Sécurité des Systèmes Industriels

Introduction aux Systèmes Industriels

Maxime Puys

22 mars 2025

Outline

1 Industrial Systems

2 Story of a Real Cyberattack : Stuxnet

3 Challenges

4 Regulation

Internet of Things

- □ Physical objects with sensors/actuators
- □ Having processing ability, software, etc
- □ Connected and exchanging data over Internet or other networks.
- □ Eg. appliance, factory, health, wearables, etc

Critical IoT

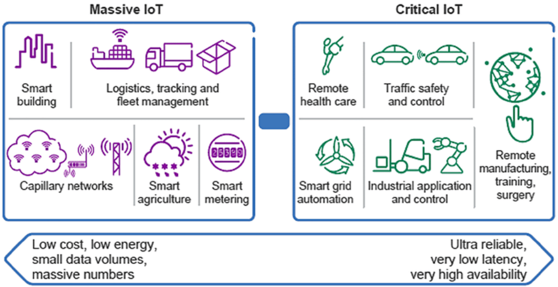

Massive IoT
Critical IoT
Smart building
Logistics, tracking and fleet management
Capillary networks
Smart agriculture
Smart metering
Remote health care
Traffic safety and control
Remote manufacturing, training, surgery
Smart grid automation
Industrial application and control
Low cost, low energy, small data volumes, massive numbers
Ultra reliable, very low latency, very high availability

Figure – Two types of IoT : [Alq19]

Massive IoT :

- □ Target collected/computed data ;
- □ Secrecy, privacy, integrity.

Critical IoT :

- □ Target physical process ;
- □ Availability, safety

Critical IoT

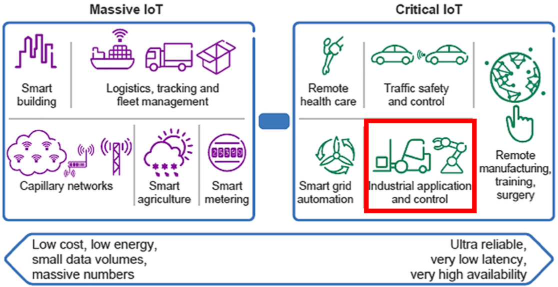

Massive IoT
Critical IoT
Smart building
Logistics, tracking and fleet management
Capillary networks
Smart agriculture
Smart metering
Remote health care
Traffic safety and control
Remote manufacturing, training, surgery
Smart grid automation
Industrial application and control
Low cost, low energy, small data volumes, massive numbers
Ultra reliable, very low latency, very high availability

Figure – Two types of IoT : [Alq19]

Massive IoT :

- □ Target collected/computed data ;
- □ Secrecy, privacy, integrity.

Critical IoT :

- □ Target physical process ;
- □ Availability, safety

Industrial Control Systems

Industrial Control Systems

Industrial Control Systems

Industrial Control Systems

Industrial Control Systems

Industrial Control Systems

Industrial Control Systems

Industrial Control Systems

Broken Myths and Legends

- □ Denial of reality :
  - ▷ ICS are isolated
  - ▷ ICS protocols and systems are incomprehensible
  - ▷ Security incidents dot not impact production
- □ Simplistic view of cybersecurity :
  - ▷ Cybersecurity can be added at the end
  - ▷ Safety protections will also handle cybersecurity

Cybersécurité des installations industrielles

Défendre ses systèmes numériques

Collectif sous la direction de
Yannick FOURASTIER
Ludovic PIETRE-CAMBACEDES

Cépaduès
EDITIONS

Properties to Ensure

For the process

Availability : System keeps running.

Integrity : Preservation of the coherence of a data over time.

Authenticity : An entity is who he/she pretends.

Non-repudiation : One cannot deny its actions.

⇒ **Safety :** Domain specific properties.

For customer data

Confidentiality : Only authorized entities can access designated data.

Privacy : Prevent linking a data with its owner.

