COLLEGIO DEGLI INGEGNERI DELLA PROVINCIA DI VENEZIA

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI VENEZIA

CYBERSECURITY NELL'AMBITO DELLE INFRASTRUTTURE CRITICHE

06/04/2016 Venezia Mestre

ABB

Power and productivity for a better world™

enel

Cyber Security nelle infrastrutture critiche

Indice

1. Prima parte: definizioni e concetti di Cyber Security e Infrastruttura Critica; requisiti di Cyber Security

2. Seconda parte: l'approccio IEC alla Cyber Security, la norma IEC 62351 e alcuni suoi esempi d'applicazione

Cyber Security nelle infrastrutture critiche

Indice prima parte:

- Cos'è un problema di Cyber Security: alcuni esempi
- Cos'è una Infrastruttura Critica: alcune definizioni
- Infrastruttura Critica energetica e Cyber Security
- Processo e ciclo di sicurezza
- Requisiti di sicurezza
- Le norme sulla sicurezza in ambito industriale

Cos’è un problema di cyber security

Alcuni esempi: Black Energy

La ricostruzione dell'incidente in Ucraina di fine 2015

(su gentile concessione di Nozomi Networks)

Cos'è un problema di cyber security

Alcuni esempi: cosa potrebbe succedere se …

- Venissero divulgate le informazioni sensibili di un impianto industriale?
- Un interruttore non si dovesse aprire quando richiesto?
- Un interruttore venisse aperto quando non deve?
- Una protezione non sganciasse a seguito del comando?
- Un controllore o un'apparecchiatura non fosse disponibile quando serve?
- Un controllore o un'apparecchiatura non eseguisse le azioni richieste?
- Un trasformatore venisse sovraccaricato a causa di una falsa lettura della sua temperatura?
- Qualcuno di non autorizzato potesse avere accesso alla rete di supervisione/controllo?
- Qualcuno potesse comandare il sistema di trasmissione/distribuzione energetica a suo piacimento?
- Improvvisamente venissero a mancare la corrente elettrica o il riscaldamento?
- … e la reputazione???

Cos'è una infrastruttura critica

Una definizione dalla Direttiva 2008/114/CE

Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, *relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.*

Infrastruttura critica : *un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni.*

European Union

Cos'è una infrastruttura critica

Interdipendenza fra infrastrutture critiche (dal libro bianco ISCOM Istituto superiore delle Comunicazioni e delle Tecnologie dell'Informazione)

"*Una Infrastruttura Critica Nazionale è definita come una qualsiasi infrastruttura pubblica o privata la cui operatività sia essenziale per la sicurezza ed il funzionamento del Paese … come i sistemi sanitario, economico, energetico, dei trasporti e delle comunicazioni, per la pubblica sicurezza, la difesa e in generale la pubblica amministrazione. I pilastri più importanti sono Energia e Telecomunicazioni (e relative IT) …* ***Per definizione, l'Energia è l'elemento senza il quale nessun lavoro può essere svolto. Energia e Telecomunicazioni sono mutuamente interdipendenti****: senza una adeguata e stabile fonte di alimentazione elettrica nessun apparato ICT può funzionare e viceversa una rete di produzione, trasmissione e distribuzione di energia può funzionare solo se i sistemi di comunicazione sono in grado di interconnettere le varie parti.*"

Infrastruttura critica energetica e cyber security

Perché un problema di cyber security diventa un problema dell'infrastruttura critica

Un problema sul sistema di controllo (sistema ICT) di un sistema energetico diventa un problema per il sistema energetico stesso, perché la perdita di controllo può portare a gravi disservizi nella catena di produzione, trasporto e distribuzione della fonte energetica.

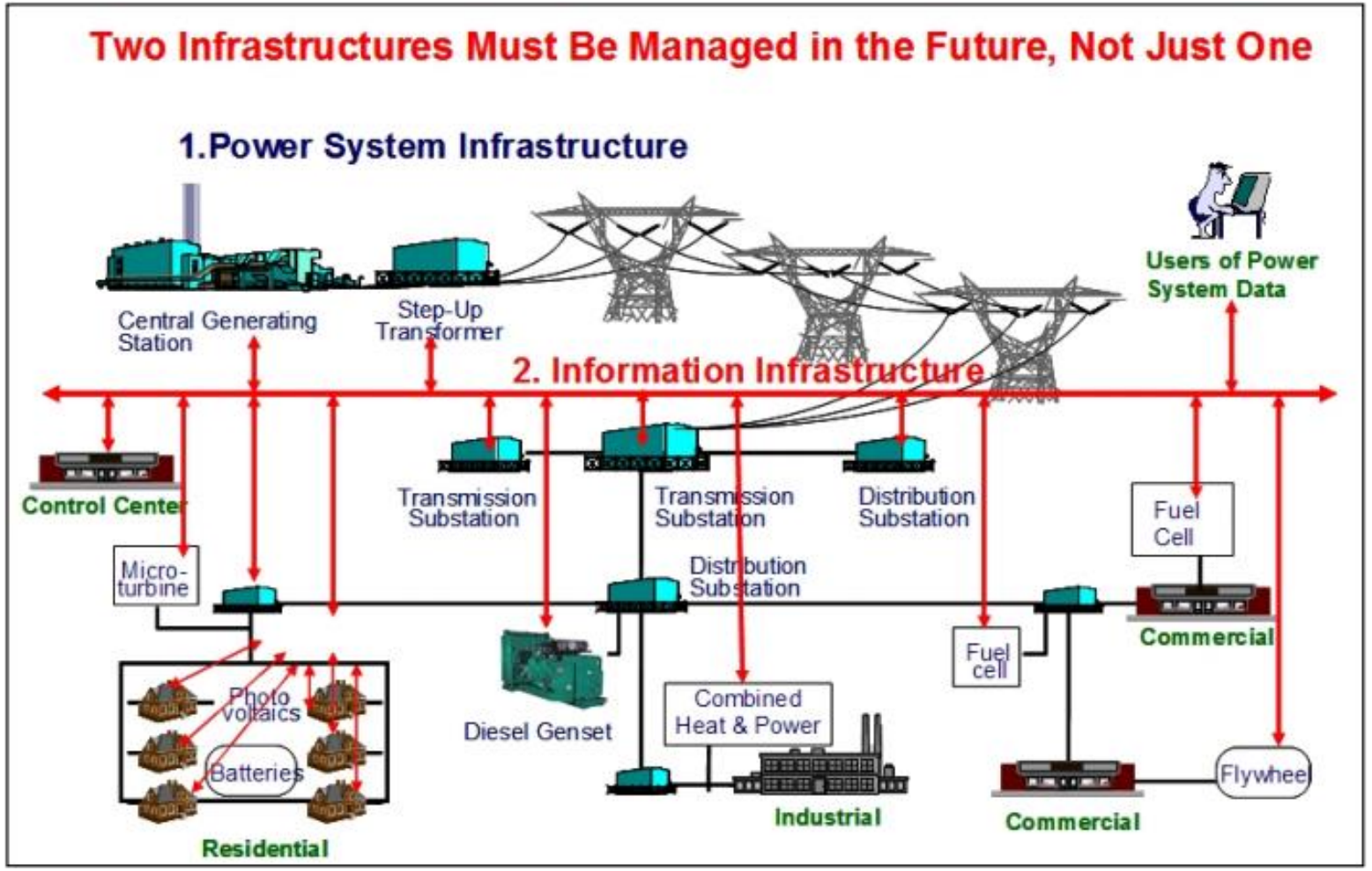
Un sistema energetico è affidabile (disponibile, resiliente) se lo è il suo sistema di controllo.

Ogni minaccia che derivi da un "attacco cibernetico" (cyber attack) al sistema di controllo diventa una minaccia per l'infrastruttura energetica stessa.

Infrastruttura critica energetica e cyber security

Perché un problema di cyber security diventa un problema dell'infrastruttura critica

Il concetto di interdipendenza com'è stato rappresentato in uno dei primi lavori del Working Group 15 del Technical Committee 57 del IEC



Infrastruttura critica energetica e cyber security

Storia dell'evoluzione dei sistemi di controllo e automazione industriale (ICS) – perché cyber security

Caratteristiche dei sistemi SCADA/DCS, di automazione, protezione e controllo attuali:

- Utilizzo di componenti IT standard (es. MS Windows, Internet Explorer)
- Utilizzo di protocolli di comunicazione basati su IP ("Internet technology")
- Connessione a reti esterne network
- Utilizzo di dispositivi portatili e memorie esterne

I sistemi di controllo moderni sono sistemi IT specializzati, attaccabili da più punti

