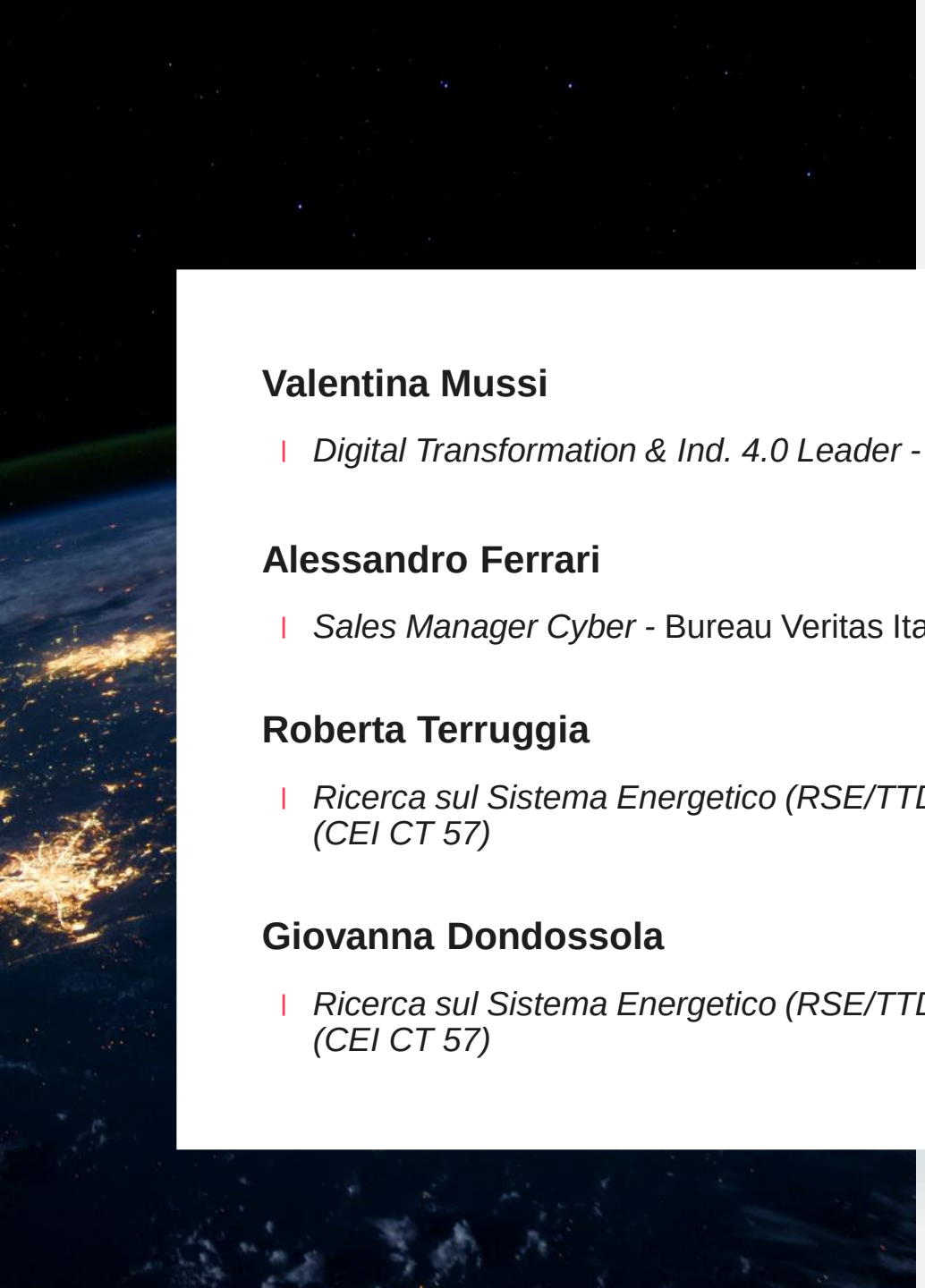
WORKSHOP

CYBERSECURITY ENERGY SECTOR: STRUMENTI E TECNICHE DI DIFESA

MILANO • 29 MARZO 2023 • 14.30



RELATORI

Valentina Mussi