Purdue Model

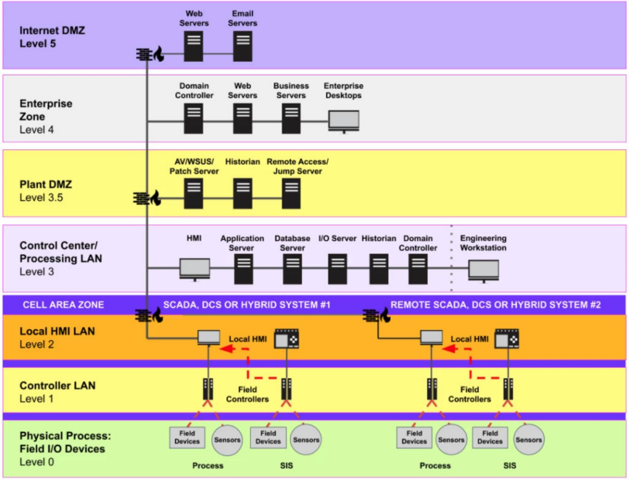


Figure – Purdue model [Wil90]

Industrial Systems (ICS) Composition 1/2

SCADA

PLC

Process

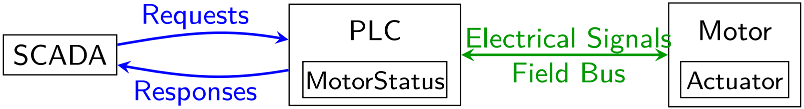
SCADA : Supervisory Control And Data Acquisition, controls and monitors the process.

PLC : Programmable Logic Controller, interprets SCADA orders for the process.

Process : Actual industrial process managed by the system.

Industrial Systems (ICS) Composition 2/2

- Variables on PLC synchronized with process.



SCADA

Requests

Responses

PLC

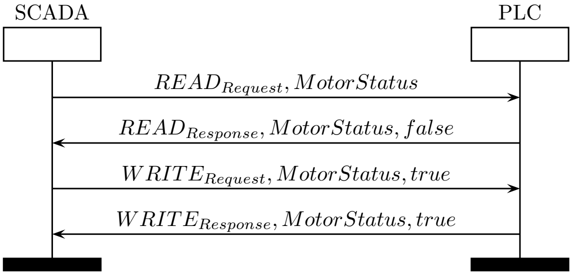
MotorStatus

Electrical Signals

Field Bus

Motor

Actuator



SCADA

PLC

$READ_{Request}, MotorStatus$

$READ_{Response}, MotorStatus, false$

$WRITE_{Request}, MotorStatus, true$

$WRITE_{Response}, MotorStatus, true$

Story of a Real Cyberattack : Stuxnet

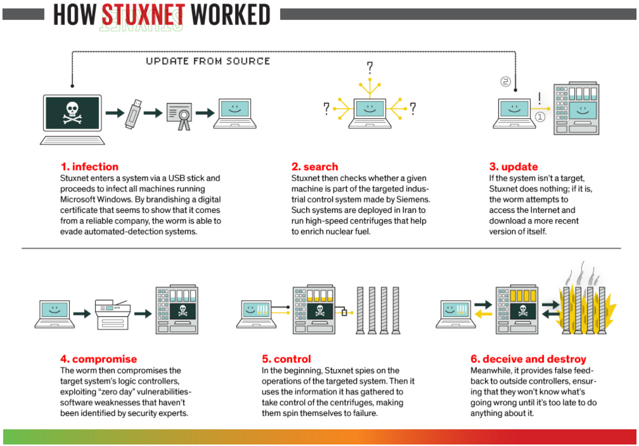
Introduction and Context

- **Stuxnet :** A sophisticated malware targeting industrial control systems (ICS), specifically PLCs (Programmable Logic Controllers).
- **Year of Discovery :** 2010, but believed to have been active since 2005.
- **Target :** Iran's nuclear enrichment facility at Natanz.
- **Objective :** Sabotage uranium enrichment by causing centrifuges to spin at destructive speeds.
- **Context :** Stuxnet was likely developed by nation-states (suspected collaboration between the U.S. and Israel) as part of a cyberwarfare strategy.

Attack Preparation

- **Reconnaissance :**
  - Detailed knowledge of Siemens Step7 software and PLCs used in Natanz.
  - Intelligence on Iran's centrifuge configurations (P-1 centrifuges).
- **Zero-Day Vulnerabilities :**
  - Utilized Windows and Siemens zero-day exploits.
- **Delivery Mechanisms :**
  - USB drives to bypass air-gapped systems.

