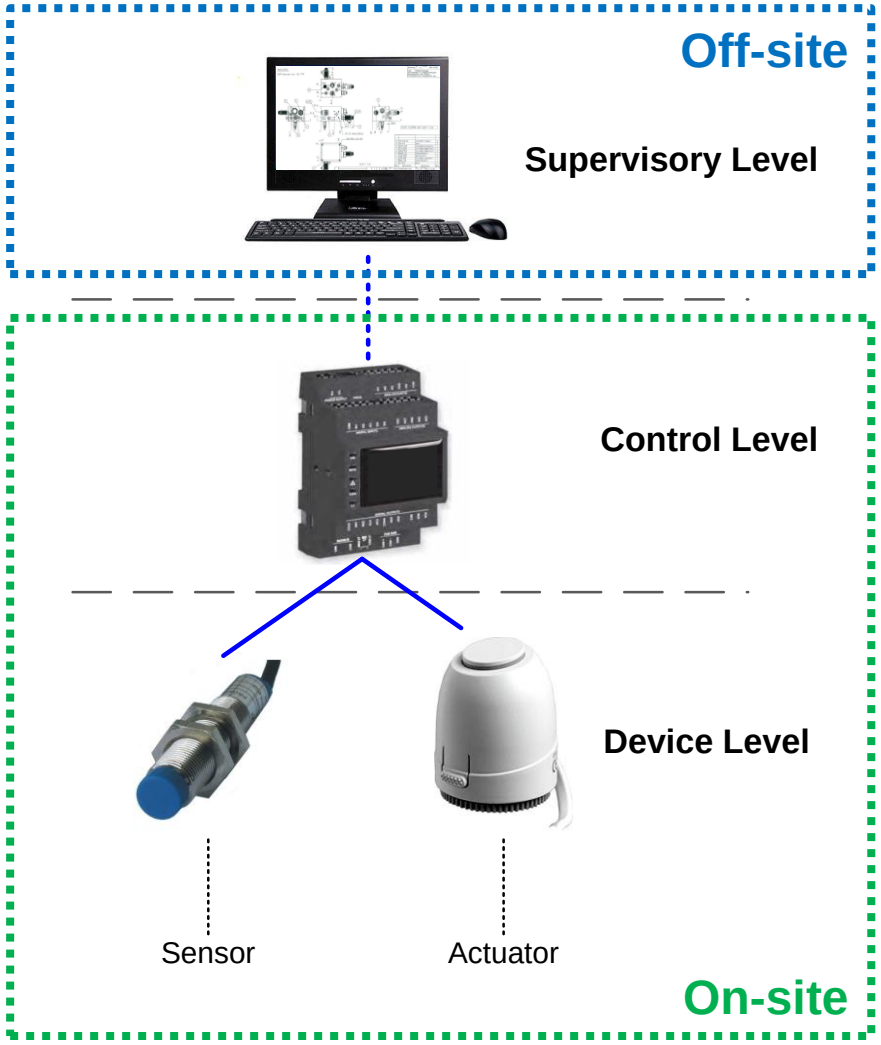
Examples of Horizontal Challenges for Cybersecurity in Critical Infrastructure

