NORCICS SFI Norwegian Centre for Cybersecurity in Critical Sectors

Integrating IT and OT: Cybersecurity challenges in industry 4.0

Sokratis K. Katsikas
sokratis.katsikas@ntnu.no

Kunnskap for en bedre verden

Agenda

- Who are we?
- IT and OT convergence: Industry 4.0, IIoT, CPS
- The NIST framework for improving CI cybersecurity
- IIoT security: state of affairs, trends, and challenges
- Experimental cybersecurity
- Conclusions

NTNU

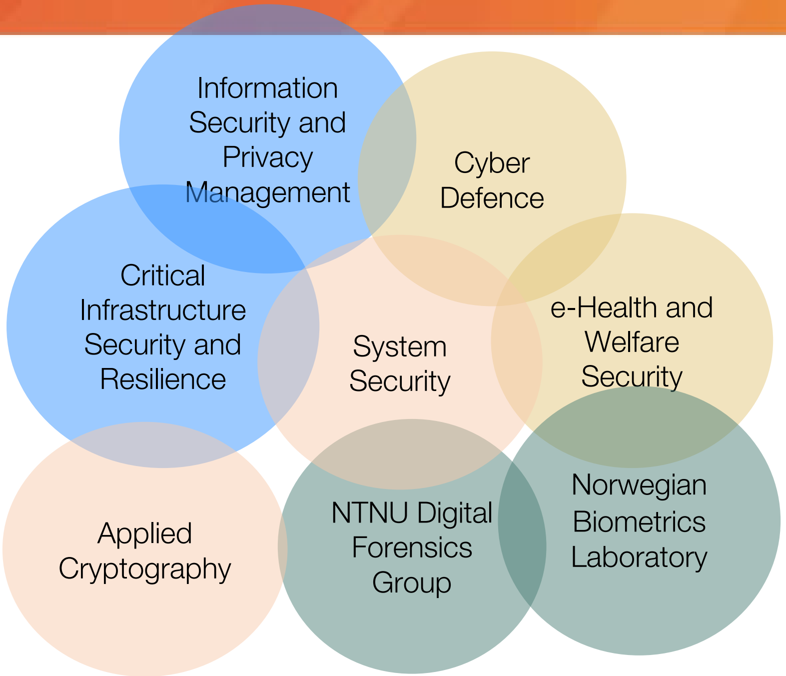
- Main profile in science and technology
- Headquarters in Trondheim with campuses in Gjøvik and Ålesund
- 8 faculties, 55 departments and NTNU University Museum
- More than 42 000 students (2020)
- 406 doctoral degrees (2020)
- Budget of NOK 9.6 billion
  - of which NOK 2.7 billion from external sources

NTNU Department of Information Security and Communication Technology
Main Norwegian supplier of research-based competence in information security and communication technology providing effective, robust and secure communication networks, information systems and digital services.

NTNU CCIS

Center for Cyber and Information Security

Our research groups



Our partners

Cyberforsvare
t

Forsvarets
høgskole

Cyberingeniørskolen

www.ccis.no

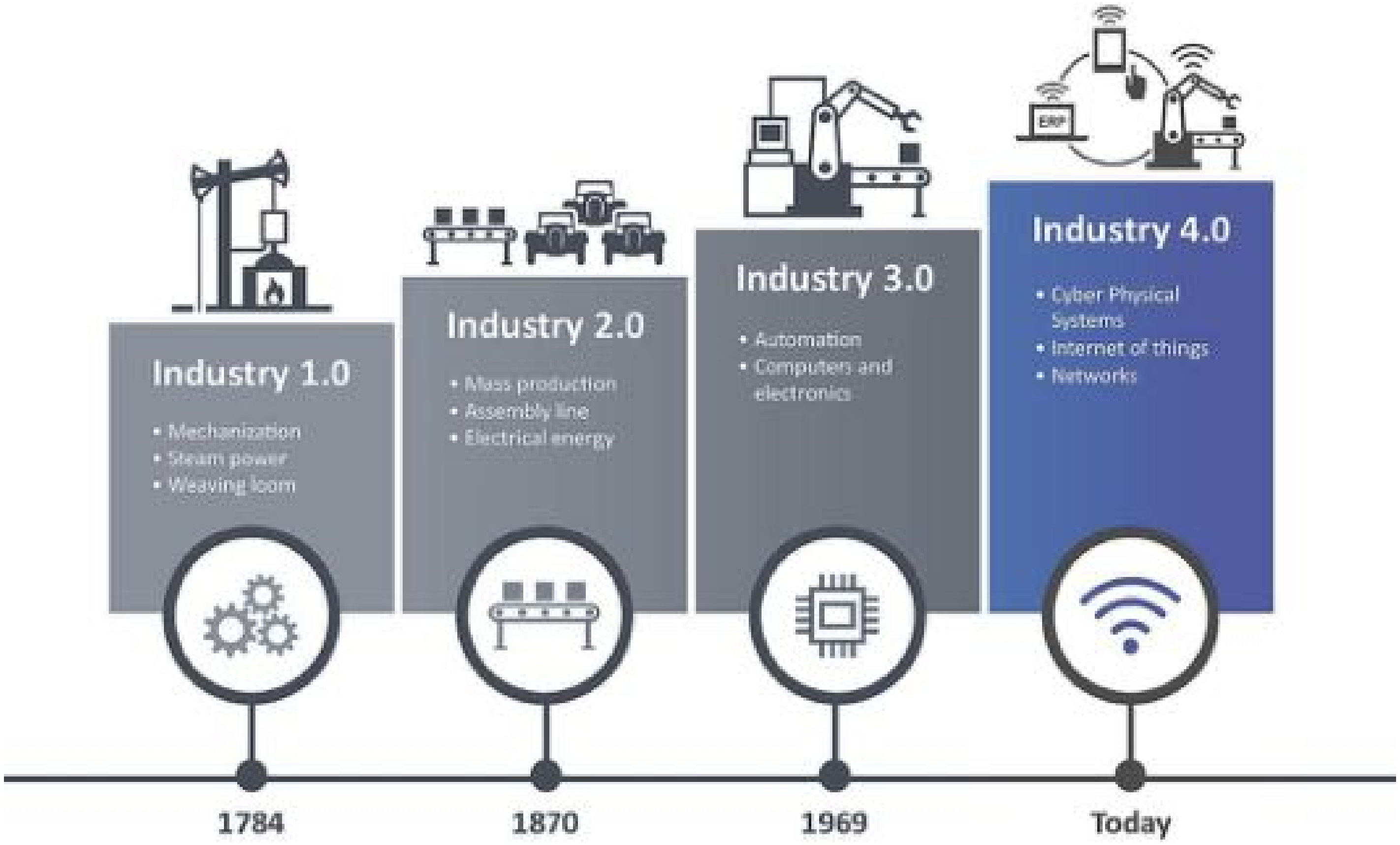
The Critical Infrastructure Security and Resilience (CISaR) Group

https://www.ntnu.edu/iik/cisar

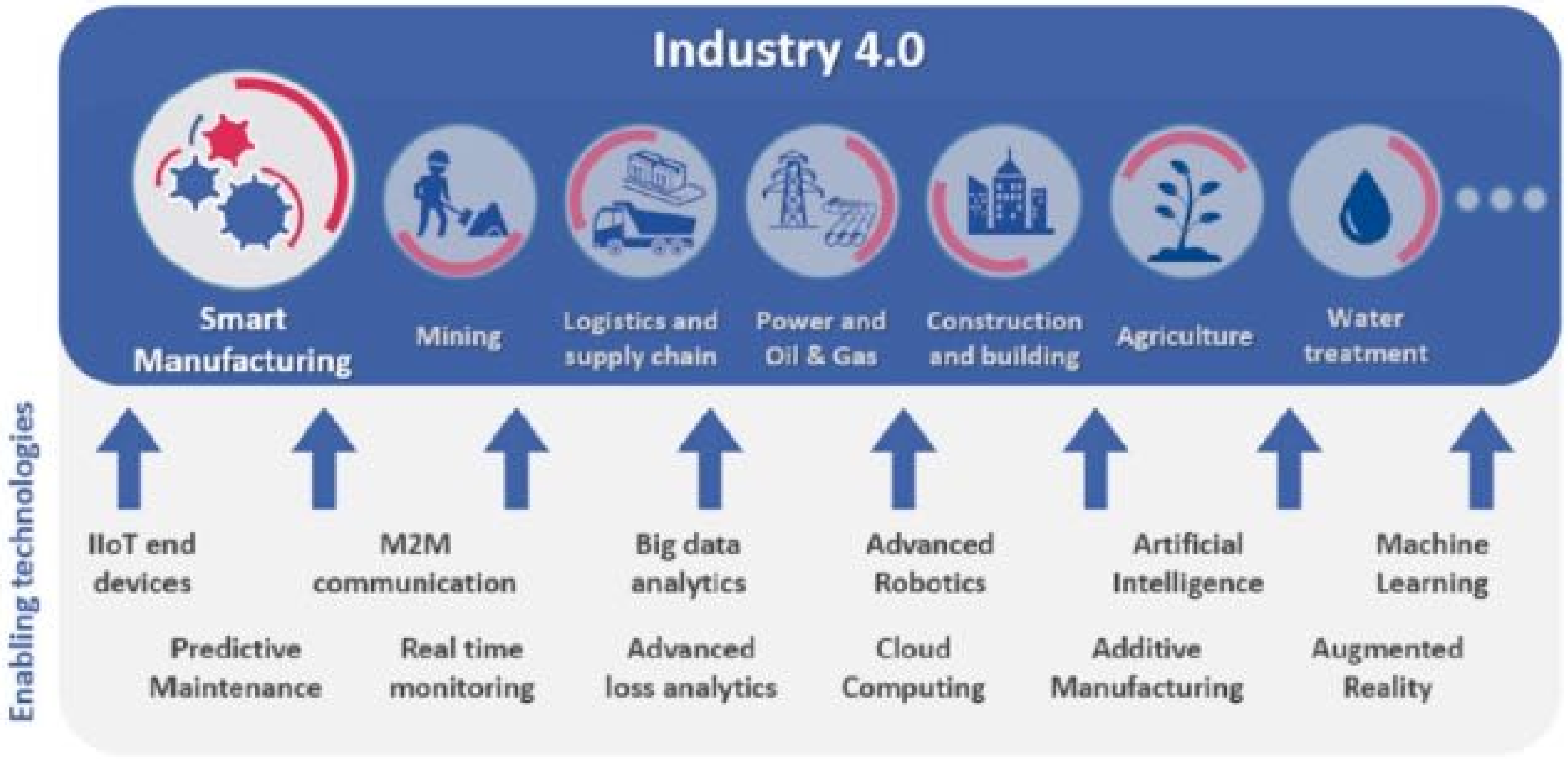
Areas of research interest

- Cyber security of the energy infrastructure
- Maritime cyber security and resilience
- Cyber security of cyber physical systems
- Blockchain technology for securing cyber-physical systems
- Cyber security of the IoT and of the industrial IoT
- Cyber security of digital twins
- SDN security
- Security Awareness

