Could standardization break the silos approach in Critical Infrastructure Protction?

ECSCI Workshop
Google Meet, 24-25. June 2020

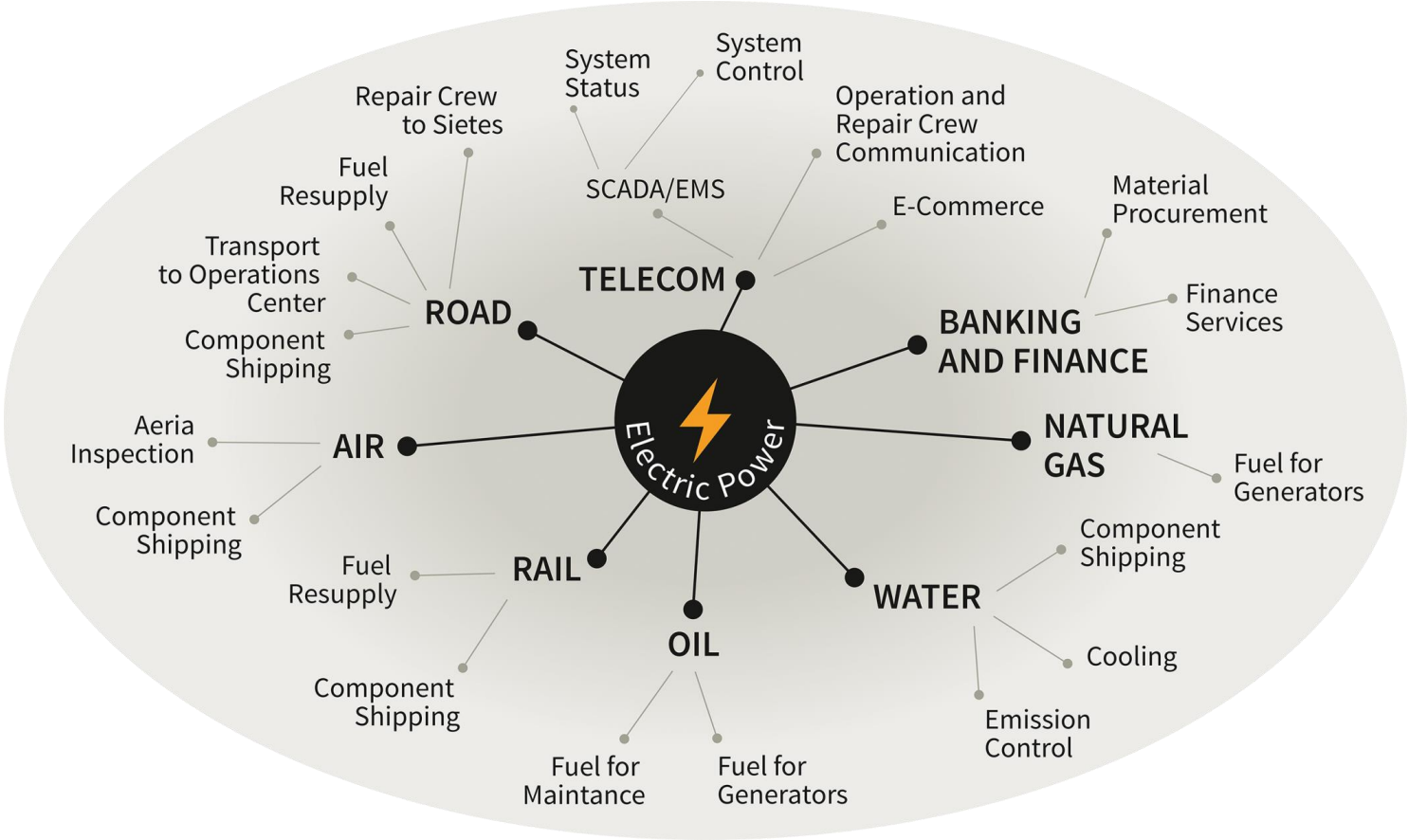
Dr. Denis Caleta
President of the Board
Institute for Corporative Security Studies (Slovenia)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 740898

While recognising the threat from terrorism and cyber attacks as a priority, the protection of critical infrastructure will be based on **an all-hazards all-sectors approach**.

