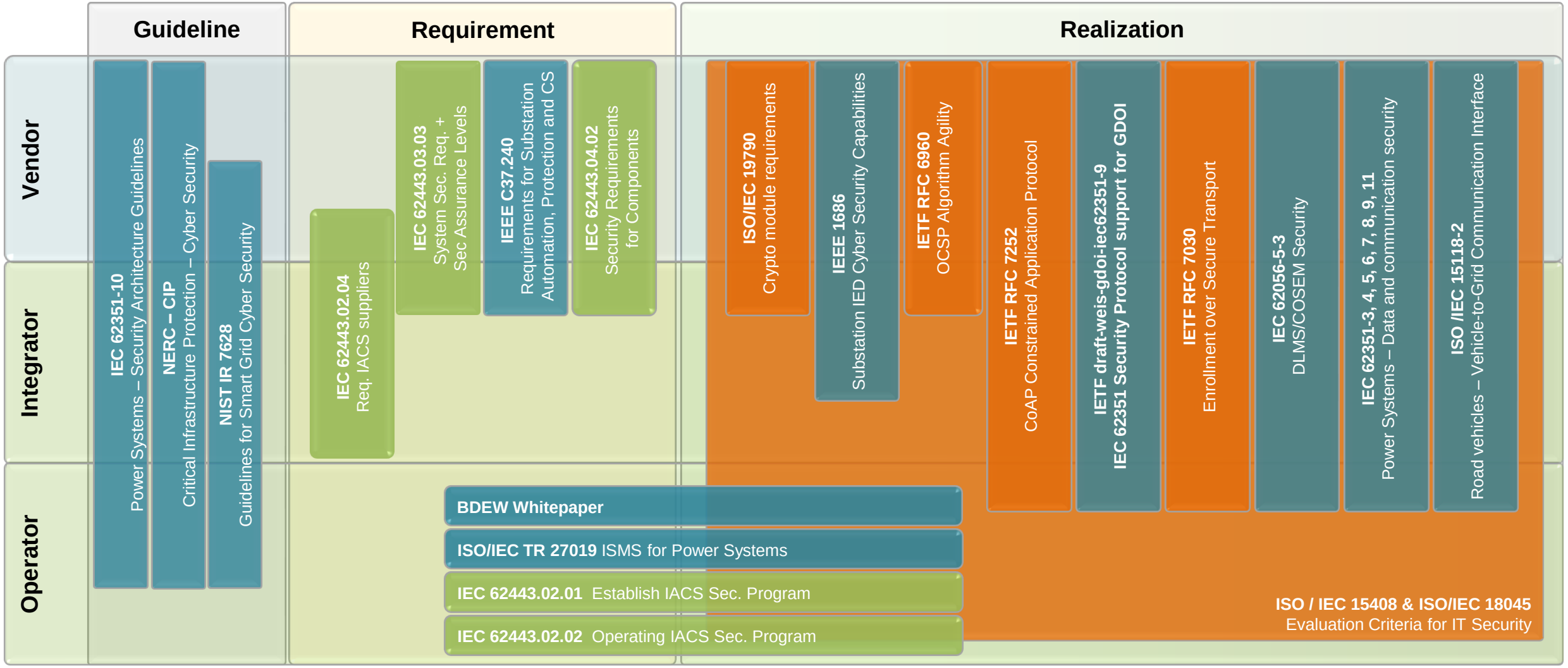
Security in Power System Automation

Status and Application of IEC 62351

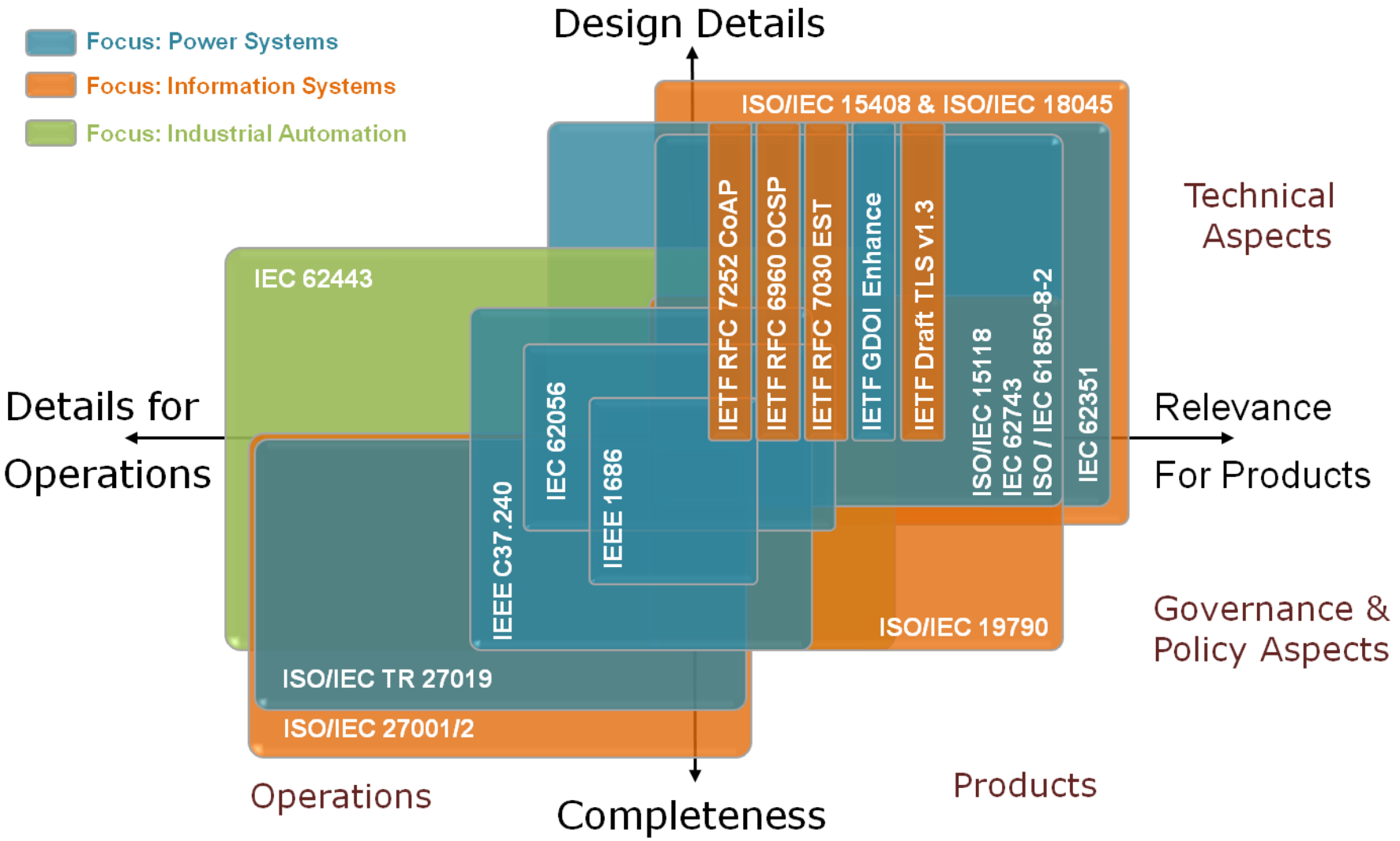
Steffen Fries, Siemens Corporate Technology, June 13th, 2017