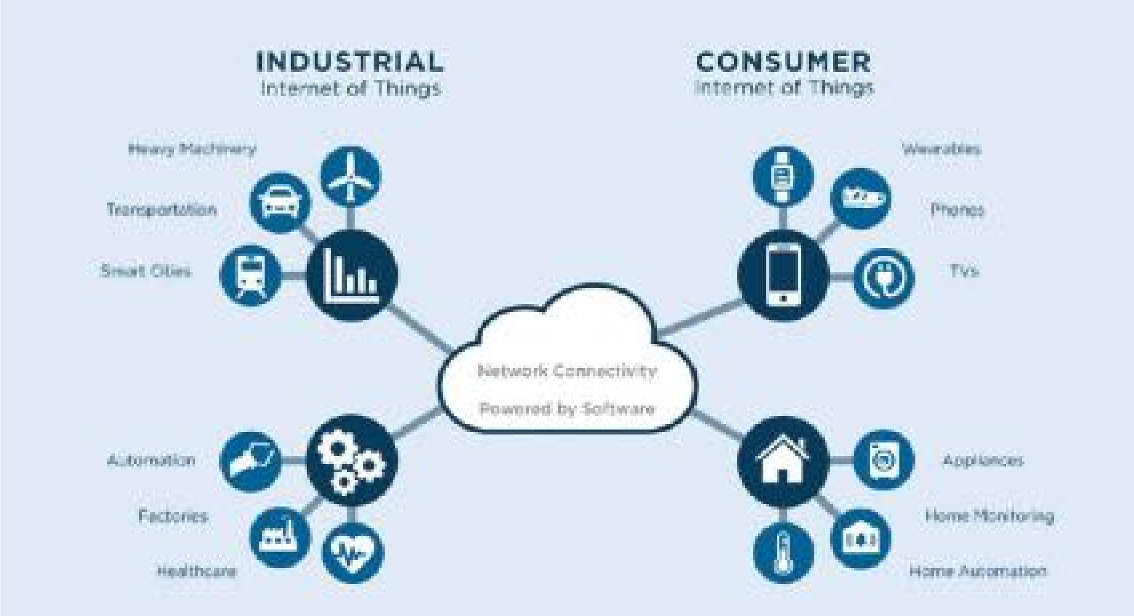
- 6 H2020 projects
- 6 NFR-funded projects
- 7 NTNU-funded projects
- 3 projects with Norsk Industri

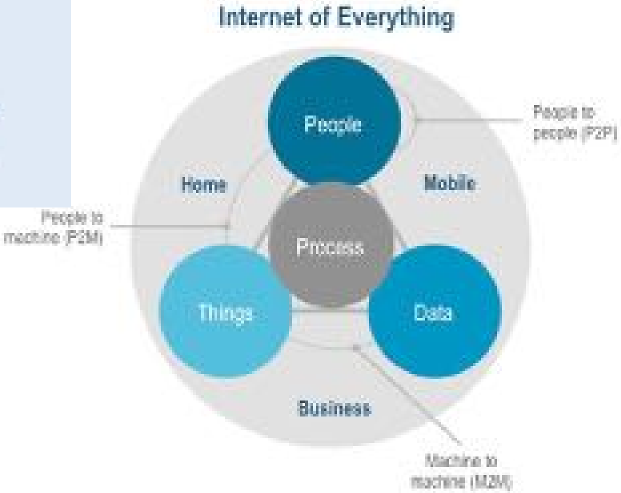


https://dzone.com/articles/industry-40-the-top-9-trends-for-2018

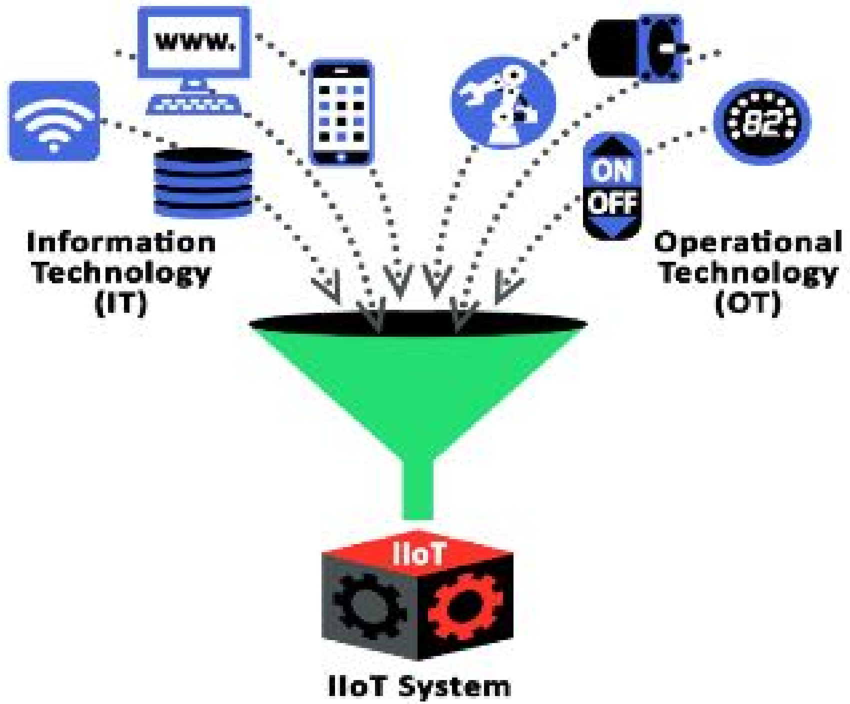


ENISA report: Good Practices for Security of Internet of Things in the context of Smart Manufacturing

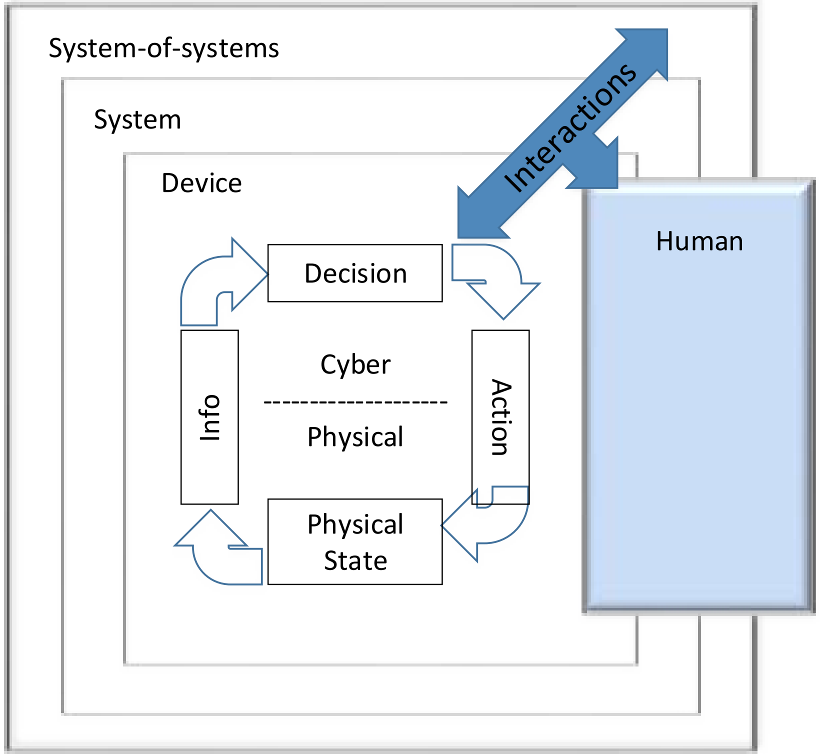




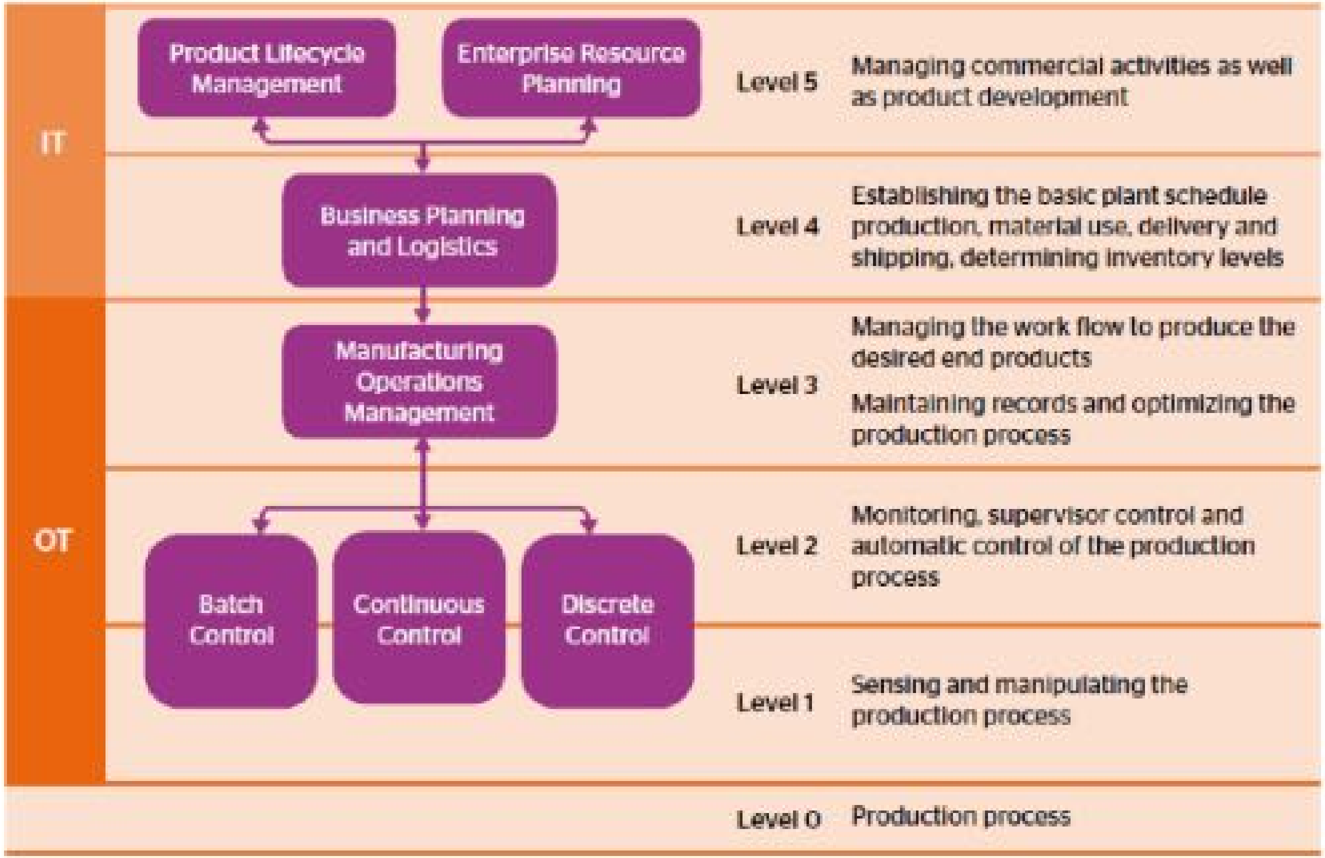
https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/industrial-internet-things-iiot/



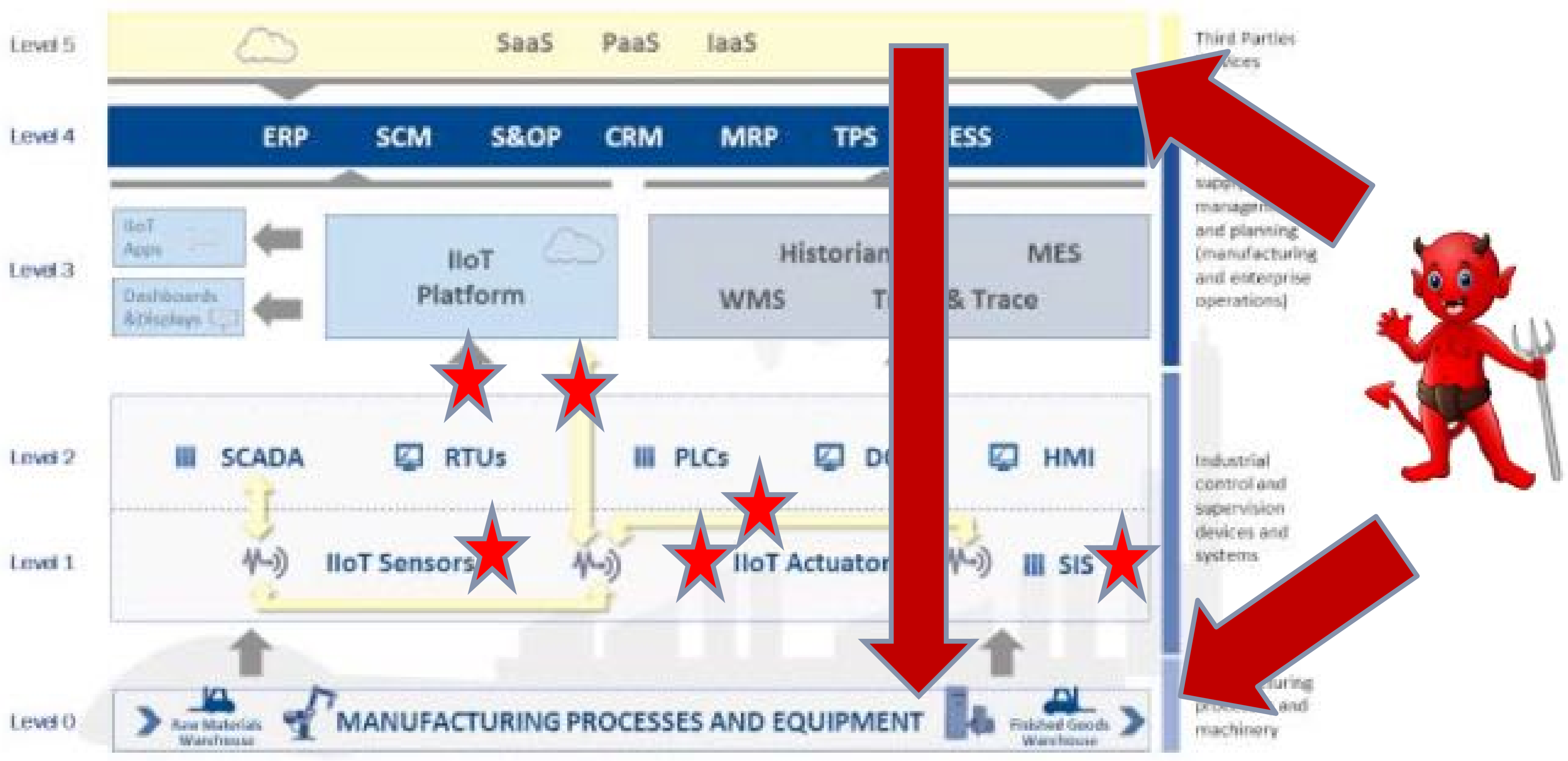
Industrial Internet Consortium, Industrial Internet of Things Volume G4: Security Framework