Il processo di sicurezza come edificio

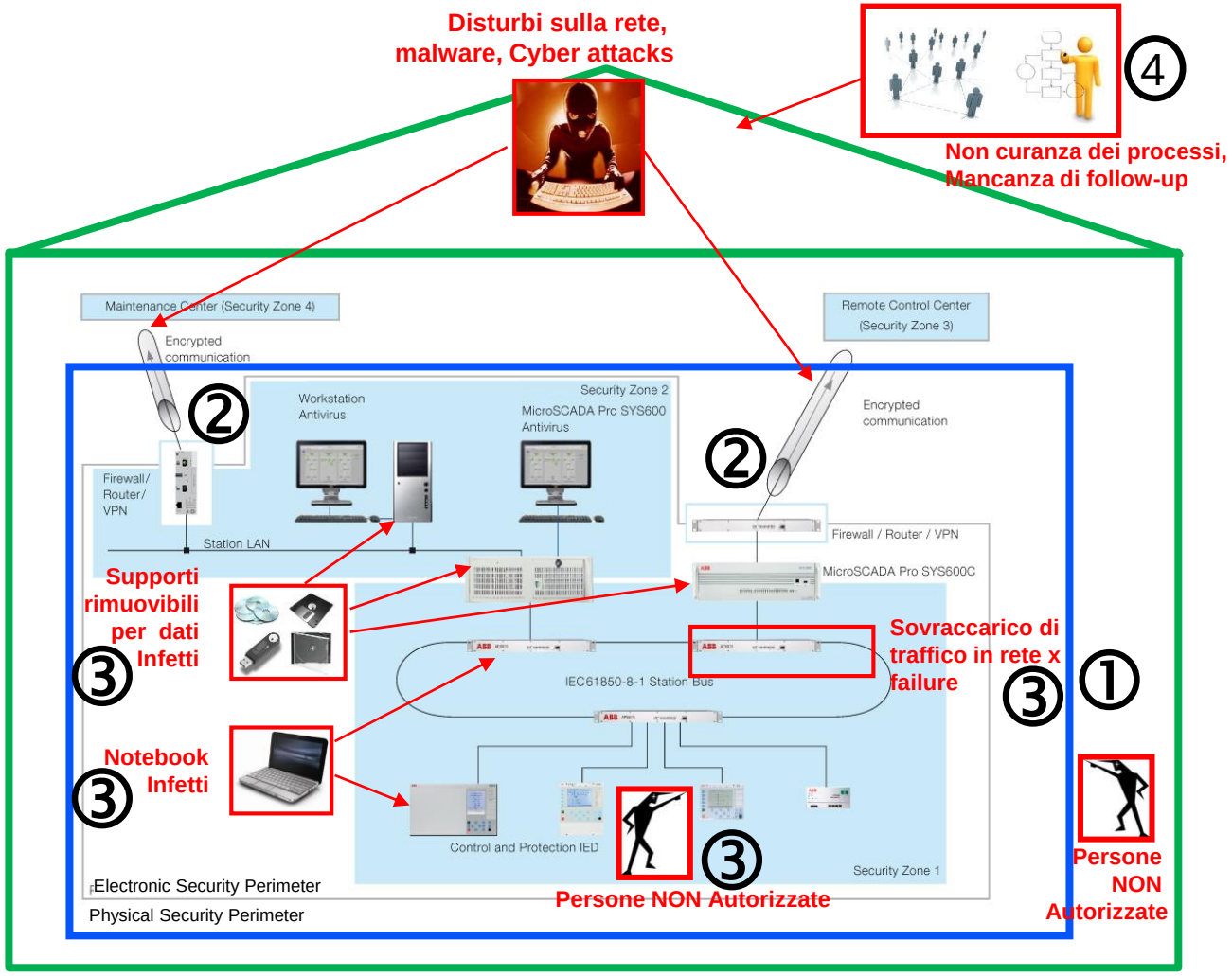
Misure di sicurezza

① Protezione fisica del perimetro

② Protezione elettronica del perimetro

③ Protezione apparati

④ Processi aziendali



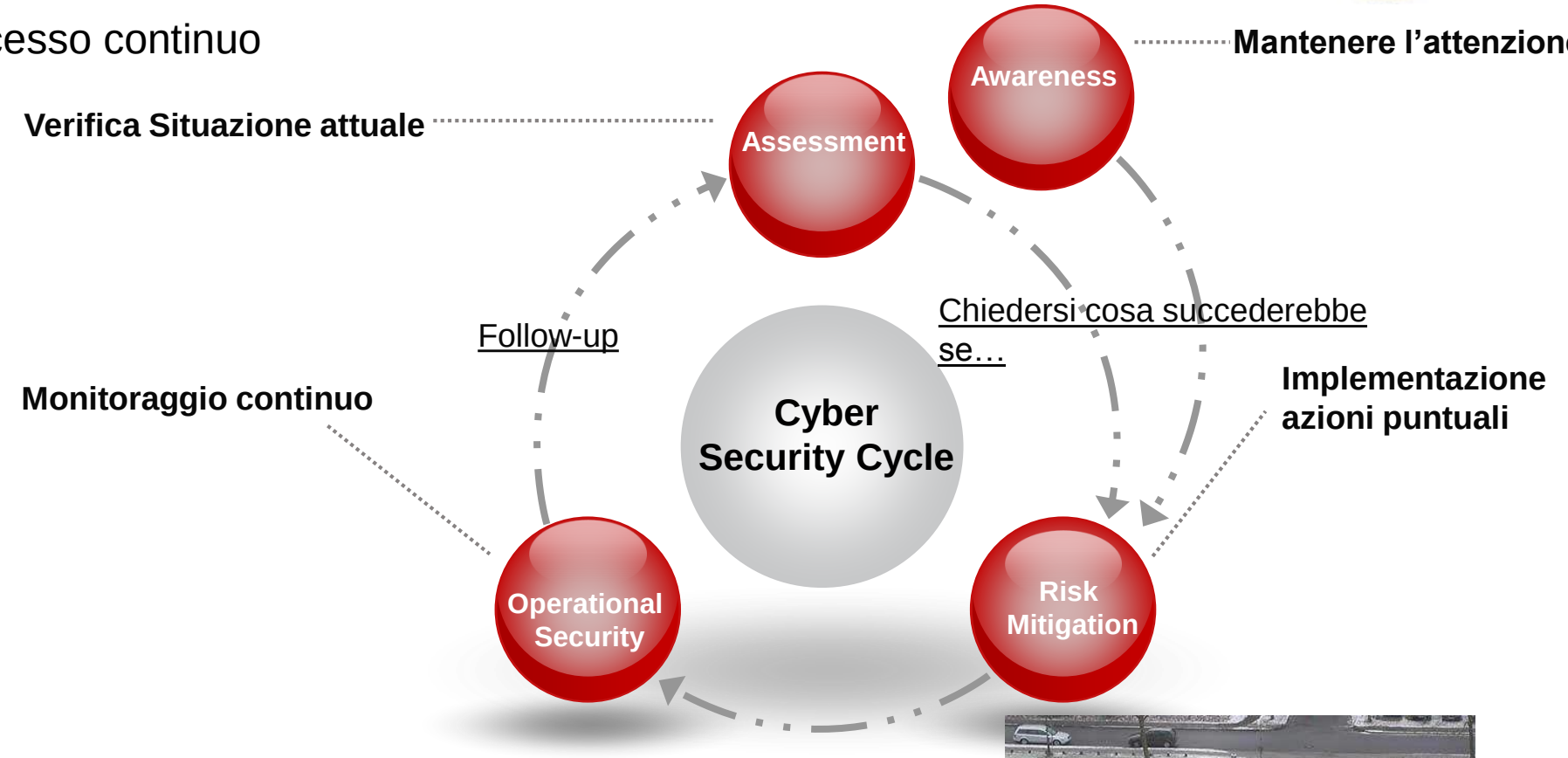
Sicurezza in sistemi d'ufficio e industriali

Due mondi a confronto diverse priorità

	Corporate/Office IT	Utilities/Industria
Condizioni ambientali	Uffici e «mobile»	Spesso «ostili», «in campo»
Caratteristiche dell' ambiente	Numero dispositvi ~= Numero di persone	Poche persone, moltissimi dispositivi**.**
Obiettivo principale da proteggere	Informazione: Riservatezza	Processi industriali: Disponibilità (availability), non interrompibilità
Principali conseguenze	Diffusione dell'informazione, $$$	Sicurezza personale (rischio vita), Salute, Ambiente, diffusione dell'informazione, perdita produttività, fermo per guasto, costi per sostituire o riparare i sistemi, $$$
Requisiti disponibilità	95%-99% (fermo per guasto/anno: 18,25 – 3,65 giorni)	99,9%-99,999% (fermo per guasto/anno: 8,76 ore – 5,25 minuti)
Tempo di vita tipico del sistema	3-5 anni	15-30 anni
«Oggetti» coinvolti	Server centrali (CPU, memoria,…) e PC	Server/PC + Sistemi distribuiti, Sensori, PLC,…
Sistemi operativi	Windows	Windows + proprietari integrati
Software	Software commerciale installato su PC	Specifici per le diverse esigenze
Protocolli / comunicazione	Ben noti (HTTP over TCP/IP ,…) / principalmente web	Industriali (TCP/IP, specifici del Vendor/settore) / polling
Procedure	Ben note (cambio password,…)	Specifiche caso per caso
Principali attori	IBM, SAP, Oracle, etc.	ABB, Siemens, GE, Honeywell, Emerson, etc.

Il ciclo di sicurezza

Un processo continuo



Non esiste la sicurezza al 100%. La sicurezza:

- Non è una meta, ma un viaggio
- Non è un prodotto ma un processo

Scopi della sicurezza logico-fisica

Cinque “strati” di sicurezza

- **Deterrenza a ritardo**: evitare o almeno ritardare l’effetto di un attacco o minaccia almeno per il tempo necessario a mettere in campo delle contromisure;
- **Rilevazione degli attacchi**: riconoscere un attacco è fondamentale ai fine di mettere in atto le contromisure di sicurezza; nulla si può fare contro azione “malevole” non riconosciute;
- **Valutazione degli attacchi:** ai fini di valutarne la gravità o il rischio che ne può derivare per il sistema da proteggere
- **Comunicazione e notifica:** comunicare tempestivamente l’attacco o il rischio d’attacco a persone o sistemi dedicate alla sicurezza in modo che vengano attivate le contromisure
- **Risposta agli attacchi:** azioni messe in campo da persone o sistemi per mitigare l’effetto dell’attacco; l’efficacia della risposta può impedire o ritardare un attacco successivo.

Requisiti di sicurezza

Dualità delle garanzie

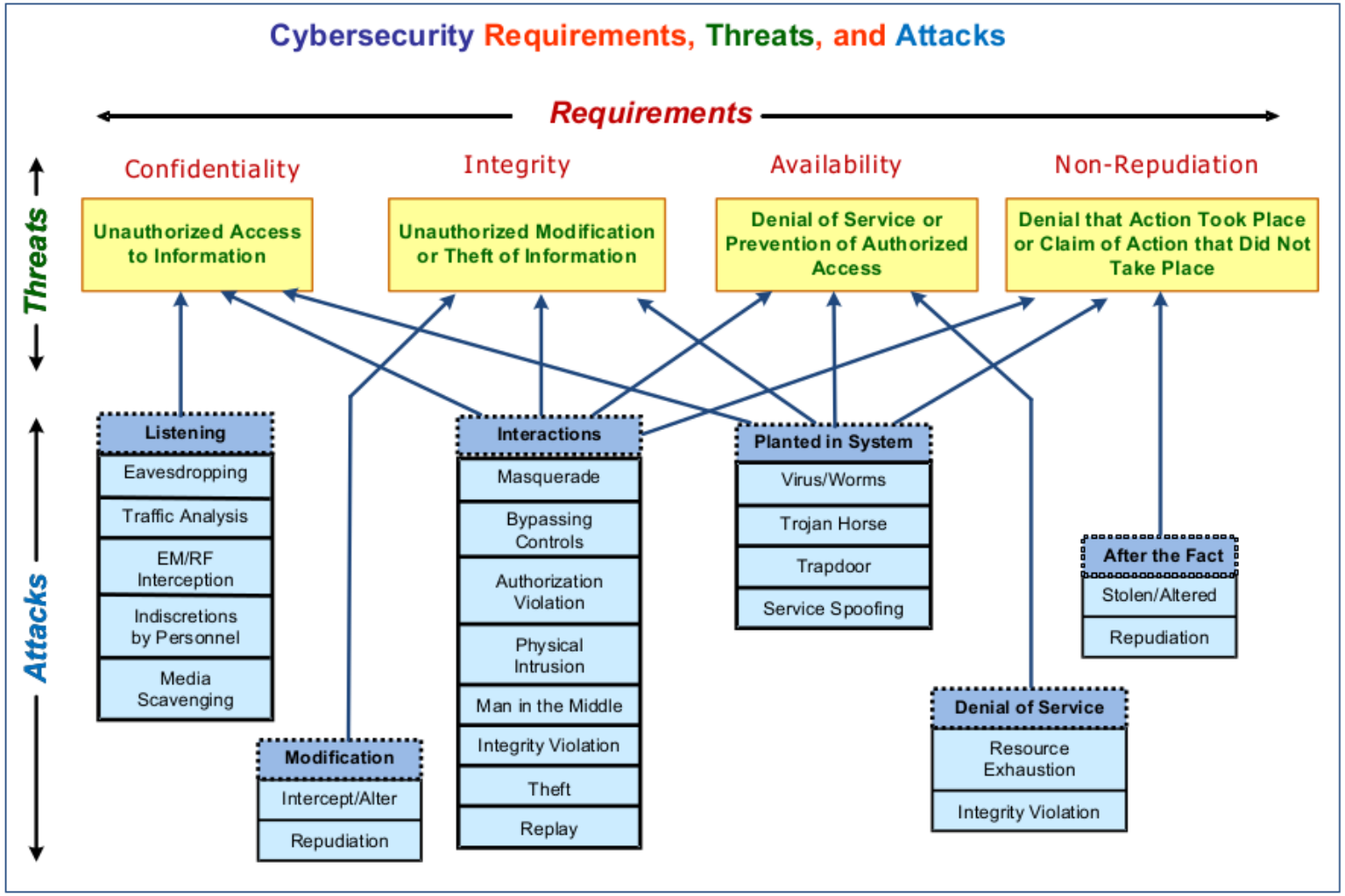
- **Riservatezza** (Confidentiality): prevenire un accesso non autorizzato ad informazioni;
- **Integrità** (Integrity): prevenire modifica non autorizzata e furto di informazioni;
- **Disponibilità** (Availability): prevenire provocate indisponibilità a servizi vitali e consentire l'accesso autorizzato ad informazioni;
- **Non-ripudiabilità o responsabilità** (Non-repudiation or accountability): prevenire rifiuto azione avvenuta o rivendicazione di un'azione non avventa.

