Cyber Security – Stato dell’arte norma IEC 62351

Federico Bellio - CEO Bjosora Srl

Gian Luigi Pugni - Cyber Security Expert

Webinar: Sicurezza e Flessibilità della rete elettrica Nazionale

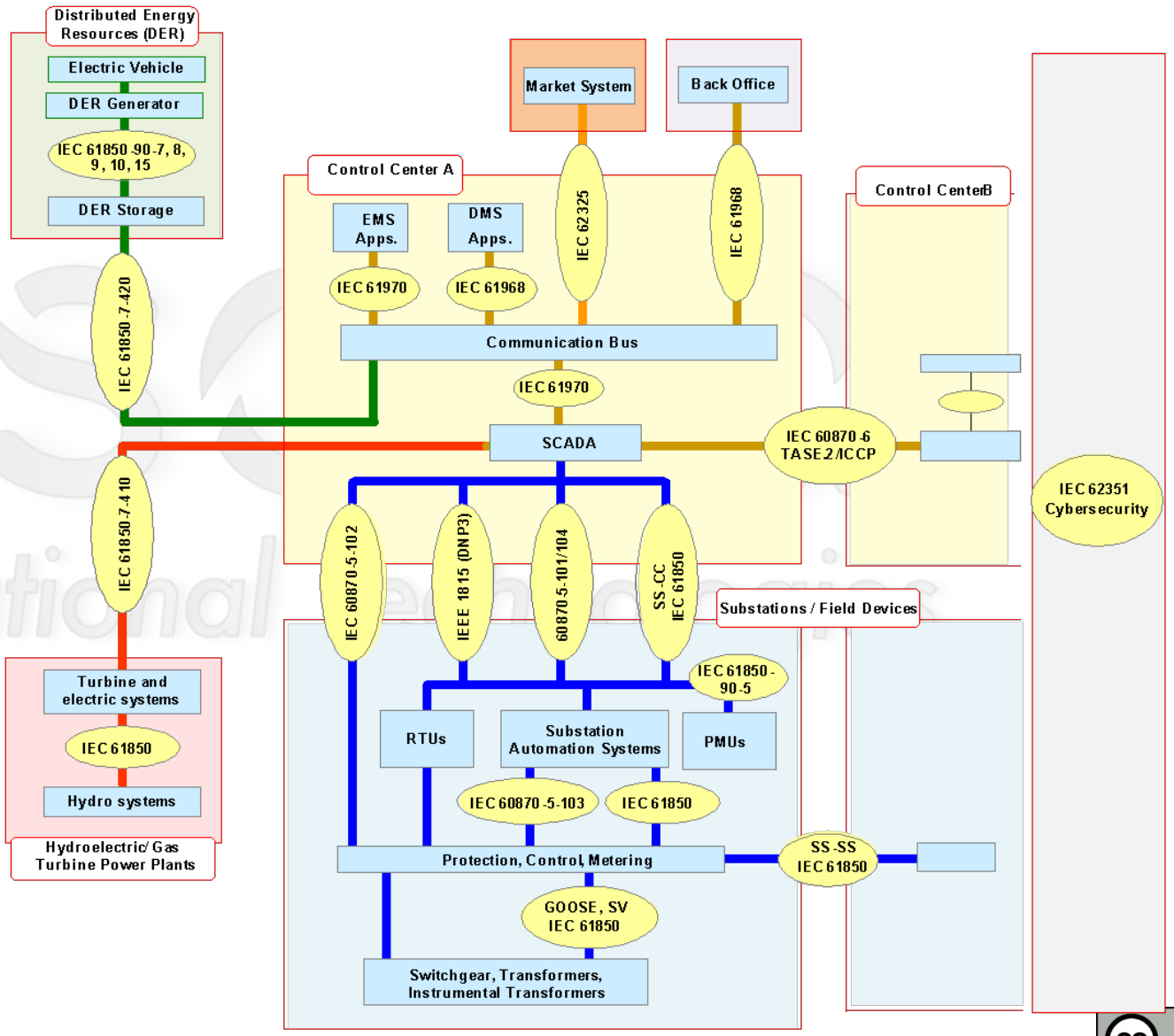
Architettura delle norme IEC TC 57

Relazione tra norma e sistema

International Electrotechnical Commission

Technical Committee 57 - Power systems management and associated information exchange

Working Group 15 - Data and communication security



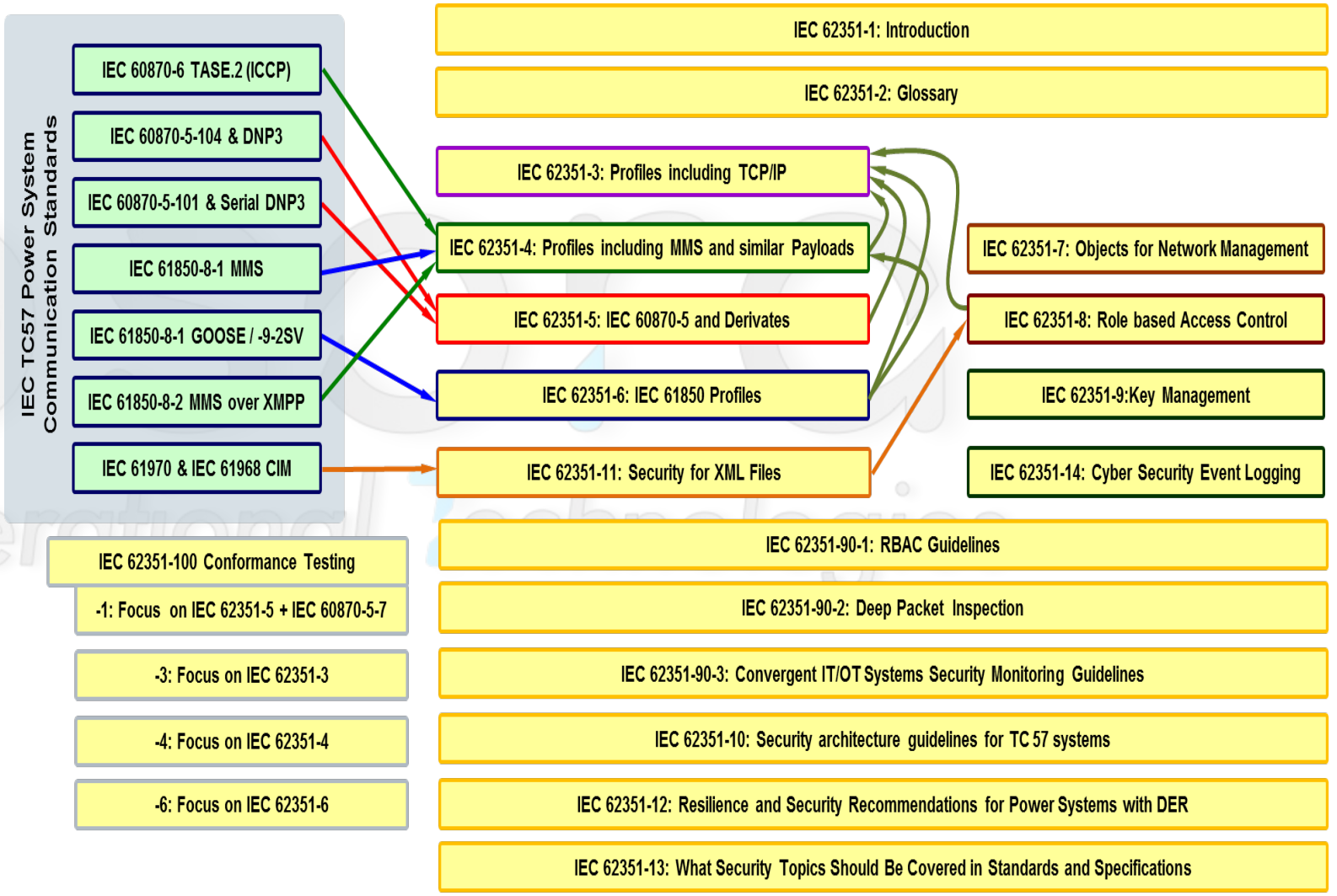
Norma IEC 62351

La scomposizione in parti

International Electrotechnical Commission

Technical Committee 57 - Power systems management and associated information exchange

