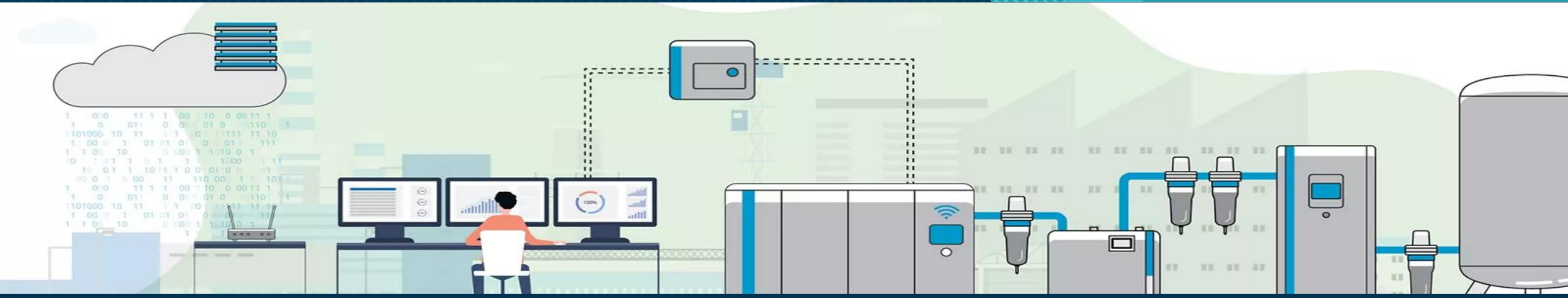
Cybersecurity in Industrial Control Systems

Challenges and Solutions in Industry 4.0

Giacomo Calabria – 17th June 2025

AGENDA



- Legacy vulnerabilities in ICS
- Modern threats and attack vectors
- Case study: the *Industroyer* malware
- Defensive strategies and future directions

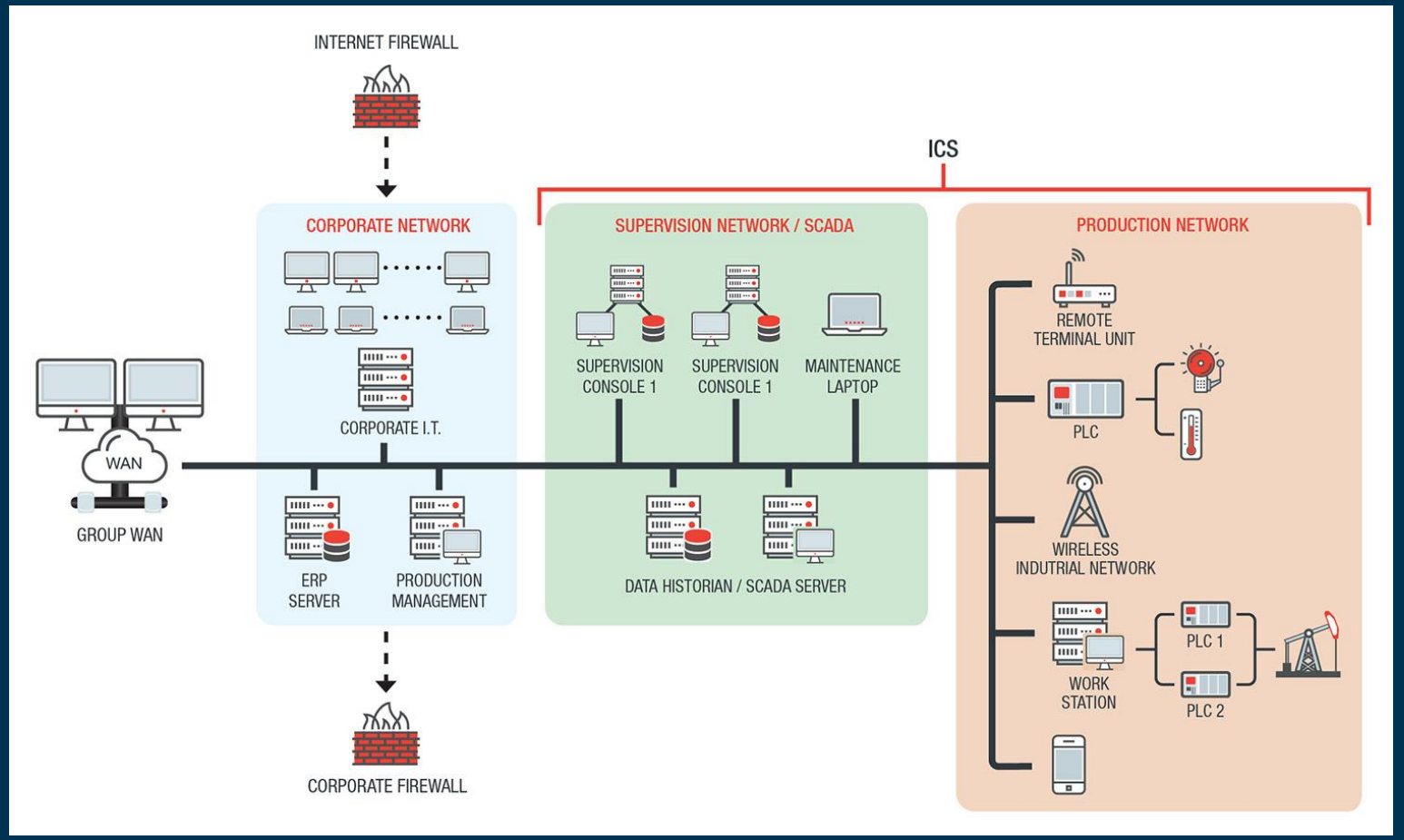
Why ICS are vulnerable ?