Attack Launch



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Figure – The Real Story of Stuxnet - IEEE Spectrum

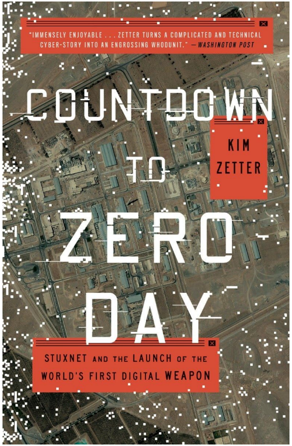
Effects of the Attack

- **Physical Impact :**
  - Caused centrifuge rotors to spin at destructive speeds, leading to mechanical failure.
  - Destroyed over 1,000 centrifuges at Natanz.
- **Operational Disruption :**
  - Significantly delayed Iran's nuclear enrichment program.
  - No immediate detection due to fake operational data.
- **Wider Implications :**
  - First documented cyberattack causing physical damage.
  - Demonstrated the potential of cyberwarfare on critical infrastructure.

Consequences and Lessons Learned

- **Global Consequences :**
  - Accelerated focus on ICS cybersecurity globally.
  - Raised awareness of vulnerabilities in air-gapped systems.
- **Nation-State Cyberwarfare :**
  - Highlighted the role of nation-states in offensive cyber operations.
  - Set a precedent for cyberweapons targeting critical infrastructure.
- **Technical Lessons :**
  - Importance of securing ICS protocols like MODBUS.
  - Necessity for robust patch management and zero-day defenses.

Summary of Attack Vectors


"IMMENSELY ENJOYABLE . . . ZETTER TURNS A COMPLICATED AND TECHNICAL CYBER-STORY INTO AN ENGROSSING WHODUNIT." — WASHINGTON POST
COUNTDOWN TO ZERO DAY
KIM ZETTER
STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON

□ **Zero-Day Exploits :** Leveraged multiple unpatched vulnerabilities in Windows.

□ **USB Propagation :** Bypassed air-gapped systems.

□ **ICS-Specific Exploits :**

- ▷ Compromised Siemens Step7 software.
- ▷ Exploited MODBUS protocol to manipulate PLCs.

□ **Stealth Features :**

- ▷ Rootkit to evade detection.
- ▷ Fake operational data to mislead operators.

Challenges

Safety vs. Cybersecurity

Security concepts

- □ Safety = Protection against identified/natural difficulties.
  - ▷ Historic industrial concern.
- □ Cybersecurity = Protection against malicious adversaries.
  - ▷ Often called Security.

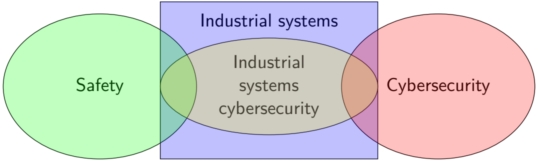
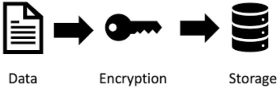


Figure – Relations among security concepts

Safety vs. Cybersecurity

- □ **Assets :** Physical infrastructure (indirectly : human life, environment, etc)
- □ **Security Properties :**
  - ▷ Availability
  - ▷ Safety (domain specific)

- □ **Assets :** Data and systems offering a digital service
- □ **Security Properties :**
  - ▷ Confidentiality
  - ▷ Integrity
  - ▷ Availability



Digital Twins

- Need to replicate ICS for testing purpose :
  - Attack testing
  - Counter-measure testing
  - Updates/patch testing

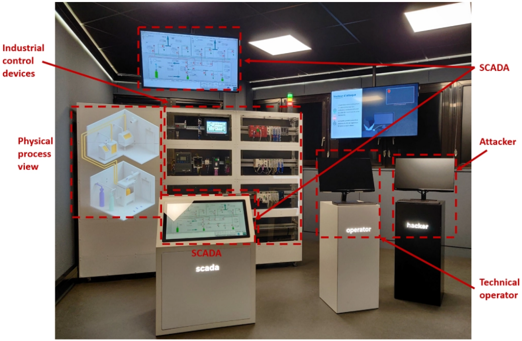


Figure – WonderICS platform [PTM21]

- Multiple levels of abstraction :
  - **Simulation :** New platform that mimics the desired behavior.
  - **Virtualization :** Virtualize/emulate process and/or control equipment to some degree (virtualized hardware, firmware, etc) in an heterogeneous fashion.
  - **Hardware-In-The-Loop :** Mixing simulation with real off-the-shelf industrial components.