NIST Special Publication 1500-201: Framework for Cyber-Physical Systems: Volume 1, Overview



Ascent, *The convergence of IT and operational technology – ISA '95*



ENISA report: Good Practices for Security of Internet of Things in the context of Smart Manufacturing

ATTACK SCENARIOS	SEVERITY
1. Against the connection between the controller (e.g. DCS, PLC) and the actuators	High
2. Against sensors (modification of measured values / states, their reconfiguration, etc.)	High
3. Against actuators (suppressing their state, modifying the configuration)	High - Crucial
4. Against the information transmitted via the network	High - Crucial
5. Against IIoT gateways	High - Crucial
6. Manipulation of remote controller devices (e.g. operating panels, smartphones)	High
7. Against the Safety Instrumented Systems (SIS)	Crucial
8. Malware	High
9. DDoS attack using (IoT) botnets	Medium - High
10. Stepping stones attacks (e.g. against the Cloud)	Medium
11. Human error-based and social engineering attacks	High
12. Highly personalised attacks using Artificial Intelligence Technologies	Medium - High

Table 3: IIoT attack scenarios

ENISA report: Good Practices for Security of Internet of Things in the context of Smart Manufacturing

Distinctive characteristics

- Resilience
- Safety
- Systems-of-Systems nature
- Extreme scalability
- Interaction with the physical world
- Time-aware and deadline-sensitive processes
- Vulnerable components
- Increased connectivity
- Supply chain complexity
- Legacy ICSs
- Resource constrained platforms
- Need to accommodate the in-place business processes
- “Always on” requirement
- Dynamic domain of use
- Difference in lifecycle between IT and OT systems
- Insecure protocols
- Unused functionalities
- Organizational and behavioral changes

Security properties: Beyond CIA

Controllability

Ability to bring the process into a desired state

- Feasibility
  - The process in a controllable state (there is a control sequence which can bring process into an intended state)
- Awareness
  - The sequence of the control commands known to the operator

Observability

Ability to determine process state and maintain situational awareness

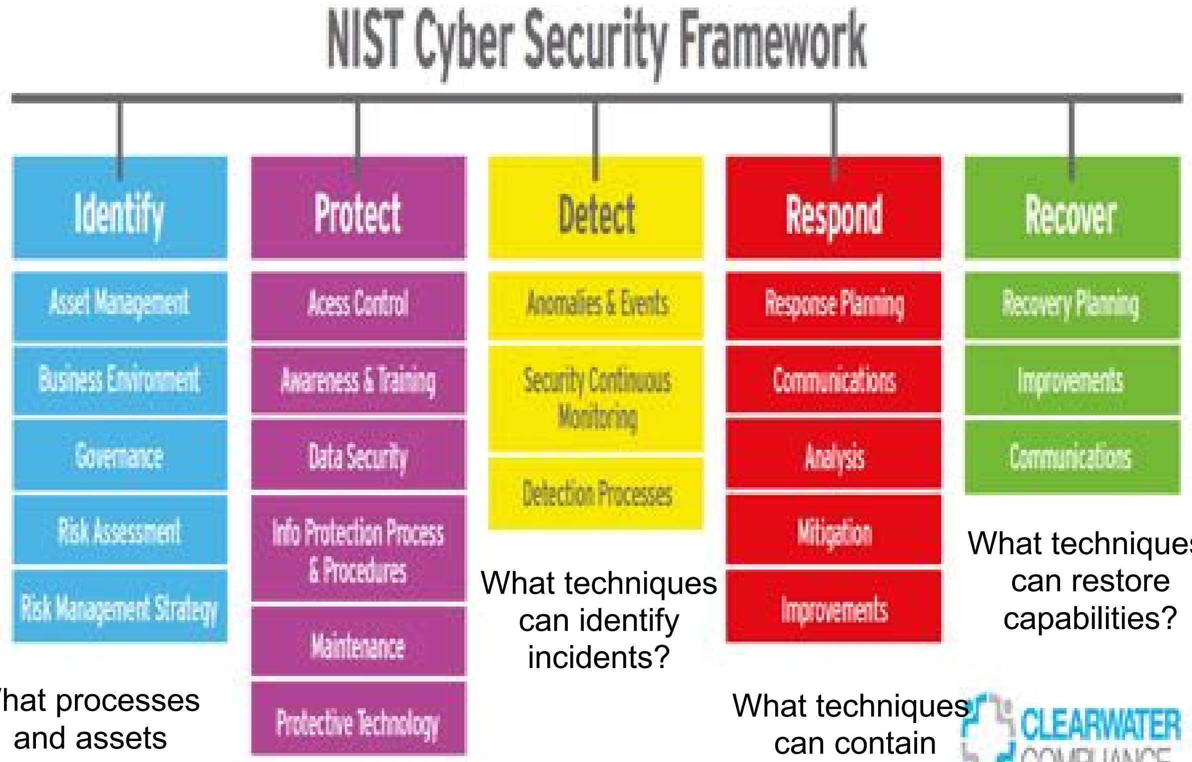
- Data quality and availability
  - Data trustworthiness (veracity)
  - Integrity and availability of data in transit and storage
- Sufficiency
  - Measuring all necessary quantities at the right locations
  - Ability to interpret the measurements

Operability

Ability of the plant to achieve acceptable operations

- Resilience
  - Ability to maintain optimal operations under attack
- Survivability
  - Ability to maintain operations at suboptimal level
- Graceful degradation
  - Ability to maintain limited plant functionality to achieve safe shut down

M. Krotofil, K. Kursawe, and D. Gollmann, "Securing Industrial Control Systems", in Cristina Alcaraz (Ed.), *Security and Privacy Trends in the Industrial Internet of Things*, Springer, 2019.



What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

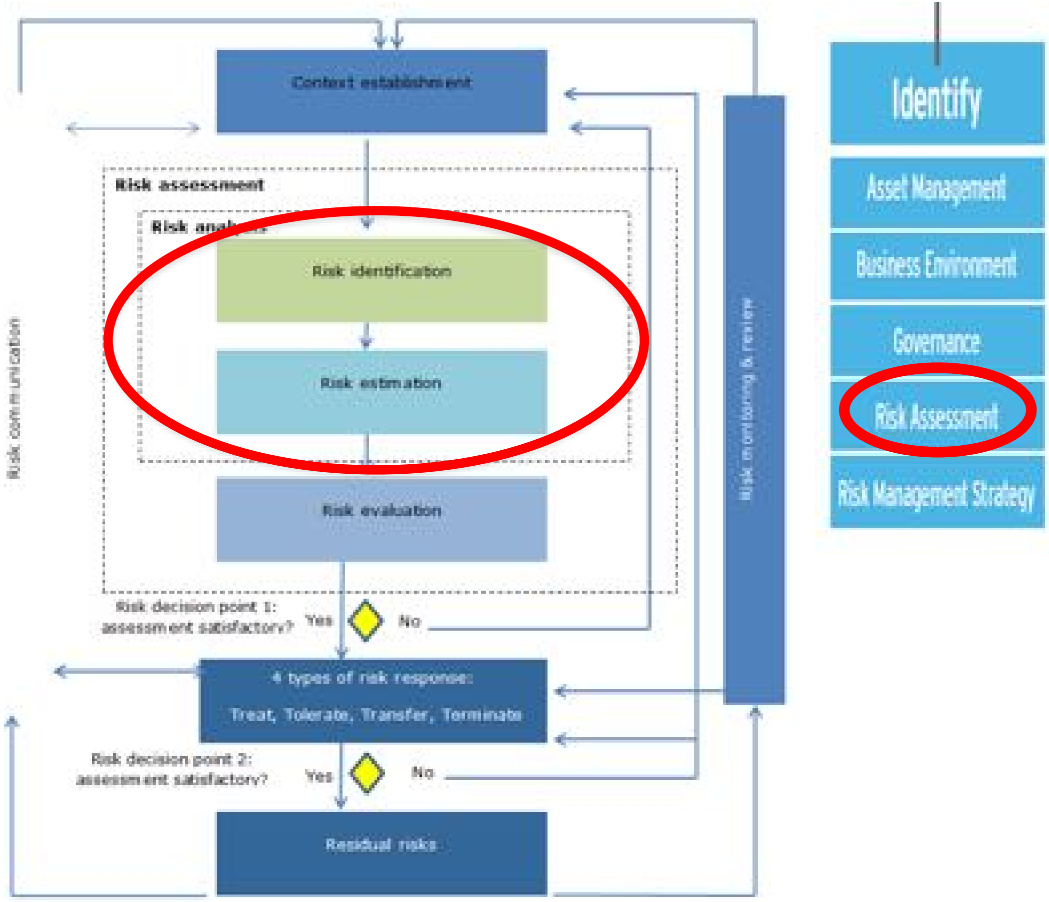
What techniques can contain impacts of incidents?

What techniques can restore capabilities?