From Isolation to Exposure: Why ICS are now a target

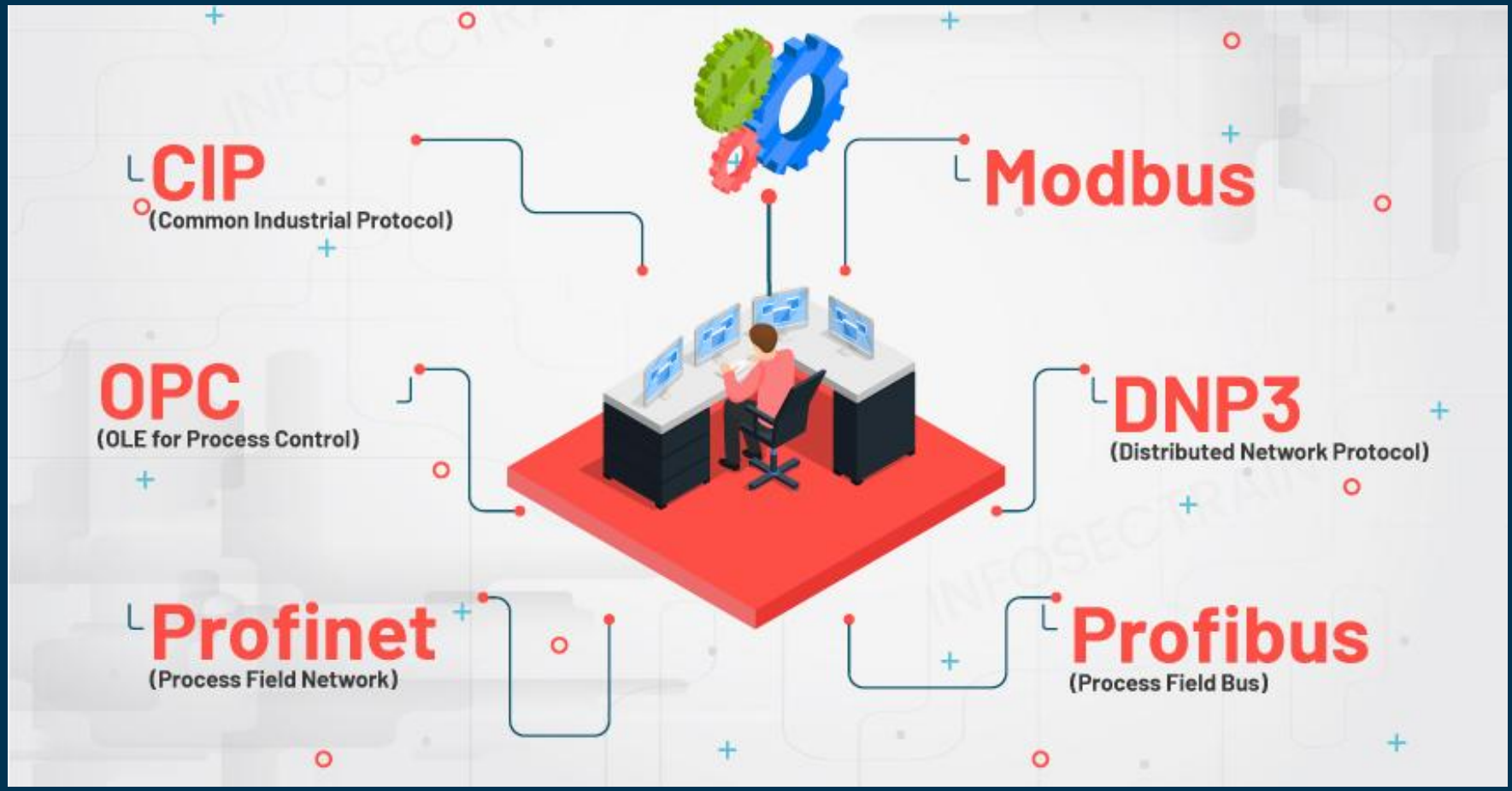
Vulnerabilities in ICS

ICS were designed for reliability, not cybersecurity	Built for closed, isolated environments ("air-gapped") Prioritised deterministic control and uptime
Industry 4.0 breaks this isolation	Integration with cloud, IT networks, IIoT devices Increased interconnectivity introduces new threat vectors
ICS control critical infrastructure	Energy, manufacturing, water, transport — highly sensitive
Modern cyberattacks now target physical operations	With real-world consequences (e.g., blackouts, safety failures)

Modern ICS architecture



Industrial Control Systems protocols



Modern Threat in Industry 4.0

Industrial IoT = More entry points	Smart sensors, mobile apps, remote access interfaces
Cloud and AI = Data centralisation, new risks	Data in transit, shared computation, and cloud misconfigurations
Mobile devices in OT networks	Often unmanaged endpoints with weak controls
Supply chain threats	Vulnerable third-party firmware and embedded components
Adversarial Machine Learning	ML models in ICS can be misled or poisoned

ICS Then vs. Now

Legacy ICS (Pre-Industry 4.0)

- Isolated, air-gapped systems
- Designed for reliability and uptime
- Plaintext protocols (Modbus, DNP3, Profibus)
- Static firmware, rarely patched
- No authentication or encryption
- Physical-only access control
- Security by obscurity

Modern ICS (Industry 4.0)

