# Security of cyber-physical systems: an old idea

## Security Issues and Mitigation in Ethernet POWERLINK

*Jonathan Yung*, Hervé Debar and Louis Granboulan

AIRBUS Group Innovations & Télécom SudParis

February 10th, 2017

# Recurrent issues in cyber-security

- Name changes, keywords and buzzwords
  - Information systems security $\rightarrow$ cyber-security
  - Intrusion detection $\rightarrow$ anomaly detection
  - Big data
  - Artificial intelligence
- Really represent persistent issues in IT
  - Security as an afterthought
  - Security as an overkill
  - Security without expectations
  - Security without specifications
  - ...

# Can we construct a better approach ?

- Safety has clear pre-specified expectations.
  - Standardized constraints
- Industrial control systems have clear specifications.
  - Control loop
- Can we leverage these two old ideas for better security ?
- *Old keyword: Resilience*

# Outline

# ICS

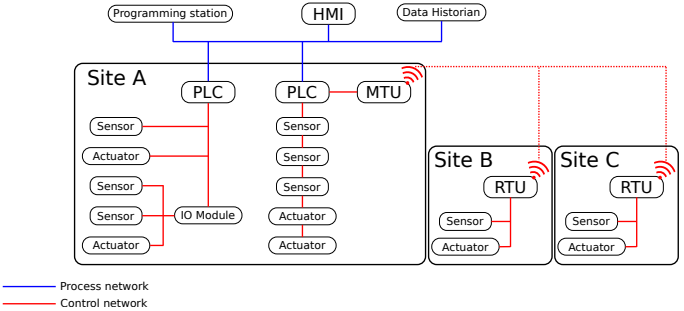
## Industrial Control System

System composed of devices producing data (sensors), and of devices which will act depending of this data (actuator) and of a program.


# ICS

## Industrial Control System

System composed of devices producing data (sensors), and of devices which will act depending of this data (actuator) and of a program.



# Industrial Ethernet Protocols

- Adaptation of the Fieldbus protocols on Ethernet.
- Classified in three types:
  - Class 1 (soft real-time): MODBUS/TCP, EtherNet/IP
  - Class 2 (hard real-time): PROFINET (RT)
  - Class 3 (isochronous real-time): PROFINET IRT, Ethernet POWERLINK, EtherCAT

# Attack State of the Art

| Attack | MODBUS/TCP (C1) | EtherNet/IP (C1) | PROFINET RT (C2) |
|---|---|---|---|
| Eavesdropping | Huitsing et al.[5]<br>Bristow[4] | | |
| Interruption | Huitsing et al.[5]<br>Queiroz[7] | Digital Bond[3] | Paul et al.[6] |
| Modification | Huitsing et al.[5] | Antonioli et al.[2] | Åkerberg et al.[1]<br>Paul et al.[6] |
| Insertion | Huitsing et al.[5] | Digital Bond[3] | Åkerberg et al.[1] |

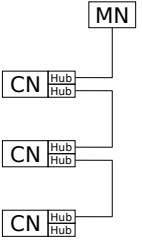
# Goal of this presentation

- Literature already presents attacks and mitigation measures...
- ... but only for class 1 and/or 2 protocols.
- The goal of this presentation is to:
  - test the security of a type 3 protocol: Ethernet POWERLINK
  - propose security improvements

# Outline

# Architecture

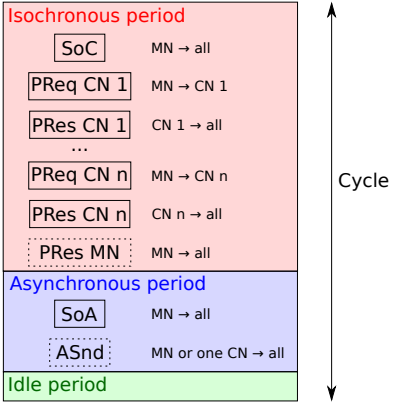
- It is specified by the EPSG (Ethernet POWERLINK Standardization Group).
- It uses the Master/Slave paradigm.
  - A Slave can send a message only if asked by the Master.
- It is composed of:
  - one *master* called Managing Node (MN)
  - up to 240 *slaves* called Controlled Node (CN)
- The master and slaves are connected through Hubs.