Interoperability through security standards for the power utility ecosystem involves vendors, integrators, operators (Results from SEG-CG 2016)



Source http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx

Digital Grid security involves vendors, integrators, and operators
Coverage of standards (Results from SEG-CG 2016)



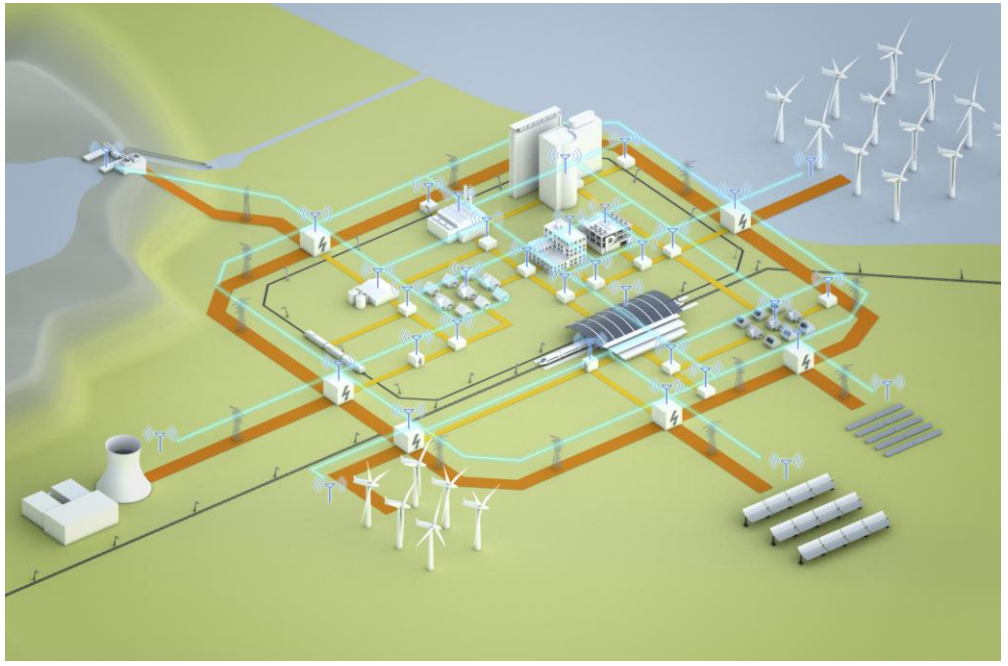
- **Standards have different importance for**
  - Product and system vendor
  - Integrator
  - Operator