Garantire l'accesso autorizzato tanto quanto impedire l'accesso non autorizzato

Requisiti di sicurezza

Tipi attacco e minacce

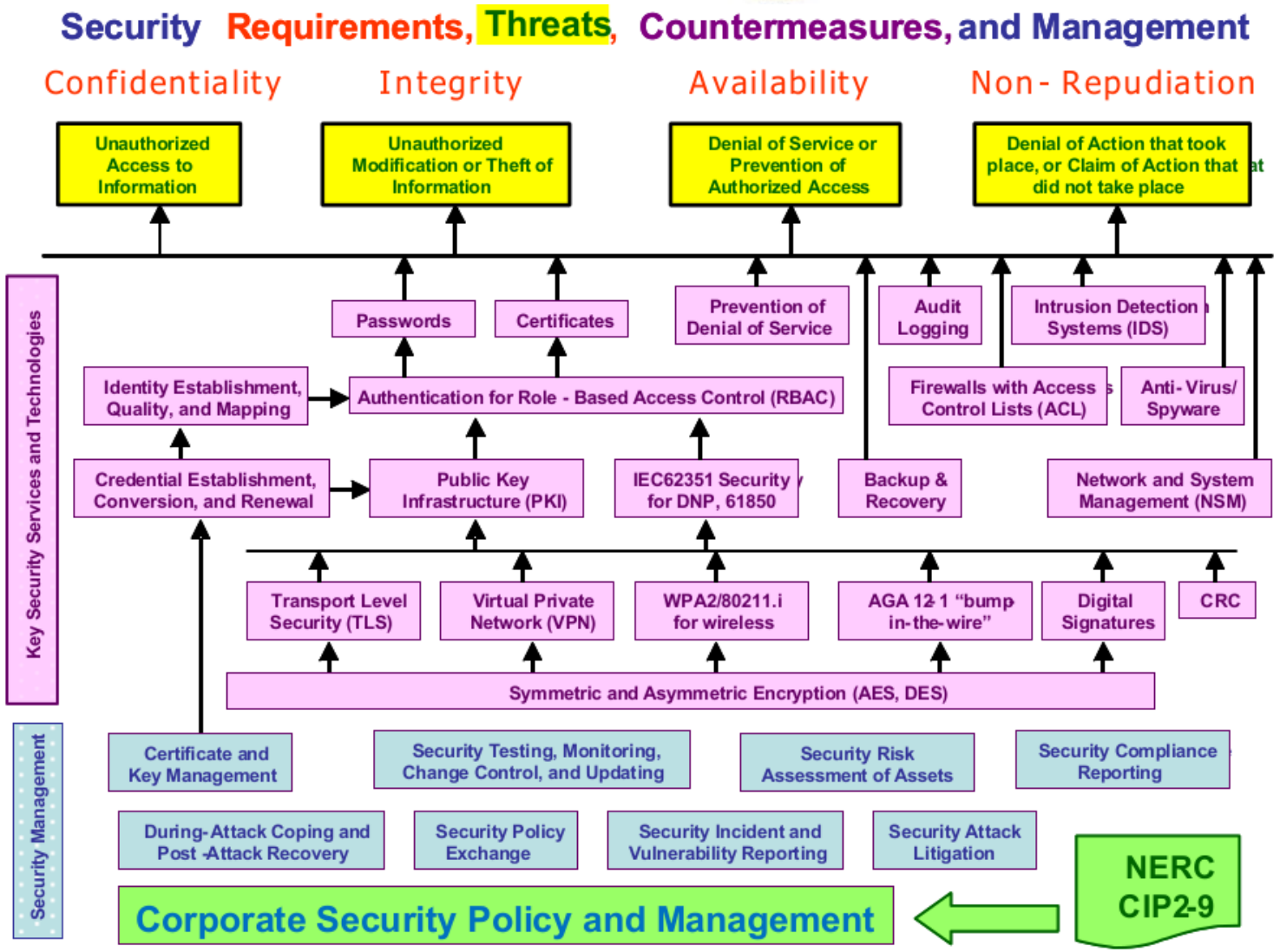
Tipi di attacco e minacce classificati in ordine ai requisiti di sicurezza fondamentali



Requisiti di sicurezza

Tipi attacco e minacce

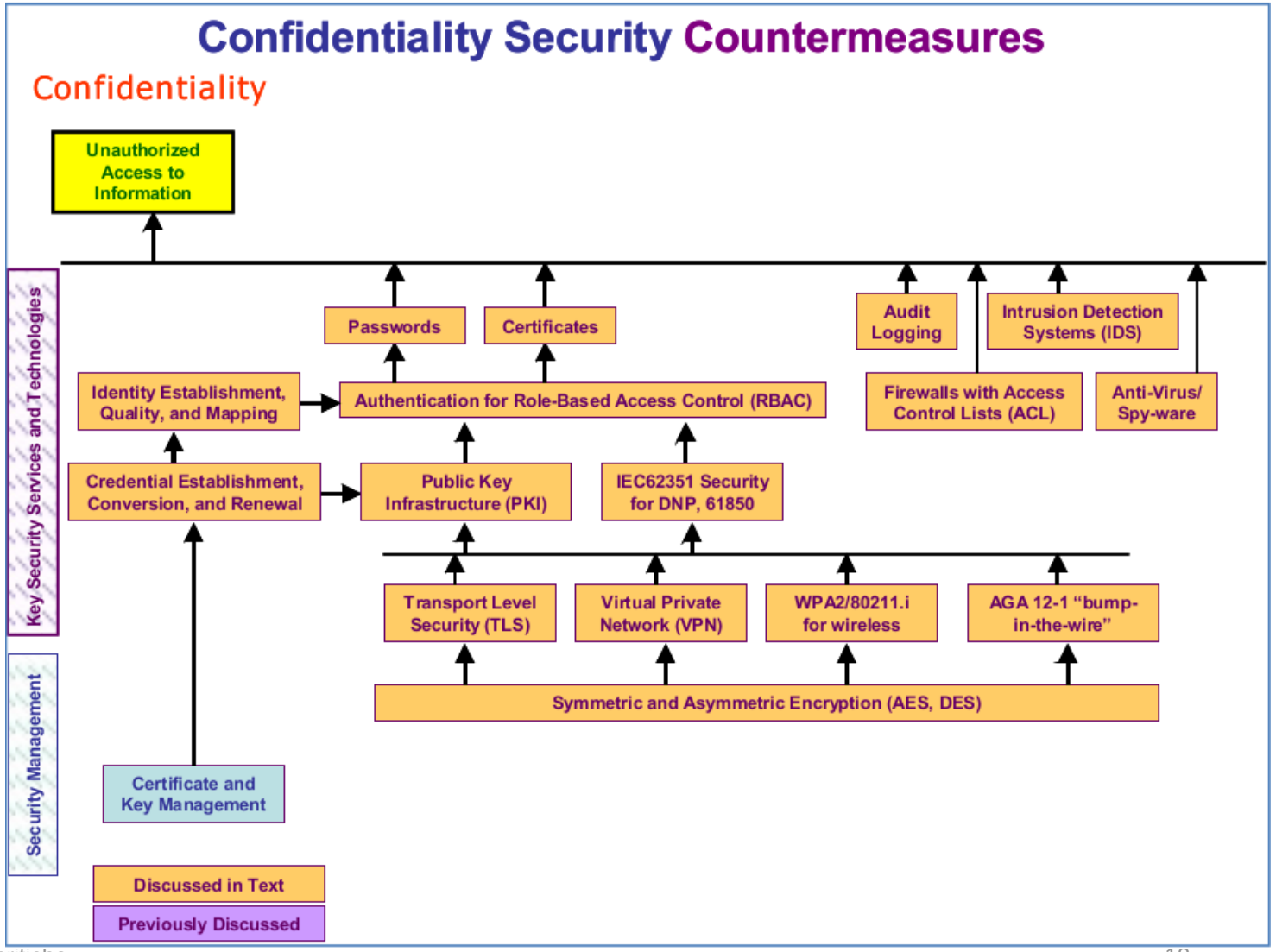
Contromisure tecniche ed organizzative in ordine ai requisiti di sicurezza fondamentali



Requisiti di sicurezza

Tipi attacco e minacce

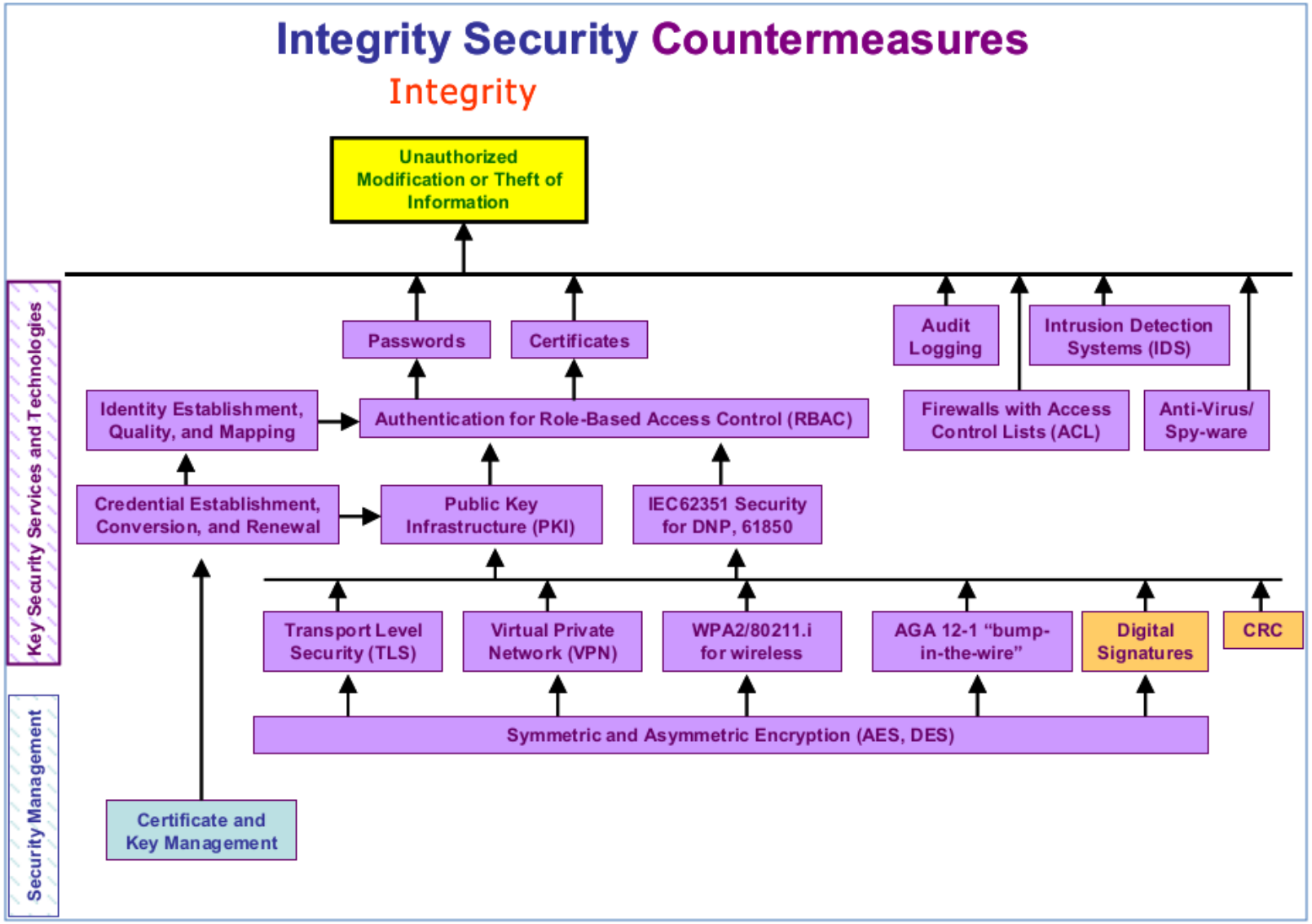
Esempi di contromisure tecniche ed organizzative do mettere in campo per il requisito di sicurezza: **Riservatezza**



