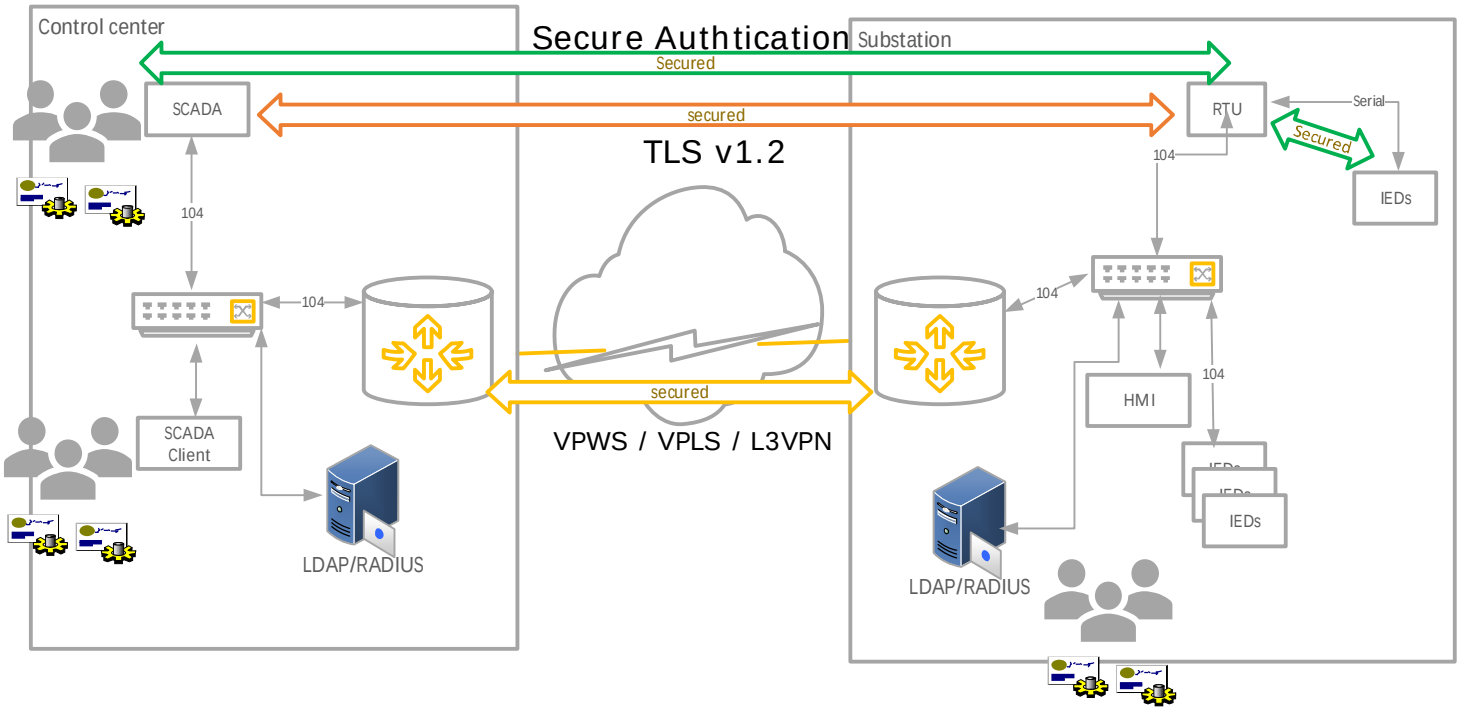
- Defines three profiles for the transmission of RBAC related information
- public key certificates, attribute certificates, or software tokens
- mandatory roles and associated rights for IEC 61850



IEC/IS 62351-9: Key Management

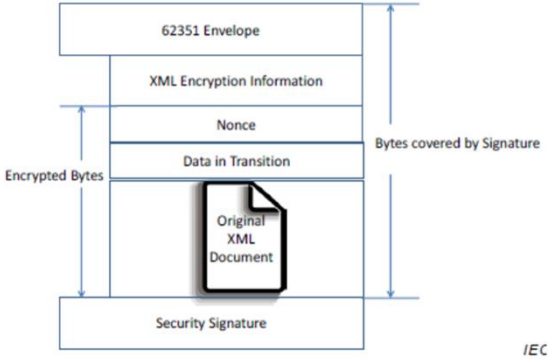
- Hantering a kryptografiska nycklar
  - Asymmetriska nycklar (privata och publika nyklar
  - Symetriska nyklar för grupper (GDOI)
- Nyckelhantering
  - Generering
  - Distrubution
  - Revokering
- Hantering av nycklar till certifikat för skydd av data och kommunikation

