Geo-Politics, Hybrid Threats, *prime target:* **Control Rooms……**



SIEMENS


Let me take you to Ukraine 2015
SIEMENS



SIEMENS

"

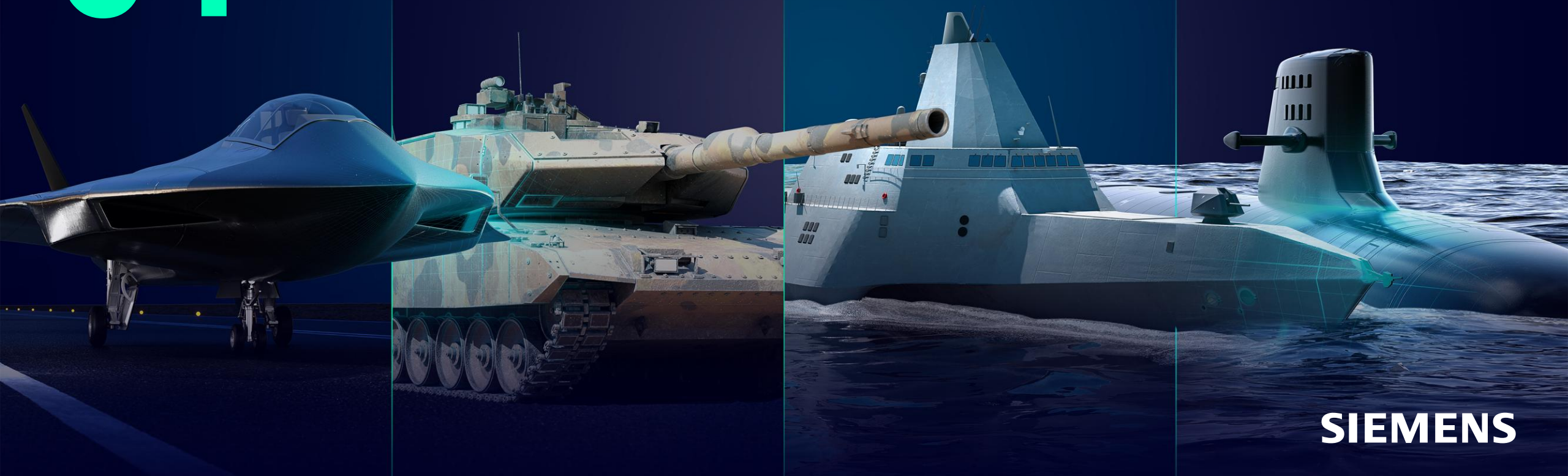
We expected them to do exactly what the U.S. military would have done, which is spend the first 24 hours taking out the command-and-control system and taking out the air defense system.

Quote from William J. Burns, former Director of the CIA, shortly after the Russian invasion of the Ukraine

SIEMENS

CHAPTER

01 Siemens



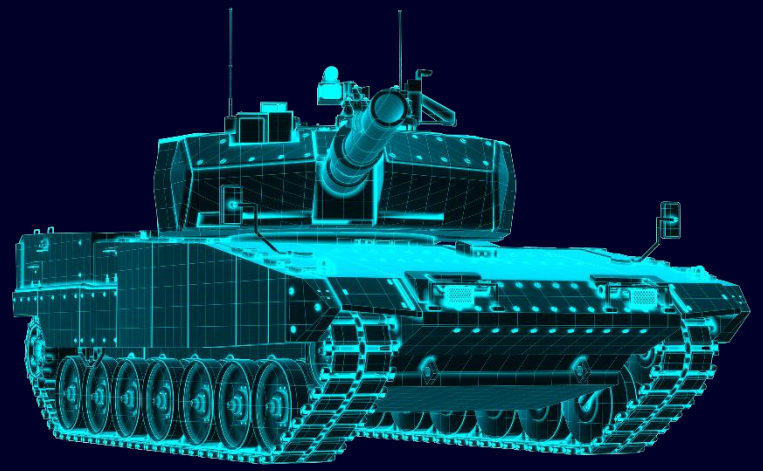
SIEMENS



As a trusted partner to the aerospace and defense industry, Siemens technologies support the entire value chain

… from design and simulation through to production …





… with an integrated portfolio spanning the digital and physical worlds!

