

Cybersecurity nella transizione energetica: dal quadro legislativo e regolatorio alle tecnologie

Giovanna Dondossola

Agenda

- Cybersecurity per i sistemi energetici
- Regolamenti Europei
 - NIS EU 2016/1148
 - EU 2019/881
 - NIS 2.0
 - Network Code on Cyber Security
 - Standard Internazionali
- Legislazione Italiana
 - DL 2018/65
 - DL 2019/105 e DPCM attuativi
- Cybersecurity per lo scambio dati con utenti attivi MT (SOGL)
 - Norme CEI e tecnologie

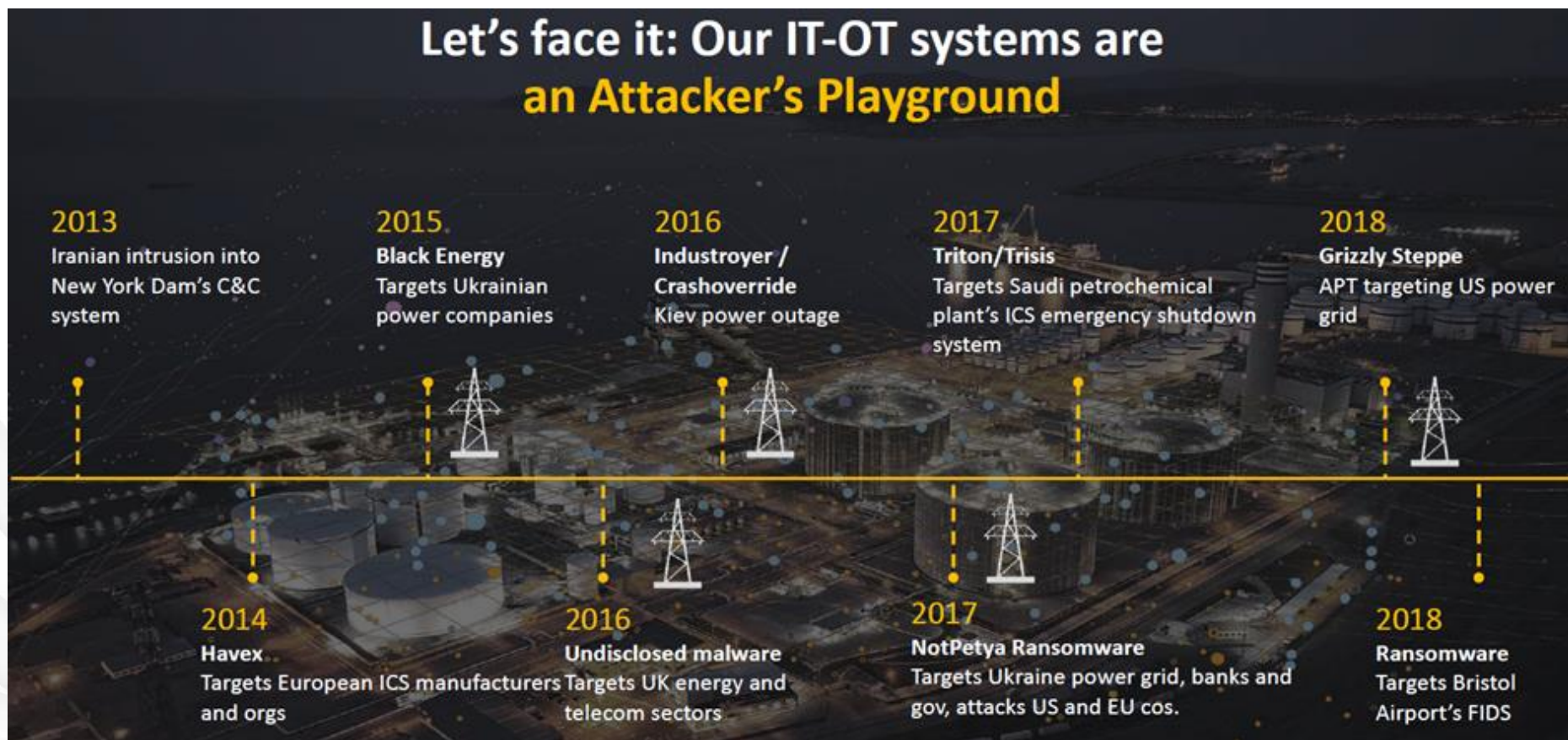
Contesto

- Infrastrutture energetiche
- Digitalizzazione
- Minacce cyber
- Legislazione e Regolamentazione



Storico attacchi

SGTech 2019, Johan Straten by Cyberbit



ENISA Threat Landscape 2021 — ENISA (europa.eu)

Figure 1: ENISA Threat Landscape 2021 - Prime threats

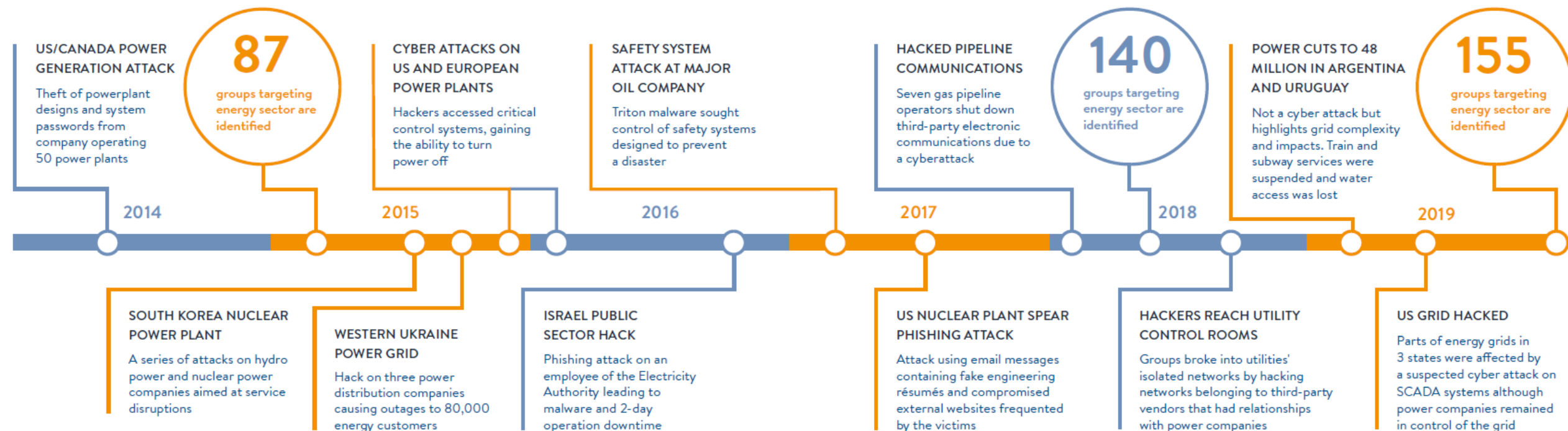


- Black Energy
- Industroyer

- NotPetya

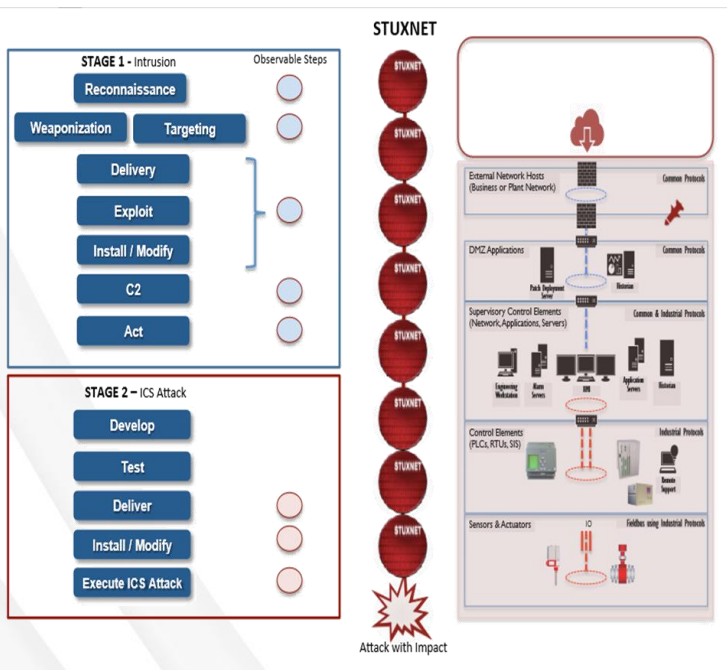
Profilo attaccanti

[Cyber Challenges to the Energy Transition WEC MMC 2019.pdf \(worldenergy.org\)](#)

