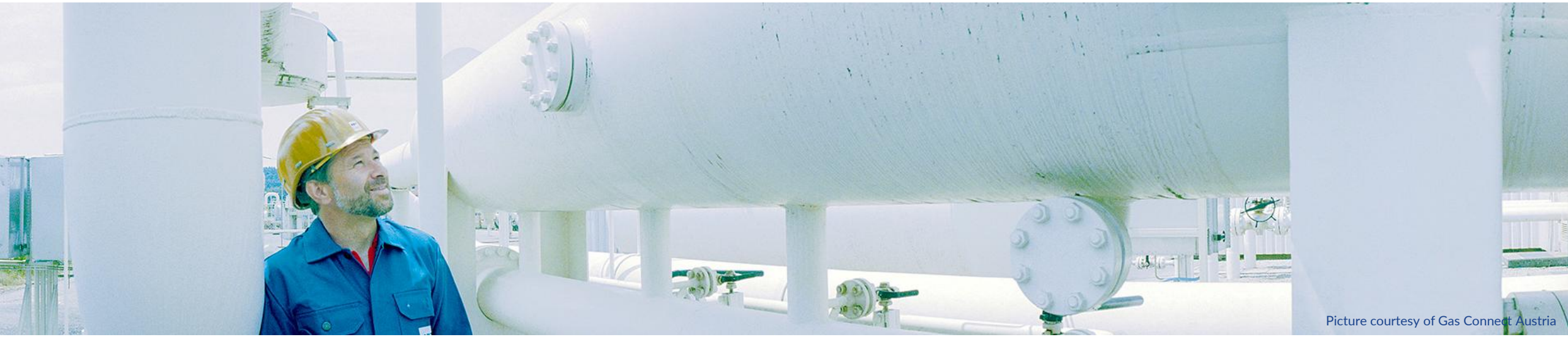
30th October 2024



Picture courtesy of Gas Connect Austria

4th Edition: Joint ENTSOG, EASEE-Gas, GIE Workshop

DAY TWO: Cybersecurity

30th October 2024

ENTSOG offices, Brussels

Hybrid

1. Welcome

Andrea Chittaro

Chair of the ENTSOG/GIE Joint Task Force on Cybersecurity

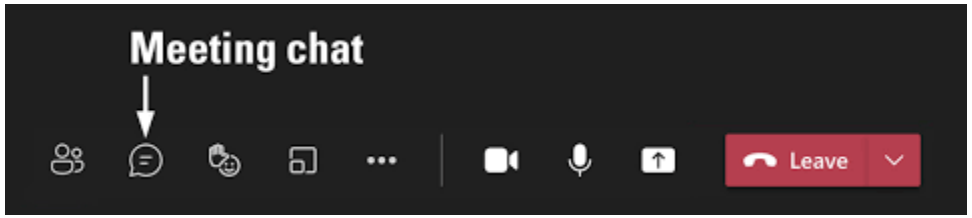
2. Agenda

Douglas Walker Hill
Interoperability & Data Exchange
ENTSOG

Cybersecurity session 09:00-14:00

DAY 2. 30 October 2024 Cybersecurity Topics	Presenter & Affiliation
Introduction and welcome	Andrea Chittaro, Snam (Chair of the ENTSOG GIE Task force on Cybersecurity)
Agenda	Douglas Walker Hill, ENTSOG
Threats: Cybersecurity landscape threat assessment	Eleni Philippou, ENISA
Legislation: NIS 2.0 updates	Konstantinos Moulinos, ENISA
Threats: Evolution of Cybersecurity attacks - A TSO perspective	Lucrezia Tunesi, Snam
ICS frontiers: Purdue Model for large grids, a point of view and future challenges	Fabrizio Zucca, Snam
BREAK	
International CS: Physical asset security and the connection to cybersecurity | EDA	Brig Gen. Ioannis Chatzialexandris, EDA
International CS: ENTSOG ReCo Security of Supply for the gas sector	Anton Kolisnyk, ENTSOG
International CS: The European Cybersecurity Scheme on Common Criteria (EUCC)	Philippe Blot, ENISA
International CS: ENTSOG GIE Joint cybersecurity task force update	Douglas Walker Hill (ENTSOG), Andrea Chittaro (Snam)
International CS: Cyber Europe Findings |ENISA	Dr Alexandros Zacharis, ENISA
LUNCH	
Awareness: Introduction to the ENISA awareness package | ENISA	Dr Alexandros Zacharis, ENISA
Awareness: Desktop exercises with ENISA | ENISA	Dr Alexandros Zacharis, ENISA
QA, Thank you and goodbye	Douglas Walker Hill, ENTSOG

Questions



- *Online please ask your questions via the **Teams chat***
- *Physical attendance please ask questions at the end of the presentation*

Slides removed

3. ENISA Cybersecurity landscape threat assessment

Eleni Philippou

Information security expert, EU
Agency for Cybersecurity - ENISA

4. Legislation: NIS 2.0 updates

Konstantinos Moulinos

Information security expert, EU Agency for Cybersecurity - ENISA

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

IMPLEMENTING THE NIS2 DIRECTIVE

BUILDING UP CYBER RESILIENCE IN THE EU'S CRITICAL SECTORS

ENISA, the EU Agency for Cybersecurity

NIS DIRECTIVE

Goal is to achieve a high common level of cybersecurity across the EU

1. National capabilities

- National authority
- National Strategy
- National CSIRT
- **National Crisis management framework**

2. EU collaboration

- NIS Cooperation group
- EU CSIRT network
- **EU Cyclone**

3. Supervision of critical sectors

- **Management responsibility**
- Security measures
- Incident reporting

New mechanisms in NIS2:

- National cyber crisis management fwks
- EU Cyber crisis management (Cyclone)
- National vulnerability disclosure policies
- **EU Vulnerability database**
- **EU Digital infrastructure registry**
- WHOIS requirements
- **Cybersecurity state of the union report**

NIS2 emphasizes

- Much broader view on sectors
  - many smaller companies
- National/EU cyber crisis mgmt
- Management responsibility
- Supply chain security for entities
- Supply chain risks for the union
- Cloud, digital infra and trust service providers

NIS DIRECTIVE FOCUS

NIS Directive is about resilience (CIIP!)

- Focus on
    - Outages, large attacks, major incidents (DDoS attacks, ransomware, etc)
    - Redundancy, failover, backups, scaling, capacity
    - Handle crisis situations, recovery, business continuity
    - Detection and response
- “Keep the (most critical) ICT systems and networks and the country working”
- NIS2 was proposed and adopted in parallel with the CER directive – for physical attacks on critical infrastructure

Resilience/CIIP/CIP is a “partnership” between national authorities and critical infrastructure owners

- “The stick is out there (ransomware), we will focus on the carrot”
- “With ISO27K1 you should be OK”

NIS2 = EU DIRECTIVE ++

It is a Directive!!!

- Each MS decides on sectors in scope, and entities in scope (the minimum is set by NIS2)
- Needs national transposition, precise national/sectorial requirements come from the country
- Entities in scope need to be registered

But with some EU harmonization built-in via

- Strategic cooperation in the NIS Cooperation group, often resulting in technical guidelines for MS
  - Strategic cooperation: 5G toolbox, requested by Commission, developed by (and for) EU Member States
  - Technical guideline: National Coordinated Vulnerability Disclosure (CVD) policies (“working with ethical hackers”)
- Operational and technical collaboration in Cyclone and CSIRT network
- EU Harmonization for the NIS2 Digital infrastructures sector, which are cross-border entities
  - EU implementing rules containing security measures and NIS2 incident reporting
    - Drafted and published by the Commission (in the official journal of EU laws)
    - Consultation over summer, adoption in October 2024
  - One-stop shop principle, main establishment, mutual assistance between authorities
  - EU Registry for digital infrastructure entities (EUDIR)
- Union coordinated supply chain risk assessments
  - Following the EU 5G toolbox process
  - Nevers process, and more are coming

SUPERVISION UNDER THE NIS2

NIS2 Supervision

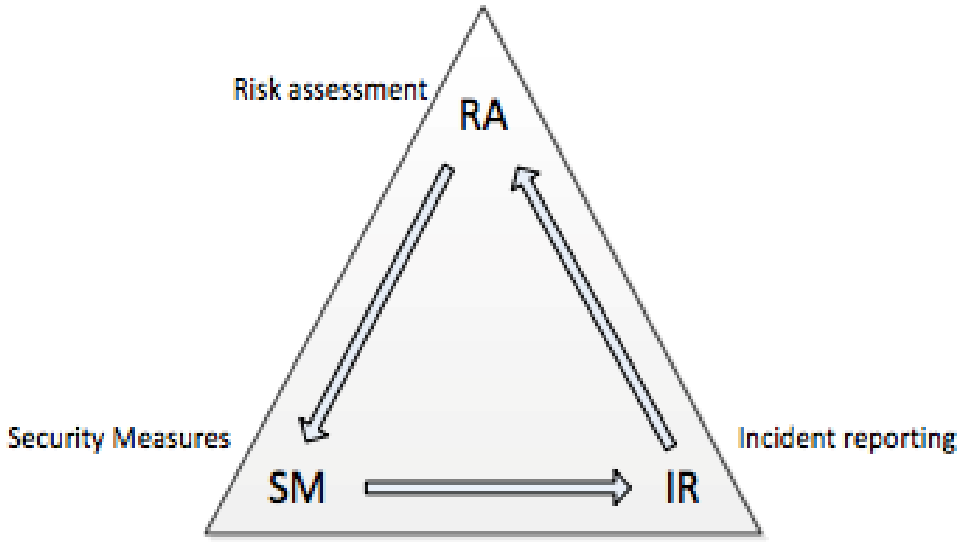
- Risk-based security measures, all-hazard approach, anything impacting the ICT
- Incident reporting
- Management responsibility (get cybersecurity training, sign off on measures)

NIS2 brings many new sectors in scope

- Twice as many sectors in scope of NIS2, compared to NIS1
- Many more companies in scope with in a sector (size caps)

NIS2 distinguishes between essential and important

- Essential – ex-ante supervision
- Important – ex-post supervision



This triangle should be implemented by the operators/providers
It is supervised by the national authorities in the EU.

Note: There is the legal scope – authority imposes requirements. Within the legal scope an authority has to focus its supervision, usually a combination of ex-ante and ex-post supervision. Goal is to increase resilience of the sector – and protect the infrastructure of the country.

NIS2 CHALLENGES

WHAT IS NEW IN NIS2?

More sectors

More entities within each sector, including smaller entities

New methods of identification, registration now necessary

New incident notification deadlines

Extra (cyber) security requirements

Several new tasks for ENISA and the EU Member States

ADDITIONAL CHALLENGES*

Address the interplay between NIS and others EU legislations (CER, DORA, EIDAS, CSA, CRA, Cyber solidarity Act, GDPR, Aviation Regulation, Electricity Regulation and other sectorial legislation).