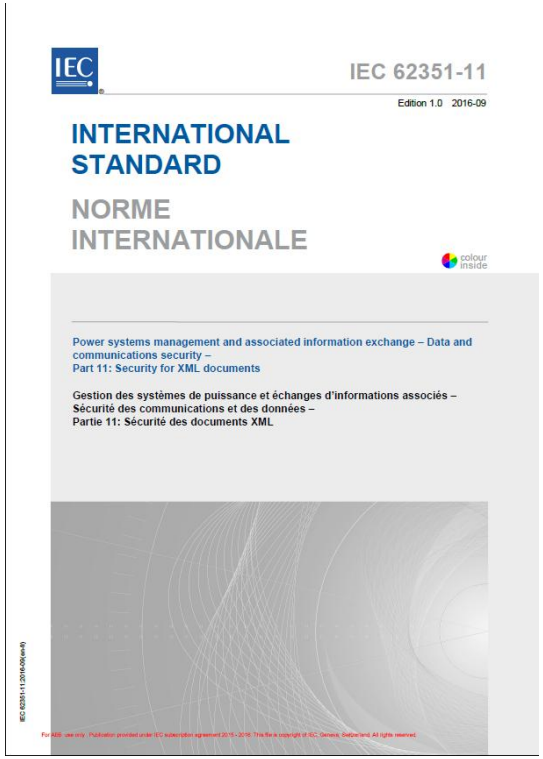
Ytterligare funktioner



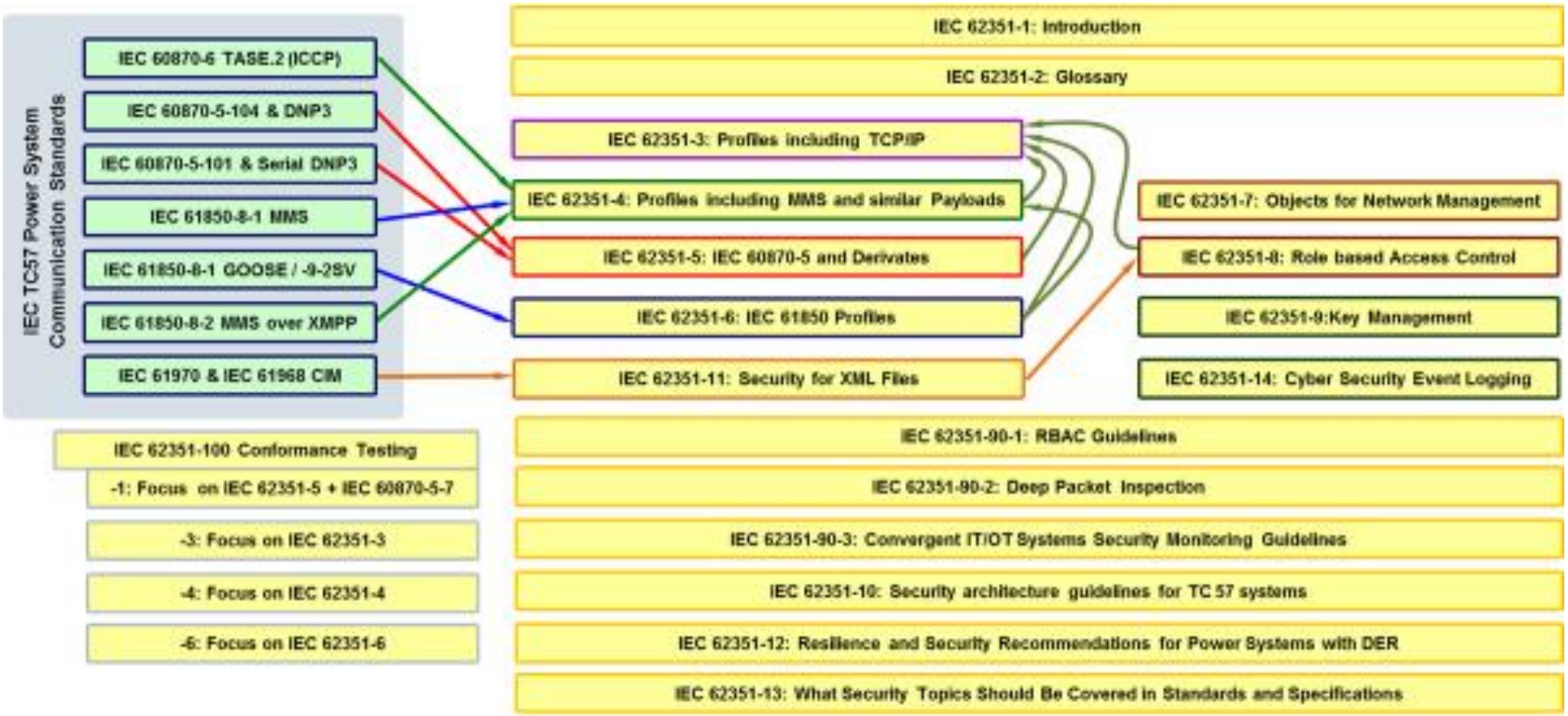
IEC/IS 62351-11: Security for XML documents