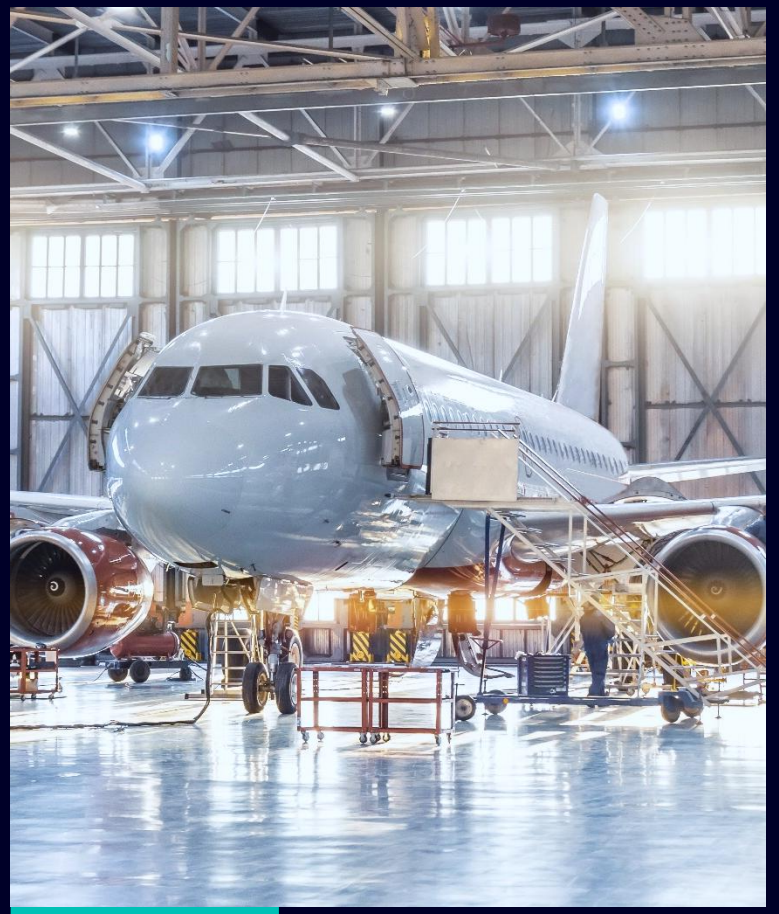
SIEMENS



We fly in aircraft developed with Siemens software …

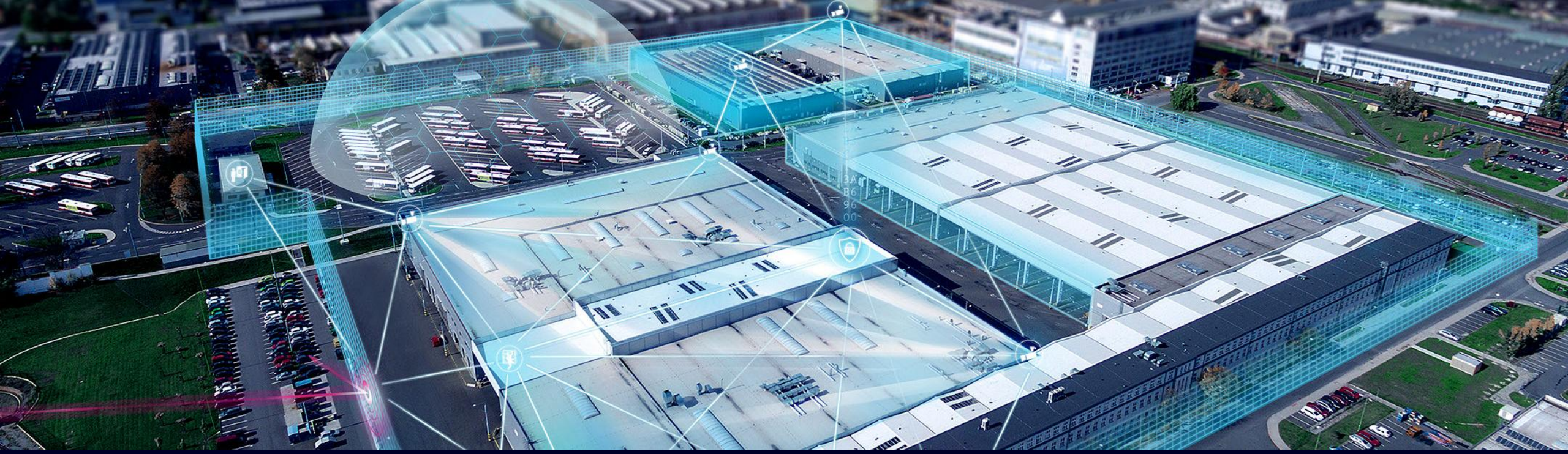
… powered by engines produced with Siemens automation …





… and assembled in factories optimized & protected with Siemens infrastructure solutions.

SIEMENS



One Integrated Security. All Domains.

Resilient defense sites to meet evolving security requirements

SIEMENS

The defense industry is security relevant and must be comprehensively protected!
Increasing threat scenarios appearing in combination





Complex threat scenarios

- Physical attacks
- Sabotage, Disinformation
- Drones
- Cybersecurity
- Industrial espionage
- Power cuts
- Hybrid threat situation/combination

Critical environment in Defense

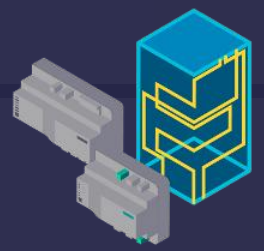
- Defense production facilities, logistics centers
- Military installations
- Research & Test Centers
- Maintenance and repair centers
- Command and Control Centers
- Airports

The threats are not abstract scenarios - they are real, present and have already caused concrete damage

SIEMENS

Siemens Smart Infrastructure Buildings: we are well positioned with a comprehensive portfolio

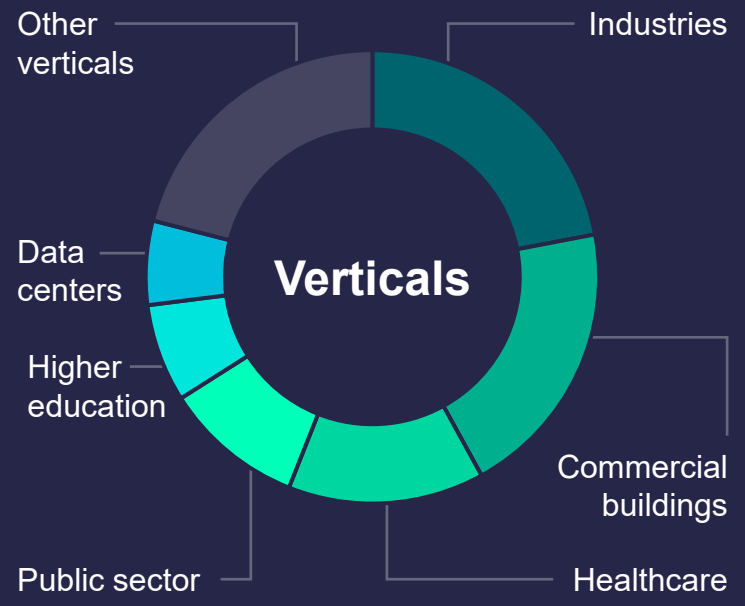
Business mix (FY24 revenue)

	Building automation	Fire safety	Security
Products 20%	• Analysis and optimization • Control • Sensors and actuators	• Detection • Alarm and evacuation • Suppression	• Access • Intrusion • Video • Mngt. Stations
Solutions 34%			
Services 46%			

Enabled by software

Broad and resilient verticals exposure

FY24 revenue



SIEMENS

To **improve your security operations**
you need to…



… look towards
a unified approach

SIEMENS

CHAPTER

02

Hybrid threats, Critical Infrastructure and Regulations



SIEMENS

Hybrid threats

The EU and its member states work together to prevent, counter and respond to hybrid threats and campaigns affecting Europe and its citizens.

Hybrid threats usually refer to coordinated **harmful activities that are planned and carried out with malign intent**. They aim to undermine a target, such as a state or an institution, through a variety of means, often combined. These means may include information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military force.

SIEMENS

Critical Infrastructure according to the NIS2 (Enisa)

Network & information Systems Directive (2023)

Critical Entities Resilience Directive (2023)



SIEMENS

NIS2 Directive

More requirements, more cooperation, more supervision



Supervision and cooperation

Stronger supervision and enforcement

More stringent oversight and sanctions, including fines for breaches of risk-management and reporting obligations.

Coordinated EU crisis response

EU coordinates large-scale incidents and crises, member States need to share more information

Coordinated vulnerability disclosure

EU-wide cooperation supports the disclosure of newly discovered vulnerabilities.

Cybersecurity risk management

Stronger security requirements

Incident response, crisis management, vulnerability handling and disclosure, cybersecurity testing and encryption.

Supply chains and management accountability

Stronger cybersecurity for key ICT supply chains. Company management is accountable for compliance with risk-management measures.

More precise incident reporting

Streamlined obligations specify the reporting process, content and timeline.

SIEMENS

Cyber Resilience Act (2027)

EU cybersecurity requirements for hardware and software



Manufacturer obligations

Security throughout the lifecycle

Build cybersecurity into planning, design, development, production, delivery and maintenance. Document all cybersecurity risks.

Vulnerability and incident management

Report actively exploited vulnerabilities and incidents. Handle vulnerabilities throughout the support period.

User guidance and security updates

Provide updates for the expected period of use.