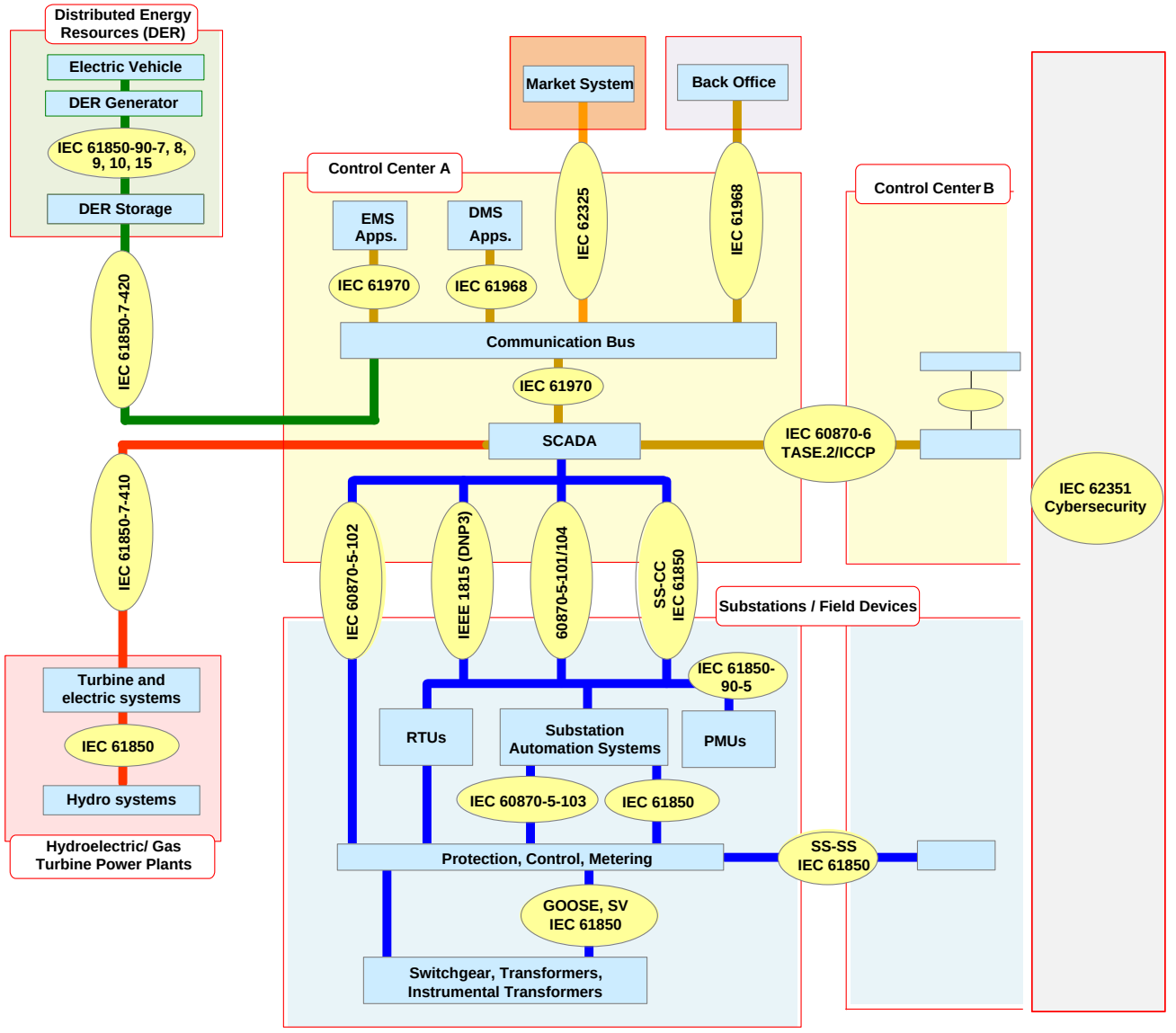
  as they target
  - specific technical means ensuring interoperability
  - procedural requirements
  - addressing risk based security requirements
  - auditablity of actions

Source http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx

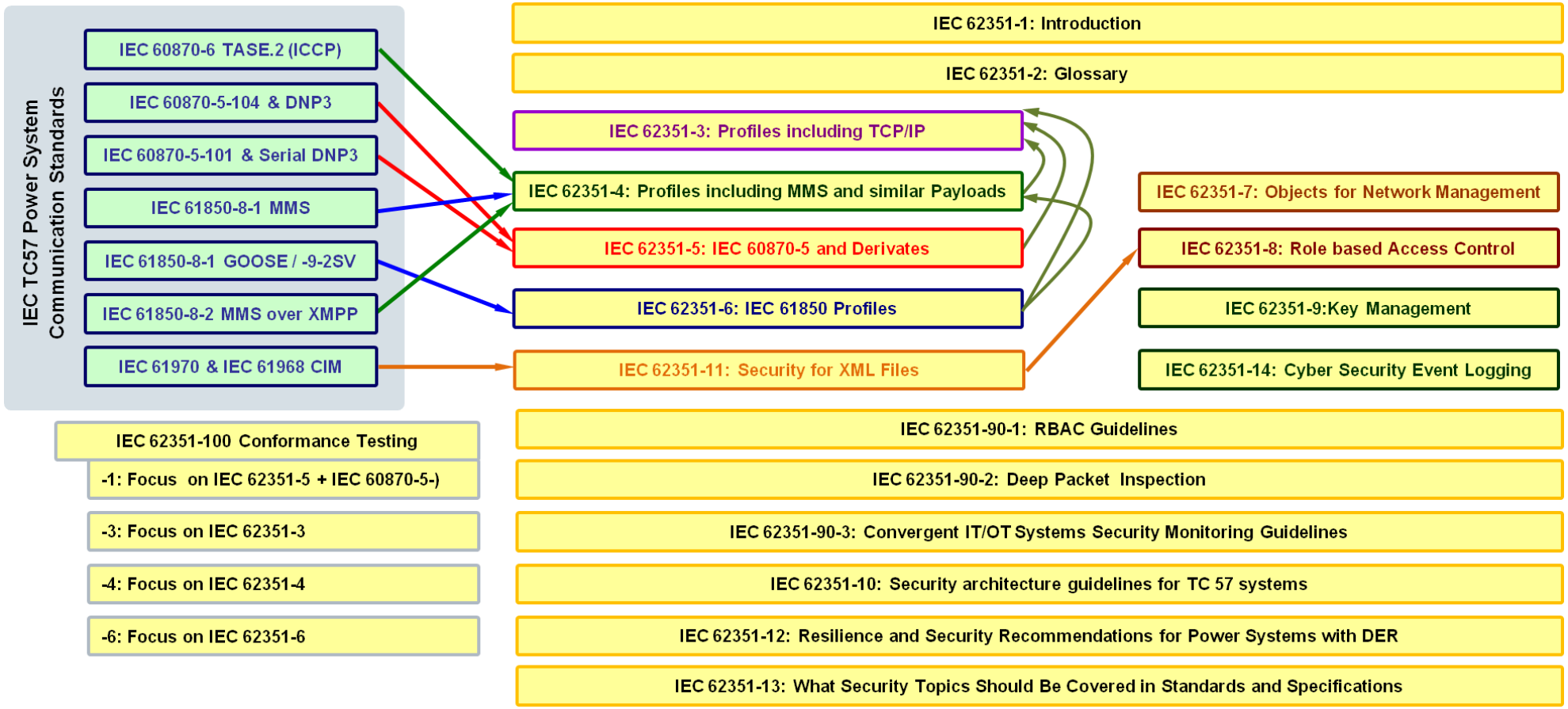
Core communication standards for Digital Grids
IEC TC57 reference architecture with domain-specific cyber security