- *Digital Transformation & Ind. 4.0 Leader* - Bureau Veritas Italia

Alessandro Ferrari

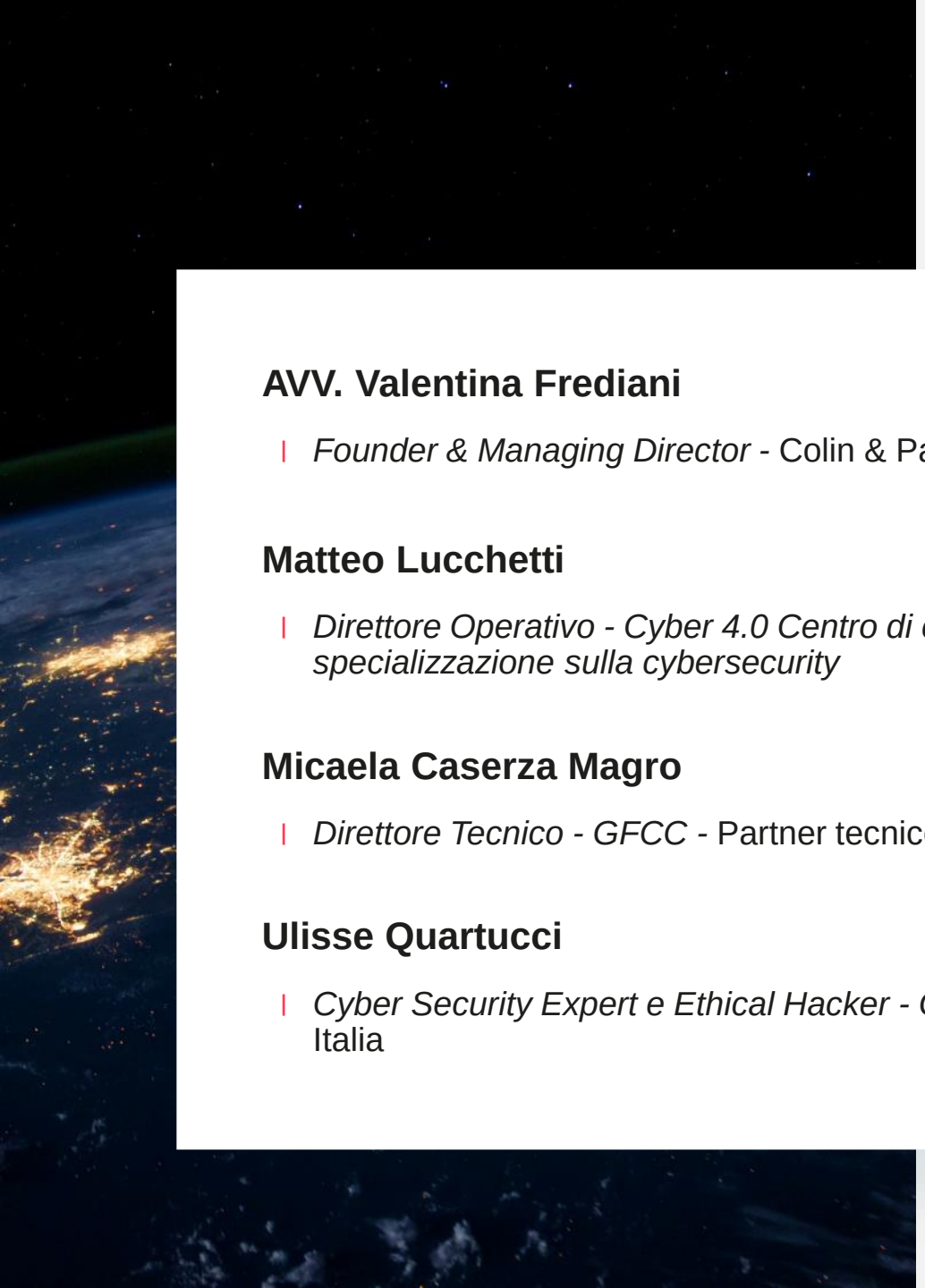
- *Sales Manager Cyber* - Bureau Veritas Italia