Dr. Martin Wimmer

June 24th, 2021

SIEMENS

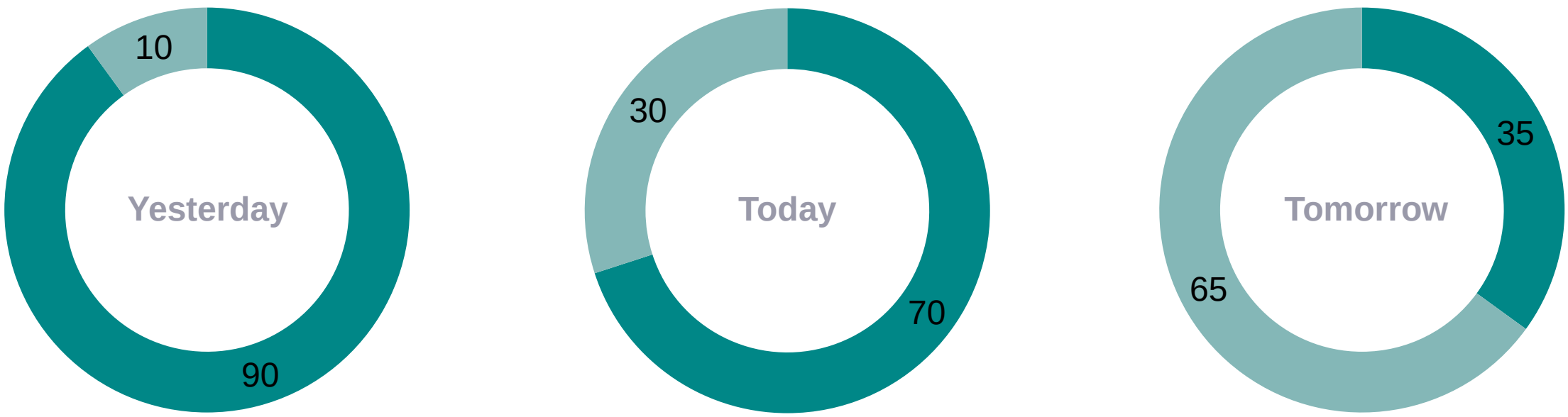
Starting Point: Operational Technology



- OT comprises *"…hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events…"*
  - Used in automation since the 70/80s
  - Originally not IP-based
- *"Secure island"* deployment model: system isolation, network segregation for the on-site components:
  - Controllers
  - Devices: sensors, actuators

SIEMENS

Paradigm Shift for OT Systems



Value proposition in OT products/systems

(indicative figures)

Hardware Software

SIEMENS

But are IT Security and OT the Same?

IT Security		OT Security
Confidentiality		**Availability**
3-5 years	**Asset lifecycle**	20-40 years
Forced migration (e.g. PCs, smart phone)	**Software lifecycle**	Usage as long as spare parts available
High (> 10 “agents” on office PCs)	**Options to add security SW**	Low (old systems w/o “free” performance)
Low (~2 generations, Windows 7 and 10)	**Heterogeneity**	High (from Windows 95 up to 10)
Standards based (agents & forced patching)	**Main protection concept**	Case and risk based

SIEMENS

Examples of What Can Go Wrong

U.S. Pipeline Attack - 2021
In May, Colonial, the operator of the biggest gasoline pipeline in the U.S. suffered from a ransomware attack and shut down operations. Colonial paid ransom of which the majority could be seized.

https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/
https://www.bloomberg.com/news/articles/2021-05-08/u-s-s-biggest-gasoline-and-pipeline-halted-after-cyberattack
https://www.nytimes.com/2021/06/07/us/politics/pipeline-attack.html

Cyberattack Targets Safety System of Saudi Arabian Petrochemical Plant - 2017
In 2017 the safety system of a petrochemical plant in Saudi Arabia was attacked. Parts of the plant were taken offline.

https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco

Ukrainian Power Grid - 2016
On December 23, 2015, the Ukrainian […] electricity distribution company, reported service outages to customers. […] outages that caused approximately 225,000 customers to lose power across various areas.

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

German Steel Mill - 2015
… hackers had struck an unnamed steel mill in Germany. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive"—though unspecified—damage.

https://www.wired.com/2015/01/german-steel-mill-hack-destruction/
https://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf

SIEMENS

Examples of What Can Go Wrong

Colonial Pipeline Attack - 2021
In May the operator of the biggest gasoline pipeline in the U.S. suffered from a ransomare attack and shut down operations. Colonial paid ransom of which the majority could be seized

https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/
https://www.bloomberg.com/news/articles/2021-05-08/u-s-s-biggest-gasoline-and-pipeline-halted-after-cyberattack
https://www.nytimes.com/2021/06/07/us/politics/pipeline-attack.html

Industroyer
"attacks ... [by] using industrial communication protocols which are standardised across a number of types of critical infrastructure" …

"The problem is that these protocols were designed decades ago, and back then industrial systems were meant to be isolated from the outside world,"

Ukrainian Power Grid - 2016
On December 23, 2015, the Ukrainian […] electricity distribution company, reported service outages to customers. […] outages that caused approximately 225,000 customers to lose power across various areas.

