ISA Ireland Section OT Cybersecurity Conference 2025

OT Resilience: Incident Prevention, Response, and Recovery

'Safety Meets Security'

Manikandan Karuppasamy Ramasamy (Mani)
Pilz Ireland

01

- Introduction to Industrial Security

INTRODUCTION TO INDUSTRIAL SECURITY

Why is Industrial security important?

- Increase in cyber-attacks, external or internal manipulation and misuse: machinery safety measures can be undermined.
- No Safety without Security: only security measures can protect safety from manipulation, and ultimately protect humans.
- The question is not if a cyber-attack will happen, but when!
- New legal requirements:
  - Machinery Regulation.
  - NIS2 Directive.
  - Cyber Resilience Act (CRA).
- In the future, a CE Mark will not be possible without complying with the security requirements.

IMPLICATIONS OF THE EU MACHINERY REGULATION, CYBER RESILIENCE ACT & NIS 2

- **Safety and Industrial Security – different "protection" functions**

Safety

Protects people from hazards due to machinery

IMPLICATIONS OF THE EU MACHINERY REGULATION, CYBER RESILIENCE ACT & NIS 2

- **Safety and Industrial Security – different "protection" functions**

Security

Protects the machine and data from manipulation and unauthorised access

ISA International Society of Automation
Setting the Standard for Automation™

02

- Cyber-Attacks on OT: Key Insights & Data

CYBER-ATTACKS ON OT SYSTEMS:

- **Numbers, data from the Dragos (2025)**

ransomware attacks against **industrial organizations** increased **87** percent over last year

of all ransomware attacks targeted **1,171 manufacturing entities** in **26 unique manufacturing subsectors**

ransoms were paid, and organizations possessed adequate capacity to **restore operations without engaging adversaries.**

Cyberattacks have increased their impact on operational technology (OT):

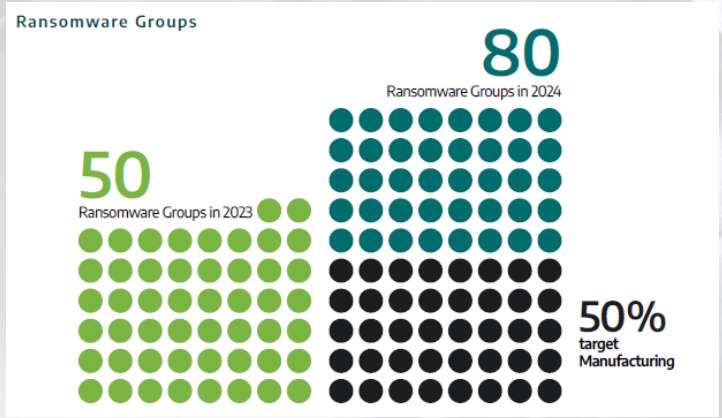
- Most incidents disrupted plant operations, and in 25% of cases, cyberattacks resulted in a complete shutdown of production site.
- 75% percent resulting in at least some disruption to operations.
- 20% of all incidents involved an exploitation of remote access, including VPN exploits, remote access applications, & RDP from corporate

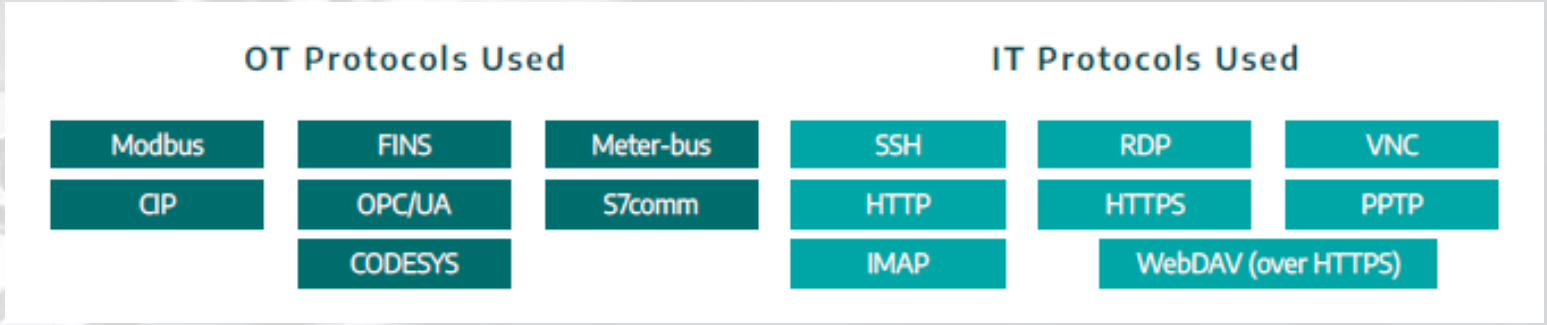
Link for the Dragos 2025 Report : https://www.dragos.com/ot-cybersecurity-year-in-review