Roberta Terruggia

- *Ricerca sul Sistema Energetico (RSE/TTD) e Comitato elettrotecnico Italiano (CEI CT 57)*

Giovanna Dondossola

- *Ricerca sul Sistema Energetico (RSE/TTD) e Comitato Elettrotecnico Italiano (CEI CT 57)*



RELATORI

AVV. Valentina Frediani

- *Founder & Managing Director* - Colin & Partners

Matteo Lucchetti

- *Direttore Operativo - Cyber 4.0 Centro di competenza nazionale ad alta specializzazione sulla cybersecurity*

Micaela Caserza Magro

- *Direttore Tecnico - GFCC* - Partner tecnico Bureau Veritas Italia

Ulisse Quartucci

- *Cyber Security Expert e Ethical Hacker - GFCC* - Partner tecnico Bureau Veritas Italia

PROGRAMMA

Benvenuto e Presentazione Bureau Veritas e Secura

Il regolamento CEI 016 – focus Cybersecurity

Nis2: i nuovi obblighi nel settore energetico in ambito di cybersicurezza

La strategia e gli strumenti per la transizione digitale sicura

Casi pratici di valutazione del rischio cybersecurity in ambito Energy

Dibattito finale

01

IL REGOLAMENTO **CEI 016**
FOCUS CYBERSECURITY

AGENDA

CEI 0-16 CYBERSECURITY

Contesto regolatorio e normativo

CEI 0-16 - Certificazioni e soluzioni di cybersecurity

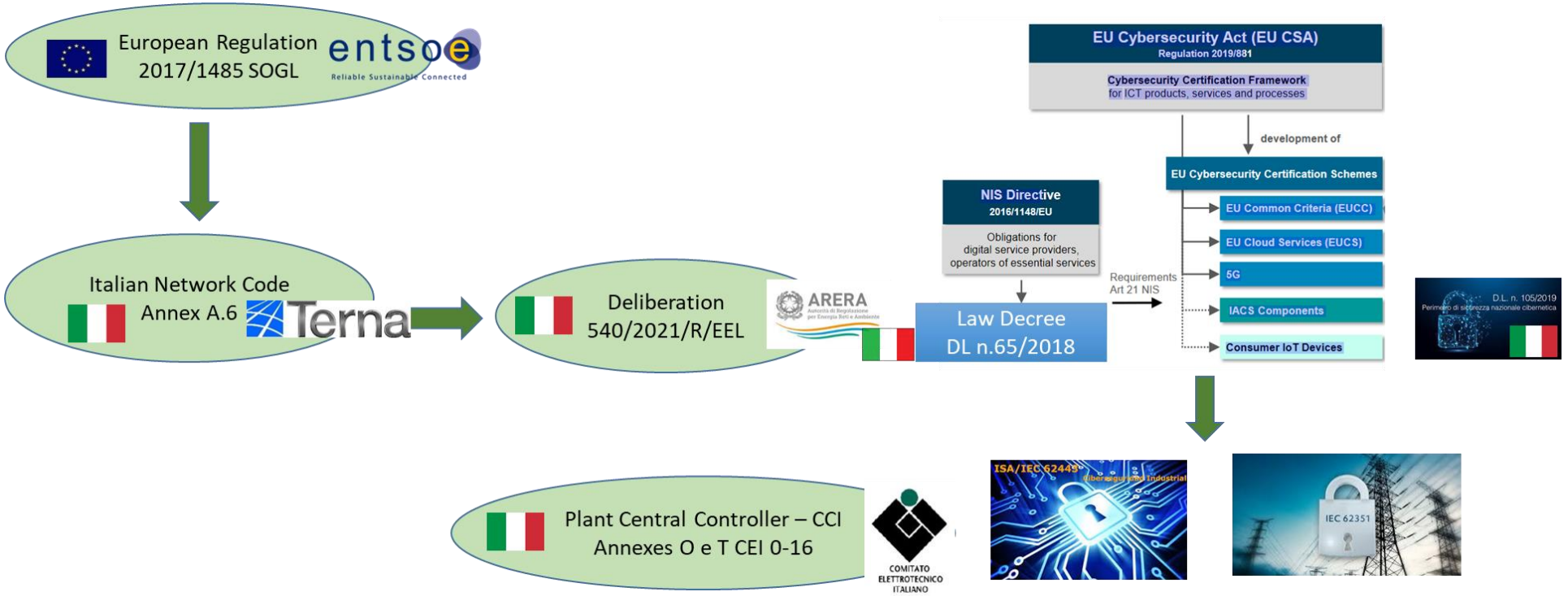
ISA/IEC 62443 – Requisiti di cybersecurity