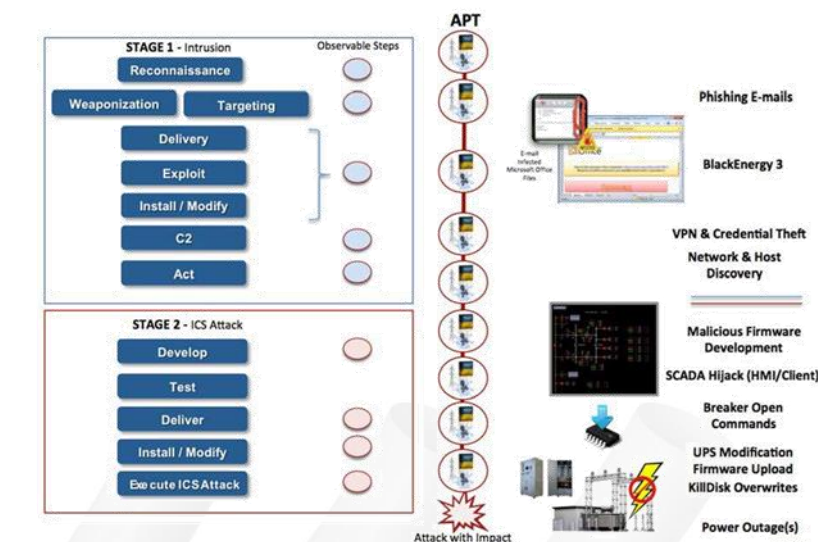


The number of known attack groups increased from 140 in 2018 to 155 in 2019.6

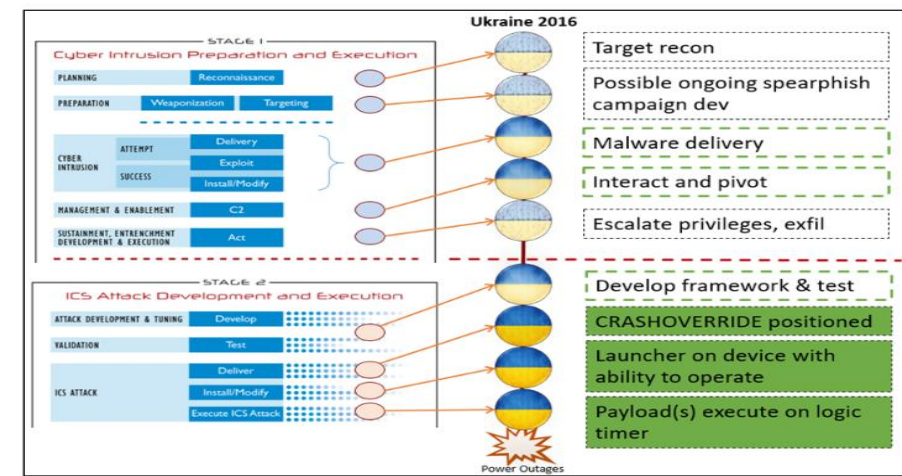
Cyber Kill Chain



Stuxnet

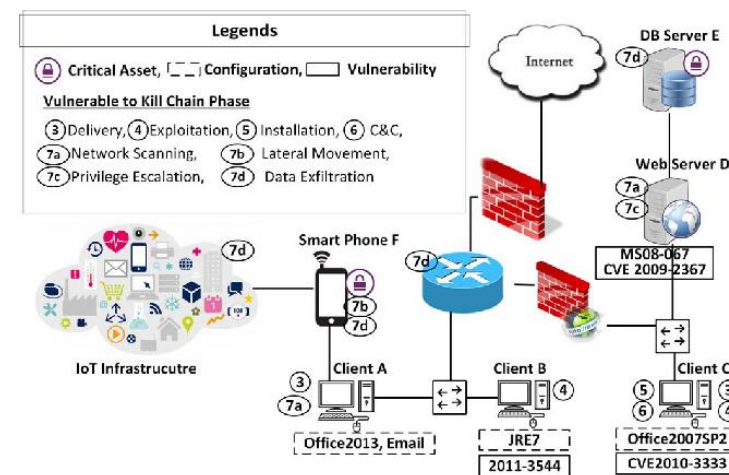


Ukraine 2015

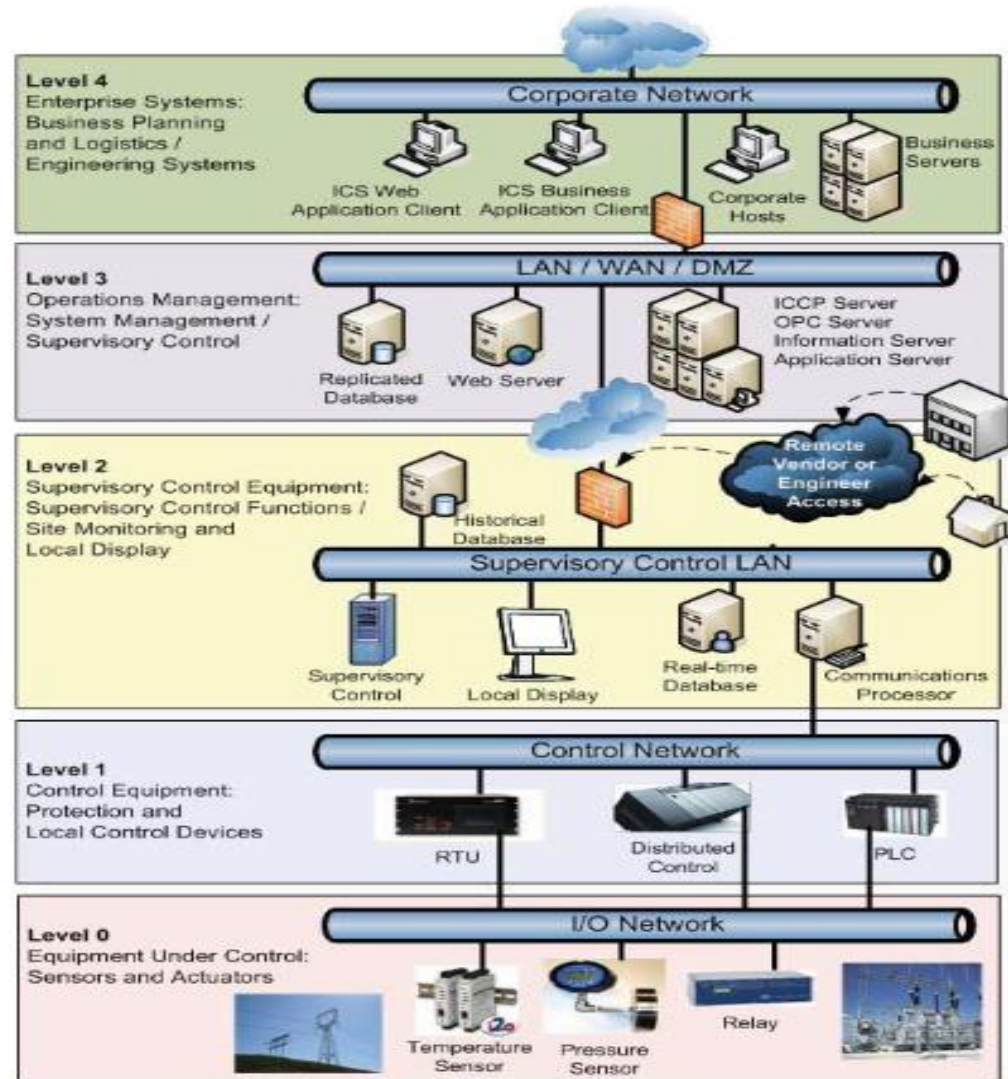


CrashOverride /Industroyer

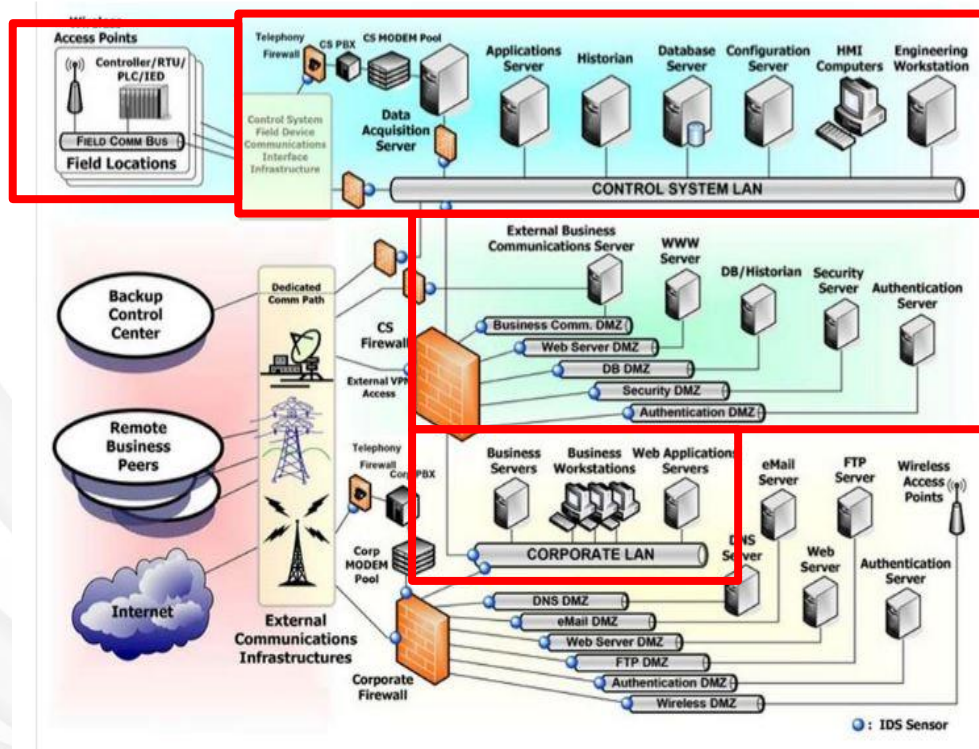
IoT



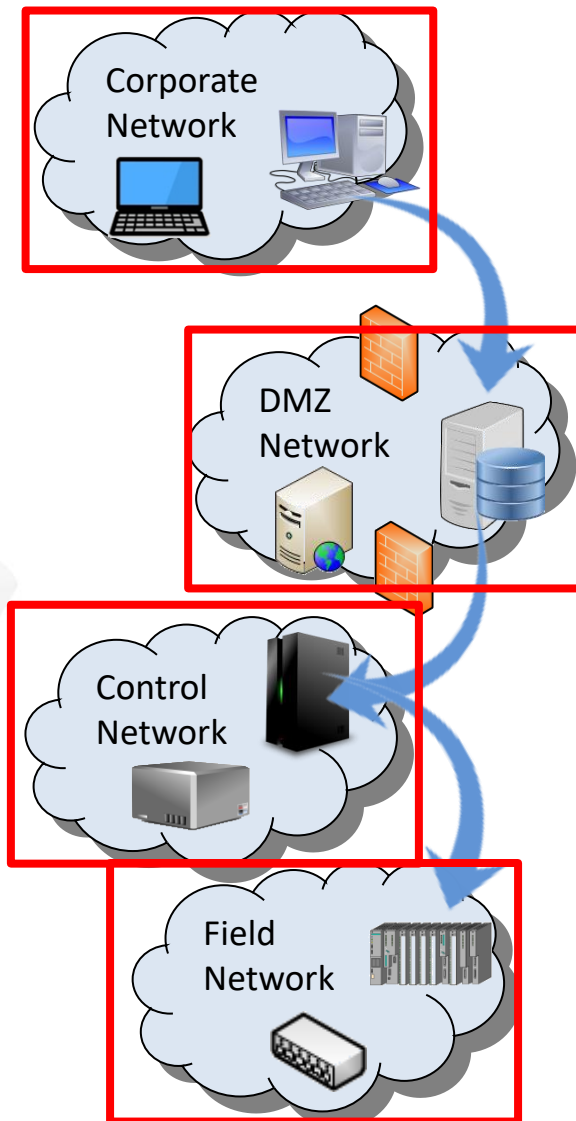
ICS Architecture



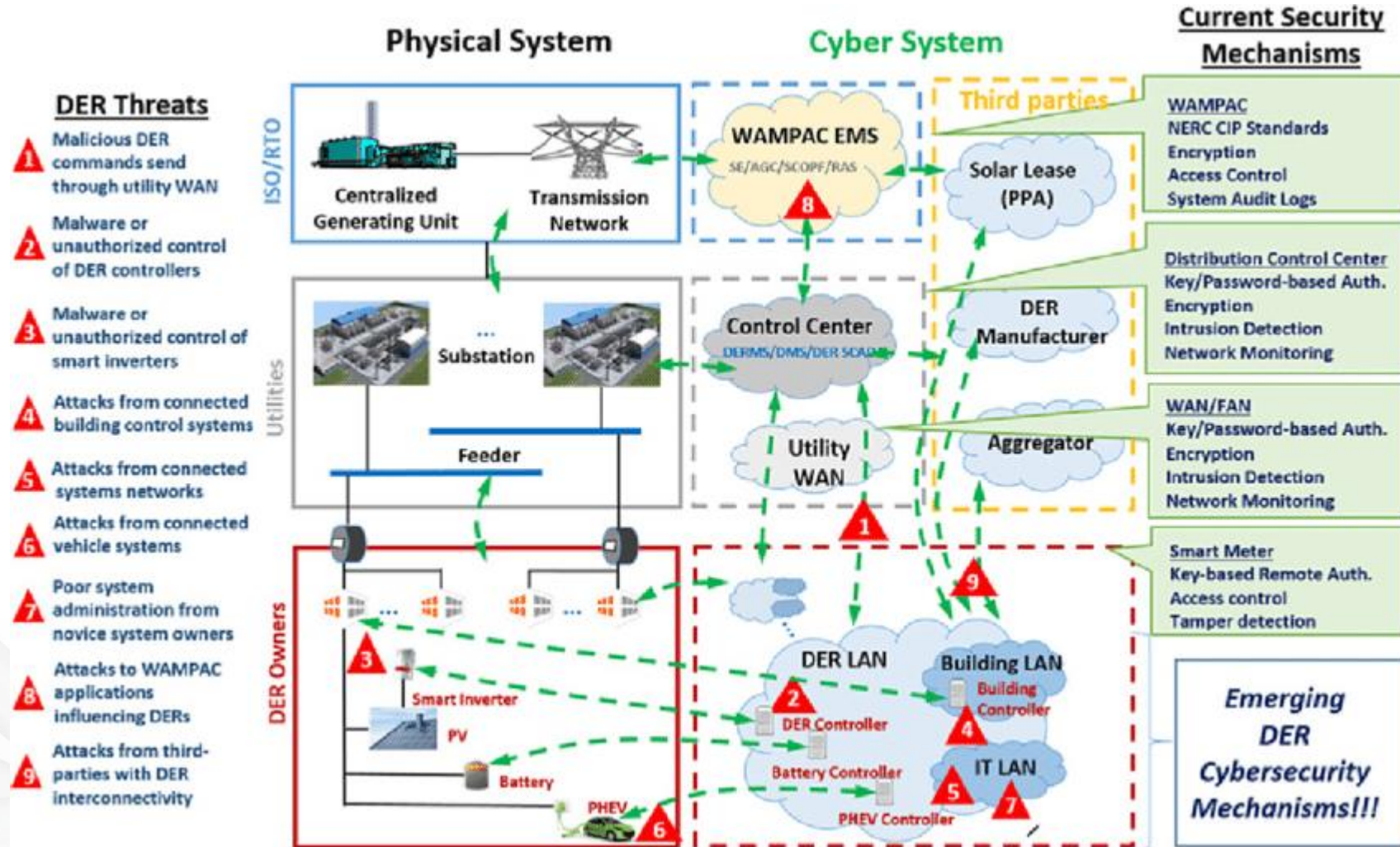
Attack process



NIST 800-82



DER attack vectors



Information Technology (IT) vs. Operational Technology (OT)

Data



Critical
Assets

IT

OT

Confidentiality

Integrity

Availability

Availability

Availability

Integrity

Confidentiality

Confidentiality

The **cyber security strategy** may need to be tailored to the **OT environment** because of the **performance** and **computing constraints**.

This difference will impact the **risk assessment** and the **specific security requirements** that are selected.