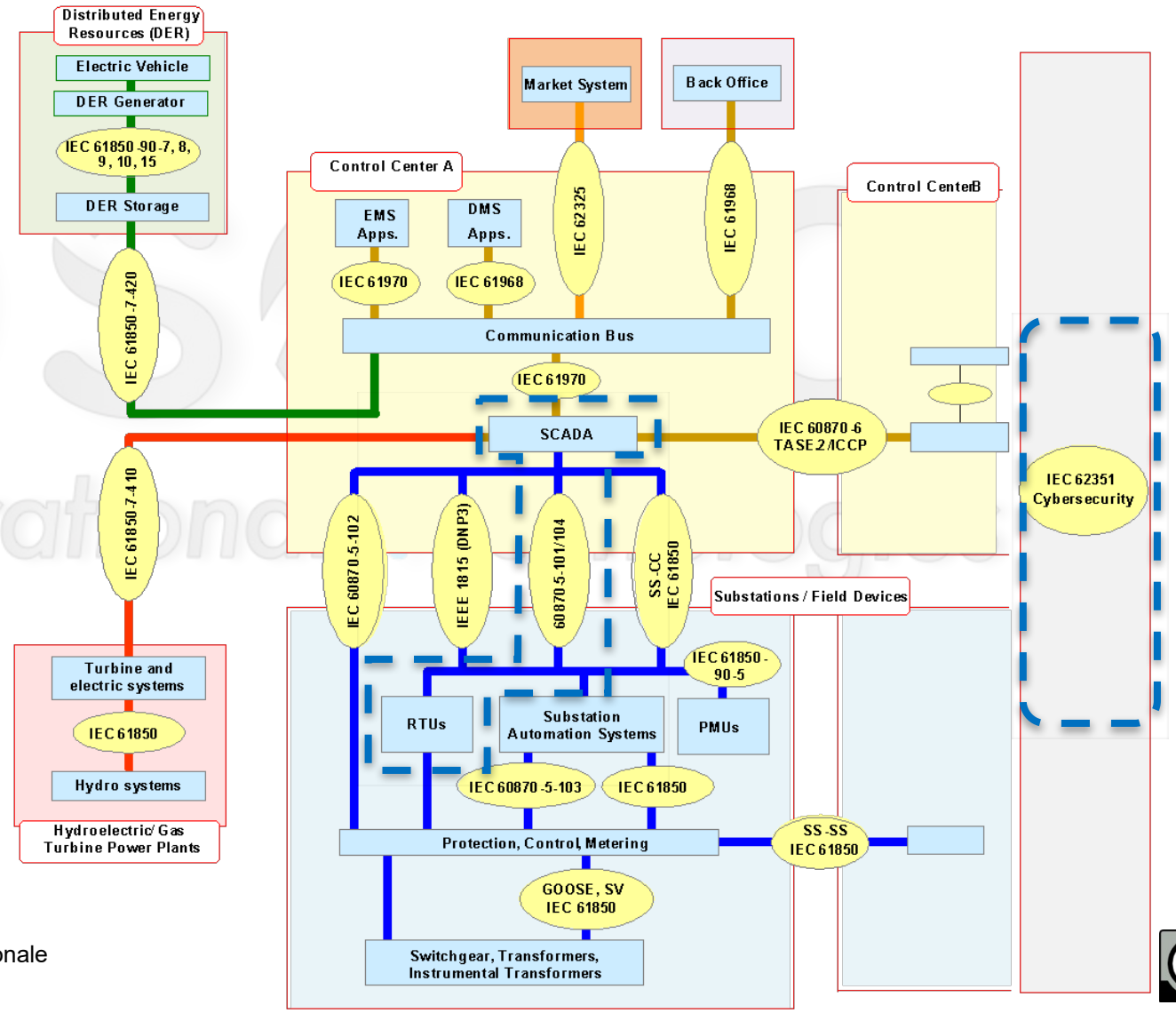
Working Group 15 - Data and communication security



Esempio di sistema di Telecontrollo

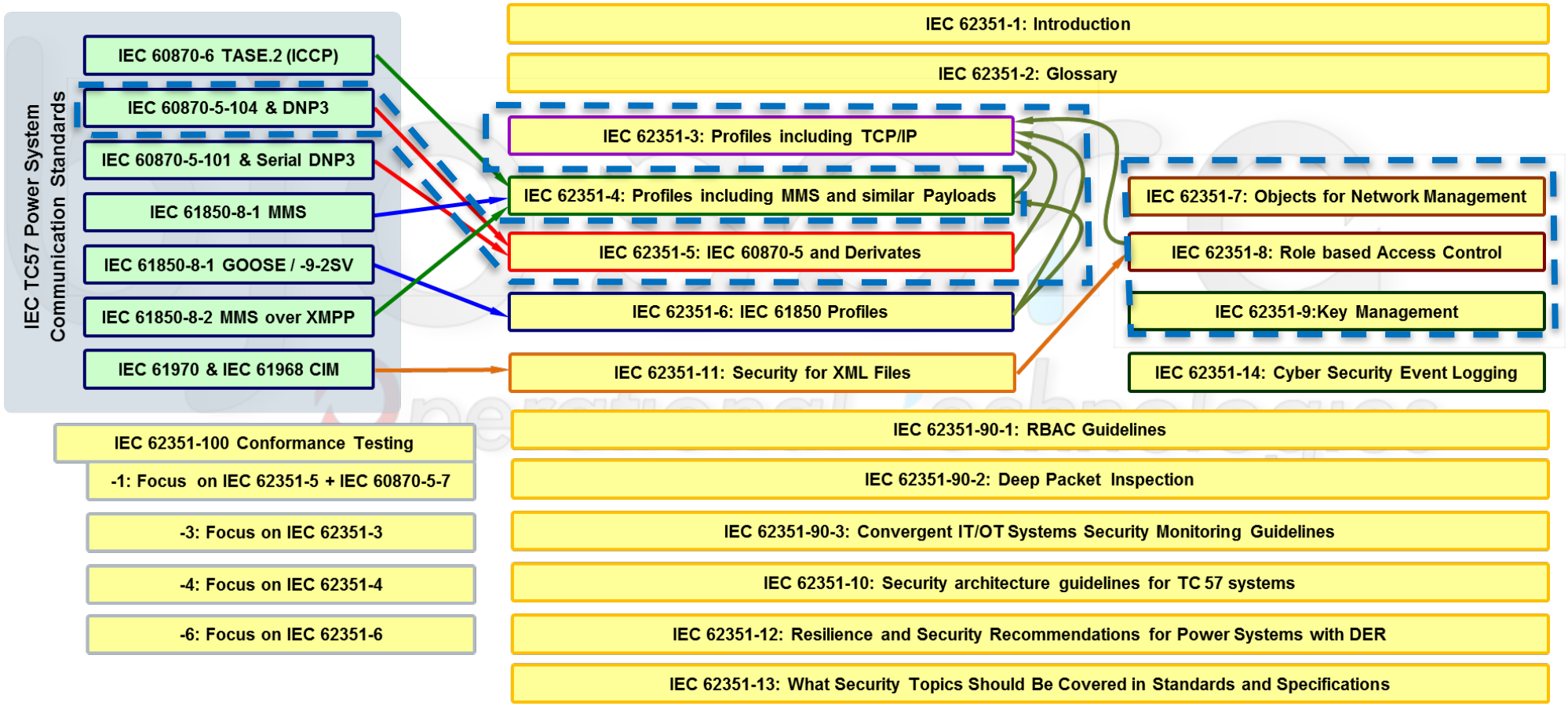
Applicazione IEC 62351 a scambio dati IEC 60870-5-104

- Applicazione della norma 62351
- Allo scambio dati tra SCADA e RTU IEC 60870-5-104