IEC 62351 – Soluzioni di cybersecurity

Mapping ISA/IEC 62443-IEC 62351 – Dai requisiti di cybersecurity alle soluzioni

CONTESTO REGOLATORIO E NORMATIVO

ENERGY E CYBERSECURITY



CEI 0-16

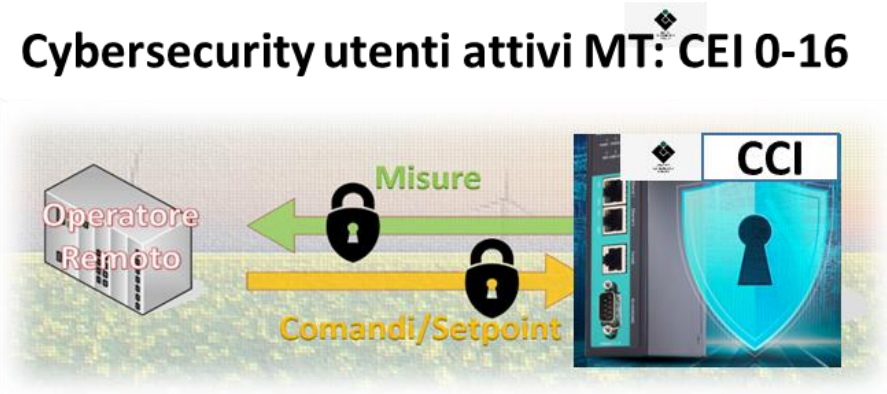
CYBERSECURITY

CEI 0-16:2022-03 «Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT e MT delle imprese distributrici di energia elettrica»

Allegato O – Controllore Centrale di Impianto - CCI

Allegato T – Funzioni, modello dati, comunicazioni e cybersecurity

Recepiscono gli standard IEC 61850 e IEC 62351



CEI 0-16 ALLEGATO O

CERTIFICAZIONE HARDWARE CYBERSECURITY

Allegato O, Sezione O.15.14

Per il componente crittografico HSM del CCI è richiesta la certificazione FIPS 140-2 L3