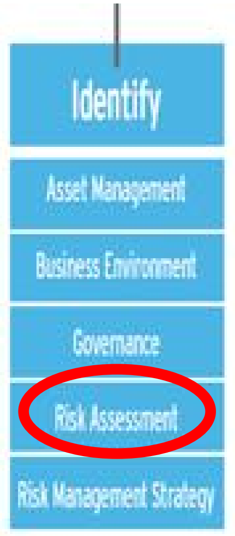
CLEARWATER COMPLIANCE

Risk assessment

- Threats, vulnerabilities, impact
- Quantitative – qualitative
- Domain specific
- Safety & Security requirements

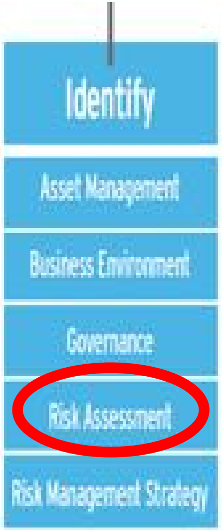


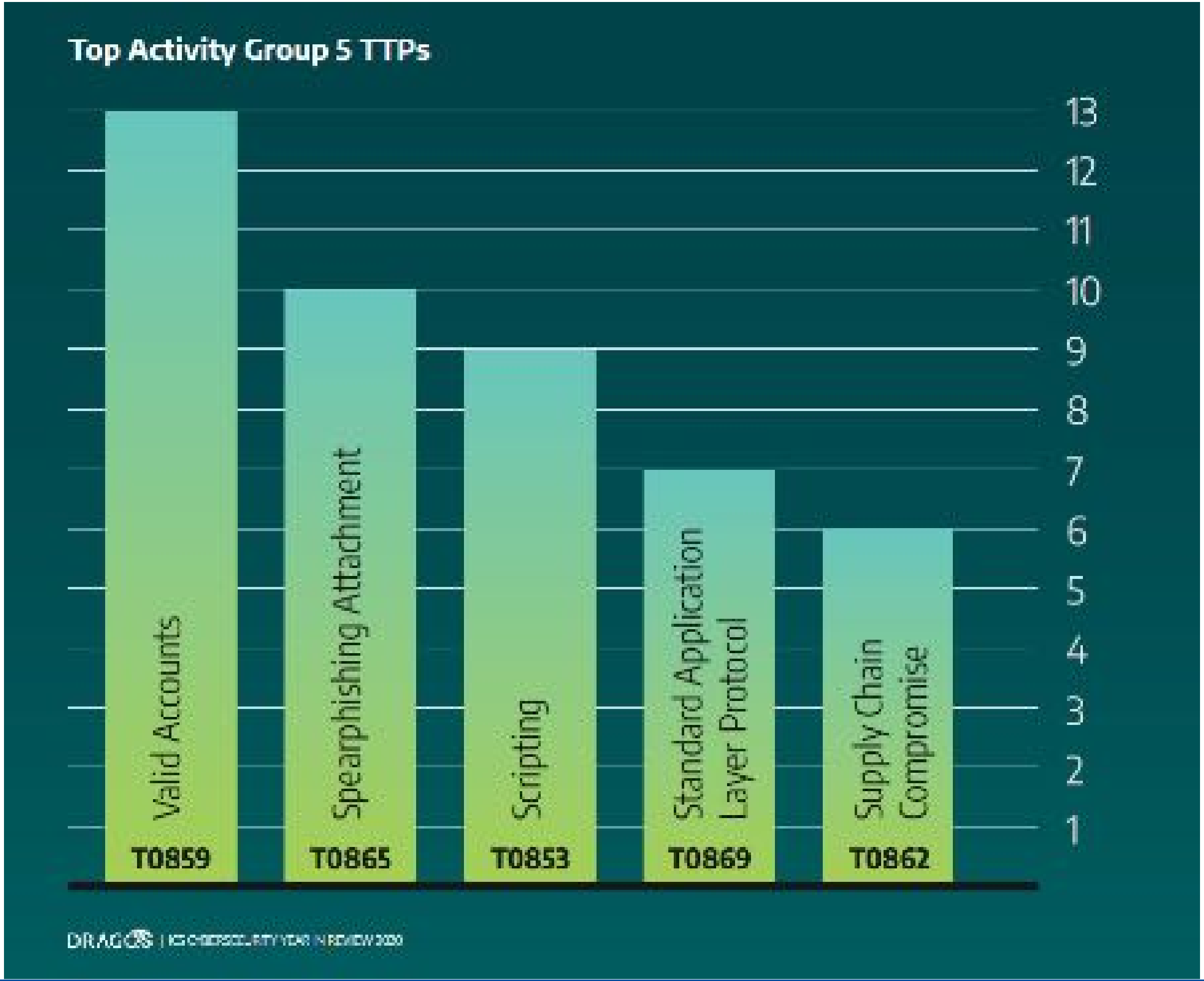
Vulnerabilities



- Most vulnerabilities resided deep within the ICS network, meaning they apply to equipment on Levels 0 to 3 of the Purdue Model. This includes engineering workstations, PLCs, sensors, and industrial controllers. These vulnerabilities require access to a control system network to exploit, offering some mitigation for organizations provided they implement proper network segmentation.
- With the increasing connectivity in organizations, this security control is diminishing in value and should be enhanced with efforts such as network monitoring, and where possible, Multi-Factor Authentication (MFA) for remote sessions.

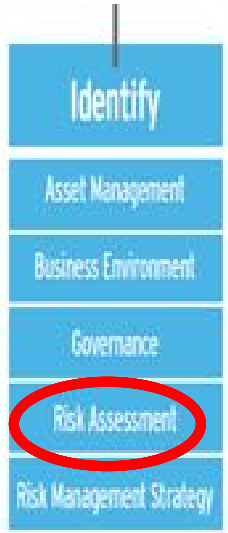
Dragos ICS CYBERSECURITY Report 2020


Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy


Top Activity Group 5 TTPs
13
12
11
10
9
8
7
6
5
4
3
2
1
Valid Accounts
T0859
Spearphishing Attachment
T0865
Scripting
T0853
Standard Application Layer Protocol
T0869
Supply Chain Compromise
T0862
DRAGOS | ICS CYBERSECURITY YEAR IN REVIEW 2020

The STRIDE Method

- **STRIDE** → **Security Properties**
  - **S**poofing → Authentication
  - **T**ampering → Integrity
  - **R**epudiation → Non-repudiation
  - **I**nformation disclosure → Confidentiality
  - **D**enial of service → Availability
  - **E**levation of privileges → Authorization



The DREAD Method

- **DREAD**
  - **D**amage
  - **R**eproducibility
  - **E**xploitability
  - **A**ffected
  - **D**iscoverability

$$Impact_i^s = \frac{Damage + Affectedsystems}{2},$$

$$Likelihood_i^s = \frac{Reproducibility + Exploitability + Discoverability)}{3},$$

$$Risk_i^s = \frac{(Impact_i^s + Likelihood_i^s)}{2}.$$

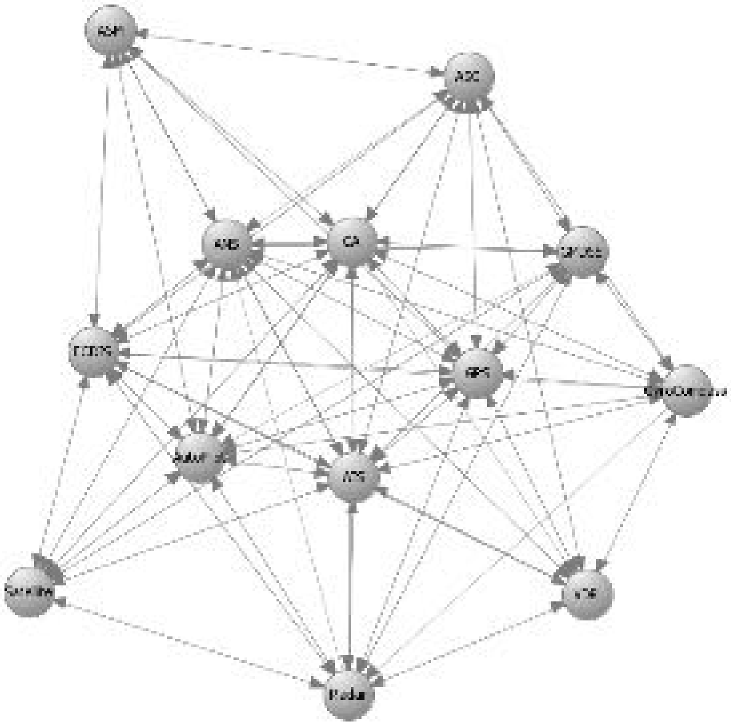
G. Kavallieratos, N. Chowdhury, S. Katsikas, V. Gkioulos, S. Wolthusen, "Threat Analysis for Smart Homes", *Future Internet*, 11(10), 207; https://doi.org/10.3390/fi11100207, 2019

Threat analysis: The STRIDE Method

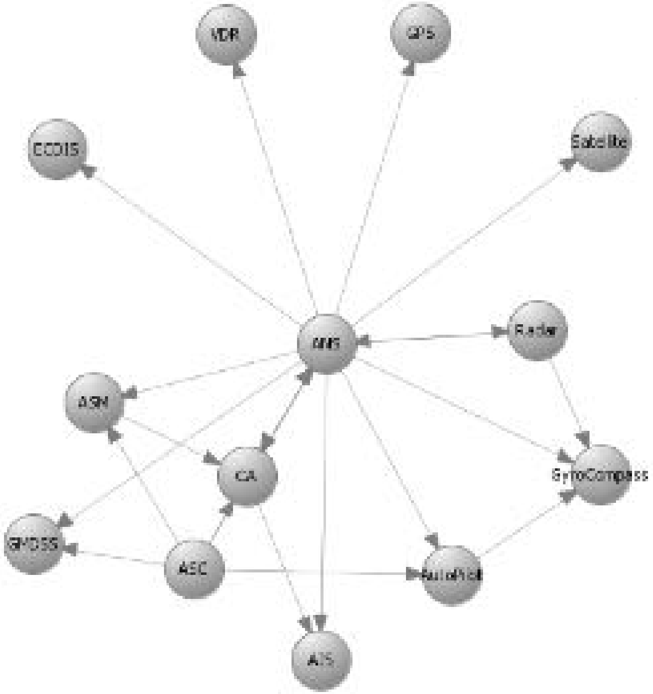
Spoofing	1. An adversary may gain access to the field gateway by leveraging default login credentials 2. An adversary may spoof IoT Device with a fake one 3. An adversary may reuse the authentication tokens of IoT Device in another 4. An adversary may spoof a device and connect to field gateway
Tampering	1. An adversary may exploit known vulnerabilities in unpatched devices 2. An adversary may tamper IoT Device and extract cryptographic key material from it 3. An adversary may execute unknown code on IoT Field Gateway 4. An adversary may tamper the OS of a device and launch offline attacks
Repudiation	1. An adversary can deny actions on Field Gateway due to lack of auditing
Information Disclosure	1. An adversary may eavesdrop the communication between the device and the field gateway
Denial of Service	N/A
Elevation of Privileges	1. An adversary may gain unauthorized access to privileged features on IoT Device 2. An adversary may exploit unused services or features in IoT Field Gateway 3. An adversary may trigger unauthorized commands on the field gateway

G. Kavallieratos, N. Chowdhury, S. Katsikas, V. Gkioulos, S. Wolthusen, "Threat Analysis for Smart Homes", *Future Internet*, 11(10), 207; https://doi.org/10.3390/fi11100207, 2019

Risk propagation and aggregation



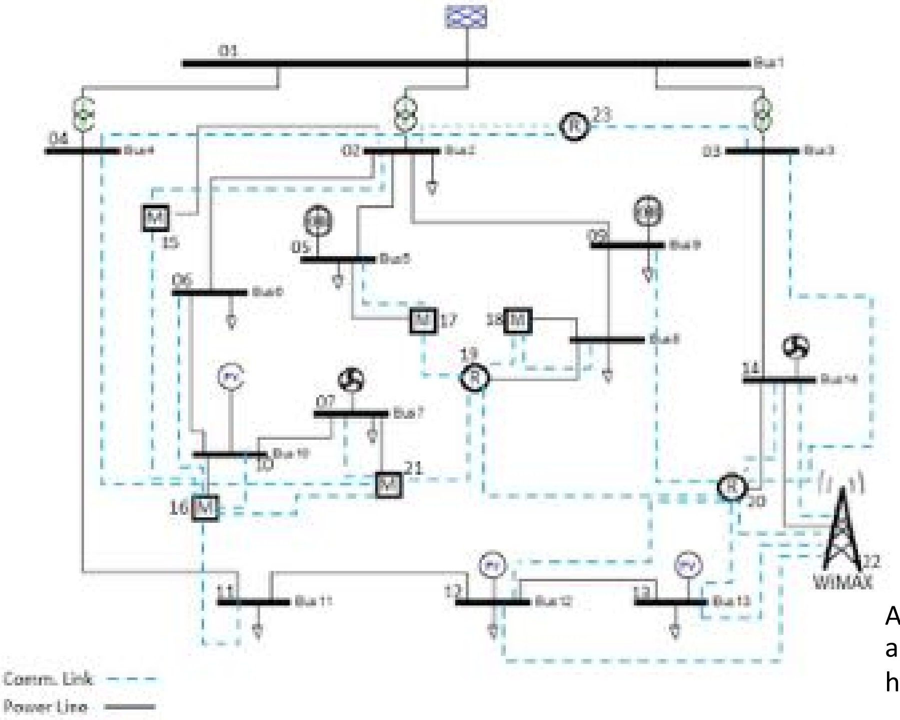
Autonomous ship – information flows

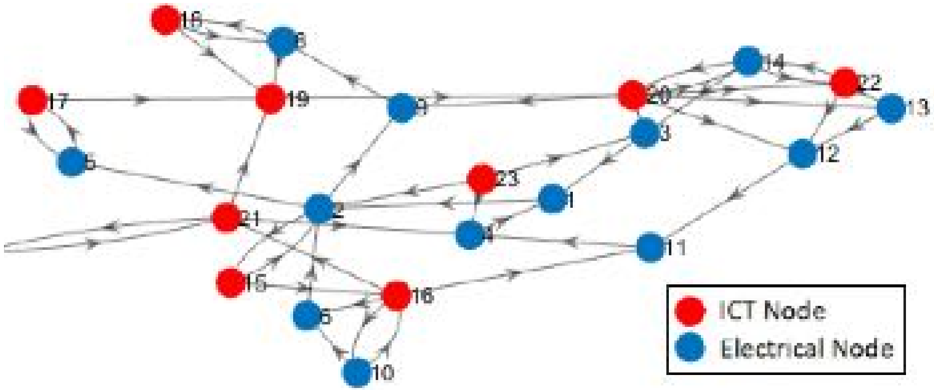


Autonomous ship – control flows

G. Kavallieratos, G. Spathoulas, S. Katsikas, "Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems", *Sensors*, Vol. 21, no. 1691, https://doi.org/10.3390/s21051691, 2021.