Esempio di sistema di Telecontrollo

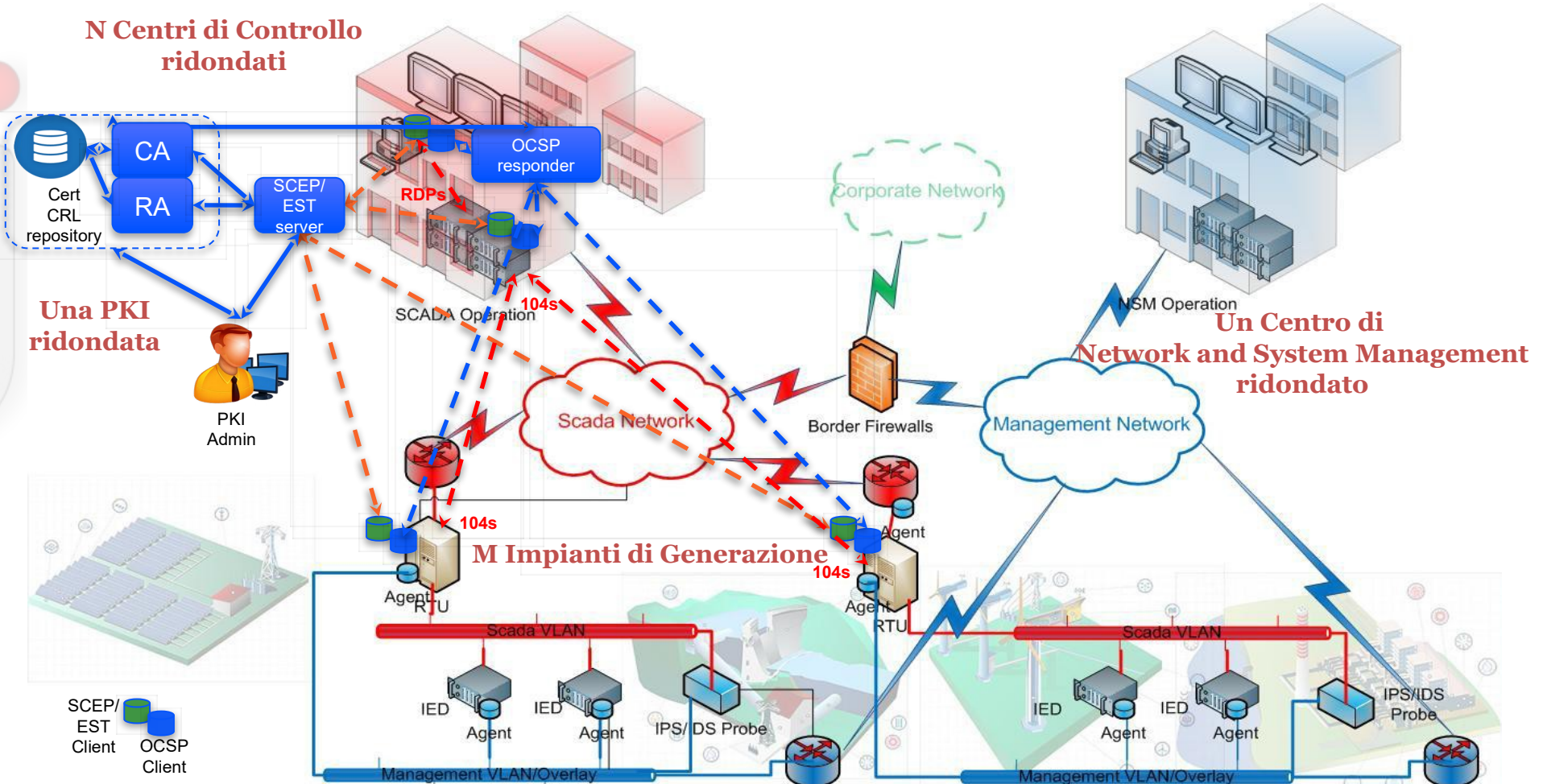
Applicazione IEC 62351 a scambio dati IEC 60870-5-104



Esempio di sistema di Telecontrollo

Applicazione IEC 62351 a scambio dati IEC 60870-5-104

- Sistema Supervisory Control And Data Acquisition (SCADA)
- Network and System Management (NSM)
- Public Key Infrastructure (PKI) Rete di accesso SCADA e NSM logicamente separate

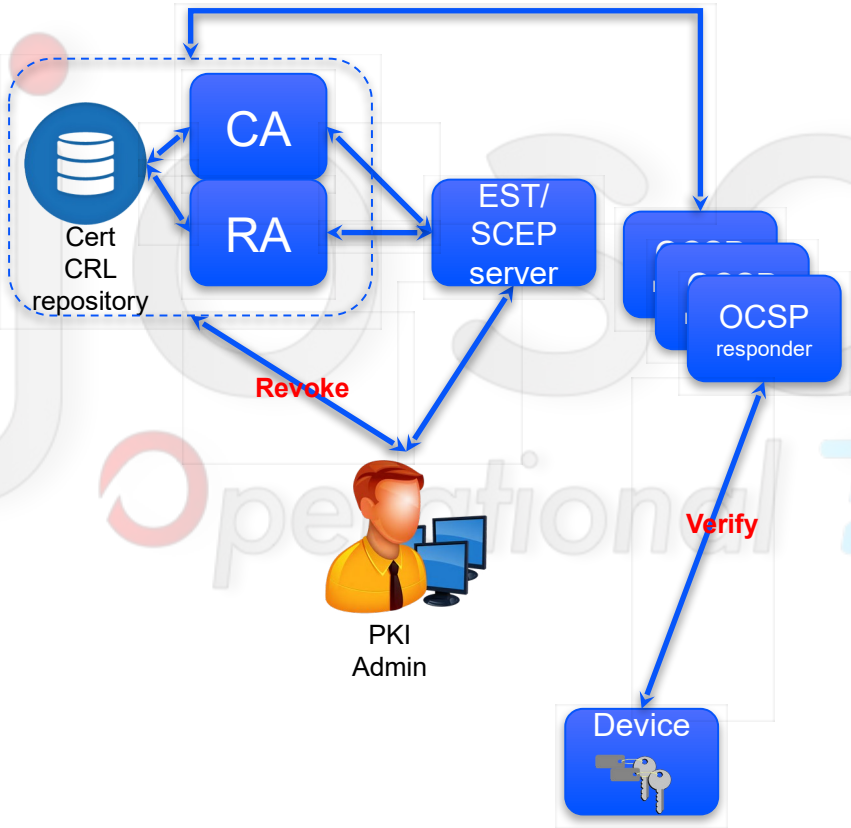


Esempio di sistema di Telecontrollo

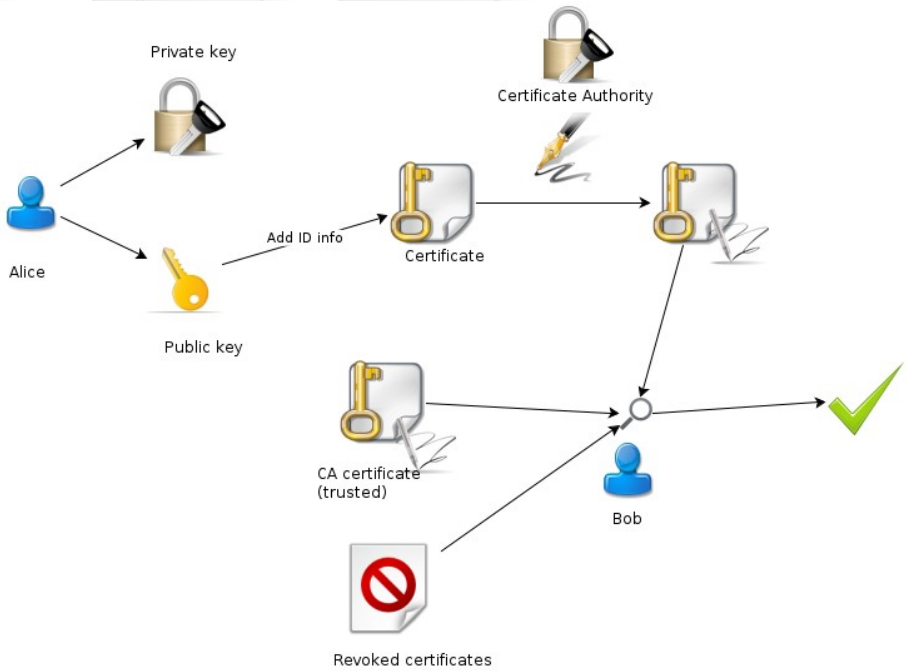
Uso della crittografia

Due operazioni eseguite tramite i servizi della PKI:

- *Revoca (Revoke) di un certificato*
- *Verifica (Verify) di un certificato*



Revoca – Verifica Validità del Certificato



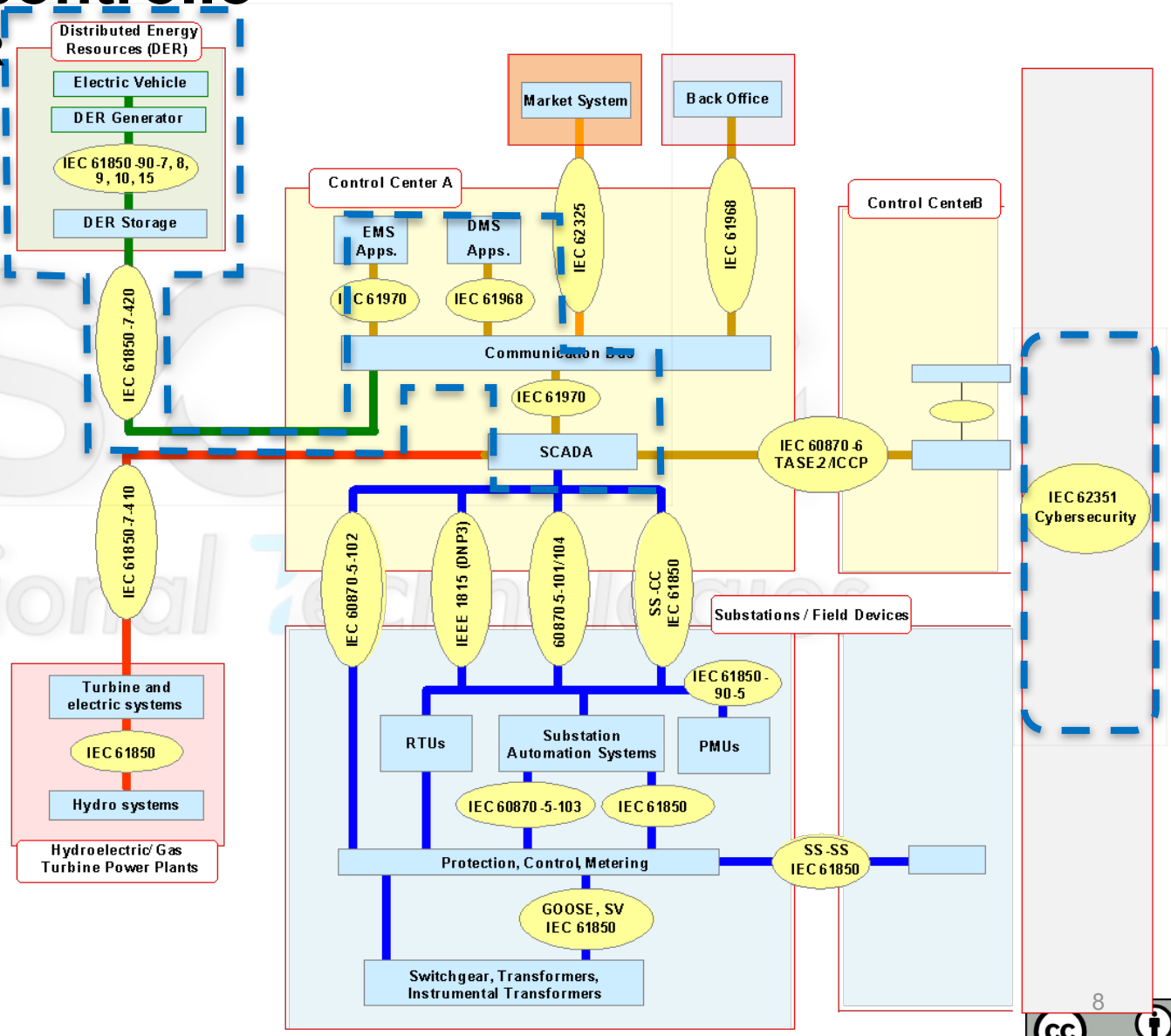
Alice e Bob possono essere rispettivamente il server SCADA e una RTU
La verifica è mutua e i ruoli si scambiano

Esempio di sistema di Telecontrollo

IEC 62351 a scambio dati IEC 61850 nei DER

La norma CEI 0-16 *"Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT ed MT delle imprese distributrici di energia elettrica"* - allegato T *"Scambio informativo basato su standard CEI EN 61850"*.

Il concetto di "*resilienza*" di IEC 62351-12 nelle Smart Grid.



Network and System Monitoring Cyber Security

The **Network and System Monitoring (NSM) is strongly needed** because **availability of systems and data** is one of the most sensitive topic for **resiliency of critical infrastructure considering that IT and OT systems need nowadays to strongly interact and therefore we need to:**.

- **Detect attack attempts** in order to **promptly activate the security measures:** in the case of a fully deployed attack you'll have less success chances in response.
- **Rate the importance of attacks**, to determine the nature and severity of the attack potential effective damage and correctly graduate the reactions.
- **Communication and notification (according to CERT procedures)**, in order to make the systems and network managers to **be aware of the attack in a timely manner**.
- **Constrantly improve Cyber Security controls** using the additional **Intelligence Knowledge** that constant monitoring will provide.
- Support and foster Operational Systems **Health and performance monitoring/diagnostics**
- **Collect Asset** status information to allow prevention toward possible threat exploits

NIST Framework perspective

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Cyber Security Lifecycle

- *Identification of risks and vulnerabilities*
- *Protection from attacks*
- ***Detection of an attack***
- ***Respond to a successful attack***
- *Recover from the attack*

Network and System Monitoring

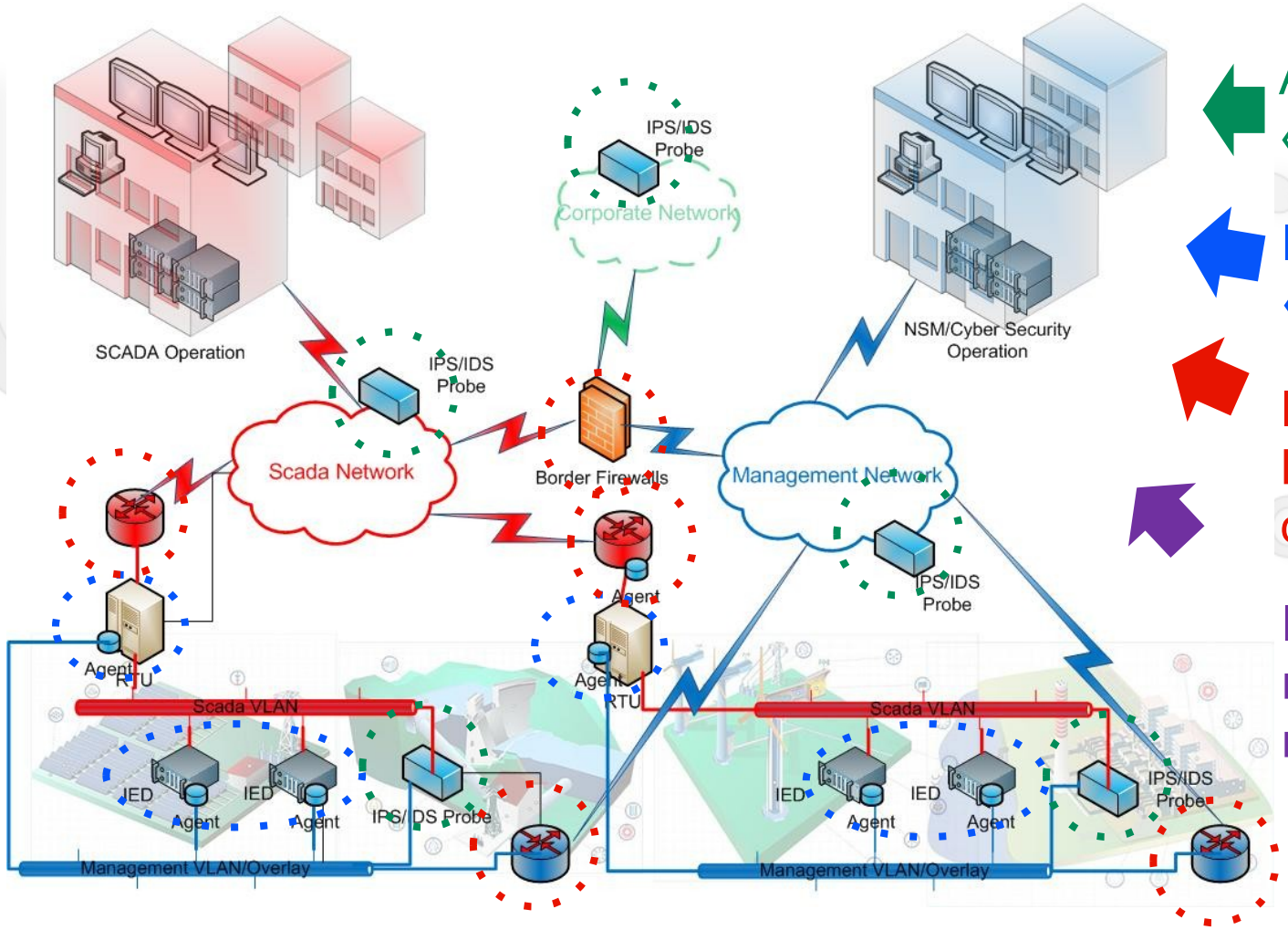
Options and strategy

Network and System Monitoring basically is the **job of collecting information and events**, analysing them on the flight through **“intelligent correlation”** providing **“well filtered”** significant events and alarms: not that easy job and basically these are our tools:

- **IEC 62351-7: Agents inside ICS and Networks devices** can provide information on system health and possible attacks. These agents can either be queried or send out events (“traps”), but **need to be installed inside the devices**. A standard example are **SNMP MIBs based agents**
- **IEC 62351-14 (under development):** Log collection: any network device can provide his own view about what’s going on through **syslog reporting.**
- **“Traditional IDS/IPS**” which can detect possible malicious events through **“signature checking**”, yet are not really focused on application payload analysis
- **Advanced Deep Packet Inspection Probes** perform **application payload analysis** to detect anomalous command and measures semantics, **even without signature checking**. The**baseline of “normal application traffic status and map”** is buildup and **automatic detection of anomalous actions is provided**.