Assessment routes

1 **Default category: 90% of products**

Self-assessment. Examples include photo editing, word processing, smart speakers and hard drives.

2 **Critical Class I**

Apply a standard or use third-party assessment. Examples include password managers and firewalls.

3 **Critical Class II**

Third-party assessment. Examples include operating systems, industrial firewalls and CPUs.

Critical Classes I and II together: 10% of products

SIEMENS

CHAPTER

03

Critical Infrastructure and Operational Technology



SIEMENS

Hybrid Threats, Critical Infrastructure, and Operational Technology



OT security must address **geopolitical threats** to **critical infrastructure** and **business operations.**

Operational technology (OT) has become a major target in geopolitical cyber conflicts. Organisations should align leadership responsibilities and resources, implement strong network segmentation, and achieve clear visibility across their environments.

Recent OT attacks (examples)

- US water and wastewater (September 2024): Attackers used basic tactics to exploit vulnerabilities in systems that provide essential services.
- Ukraine power grid (2024–2025): Cyberattacks disrupted power distribution and caused major outages, exposing energy infrastructure vulnerabilities.
- US substations (2023): Cyber intrusions targeted California and North Carolina, raising concerns about national electricity grid security.

SIEMENS

CHAPTER

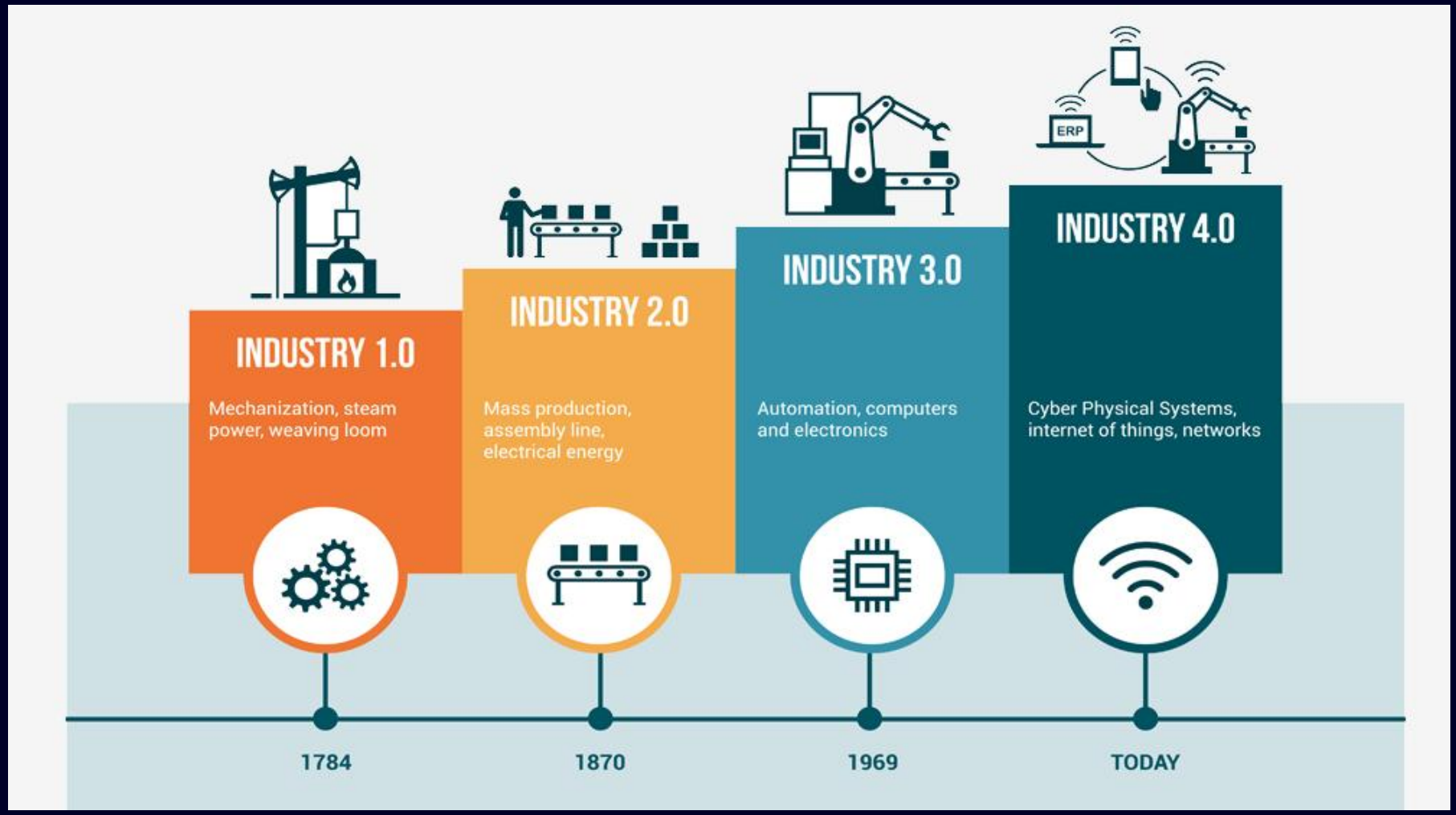
04

What is Operational Technology?



SIEMENS

Revolutions are only visible in retrospect…..