- securing XML
  - within the scope of the IEC
  - IEEE, etc



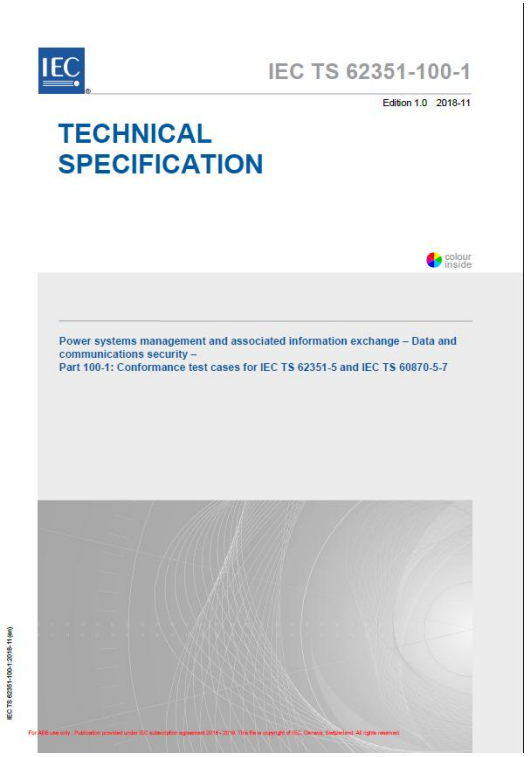


100-1…


IEC TC-57 Power System Communication Standards
IEC 60870-6 TASE.2 (ICCP)
IEC 60870-5-104 & DNP3
IEC 60870-5-101 & Serial DNP3
IEC 61850-8-1 MMS
IEC 61850-8-1 GOOSE / -9-2SV
IEC 61850-8-2 MMS over XMPP
IEC 61970 & IEC 61968 CIM
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:Key Management
IEC 62351-14: Cyber Security Event Logging
IEC 62351-100 Conformance Testing
-1: Focus on IEC 62351-5 + IEC 60870-5-7
-3: Focus on IEC 62351-3
-4: Focus on IEC 62351-4
-6: Focus on IEC 62351-6
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 62351-10: 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

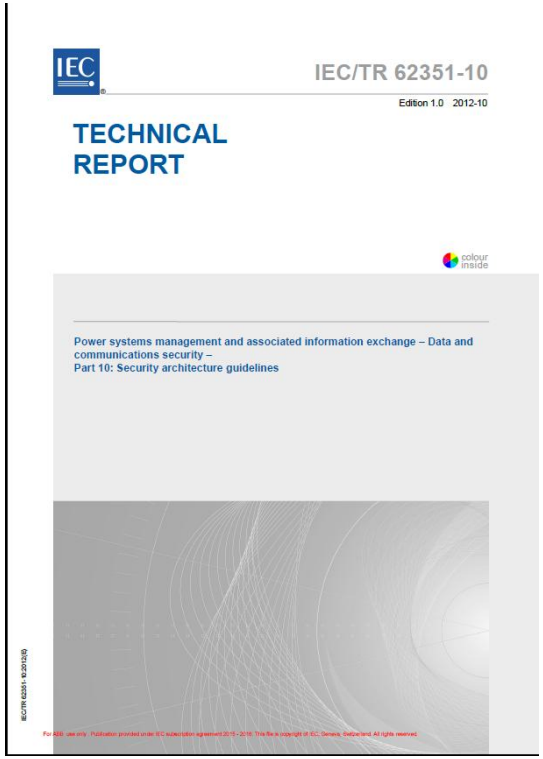
IEC/TS 62351-100-1: Conformance test cases for IEC 62351-5 and IEC 60870-5-7