Network and System Monitoring

Overall view



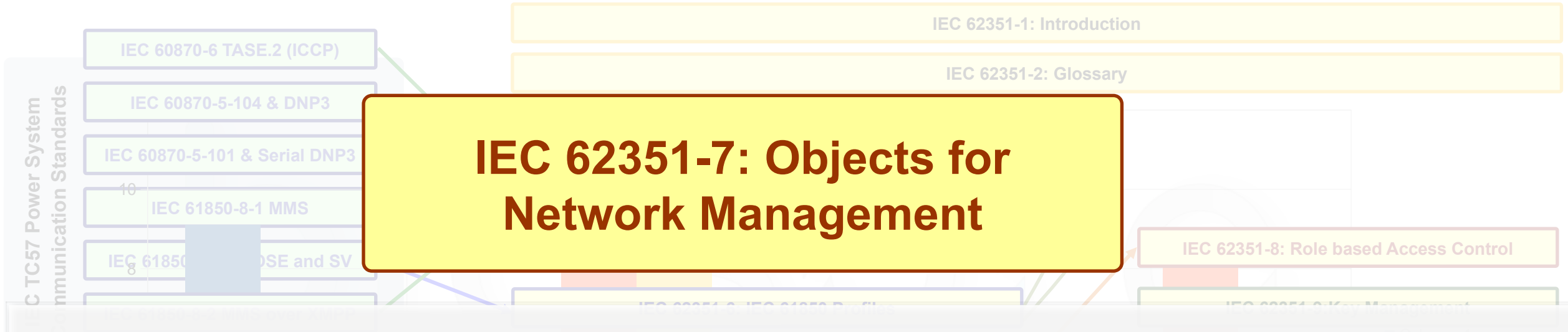
Advanced DPI Probe
«External» observer view

IEC 62351-7
«Insider» IEDs view

IETF MIBs
Network & Infrastructure devices view

IEC 62351-14: Syslog messages; additional log reportings

IEC 62351-7 NSM Objects – Monitoring through MIBs object query



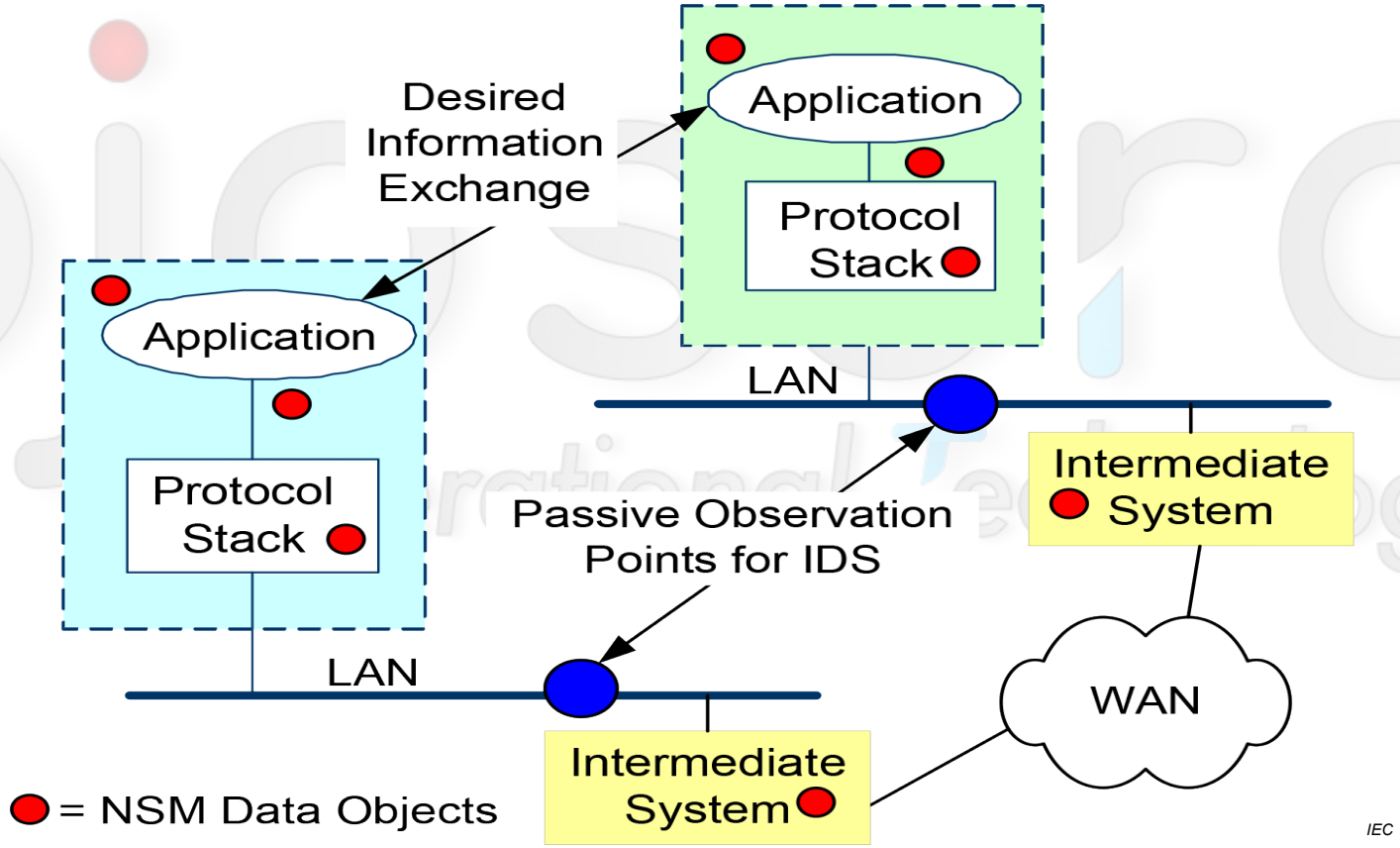
IEC 62351-7: Objects for Network Management

- **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.**

This additional set of information complements the "passive" DPI information collection, refining and enriching collected information.

Network and System Monitoring

Network vs Device perspective



IEC 62351-7:2017

Concepts and Why SNMP embedded support?

The goal is to define **Network and System Management (NSM) data object models that are specific to power system operations**. These NSM data objects will be used to monitor the health of networks and systems, to detect possible security intrusions, and to manage the performance and reliability of the information infrastructure.

These "data object" shall be "Abstract" because it must be possible to transport them with different monitoring protocols.

A first **translation of the Abstract Object into** a real monitoring protocol is provided with IEC 62351-7 edition2. This protocol is **SNMP (Simple Network Management Protocol)** and the Abstract object are translated into **MIB (Management Information Base) objects**

SNMP is a widely used IT standard monitoring protocol.

Simpler correlation of information Objects and Alert is possible with other monitoring information (e.g. from **routers, switches, IDS/IPS, Firewalls**).

About SNMP itself security: IEC 62351-7 mandates SNMP v3 (v1 and v2c are insecure).