Sufficient resources for ENISA, European Commission and MS to support the additional tasks of the CG.

Outreach and collaboration with private stakeholders (companies, industries, education, etc) and law enforcement.

More frequent and concrete interactions with CSIRTs network, CyCLONe & CERG.

**as presented by the BE Presidency to the HWPCI*

WHAT IS COMING UP NEXT

NIS2 implementing rules for digital infrastructure

- Entry into force by 7 November 2024

ENISA technical guidance on NIS2 reporting (one template) and measures (mapped to standards)

- Publication by October 2024

Transposition by the 27 EU Member States

- Deadline October 2024

In 2025 the real work starts

- Registration of entities under the NIS2 – 1000s or 10.000s of companies (plenty of scope issues to be solved)
- Incident reporting – significant impact, but also voluntary reporting, e.g. about near-misses (create culture, trust!)
- Supervision of security measures – get to know each other (partner with big ones, guide smaller ones, help the sector)

Q&A

INPUT, IDEAS, SUGGESTIONS VERY WELCOME – ALSO VIA EMAIL OR LINKEDIN

Connect on Linkedin

ENISA-NIS-Directive@enisa.europa.eu

THANK YOU

European Union Agency for Cybersecurity

Agamemnonos 14 Str., 15231 Chalandri Attiki,

Greece

+30 28 14 40 9711

info@enisa.europa.eu

http://www.enisa.europa.eu

5. Evolution of Cybersecurity attacks - A TSO perspective

Lucrezia Tunesi
Cyber security expert
Snam

Evolution of Cybersecurity Attacks

A TSO perspective

Snam Spa

Lucrezia Tunesi

October 30th, 2024

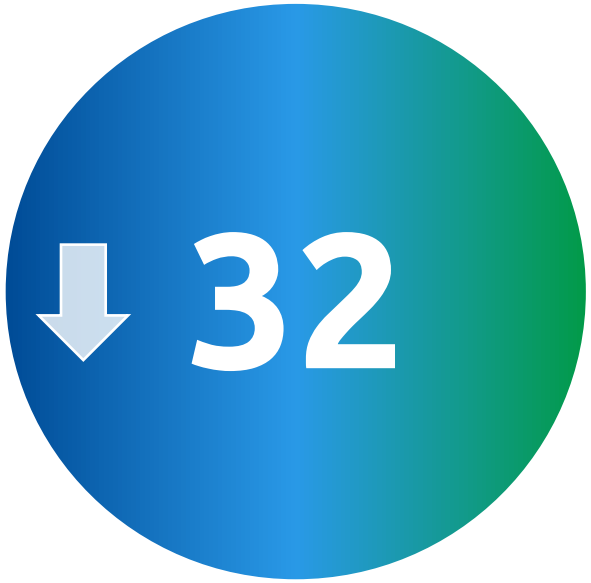
Threat Intelligence from a TSO perspective – 2024 Higlights

energy to inspire the world

As threats continue to escalate, relying solely on monitoring is no longer sufficient to ensure success. It is necessary to complement prevention strategies with mitigation plans to contain the issue. Automation can make the process more effective

Threats added to our monitoring

Third Parties Compromised



Accounts Compromised

IoCs Observed

In 2024, the Threat Intelligence team has **managed more than 6.000 events**, primarily through automated processess. The inputs for managing these events are gathered by aggregating data from **hundreds of sources** (e.g. website, forum, messaging chats, social media, blogs, etc.)

Threats in the "post-truth" era

energy
to inspire the world

In the "post-truth" era, people are more likely to accept arguments based on their emotions and beliefs rather than on factual evidence. This vulnerability can be exploited by malicious entities to manipulate public opinion, spread disinformation and create new threats (Deepfakes)

Fraudsters Used AI to mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

Cyber Threats

A Deepfake Scammed a Bank out of $25M – Now What?

A finance worker in Hong Kong was tricked by a deepfake video conference.

Elon Musk Deepfakes Feature in SpaceX Giveaway Scam on YouTube

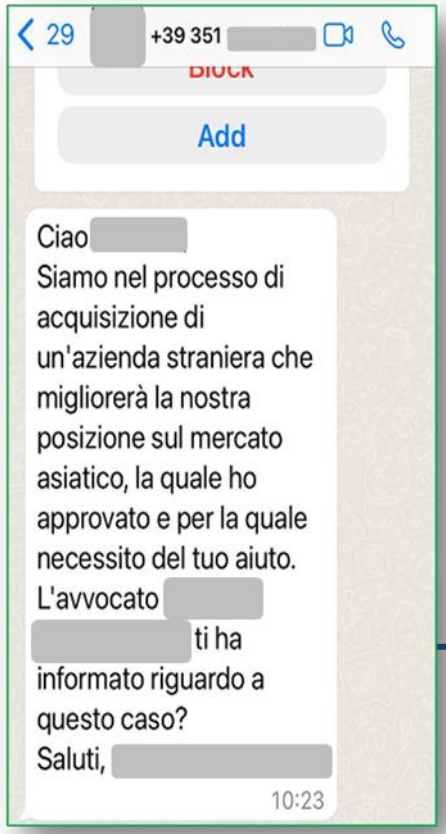
FIN7 hackers launch deepfake "generator" sites to spread malware

Criminal **interest in deepfakes on darkweb** forums **increased by approximately 32%** between Q1 2023 and Q1 2024, indicating the **growing number of users seeking to leverage this technology** for illicit financial gain.

The Deepfake Era

…Some real examples from our environment

Deepfake audio



The message is followed by a deepfake audio

COGnitive SECurity
AS DEFENSIVE STRATEGY

- AWARENESS & READINESS
- TECHNOLOGIES
- MONITORING
- POLICIES & PROCEDURES

energy to inspire the world

THANK YOU

6. ICS frontiers: Purdue Model for large grids, a point of view and future challenges

Fabrizio Zucca, Snam

Purdue Model for large grids

a point of view and future challenges

Snam Spa

Fabrizio Zucca

October 30th, 2024

Purdue Model – What is it?

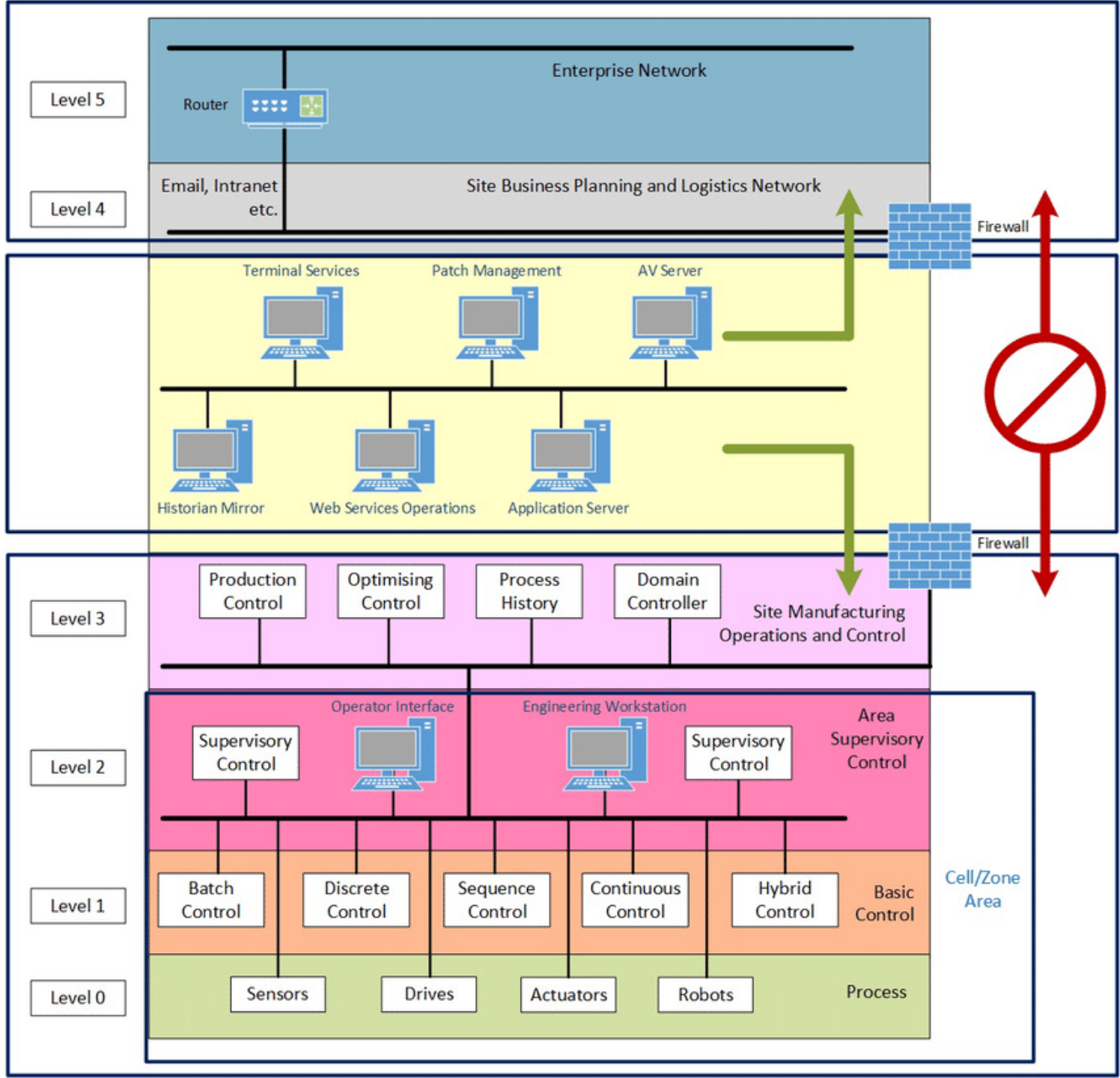
It is a reference architecture model made of levels based on functionalities of systems

History

Developed in 1990s at Pudue University to describe how organize computes in the production environment. The chosen by ISA-99 as a lighthouse for OT Secure architecture

Relevance

It is a linguistic tool to enable the collaboration of stakeholders with different background, (e.g. OT engineers, Network experts, security people)