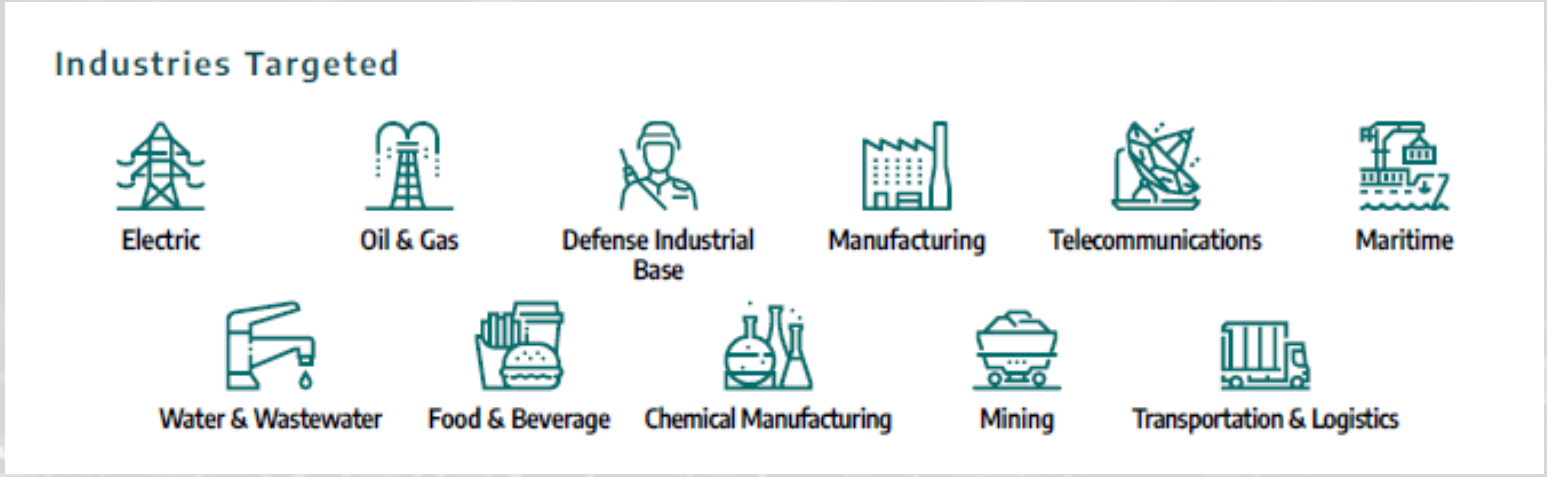
Dragos - International Industrial Cybersecurity Company

CYBER-ATTACKS ON OT SYSTEMS:

- **Numbers, data from the Dragos (2025)**







Link for the Dragos 2025 Report : https://www.dragos.com/ot-cybersecurity-year-in-review

#Dragos - International Industrial Cybersecurity Company

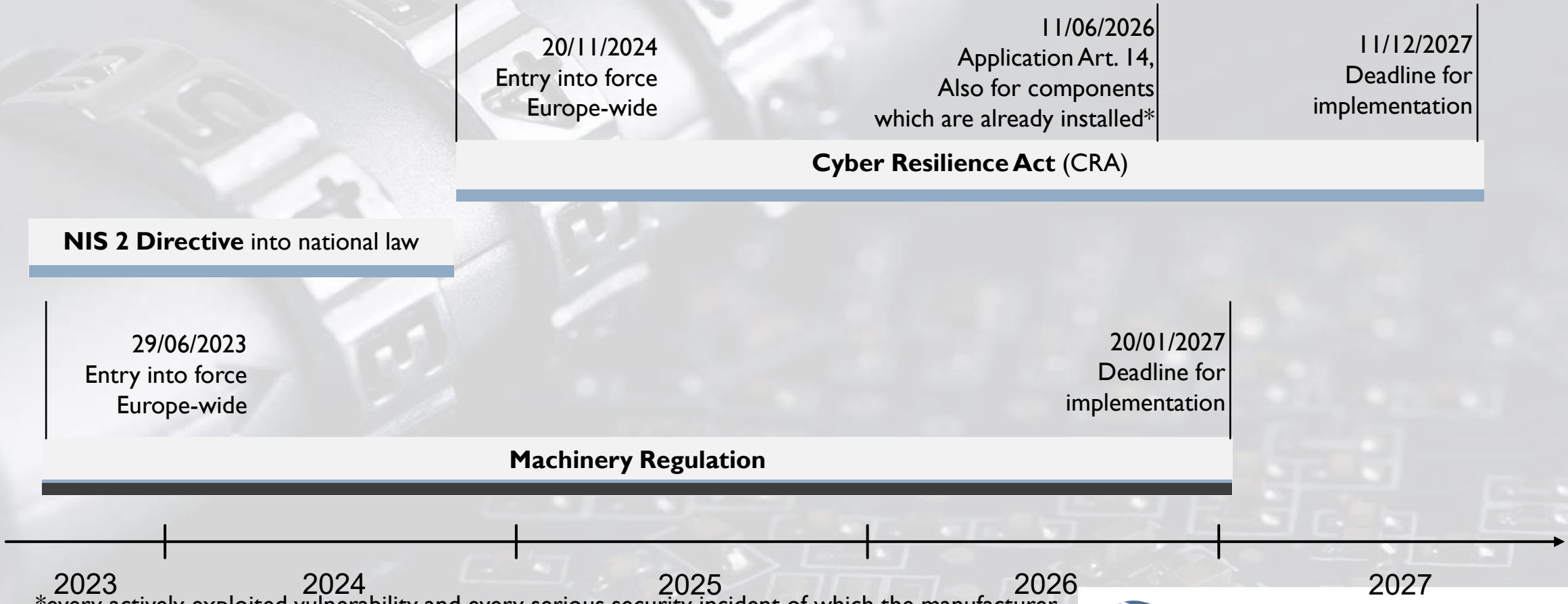
ISA International Society of Automation
Setting the Standard for Automation™