Requisiti di sicurezza

Tipi attacco e minacce

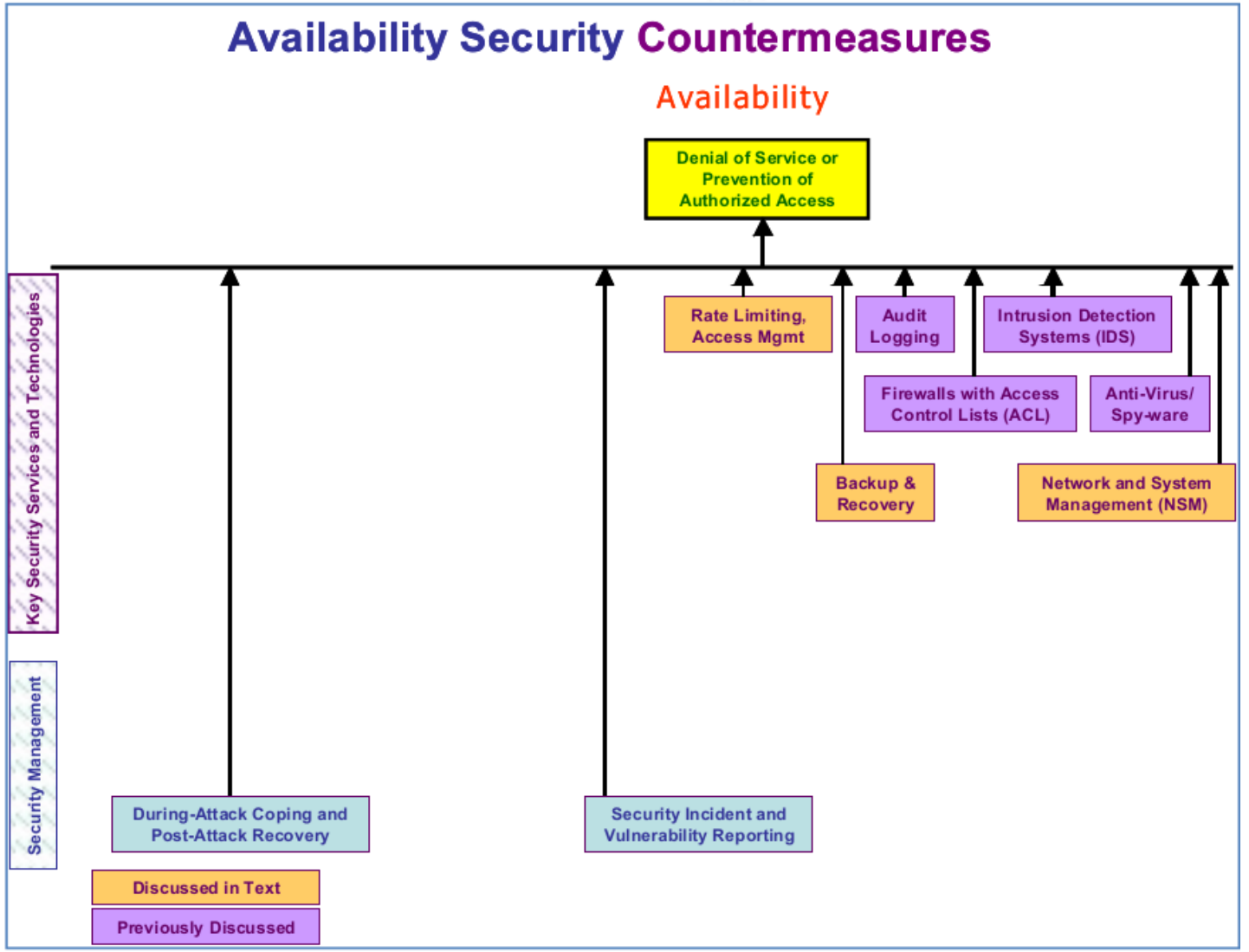
Esempi di contromisure tecniche ed organizzative do mettere in campo per il requisito di sicurezza: **Integrità**



Requisiti di sicurezza

Tipi attacco e minacce

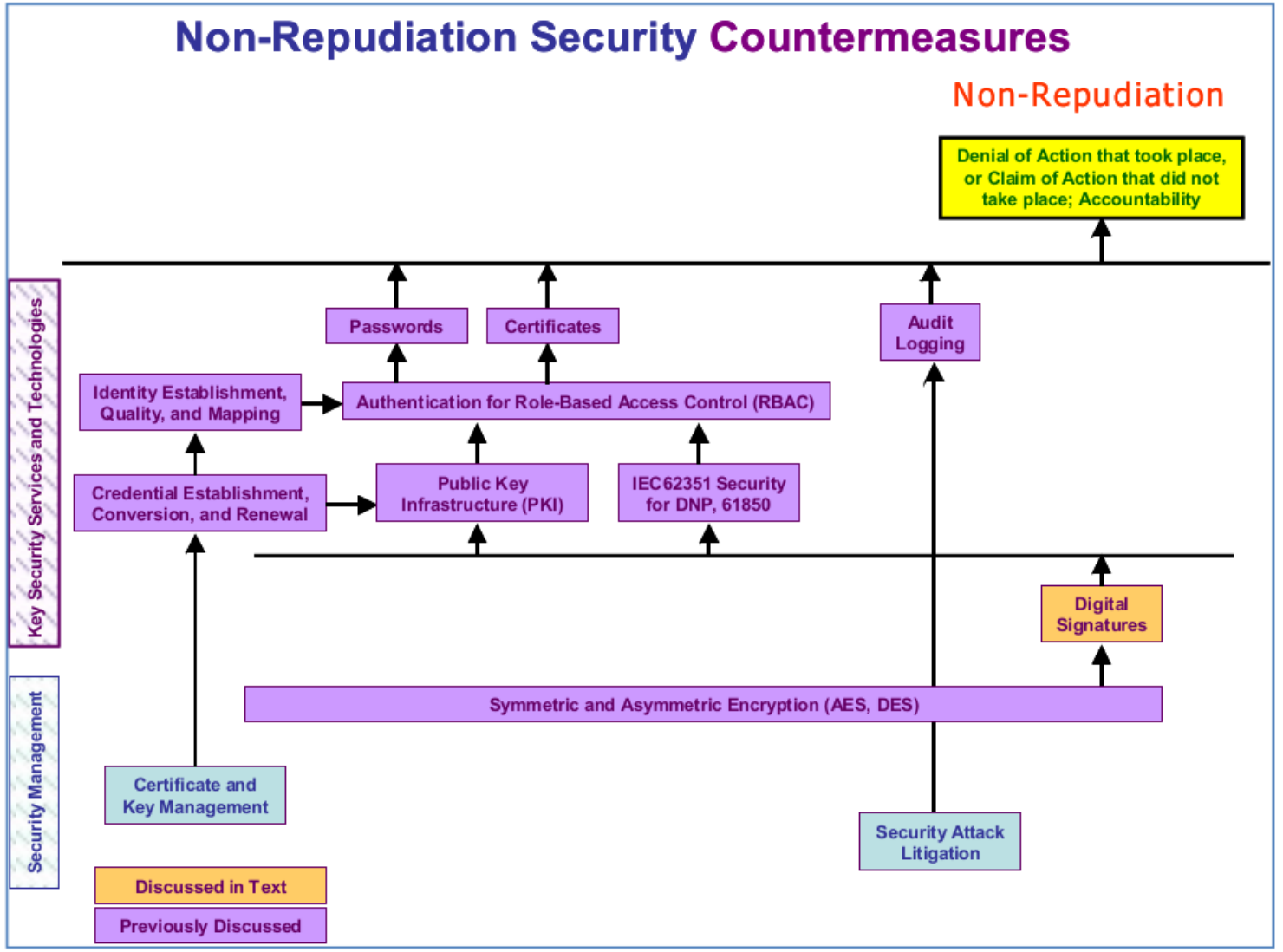
Esempi di contromisure tecniche ed organizzative do mettere in campo per il requisito di sicurezza: **Disponibilità**



Requisiti di sicurezza

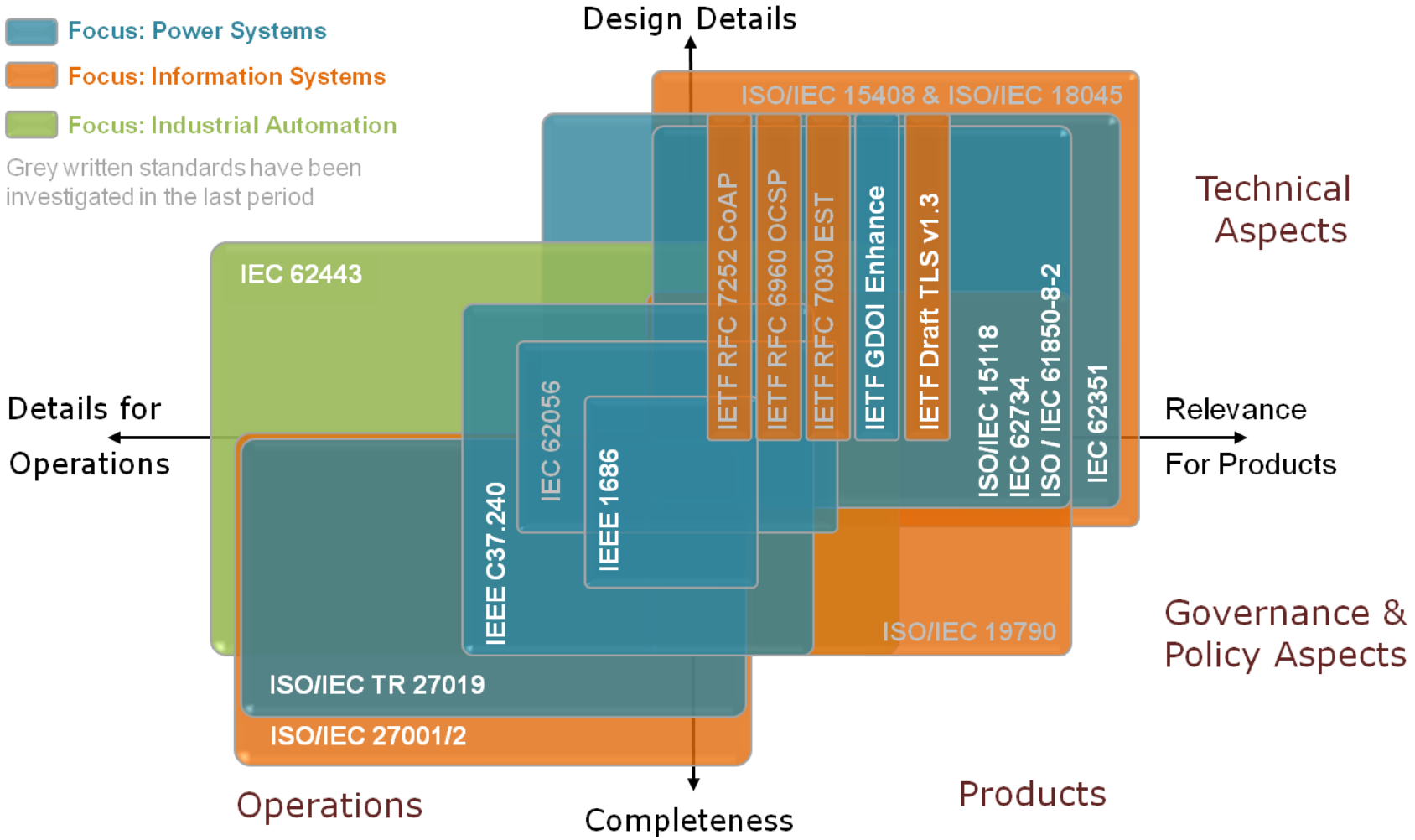
Tipi attacco e minacce

Esempi di contromisure tecniche ed organizzative do mettere in campo per il requisito di sicurezza: **Non-ripudiabilità o responsabilità**