SIEMENS

The rise of Cyber - Physical systems



IT

Applications & Software

Cloud

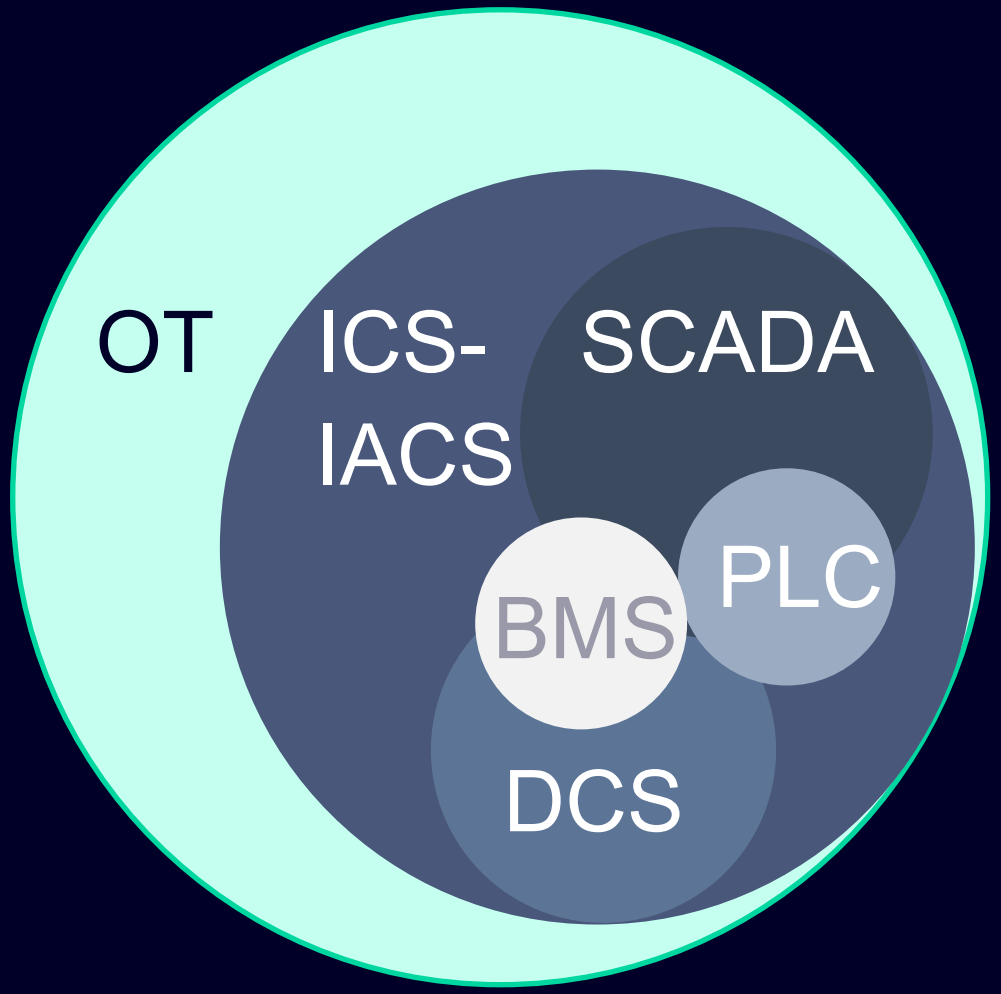
Edge Computing

Field devices, sensors …

OT

SIEMENS

ICS, OT, SCADA, PCS, DCS, IACS: Proces Automation

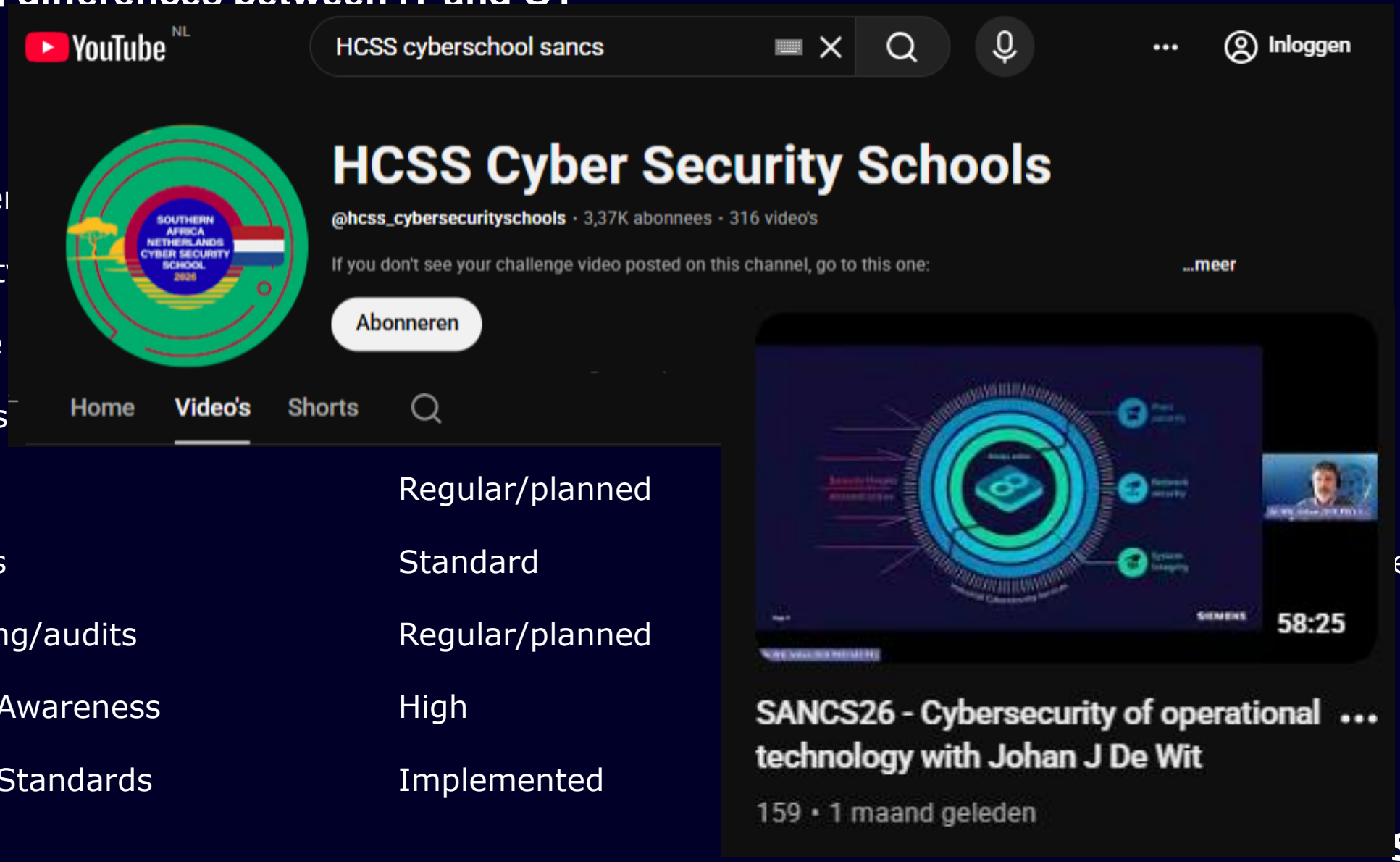


OT:	Operational Technology
ICS:	Industrial Control System
IACS:	Industrial Automation and Control System
SCADA:	Supervisory Control And Data Acquisition
DCS:	Distributed Control System
PCS:	Process Control System
PLC:	Programmable Logic Controllers
BMS:	Building Management System

SIEMENS

The main differences between IT and OT

Componer	
Availabilit	
Real time	
Physical s	
Patching	Regular/planned
Anti-virus	Standard
Sec.testing/audits	Regular/planned
Security Awareness	High
Security Standards	Implemented



SIEMENS

"Industrial Control Systems (ICS) and (office) IT have historically been managed by seperate organisational units."

The IT department is unfamiliar with the peculiarities and limitations of ICS technology."

"ICS people do not consider their ICS to be IT. ICS People lack cyber security education."

Referentie:
TNO for GCCS 2015, Cyber Security of Industrial Control Systems, 2015

SIEMENS

CHAPTER

05

Two recent (unfortunate) examples



SIEMENS

Cyberattack on supermarket refrigeration

Reported operational impact

Connected refrigeration systems in French supermarkets were manipulated to reach up to 50°C (122°F), causing fires and food spoilage.

Intermarché's parent group, Les Mousquetaires, reported about 150 affected stores, with units heated for six hours overnight.