1. Image from researchgate.com

Data hunger and Connectivity

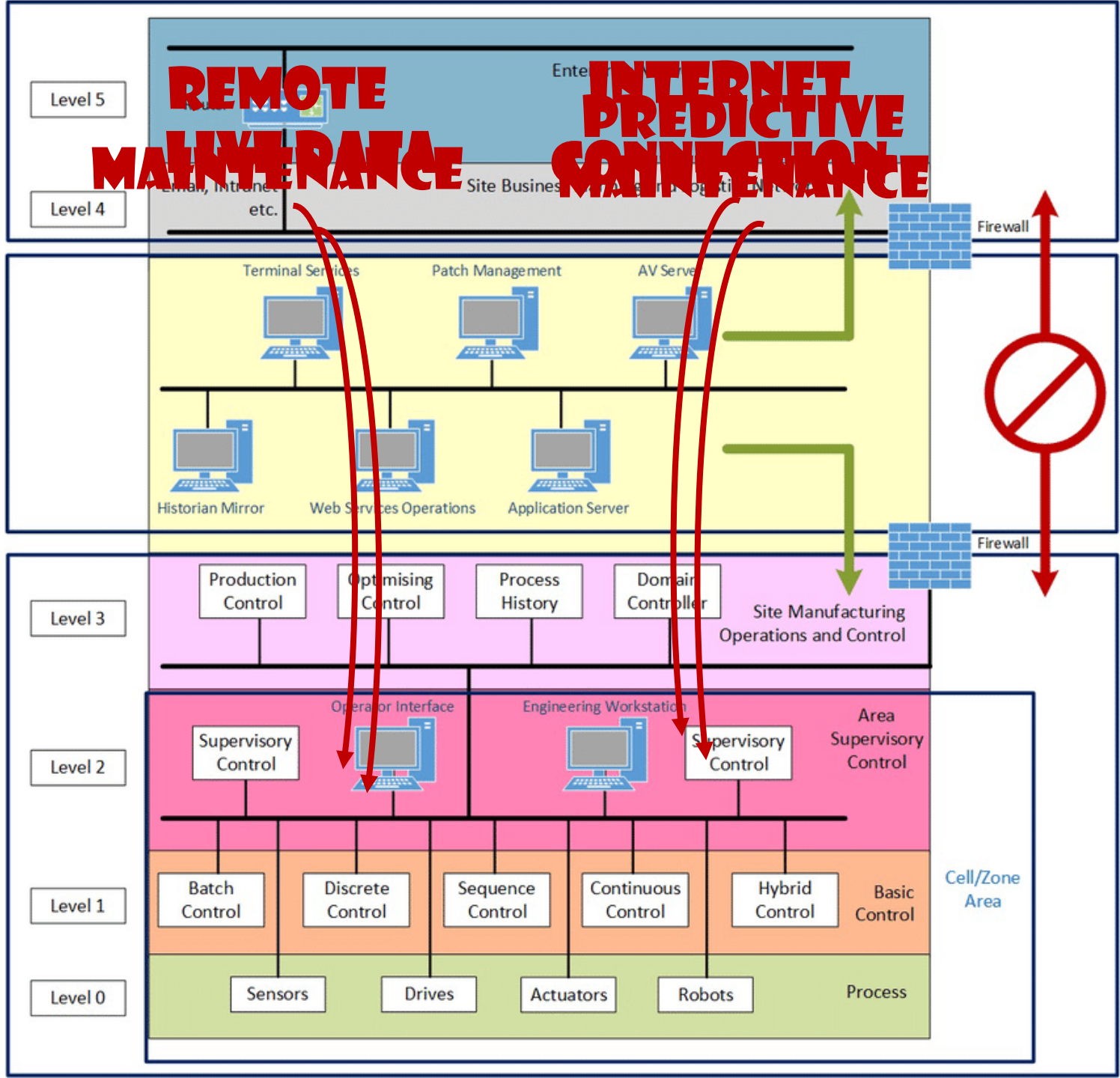
The forth industrial revolution brought a need of data from the lower levels of Purdue Model to support operations optimization and business decision making

Approaches

- Decoupling layer for data exchange
- Data streaming
- Data Diode Firewalls

Challenges

- Managing Asset in demilitarized zone
- Obsolete Operational Asset
- Large amount of resources needed



1. Image from researchgate.com

From Purdue model to the architecture

Where do you to set the border of the industrial control systems?

energy
to inspire the world

snam

Drivers

- More Complex ICS Components
- Advanced Security Measures and capabilities
- Corporate cloud computing migrations and cost optimization

Shared

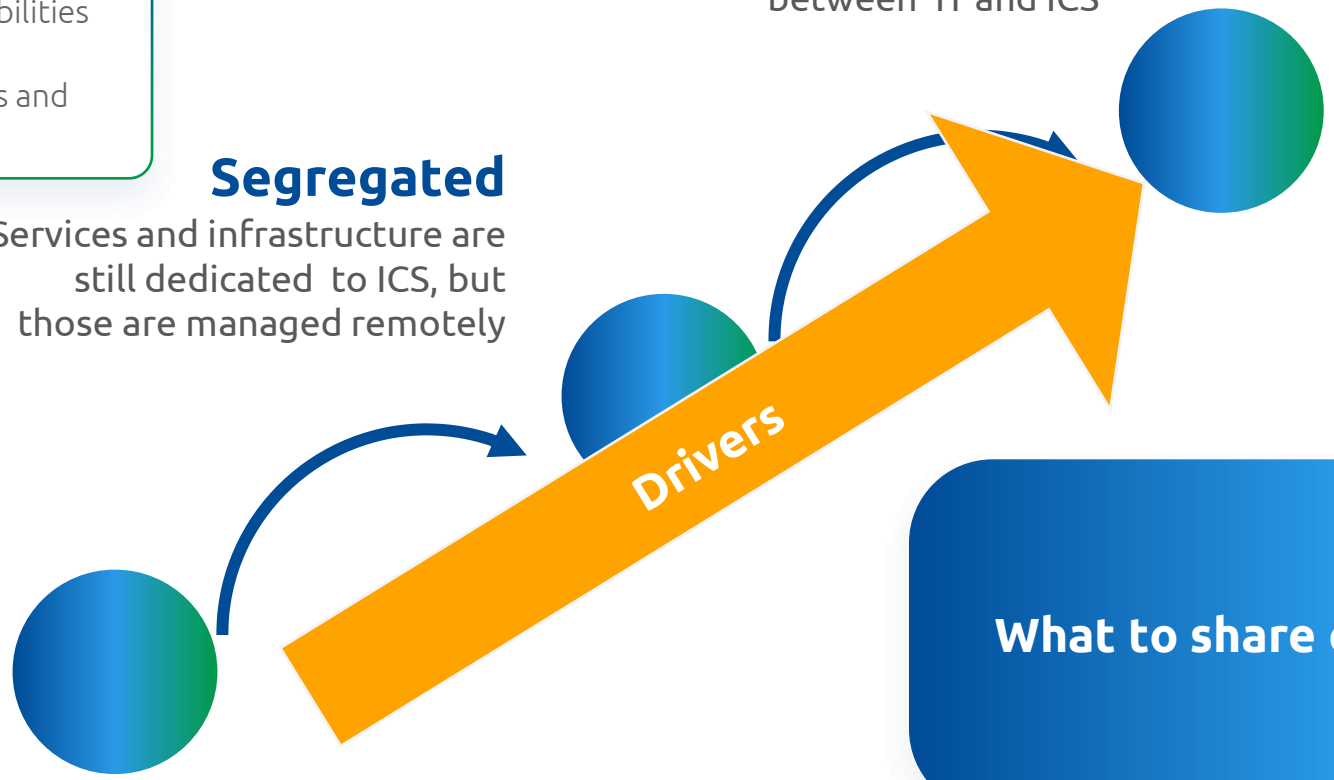
A part of the infrastructure and services are shared between IT and ICS

Segregated

Services and infrastructure are still dedicated to ICS, but those are managed remotely