- **Grado di resistenza del componente alla manomissione fisica**

CEI 0-16 ALLEGATO O

CERTIFICAZIONE CYBERSECURITY PRODOTTO CCI

Allegato O, sezione O.15.5

Certificazione di conformità allo standard CEI EN 62443-4-1

- **Sicurezza del processo di sviluppo del CCI**

Certificazione di conformità alla CEI EN 62443-4-2

CEI 0-16

CERTIFICAZIONI CYBERSECURITY COMUNICAZIONI CCI

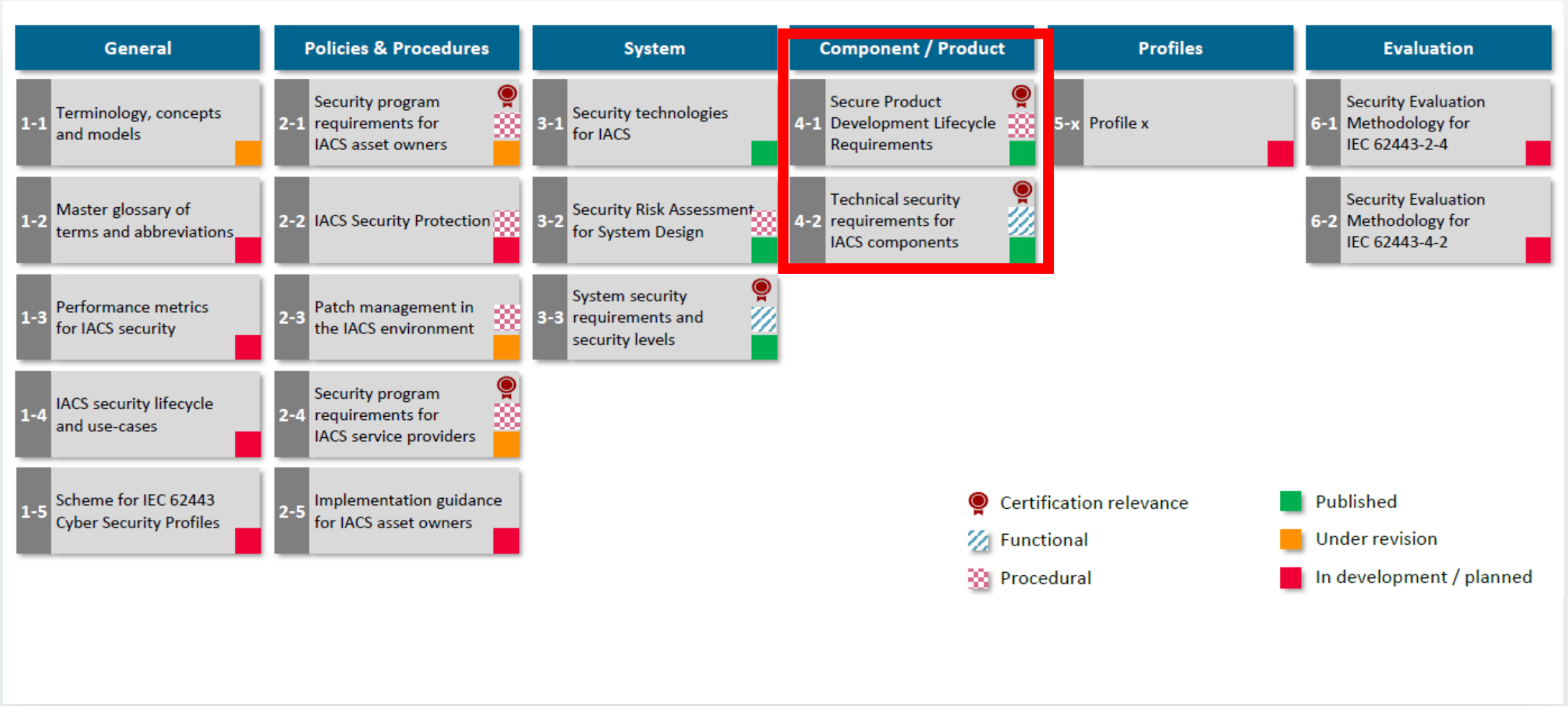
Allegato O, sezione O.15.5

Certificazione di conformità alla IEC TS 62351-100-3

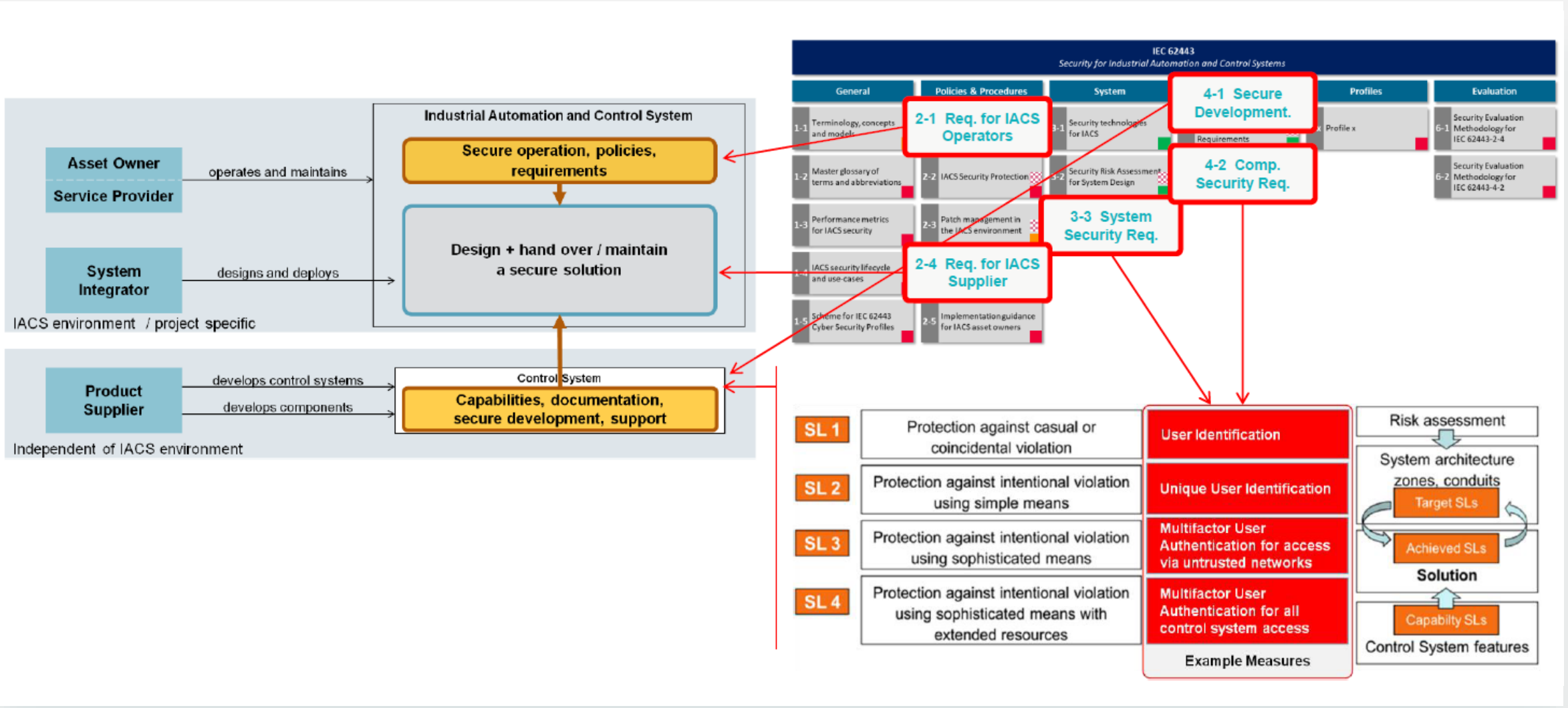
In futuro Certificazione di conformità alla IEC TS 62351-100-4