- **IEC 61970 / 61968** Common Information Model (CIM)
- **IEC 62325** Market Communication using CIM
- **IEC 61850** Substation, Distribution, DER Automation
- **IEC 60870** Telecontrol Protocols (serial/TCP)
- **IEC 62351** Security for Power Systems





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

by utilizing or profiling

- existing standards and recommendations

IEC 62351 Overview
Introduction to the standard, guidelines, and recommendations

IEC 62351-1: Introduction

IEC 62351-2: Glossary

The standard comprises several technical reports, which either provide overview about applications or a specific solution examples

- **Part 1 and 2:** Introduction and glossary
- **Part 90-1:** Guidance for using role-based access control (RBAC) specifically the handling of custom based roles
- **Part 90-2:** Guidance for supporting deep packet inspection (DPI) when using encrypted communication links
- **Part 90-3**: Guidance on applying monitoring and logging in power systems (using SNMP and syslog)
- **Part 10:** Overview and typical requirements to security architectures in power automation
- **Part 12:** Recommendations for the incorporation of decentralized energy resources DER in the power grid
- **Part 13:** Recommendations for editors of standards and specifications regarding the handling of security specific requirements in power systems

IEC 62351-90-1: RBAC Guidelines

IEC 62351-90-2: Deep Packet Inspection

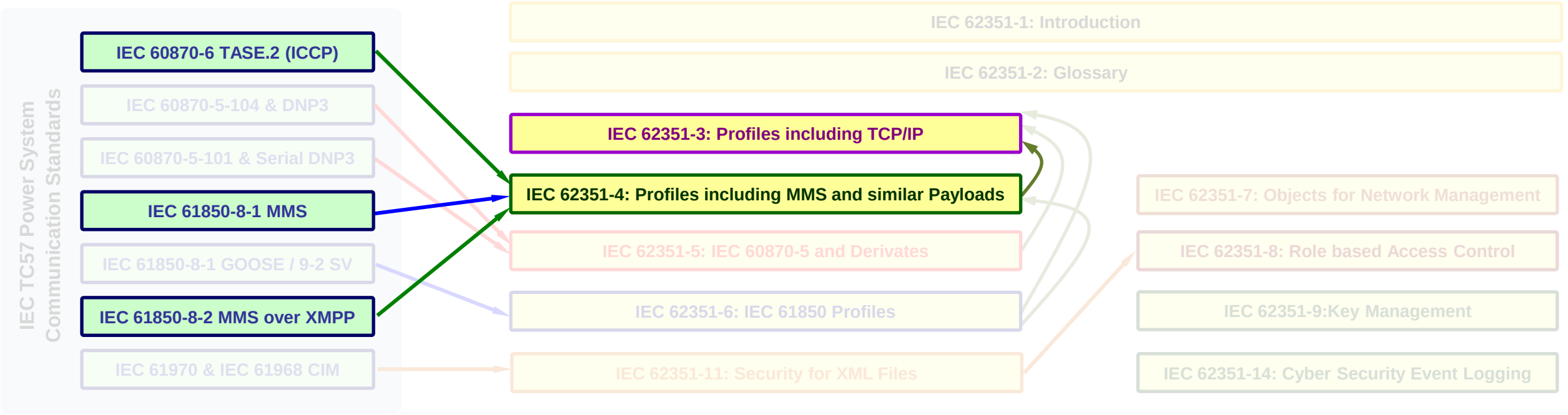
IEC 62351-90-3: Convergent IT/OT Systems Security Monitoring Guidelines