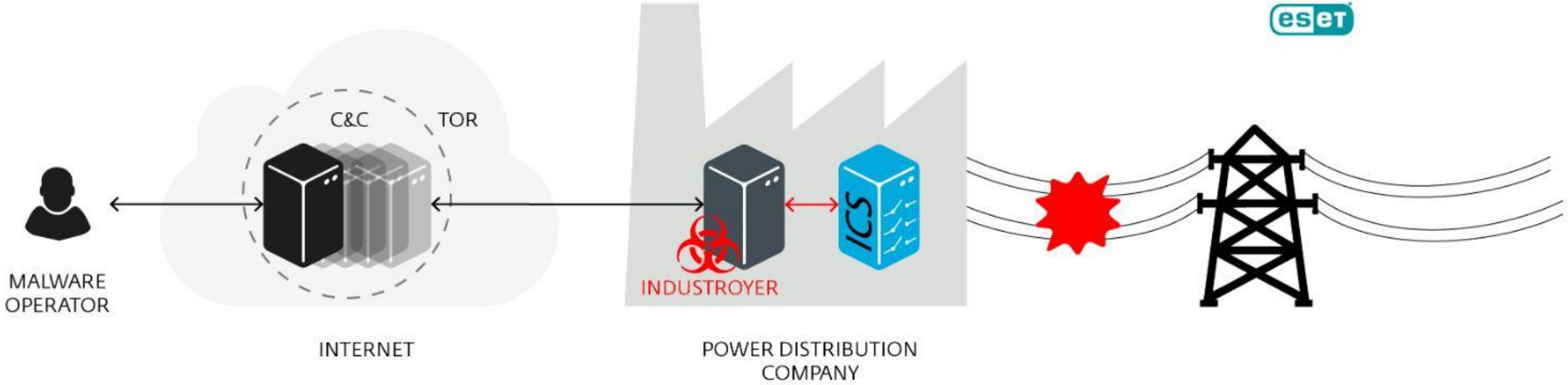
- Integrated with IT, Cloud, and IIoT
- Expected to be smart, connected, and adaptive
- Mixed protocols with partial or no hardening
- Dynamic, software-driven logic and updates
- Growing need for identity, trust, segmentation
- Remote access, mobile management tools
- Requires formal threat modelling and monitoring