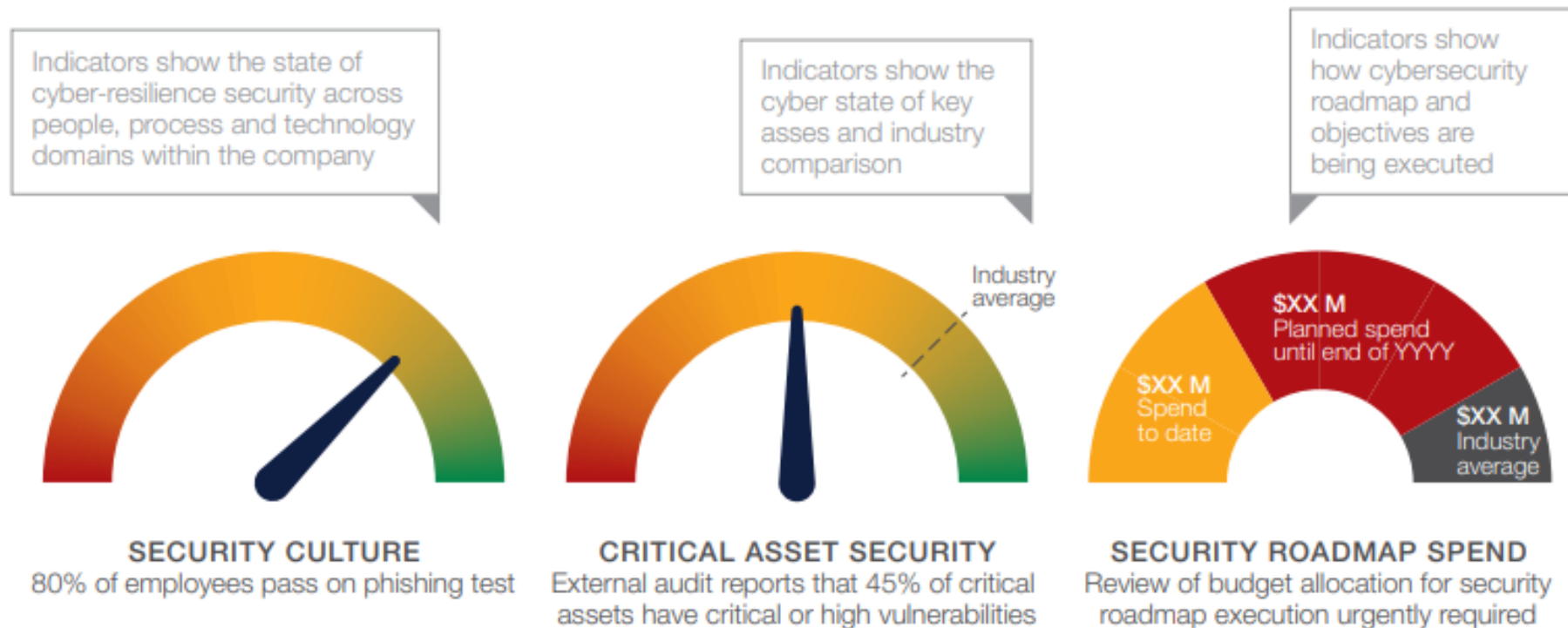
IT vs OT

	Energy Control Systems 	Office IT 
Anti-virus / mobile code	Uncommon / hard to deploy	Common / widely used
Component Lifetime	Up to 20 years	3-5 years
Outsourcing	Rarely used	Common
Application of patches	Use case specific	Regular / scheduled
Real time requirement	Critical due to safety	Delays accepted
Security testing / audit	Rarely (operational networks)	Scheduled and mandated
Physical Security	Very much varying	High
Security Awareness	Increasing	High
Confidentiality (Data)	Low – Medium	High
Integrity (Data)	High	Medium
Availability / Reliability	24 x 365 x ...	Medium, delays accepted
Non-Repudiation	High	Medium

Ref: IEC 62351-10

Indicators of Cyber Resilience

Sample cyber-resilience officer executive dashboard High level state of cyber resilience



[WEF Cyber Resilience in the Electricity Ecosystem Playbook for Boards and Cybersecurity Officers 2020.pdf \(weforum.org\)](#)

Energy cybersecurity

Key actors in the value chain



• Operators

- Energy Operators
- Telco Operators
- IT Service Providers

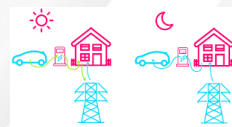


• Suppliers

- OT product Manufacturers
- EV product Manufacturers
- ICT product Manufacturers
- Security Solutions Providers
- Security System Integrators



• Prosumers



• Regulators



Direttiva (UE) 2016/1148 /1

- **Art. 5** criteri per l'identificazione degli **operatori di servizi essenziali**
 - a) un soggetto fornisce un servizio che è essenziale per il **mantenimento di attività sociali e/o economiche fondamentali**
 - b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi
 - c) un incidente avrebbe **effetti negativi rilevanti** sulla fornitura di tale servizio
- **All. II Settori**
 1. **Energia: Energia elettrica, Petrolio, Gas**
 2. Trasporti: aereo, ferroviario, vie d'acqua, su strada
 3. Bancario
 4. Mercati finanziari
 5. Sanitario
 6. Acqua potabile
 7. **Infrastrutture digitali: IXP, DNS, TLD**

Direttiva (UE) 2016/1148 /2

- **Art. 6** Effetti negativi rilevanti – fattori intersettoriali
 - a) il **numero di utenti** che dipendono dal servizio fornito dal soggetto interessato;
 - b) la **dipendenza di altri settori** di cui all'allegato II dal servizio fornito da tale soggetto
 - c) l'impatto che gli incidenti potrebbero avere, in termini di **entità** e di **durata**, sulle attività economiche e sociali o sulla pubblica sicurezza
 - d) la **quota di mercato** di detto soggetto
 - e) la **diffusione geografica** relativamente all'area che potrebbe essere interessata da un incidente
 - f) l'**importanza del soggetto** per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio

Direttiva (UE) 2016/1148 /3

- **Art. 9** Gruppi di intervento per la sicurezza informatica in caso di incidente (**CSIRT**)
 1. Ogni Stato membro designa uno o più CSIRT, che abbia il compito di trattare gli incidenti e i rischi secondo una procedura ben definita. È possibile creare un CSIRT all'interno dell'autorità competente

Direttiva (UE) 2016/1148 /4

CAPO IV

SICUREZZA DELLA RETE E DEI SISTEMI INFORMATIVI DEGLI OPERATORI DI SERVIZI ESSENZIALI

Articolo 14

Obblighi in materia di sicurezza e notifica degli incidenti

Direttiva (UE) 2016/1148 – art. 14 /5

1. Gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino **misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi** posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni. Tenuto conto delle **conoscenze più aggiornate in materia**, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente
2. Gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino misure adeguate per **prevenire e minimizzare l'impatto** di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di **assicurare la continuità** di tali servizi

Direttiva (UE) 2016/1148 – art. 14 /6

3. Gli Stati membri provvedono affinché gli operatori di servizi essenziali **notifichino senza indebito ritardo** all'autorità competente o al **CSIRT** gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati. Le notifiche includono le informazioni che consentono all'autorità competente o al CSIRT di determinare qualsiasi **impatto transfrontaliero** dell'incidente. La notifica non espone la parte che la effettua a una maggiore responsabilità
4. Per determinare la rilevanza dell'impatto di un incidente si tiene conto in particolare dei seguenti parametri: a) **il numero di utenti** interessati dalla perturbazione del servizio essenziale; b) **la durata** dell'incidente; c) **la diffusione geografica** relativamente all'area interessata dall'incidente

Direttiva (UE) 2016/1148 – art. 14 /7

5. Sulla base delle informazioni fornite nella notifica da parte dell'operatore di servizi essenziali, **l'autorità competente o il CSIRT informa l'altro o gli altri Stati membri interessati se l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali in quello Stato membro.** A tal fine l'autorità competente o il CSIRT preserva, conformemente al diritto dell'Unione o alla legislazione nazionale conforme al diritto dell'Unione, la sicurezza e gli interessi commerciali dell'operatore di servizi essenziali, nonché la riservatezza delle informazioni fornite nella sua notifica. **Ove le circostanze lo consentano, l'autorità competente o il CSIRT fornisce all'operatore di servizi essenziali che effettua la notifica di incidente le pertinenti informazioni relative al seguito della notifica stessa, come le informazioni che possano facilitare un trattamento efficace dell'incidente.** Su richiesta dell'autorità competente o del CSIRT, il punto di contatto unico trasmette le notifiche di cui al primo comma ai punti di contatto unici degli altri Stati membri interessati

NIS 2.0 /1



- NIS 2.0 revised Directive proposed on December 2020
- **Essential entities, electricity**
 - Electricity undertakings which carry out the function of ‘supply’
 - Distribution system operators
 - Transmission system operators
 - Producers
 - Nominated electricity market operators
 - Electricity market participants providing aggregation, demand response or energy storage services
- **Essential and important entities (e.g. manufactures)**