Abstract Objects translation into NSM objects

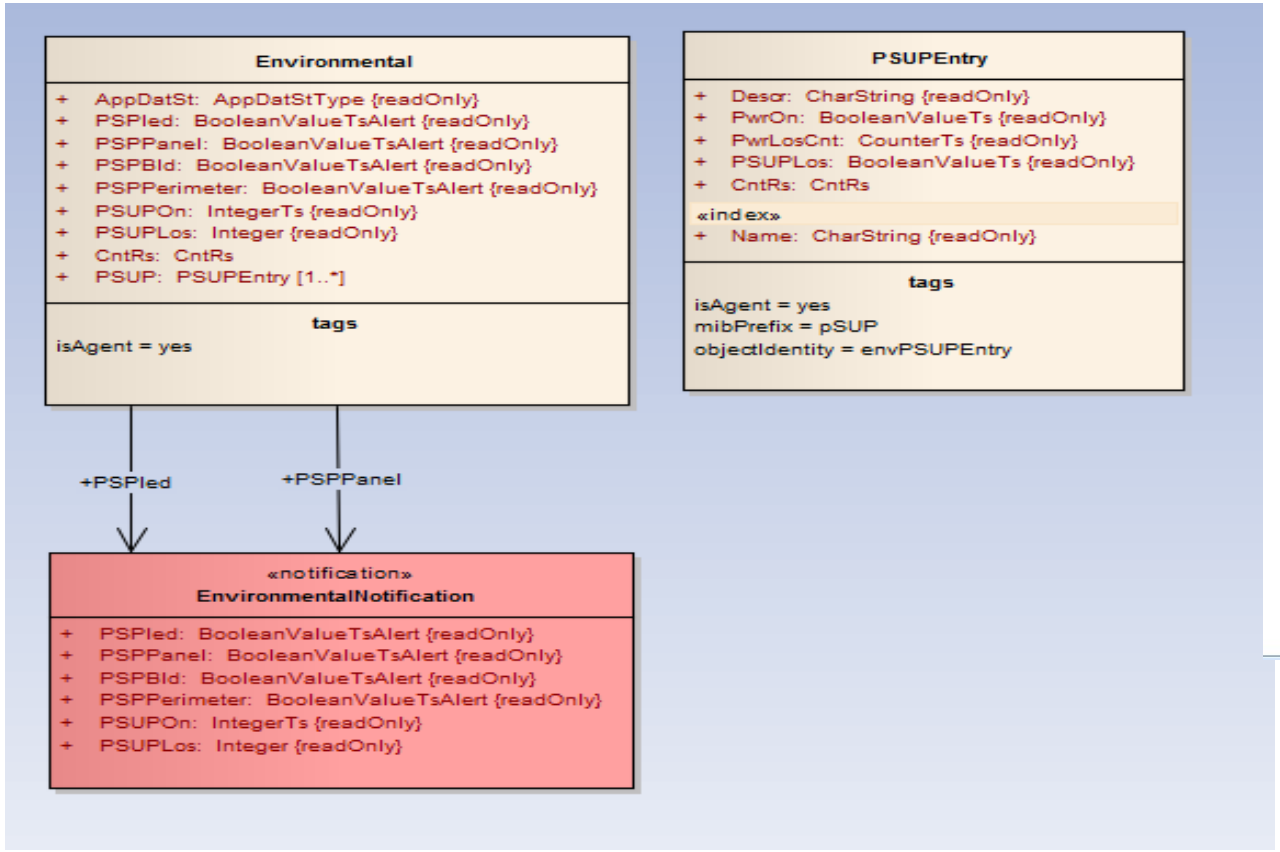
SNMP MIBs and future

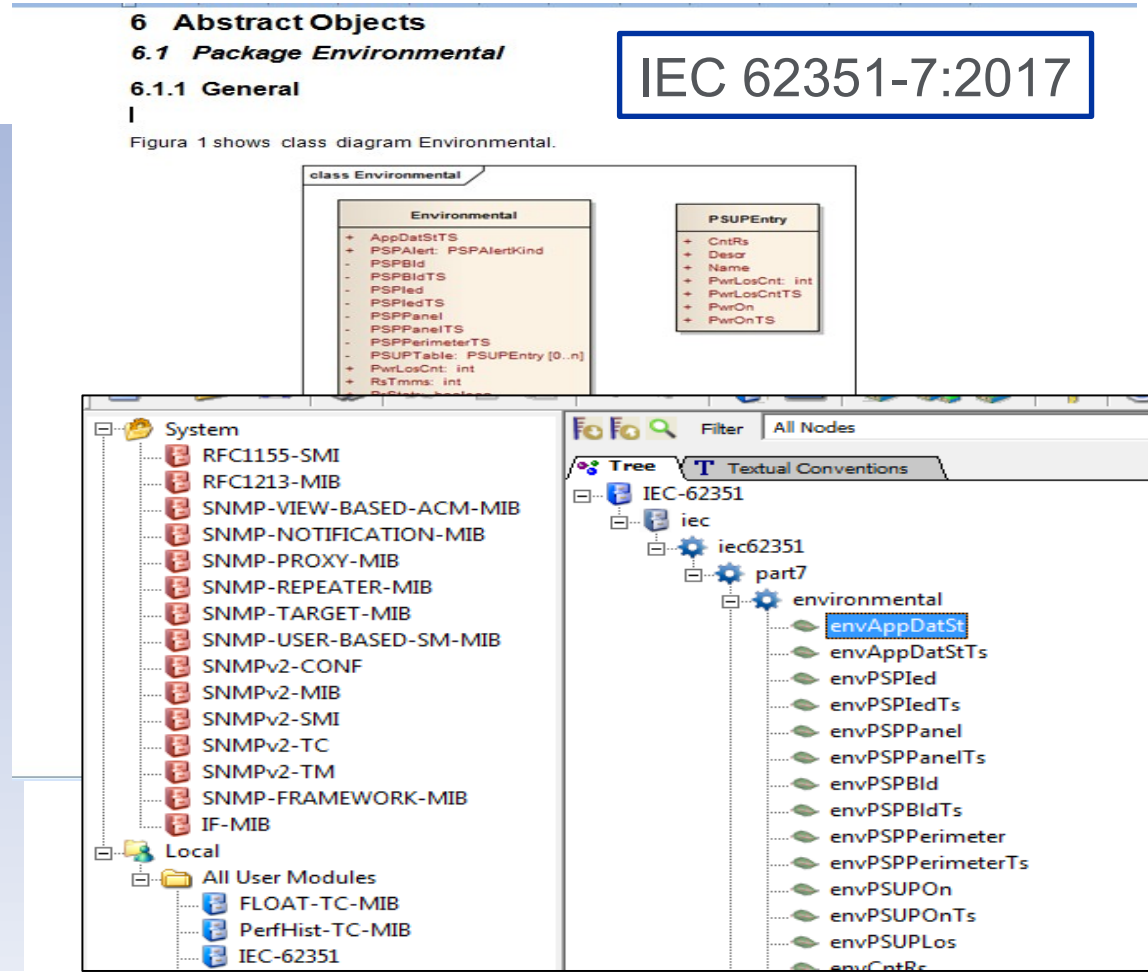
IEC 62351-7 already include the SNMP MIBs mapping. Beside this objective we had anyway the goal to **keep the Abstract Objects modeling indipendent from SNMP MIBs** specific syntax and logic:

- **UML Model a the concept of multiplicity is in use**(… that translates into tables for SNMP)
- **UML Model Abstract Object are expressed as attributes of classes**.
- **Attribute versioning is provided** in order to keep track of model changes
- The Abstract nature of the UML model allow the translation toward different NSM protocols

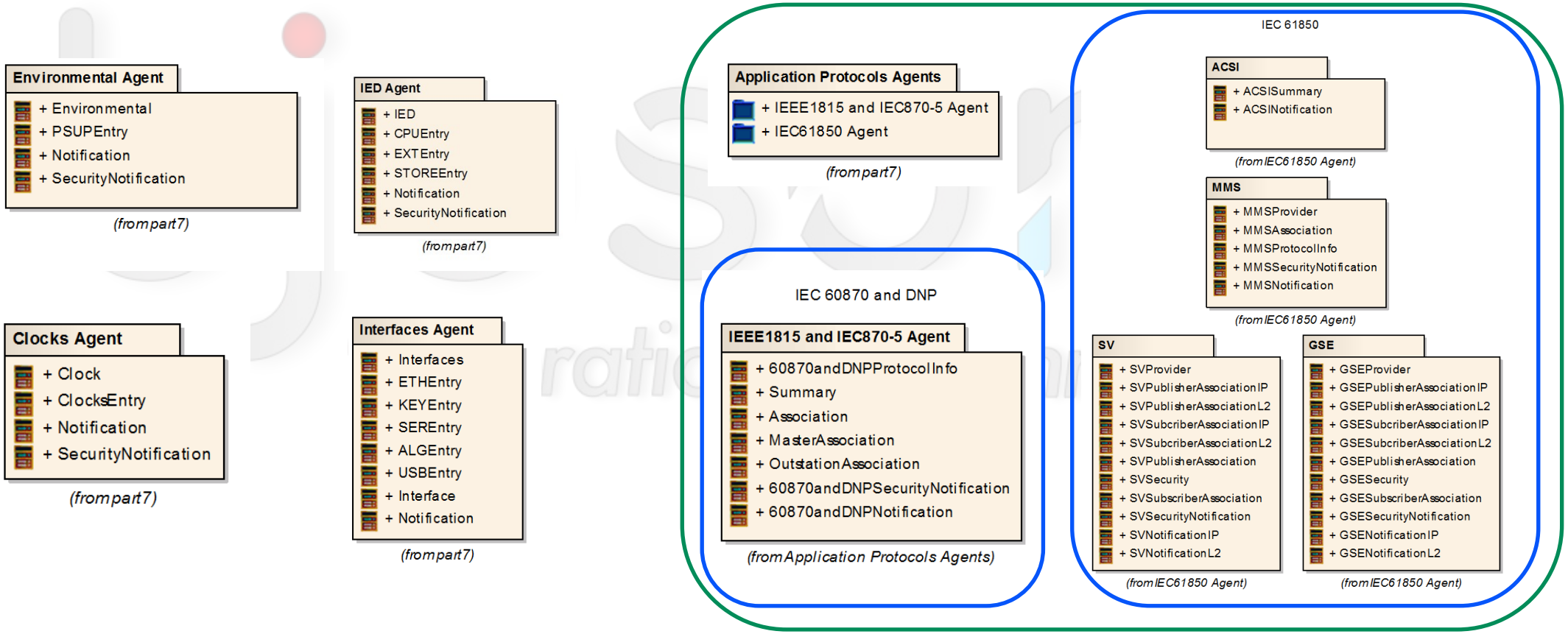
Beside IEC 62351-7 we have now a methodology that allow the maintenance of the model and the flexible Standard document, MIBs update and extension toward other protocols.