Conformance Testing IEC 62351

ISA/IEC 62443



ISA/IEC 62443

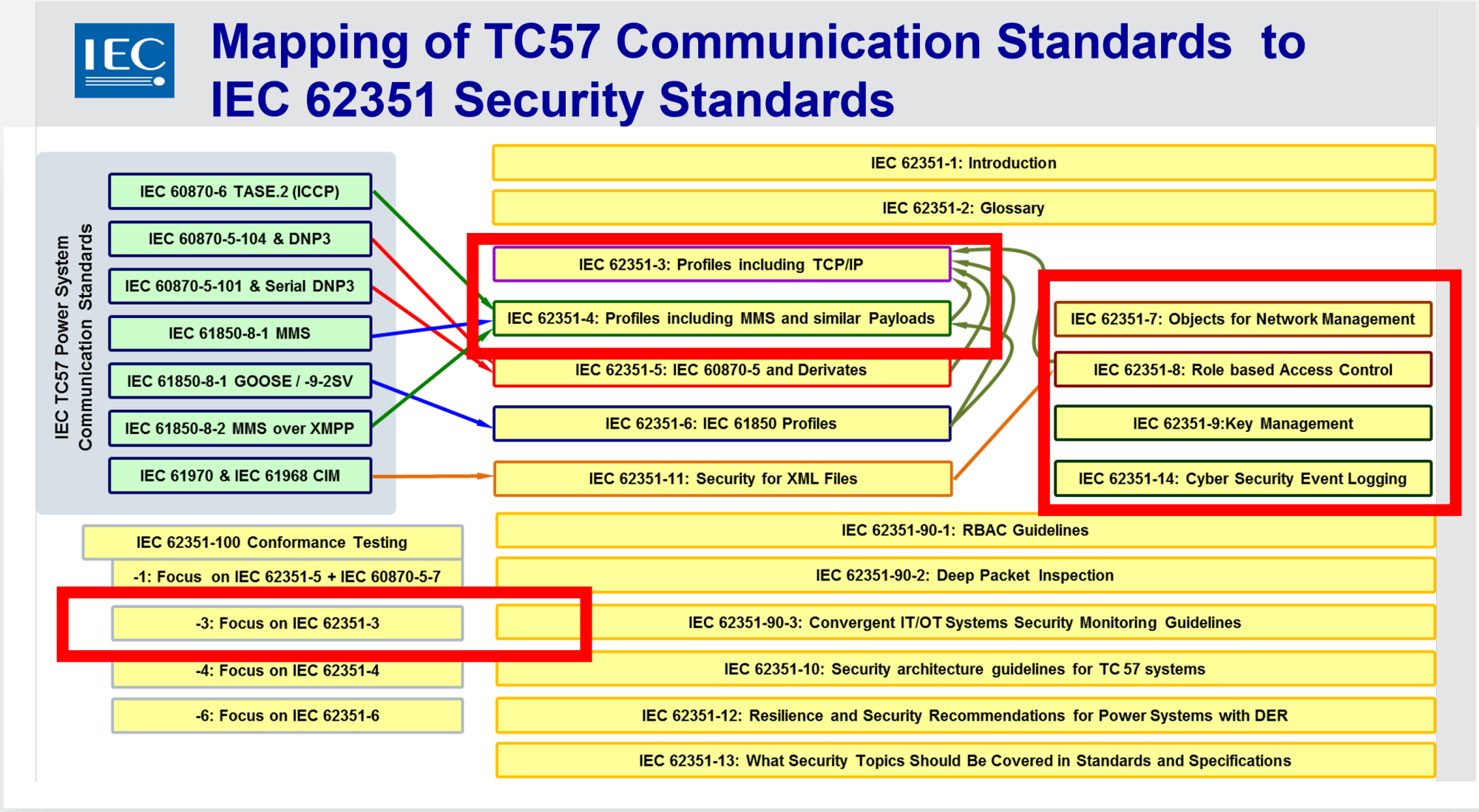


APPLICAZIONE ISA/IEC 62443-4-2 AL CCI

FUNCTIONAL REQUIREMENTS - SECURITY LEVELS

Functional Requirement	Descrizione	Security level
FR1	Identification and authentication control(IAC)	2
FR2	Use control (UC)	2
FR3	System integrity (SI)	2
FR4	Data confidentiality (DC)	1
FR5	Restricted data flow (RDF)	1
FR6	Timely response to events (TRE)	1
FR7	Resource availability (RA)	3

SERIE IEC 62351



APPLICAZIONE IEC 62351 AL CCI

Sicurezza delle comunicazioni IEC 62351-3, IEC 62351-4

- Livello trasporto: profili di sicurezza TLS
- Livello applicativo: sicurezza end-to-end