Case Study: Industroyer

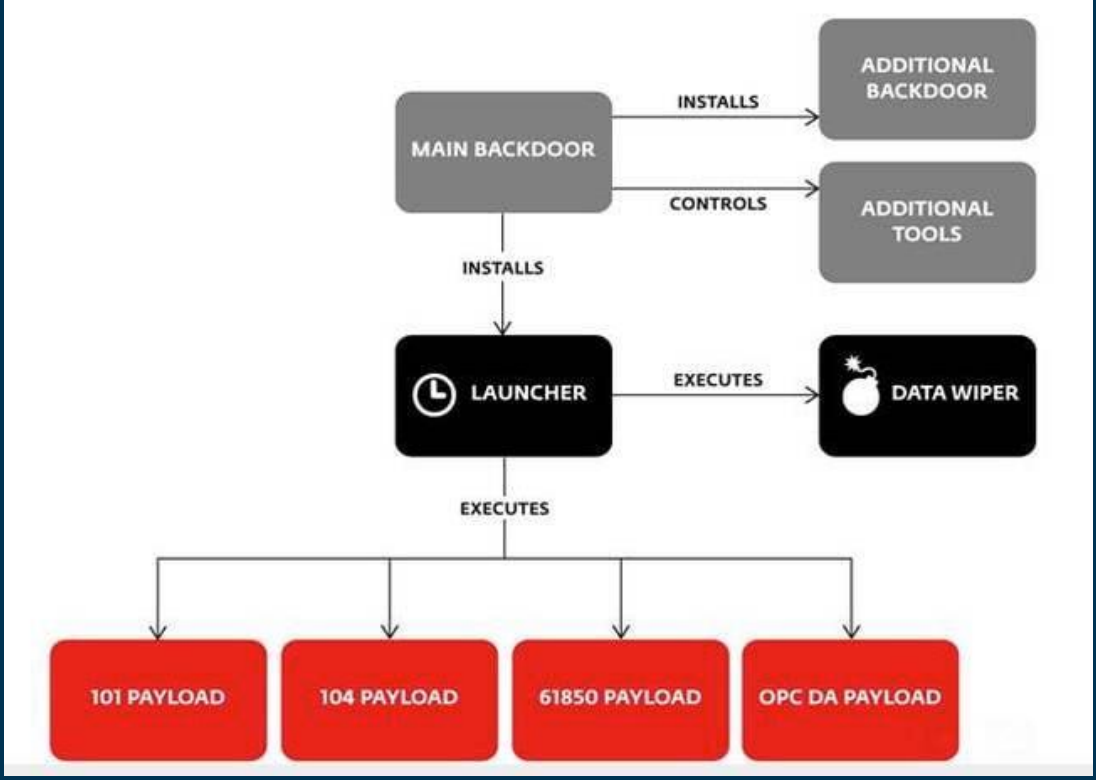
Industroyer in bullet points

- **Discovered**: June 2017 by ESET and Dragos
- **Target**: Ukrainian power grid (December 2016 outage)
- **Modular malware** with protocol-specific payloads: IEC-101, IE-104, OPC DA, IEC-61850
- **Protocol-aware**: Did not exploit vulnerabilities, but used legitimate functions to control substations
- **Included components**: backdoor, launcher, payload modules, DoS tool
- **Impact**: Power loss in Kyiv, ~1 hour
- **Limited global spread**, but demonstrated proof of concept for grid disruption

High-level architecture of Industroyer



Industroyer's Execution Chain



1. **Initial access via backdoor**
   Delivered through spear-phishing or unsecured access
2. **Launcher activates payload modules**
   Each module targets a specific industrial protocol
3. **Payloads send control commands to substations**
   Legitimate but malicious commands (e.g., open breakers)
4. **Denial-of-service (DoS) tool wipes traces**
   Clears system logs and disables recovery
5. **System blackout achieved**
   Power grid segment is disrupted without physical damage

Lessons Learned and Persistent Risks

Network segmentation
Limit lateral movement between IT and OT zones

Protocol-aware monitoring (ICS-specific IDS)
Detect misuse of IEC-104, OPC, etc.

Allowlisting and access control
Only authorised commands/devices allowed

Incident response planning
Preparedness for targeted ICS attacks

Unidirectional gateways
Prevent command injection into critical systems

Why It Still Matters?

- Same vulnerable protocols are still in use
- Modular, protocol-aware malware is replicable
- Threat actors now better funded and coordinated
- Growing convergence (IT/OT, Cloud, IIoT) → more entry points
- Successor malware likely (e.g., Industroyer2, CrashOverride)