# Cycle Structure

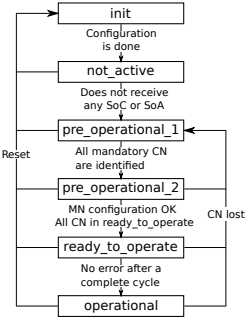
Composed of three periods:

- Isochronous period
- Asynchronous period
- Idle period



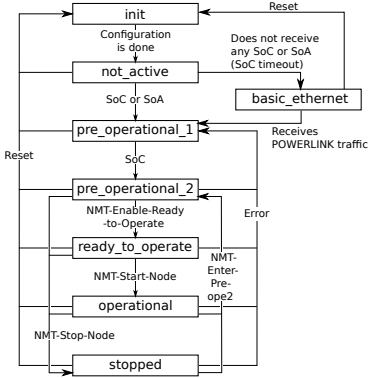
# Network Management

- The Network Management (NMT) State Machine describes a device behavior.
- The master can change the NMT state of a slave through an ASnd command.
- A slave can ask the master to send an NMT command to change the NMT state of a slave or of the master.
- The NMT states of an master are (non exhaustive list):
  - init
  - not_active
  - pre_operational_1
  - pre_operational_2
  - ready_to_operate
  - operational



# Network Management

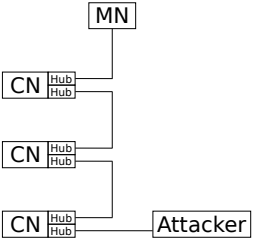
- The Network Management (NMT) State Machine describes a device behavior.
- The master can change the NMT state of a slave through an ASnd command.
- A slave can ask the master to send an NMT command to change the NMT state of a slave or of the master.
- The NMT states of a slave are (non exhaustive list):
  - init
  - pre_operational_1
  - pre_operational_2
  - ready_to_operate
  - operational
  - stopped



# Outline

# Attacker Model

- Our attacks are on the Ethernet POWERLINK protocol.
- We consider an attacker connected to the Ethernet POWERLINK network.
  - We need physical access.
  - We need a free port.
- Attacker positions
  - Most likely position: end of bus (free port)
  - Inserted after the master (requires interruption)
- Attacker capabilities
  - Listen to and analyze traffic
  - Sufficiently fast to impersonate any slave
  - With enough computational power for crypto operations



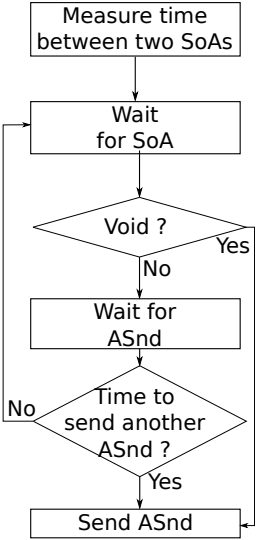
# Attacks Description

- Denial of service

Send many SoCs

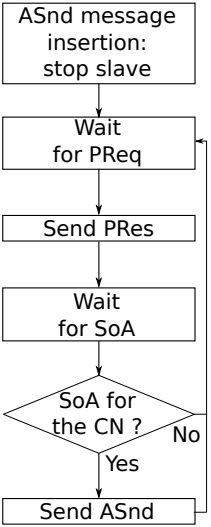
# Attacks Description

- Denial of service
- Acyclic command insertion



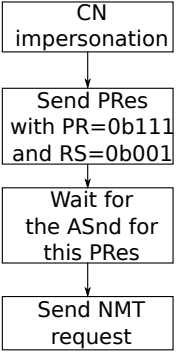
# Attacks Description

- Denial of service
- Acyclic command insertion
- slave impersonation



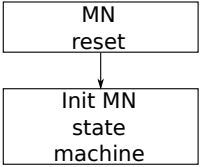
# Attacks Description

- Denial of service
- Acyclic command insertion
- slave impersonation
- master reset