03

- Industrial Security Legislation

IMPLICATIONS OF THE EU MACHINERY REGULATION, CRA & NIS 2

- **Timeline**



*every actively exploited vulnerability and every serious security incident of which the manufacturer or distributor becomes aware must be reported within 24 hours simultaneously to ENISA and to the CSIRT of the EU Member State. Information on measures and corrections must be provided for each report once the cause has been clarified.

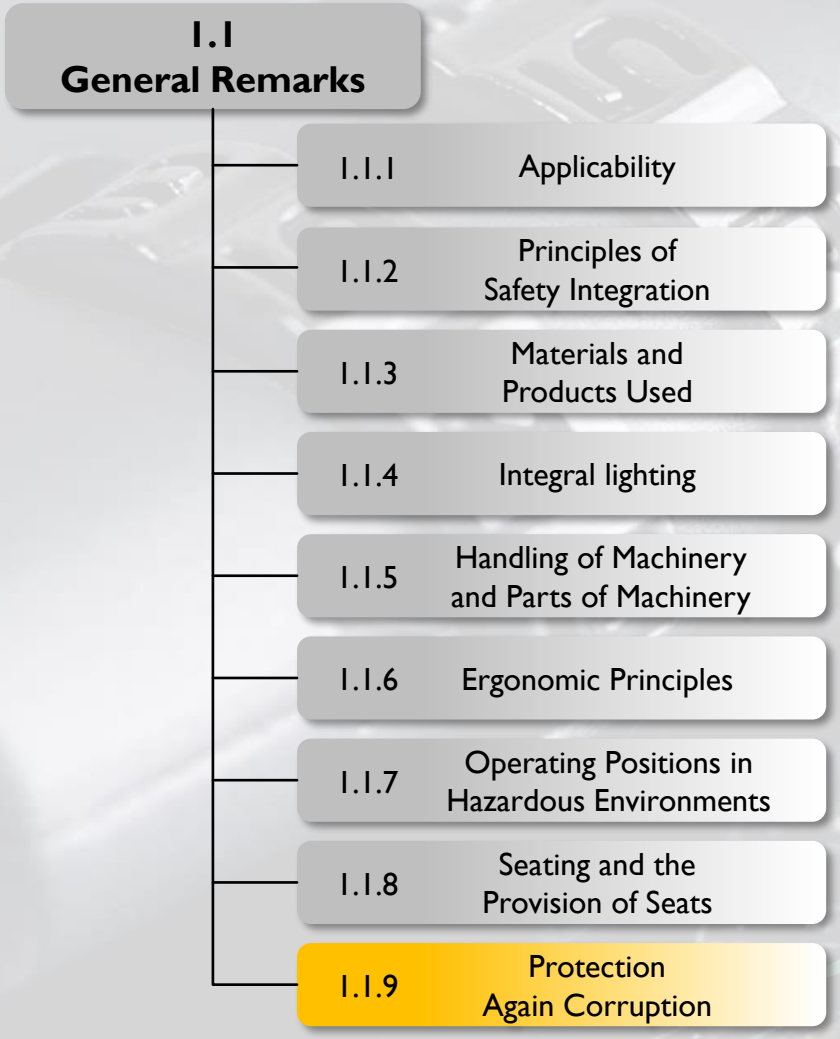
04

- Machinery Regulation

TECHNICAL CHANGES

New addition to MR

- **Machinery Regulation: ESR's – Annex III (Chapter 1)**



- Machinery must be designed to prevent hazardous situations when connected to other devices, whether **directly or remotely**.
- Hardware components that **transmit safety signals or critical data** must be protected against accidental or intentional corruption.
- **Safety-critical software and data must be clearly identified** and protected from corruption.
- The machinery must always be able to identify and provide information about the **software related to safety**
- Evidence must be collected of any legitimate or illegitimate **intervention or modification of the software or its configuration.**