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

German Steel Mill - 2015
… hackers had struck an unnamed steel mill in Germany. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive"—though unspecified—damage.

https://www.wired.com/2015/01/german-steel-mill-hack-destruction/
https://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf

SIEMENS

Generic Attack Vectors

SIEMENS

Generic Attack Vectors … and the Need for Mitigations

Supply Chain Attacks

SCADA System Attacks

Communication/ Protocol Attacks

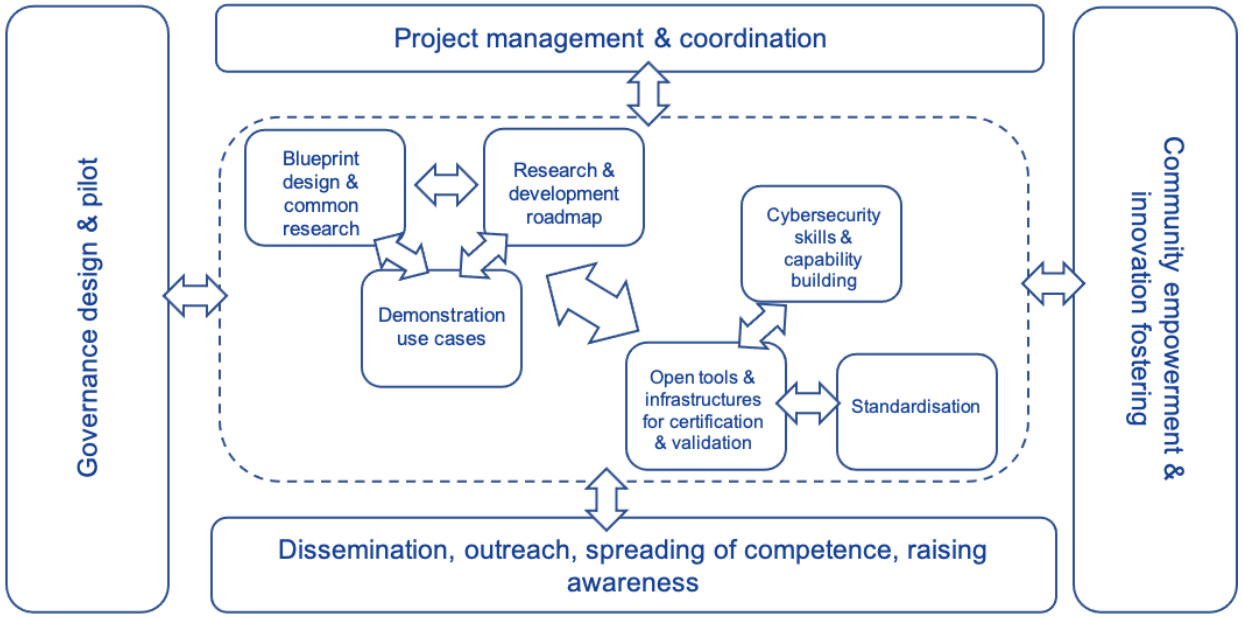
Phishing Attacks

Ransomwares

What Is CyberSec4Europe

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

Cyber Security for Europe



- Ensure the adequacy and availability of cybersecurity education and training as well as common open standards
- Communicate widely and build communities

CyberSec4Europe is a research-based consortium working across four different but inter-related areas with a strong focus on openness and citizen-centricity in order to:

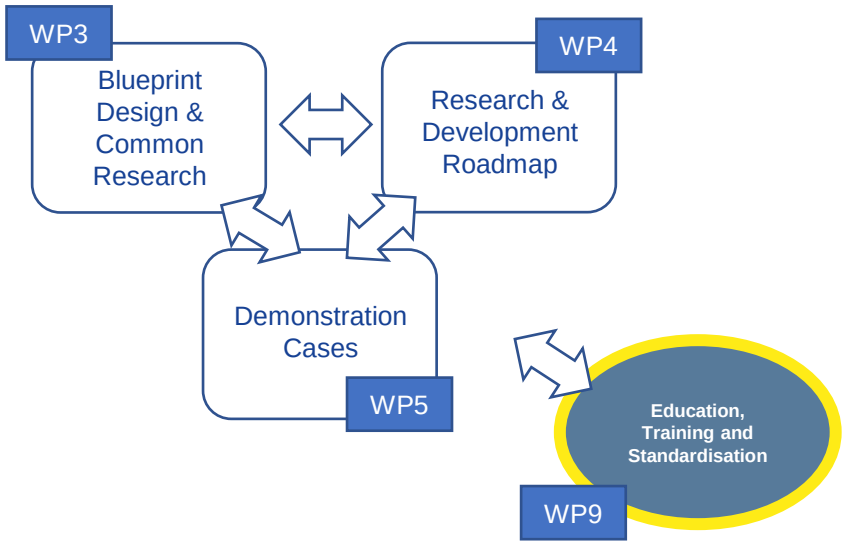
- Pilot a European Cybersecurity Competence Network
- Design, test and demonstrate potential governance structures for the network of competence centres
- Harmonise the journey from software componentry identified by a set of roadmaps leading to recommendations