NIS 2.0 /2



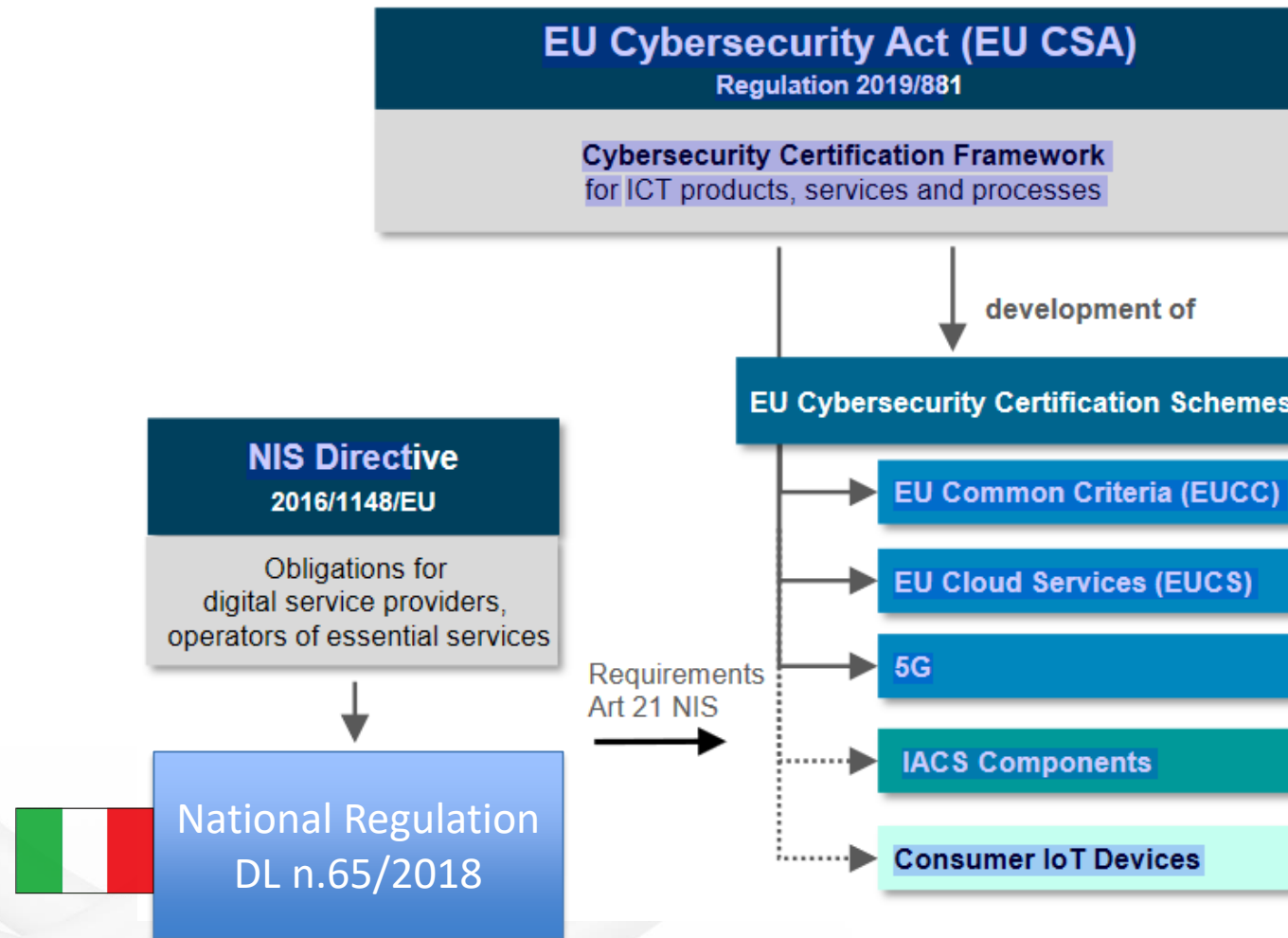
- all **medium-sized** and **large entities** active in the sectors covered by the NIS2 framework would hence have to comply with the security rules put forward in the proposal
- It removes the possibility for Member States to tailor the requirements in certain cases (which had led to much fragmentation with NIS1 implementation)
- It removes the distinction made between OESs and digital DSPs, which currently fall into three categories: online marketplaces, search engines and cloud service providers
- seven key elements that all companies must address or implement as part of the measures they take, including incident response, **supply chain security**, encryption and vulnerability disclosure
- a two-stage approach to incident reporting. Affected companies have **24 hours** from when they first become aware of an incident to submit an initial report, followed by a final report no later than **one month** later

NIS 2.0 /3



- Regarding enforcement, it establishes a **minimum list of administrative sanctions** (up to **€10 million** or 2 % of the entities' total turnover worldwide, whichever is higher)
- improve the level of **joint situational awareness** and the **collective capability to prepare and respond**, by
 - i) taking measures to increase the level of trust between competent authorities
 - ii) by sharing more information
 - iii) setting **rules and procedures in the event of a large-scale incident or crisis**. The proposed new rules improve the way the EU prevents, handles and responds to large-scale cybersecurity incidents and crises by introducing clear responsibilities, appropriate planning and more EU cooperation

Direttiva (UE) 2019/881

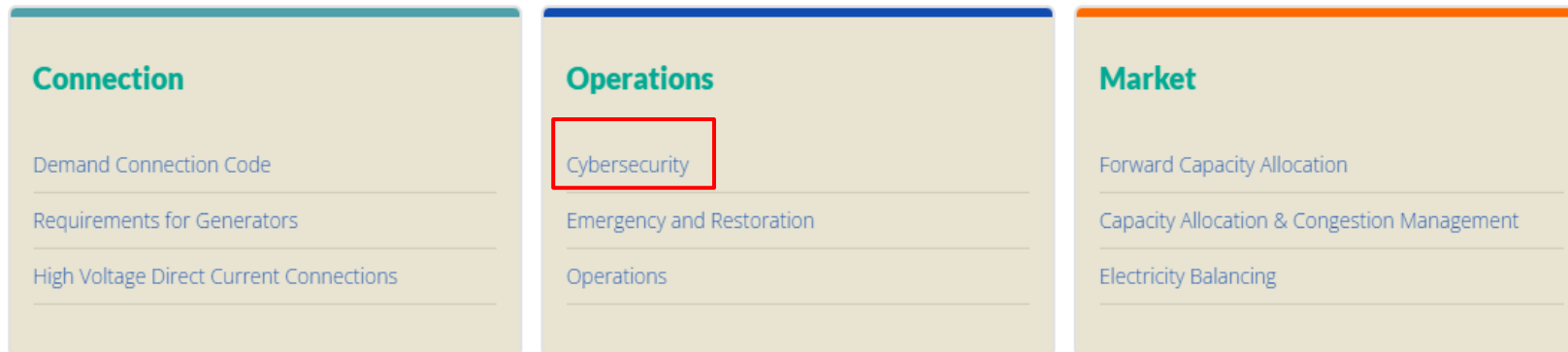


Codice di Rete Europeo /1



- Set of rules drafted by ENTSO-E and in the future EU-DSO with guidance from ACER
- Adopted by the European Commission

The code families



Codice di Rete Europeo /2

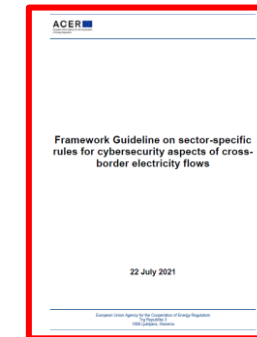
[Cybersecurity \(entsoe.eu\)](https://entsoe.eu)