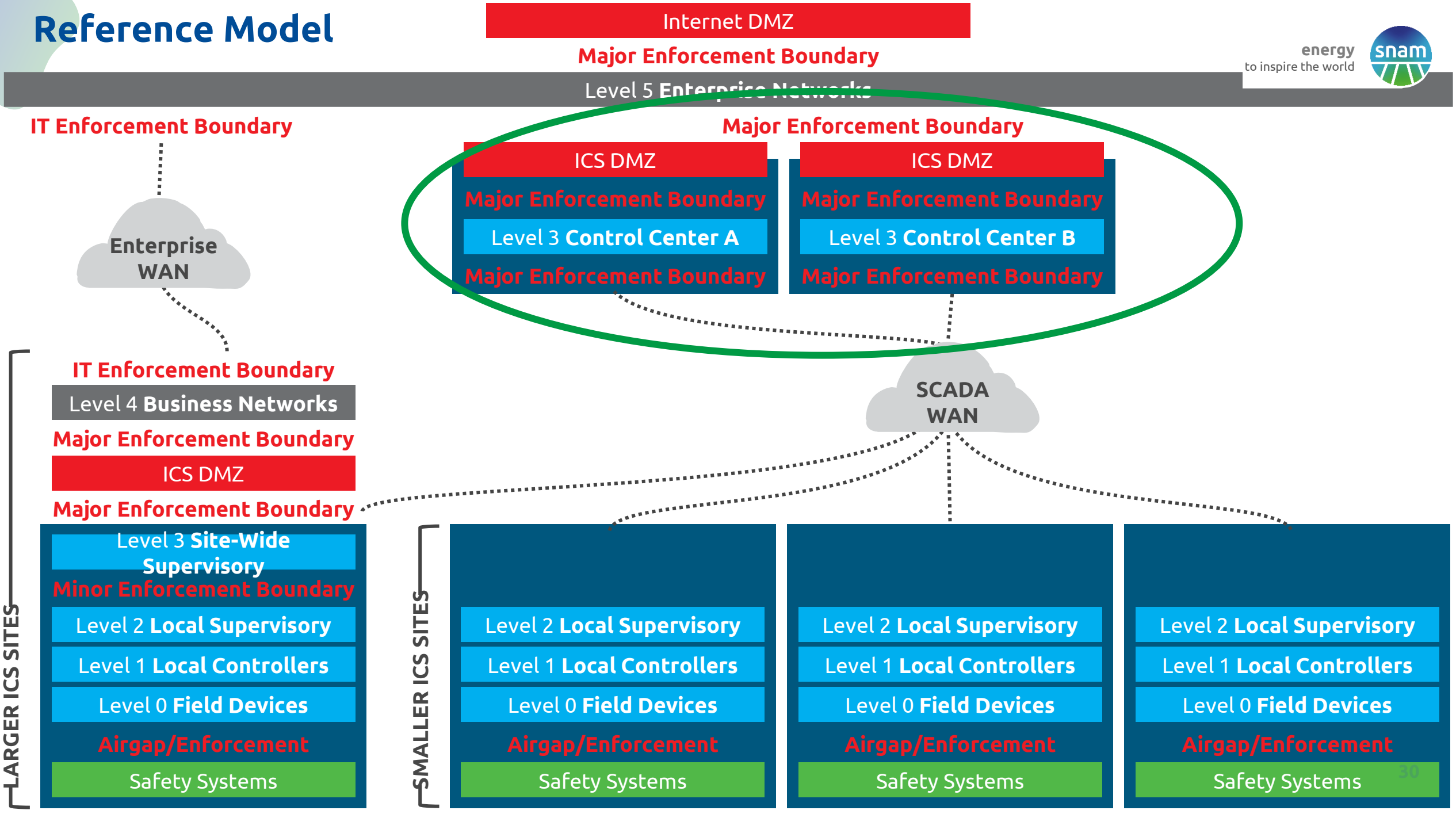
Isolated

Air Gapped ICS Systems, all supporting systems are in the same area

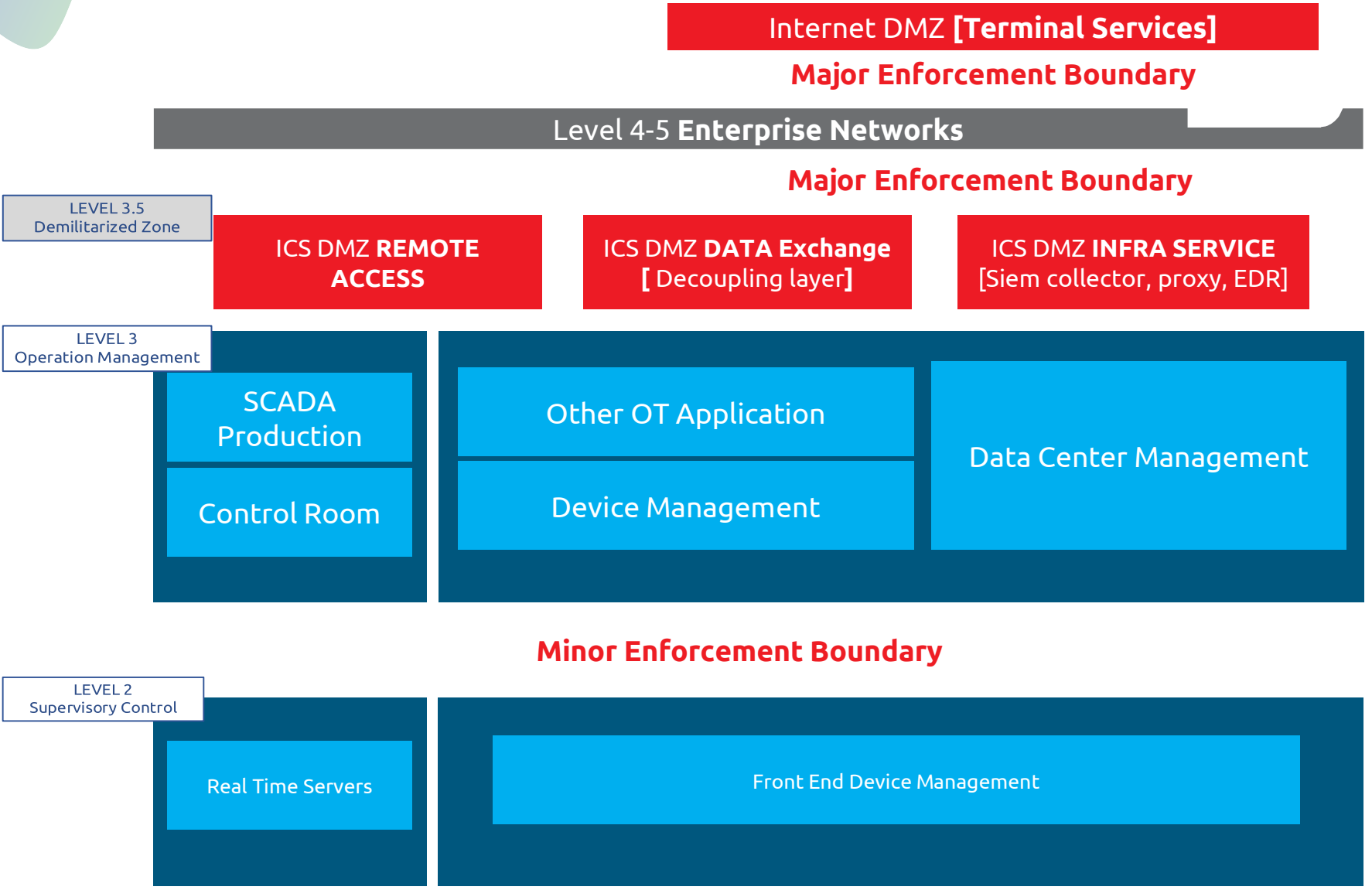


What to share or not to share?

Reference Model



Focus on the center



Systems that need to communicate to IT Systems

Systems related to the supervisory control, optimization and scheduling

Services that should communicate with the field [IED, RTU, PLC]

energy to inspire the world

THANK YOU

7. 20 min Coffee break 10:10 - 10:30

8. International C ion to cybersecurity

Presentation Cancelled

Brigadier General
Ioannis Chatzialexandris
European Defence Agency

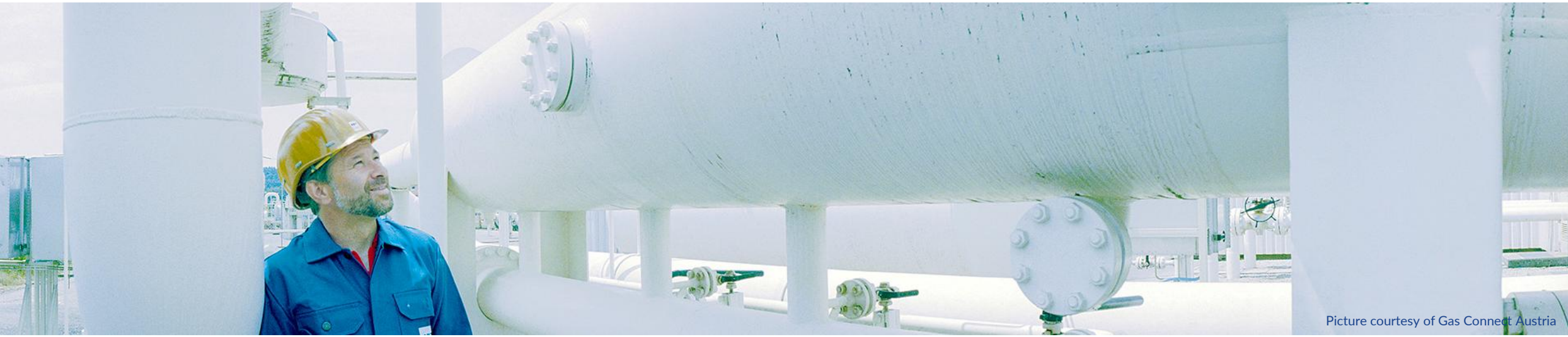
International CS: Physical asset security and the connection to cybersecurity

Ioannis CHATZIALEXANDRIS

Project Officer Energy & Environment Systems
Ioannis.Chatzialexandris@eda.europa.eu

9. International CS: ENTSOG Managing cybersecurity risks

Anton Kolisnyk – ENTSOG
ReCo KG Chair



Picture courtesy of Gas Connect Austria

Regional Coordination (ReCo) System for Gas

Managing cyber security risks

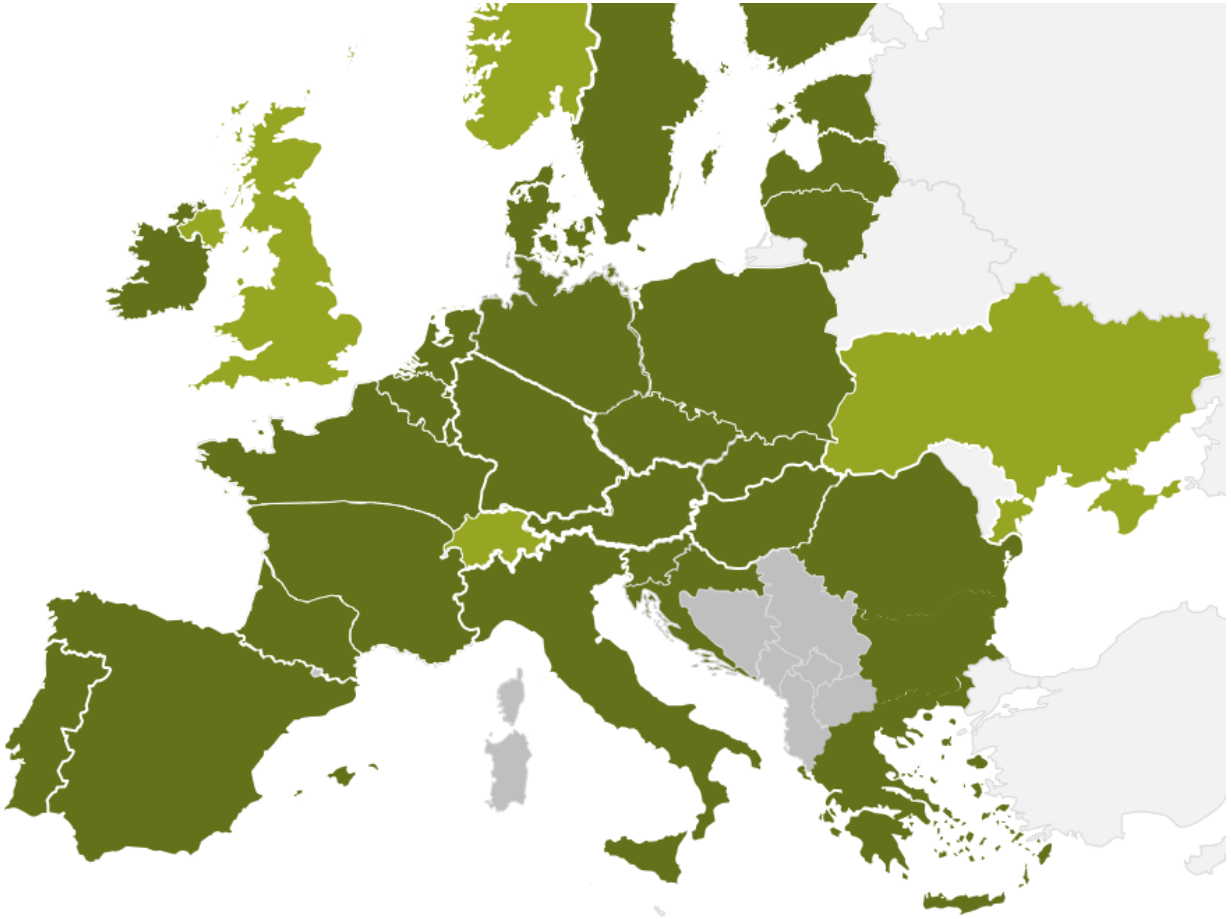
System Operation Team

ReCo System for Gas

ReCo is a concept for fast exchange of information and solutions between TSOs dispatching teams in case of:

- Potential risk for TSOs
  - Risks of gas flows disruptions
  - Unavailability of gas transport infrastructure
  - Extreme cold weather conditions
- Significant incidents impacting TSOs dispatching and operational procedures (incl. cyber-attacks)
- Declarations of crisis levels in MSs and extra need for cooperation
- Uncertainties and need of information exchange in case of SoS risks