Norme di sicurezza in campo industriale

Norme diverse per scopi diversi



Sicurezza in sistemi d’ufficio e industriali

Due mondi a confronto diverse priorità

Fine Prima Parte

Commenti

Pausa

Cyber Security nelle infrastrutture critiche

Indice seconda parte:

- La norma IEC 62351: architettura e parti
- Un sistema di telecontrollo per una infrastruttura critica
- La separazione logica fra SCADA e NSM
- Applicazione IEC 62351 a scambio dati IEC 60870-5-104
- IEC 62351 a scambio dati IEC 61850 nei DER (Smart Grid)
- Conclusioni

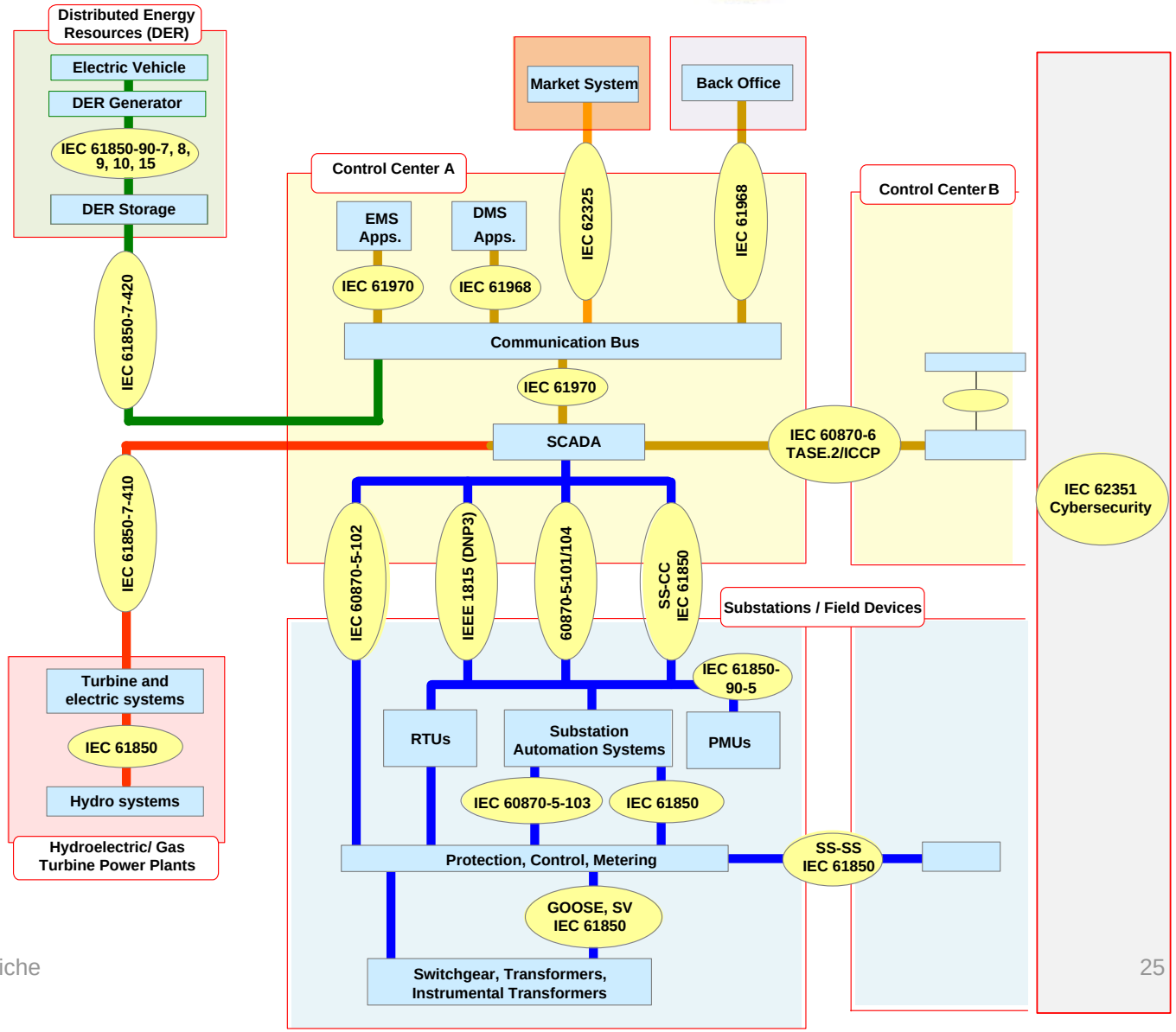
Architettura delle norme IEC TC 57

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



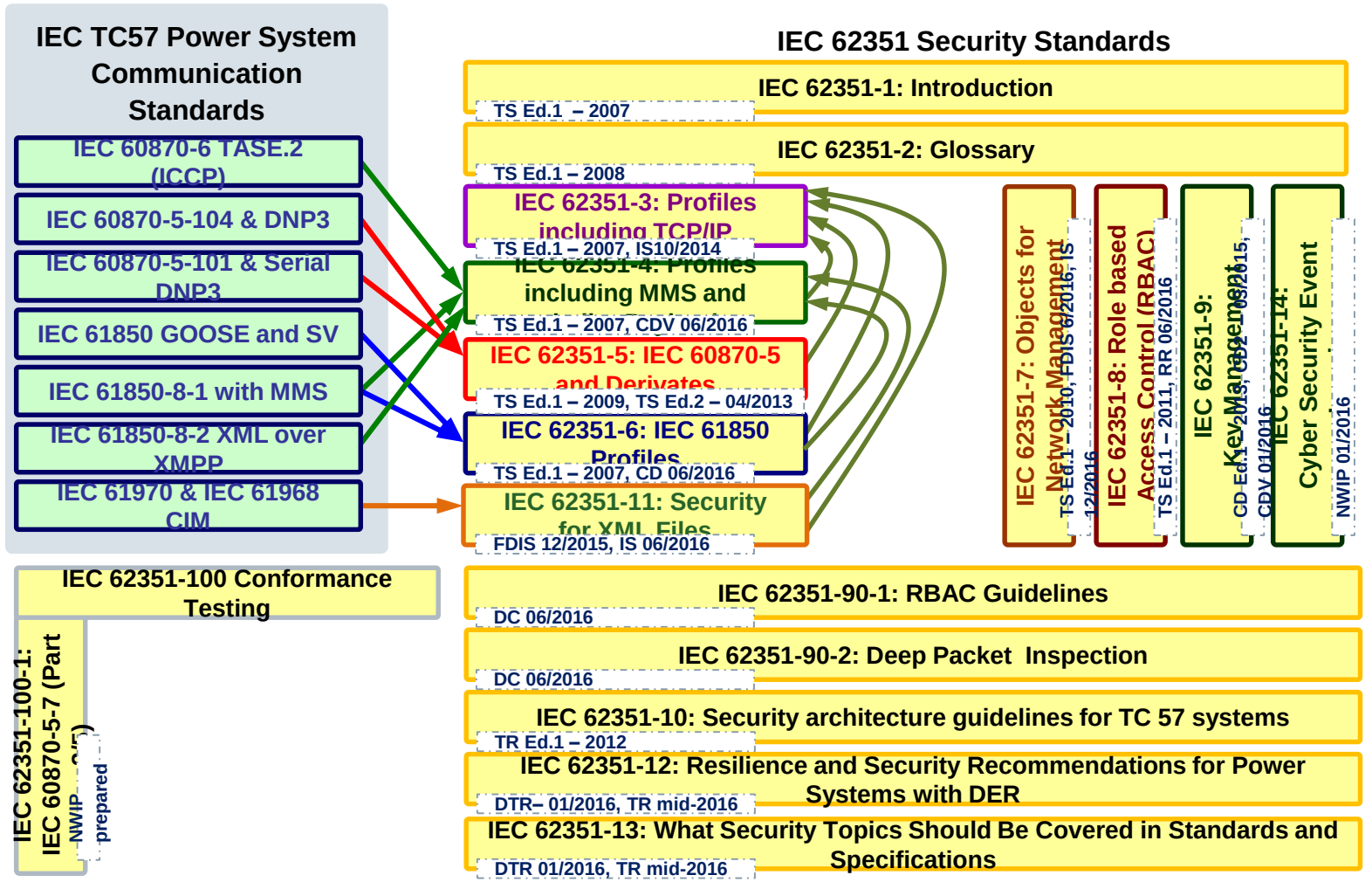
Norma IEC 62351

La scomposizione in parti

International Electrotechnical Commission

Technical Committee 57 - Power systems management and associated information exchange