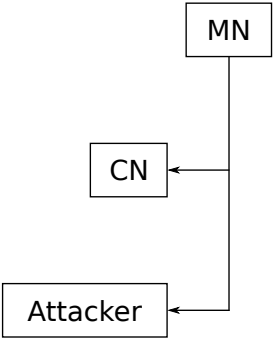
# Attacks Description

- Denial of service
- Acyclic command insertion
- slave impersonation
- master reset
- master impersonation



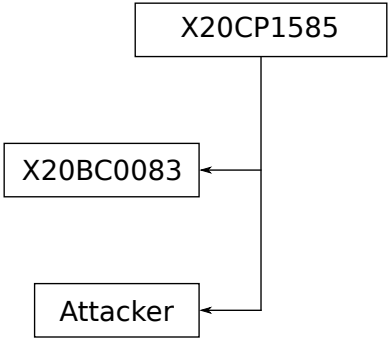
# Testbed for the implementation of the attacks

- Composed of an master, a slave and an attacker (attacker is a computer, with Linux 3.13.0-95-lowlatency kernel).
- Two testbeds implemented:



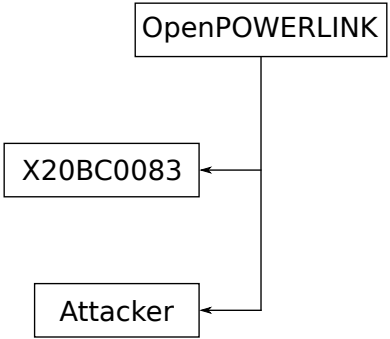
# Testbed for the implementation of the attacks

- Composed of an master, a slave and an attacker (attacker is a computer, with Linux 3.13.0-95-lowlatency kernel).
- Two testbeds implemented:
  - one using B&R components for the master and slave



# Testbed for the implementation of the attacks

- Composed of an master, a slave and an attacker (attacker is a computer, with Linux 3.13.0-95-lowlatency kernel).
- Two testbeds implemented:
  - one using B&R components for the master and slave
  - one using openPOWERLINK for the master on the same computer as the attacker, and B&R components for the slave



# Results

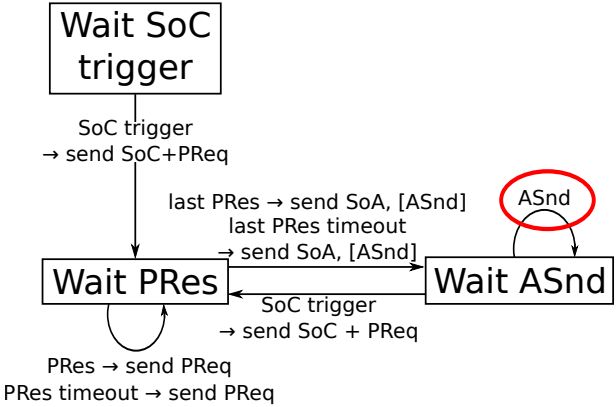
| Attacks | B&R components | openPOWERLINK |
|---|---|---|
| Denial of service | OK | OK |
| Acyclic command insertion | OK | OK |
| CN impersonation | ~OK | OK |
| MN reset | OK | OK |
| MN impersonation | OK | OK |

# Outline

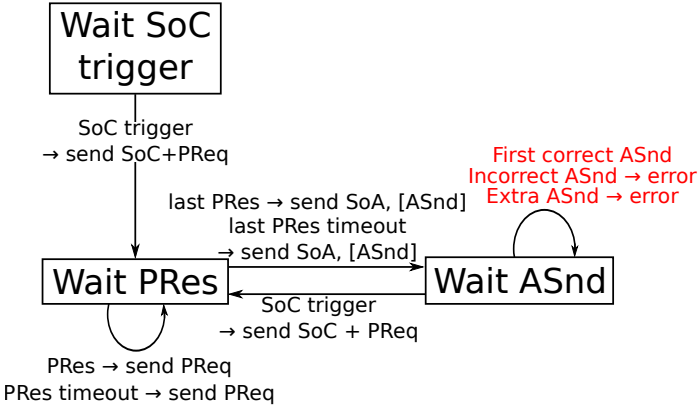
# Summing Up the Attacks

- The Master/Slave paradigm simplifies any DoS attacks.
  - we do not handle mitigation against DoS attacks here
- The other attacks are due to weaknesses in the asynchronous period:
  - no basic authentication of the command
  - no verification that the ASnd and SoA are consistent
  - several ASnd can be accepted by a slave