NC CS drafting status

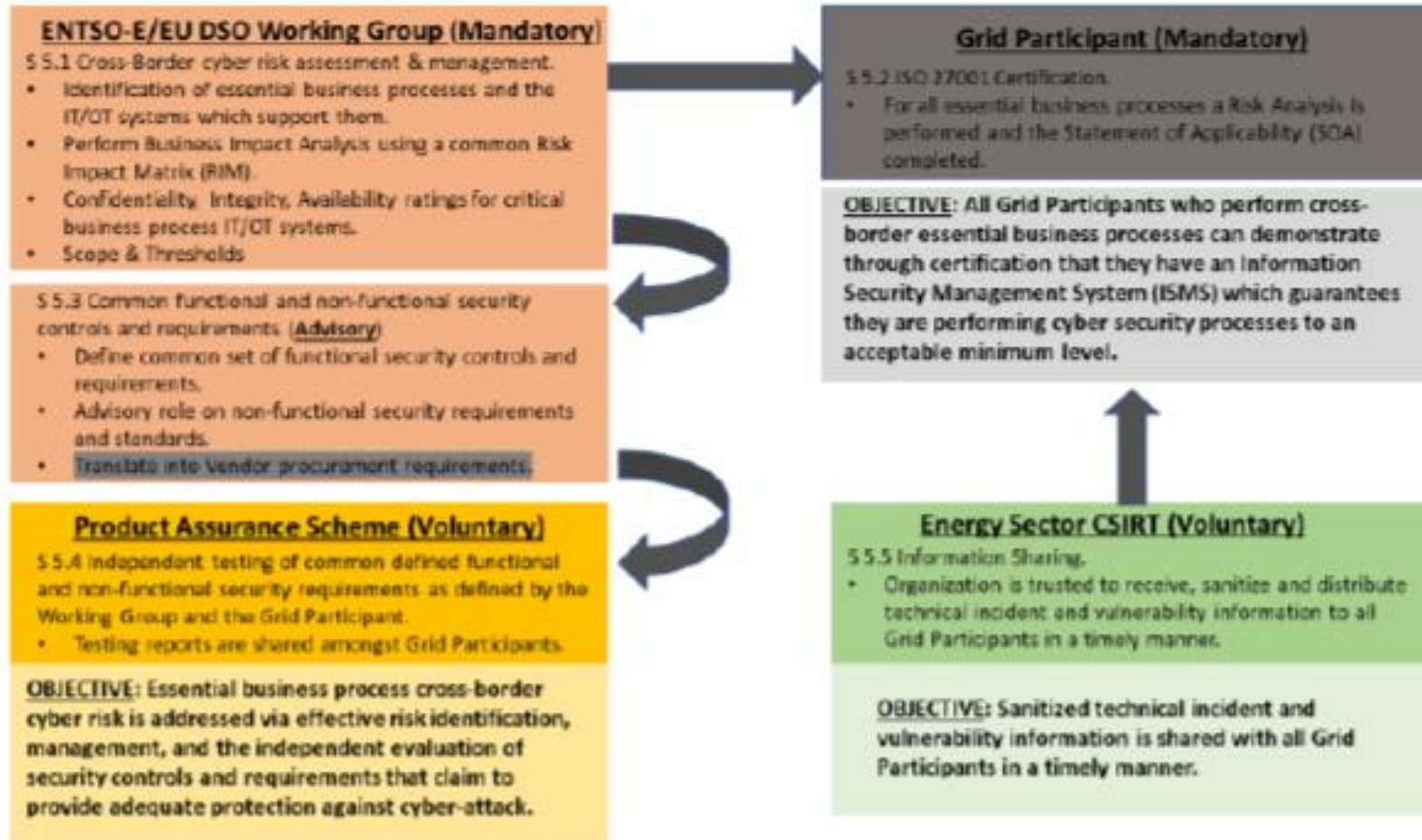
Timeline



- NETWORK CODE ON CYBERSECURITY – INFORMAL DRAFTING TEAM
- Final Report**
- Recommendations for the European Commission on
a Network Code on cybersecurity**
- 19 February 2021**
- Disclaimer:** This document represents the opinion of all the contributors (listed in Annex A). It does not represent the opinion of the European Commission. The European Commission, on any page appearing in the behalf of the European Commission, is responsible for the use that may be made of the information arising from this document.



Codice di Rete Europeo /4



NETWORK CODE ON CYBERSECURITY – INFORMAL DRAFTING TEAM

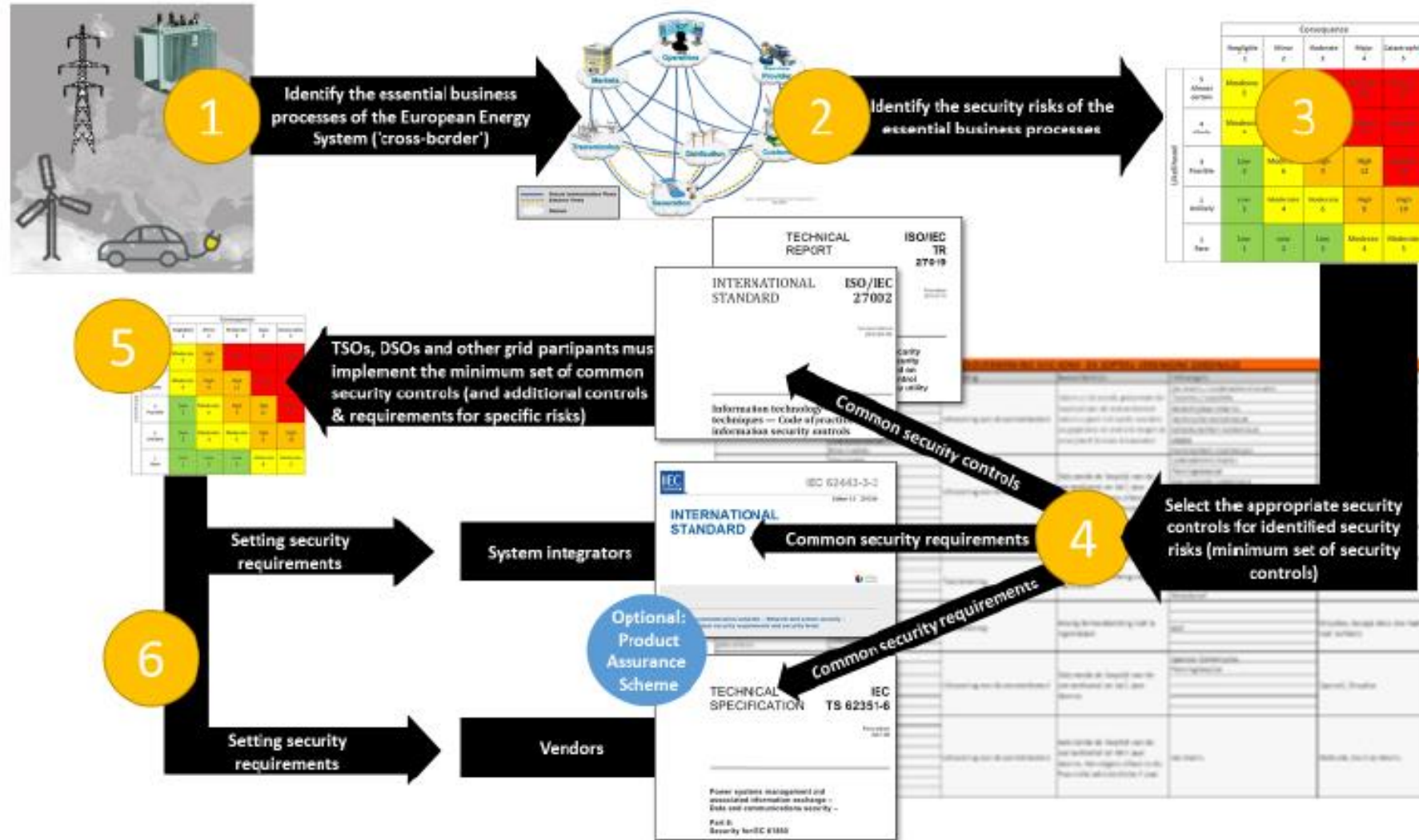
Final Report

Recommendations for the European Commission on
a Network Code on cybersecurity

19 February 2021

Disclaimer: This document represents the opinion of all the contributors listed in Annex A. It does not represent the opinion of the European Commission. Neither the European Commission, nor any person acting on the behalf of the European Commission, is responsible for the use that may be made of the information arising from this document.

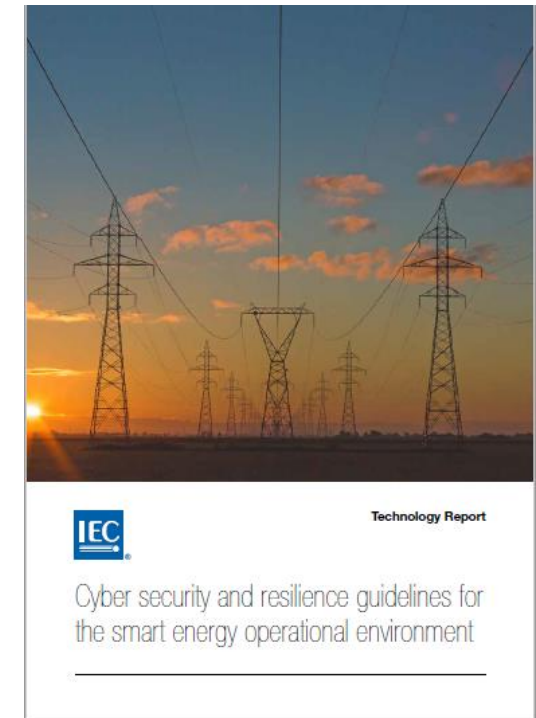
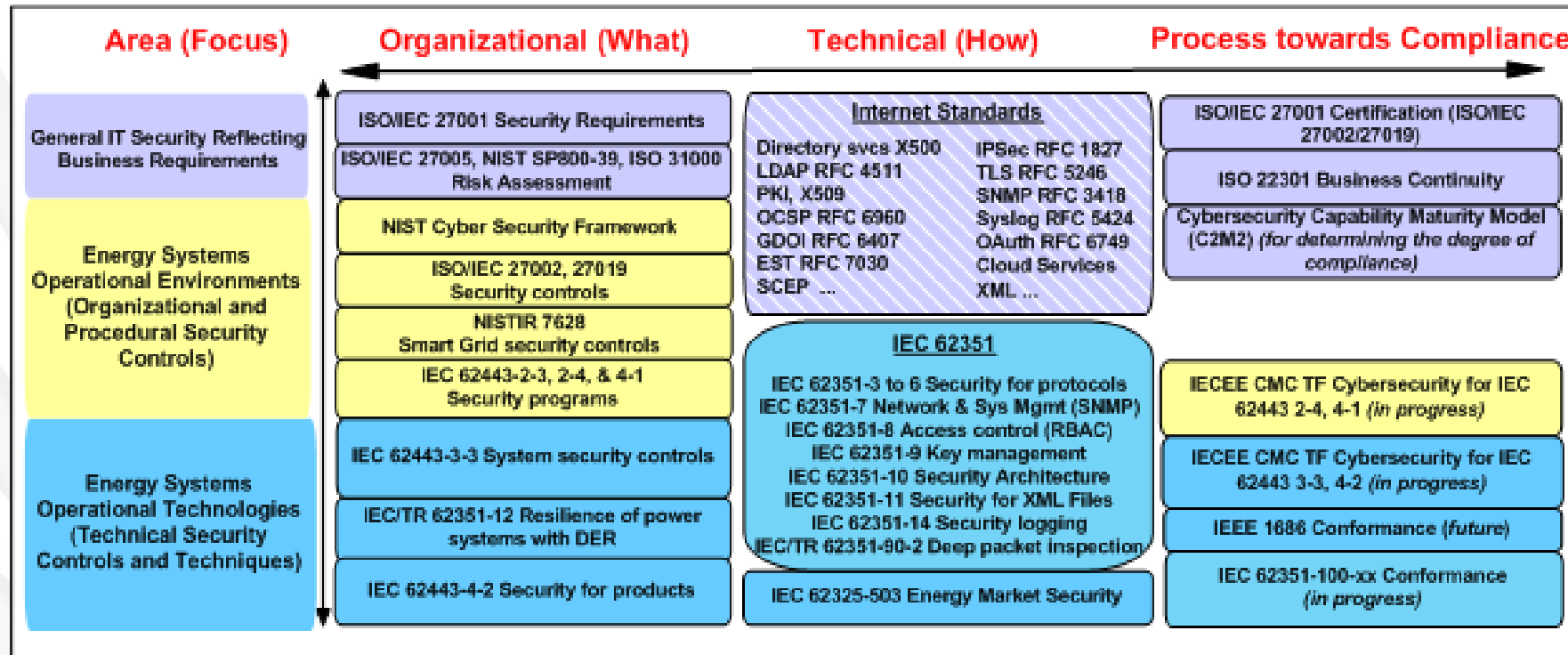
Codice di Rete Europeo /6