Dependency analysis

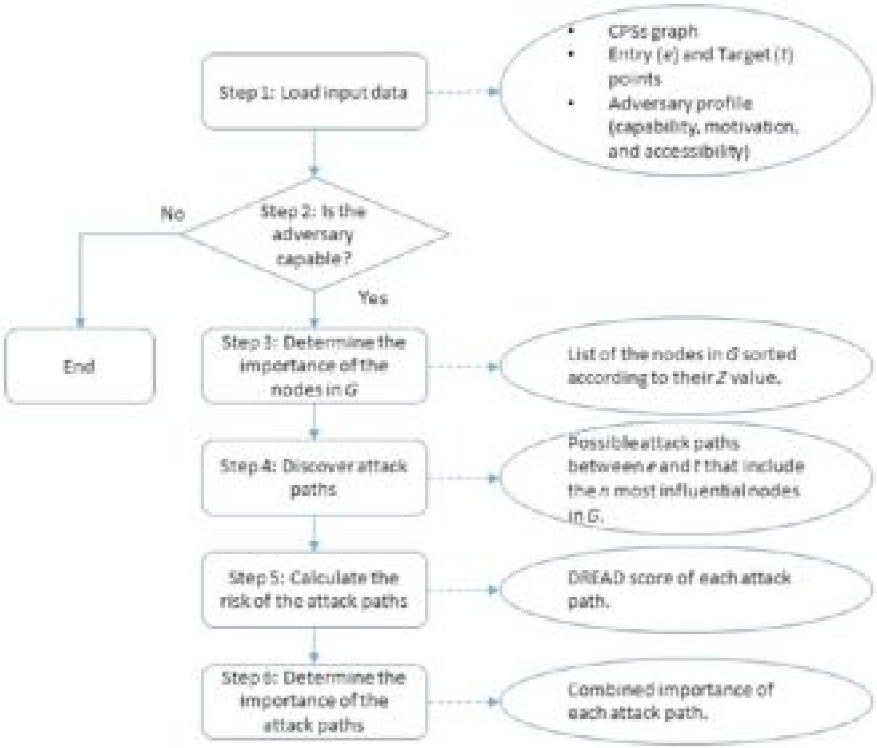




A. Akbarzadeh, S. Katsikas, “Identifying and analyzing dependencies in and among complex Cyber Physical Systems”, *Sensors*, Vol. 21, no. 5, art. No. 1685, https://doi.org/10.3390/s21051685, 2021.

Critical nodes and attack paths

Kavallieratos G., Katsikas S. (2020) Attack Path Analysis for Cyber Physical Systems. In: Katsikas S. et al. (eds) Computer Security. CyberICPS 2020, SECPRE 2020, ADIoT 2020. Lecture Notes in Computer Science, vol 12501. Springer, Cham. https://doi.org/10.1007/978-3-030-64330-0_2



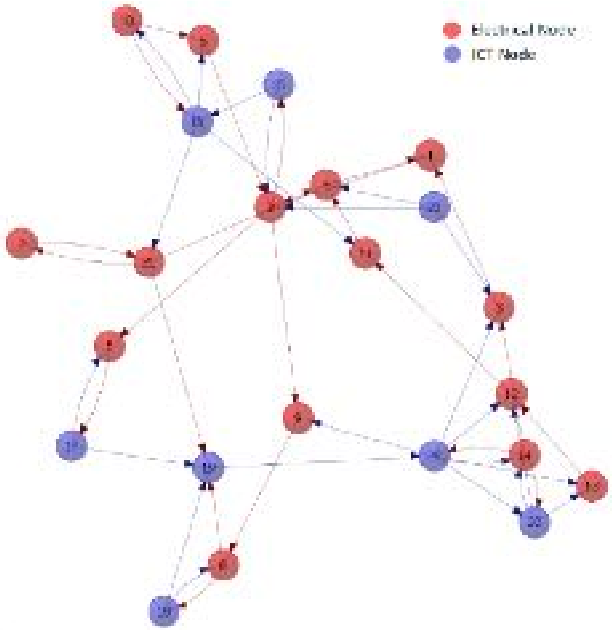
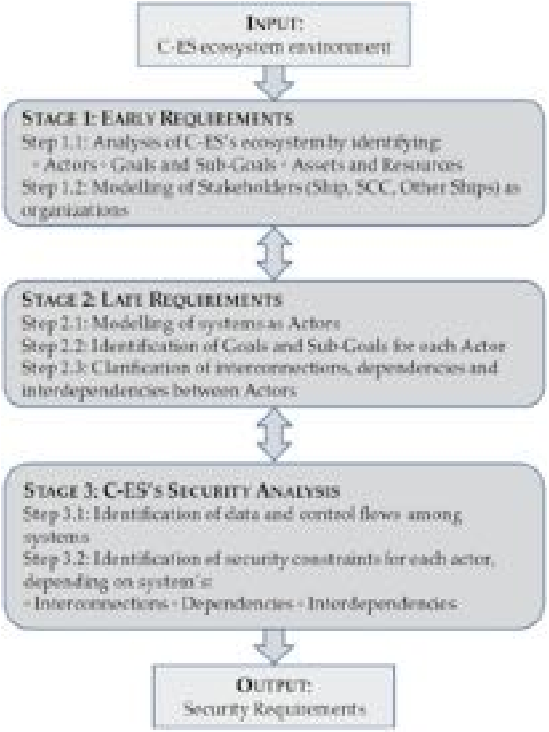


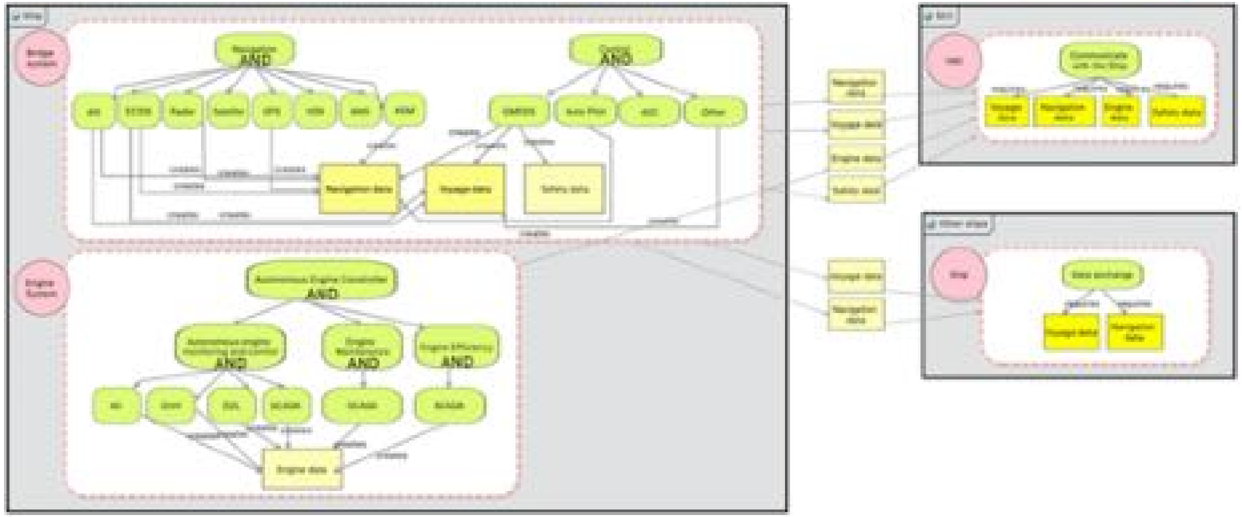
Figure 2: Directed graph G for the SINARI project system model [23]

A. Akbarzadeh and S. Katsikas, "Identifying Critical Components in Large Scale Cyber Physical Systems", in *Proceedings, 1st International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS 2020)*, Seoul, South Korea, 2020.

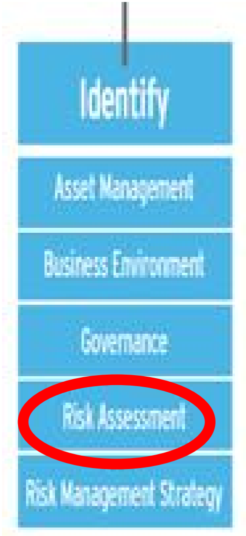
Security requirements elicitation

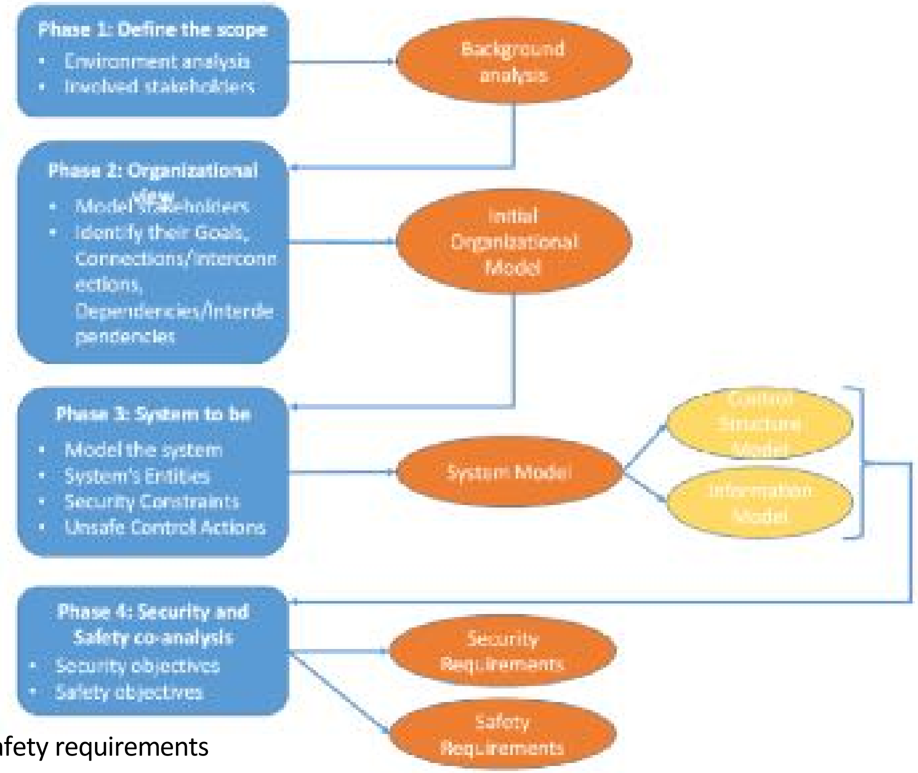


G. Kavallieratos, V. Diamantopoulou, S. Katsikas, “Shipping 4.0: Security requirements for the Cyber-Enabled Ship”, *IEEE Transactions on Industrial Informatics*, Vol. 16, issue 10, pp. 6617-6625, 2020doi: 10.1109/TII.2020.2976840.