Working Group 15 - Data and communication security



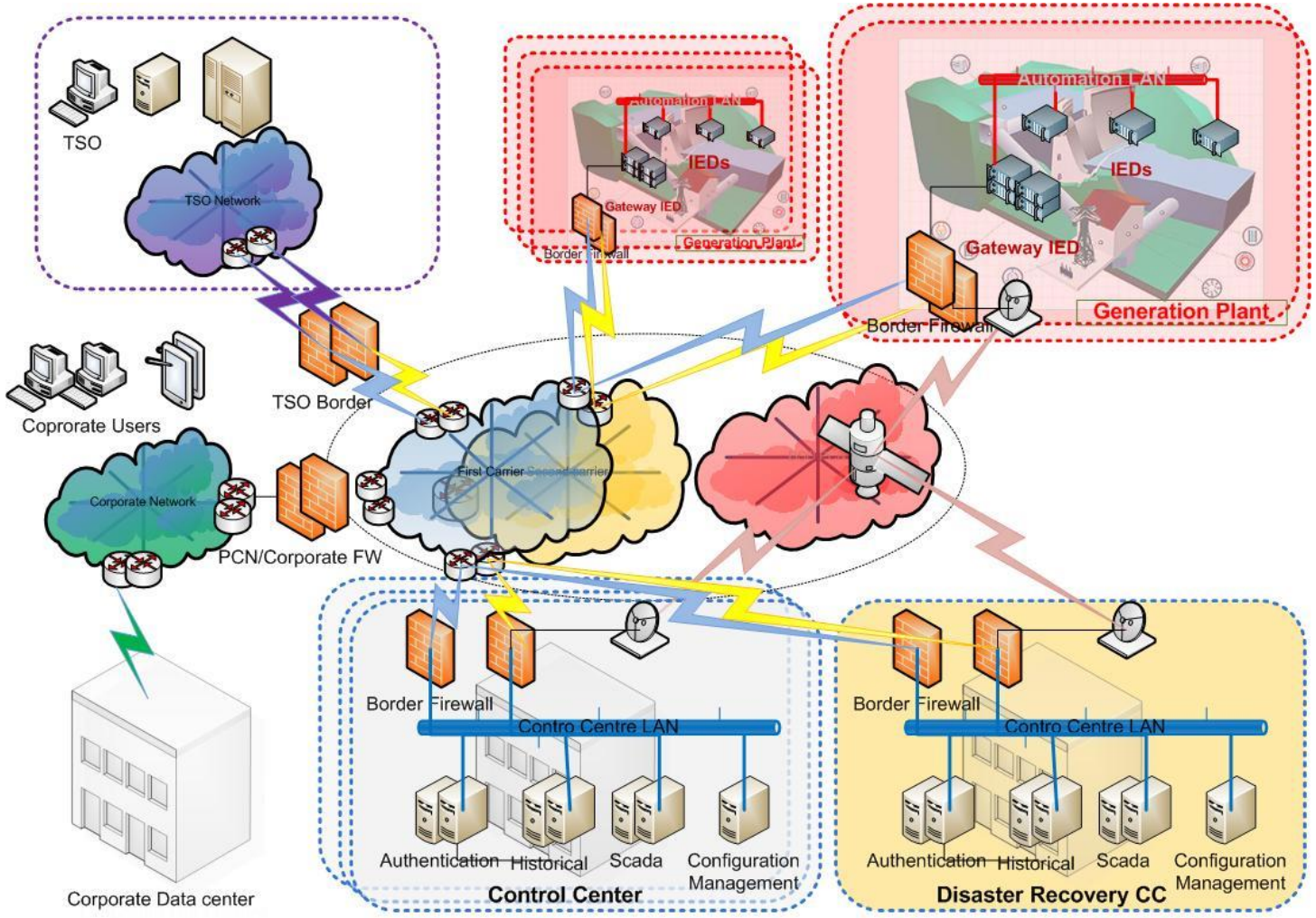
Norma IEC 62351: stato a febbraio 2016

IEC 62351 Part	Released	Activities (by January 2016)	Planned Release (New)
IEC/TS 62351-1: Introduction	2007	May need to be updated	
IEC/TS 62351-2: Glossary of terms	2008	Review Report pending	Pending
IEC/IS 62351-3: Security for profiles including TCP/IP	2014		IS Ed. 2 in 2014
IEC/TS 62351-4: Security for profiles including MMS	2007	Work on the A Profile enhancements. How much of the XMPP should be addressed here since security is discussed in 61850-8-2?	IS Ed. 2: **CDV 7/2016**, FDIS 12/2016, IS Jun 2017
IEC/TS 62351-5: Security for IEC 60870-5 and derivatives	2013	Released April 2013	**RR for IS process to be issued ?/2016;**
IEC/TS 62351-6: Security for IEC 61850 profiles	2007	Updates underway, based on security requirements in IEC 61850-90-5	RR was issued mid-2014, **CD 7/2016** in parallel with Part 4
IEC/TS 62351-7: Objects for Network Management	2010	CD issued 1/2015, responded to CD1 comments, updating UML model	**CDV 12/2015**, FDIS 6/2016, IS 12/2016
IEC/TS 62351-8: Role-Based Access Control	2011	Discussions on developing categories of roles	**Issue RR for IS by 6/2016** after TR 90-1 issued
IEC/IS 62351-9: Key Management	Pending	CDV in early 2016	**CDV by 2/2016** and FDIS in mid 2016, IS in late 2016
IEC/TR 62351-10: Security Architecture	2012	TR published Oct 2012	
IEC/IS 62351-11: Security for XML Files	2016	Going out as FDIS	**FDIS 12/2015**, IS 6/2016
IEC/TR 62351-12: Resilience and Security Recommendations for Power Systems with DER	2016	Sent out as DTR 1/2016	**DTR 1/2016**
IEC/TR 62351-13: Guidelines on What Security Topics Should Be Covered in Standards and Specifications	2016	Sent out as DTR 2/2016	**DTR 2/2016**
PWI: IEC/TR 62351-90-1: Guidelines for Using Part 8 Roles	DC in 2016	Actively being developed	**WD 3/2016, DC 6/2016**, TR maybe by 12/2016 if 2nd DC not needed
IEC 62351-100-1: Conformance test cases for IEC 62351-5 and companion standards	NWIP 2016	Starting with conformance testing of IEC 62351-3, 62351-5, and 60870-5-7	**NWIP by 2/2016**
IEC 62351-14 Security Event Logging and Reporting	PWI NWIP	Based on existing security logging	**NWIP by 3/2016**
IEC/TR 62351-90-2 Deep Packet Inspection	PWI DC Pending	TR to discuss the issues around deep packet inspection	**DC 6/2016,** DTR 12/2016

Esempio di sistema di Telecontrollo

Le parti di un sistema per una infrastruttura critica

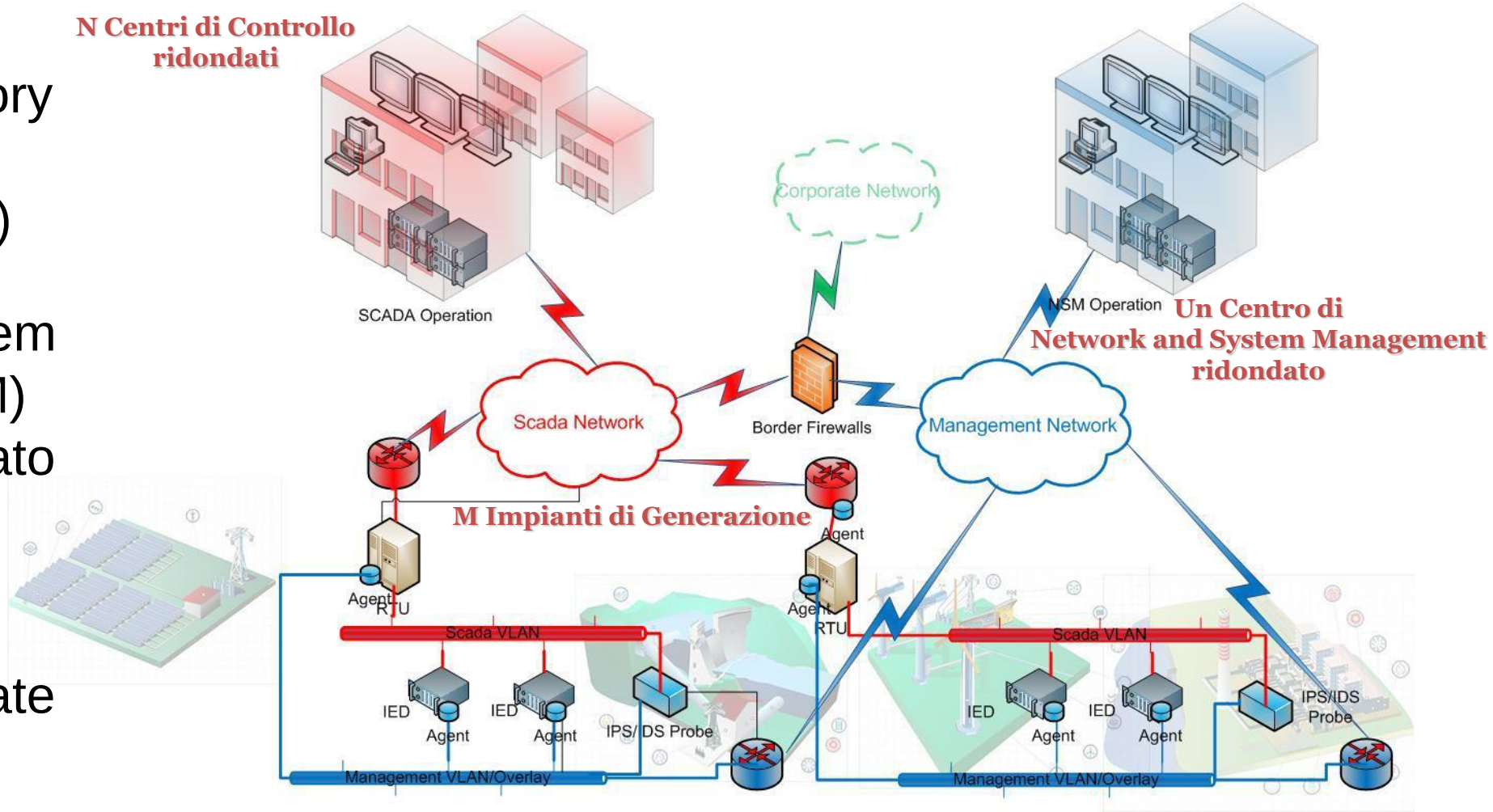
- Ridondanza degli apparati
- Alta disponibilità delle telecomunicazioni
- Prevenzione e rilevazione delle intrusioni



Esempio di sistema di Telecontrollo

SCADA e NSM due parti dello stesso sistema

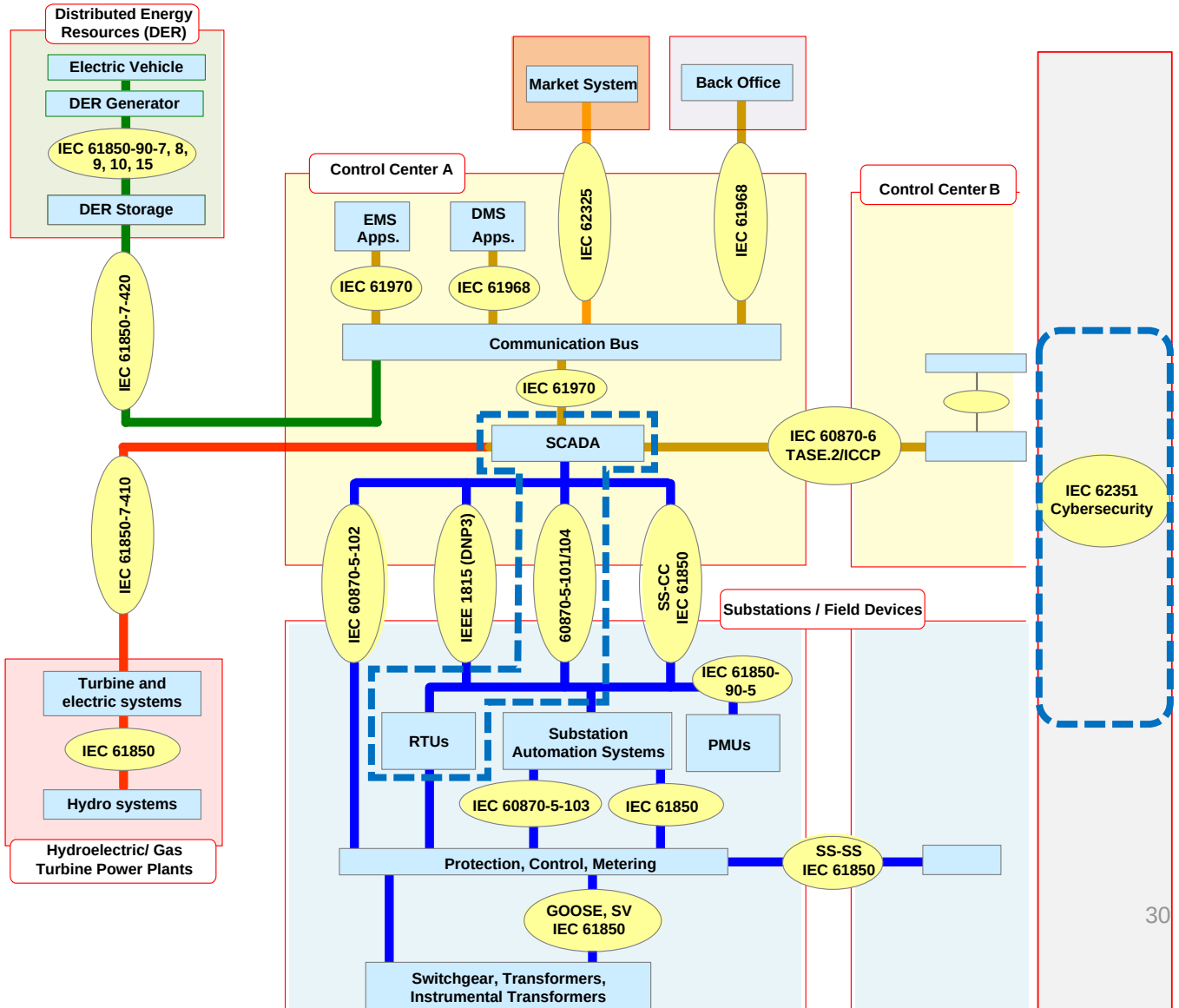
- Sistema Supervisory Control And Data Aquisition (SCADA)
- Network and System Management (NSM) logicamente separato
- Rete di accesso SCADA e NSM logicamente separate