- test cases for conformance testing of telecontrol equipment or systems using the IEC TS 62351-5



IEC/TR 62351-10: Security Architecture

- Guideline för implementation av säkerhetsfunktioner
- Baserad på installations exempel



IEC/TR 62351-12:Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems

- cyber security recommendations and engineering/operational strategies for improving the resilience of power systems with interconnected DER systems

IEC/TR 62351-13:Guidelines on security topics to be covered in standards and specifications

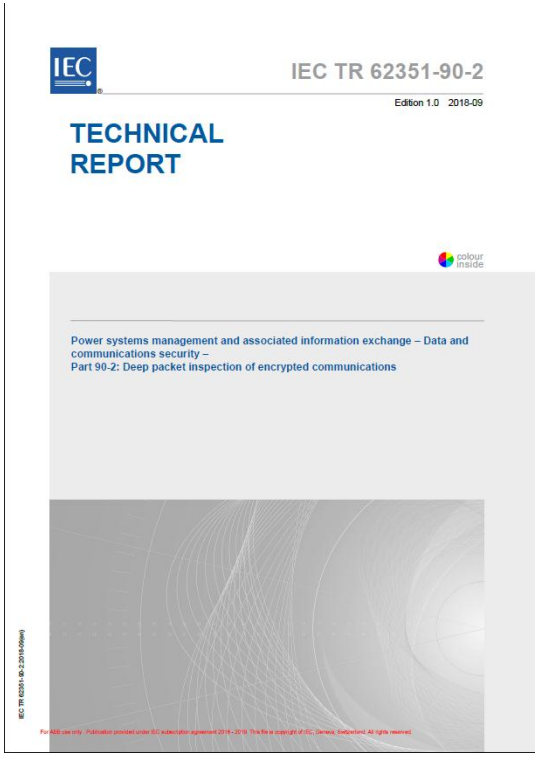
- Riktar sig till utvecklare av standarder.
- guidelines on what security topics could or should be covered in standards and specifications

IEC/TR 62351-13:Guidelines on security topics to be covered in standards and specifications

- Riktar sig till utvecklare av standarder.
- guidelines on what security topics could or should be covered in standards and specifications

IEC/TR 62351-90-2: Deep packet inspection of encrypted communications

- analyses the impact of encrypted communication channels in power systems introduced with the IEC 62351 series
- different techniques are analysed that can be employed to circumvent these issues when DPI of communications is required



Ongoing work

IEC/IS 62351-3: Security for profiles including TCP/IP	Ed 1.1 05/2018	IS Ed. 1 in 2014, updated to IS Ed.1.1 in 2018, currently in AMD2 phase. Revision to Ed.2 in discussion
IEC/IS 62351-4: Security for profiles including MMS and derivatives	IS 11/2018	IS in 11/2018, COR #1, AMD #1
IEC/IS 62351-5: Security for IEC 60870-5 and derivatives	DC, CD	TS Ed2 Released April 2013, IS underway
IEC/IS 62351-6: Security for IEC 61850 profiles	CDV	Updates underway
IEC/IS 62351-8: Role-Based Access Control	CDV	Finalization of CDV and conversion to IS
IEC/IS 62351-14 Cyber Security Event Logging	NWIP	Based on existing security logging
IEC/TR 62351-90-3 Guidelines for Network Management	DC	Ready to submit DC
IEC/TS 62351-100-3: Conformance test cases for IEC 62351-3	CD	Separated Part 3 from this TS to 100-3 as CD
IEC/TS 62351-100-4: Conformance testing for 62351-4 with IEC 61850	NWIP	Conformance testing for IEC 61850
IEC/TS 62351-100-6-1: Conformance testing for 62351-6 with IEC 61850-8-1 and 61850-9-2	NWIP	Conformance testing for IEC 61850
IEC/TR 61850-90-19: Using Role Based Access Control (RBAC) and IEC 61850 (joint with WG10)	WG10 Effort	Joint effort with WG10
IEC/TR 62351-90-4 or White Paper? Use cases for how best to use the IEC 62351 series	Starting on DC	Use cases for how best to use the IEC 62351 series