Carrefour reported 80 affected supermarkets. Monoprix reported impacts at 5% of its approximately 490 French stores.

Research cited in the article

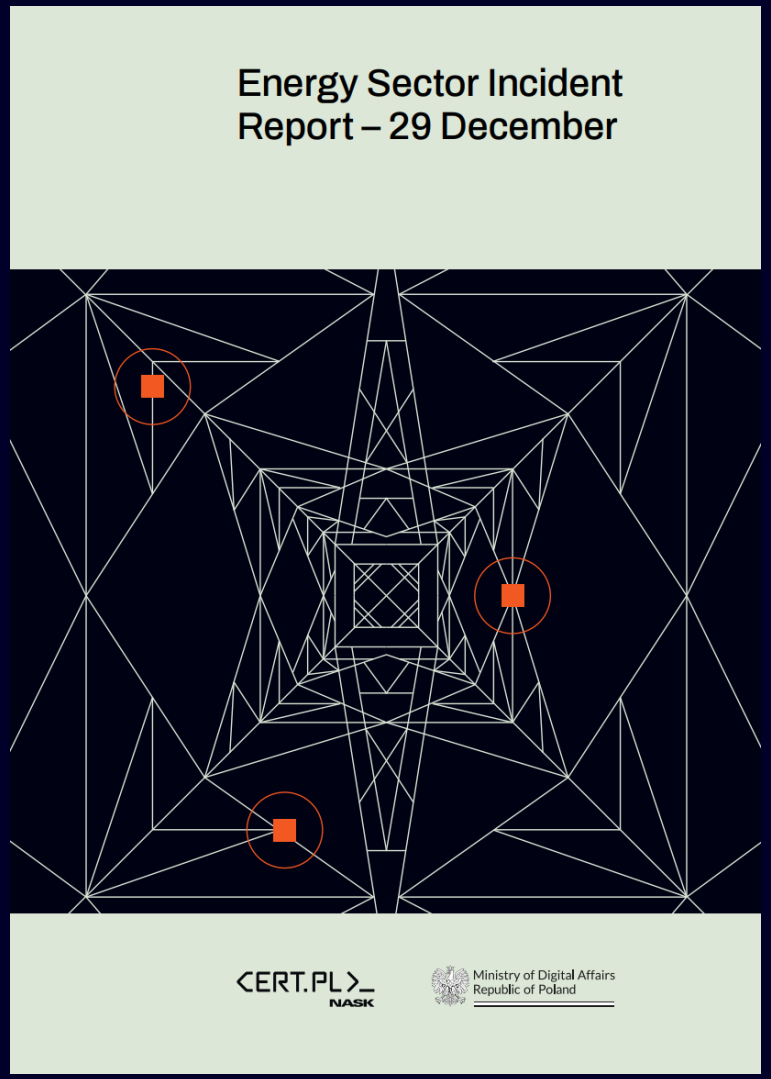
Refrigeration controllers are a target for disrupting critical operations and often escape security teams' attention.

The cited research found many controllers directly exposed to the public internet, despite assumptions that industrial control systems run on isolated networks.



SIEMENS

Who is to blame……..? > Installer, System Integrator?



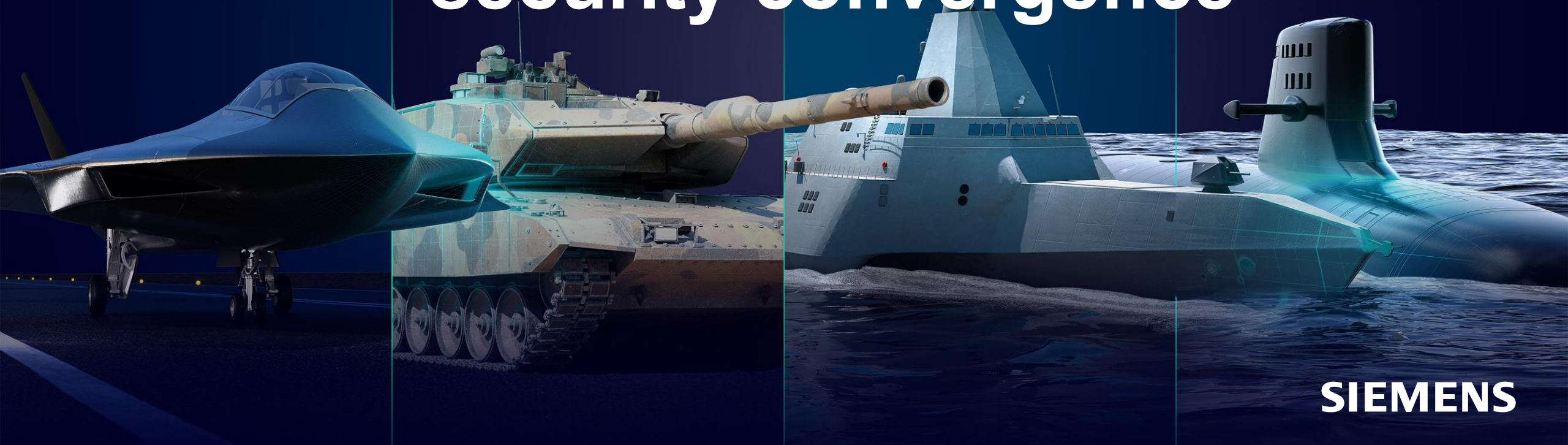
On 29 December 2025, during the morning and afternoon hours, coordinated attacks occurred in Poland's cyberspace. The attacks targeted numerous wind and solar farms, a private company in the manufacturing sector, and a combined heat and power (CHP) plant supplying heat to nearly half a million customers in Poland. All of the attacks were purely destructive in nature by analogy to the physical world, they can be compared to deliberate acts of arson.