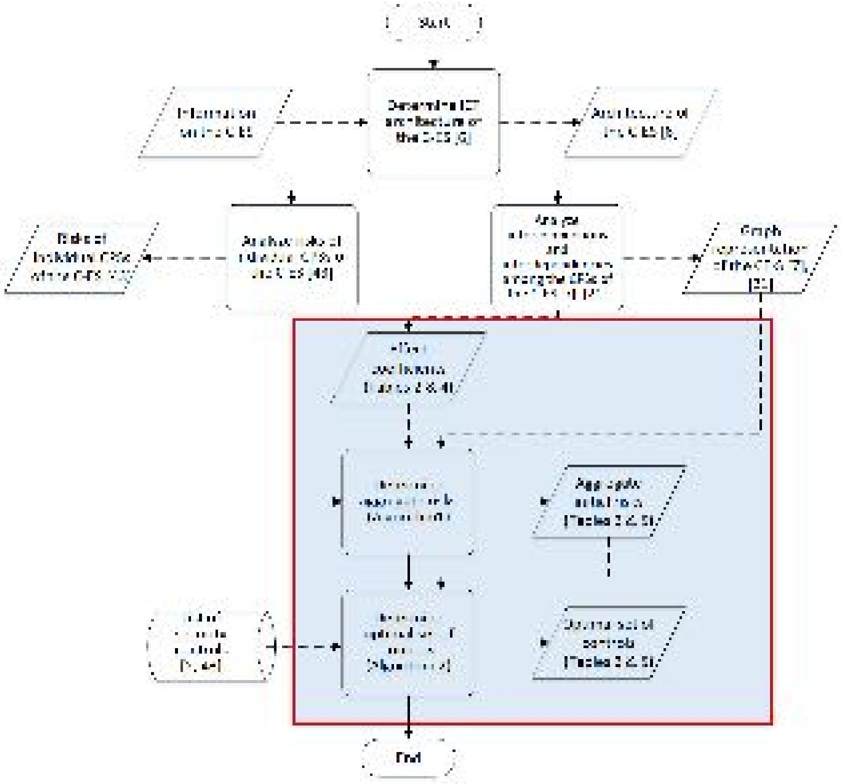
Combined safety and security requirements elicitation: SafeSecTropos





G. Kavallieratos, S. Katsikas, V. Gkioulos, "SafeSec Tropos: Joint security and safety requirements elicitation", *Computer Standards & Interfaces*, Volume 70, 2020.

Optimal control selection

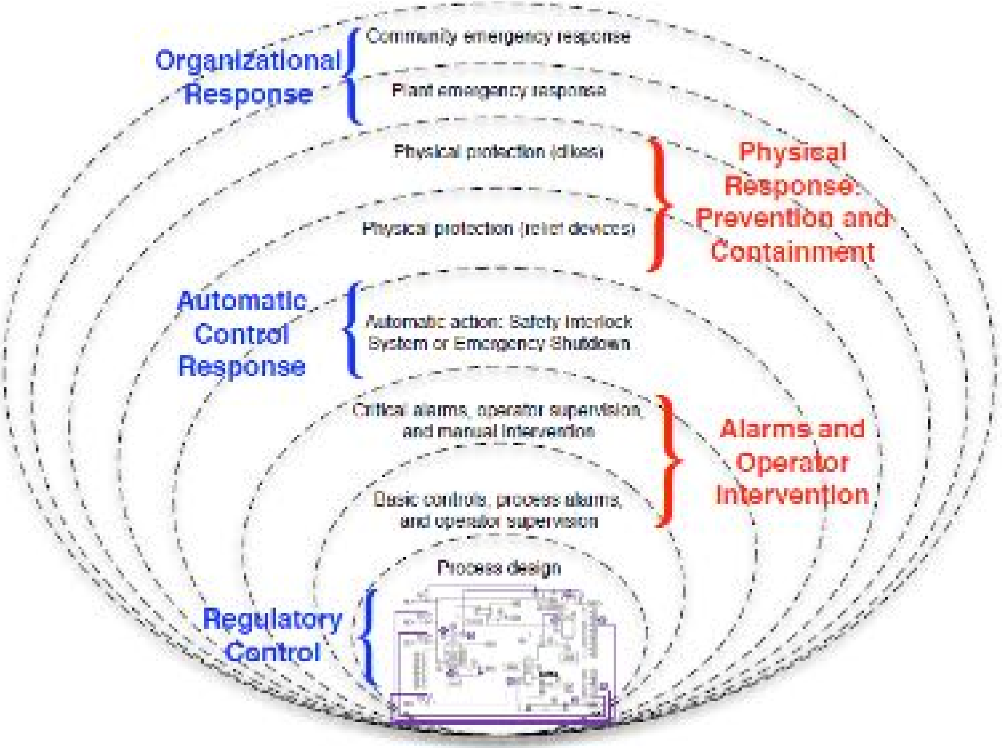


G. Kavallieratos, G. Spathoulas, S. Katsikas, "Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems", *Sensors*, Vol. 21, no. 1691, https://doi.org/10.3390/s21051691, 2021.

Protect

- Encryption
- Hardware security measures
  - Secure execution environment
  - IoT Trusted Execution Environment for Edge Devices (IoTEED)
  - Near Field Communication (NFC)
- Communication channels security
  - Use of a 5G radio access network for the industrial and tactile Internet of Things
  - Use of the Message Queuing Telemetry Transport (MQTT)
  - Network tunneling (Virtual Private Network - VPN)
- General protection approaches
  - A one-size-fits-all approach is usually not efficient, and there is no unique methodology that can protect all different IIoT installations
  - Flexible encryption algorithms, that enable more options than just encrypting and decrypting data
  - Blockchain technology

Protect: defense in depth

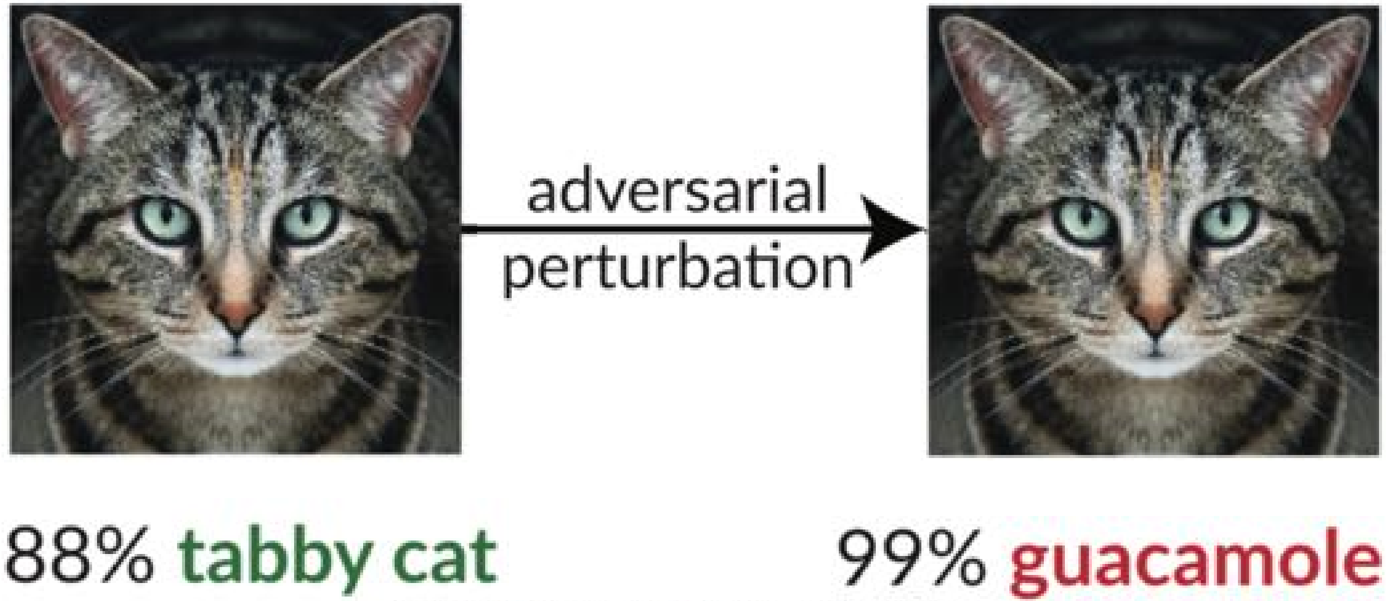


Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin, The Cyber Security Body of Knowledge, 2019.

- Protect
- Acess Control
- Awareness & Training
- Data Security
- Info Protection Process & Procedures
- Maintenance
- Protective Technology

Detect

- Intrusion detection for industrial control systems
  - Machine learning
  - Physical Process Monitoring (PPM)
  - Closed Control Loops (CCL)
  - Attack Sophistication (AS)
  - Legacy Technology (LT)
  - Knowledge-based designs are not effective on their own
    - Large storage requirement
    - Frequent dictionary updates needed
    - Unable to detect unknown attacks
  - Behavior-based designs are more effective
  - Behavior-specification–based designs are more effective
  - Physics-based/Process-aware IDS
  - Adaptive IDS

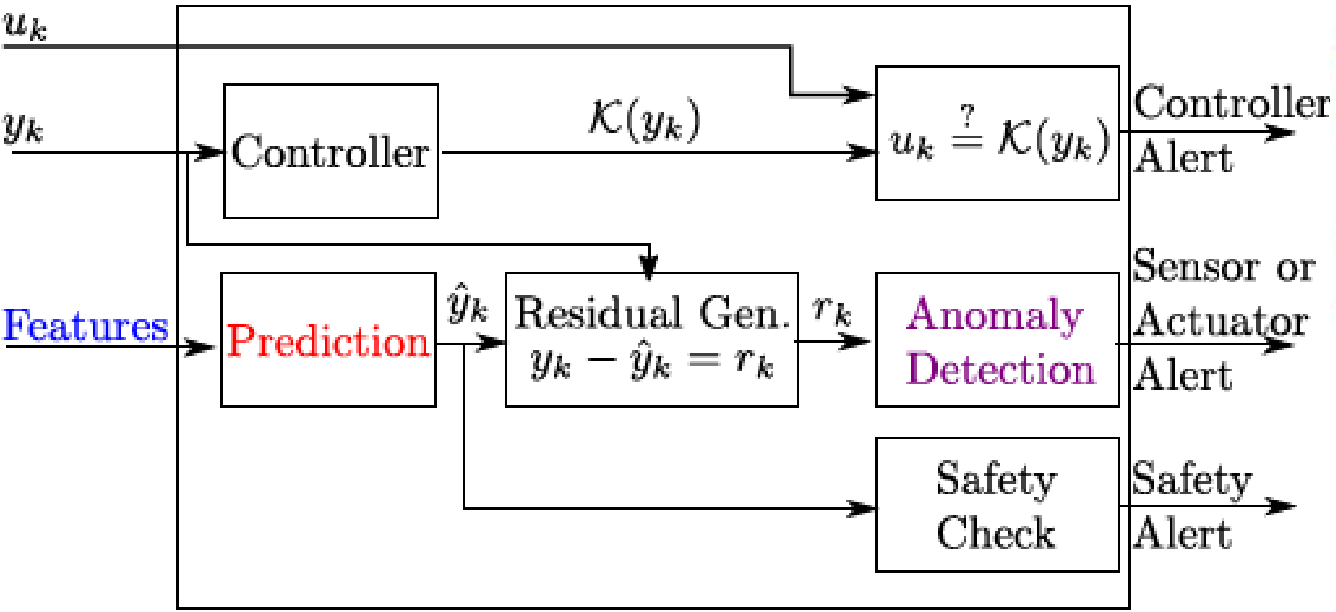


A Simple Explanation for the Existence of
Adversarial Examples
with Small Hamming Distance

Adi Shamir[1], Itay Safran[1], Eyal Ronen[2], and Orr Dunkelman[3]

[1] Computer Science Department, The Weizmann Institute, Rehovot, Israel
[2] Computer Science Department, Tel Aviv University, Tel Aviv, Israel
[3] Computer Science Department, University of Haifa, Israel

Physics-Based Attack Detection in Control Systems (3)



Nils Ole Tippenhauer, Justin Ruths, Richard Candell, Henrik Sandberg, Survey and New Directions for Physics-Based Attack Detection in Control Systems, NIST GCR 16-010, 2016.