SIEMENS

Supply Chain Security

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

Cyber Security for Europe



Supply Chain Security is addressed by the programme through closely coordinated parallel streams

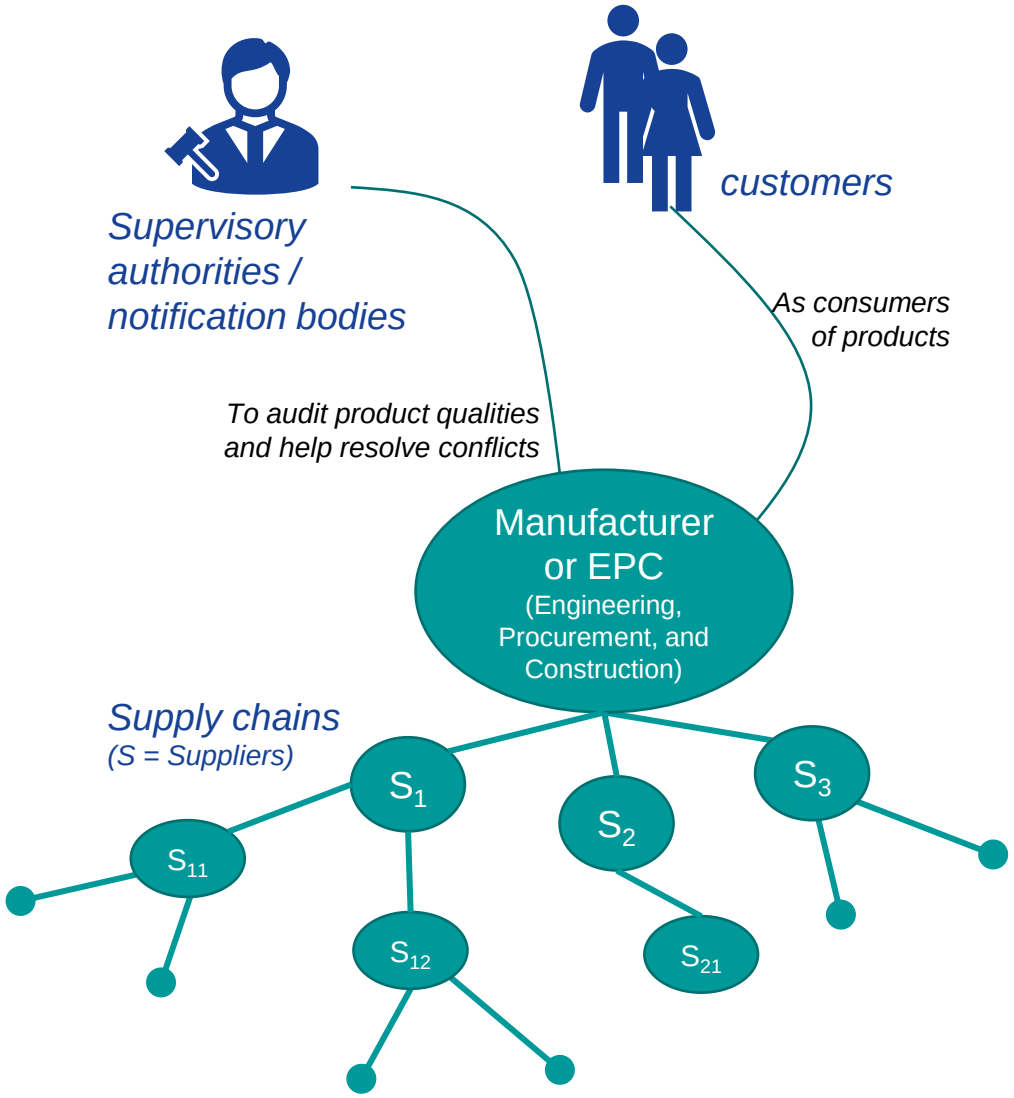
- WP3's research and integration on cybersecurity enablers and underlying technologies, e.g., blockchain
- WP4's definition and review of the research and development roadmap for industrial challenges, e.g., with focus on supply chain security
- WP5's demonstrator development, with two use cases for supply chain security
- WP9's cybersecurity awareness initiative, e.g., with regard to "Supply Chain Security Recommendations"