SIEMENS

CHAPTER

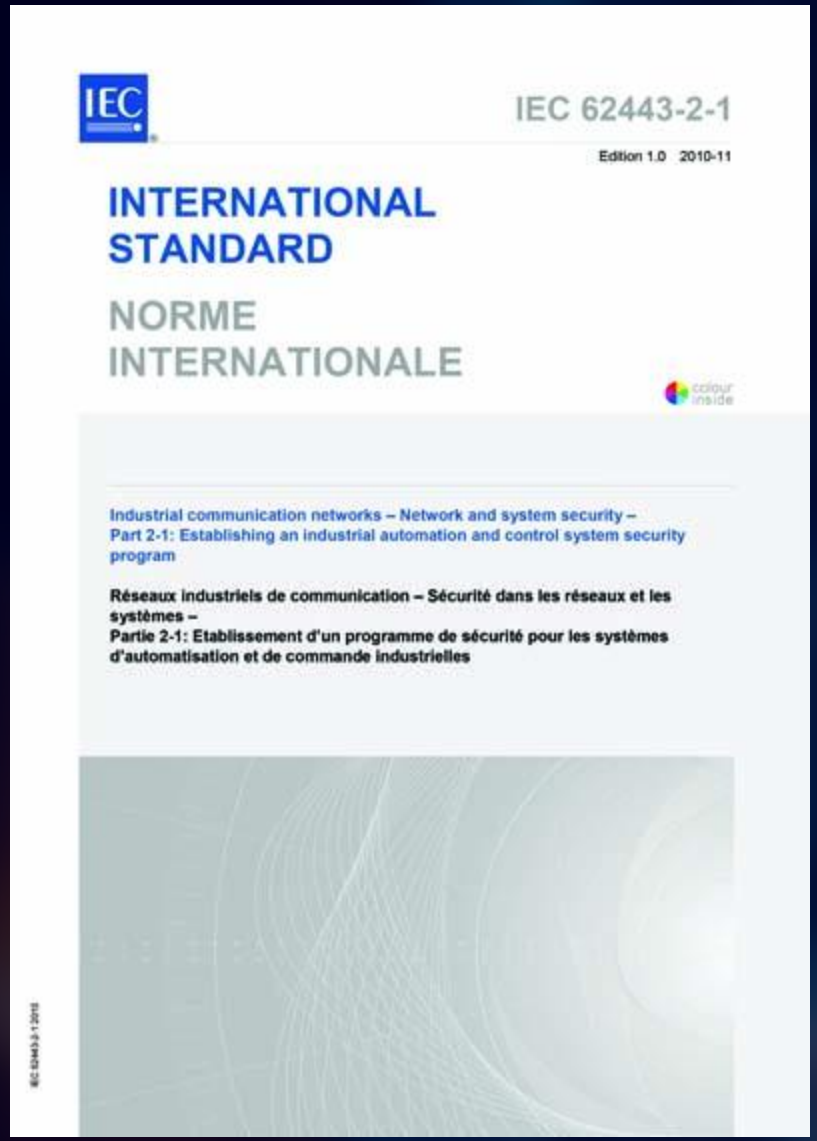
06

Two solutions: IEC 62443 & security convergence



SIEMENS

Standard IEC 62443



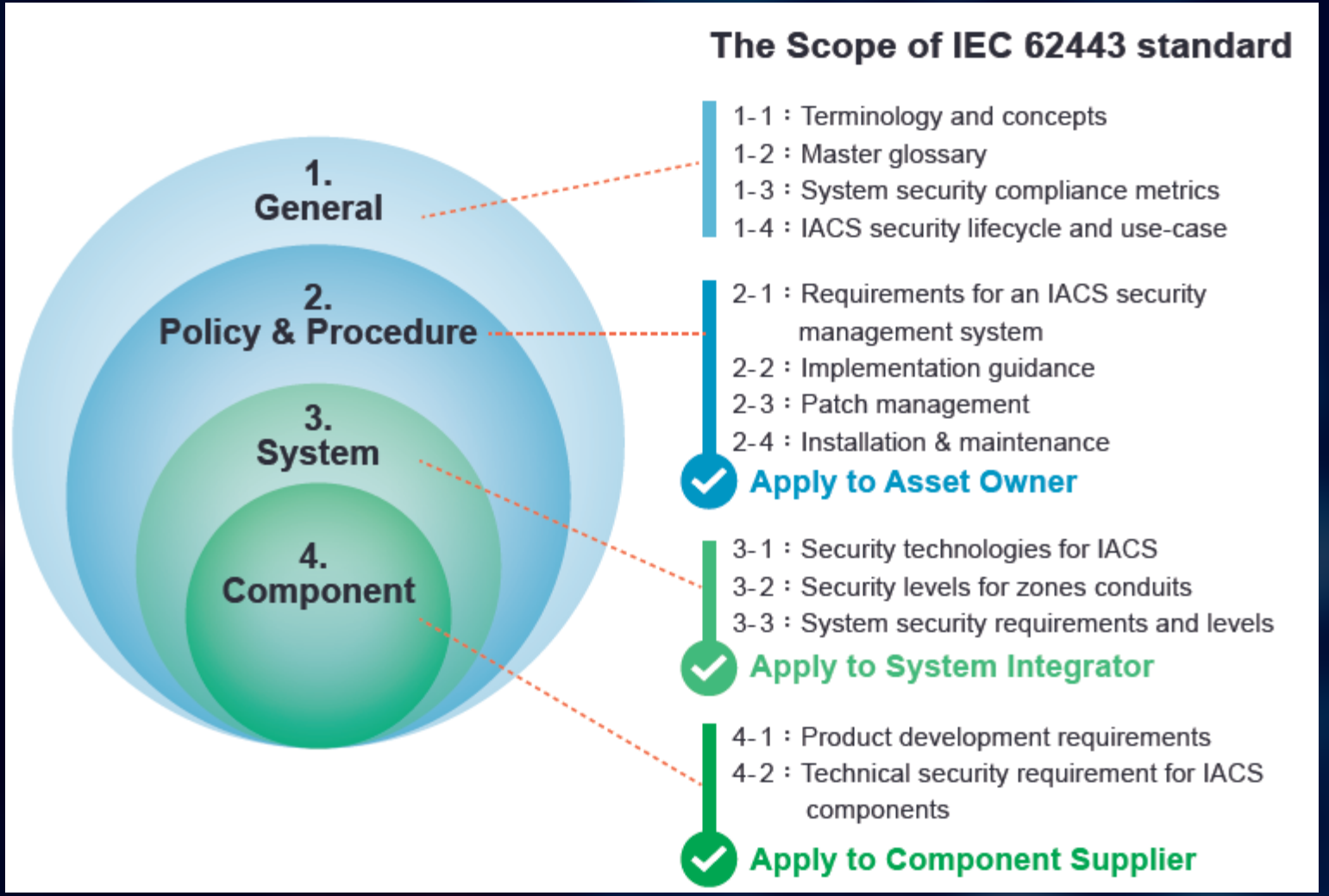
SIEMENS

IEC 62443

4 Security Level (SL)	
SL 1	Protection against **casual or coincidental** violation
SL 2	Protection against **intentional violation** using **simple means** with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using **sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with **extended resources**, IACS specific skills and high motivation