Standard internazionali /1

IEC SyC Smart Energy – Cyber Security Task Force

Cyber Security Standards and Guidelines that Apply to Smart Energy Operational Environments



Legislazione italiana /1

- Il **decreto-legge n. 65**, entrato in vigore il 24 Giugno 2018, costituisce l'attuazione italiana della Direttiva europea NIS (EU 2016/1148)
- Un primo fondamentale provvedimento stabilito dal decreto n.65 è relativo all'identificazione degli **operatori** classificati come fornitori **di servizi essenziali**, quali quelli energetici, soggetti agli **obblighi** in materia di sicurezza e notifica degli incidenti indicati dall'**Art. 14**, e alle relative **sanzioni amministrative** in caso di inadempienza di cui all' **Art. 21**
- L' Art.21 stabilisce che gli operatori dei servizi essenziali che risultano inadempienti agli obblighi stabiliti dalla legge nazionale sono soggetti a **sanzioni pecuniarie che, a seconda dei casi, variano da € 12,000 a € 150,000**

Legislazione italiana /2



- Il **decreto-legge n. 105**, approvato il 21 Settembre 2019 dal Consiglio dei Ministri, modificato e convertito dal **decreto per la legge di conversione n.133** entrato in vigore il 21 Novembre 2019, introduce **disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica**
- Il perimetro riguarda tutte le ***infrastrutture critiche, private e pubbliche aventi una sede nel territorio nazionale***, che assicurano un ***servizio essenziale per le attività civili, sociali o economiche fondamentali per la nazione***, e che per la fornitura di tale servizio si avvalgono di *reti, sistemi informativi e servizi informatici* dal cui malfunzionamento o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale
- L' **Art.1** stabilisce che entro quattro mesi dall'entrata in vigore della legge di conversione è richiesta l'***individuazione delle amministrazioni, degli enti e degli operatori*** inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto degli obblighi stabiliti dalla legge

Legislazione italiana /3



- L' **Art.1** stabilisce che **entro dieci mesi** dall'entrata in vigore della legge di conversione il Ministero dello Sviluppo Economico definisce **le procedure** che i soggetti privati del settore energia devono seguire **per la notifica degli incidenti cyber al gruppo di intervento per la sicurezza informatica (CSIRT)** già prevista dal D.L. n.65
- Vengono inoltre stabilite le **misure organizzative, di gestione del rischio e di mitigazione e gestione degli incidenti** che garantiscono elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici **tenendo conto degli standard definiti a livello internazionale ed europeo**

Legislazione italiana /4



- *I soggetti individuati che intendono approvvigionarsi di beni, sistemi e servizi ICT devono darne comunicazione al CVCN, unitamente alla valutazione del rischio associato all'oggetto della fornitura in relazione all'ambito di impiego*
- *Entro al massimo sessanta giorni dalla comunicazione, il CVCN può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software da effettuare in collaborazione con i soggetti individuati secondo un approccio gradualmente crescente nelle verifiche di sicurezza*
- *Tali condizioni e test di hardware e software **condizionano i relativi bandi di gara e contratti** al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN*
- *L'onere dell'effettuazione delle attività di test risulta a carico dei soggetti inclusi nel perimetro di sicurezza nazionale*

Legislazione italiana /5



- Il CVCN assume il compito di *elaborare le misure di sicurezza che riguardano l'affidamento di forniture di beni, sistemi e servizi ICT, definisce le metodologie di verifica e di test, effettua le verifiche avvalendosi di laboratori accreditati dallo stesso CVCN, se necessario elabora ed adotta nuovi schemi di certificazione cibernetica tenendo conto degli standard definiti a livello internazionale ed europeo*
- Il mancato adempimento da parte dei soggetti inclusi nel perimetro degli obblighi previsti dalla legge comporta **sanzioni amministrative e pecuniarie fino a 1.8 Meuro**

Legislazione italiana /7

- DPCM n. 131 30/07/2020
 - **Regolamento in materia di perimetro di sicurezza nazionale cibernetica**
 - Criteri e modalità per l'individuazione dei soggetti inclusi nel perimetro
 - Criteri che i soggetti inclusi devono adottare per la predisposizione dell'elenco delle reti, dei sistemi e dei servizi, loro architettura e componentistica
- DPR n. 54 5/02/2021
 - **Regolamento CVCN**
 - Procedure, modalità e termini di funzionamento del CVCN
 - Criteri tecnici per l'individuazione delle categorie e dell'elenco dei beni, dei sistemi e dei servizi a cui si applica la procedura di valutazione
 - Procedure, modalità e termini con cui le autorità competenti effettuano le verifiche e le ispezioni per l'accertamento del rispetto degli obblighi stabiliti dal DL 105
- DPCM n.81 14/04/2021
 - **Regolamento in materia di notifiche degli incidenti** aventi impatto su reti, sistemi informativi e servizi informatici

Legislazione italiana /8

- DPCM n.82 14/06/2021
 - Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza
 - Istituzione dell'**Agenzia per la Cybersicurezza Nazionale (ACN)**
- DPCM
 - **Individuazione delle categorie di beni, sistemi e servizi ICT** destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica

Norme CEI

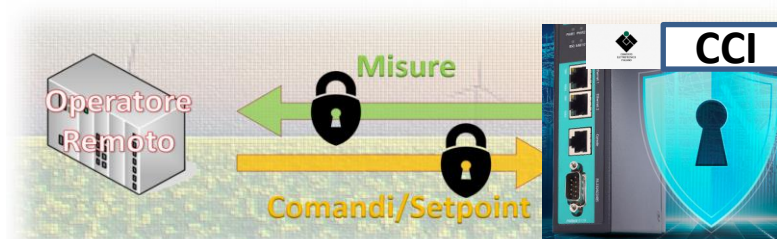
The code families

Connection	Operations	Market
Demand Connection Code	Cybersecurity	Forward Capacity Allocation
Requirements for Generators	Emergency and Restoration	Capacity Allocation & Congestion Management
High Voltage Direct Current Connections	Operations	Electricity Balancing

- CEI 0-16 «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
 - Allegato T – Modello dati e **cybersecurity**
 - Recepiscono lo standard IEC 61850 e IEC 62351
- CEI 0-21 «Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti BT delle imprese distributrici di energia elettrica»
 - PAS Allegato X – Controllore Infrastruttura di Ricarica VE
 - incluso nel il Progetto di Norma CEI 0-21 in Inchiesta Pubblica C. 1267, scadenza **22 giugno 2022**



Cybersecurity utenti attivi MT: CEI 0-16



Cybersecurity utenti attivi BT: CEI 0-21



T.3.3.4 Sicurezza informatica del CCI

- T.3.3.4.1 Sicurezza delle comunicazioni IEC 61850/MMS
- T.3.3.4.2 Sicurezza delle comunicazioni IEC 61850/GOOSE [INFORMATIVO]
- T.3.3.4.3 Gestione dei ruoli nelle comunicazioni IEC 61850/MMS
- T.3.3.4.4 Sicurezza dei servizi logici di comunicazione con attori abilitati alla connessione remota diversi dal DSO
- T.3.3.4.5 Sincronizzazione temporale
- T.3.3.4.6 Gestione dei log
- T.3.3.4.7 Gestione degli asset
- T.3.3.4.8 Aggiornamento firmware
- T.3.3.4.9 Gestione delle chiavi e dei certificati
- T.3.3.4.10 Segregazione del traffico del CCI
- T.3.3.4.11 Sicurezza delle comunicazioni locali