TECHNICAL CHANGES

New addition to MR

- **Machinery Regulation: ESR's – Annex III (Chapter 1)**

1.2 Control Systems

- 1.2.1 Safety and Reliability of Control Systems
- 1.2.2 Control Devices
- 1.2.3 Control of Starting
- 1.2.4 Stopping
- 1.2.5 Mode Selection
- 1.2.6 Failure of the Power Supply or Communication Network Connection

- The control system is designed and constructed in such a way that it can withstand
  - **Intended and unintended** external influences
  - **Malicious attempts** from third parties leading to a hazardous situation
- The limits of the safety functions are to be established as a part of risk assessment
- Modifications to the settings of the machinery must prevent hazardous situations
- **Failures in wireless control communication** shall not lead to a hazardous situation
- Control systems with **self-evolving behaviour or logic** must be designed to stay within defined operational limits, ensure traceability of safety-related decisions for one year, and allow corrections to maintain inherent safety.

05

- prEN 50742 Protection against corruption (TC 44X)

prEN 50742 PROTECTION AGAINST CORRUPTION (TC 44X)

- **Overview of the standard**

Standard still in development by CENELEC's Technical Committee 44X

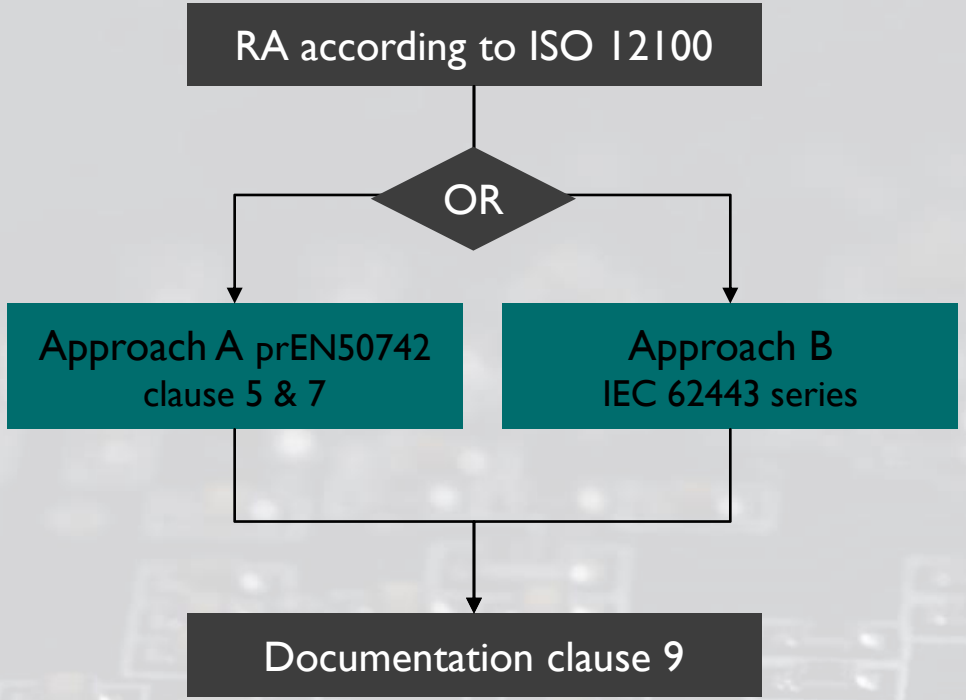
Scope

- Standard defines requirements and recommendations for protection against corruption (accidental and unintentional) for machinery, related products and partly completed machinery. The standard applies to hardware software and data that can influence the safety of machinery

The standard is intended to be harmonized for the MR **(EU) 2023/1230 – Annex III, 1.1.9.,** and associated requirements of **Annex III, 1.2.1.**

Note 1: Topics can overlap with the domain of cybersecurity but are not necessarily identical in their coverage.

Note 2: This standard does not cover the safety of control systems in machinery.