Critical Infrastructures depend on each other, but…

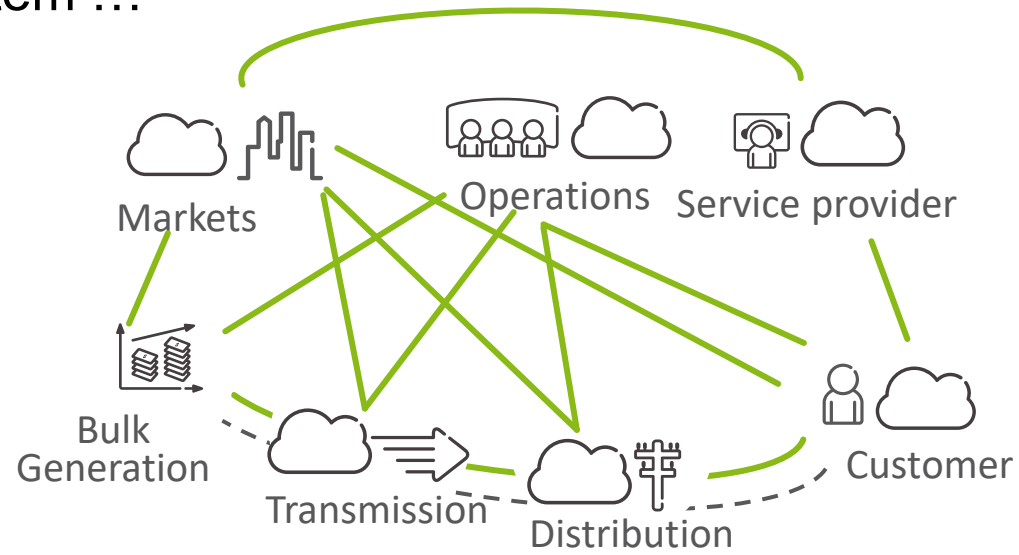
… all the other critical infrastructures have a **strong dependency from Critical Energy Infrastructures**



Source: European Programme for Critical Infrastructure Protection - Council Directive 2008/114/EC
Source: A new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure EPCIP [SWD (2013) 318]

Security is fundamental for smart critical energy infrastructures (CEIs)

ICT provides new opportunities to gather and analyze performance data, making it possible to preemptively notice and remedy technical vulnerabilities in the system …



… but the **increased interconnectivity associated with ICT** exposes CEIs to increased **cyber-risks and vulnerabilities**, and global **security** issues that arise in the **interaction between the cyber and the physical, institutional and human layers of the system**