ReCo System for Gas - ReCo Team Europe



ReCo Team Europe – community of European Gas TSOs

TSOs: *52 from 29 countries (25 EU countries)*

Facilitator: *Fluxys Belgium (since 2022)*

Reachability: *24/7 (phone, e-mail) TSOs dispatching*

Goal: to avoid, prevent, or mitigate negative impact of crisis events

How:

- Operational and technical expertise, knowledge sharing
- Gas flows patterns and gas market behavior analysis
- Looking for technical solutions on how to mitigate and cope with negative impact of a crisis
- Information exchange and provision to EC, GCG, MSs, ACER, other stakeholders

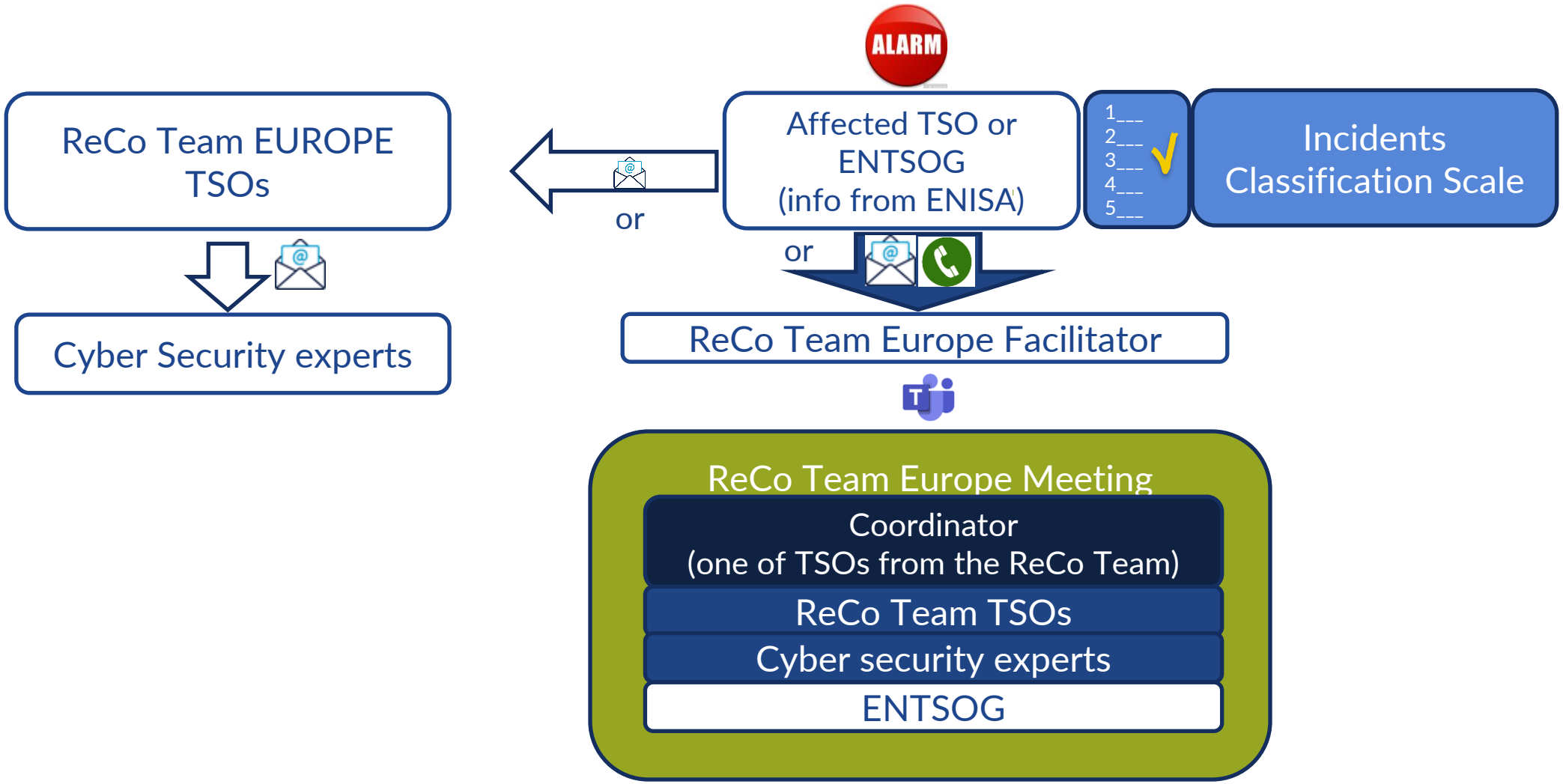
Cyber Security in the ReCo

- Goal: To exchange information between TSOs about potential or current cyber-attacks causing risks for TSOs operational procedures and security of gas supply.

- Tools:
  - 24/7 reachability – TSOs dispatching centres
  - Incidents classification scale (ICS): *focus on any issues impacting TSOs operations*
  - Guidelines for TSOs about how to act
  - Responsible bodies (Facilitators, ENTSOG)

ReCo Team Meeting. High Level Setup

Cyber security INCIDENT



Cyber Security Threats in the ReCo

- Cyber-attack with significant risks to perform TSOs tasks and potential risks for other TSOs, including impact on TSOs dispatching activities
  (ICS: Level 2 - potential events in the future and inability to execute data exchange)
- Cyber-attack causing gas flow disruptions with significant impact on demand/supply situation in a balancing zone(s).
  (ICS: Level 3 - a significant effect on gas transmission operation and reliability)

Coordination between TSOs in case of cybersecurity risks

ReCo setup will be used only for Cyber Security cases which impact TSOs operational and dispatching procedures

Other relevant highlights:

- Cyber security for gas included in the Reg.2024/1789 (SoS, Measures on cybersecurity)
- High importance and focus on cyber security from ACER, EC, MSs.
  - ENTSOG and ENISA developed an information session on cyber security issues where parties exchange their experiences, knowledge, and solutions for strengthening TSOs cyber security.
- TSOs & ENTSOG, ENTSOG & GIE, ENTSOG & ENISA working groups cover cyber security topics on a regular basis

Thank you for your attention

System Operation Team

Anton.Kolisnyk@entsog.eu

ENTSOG - European Network of Transmission System Operators for Gas
Avenue de Cortenbergh 100, 1000 Bruxelles

www.entsog.eu | info@entsog.eu

10. International CS: The European Cybersecurity Scheme on Common Criteria (EUCC)

Philippe Blot, ENISA

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA PQC RELATED ACTIVITIES

Philippe Blot
Head of sector Certification
Market Certification & Standardisation Unit
ENISA

30 10 2024

CERTIFICATION AND CRYPTOGRAPHY

Content of the presentation

- Main characteristics of EUCC, a recently adopted certification Scheme
- Cryptography supporting EUCC certification
- ENISA Certification website
- Q&A

EUCC MAIN CHARACTERISTICS

- Sets out the European Common Criteria-based cybersecurity certification scheme
- Focuses on the “how to certify”
- Certification of ICT products and Protection Profiles
- 2 assurance levels (substantial, high) with possible private & public CBs
- Requirements for CABs (CB, ITSEF): accreditation, authorisation, notification
- Certificates validity of 5 years
- Mandatory monitoring and vulnerability management
- Peer Assessment of CBs each 5 years

UNDERSTANDING THE PUBLICATION OF EUCC

Implementing Act:

Published at Implementing regulation - EU - 2024/482 - EN - EUR-Lex (europa.eu) :

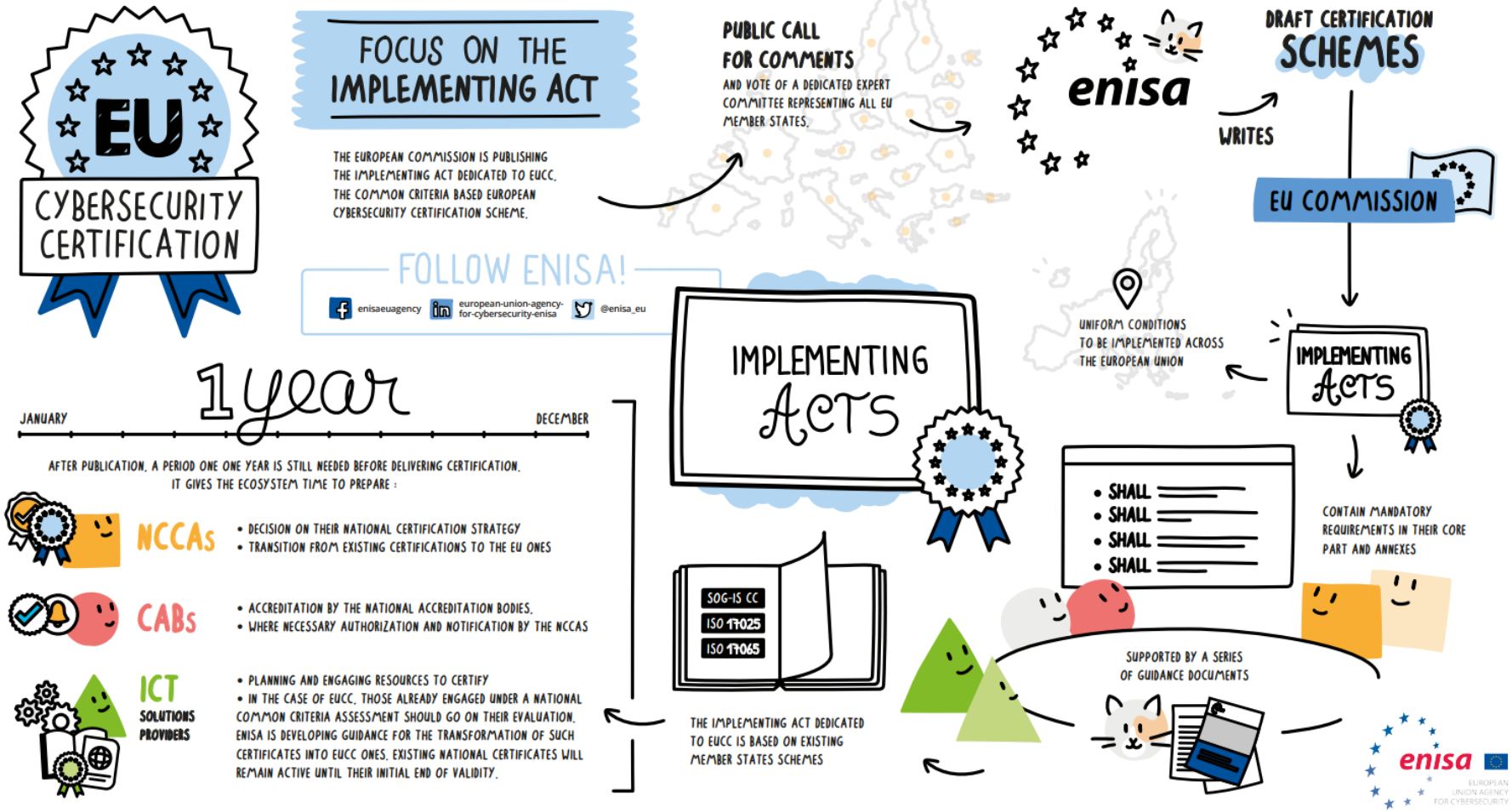
Legislative text published by the European Commission based on the candidate scheme written by ENISA with the Ad-Hoc Working Group & EU Member States