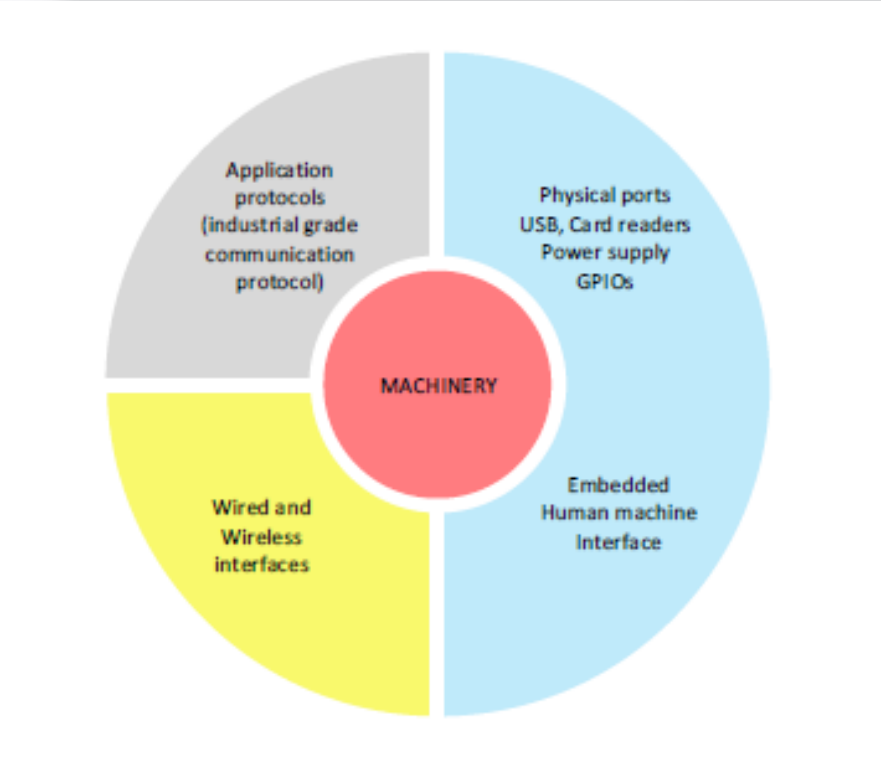
prEN 50742 PROTECTION AGAINST CORRUPTION (TC 44X)

Approach A

Safety-related Security levels

- SRSL0 completely isolated safety system
- SRSL1 low level of an attack potential
- SRSL2 moderate level of an attack potential
- SRSL3 significant or critical level of an attack potential

Annex A provides an informative approach to define the SRSL by means of a threat assessment



Security protection requirements

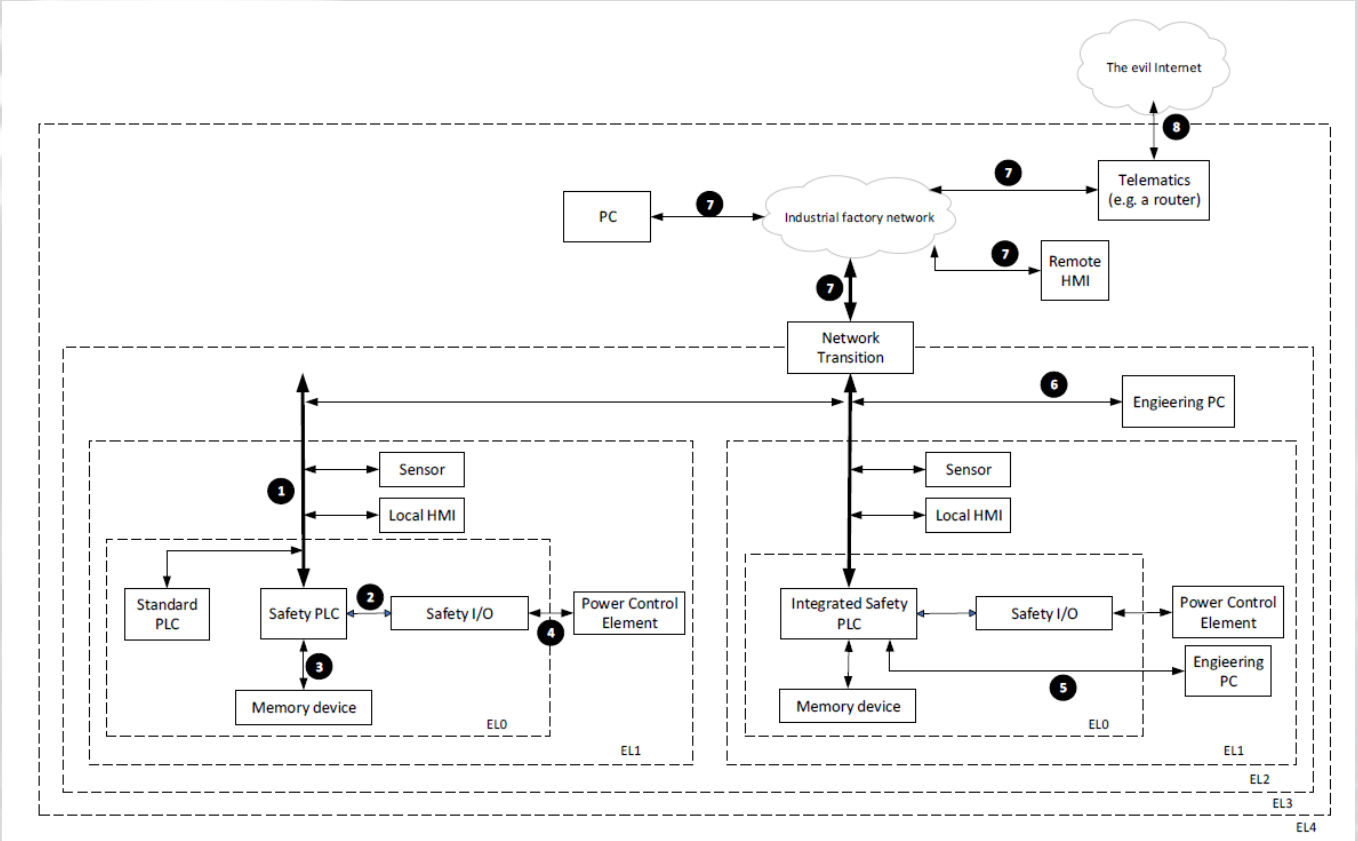
- Depending on the SRSL
- Aligned with the FR of IEC 62443