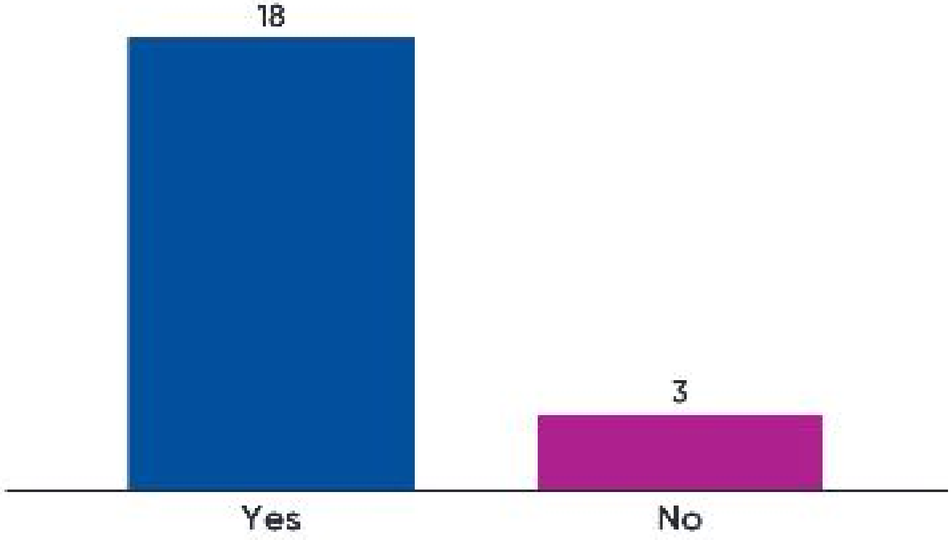
Is cybersecurity a science?

Hint: Science, any system of knowledge that is concerned with the physical world and its phenomena and that entails unbiased observations and systematic experimentation. In general, a science involves a pursuit of knowledge covering general truths or the operations of fundamental laws.

https://www.britannica.com/science/science

Go to **www.menti.com** and use the code **9238 6396**

Is cybersecurity a science?



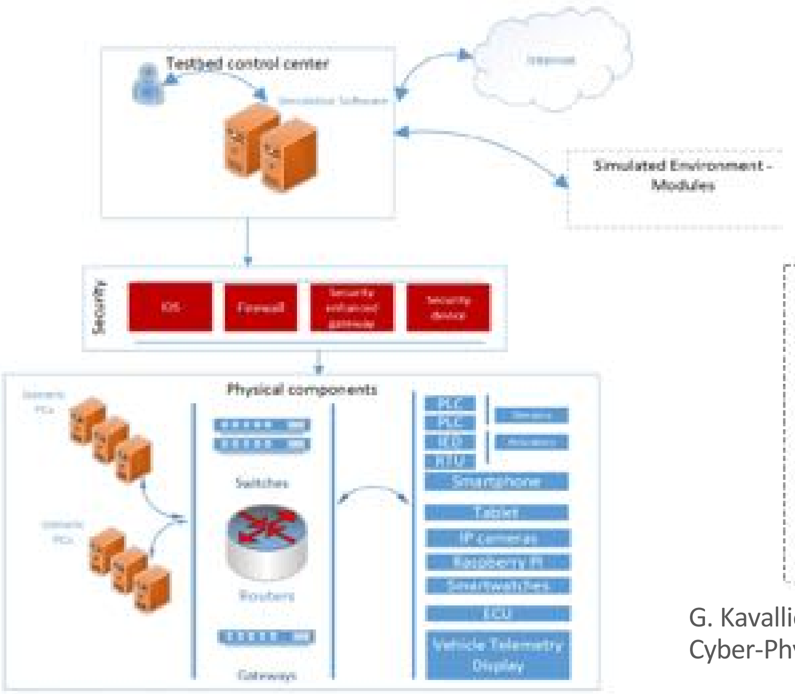
21

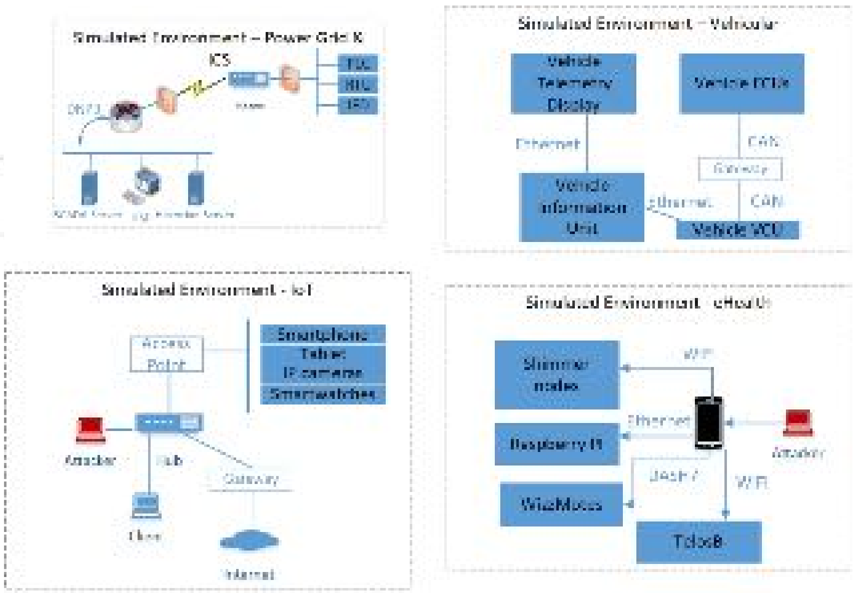
IIOT security research: testbed requirements

- Flexibility
- Scalability
- Isolation
- Interoperability
- Cost-Effectiveness
- Built in monitoring
- Easy access
- Adaptability
- Shareability

IIOT security testbed → cyber-physical range

IIOT security research: testbed reference architecture





G. Kavallieratos ,S. Katsikas, V. Gkioulos, «Towards a cyber-physical range», Proceedings, 5th ACM Cyber-Physical System Security Workshop (CPSS 2019), Auckland, New Zealand, pp. 25-34,

The Norwegian Cyber Range

- A digital cyber arena for:
- Research
- Education
- Training and exercise
- Testing

https://www.ntnu.no/ncr

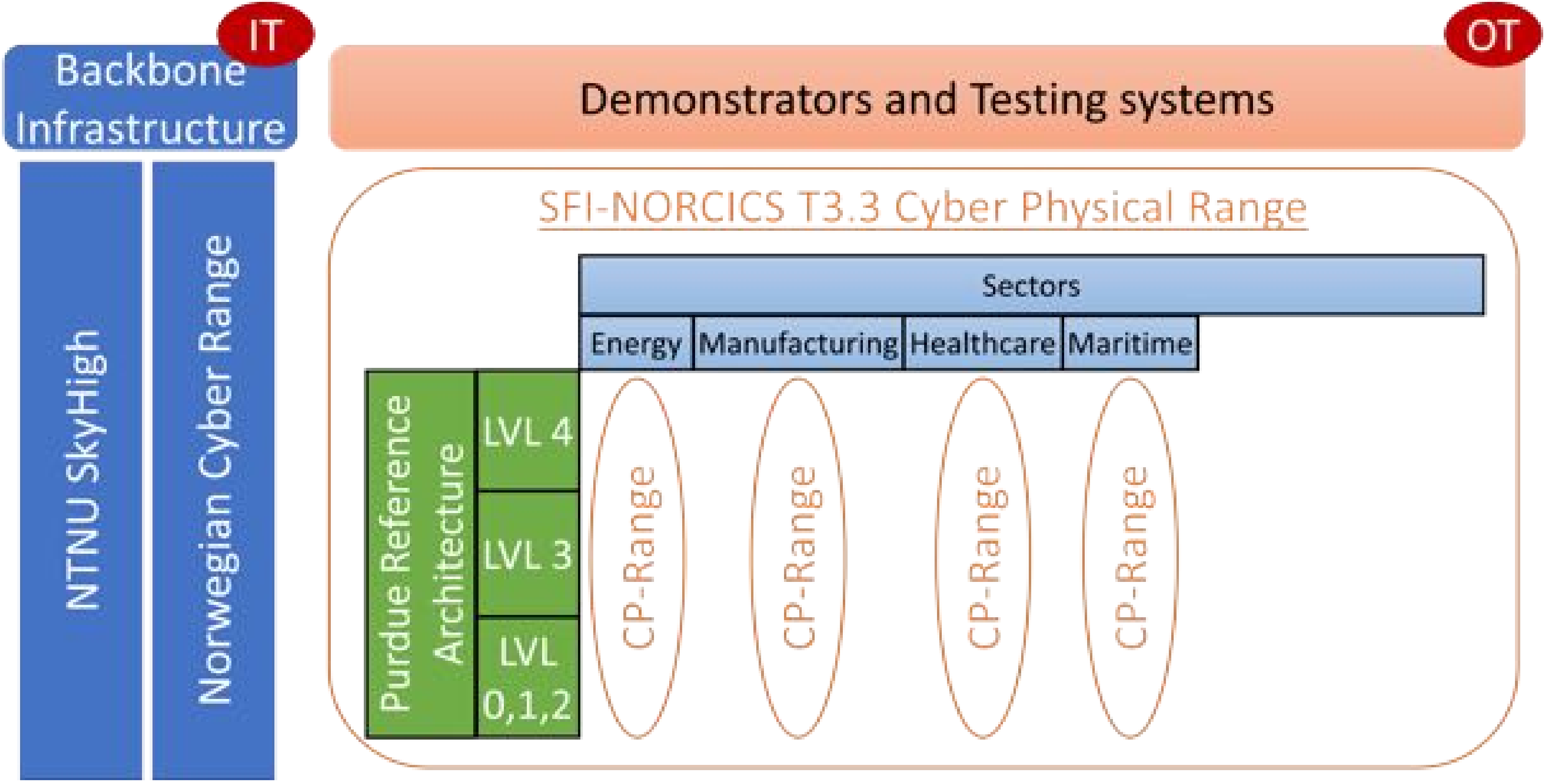
OPPLAND fylkeskommune | FORSVARET Cyberforsvaret | SIVILFORSVARET | telenor | EVRY | NorSIS

Innovasjon Norge | Republic of Estonia Ministry of Defence | Tallinn University of Technology | NTNU Kunnskap for en bedre verden