Supporting Documents:

Published at https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

Documents to help implement the legislative act:

- **State of the Art Documents**
  - listed in Annex 1 of the scheme (mostly SOG-IS documents adopted at EU level)
  - Ongoing work for additional documents (e.g.: accreditation)
- **Guidelines**
  - Existing guidance established by EUCC AHWG (e.g.: SOG-IS transition) to be updated
  - New guidelines (e.g: authorisation, vulnerability handling)

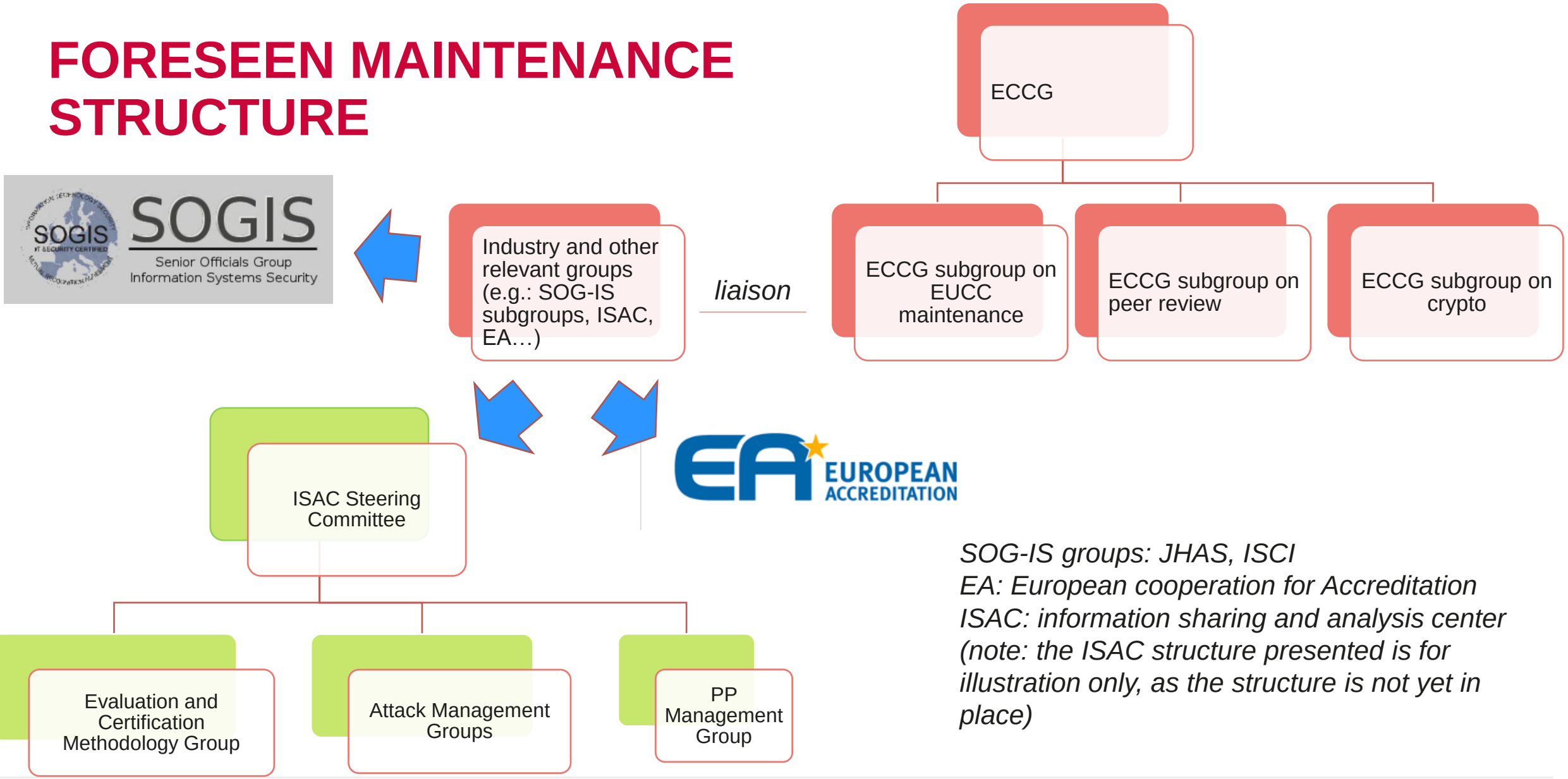


EUCC

Adoption as Commission Implementing Regulation (EU) 2024/482 of 31 January 2024
First year dedicated to accreditation, authorization and notification of CABs

https://videos.enisa.europa.eu/w/obA5BmahdjvEXmdvNqZCyC

FORESEEN MAINTENANCE STRUCTURE



SOG-IS groups: JHAS, ISCI
EA: European cooperation for Accreditation
ISAC: information sharing and analysis center
(note: the ISAC structure presented is for illustration only, as the structure is not yet in place)

CRYPTOGRAPHY SUPPORTING EUCC CERTIFICATION

New ECCG dedicated subgroup launched

Short-term objective already achieved:

- **SOG-IS ACM https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf is now a guidelines document for EUCC**

mid-term objective:

- **Adopt ACM 1.4 which also covers PQC**
- **Develop harmonised elevation procedures**

Parallel activity on a EU PQC roadmap (what and when to transition)

HOW TO BE INVOLVED

AHWGs and public consultations

Website: https://certification.enisa.europa.eu/

CEF platform

Awareness Raising Videos :

3 episodes on Youtube: **ENISAvideos**

Tradeshows and Events:

Annual Cybersecurity Certification Conference

FIC, ITSA Nuremberg, Jornadas, One-Conference, ICCC

Presentations, Talks & Social Media:

Follow **European Union Agency for Cybersecurity (ENISA)** on Linkedin

and **@enisa_eu** on Twitter

ENISA Certification video playlist:

THANK YOU FOR YOUR ATTENTION

+30 6936000147

philippe.blot@enisa.europa.eu

www.enisa.europa.eu,
https://certification.enisa.europa.eu/

11. International CS: ENTSOG GIE Joint cybersecurity task force update

Douglas Hill and Andrea Chittaro (ENTSOG/Snam)

What is the ENTSOG GIE Joint Task Force on Cybersecurity?

- **Scope:** EU regulatory initiatives on Cybersecurity
- **Objective:** Managing ENTSOG and GIE members' interests in the current European discussions around Cybersecurity
- Build common views on CS policy (NCs, Regs, DIR)
- Build external relations with EDA, ENISA, ENCS, DG ENER, CERT-EU, etc.
- Offer insights into certain pieces of CS legislation

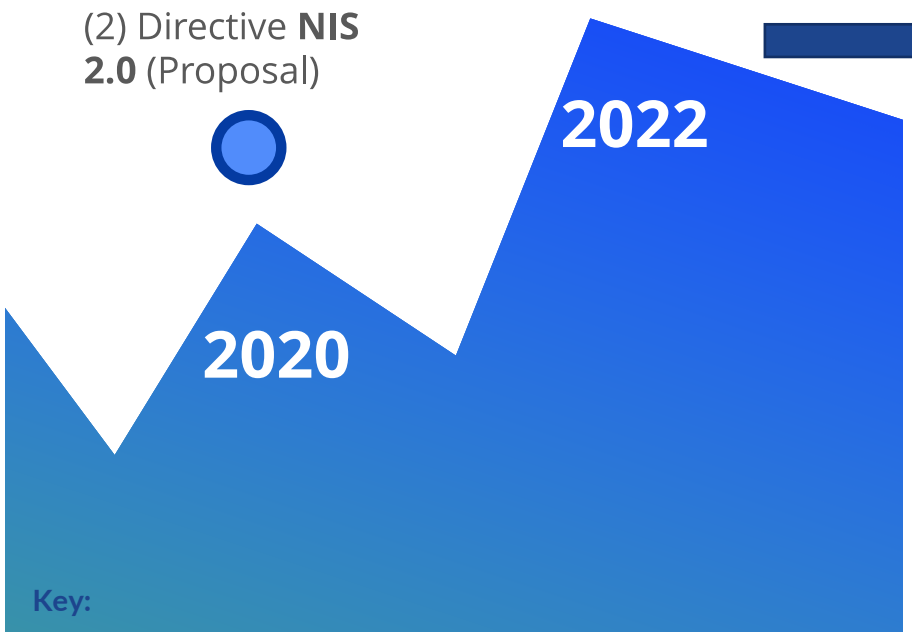
The Cybersecurity Normative Landscape in Security and Resilience

Normative Landscape in Security and Resilience

(1) Directive on **Resilience of Critical Entities** (Proposal)

(2) Directive **NIS 2.0** (Proposal)

NIS 2.0
CER
DORA regulation
(promulgated)



Key:

NIS 2.0
DIR
Digital IS security


27.12.2022 EN Official Journal of the European Union L 333/80

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

CER
Critical Entities Resilience
DIR
Physical IS security

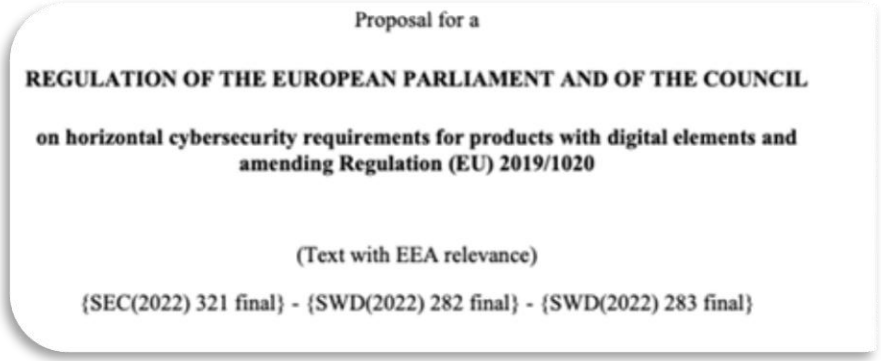

27.12.2022 EN Official Journal of the European Union L 333/164

DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on the resilience of critical entities and repealing Council Directive 2008/114/EC

CRA
Cyber Resilience Act
product/services certification


Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

1. NIS 2.0 Dir = Network and Information Systems Directive, 2. CER= Critical Entities Resilience Directive, 3. DORA=Digital Operational Resilience Act (REGULATION)
promulgated = promoted, made known, CRA=Critical Resilience Act, Draft Reg

NIS 2.0 Directive

NIS 2.0 promotes resilience of critical digital infrastructure

Focus is on:

- Outages
- Large attacks, major incidents (DDOS, ransomware *etc.*)
- Redundancy, backups
- Handle crisis situations, recovery, biz cont.
- Detection and response.
- Reporting incidents