		Attack Potential (AP)	AP= (EL*WoO) +AC			
		AP0	AP1	AP2	AP3	AP4
Severity Level	low/e.g. reversible	SRSL0	SRSL1	SRSL1	SRSL2	SRSL3
	high/e.g. non reversible	SRSL0	SRSL1	SRSL2	SRSL3	SRSL3

prEN 50742 PROTECTION AGAINST CORRUPTION (TC 44X)

Approach A - Exposure Levels

- **EL 0 Complete trusted environment**
- EL 1 Physical access to a trusted environment
- EL 2 Local OT network access for production control
- EL 3 Extended industrial factory network
- EL 4 Remote connection with an untrusted network



prEN 50742 PROTECTION AGAINST CORRUPTION (TC 44X)

Approach B

Process

- EN IEC 62443-4-1:2018, shall apply

Product

- Machinery systems shall comply with EN IEC 62443-3-3:2019/AC:2019
- Machinery components shall comply with EN IEC 62443-4-2:2019/AC:2022

ICE 62443 Standard Series

General		OT Security Management System		Requirements IACS / Risk Analysis		IACS Components		Profiles		Evaluation	
1-1	Terminology, concepts and models	2-1	Requirements for a Security Program	3-1	Security technology for IACS	4-1	Requirements for the product development	5-1	In Progress	6-1	Methodology for security assessment - 2-4
1-2	Glossary of the terms and abbreviations	2-2	Operation of an IACS Security Program	3-2	Security risk evaluation and system design	4-2	Technical requirements for IACS components	5-2	In Progress	6-2	Methodology for security assessment - 4-2
1-3	Metrics for Compliance with system security	2-3	Patch Management in IACS handling	3-3	System Security requirements and Levels						
1-4	ICS security lifecycle und use-cases	2-4	Requirements for providers of IACS solutions								
1-5	Scheme for cyber security profile	2-5	Implementation guide IACS asset owner								
1-6	Application of the IEC 62443 standards to the IIoT										

06

- Cyber Resilience Act (CRA)

CYBER RESILIENCE ACT (CRA): WHAT OEMS MUST KNOW

- Essential Requirements (ERs) - Annex I

Incident Prevention Design Principle	Incident Readiness Resilience	Incident & Vulnerability Handling
Integrity and confidentiality of data	Impact reduction in case of an incident	Coordinated disclosure process (share and publicly disclose information about fixed vulnerabilities)
Secure by default configuration	Minimise the negative effect on other services	Remediate vulnerabilities without delay (Security updates: fast, free, automated, through a secure distribution channel)
Availability of essential functions	Logging	Apply effective and regular tests and reviews of the security of the product with digital elements
Access control and authentication	SBOM	
Hardening (attack surface, data use)		

Note: ERs will be detailed in harmonised standards (EN)

CYBER RESILIENCE ACT (CRA): WHAT OEMS MUST KNOW

- **Risk–Based Product Classification – Annexes III & IV**

Category	Products Examples	Requirement	Assessment
Default category	All digital products, including consumer devices, connected hardware, and software.	Security design, no known exploitable vulnerabilities, timely security updates	Module A
Important – Class 1 (Annex III)	Products critical to cybersecurity or carrying significant risk, such as identity management systems, VPN's, routers, and operational systems.	Same as default category products, plus stricter conformity assessment	If harmonised standard: Module A Otherwise: Modules B+C
Important – Class 2 (Annex III)	Higher-risk cybersecurity tools like IoT Gateways, firewalls, intrusion detection and prevention systems	Same as class 1, but requires third-party conformity assessment	Modules: B+C, or H or cybersecurity certification
Critical (Annex IV)	High-impact products that, if compromised, could disrupt or control essential systems and infrastructure. This included hardware devices, with security boxes, smartcards, smart meter gateway	Strictest cybersecurity requirements. May require European cybersecurity certification	Modules: B+C, or H or European cybersecurity certification