IEC 62351-7 - From UML model to Standard and MIBs





The subagents overview



IEC 62351-7 Ed.2 – Upcoming review

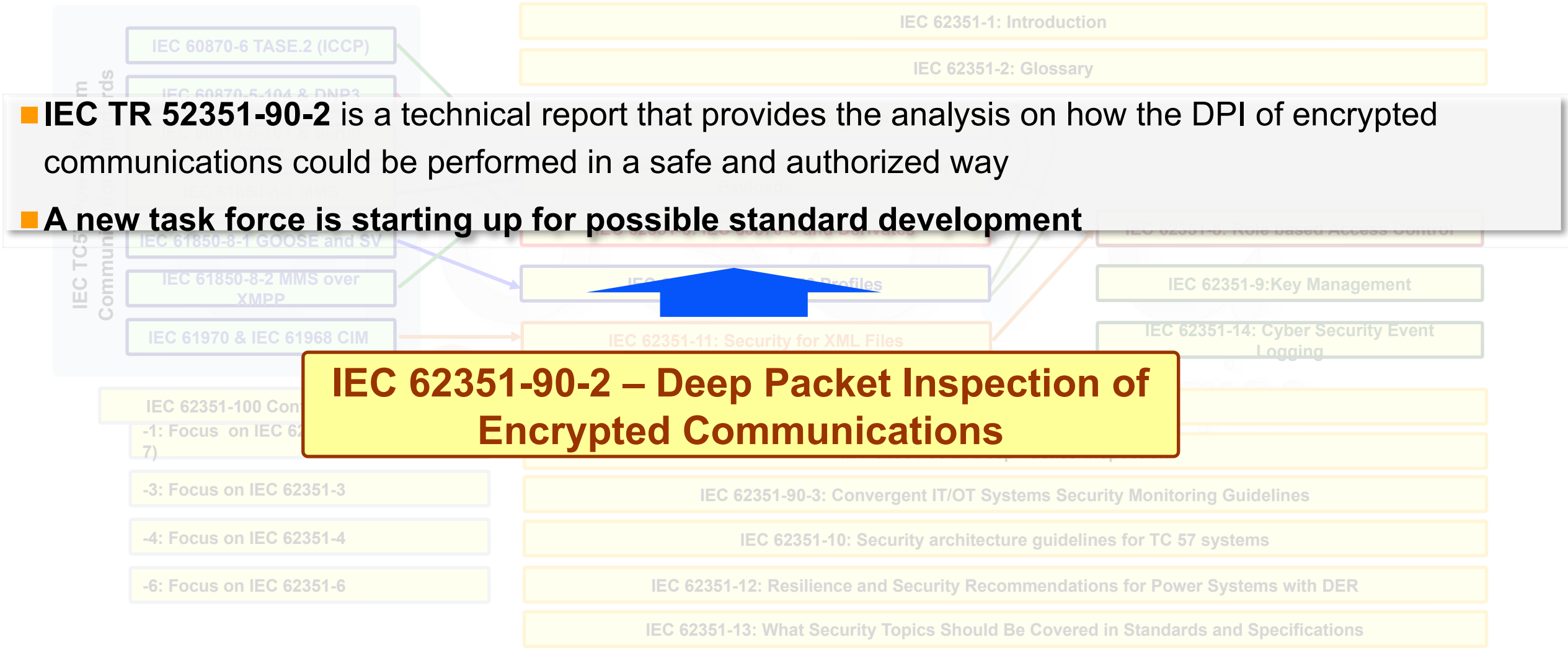
IEC 62351 Ed.1 has been released in 2017 with stability date 2021: It's time to go for the update process:

- **Make selected objects mandatory** (**IEC 62351-3 90-3 will be the starting reference)**:
  - Some companies already include IEC 62351-7 support in their products, some are developing
  - vendors see the fact that all objects are optional as one impediment/excuse to implementation
- **Harmonization with new IEC 62351-x versions (-5 and -4, maybe more)**: since 2017 several additions have been done in the various parts, and we have an **opportunity to expand the objects set to cover the new developments**.
- **Generic observability**: Allow devices to expose information about general communications, implicitly allowing some visibility into non-IEC protocols
- **Extensibility documentation**: Document how to extend the standard for more specific protocols
- **IEC 61850 monitoring objects**: - Evaluate and clarify the possible sinergy with 62351-7 objects

Task force for the new edition is now starting up:
a good time to provide feedback and (possibly) help!

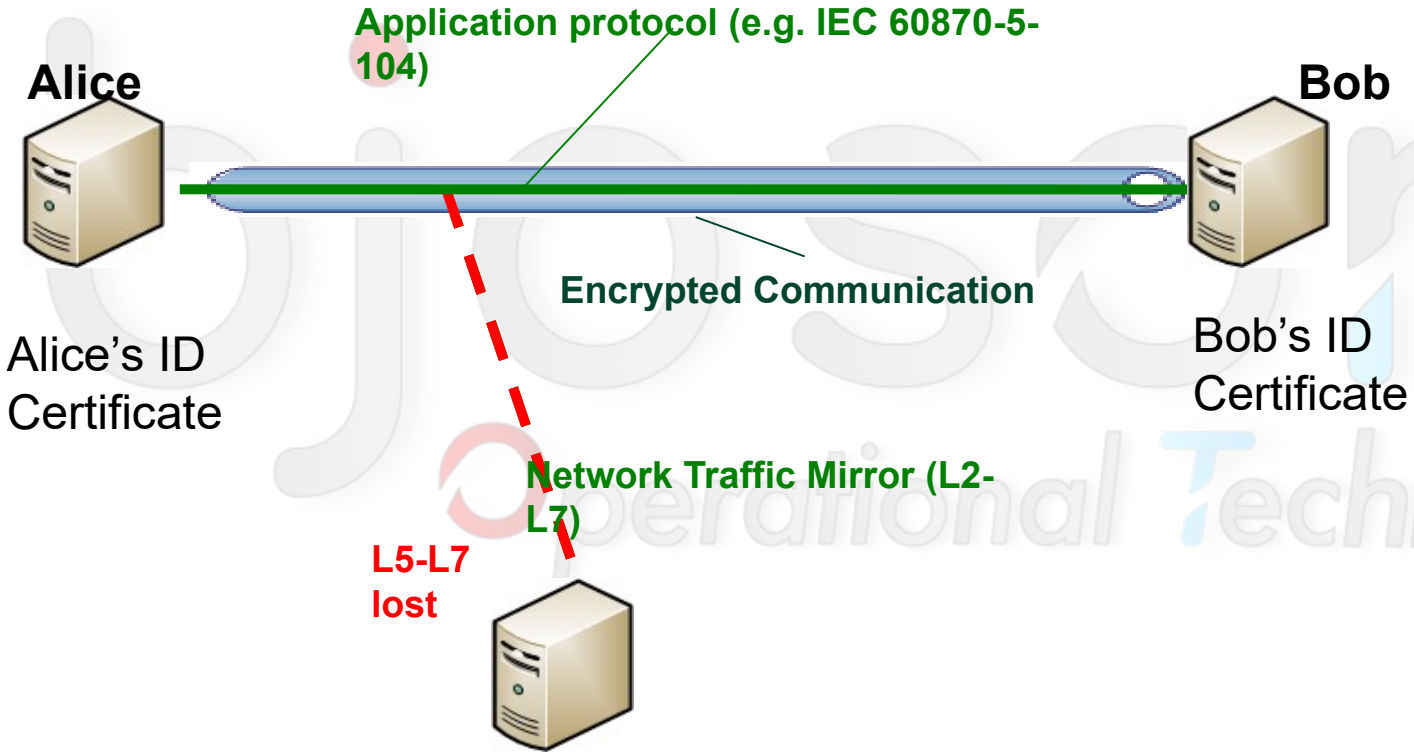
IEC TR 62351-90-2 – DPI of encrypted communications

- **IEC TR 52351-90-2** is a technical report that provides the analysis on how the DPI of encrypted communications could be performed in a safe and authorized way
- **A new task force is starting up for possible standard development**



IEC TR 62351-90-2 example

The issue (encrypted end-to-end protocols)



How to handel this issue:

- Unencrypted TLS?
- Proxy systems?
- Secure Private Key Sharing?
- Secure session Key Sharing?
- data collection from IEDs/SCADA?
- Others?