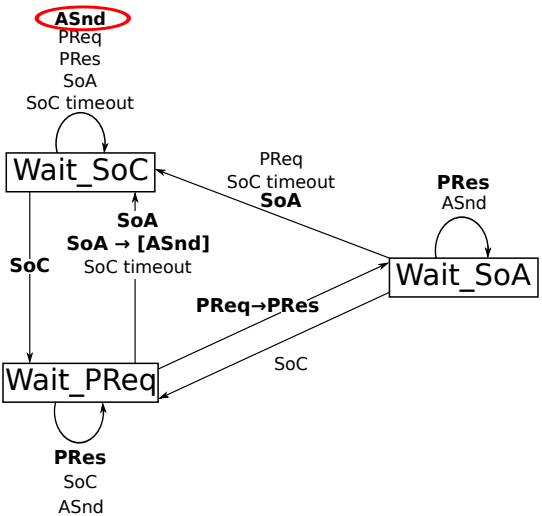
# DLL State Machine Modification - master



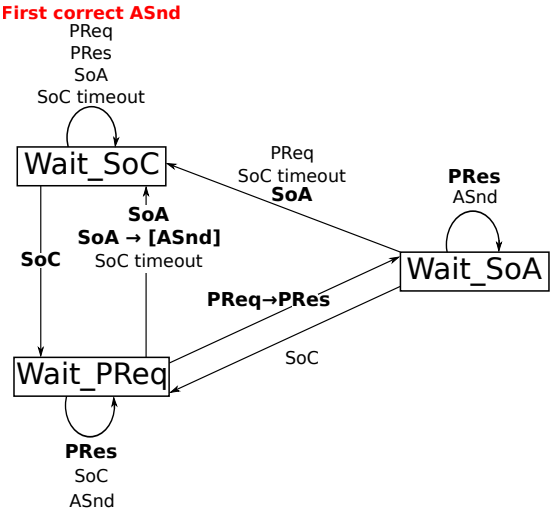
# DLL State Machine Modification - master



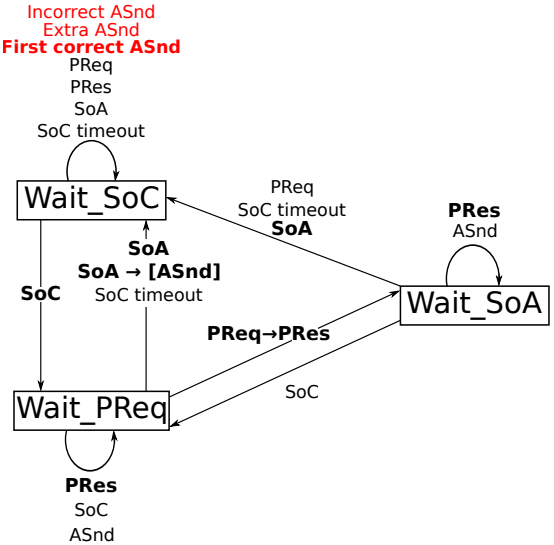
# DLL State Machine Modification - slave



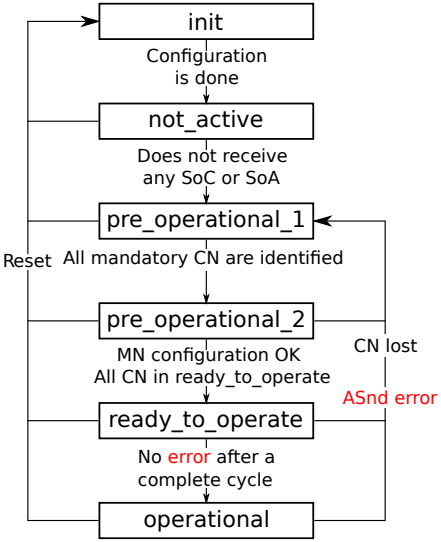
# DLL State Machine Modification - slave