Proprietary World

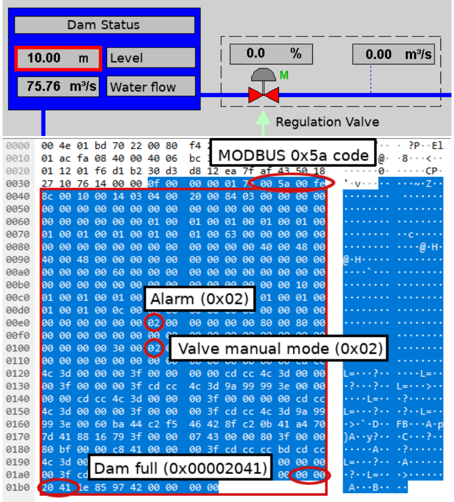
- Public norms but closed specs
- Closed devices :
  - No open source software
  - No open source hardware
- Each vendor has their own comm protocol, software, and sometimes hardware

⇒ Huge work on reverse engineering

Insecure World

- ICS devices have a huge lifespan ($>$ 10 years)
- Barely any security :
  - Industrial protocols have no security
  - Devices are not hardened
- Pure IT attacks :
  - Ransomware (Saint-Gobain, Merck, Continental, Tchernobyl, etc)
  - Social Engineering, etc
- Attacks link to physical process :
  - Manufacturing secrets disclosure
  - Sabotage

Attack Example [Lef20]



Dam Status

10.00 m Level

75.76 m³/s Water flow

0.0 %

0.00 m³/s

```
0000  00 4e 01 bd 70 22 00 80  f4                                    ?P··El
0010  01 ac fa 08 40 00 40 06  bc                              @·  ·8···<··
0020  01 12 01 f6 d1 b2 30 d3  d8 12 ea 7f af 43 50 18   ······0· ·····CP·
0030  27 10 76 14 00 00 0f 00  00 00 01 7e 00 5a 00 fe   '·v····· ····~·Z··
0040  8c 00 10 00 14 03 04 00  20 00 84 03 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 01 00  01 00 01 00 01 00 01 00   ········ ········
0070  01 00 01 00 01 00 01 00  01 00 63 00 00 00 00 00   ········ ··c·····
0080  00 00 00 00 00 00 00 00  00 00 00 00 40 00 48 00   ········ ····@·H·
0090  40 00 48 00 00 00 00 00  00 00 00 00 00 00 00 00   @·H····· ········
00a0  00 00 00 00 60 00 00 00  00 00 00 00 00 00 00 00   ····`··· ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 10 00   ········ ········
00c0  01 00 01 00 01 00                    01 00 01 00   ········ ········
00d0  01 00 01 00 0c 00                    00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 02 00  00 00 00 00 80 00 80 00   ········ ········
00f0  00 00 00 00 00 00 00                                        ········
0100  00 00 00 00 30 00 02                                        ········
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 cd cc            ········
0120  4c 3d 00 00 00 3f 00 00  00 00 cd cc 4c 3d 00 00   L=···?·· ····L=··
0130  00 3f 00 00 00 3f cd cc  4c 3d 9a 99 99 3e 00 00   ·?···?·· L=···>··
0140  00 00 cd cc 4c 3d 00 00  00 3f 00 00 00 00 cd cc   ····L=·· ·?······
0150  4c 3d 00 00 00 3f 00 00  00 3f cd cc 4c 3d 9a 99   L=···?·· ·?··L=··
0160  99 3e 00 60 ba 44 c2 f5  46 42 8f c2 0b 41 a4 70   ·>·`·D·· FB···A·p
0170  7d 41 88 16 79 3f 00 00  07 43 00 00 80 3f 00 00   }A··y?·· ·C···?··
0180  80 bf 00 00 c8 41 00 00  00 3f cd cc cc bd cd cc   ·····A·· ·?······
0190  4c 3d 00                          00 00 00   L=···?·· ·A······
01a0  00 3f cd                          00 00 00   ·?··L=·· ·>······
01b0  20 41 1e 85 97 42 00 00  00 00                      A···B·· ··
```