Cyber attacks on the power grid are constantly **increasing in sophistication**

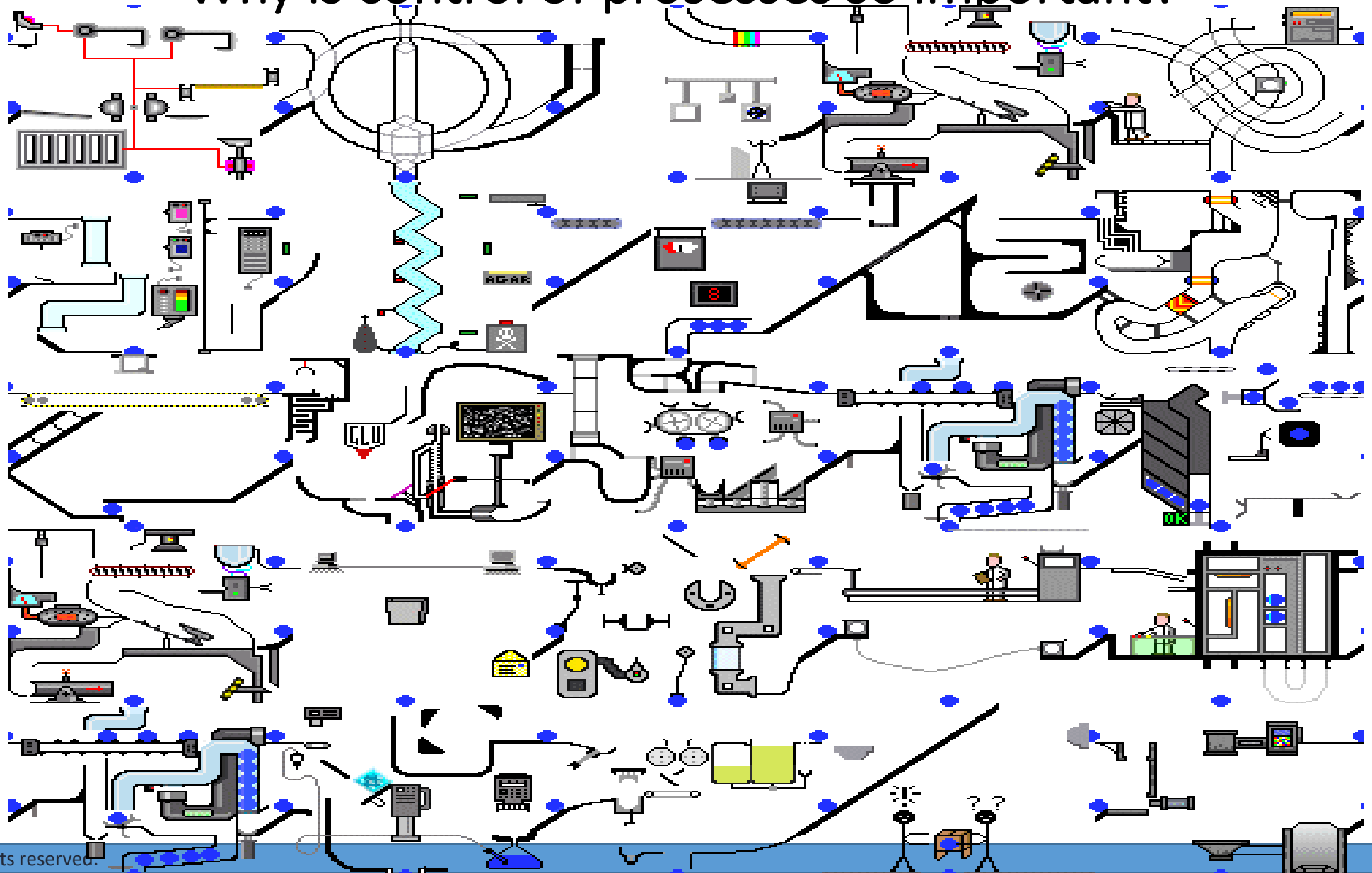
EU Policy Goals

- **Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU !!!**
- Ongoing processes in EU Commission according to European Programme for Critical Infrastructure Protection are:
  - Collection of CIP related best practices, risk assessment tools and methodologies
  - Commissioning studies concerning interdependencies
  - Implementation of minimum protection measures
- Ongoing processes of collecting suggestion for updating COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the needs to improve their protection

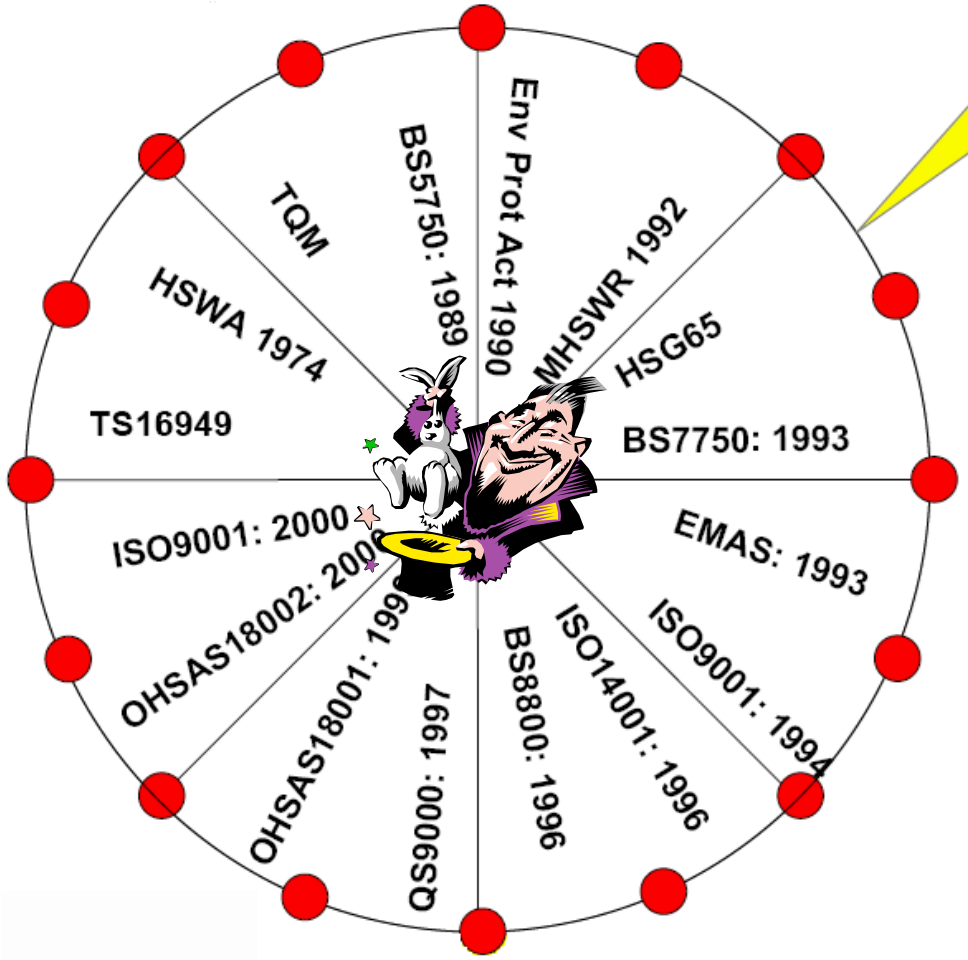
Fragmented landscape of operational approaches for CIP