CYBER RESILIENCE ACT (CRA): WHAT OEMS MUST KNOW

- Obligations for OEMs

EU Declaration of Conformity

Formal declaration of conformity with Essential Requirements

Conformity Assessment Procedure
Annex VIII

Internal Assessment
Module A

Third-party Assessment
Module B+C, Module H or
EU cybersecurity certificate

Technical Documentation

Reports of tests carried out to verify conformity

Design, development and production process

Vulnerability handling process

Cybersecurity risk assessment

Cybersecurity solution

Instruction to the User

Excerpts from Technical Documentation

- Intended purpose
- Essential functionalities

- Support period, point of contact
- How to install updates
- SBOM (if Applicable)

- Foreseeable circumstances, misuse or changes leading to risk

- Security properties & environment
- Secure use and (de-) commissioning
- Information to the integrator

RESPONSIBILITIES

Cyber Resilience Act: Shared Responsibility in Industrial Cybersecurity

OEM – Sole Legal Responsibility

- Must ensure secure design, development, and vulnerability handling
- Required to provide updates and documentation throughout product lifecycle

End User – Critical Operational Responsibility

- Must install, configure, and maintain products securely
- Responsible for applying updates and managing lifecycle use
- Is responsible to determine the Business Processes (BP)

- Without active end-user involvement, the systems become vulnerable
  - Poor practices (e.g. ignoring updates, misconfiguration) weaken security
  - CRA assumes secure use under "reasonably foreseeable conditions"

- Security by design is not enough – Security by deployment is essential
  - Industrial security requires collaboration between manufacturer and user

ALIGNING CRA & MR

- **Coordinated Compliance Between CRA and MR**

Key message: CRA Recital 53 confirms the dual requirement:

- Machinery must be CE marked under MR for safety
- Digital elements must be CE marked under CRA for cybersecurity

Manufacturers should demonstrate the synergy between these regulations:

a) Through coordinated risk assessments covering both safety and cybersecurity
b) By using harmonised standards or technical specifications that address both sets of requirements – these standards are still under developing phase

However: CRA Article 7 allows reuse of CE marking for digital elements if already CRA-compliant and not modified during integration

Problem: How to document reused CE marking for digital elements is not yet standardized. Awaiting:

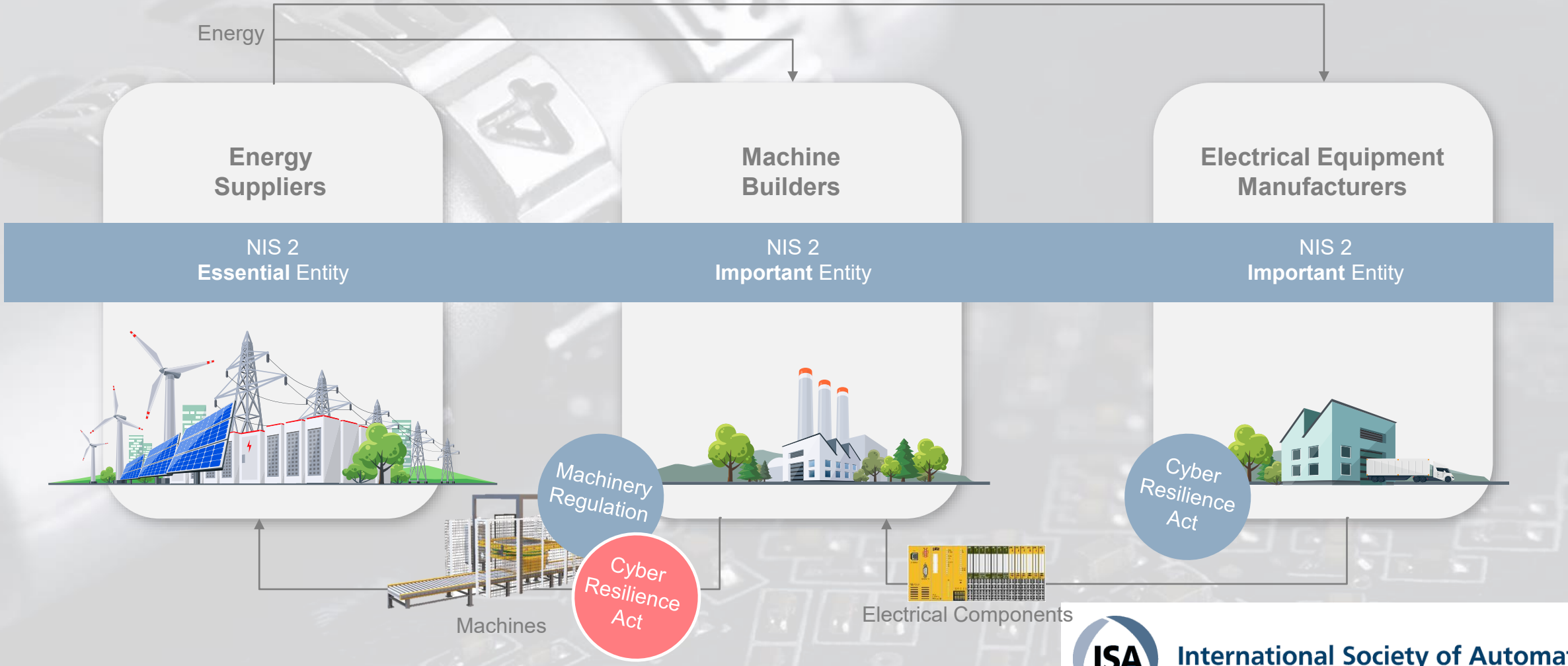
- Implementing acts by December 2025
- Guidance from the Commission
- Harmonised standards