SIEMENS

The Supply Chain Security Demonstrator is About

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

Cyber Security for Europe



- … assessing the security requirements of highly distributed, cross-organizational business processes, e.g.,
  - guaranteeing non-repudiation and enforcing workflow compliance and
  - identifying and resolving disputes amongst business partners
- … demonstrating security architectures and processes that allow **building up trust** amongst business partners **without the need (and/or possibility) to rely on a trusted 3rd party**

SIEMENS

Generic Attack Vectors

SIEMENS

Generic Attack Vectors … and the Need for Mitigations

Supply Chain Attacks

SCADA System Attacks

Communication/ Protocol Attacks

Ransomwares

Phishing Attacks

SIEMENS

Secure Data Acquisition Through Unidirectional Connectivity

Firewall

Medium risk of remote attacks can disrupt operations

- SW can & has been hacked
- IT Lifecycle (5yrs)
- Patches, monitoring & audits $$

Data Diode

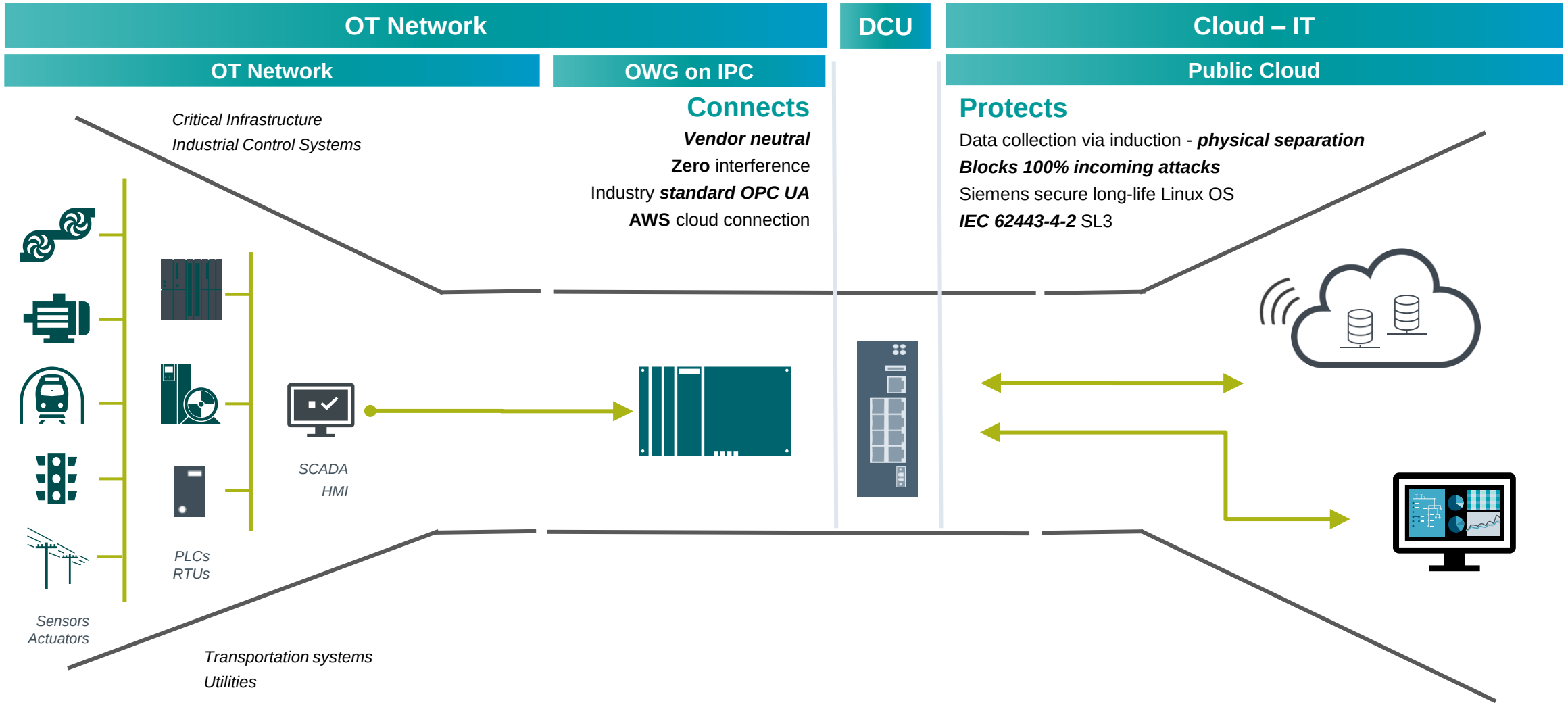
(DCU; siemens.com/dcu)