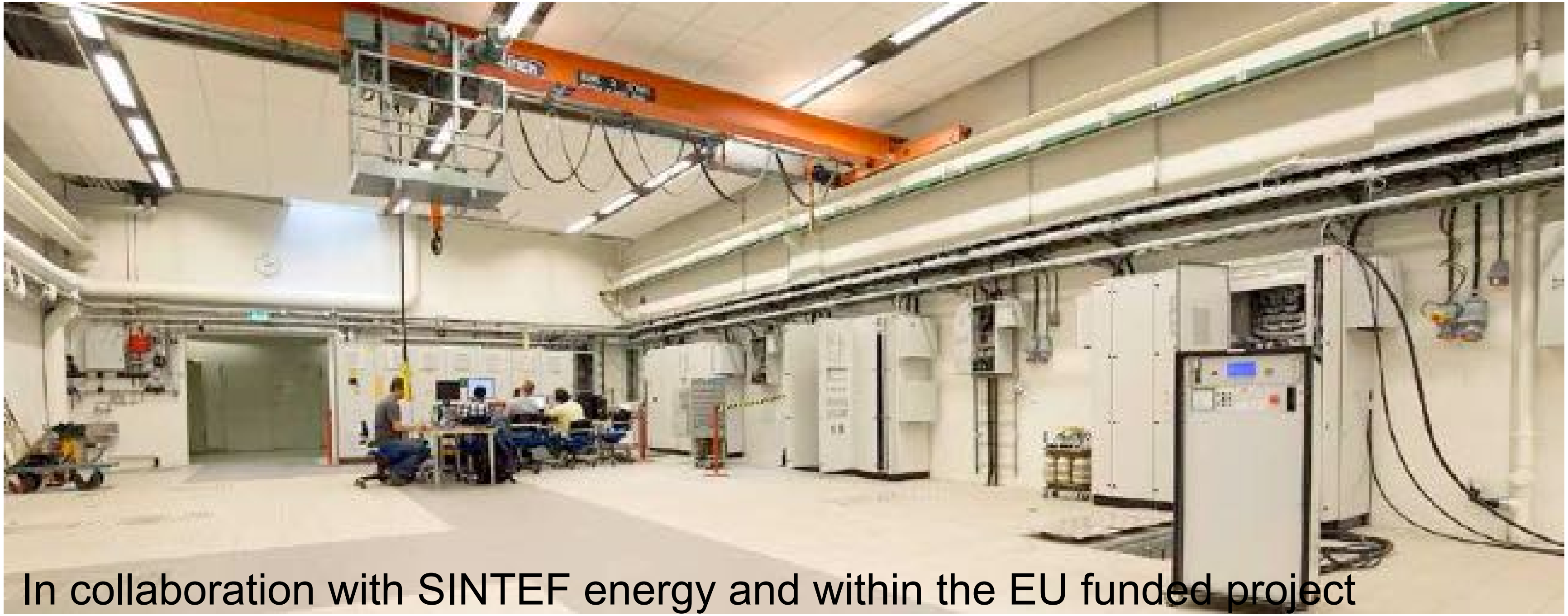
NCR and Cyber Security Challenges

- NCR runs the Norwegian Cyber Security Challenge
- Picks team for the European Cyber Security Challenge
- NCR will host ECSC in 2022
- Working on plans for A Nordic and Baltic CSC
  - Might run in late August

NCR <-> CP-Range


IT
Backbone Infrastructure
OT
Demonstrators and Testing systems
NTNU SkyHigh
Norwegian Cyber Range
SFI-NORCICS T3.3 Cyber Physical Range
Sectors
Energy
Manufacturing
Healthcare
Maritime
Purdue Reference Architecture
LVL 4
LVL 3
LVL 0,1,2
CP-Range
CP-Range
CP-Range
CP-Range

CP-Range (Energy-1)

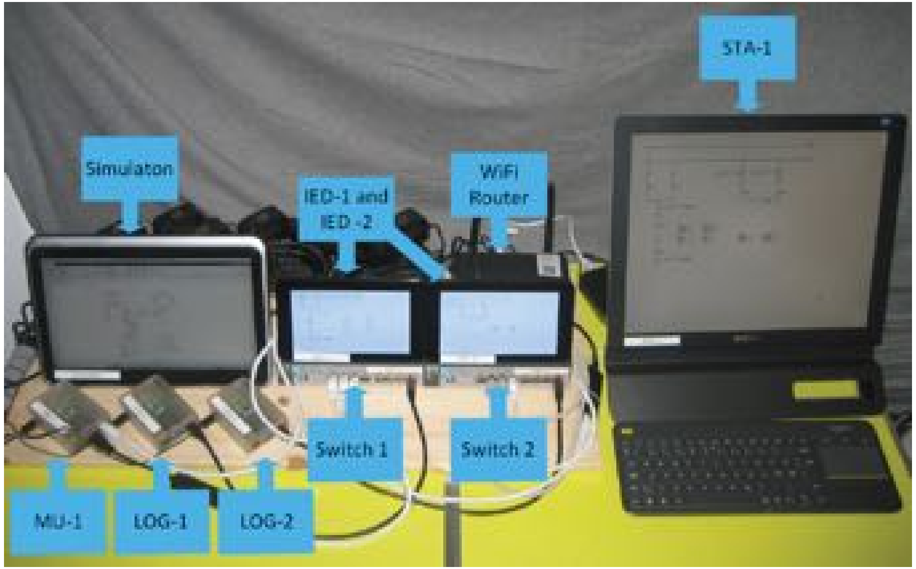


In collaboration with SINTEF energy and within the EU funded project SDNmicroSENSE we interfaced the CP-Range with the Smart grid laboratory, for testing and research in the energy domain.

CP-Range (Energy-2)

- NVE and KraftCert have supported the establishment of a SCADA laboratory at NTNU
  - S7-1500 systems are used as main CPU
  - This is augmented with Simatic TP1500 HMIs

- Activities in the lab
  - Construction of Emulated IEDs
  - Attacks against substations and regional control
  - Impact of migration to SDN substrate on IEC 61850 GOOSE/SV

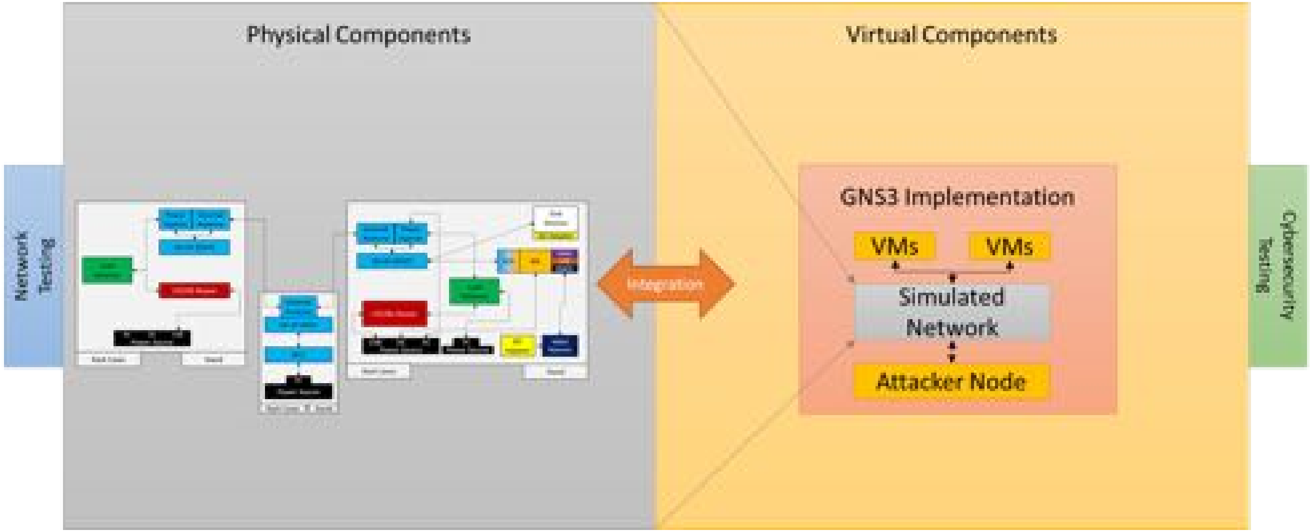


CP-Range (Manufacturing)

- In collaboration with Manulab and SINTEF manufacturing we are expanding existing FESTO infrastructure to support activities on Networks and IT security in the context of Industry 4.0

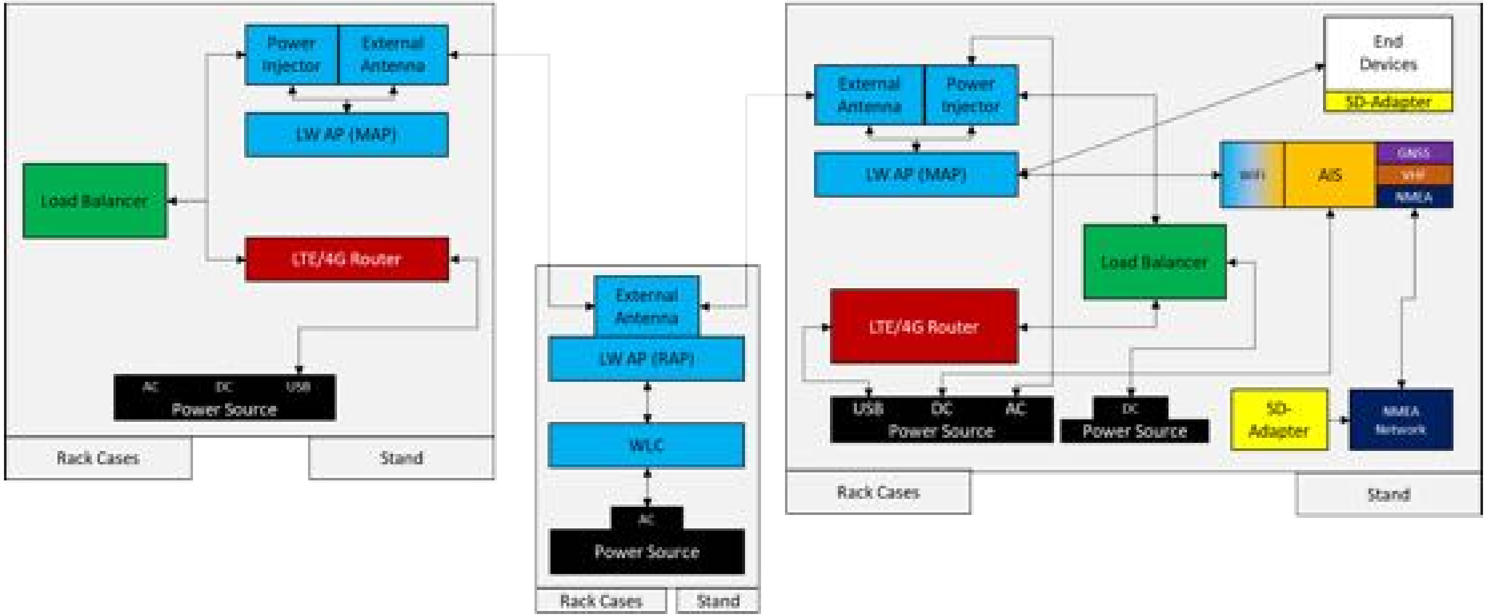
CP-Range (Maritime)

We are currently developing a laboratory setup for system security testing of both conventional and autonomous ships



CP-Range (Maritime)

Testbed Architecture: Physical



CP-Range (Maritime)

- We collaborate with NTNU Ålesund maritime simulators to support activities on Networks and IT security in the context of Shipping 4.0

NORCICS SFI

- Funding for 5(+3) years
- Total budget: 215,645,000 NOK
- Funding: 96,000,000 NOK NFR (41.9%)
- Coordinator (NTNU) + 18 partners (4 research, 14 user)
- Sectors represented: Energy, Manufacturing, Oil & Gas, Security, Healthcare, Police, Process industry

Annual workplan 2021 (extract)

Task/WP#	Title	Task leader	Start - End
WP2 - T2.2	Modelling distributed subversion attacks in cyber physical systems	Stephen Wolthusen (NTNU)	07.2021 – 06.2024
WP2 - T2.3	Digital Twin Security Models and Mechanisms	Vasileios Gkioulos (NTNU)	07.2021 – 06.2024
WP2 - T2.4	Human side of secure Industry 4.0	Halvor Holtskog (NTNU)	01.2021 - 12.2023
WP3 – T3.1.1	Assessing 5G and beyond as an element of critical services	Bjarne Helvik (NTNU)	04.2021 – 03.2024
WP3 - T3.1.2	Autonomous Adaptive Security for 5G-enabled IoT	Habtamu Abie (NR)	01.2021 – 12.2023
WP3 - T3.3.2	Reverse engineering lab	Geir Olav Dyrkolbotn (NTNU)	01.2021 – 12.2022
WP3 – T3.4	Humanised deep Learning & Big-data Analytics	Christian Walter Peter Omlin (UiA)	01.2021 – 12.2023
WP3 - T3.5.1	Codes for sub-millisecond latencies in 5G and beyond	Danilo Gligoroski (NTNU)	01.2021 – 12.2024
WP3 - T3.5.2	Secure broadcasting in wireless critical systems	Sigurd Eskeland (NR)	01.2021 – 12.2023

Conclusions

- IT-OT convergence gives rise to serious security challenges
- Simply porting security solutions from IT security paradigm does not suffice
- Securing legacy systems is equally important to securing modern (and future) architectures
- Several (exciting) open research problems exist
- (In)security situation is likely to continue for some time

Thank you!

"Collaboration = innovation"