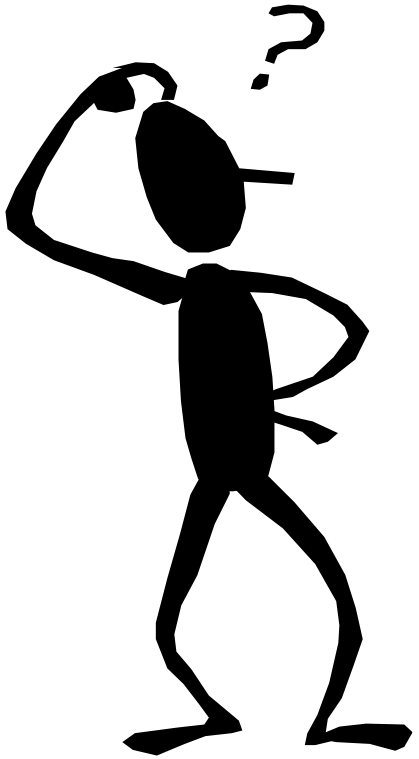
- Limits in the **threat scope** (e.g. either cyber or physical threats)
- Limits in the **coverage of the energy value chain** (from generation to consumer, from operation to market)
- Limits within the **organisation, silos** (e.g. technical, operations, business)
- Rarely involving **human dimension** (citizens or workers)
- **Little systematic relationship** between Power Network Operators and Security Operators/Service Providers and/or Law Enforcement Agencies
- Interaction and underlying procedures for linking **Power Network Operators** with **Computer Emergency Response Teams** (**CERTs)** and **Information Sharing & Analysis Centres (EE-ISAC)** still challenging at both **governance and technological levels**