Gestione delle chiavi e dei certificati IEC 62351-9

- Chiavi pubbliche/private
- Public Key Infrastructure (PKI)
- Gestione dei certificati

Gestione dei ruoli IEC 62351-8

- Ruoli standard e ruoli customer

Monitoraggio della sicurezza IEC 62351-7, IEC 62351-14

- Misure ed eventi significativi

Test di Conformità 62351-100-3

- Conformità alla IEC 62351-3

ISA/IEC 62443 – IEC 62351 MAPPING

Functional Requirement	Descrizione	Security level	IEC 62351
FR1	Identification and authentication control(IAC)	2	Part 3, Part 4, Part 9
FR2	Use control (UC)	2	Part 8
FR3	System integrity (SI)	2	Part 3, Part 4
FR4	Data confidentiality (DC)	1	Part 3, Part 4
FR5	Restricted data flow (RDF)	1	Part 7
FR6	Timely response to events (TRE)	1	Part 14
FR7	Resource availability (RA)	3	Part 7 Part 14

ESEMPI DI MAPPING (1)

FR1	Identification and authentication control(IAC)	SL 2	Part 3, Part 4, Part 9	
CR 1.2 – Software process and device identification and authentication		SL 2	Part 3 Part 4	• identify itself and authenticate to any other component
CR 1.8 – Public key infrastructure certificates		SL 2	Part 9	• selection of an appropriate PKI
CR 1.9 – Strength of public key-based authentication		SL 2	Part 3 Part 9 Part 9 Part 4	• certificate's signature • certificate chain • certificate's revocation status • algorithms and keys used for the public key authentication conform

ESEMPI DI MAPPING (2)

FR2	Use control (UC)	SL 2	Part 8	

• CR 2.1 – Authorization enforcement
  • RE (1) Authorization enforcement for all users (humans, software processes and devices)
  • RE (2) Permission mapping to roles
		SL 2	Part 8	• authorization enforcement mechanism
				  • mapping of permissions to roles

FR3	System integrity (SI)	SL 2	Part 3, Part 4	
• CR 3.1 – Communication integrity • RE (1) Communication authentication		SL 2	Part 3	• capability to verify the authenticity of received information during communication.
• CR 3.8 – Session integrity		SL 2	Part 4	• protect the integrity of communications sessions

ESEMPI DI MAPPING (3)

FR4	Data confidentiality (DC)	SL 1	Part 3, Part 4	
CR 4.3 – Use of cryptography		SL 1	Part 3	• use cryptographic security mechanisms
CR 4.3 – Use of cryptography		SL 1	Part 4	• encryption and hash algorithms, such as the advanced encryption standard (AES) and the secure hash algorithm (SHA) series, and key sizes and changes based on an assigned standard
FR5	**Restricted data flow (RDF)**	**SL 1**	**Part 7**	
CR 5.1 – Network segmentation		SL 1	Part 7	• In response to an incident, it may be necessary to break the connections between different network segments. • Use of network and protocol metrics

ESEMPI DI MAPPING (4)

FR6	Timely response to events (TRE)	SL1	Part 14	
• CR 6.1 – Audit log accessibility		SL 1	Part 14	• access audit logs

FR7	Resource availability (RA)	SL3	Part 7 Part 14	
• CR 7.1 – Denial of service protection		SL 2	Part 7 Part 14	• maintains essential functions necessary for continued safe operations while in a degraded mode
• CR 7.6 – Network and security configuration settings • RE (1) Machine-readable reporting of current security settings		SL 3	Part 14	• generate a report listing the currently deployed security settings in a machine-readable format

CONTATTI

GIOVANNA DONDOSSOLA

Capo Progetto

+320.8399635
giovanna.dondossola@rse-web.it

RICERCA SUL SISTEMA ENERGETICO

RSE - SPA

ROBERTA TERRUGGIA

Ricercatrice

+393246008062
roberta.terruggia@rse-web.it

RICERCA SUL SISTEMA ENERGETICO

RSE - SPA