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

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

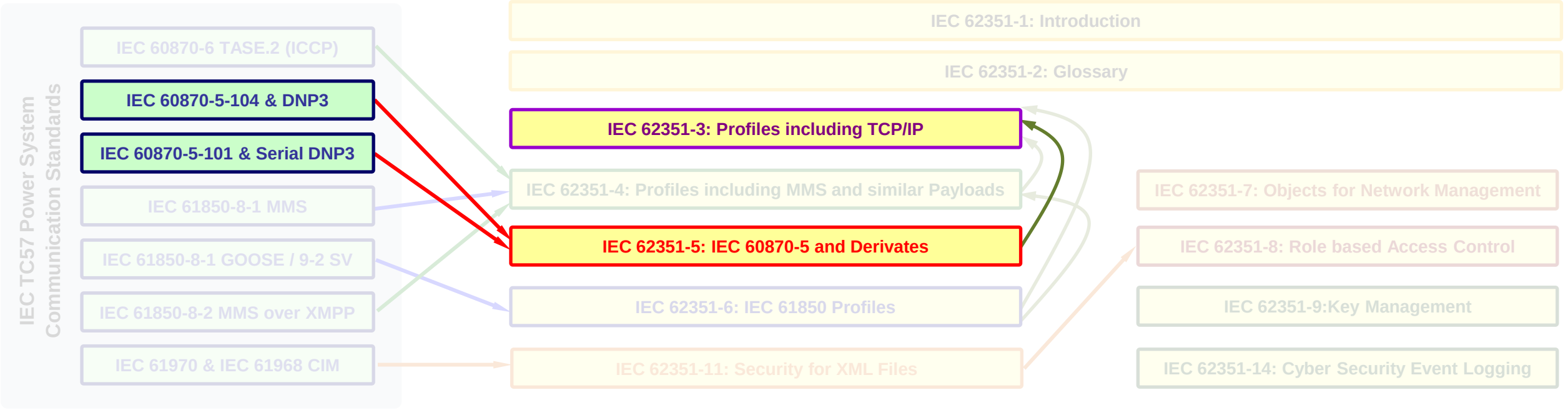
IEC 62351-13: What Security Topics Should Be Covered in Standards and Specifications

IEC 62351 Overview
Protection of control centers and substations



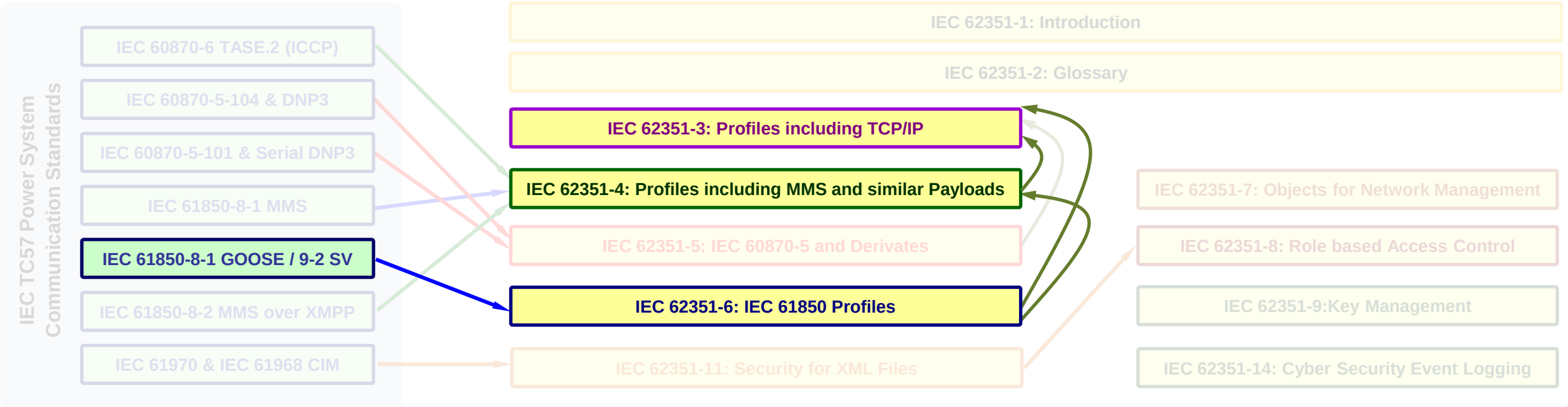
- **Part 3:** Profiling of the existing security protocol Transport Layer Security (TLS) to protect TCP based communication. This part is used in conjunction with other parts of IEC 62351 and enables a re-use of existing solutions.
- **Part 4:** Utilizes part 3 to protect the TCP based IEC 61850 communication (T-profile) and defines additional security mechanisms on application layer (A-profiles) to protect end-to-end security in scenarios with classical communication (e.g., control center to substation) or web-based approaches (e.g., for the introduction of DER using publish-subscribe mechanisms)
- **Example applications are control center communication and substation automation.**

IEC 62351 Overview
Protection of telecontrol



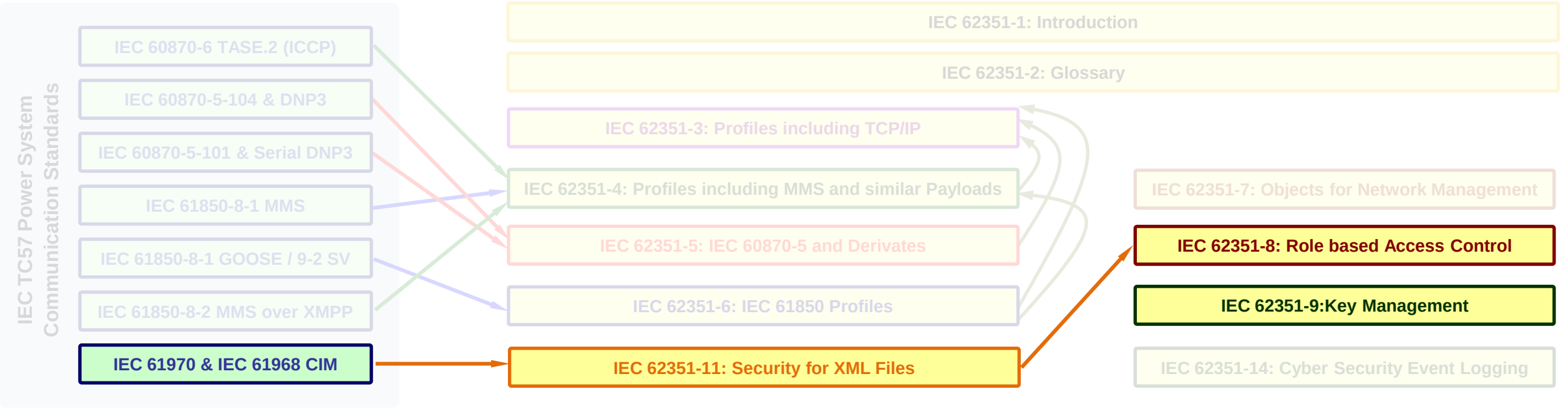
- **Part 3:** Profiling of the existing security protocol Transport Layer Security (TLS) to protect TCP based communication. This part is used in conjunction with other parts of IEC 62351 and enables a re-use of existing solutions.
- **Part 5:** Utilizes part 3 to protect the TCP based IEC 61850 communication (T-profile). Additionally, security mechanisms are defined to protect serial communication (IEC 61850-5-101) and CNP3 (IEEE 1518)
- **Example applications are control center communication and substation automation.**