Network Probe- Advanced Deep Packet Inspection - L7 analysis - Protocol certification inspection

IEC 62351-90-2 Technical Report provides and compares solutions

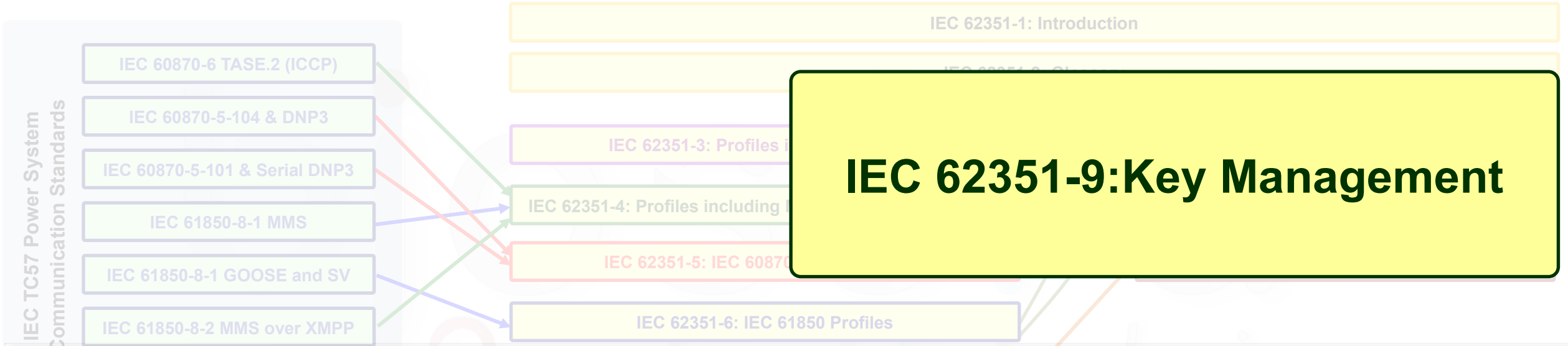
IEC 62351-90-2 Key sharing options

- **IEC TR 62351-90-2 provides** ideas and possible solutions, among these some **secure key sharing options** are described but
- • **DPI Monitoring solutions** can implement decryption capabilities and **leverage the options outlined in that TR** but:
- How can keys be shared?
  - Manually (not scalable)
  - Automatically from the KMS, or from the endpoints

A standard and secure solution for authenticated and protected key sharing is actually required and shall be selected among the existing and also proposed by manufacturers

A **New Work Item Proposal for a new IEC 62351 part** is currently in preparation:
again any suggestion or help is very welcome

IEC 62351-9 - 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.

IEC 62351-9 Key Management

All IEC 62351 series standard expecially part 3,4,5,6 and 11 depend on encryption for the integrity and confidentiality protection of messages ad data.

The possible **techniques for Machine to Machine authentication** rely basically on **secret keys** that allow each party to demonstrate his own identity through a mathematical process.

Every possible solutions is actually based on the use of cryptography, a science "antique" that has found a huge application in the modern ICT systems, IEC 62351-9 defines standard specifications for:

- **Public Key Infrastructure (PKI)** that release X.509 Certificates managed by **Certificate Autorities (Cas)**
  - **Certificates are already widely used** all over the web to protect web site server communication. (**Many public CAs are operated on the public Internet**)
  - **OT/IoT environment have particular requirements**
- **group based communication security (GDOI)** in the context of multicast communication scenarios (e.g. IEC 61850 GOOSE)

IEC 62351-9

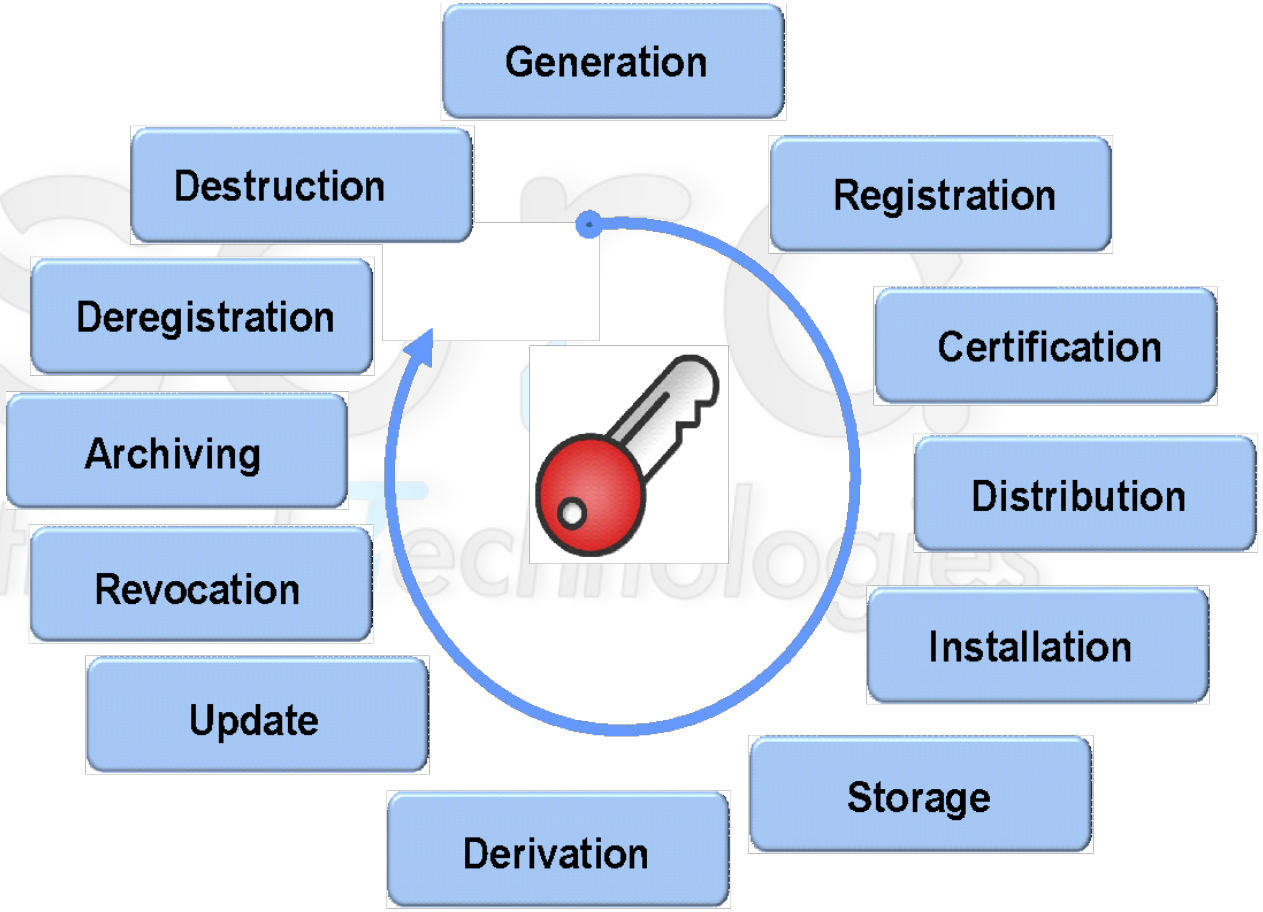
Key Management Systems

The **lifecycle of any Key** can be seen from the perspective of **several phase**.

Each of this phases require a **specific process and standard approach** in order to provide interoperability.

Also each phase of the lifecycle imply cautions because keys must of course be always secure.

Public Key Infrastructures are a widely adopted mechanism for managing key lifecycle…



OT and IoT systems Key Management PKI requirements

OT and IoT environments are not confortable with traditional monolitic PKI systems based on centralized architectures.

From a **technical perspective PKI system shall be able to:** :

- **run on Public SaaS, IaaS cloud infrastructure (private and public)** but also on **segregated networks over on premises environments**.
- **create and manage in a flexible way Subordinate CA** in order to allow the support of **multiple environments**
- **Adopt of the art enrollment procedure using automated protocols and tools.**
- **Bring easy (and sustainable) scalability** in terms of certificate numbers and **service deployment**
- Support both **Public Key Certificates and Attribute Certificates** in order to completely **enable Role Based Access Control** profiles
- Full state of the art PKI standard support **compliant to IEC 62351-9 and IEC 62351-8**

Furthermore key management it's not only a technical matter. CA imply:

- **implementation and management of all the processes related to each lifecycle phase.**
- **The definition and the management of the CA trusts and relationships**

Thank You