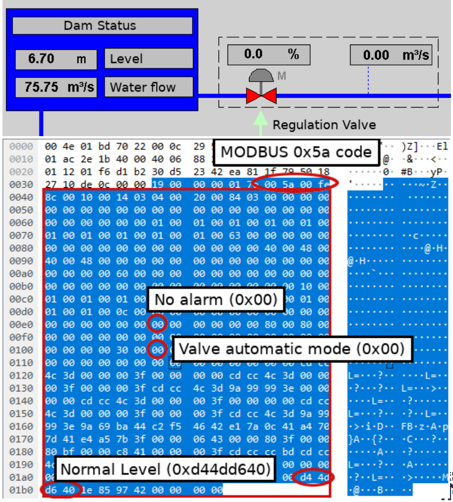
MODBUS 0x5a code

Alarm (0x02)

Valve manual mode (0x02)

Dam full (0x00002041)

Figure – Before Attack



Dam Status

6.70 m Level

75.75 m³/s Water flow

0.0 %

0.00 m³/s

```
0000  00 4e 01 bd 70 22 00 0c  29                                  )Z]···El
0010  01 ac 2e 1b 40 00 40 06  88                              @·  ·&···<··
0020  01 12 01 f6 d1 b2 30 d5  23 42 ea 81 1f 79 50 18   ······0· #B···yP·
0030  27 10 de 0c 00 00 19 00  00 00 01 7e 00 5a 00 fe   '······· ····~·Z··
0040  8c 00 10 00 14 03 04 00  20 00 84 03 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 01 00  01 00 01 00 01 00 01 00   ········ ········
0070  01 00 01 00 01 00 01 00  01 00 63 00 00 00 00 00   ········ ··c·····
0080  00 00 00 00 00 00 00 00  00 00 00 00 40 00 48 00   ········ ····@·H·
0090  40 00 48 00 00 00 00 00  00 00 00 00 00 00 00 00   @·H····· ········
00a0  00 00 00 00 60 00 00 00  00 00 00 00 00 00 00 00   ····`··· ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 10 00   ········ ········
00c0  01 00 01 00 01 00                       00 01 00   ········ ········
00d0  01 00 01 00 0c 00                       00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 80 00 80 00   ········ ········
00f0  00 00 00 00 00 00 00                                        ········
0100  00 00 00 00 30 00 00                                        ········
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 cd cc   ········ ········
0120  4c 3d 00 00 00 3f 00 00  00 00 cd cc 4c 3d 00 00   L=···?·· ····L=··
0130  00 3f 00 00 00 3f cd cc  4c 3d 9a 99 99 3e 00 00   ·?···?·· L=···>··
0140  00 00 cd cc 4c 3d 00 00  00 3f 00 00 00 00 cd cc   ····L=·· ·?······
0150  4c 3d 00 00 00 3f 00 00  00 3f cd cc 4c 3d 9a 99   L=···?·· ·?··L=··
0160  99 3e 9a 69 ba 44 c2 f5  46 42 e1 7a 0c 41 a4 70   ·>·i·D·· FB·z·A·p
0170  7d 41 e4 a5 7b 3f 00 00  06 43 00 00 80 3f 00 00   }A··{?·· ·C···?··
0180  80 bf 00 00 c8 41 00 00  00 3f cd cc cc bd cd cc   ·····A·· ·?······
0190  4c                                      00 00 00   L=···?·· ·A······
01a0  00                                      00 d4 4d   ·?··L=·· ·>······
01b0  d6 40 1e 85 97 42 00 00  00 00                     ·@···B·· ··
```

MODBUS 0x5a code

No alarm (0x00)

Valve automatic mode (0x00)

Normal Level (0xd44dd640)