Very low risk of operational disruption due to remote attacks

- HW can't be hacked 0110110 1011101 0011011 0101010 1100101
- OT Lifecycle (+20yrs)
- No patches or audits needed $

SIEMENS

How Does It Work?

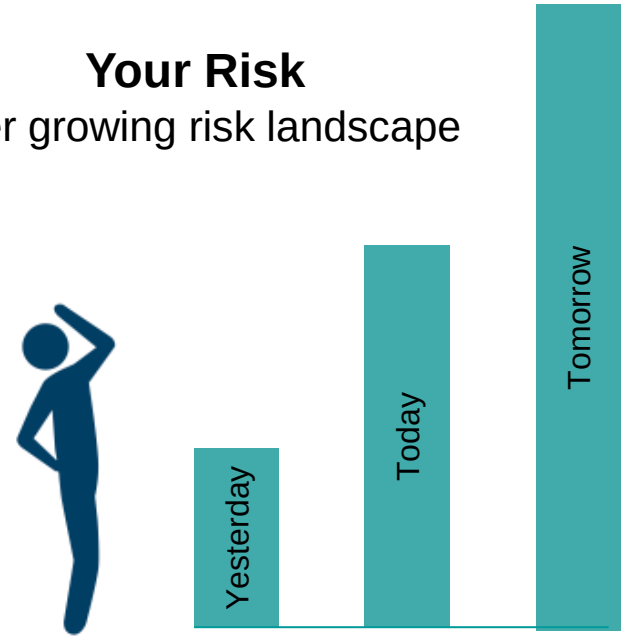


SIEMENS

All Solved? How to Proceed?

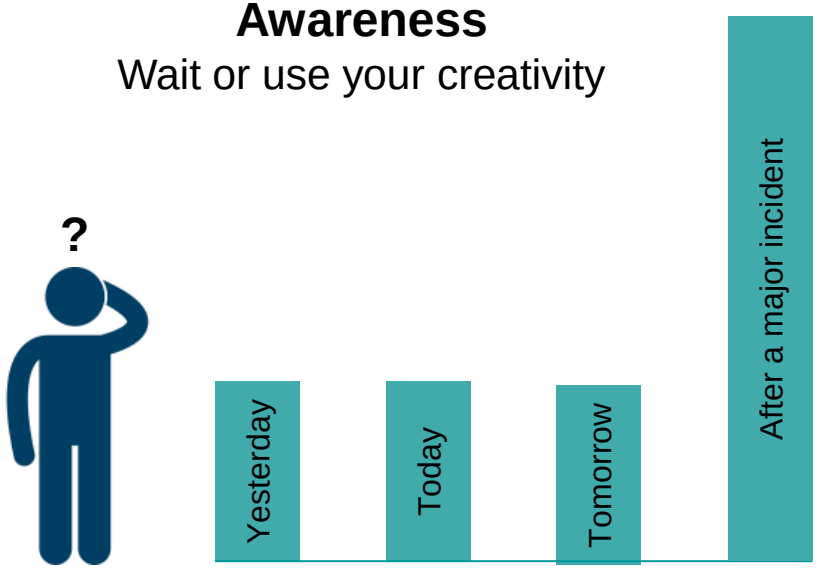
Your Risk

Ever growing risk landscape



Awareness

Wait or use your creativity



SIEMENS