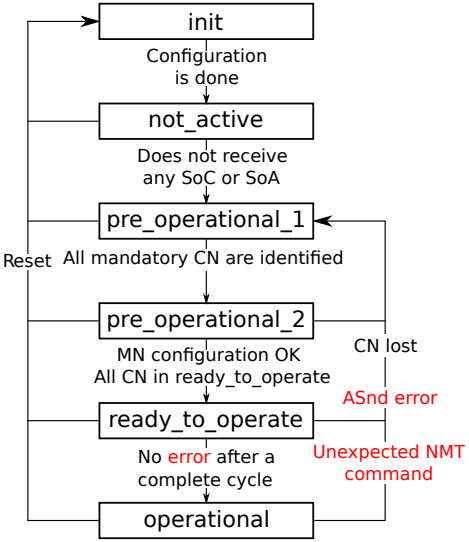
# DLL State Machine Modification - slave



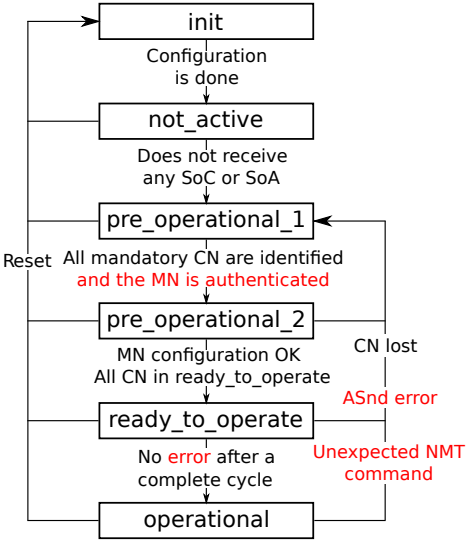
# NMT master State Machine Modification



# NMT master State Machine Modification



# NMT master State Machine Modification



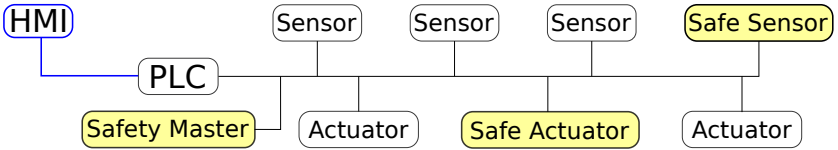
# Summary

- Denial of Service:
  - not handled here
- Acyclic command insertion:
  - The slave only accepts one correct command consistent with SoA.
  - It is not totally perfect: an attacker can be quick enough to send such a command before the master.
  - However, even in this case, it will be detected provided authentication (protection) behaves properly.
- slave impersonation:
  - The master checks the ASnd sent on the wire; the attacker can't send an NMT command without being spotted by the master.
- master reset:
  - This attack needs the impersonation of a slave.
- master impersonation:
  - The authentication phase during start-up blocks this attacks.

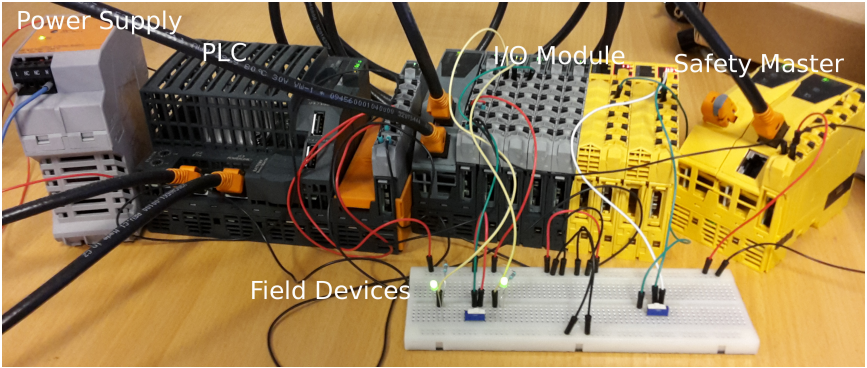
# Outline

# Industrial Safety Protocols

- Specific protocols used on top of an Industrial Ethernet protocol to ensure the safety of a system
  - For example: PROFIsafe, FSoE, CIP Safety, OpenSafety
- In an Industrial Safety network, "critical" sensors or activators are changed to become Safe Sensors and Safe Actuators.
- A Safety Master is also added.