Figure — After Attack

Regulation

Legal Status for ICS

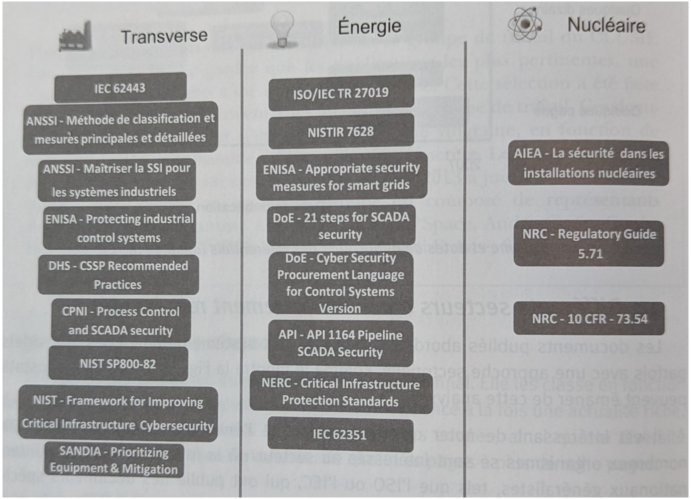
Safety related status

- □ SEVESO - EU directive, status according to threshold of dangerous substances
- □ ICPE - FR directive regarding impacts on environment, includes SEVESO

Cybersecurity related status

- □ SAIV - *Secteurs d'Activités d'Importance Vitale* (e.g., Energy)
- □ OIV - *Opérateurs d'Importance Vitale* (e.g., EDF)
- □ PIV - *Points d'Importance Vitale* (e.g., Tricastin nuclear plant)

Overview of ICS Cybersecurity Norms



Transverse

- IEC 62443
- ANSSI - Méthode de classification et mesures principales et détaillées
- ANSSI - Maîtriser la SSI pour les systèmes industriels
- ENISA - Protecting industrial control systems
- DHS - CSSP Recommended Practices
- CPNI - Process Control and SCADA security
- NIST SP800-82
- NIST - Framework for Improving Critical Infrastructure Cybersecurity
- SANDIA - Prioritizing Equipment & Mitigation

Énergie

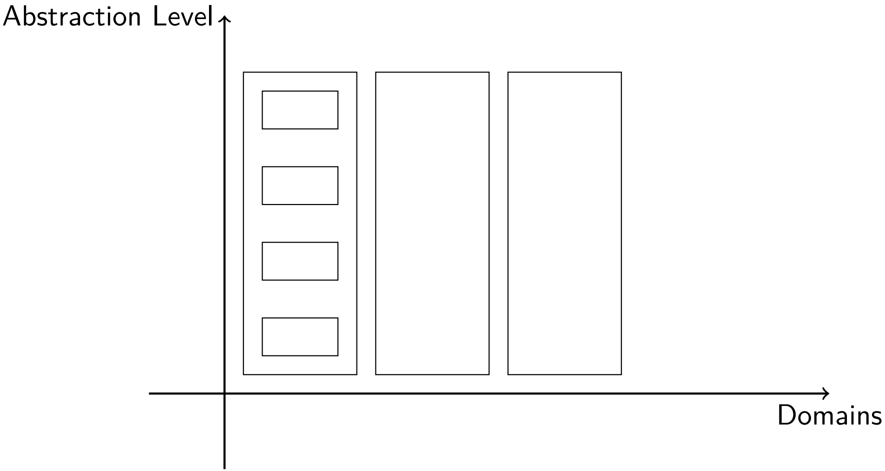
- ISO/IEC TR 27019
- NISTIR 7628
- ENISA - Appropriate security measures for smart grids
- DoE - 21 steps for SCADA security
- DoE - Cyber Security Procurement Language for Control Systems Version
- API - API 1164 Pipeline SCADA Security
- NERC - Critical Infrastructure Protection Standards
- IEC 62351

Nucléaire

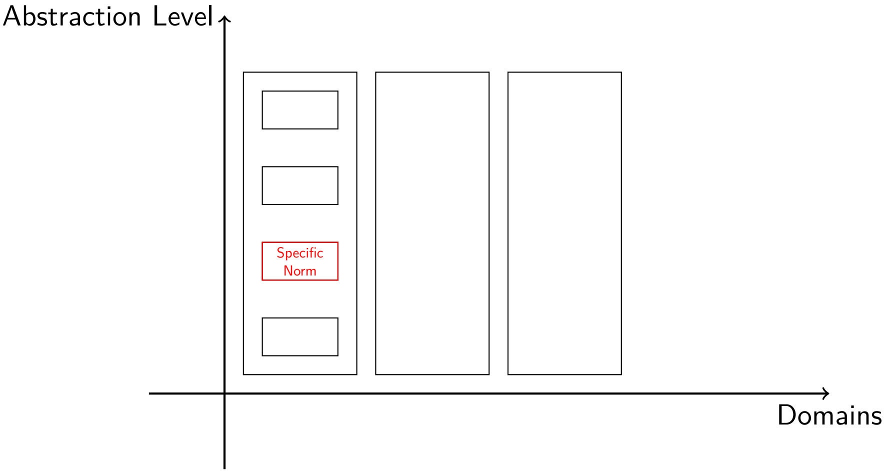
- AIEA - La sécurité dans les installations nucléaires
- NRC - Regulatory Guide 5.71
- NRC - 10 CFR - 73.54