IEC 62351 Overview
Data exchange in real-time targeting reliable protection



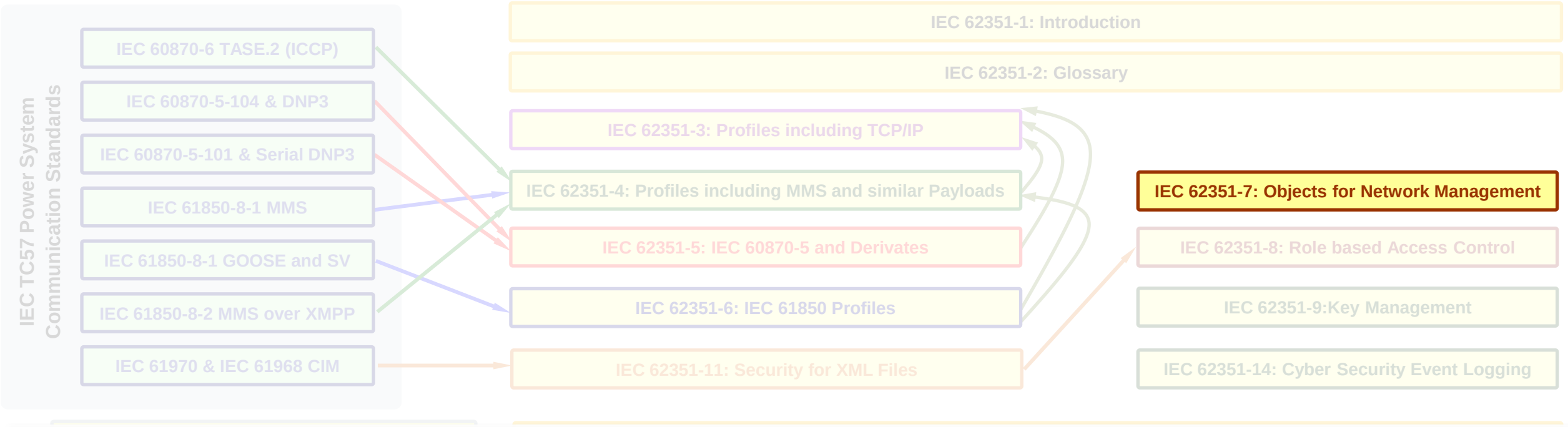
- **Part 3:** Profiling of the existing security protocol Transport Layer Security (TLS) to protect TCP based communication. This part is used in conjunction with other parts of IEC 62351 and enables a re-use of existing solutions.
- **Part 6:** Utilizes part 3 to protect the TCP based IEC 61850 communication (T-profile in conjunction with Part 4). Additionally, security mechanisms are defined to protect GOOSE and SV supporting multicast communication
- **Example applications stem from substation automation, specifically the data exchange of protection devices or between PMUs in the transmission network.**

IEC 62351 Overview
Data exchange via XML based files – Yes, but secure!



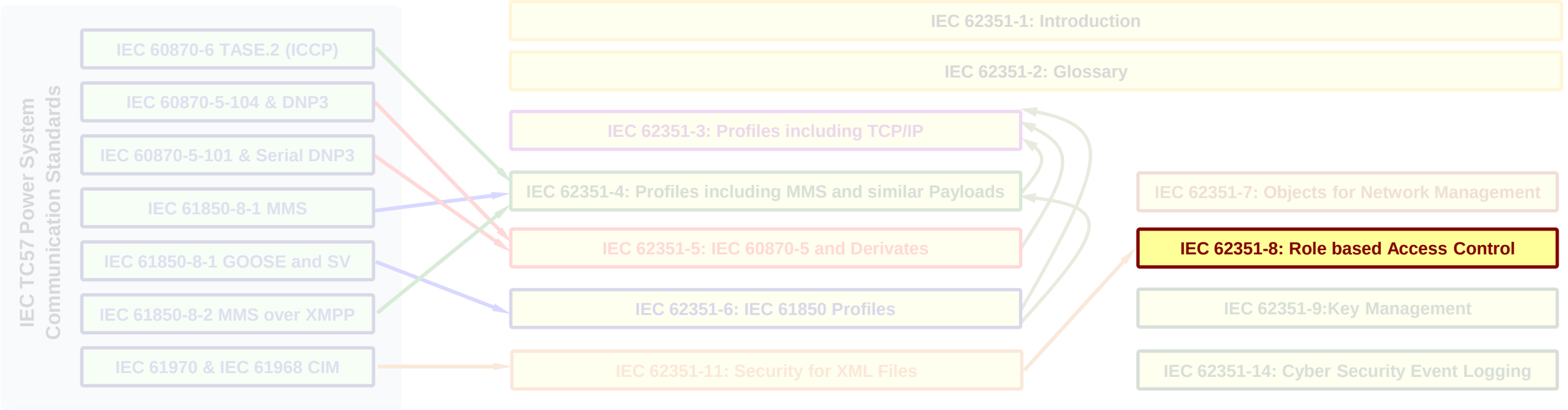
- **Part 11:** Provides protection of XML based data, which can be enhanced with RBAC elements
- **Example applications are provided by the data exchange between energy providers**