Modern ICS Defence Strategies

Rethinking ICS security after Industroyer

Modernising ICS Security in a Hyperconnected World

Network segmentation & zoning (e.g., Purdue Model)	Isolates critical assets, limits propagation of attacks
AI-powered intrusion detection systems (IDS)	Behavioural models detect protocol misuse & anomalies
Legacy hardening via virtual patching	Filters/blockers compensate for unpatchable firmware
Identity and Access Management (IAM)	Role-based control, time-bound access, multi-factor auth
Zero Trust Architecture	No implicit trust — every access is verified & contextual
Compliance with ICS standards	IEC 62443, NIST SP 800-82 guide secure architectures

Secure-by-Design & Industry 5.0

Secure-by-Design Principles

- Security embedded at hardware, firmware, and software levels
- Follows principles like:
  - **Least privilege**
  - **Defence in depth**
  - **Fail-secure defaults**
- Standards: **IEC 62443-4-1**, **IEC 62443-4-2**, **NIST SP 800-82**

Industry 5.0 Perspective

- Human-machine collaboration & ethical technology use
- Cybersecurity expands to include:
  - Transparency in AI-driven decisions
  - Security in decentralised, edge-based systems
  - Sustainability and societal resilience
- Emphasis on **trust, adaptability, and safety**

Key Takeaways:
Securing the Unsecurable

ICS were never built for today's threats
→ Security must be added without breaking functionality

Industry 4.0 expands the attack surface
→ Cloud, IIoT, AI, mobile = new vectors

Industroyer proved disruption is possible
→ Real-world ICS attacks are no longer theoretical

Layered defence and visibility are essential
→ Segmentation, monitoring, IAM, Zero Trust

Secure-by-Design is the long-term vision
→ Industry 5.0 needs trust, transparency, and resilience

Thank you