Esempio di sistema di Telecontrollo

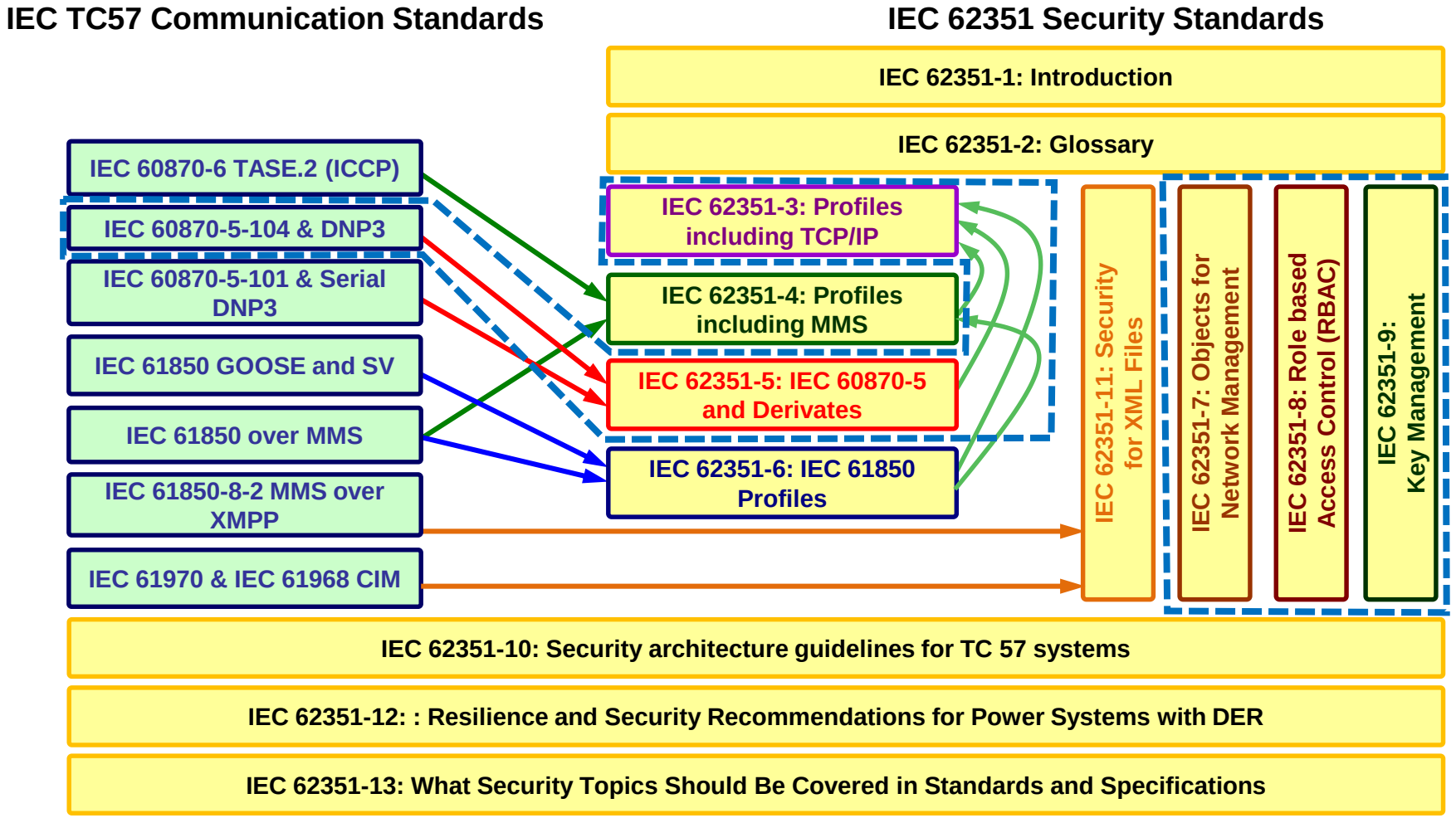
Applicazione IEC 62351 a scambio dati IEC 60870-5-104

- 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

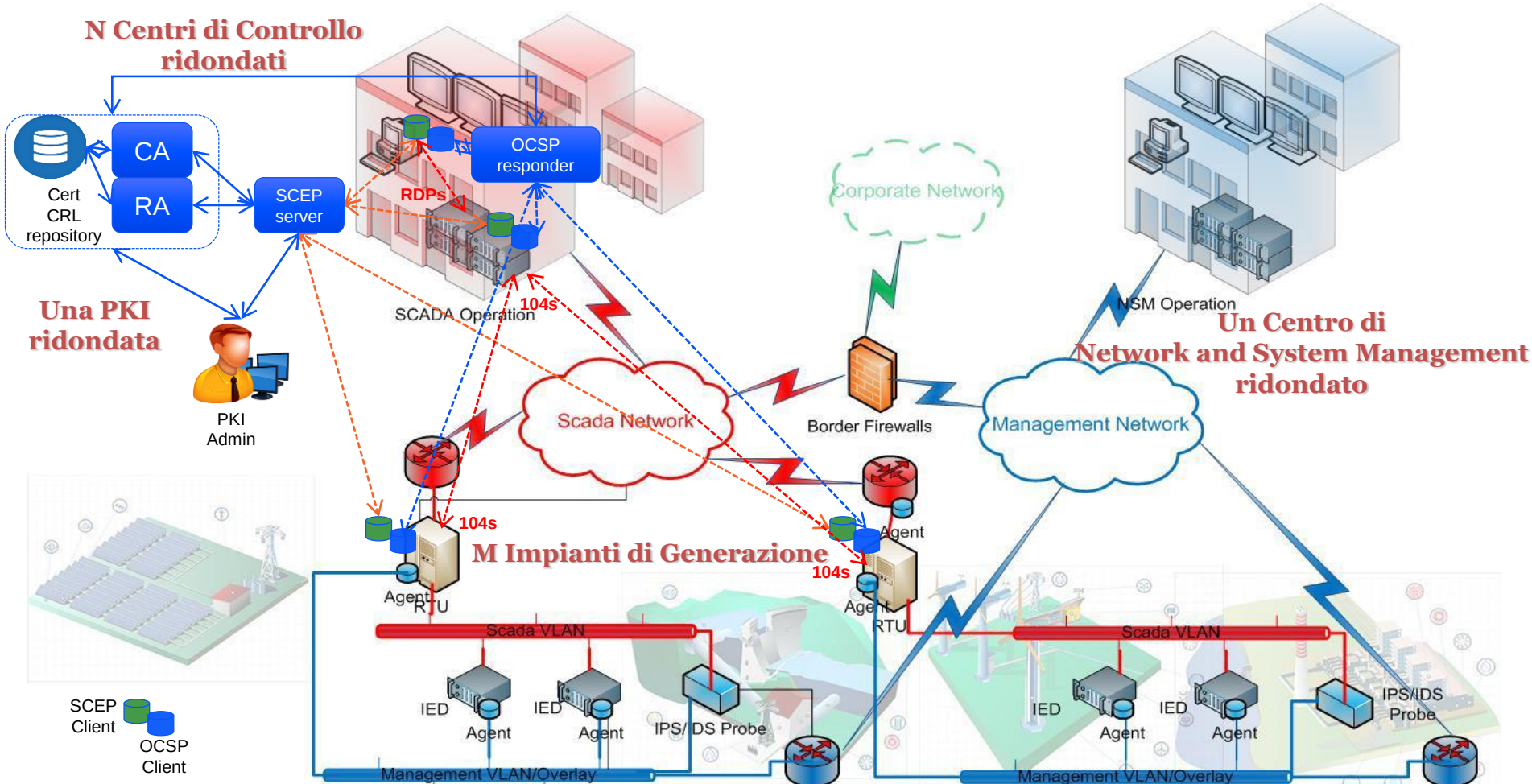


Esempio di sistema di Telecontrollo

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

- Sistema Supervisory Control And Data Aquisition (SCADA)
- Network and System Management (NSM)
- Public Key Infrastructure (PKI)