Figure – [PCET^{+}15]

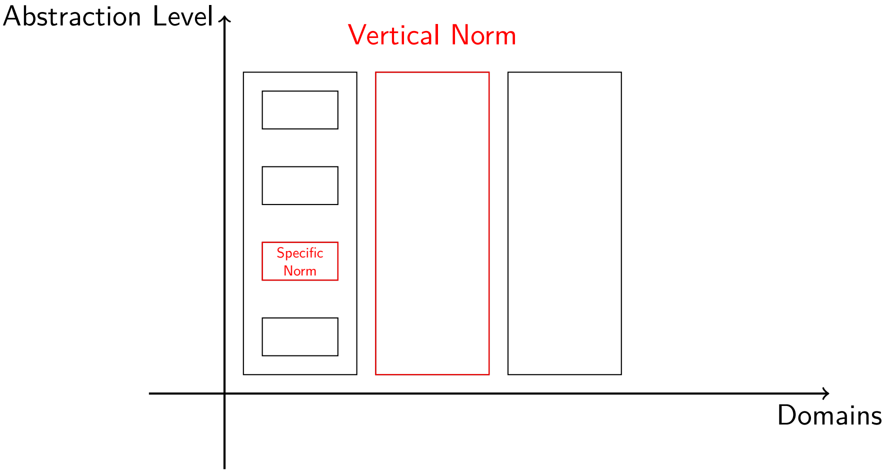
Vertical and Horizontal Norms



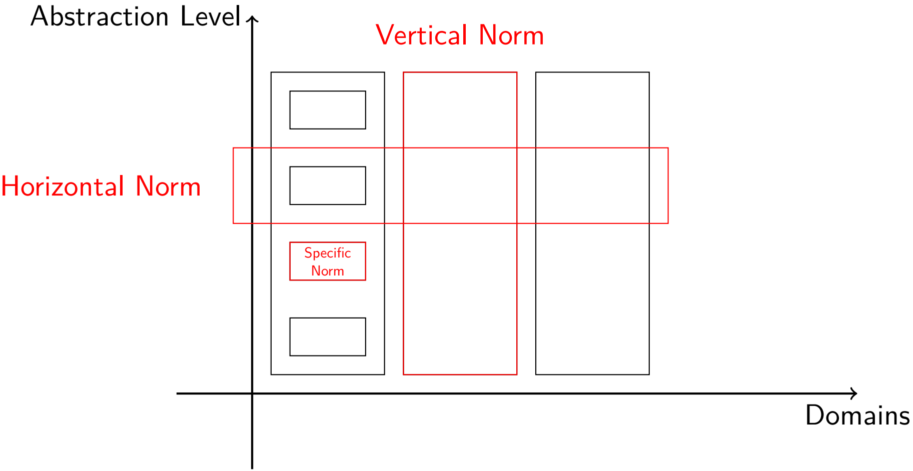
Vertical and Horizontal Norms



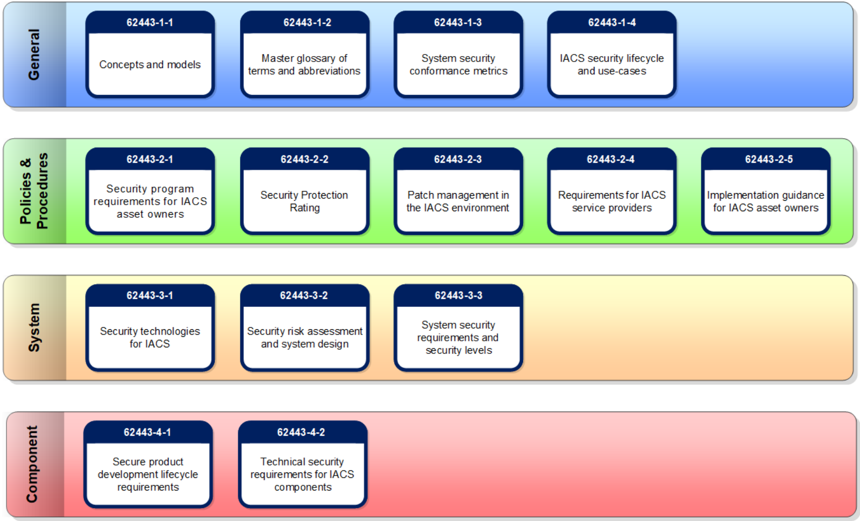
Vertical and Horizontal Norms



Vertical and Horizontal Norms



IEC 62443



General

- 62443-1-1: Concepts and models
- 62443-1-2: Master glossary of terms and abbreviations
- 62443-1-3: System security conformance metrics
- 62443-1-4: IACS security lifecycle and use-cases

Policies & Procedures

- 62443-2-1: Security program requirements for IACS asset owners
- 62443-2-2: Security Protection Rating
- 62443-2-3: Patch management in the IACS environment
- 62443-2-4: Requirements for IACS service providers
- 62443-2-5: Implementation guidance for IACS asset owners

System

- 62443-3-1: Security technologies for IACS
- 62443-3-2: Security risk assessment and system design
- 62443-3-3: System security requirements and security levels

Component

- 62443-4-1: Secure product development lifecycle requirements
- 62443-4-2: Technical security requirements for IACS components

Cyber Resilience Act (CRA) [PDL22]

- **Adopted in 2022, details not finalized and may be subject to changes**

Global concepts

- Horizontal legislation
- Security monitored during lifecycle (up to 5 years after product is put on the market)
- All products will have to comply to a certain scheme
- Retailers will have to ensure that the products they sell is compliant
- In case of new vulnerability, communication must be released within 24h

Two levels

- Level 1 ($\approx$ 90% of products) : self-assessment
- Level 2 (critical devices) : mandatory certification (ETSI 303 645, specific schemes ?)

Conclusion

Conclusion

- Industrial systems currently lack security