# Yes, it can be real



# Message security

- Context: OpenSafety
  - Message size limitation
  - Message duplication
- Requirement: mutually authenticate messages
- Solution: CMAC-based authentication (space and timing constraints)
- Modifications to message structure:
  - Header (6 bytes)
    - Frame identifier for message identification
    - Security identifier for component identification
    - Sub-protocol message length
    - Sequence number to prevent replay attacks
  - Sub-protocols (adapted from standard IEC mechanisms):
    - Secure cyclic: authentication and integrity
    - Secure acyclic control: NMT messages security (e.g. for secure slaves)
    - Error reporting and heartbeat: reporting from the security master to the HMI
    - Key management
    - Extensions for monitoring only

# Defense timing characteristics

Timings computed using the characteristics of the B&R testbed.

| Nb slaves | Data | No Security | Isolated SecMaster | Monitored master | Monitored slave | Full security | OpenSAFETY |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 102.12µs | +36.7% | +37.6% | +39.4% | +43.1% | +36.75% |
| 1 | 200 | 127.72µs | +49.4% | +59.3% | +60.7% | +79.3% | +106.2% |
| 1 | 1490 | 334.12µs | +80.7% | +101% | +101% | +141% | (+231.25%) |
| 20 | 1 | 815.00µs | +4.60% | +5.76% | +5.98% | +10.9% | +4.62% |
| 20 | 200 | 1327.0µs | +4.76% | +14.7% | +14.9% | +33.7% | +62.1% |
| 20 | 1490 | 5455.0µs | +4.94% | +17.8% | +17.8% | +43.2% | (+102%) |
| 238 | 1 | 8994.4µs | +0.42% | +1.61% | +1.63% | +6.67%) | +0.44% |
| 238 | 200 | 15087µs | +0.42% | +10.4% | +10.4% | +29.3%) | +57.9% |
| 238 | 1490 | 64210µs | +0.42% | +12.8% | +12.8% | +37.4%) | (+94.1%) |

# Outline

# Lessons learned for ICS security

- Ethernet POWERLINK communications are not secure.
  - *Unsurprising...*
- They can be secured at equivalent cost to safety.
  - (*Upcoming work*)We can obtain both security and safety with the same add-on.
- This can be extended to less constrained protocols.

# Lessons learned for Intrusion Detection and Network Security

- Clear specifications provide opportunity for extension.
- Intrusion detection may benefit from additional support.
- The more security can be built-in the more benefits we obtain.
- Better detection benefits from the *process* knowledge.

  **Software** Control flow for malicious code detection
  **Protocols** Coherence of transport (flows, routing, ...)
  **Industrial process** Control loop for logical-physical dependencies
  **Business process** Interactions between physical, virtual and business assets
  ...

- Need for a better equilibrium between protection, detection and mitigation
- Need for time-tested solutions: better awareness and training

## Thank you for your attention!

### Security Issues and Mitigation in Ethernet POWERLINK

Any questions?

AIRBUS Group Innovations & Télécom SudParis

# Bibliography


Johan Åkerberg and Mats Björkman.
Exploring security in profinet io.
In *Computer Software and Applications Conference, 2009. COMPSAC'09. 33rd Annual IEEE International*, volume 1, pages 406–412. IEEE, 2009.

Daniele Antonioli and Nils Ole Tippenhauer.
Minicps: A toolkit for security research on cps networks.
In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, pages 91–100. ACM, 2015.

Basecamp Digital Bond.
*Attacking ControlLogix: ControlLogix Vulnerability Report*, 2012.

M Bristow.
Modscan: a scada modbus network scanner.
In *DefCon-16 Conf., Las Vegas, NV*, 2008.

Peter Huitsing, Rodrigo Chandia, Mauricio Papa, and Sujeet Shenoi.
Attack taxonomies for the modbus protocols.
*International Journal of Critical Infrastructure Protection*, 1:37–44, 2008.

Andreas Paul, Franka Schuster, and Hartmut König.
Towards the protection of industrial control systems–conclusions of a vulnerability analysis of profinet io.
In *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 160–176. Springer, 2013.

Theodoros Spyridopoulos, Ioanna Ailiotsiri Tang, Thea Tryfonas, and Maria Karyda.