IEC 62351 Overview
Determination of power system security status



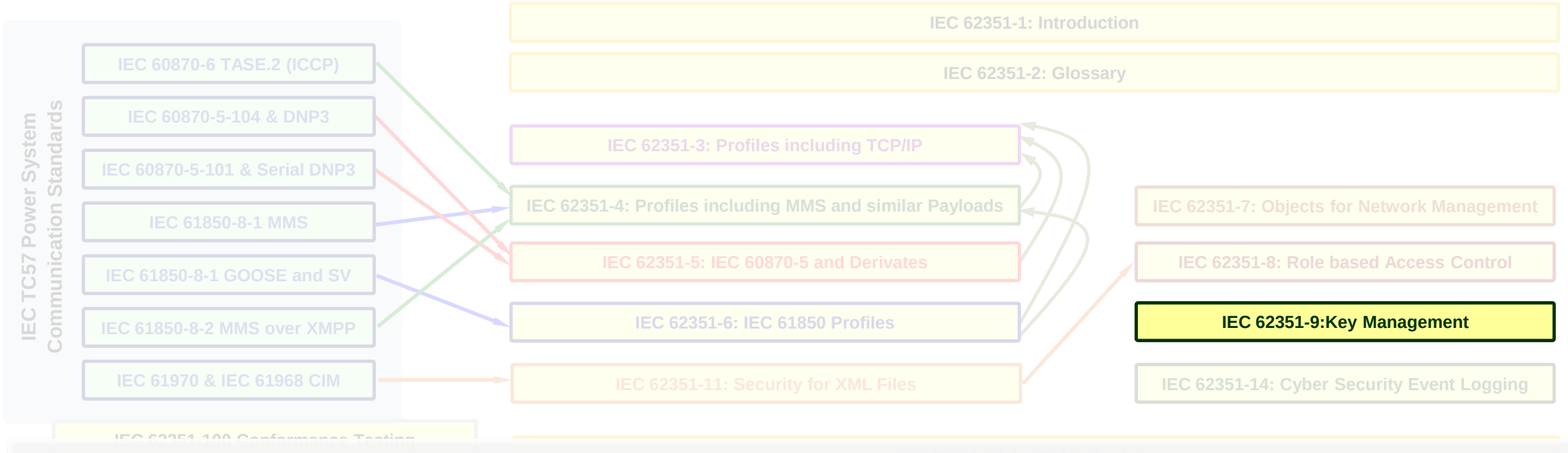
- **Part 7:** Defines monitoring events for network management, which can be utilized over standard protocols for management to exchange monitoring information. The definition is in form of a Management Information Base (MIB) and is explicitly mapped to SNMP.
- **Example applications are network management and enable, e.g., the joint analysis of power system specific monitoring events in the context of an existing network management. This in turn enables the closer exchange of IT and OT relevant information to derive a system view.**

IEC 62351 Overview
Access control to system resources



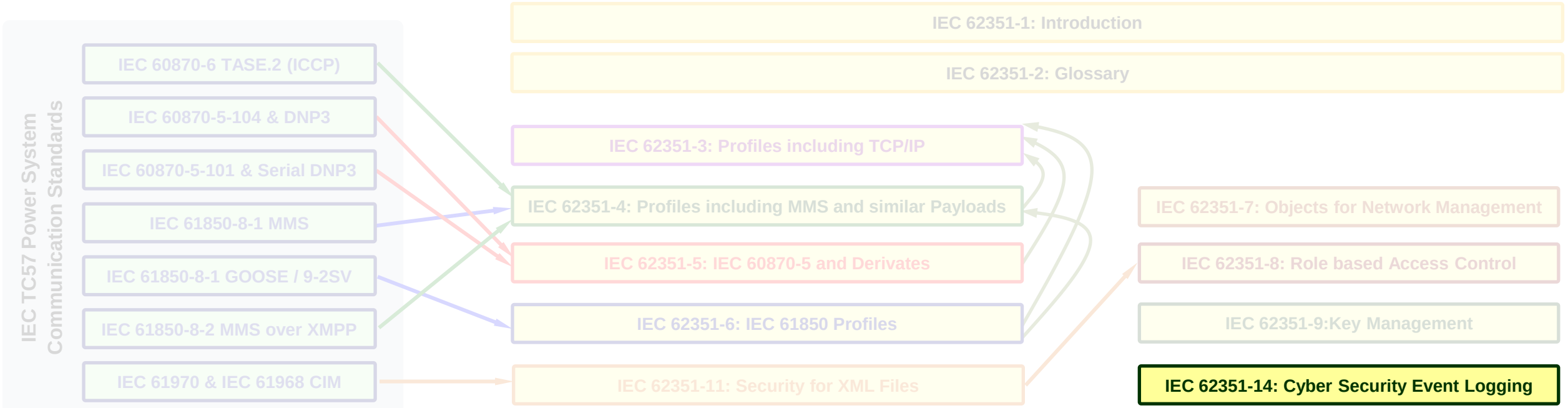
- **Part 8:** Defines 3 profiles for role-based access control. They enable the assignment of roles to authorized users or applications, which can be dynamic. The assignment of one or more rights to a role has a more static character. The role information is either provided directly to the user/application or may be fetched by the accessed entity, e.g., via LDAP.
- **Example applications target access control of local applications (HMI) but also remote administration and maintenance.**