- Important regulation effort
- Leading to an important technical effort from vendors
- Yet, huge work to be done for secure systems and device to be in place
- Yet, multidisciplinary field, requiring hybrid knowledge :
  - Will require new positions in companies or new skill for team in place

Conclusion

Thanks for your attention !

References I

- Salman Alqahtani, *Performance evaluation of a priority-based resource allocation scheme for multiclass services in iot*, International Journal of Communication Systems **32** (2019), no. 18, e4151.
- Fabien Lefebvre, *Recherche de vulnérabilités dans les protocoles de communication industriels*, Tech. report, Univ. Grenoble Alpes, 2020.
- Ludovic Pietre-Cambacedes, Yannick Fourastier, Fabrice Téa, Laurent Platel, David Boucart, Peslouan Nicolas de, Orion Ragozin, Patrice Bock, Jean-Claude Jabot, Pascal Sitbon, Marc Bouissou, Gérôme Billois, Pierre Kobes, Frédéric Guyomard, Stéphane Meynet, Thomas Demongeot, Frédéric Duflot, Mathieu Feuillet, and Thierry Lusseyran, *Cybersécurité des installations industrielles : défendre ses systèmes numériques*, Cépadusès, 2015.

References II

- Car Polona and Stefano De Luca, *Eu cyber-resilience act*, EPRS : European Parliamentary Research Service (2022).

- Maxime Puys, Pierre-Henri Thevenon, and Stéphane Mocanu, *Hardware-In-The-Loop Labs for SCADA Cybersecurity Awareness and Training*, Proc. of the 16th ACM International Conference on Availability, Reliability and Security (ARES), Virtual Conference, ACM, August 2021, pp. 1–10.

- Theodore J. Williams, *A reference model for computer integrated manufacturing (CIM)*, Proc. of the 11th IFAC World Congress on Automatic Control, Tallinn, Finland **23** (1990), 281–291.