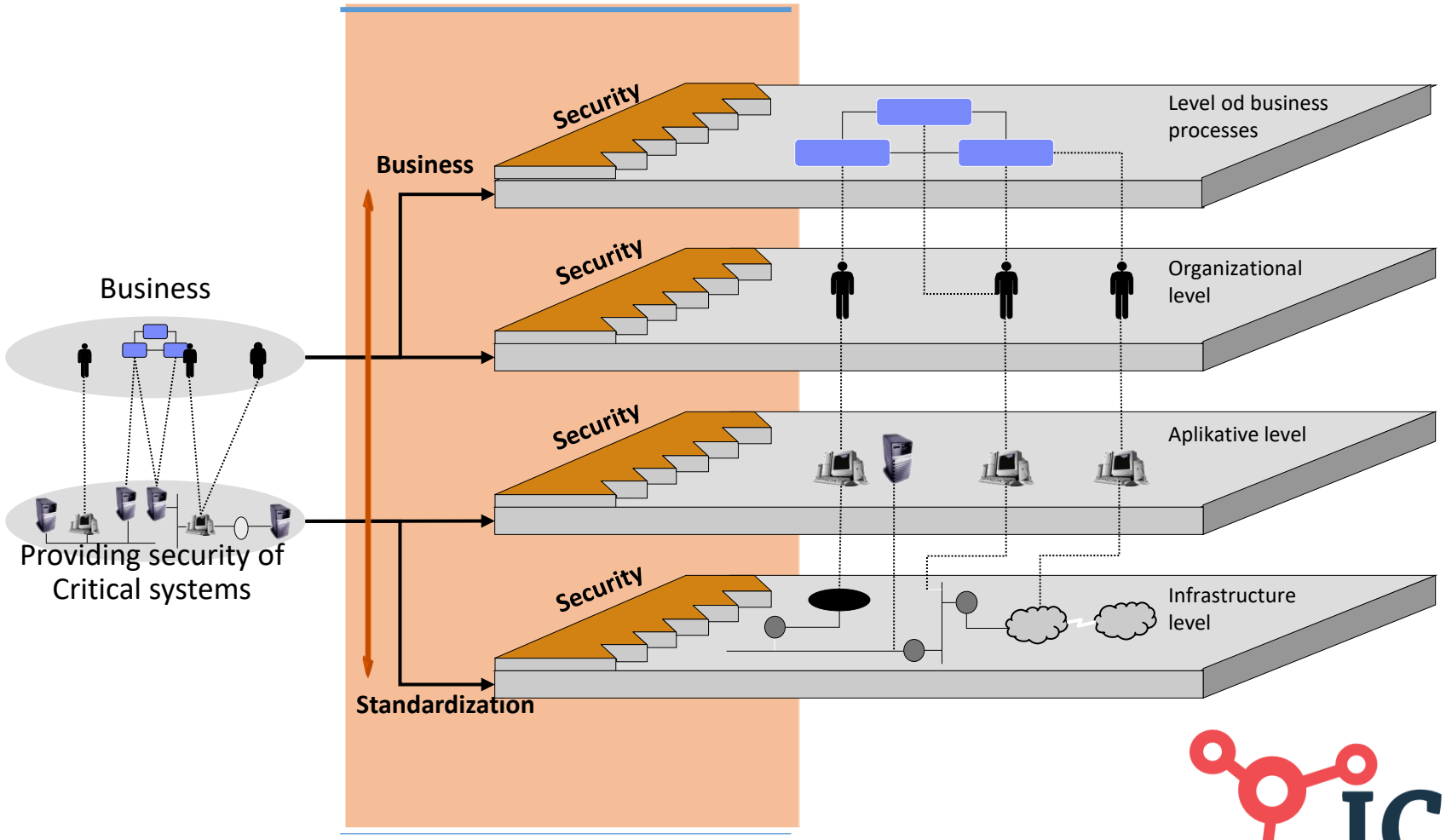
Why is control of prosesses so important?



Standardization circle of luck







DEFENDER contribution to EU policy goals

- Analysis of **new and future** complex threats to CEI
- Analysis of **selected scenarios** of threats to CEI (attack tree method evaluation)
- Analyses of processes and procedures that address certain **security gaps** in the field of physical and cyber security including human in the loop approach)
- Analysis of **interdependency** between CEI and other CI sectors
- Establishment of DEFENDER Critical Energy Infrastructure Security Stakeholders Group (**CEIS-SG**) (exchanging best practices, new knowledge and developments)

ICS INSTITUTE FOR CORPORATIVE SECURITY STUDIES

Standardisation: ongoing Work and Potential Impact

- Impact on Standards focusing on **information security** (family of ISO 27000) guidelines and threats assessment for **industrial system control** (incl. SCADA) (IEC 62443, NIST 800-82) guidelines
  - incorporating **physical and human aspects/threats into combined threat assessment and vulnerability management** (Human in the loop)
- Standards targeting **technical security systems** (cameras, sensors, security centres)
- Input to potential standards (communication protocols and data exchange)
  - among **power network operators and LEAs**
  - TSOs vs National-level CERTs (ENISA) and EE-ISAC
- Drone‘s and preparation new EU regulative;

Conclusions

- DEFENDER as ***First-of-this-kind EU-scale solution for cyber-physical protection and security fully tailored to cover the complete value chain of smart Critical Energy Infrastructures***
- Bringing citizens and CEI stakeholders workforce at a center stage, as key elements of the proposed solution (**human dimension**)
- One of the very first attempts to bring together in a systematic way **electrical energy network operators and Law Enforcement Agencies (LEAs)** at the same table.
- **Standardization could break the silos approaches in CIP but should be carefully developed through prism of processes complexity in organization‘s and take into consideration landscape of threats from security environment!**

DEFENDER

Defending the European Critical Energy Infrastructure

Thank you for your attention

For further information do not hesitate to contact me at the following email:

denis.caleta@ics-institut.si

ICS INSTITUTE FOR CORPORATIVE SECURITY STUDIES

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 740898