IEC 62351 Overview
Management of security credentials



- **Part 9:** Provides the base for the management of credentials and keys to be used in the security mechanisms of the different IEC 62351 parts, It addresses the management of certificates and corresponding private keys, which are utilized in almost every part of IEC 62351. Additionally it defines the group based communication security in the context of multicast communication scenarios.
- **Example applications for certificate and corresponding private keys comprise the user and component authentication. Group based security is applied in substation communication using GOOSE.**

IEC 62351 Overview
Secure logging



- **Part 14:** Defines security events to be logged by the components used for error analysis and auditing. The events are defined in a general format, while the transport mapping is done to syslog specifically.
- **Example applications are substation automation, specifically events generated in protection devices and substation controllers.**

IEC 62351 Overview
Conformance testing

- **Part 100:** Umbrella standard for conformance test descriptions of the IEC 62351 parts to help implementers to provide standard compliant functionality. The conformance test descriptions are intended to be applied in context with the associated communication standards (e.g., IEC 61850, IEC 60870, etc.)
- **Part 100-1:** Test cases associated with IEC 62351-5 and companion standards. Focus is on secure telecontrol over TCP and serial protocols in the context of IEC 60870-5-7.
- **Part 100-3**: Test cases associated with IEC 62351-3 as general base to be used by other test specifications
- **Part 100-4**: Test cases associated with IEC 62351-4
- **Part 100-6:** Test cases associated with 62351-6

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 – Overview and Status 06/2017

IEC 62351 Part	Release	Activities (by June 2017)	Planned Release (New)
IEC/TS 62351-1: Introduction	2007	May need to be updated eventually	**No revision planned**
IEC/TS 62351-2: Glossary of terms	2008	http://std.iec.ch/terms/terms.nsf/ByPub?OpenView&Count=-1&RestrictToCategory=IEC%2062351-2	Pending – no specific date
IEC/IS 62351-3: Security for profiles including TCP/IP	2014		**IS Ed. 1 in 2014, updating the IS – AMD 11/2016, AMD-CDV 07/2017, AMD-FDIS12/2017, AMD-IS 04/2017**
IEC/TS 62351-4: Security for profiles including MMS and Similar Payloads	2007	Work on the A Profile enhancements.	**IS Ed. 1: CDV 6/2017, FDIS 12/2017, IS 6/2018**
IEC/TS 62351-5: Security for IEC 60870-5 and derivatives	2013	Released April 2013	**RR for IS process to be issued 10/2016;**
IEC/TS 62351-6: Security for IEC 61850 profiles	2007	Based on security requirements in IEC 61850-90-5	**CDV ?/2017** in parallel with Part 4
IEC/TS 62351-7: Network and System Management (NSM) data object models	2010	CDV issued 12/2015,	**FDIS submitted 1/2017**, IS 2017
IEC/TS 62351-8: Role-Based Access Control	2011	Discussions on developing categories of roles	**Issue RR for IS** after TR 90-1and 61850-90-19 issued
IEC/IS 62351-9: Key Management	2017	CDV in early 2016	**FDIS in late 2016**, IS in late 2017
IEC/TR 62351-10: Security Architecture	2012	TR published Oct 2012	**TR 10/2012**
IEC/IS 62351-11: Security for XML Files	2016	Going out as FDIS	**IS 9/2016**
IEC/TR 62351-12: Resilience and Security Rec. for Power Systems with DER	2016	Sent out as DTR 1/2016	**TR 4/2016**
IEC/TR 62351-13: Guidelines on Security Considerations in Standards and Specifications	2016	Sent out as DTR 2/2016	**TR 8/2016**
IEC/TR 62351-90-1: Guidelines for Using Part 8 Roles	DC in 2016	Actively being developed	**WD 3/2016, DC 8/2016, DTR 06/2017**
IEC/TS 62351-100-1: Conformance test for IEC 62351-5 and companion standards	NWIP 2016	Conformance testing of IEC 62351-3, 62351-5, and 60870-5-7 NWIP submitted 5/2016	**CD by 3/2017, Comments received =6/2017, CDV q1/2018, TS by ?/2018**
IEC/TS 62351-100-2: Conformance test for IEC 62351-4/5 and companion standards	NWIP 2017		
IEC/TS 62351-100-3: Conformance test for IEC 62351-3	NWIP 2017		**NWIP for 100-3 6/2017**
IEC 62351-14 Cyber Security Event Logging	NWIP	Based on existing security logging	**NWIP by 6/2016, CDV11/2017**
IEC/TR 62351-90-2 Deep Packet Inspection	DC	TR to discuss the issues around deep packet inspection	**DC 10/2016,** comments received 01/2017, DTR 08/2017
IEC/TR Part 90-19: Using Role Based Access Control (RBAC) and IEC 61850	WG10	Joint effort with WG10	??
IEC/TR 62351-90-3 Guidelines for Network Management	Hold No PWI	Hold until ready to start document – Wait to submit PWI	**PWI, DC 12/2017**