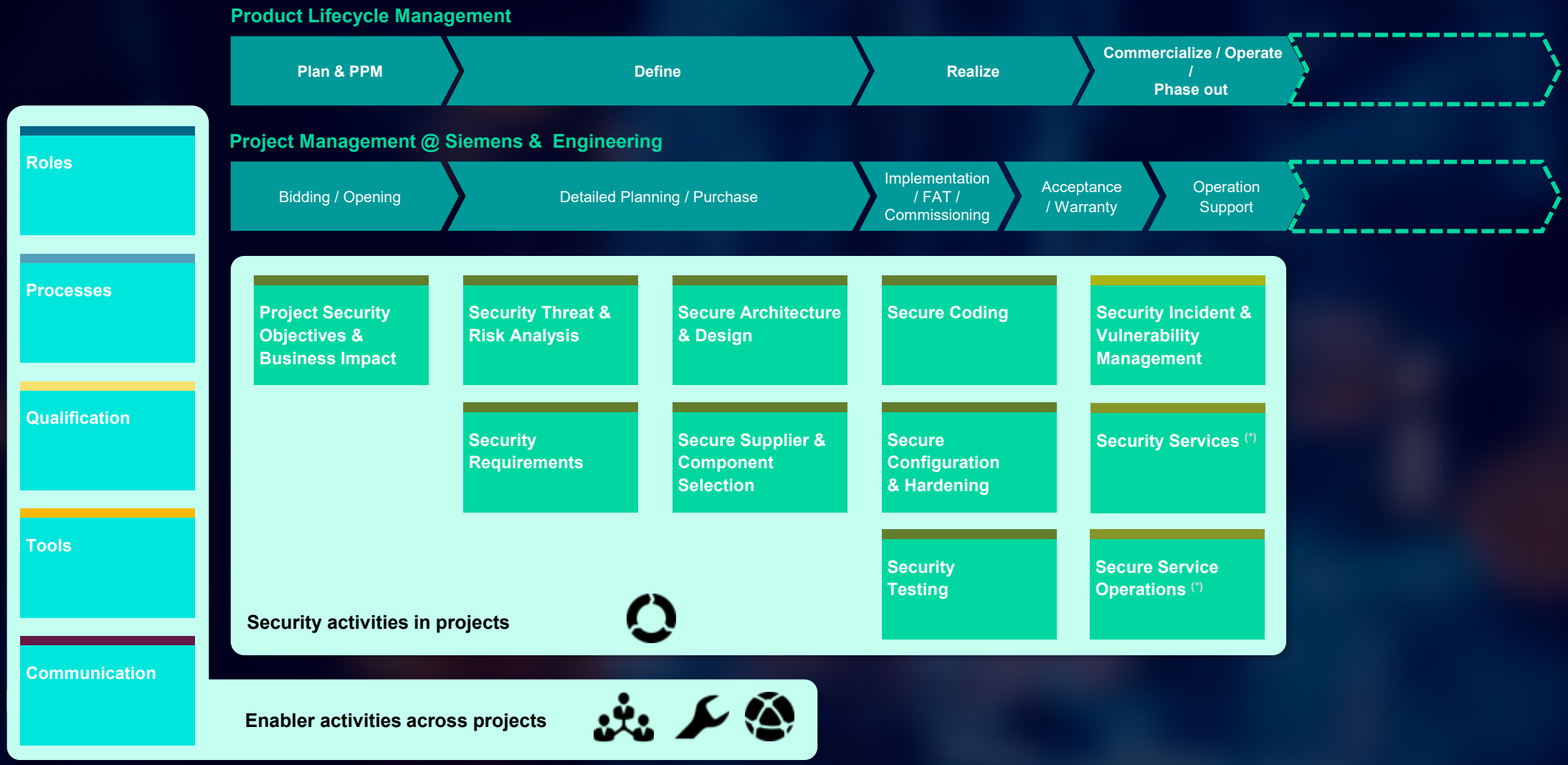
SIEMENS

IEC 62443

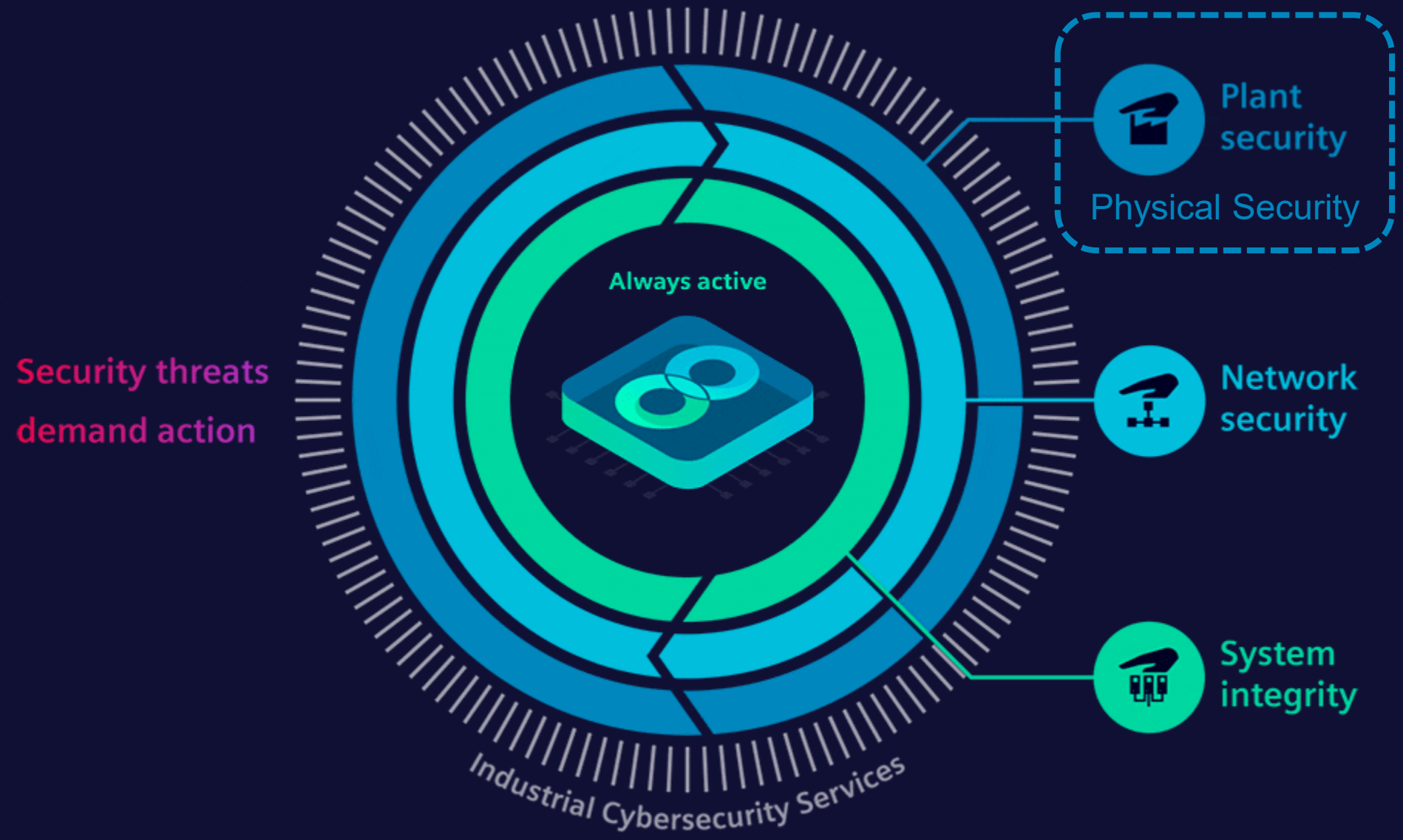


SIEMENS

Product & Solution Security Initiative (based on IEC 62443)