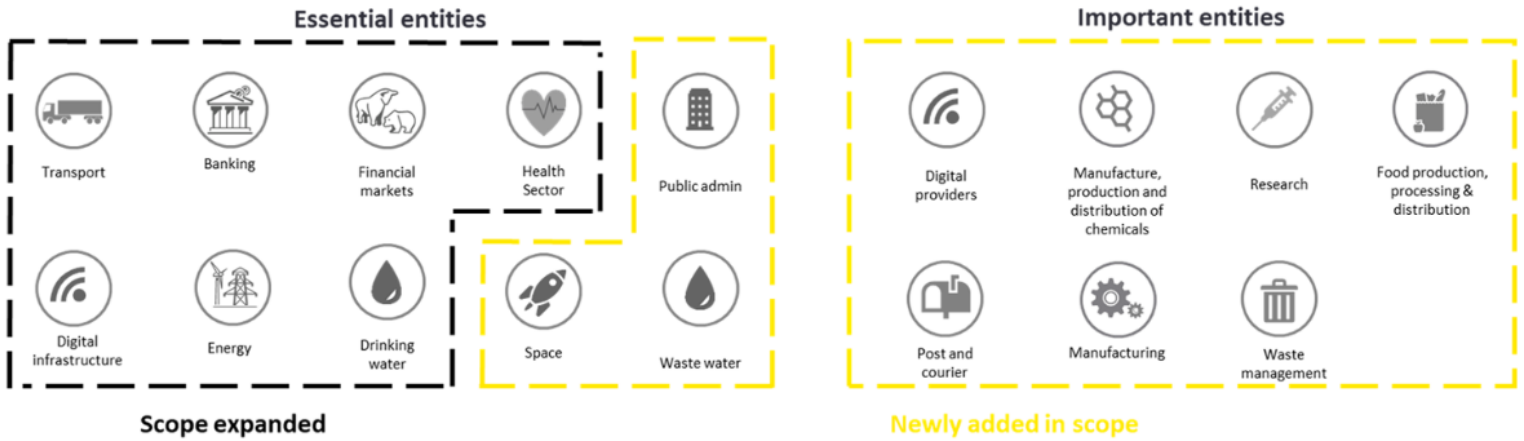
ALL ABOUT THE OPERATIONAL SERVICES & DIGITAL RESILIENCE

Extended scope NIS 1 to NIS 2: Essential and important entities

Extension of the scope

NIS2 defines two categories for entities in scope: important and essential. Entities in both categories will have to meet the same requirements. However, the distinction will be in the supervisory measures and penalties. Essential entities will be required to meet supervisory requirements as of the introduction of NIS2, while the important entities will be subject to ex-post supervision, meaning that in case authorities receive evidence of non-compliance, action is taken.

The NIS2 has simplified the scoping exercise the competent authorities have to make. A list of sectors was defined and a base rule of any large (headcount over 250 or more than 50 million revenue) or medium (headcount over 50 or more than 10 million revenue) enterprise from those sectors will be directly included in the scope. However, small or micro-organizations are not necessarily excluded; Member States can extend these requirements if an enterprise fulfills specific criteria that indicate a key role for society, the economy or for particular sectors or types of service.



Text here

The Network and information security NIS 2 Directive

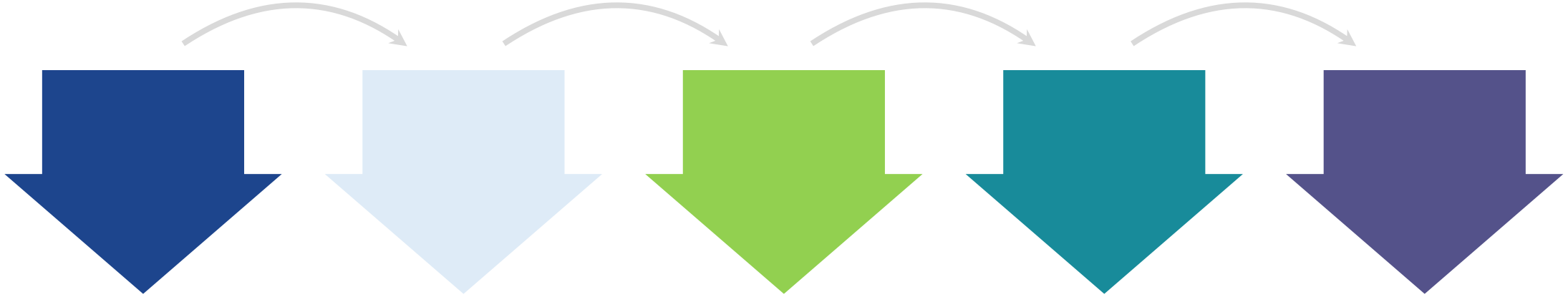
In force 16-1-2023
MSs have 21 Months to transpose Oct 2024.

27.12.2022 EN Official Journal of the European Union L 333/80

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)



creating the necessary cyber crisis management structure (CyCLONe)

increasing the level of harmonization regarding security requirements and reporting obligations

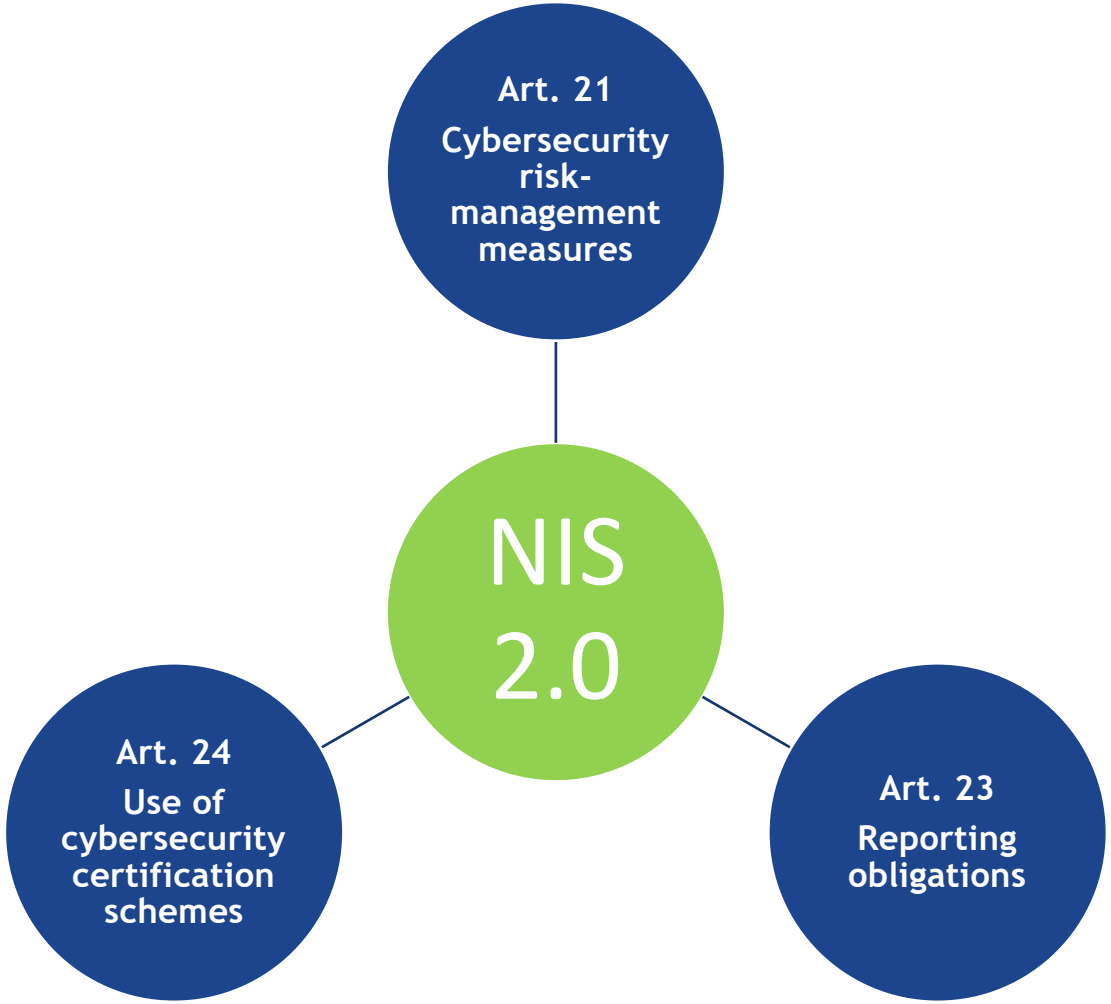
encouraging Members States to introduce new areas of interest in their national cybersecurity strategies

covering a larger share of the economy and society by including more sectors

bringing novel harmonization efforts such as the peer reviews for enhancing collaboration and knowledge sharing amongst the Member States

The European cyber crises liaison organisation network (EU-CyCLONe) https://www.enisa.europa.eu/topics/incident-response/cyclone

Network and Information Security Directive NIS 2.0. Articles of interest for the gas sector



Scope TSOs
Annex 1
SECTORS OF HIGH CRITICALITY

	— Central stockholding entities as defined in Article 2, point (l), of Council Directive 2009/119/EC (*)
(d) Gas	— Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parli
	— Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC
	— Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC
	— Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC
	— LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC
	— Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC
	— Operators of natural gas refining and treatment facilities
(e) Hydrogen	— Operators of hydrogen production, storage and transmission

Art 21. Cybersecurity risk-management measures.