07

- Use Case

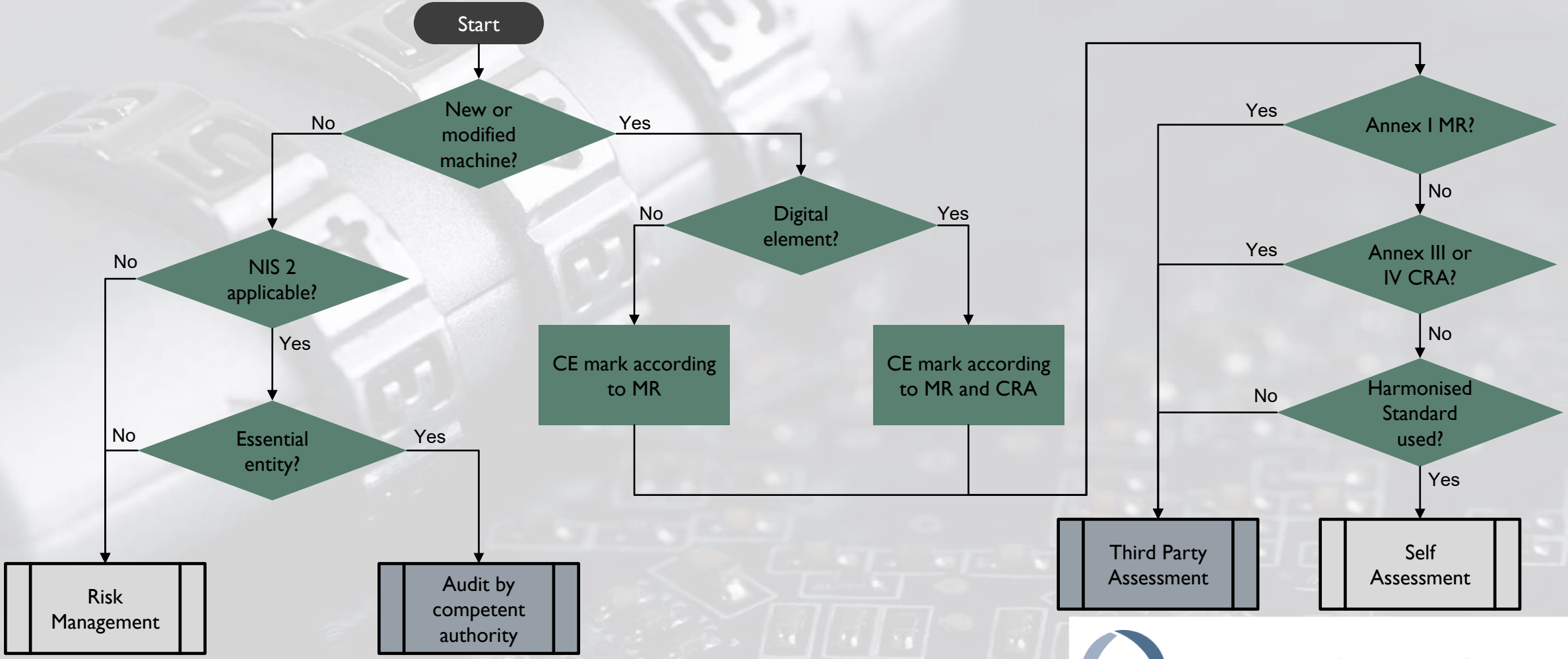
COMPONENTS TO COMPLIANCE: CRA, NIS 2 & MR IN ACTION

- **Correlation between Safety and Security Legislation**



DESIGN AND DOCUMENTATION UNDER NEW REGULATIONS

- **Safety and Security Procedure Assessment**



Thank You