SIEMENS


Security threats
demand action
Always active
Plant
security
Physical Security
Network
security
System
integrity
Industrial Cybersecurity Services

SIEMENS

"

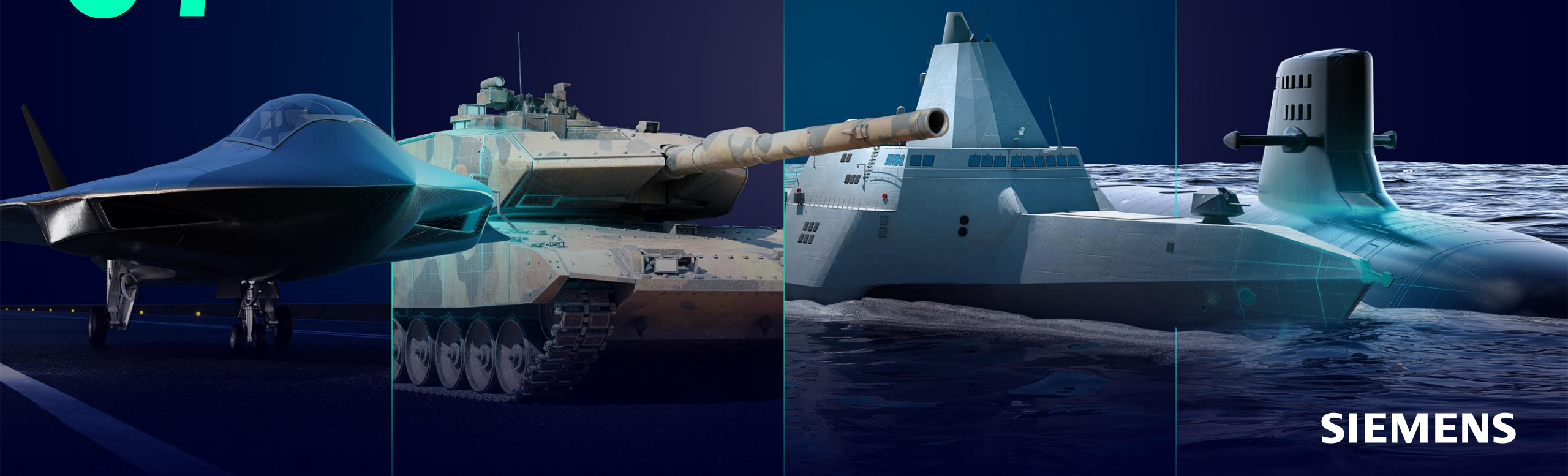
The measures shall be based on an **all-hazards** approach that aims to protect network and information systems and the **physical environment** of those systems from incidents.



SIEMENS

CHAPTER

07 Shifting frontiers & Closing



SIEMENS

Mass criticality

Rethinking critical infrastructure in the UK

“Ordinary” digital components can become critical infrastructure

Interdependence and concentration create bottlenecks whose failure can disrupt daily life and the economy.

Hybrid threats reach beyond military targets

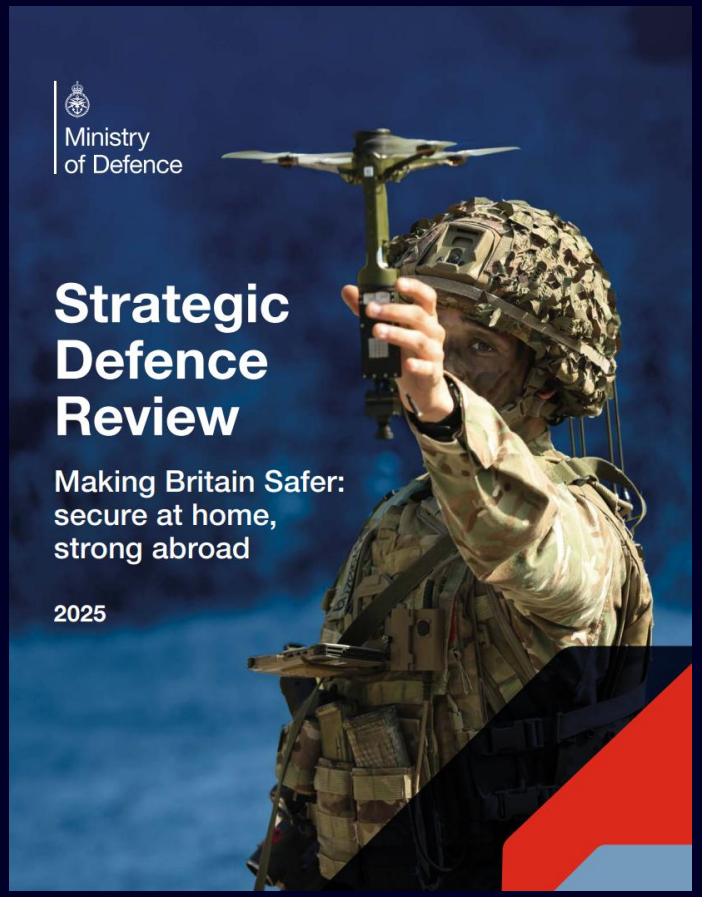
Remote cyber operations and local cyber-physical attacks, including insider-enabled activity, can disrupt civilian services.

Traditional definitions miss new dependencies

A focus on utilities such as electricity grids and power plants overlooks other critical bottlenecks. Fragile dependencies can cause major disruption even without malicious activity.

SIEMENS

Critical infrastructure security and renewal



A new partnership for CNI protection

Many critical national infrastructure (CNI) operators cannot address complex, evolving threats alone. The MOD and wider Government should explore a “new deal” with private-sector and allied operators to protect CNI and sustain essential UK services.

Infrastructure Recapitalisation Plan

The review requires the MOD to deliver a plan to the Secretary of State by February 2026, identifying opportunities to draw in private-sector expertise and capital quickly, and mechanisms to realise them urgently.

Five key takeaways

01 **Hybrid threats make control rooms a priority**

Control rooms contain the mngt software managing Operational Technology.

02 **OT security must protect safety and continuity**

OT is the central backbone of almost all critical processes yet often neglected in security policies.

03 **Regulation raises accountability across the lifecycle**

NIS2 strengthens governance and reporting. The CRA adds product security obligations.

04 **Secure deployment is as important as secure products**

Apply IEC 62443 across product design, security convergence ensures a holistic approach.

05 **Private critical infrastructure operators are now in the line of fire.**

Many are not equipped to meet these threats alone.

SIEMENS

Contact

Siemens Smart Infrastructure

Dr. Johan J. de Wit MSSM
Technical Officer Enterprise Security

Theiler Strasse 1a
Zug, Switzerland

E-mail: johan.de.wit@siemens.com



SIEMENS