The measures shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

1. Policies on risk analysis and information system security;
2. Incident handling;
3. Business continuity, such as backup management and disaster recovery, and crisis management;
4. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
5. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
7. Basic cyber hygiene practices and cybersecurity training;
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
9. Human resources security, access control policies and asset management;
10. The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Art 23. Reporting obligations to national CSIRT (Computer Security Incident Response Team)

An incident shall be considered to be significant if:

- It has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
- It has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Member States shall ensure that the entities concerned submit to the CSIRT :

a. Without undue delay and in any event **within 24 hours of becoming aware of the significant incident**, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

b. Without undue delay and in any event **within 72 hours of becoming aware of the significant incident**, an incident notification, which, where applicable, shall update the information referred to in point (a) and **indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise**;

c. Upon the request of a CSIRT or, where applicable, the competent authority, **an intermediate report on relevant status updates**;

d. A final report not later than one month after the submission of the incident notification

Art 24. Use of European cybersecurity certification schemes

- Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes (CRA refers)
- The Commission may, after consulting the Cooperation Group and the European Cybersecurity Certification Group, request ENISA to prepare a candidate scheme

My personal take-aways and where ENTSOG can add value

1. The NIS 2.0 Directive almost exclusively puts the burden of set–up on MSs
2. ENISA are also obligated to facilitate oversight of various aspects and provide tools and templates for important and essential entity event reporting
3. Coordination group 27 MSs + ENISA coordinate the NIS
4. MSs shall have a SPOC at national level CSIRT/CERT
5. Sets out the framework for Certification of products (CRA proposal)
6. ENTSOG AS4 security for transmitted document data
7. TSOs can become more informed as we discuss NIS 2.0, CRA and CER in the GIE/ENTSOG Joint CS TF
8. ENTSOG can facilitate knowledge sharing through the ENISA courses we have put together for 2024/5 – dates to be announced

Text here

27.12.2022 EN Official Journal of the European Union L 333/164

DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on the resilience of critical entities and repealing Council Directive 2008/114/EC

The Critical Entities' Resilience CER Directive 2022/2557

The Critical Entities Directive wants to address physical resilience…

CER was proposed in parallel to NIS 2.0 as the physical counter part to NIS 2.0:

1. NIS 2 is for critical digital ICT infrastructure
2. CER is for critical physical infrastructure

ALL ABOUT THE PHYSICAL RESILIENCE

* https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

The CER Directive 2022/2557

In force 16-1-2023
MSs have 21 Months to transpose Oct 2024.

new rules strengthen the resilience of critical infrastructure to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage

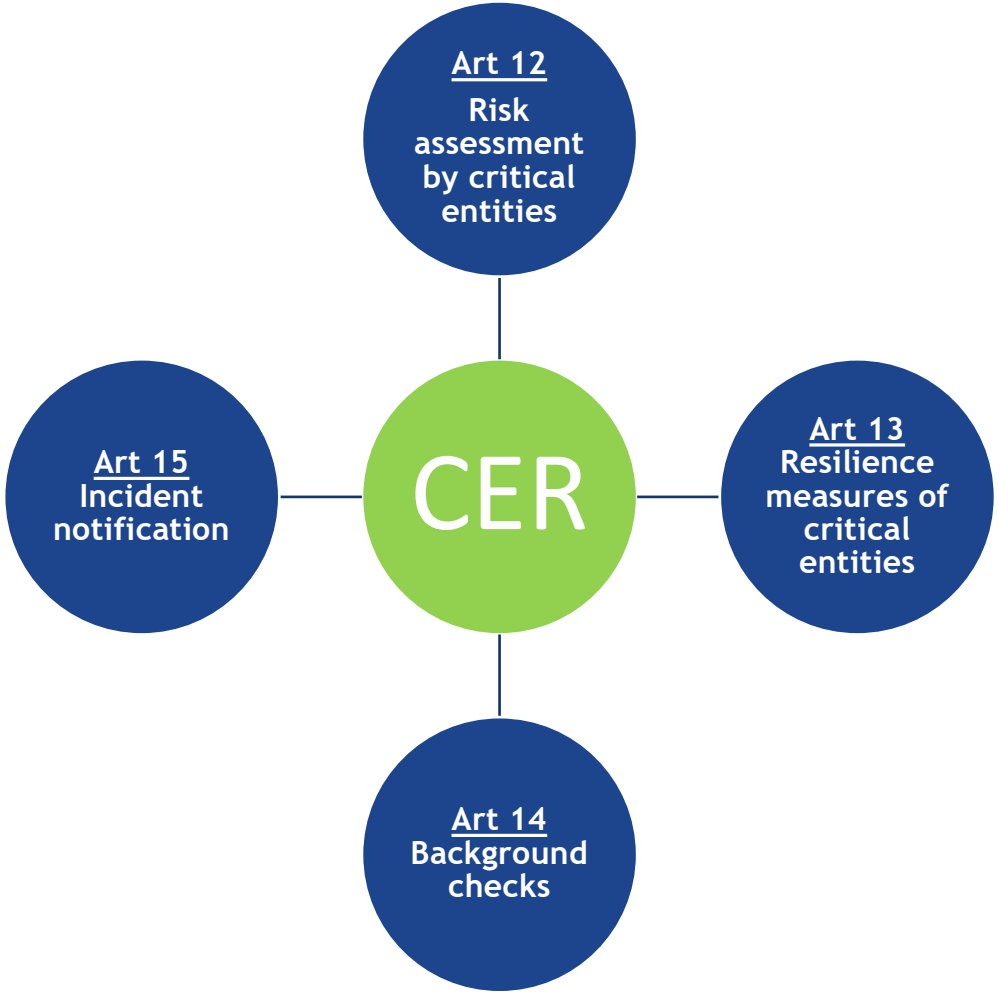
security requirements and reporting obligations complementary to the NIS 2

Members States to adopt a strategy on the resilience of critical entities and perform National Risk Assessments

covering a larger share of the economy and society by including 11 sectors

creation of the Critical Entities Resilience Group

Points of CER DIR interest for the gas sector



Scope TSOs same as NIS2
Annex
SECTORS OF HIGH CRITICALITY

	— Central stockholding entities as defined in Article 2, point (l), of Council Directive 2009/119/EC (*)
(d) Gas	— Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parli
	— Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC
	— Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC
	— Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC
	— LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC
	— Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC
	— Operators of natural gas refining and treatment facilities
(e) Hydrogen	— Operators of hydrogen production, storage and transmission

Risk assessment by critical entities Article 12, CER

Don’t propose we go through these in detail given the time constraints

1. Member States shall ensure that critical entities carry out a **risk assessment within nine months** of receiving the notification referred to in Article 6(3), whenever necessary subsequently, **and at least every four years**, on the basis of Member State risk assessments and other relevant sources of information, in order **to assess all relevant risks that could disrupt the provision of their essential services (‘critical entity risk assessment’**).

2. Critical entity risk assessments shall account for **all the relevant natural and man-made risks which could lead to an incident, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences** as provided for in Directive (EU) 2017/541. A critical entity risk assessment **shall take into account the extent to which other sectors as set out in the Annex depend on the essential service provided by the critical entity and the extent to which that critical entity depends on essential services provided by other entities** in such other sectors, including, where relevant, in neighbouring **Member States and third countries**.

Resilience measures of critical entities Article 13, CER

Don’t propose we go through these in detail given the time constraints

Member States shall ensure that critical entities **take appropriate and proportionate technical, security and organisational measures to ensure their resilience**, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

a. prevent incidents from occurring, duly considering **disaster risk reduction and climate adaptation measures**;

b. ensure adequate **physical protection of their premises and critical infrastructure**, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;

c. respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;

d. recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;

e. ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;

f. raise awareness about the measures referred to in points (a) to (e) among relevant personnel, duly **considering training courses, information materials and exercises**.

Background checks
Article 14, CER

Member States shall specify the conditions under which a critical entity is permitted, in duly reasoned cases and taking into account the Member State risk assessment, to **submit requests for background checks on persons who**:

a. **hold sensitive roles in or for the benefit of the critical entity**, in particular in relation to the resilience of the critical entity;
b. **are authorised to directly or remotely access its premises, information or control systems, including in connection with the security of the critical entity**;
c. **are under consideration for recruitment to positions that fall under the criteria set out in point (a) or (b).**

Don’t propose we go through these in detail given the time constraints

Incident notification
Article 15, CER

Don’t propose we go through these in detail given the time constraints

Member States shall ensure that critical entities notify the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Member States shall ensure that, unless operationally unable to do so, **critical entities submit an initial notification no later than 24 hours after becoming aware of an incident**, followed, where relevant, by a **detailed report no later than one month thereafter**. In order to determine the significance of a disruption, the following parameters shall, in particular, be taken into account:

a. **the number and proportion of users affected by the disruption**;
b. **the duration of the disruption**;
c. **the geographical area affected by the disruption**, taking into account whether the area is geographically isolated.

My personal take-aways for CER – what can ENTSOG add?

- The responsibility is on MSs to put the CER frameworks in place
- Background checks of critical infrastructure staff
- Incident reporting
- ENTSOG, an awareness raising role of CER articles relevant for Gas
- Discuss and dig into the various pieces of legislation at the GIE/ENTSOG JT TF CS
- Offer ReCo infrastructure to facilitate physical incident sharing (when permissible)

ENTSOG/GIE JT TF Cybersecurity CS focus 2025

TF Cybersecurity Next Steps Proposal

- Build procedural and technical solution adoption schemes to enhance Cybersecurity controls on gas infrastructure
- Develop common tools to address ICS Security requirements on procurement phases
- Evaluate to join and support other networks focusing on Cybersecurity of grids

EUROPEAN COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

The Cyber Resilience Act (DRAFT PROP) 2022/0272(COD)

NB: Where NIS2 focuses on enhancing the security posture of companies themselves, the CRA requires companies to prioritize the security of the products they manufacture or sell.

The Cyber Resilience ACT wants to address…

Hardware and software products suffer from **two major problems** adding costs for users and the society:

1. A low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and
2. An insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

ALL ABOUT THE PRODUCTS AND SERVICES THAT CRITICAL AND IMPORTANT ENTITIES USE AND THEIR ASSOCIATED CERTIFICATION DENOTING THEM AS 'CYBERSECURE BY DESIGN'

* https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

The Cyber Resilience ACT (2)

Two main objectives were identified aiming to ensure the proper functioning of the internal market:

1. Create conditions for the **development of secure products** with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and

2. Create conditions allowing users to **take cybersecurity into account when selecting and using products** with digital elements.

Four specific objectives were set out:

1. Ensure that **manufacturers improve the security of products** with digital elements since the design and development phase and throughout the whole life cycle;

2. Ensure a **coherent cybersecurity framework**, facilitating compliance for hardware and software producers;

3. Enhance the **transparency of security properties** of products with digital elements, and

4. Enable businesses and consumers to **use products with digital elements securely**.

* https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

My personal take-aways for CRA – where can ENTSOG facilitate

- CRA requires companies to prioritize the security of the products they manufacture or sell
- Product and services to be certified
- Ensure product 'CS by design' concept
- ENTSOG, an awareness raising role
- Share ENISA course material
- Discuss and dig into the various pieces of legislation at the GIE/ENTSOG JT TF CS
- AS4 ENTSOG profile – SPs need to be certified according to the CRA Reg
  - ENTSOG can add this to the AS4 wksp and the DE & CS WKSP agendas

Thank you for your attention

Douglas Walker Hill

Douglas.Hill@ENTSOG.EU

12. International CS: Cyber Europe 2024 review

Dr. Alexandros Zacharis - ENISA


Enjoy your lunch
see you at 13:00

Slides removed

14. Awareness: Introduction to the ENISA awareness package

Dr. Alexandros Zacharis - ENISA

15. Tabletop cybersecurity exercises

Dr. Alexandros Zacharis - ENISA

Tabletop Cybersecurity exercise, team work!

16. Q&A and goodbye

Douglas Walker Hill
Interoperability & Data Exchange Adviser
ENTSOG

Thank you for your attention & being an active part at this event, see you in 2025!

Douglas Walker Hill, Interoperability & Data Exchange Adviser

douglas.hill@entsog.eu

ENTSOG - European Network of Transmission System Operators for Gas

Avenue de Cortenbergh 100, 1000 Bruxelles

www.entsog.eu | info@entsog.eu