T.3.3.4.1 Sicurezza delle comunicazioni IEC 61850/MMS

- n Conformità alla **IEC 62351-4**
 - n Sicurezza del livello applicativo
 - n Profilo End-To-End (E2E)
 - n Mutua autenticazione delle parti in comunicazione
 - n Integrità delle comunicazioni
 - n Confidenzialità (disattivabile)
- n Conformità alla **IEC 62351-3**
 - n Sicurezza del livello trasporto
- n Integrità e confidenzialità sono garantite da algoritmi crittografici
 - n Organizzati in suite che raggruppano algoritmi per generazione e scambio chiavi, cifratura e hash crittografici
 - n Algoritmi chiavi asimmetriche: RSA, ECDSA
 - n Hashing: SHA256
 - n Calcolo ICV: hmac
 - n Algoritmi chiavi simmetriche: AES128-CBC, AES256-CBC, AES128-GCM, AES256-GCM
- n Autenticazione basata su certificati elettronici ITU-T X-509



T.3.3.4.7 Gestione degli asset

- CCI identificato dal nodo logico LPHD
 - Data Object PhyNam
 - informazioni relative al costruttore, al numero di serie del dispositivo, alla versione del software, alla denominazione dell'impianto di appartenenza, l'identificativo del punto di connessione, ed eventualmente alla sua localizzazione geografica
 - Mappatura di PhyNam su MIB SNMP
 - Invio tramite SNMPv3, profilo TSM basato su TLS
- Riferimento alla IEC 62351-7



T.3.3.4.9 Gestione delle chiavi e dei certificati

- Conformità alla **IEC 61351-9, standard ITU-T X.509**
 - T.3.3.4.9.1 Public Key Infrastructure
 - T.3.3.4.9.2 Privilege Management Infrastructure
 - T.3.3.4.9.3 Procedure della PKI
 - T.3.3.4.9.4. Registrazione del dispositivo
 - T.3.3.4.9.5 Configurazione del dispositivo
 - T.3.3.4.9.6 Arruolamento (enrollment)
 - Protocolli IETF SCEP, EST
 - T.3.3.4.9.7 Rinnovo di un Certificato
 - T.3.3.4.9.8 Revoca di un Certificato
 - T.3.3.4.9.9 Controllo dello stato di validità del certificato



O.15.5 Conformità dei profili di sicurezza

- Certificazione di conformità alla IEC TS 62351-100-3
- In futuro certificazione di conformità alla IEC TS 62351-100-4



**Conformance
Testing IEC 62351**

O.15.5 Conformità del CCI

- Certificazione di conformità allo standard CEI EN 62443-4-1 ML3
 - sicurezza del processo di sviluppo del CCI
- Certificazione di conformità alla CEI EN 62443-4-2 SL = (2,2,2,1,1,1,3)
 - identificazione e autenticazione (FR1)
 - utilizzo (FR2)
 - integrità del sistema (FR3)
 - riservatezza dei dati (FR4)
 - flusso dati (FR5)
 - risposta tempestiva agli eventi (FR6)
 - disponibilità delle risorse (FR7)



O.15.14 Prove relative alla Cybersecurity Hardware

- Per il componente crittografico HSM del CCI è richiesta la certificazione FIPS 140-2 L3
 - grado di resistenza del componente alla manomissione fisica



Riferimenti /1

1. NIS Directive EU 2016/1148 <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>
2. CEN-CENELEC-ETSI Smart Energy Grid – Coordination Group, Cyber Security & Privacy, Dec 2016, <https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/smart-grids-and-meters/smart-grids/>
3. the Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector from Energy Expert Cyber Security Platform (2017) https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
4. the European Commission Recommendation C(2019)2400 on cybersecurity in the energy sector https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf
5. the Cybersecurity Act Regulation (EU 2019/881) <https://eur-lex.europa.eu/eli/reg/2019/881/oj>
6. Clean Energy for all Europeans Package, European Union 2019
7. ENISA CYBERSECURITY CERTIFICATION (2020) Cybersecurity Certification: EUCC Candidate Scheme — ENISA (europa.eu)
8. Evaluating the prudence of cybersecurity investments: Guidelines for Energy Regulators, National Association of Regulatory Utility Commissioners (NARUC), May 2020

Riferimenti /2

9. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, December 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0823&from=EN> Cybersecurity Act Regulation (EU 2019/881) <https://eur-lex.europa.eu/eli/reg/2019/881/oj>
10. ENTSO-E / EU DSO, «Recommendations for the European Commission on a Network Code on Cybersecurity», Final Report, 19 February 2021
11. ACER, Framework Guideline on sector-specific rules for cybersecurity aspects of crossborder electricity flows, July 2021, https://documents.acer.europa.eu/Official_documents/Acts_of_the_Agency/Framework_Guidelines/Framework%20Guidelines/Framework%20Guideline%20on%20Sector-Specific%20Rules%20for%20Cybersecurity%20Aspects%20of%20Cross-Border%20Electricity%20Flows_210722.pdf
12. NIST Cybersecurity Framework Version 1.1, Aprile 2018, <https://www.nist.gov/cyberframework/framework>
13. IEC Technology Report, “Cyber security and resilience guidelines for the smart energy operational environment”, 2019

- # in questo numero
- Proprietà e
ed Editoria:** G. Assolombardo, Informatica,
Automazione, Informatica
e Telecomunicazioni - AETI
- Direttore Responsabile:** Roberto Galassi - AETI
- Comitato di Redazione:**
- A. Arzuffi - EDN
 - V. Balamore - ADPPT
 - M. Benini - RSE
 - S.M. Carlini - TESI/PA
 - L. Cavallotti - L'Espresso
 - A. Cera - IREX
 - B. Ciola - CIR
 - M. Corvino - ENEL Italia
 - A. Perocco - Hiachi Energy
 - R. Lanza - ENES
 - M. Longo - Politecnico di Milano
 - F. Luzzi - AREVA
 - M. Mengoni - Euronews
 - T. Neri - ST Televisi Italia
 - N. Reale - OZIE
 - G. Roggeri - Gruppo IRIEN
 - E. Rossetti - Edizioni
 - F. Zambelli - ANE
- Redazione:** AETI
Aria Line Fortuna
elettronica@et.it
- Progetto Grafico e Impaginazione:** Antonella Dotti
- Direzione Amministrativa:** AETI Ufficio Generale
Via Mazzini, 32
20134 Milano
Tel. 02/7539900-7
Telex 02/ 555595303
- Abbonamenti/Pubblicità:** Tel. 02/7539900-7
Fax 02/555595303
E-mail abbonamenti@et.it
- Sito internet:** <http://www.et.it>
- Stampa:** Artigrafiche Mulino SNC
Pubblicazione: Via Garibaldi, 40
Distribuzione: Fininvestimenti di Poste Emmevi SRL
- NUMERO 12 - LUGLIO/AUGUSTO 2002
-
- ## articoli
- La Cyber Security nei sistemi elettrici
G. Piccini, R. Dellera, C. Zardetto, F. Veronesse 3
 - Implementazione della cybersecurity per la scambio dati con utenti attivi MT
G. Dondosio, R. Terragga, M. G. Todeschini, G. Bianco, M. Modugno 11
 - La cybersecurity nelle infrastrutture di ricarica di veicoli elettrici
G. Dondosio, R. Terragga, M. G. Todeschini, G. Marchegiani 21
 - Tema: evoluzione della strategia di Cyber Security per i sistemi industriali
I. Monetti, L. Balzano 33
 - La Cybersecurity delle infrastrutture elettriche
E. M. Tinagli, M. Besimo, M. Genovesio, U. Cattaneo, G. Wobben, E. Orsanges, M. Vecchio 41
 - IEC 62443: le standard per la cybersecurity dei sistemi di controllo industriali
M. Cozza Magni, U. Cattaneo, R. Mosiconi, F. Russo 55
 - La formazione sulla sicurezza informatica per diminuire il rischio cyber
A. Catalano, E. Roggeri 63
- tutti gli indirizzi sono quelli indicati.
- Se non è possibile inviare la rivista per posta ordinaria, si prega di spedirla all'indirizzo di redazione o al mittente.
- Registrazione Tribunale di Milano del 10 luglio 1974, numero 8242, n. 2687 - 10 dicembre 1971. Poste Italiane SpA. Spedizione in abbinamento postale - DL 350/2003 art. 1, n. 27-D - ISSN 1120-4009, n. 40, art. 1 comma 1, 1204/Milano.
-
- Associato all'Unione Stampa Periodica Italiana.
- L'Energia Elettrica 2 gennaio/gennaio 2002



WE MOVE
Research
Search