Rete di accesso SCADA e NSM logicamente separate

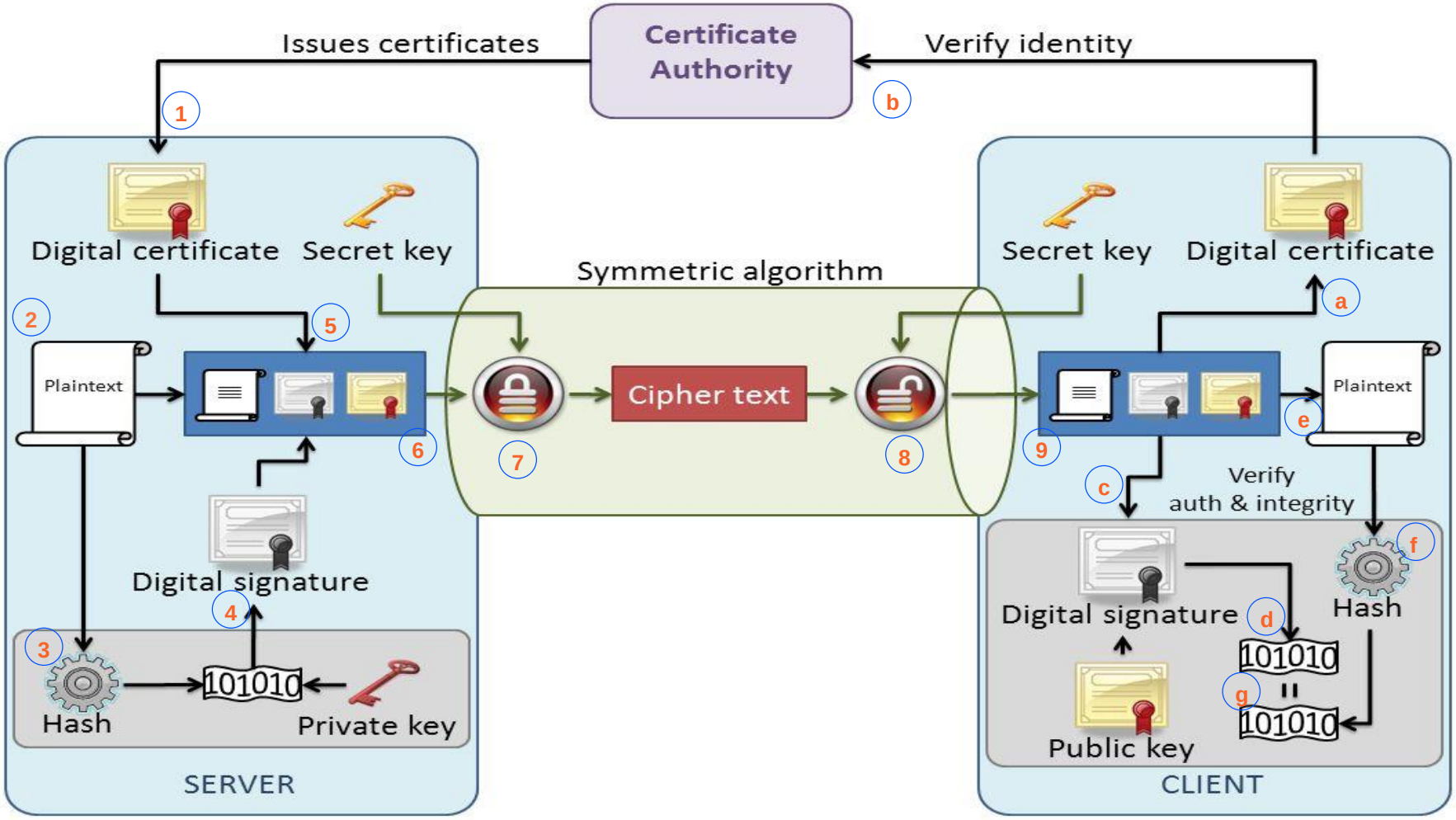


Esempio di sistema di Telecontrollo

Uso della crittografia

Esempio passo-passo per uno scambio cifrato di cui viene verificata:

- *Autenticità (il messaggio proviene da fonte autentica)*
- *Integrità (il messaggio non è stato modificato in transito)*

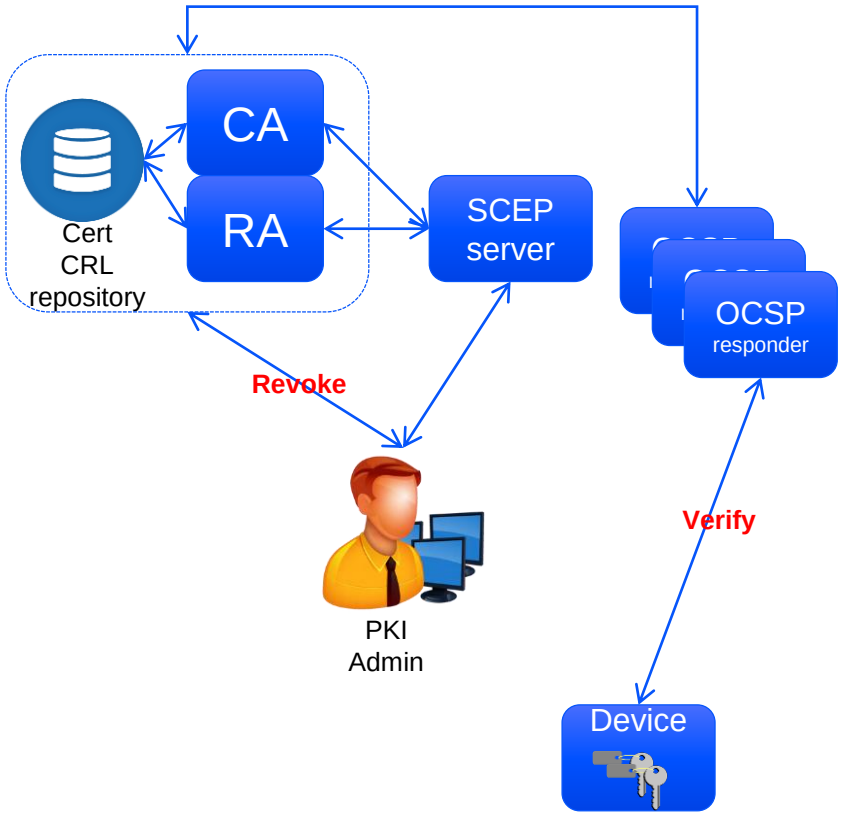


Esempio di sistema di Telecontrollo

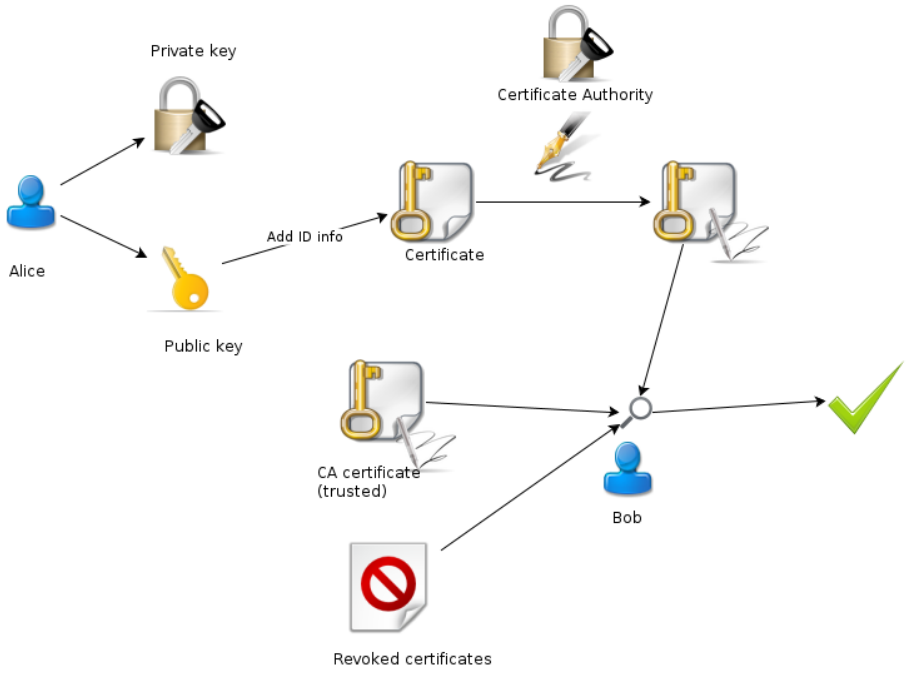
Uso della crittografia

Due operazioni eseguite tramite i servizi della PKI:

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



Revoca – Verifica Validità del Certificato



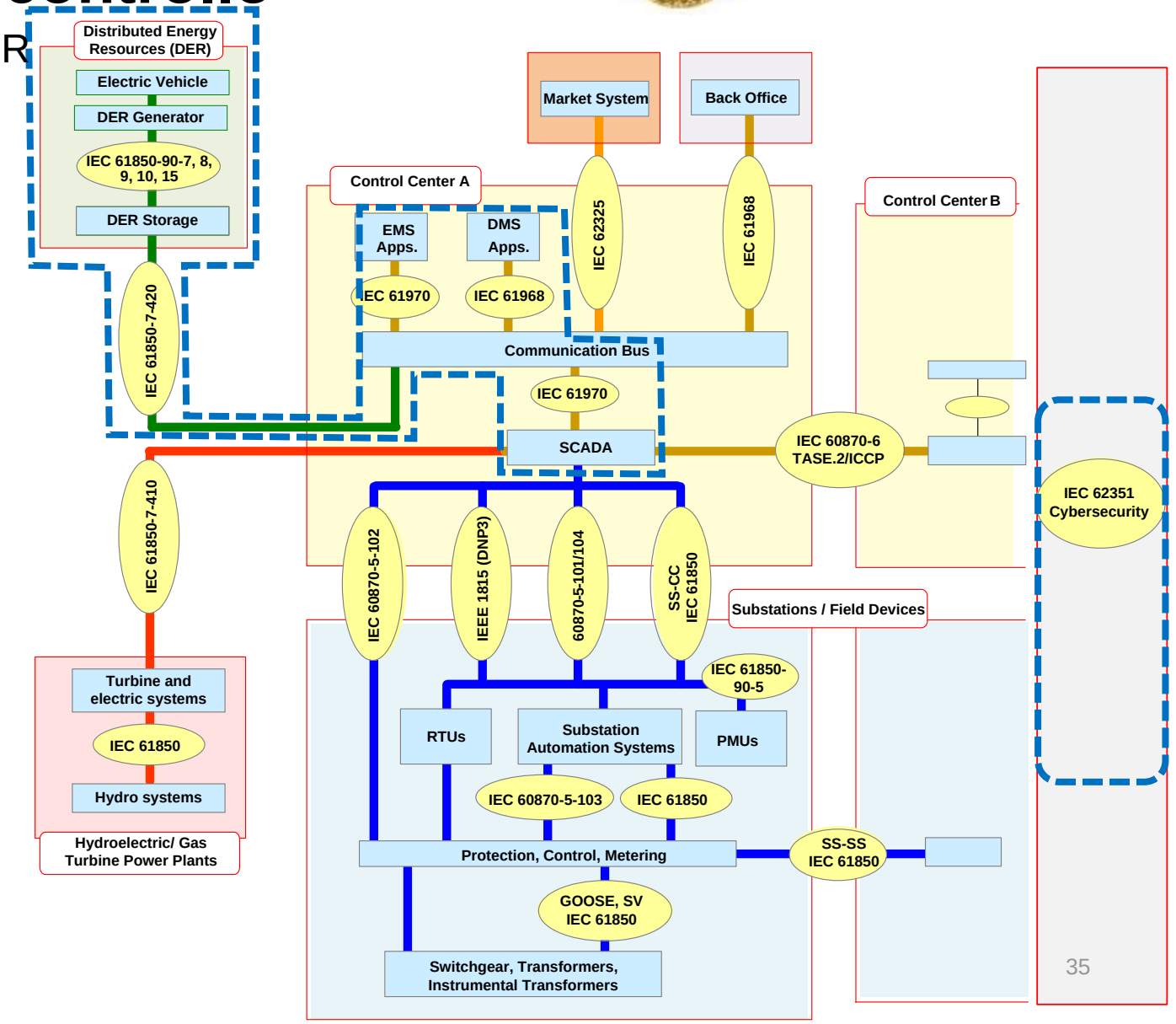
Alice e Bob possono essere rispettivamente il server SCADA e una RTU
La verifica è mutua e i ruoli si scambiano

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



Cyber Security nelle infrastrutture critiche

Conclusioni

(1)Essere coscienti sull'argomento

(2)Promuovere la sensibilità sul tema della Cyber Security a tutti i livelli (dal progetto alla manutenzione)

(3)La Cyber Security è un indice diretto della robustezza (resilienza) di una infrastruttura critica

(4)Non esiste la sicurezza al 100%

(5)La Cyber Security è un processo continuo

(6)La Cyber Security non è gratis

COLLEGIO DEGLI INGEGNERI DELLA PROVINCIA DI VENEZIA

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI VENEZIA

GRAZIE PER LA VOSTRA ATTENZIONE

Stefano Doga: stefano.doga@it.abb.com

Federico Bellio: federico.bellio@enel.com

Power and productivity
for a better world™