Hochschule Augsburg
University of Applied Sciences
HSA_innos
Institut für innovative Sicherheit 1

Freie Universität Berlin 2

You Snooze, You Lose: Measuring PLC Cycle Times under Attacks

Matthias Niedermaier[1], Jan-Ole Malchow[2], Florian Fischer[1], Daniel Marzin[2], Dominik Merli1[1], Volker Roth[2] and Alexander von Bodisco[1]

Agenda

Motivation

- Common industrial topology
- Electrical monitoring of a PLC

Communication Robustness Testbed (CoRT)

- Overview
- Currently deployed devices in our test set-up
- Measurement schematic
- Measurement adapter

Cycle time measurement

- Increasing SYN loads over all DUTs
- Detailed analysis with different attacks
- Measurement results in detail
- To scan, or not to scan: that is the question
- CPU load during SYN flooding attacks

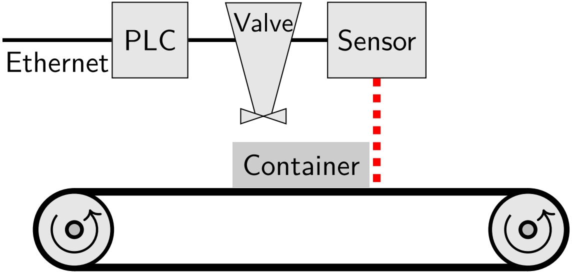
Mitigation

Conclusion and Outlook

Motivation

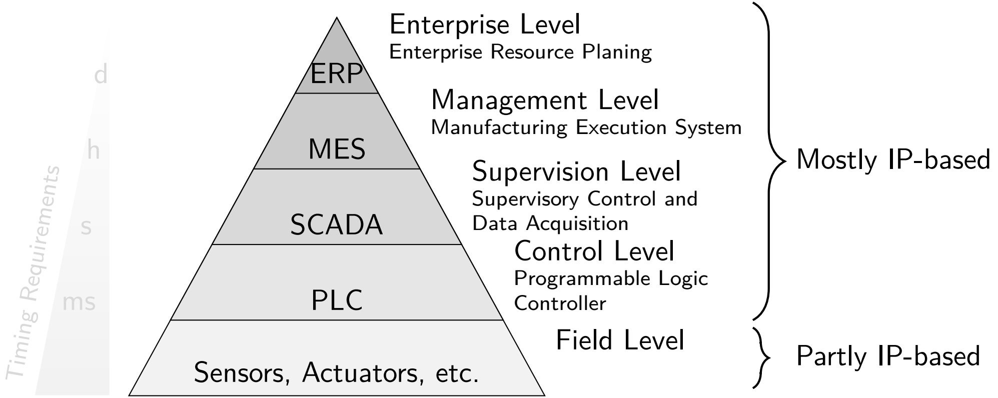
Example PLC application

- Simple example application where a Programmable Logic Controller (PLC) controls the filling of a container on a conveyor belt.
- This process must have the right timing.



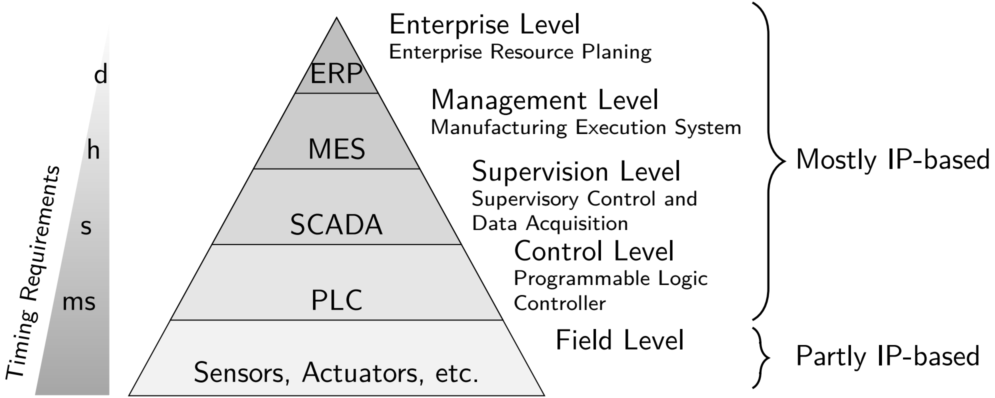
Common industrial topology

- Modern ICS systems mostly have IP-based communications in the higher levels



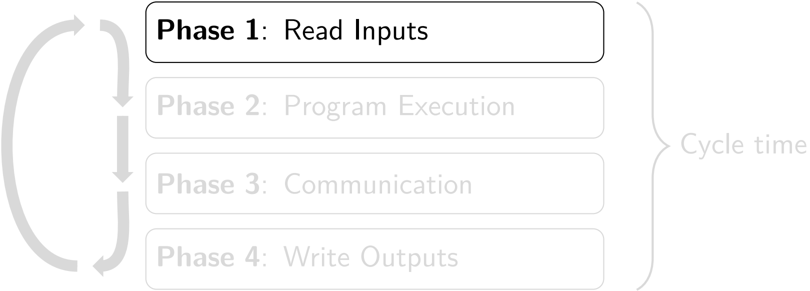
Common industrial topology

- Modern ICS systems mostly have IP-based communications in the higher levels



Simplified PLC cycle time

- The time for program execution and communication depends on the actual program, communication load, etc.



Phase 1: Read Inputs

Phase 2: Program Execution

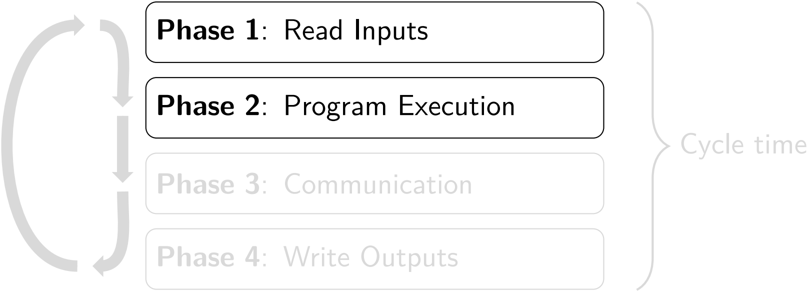
Phase 3: Communication

Phase 4: Write Outputs

Cycle time

Simplified PLC cycle time

- The time for program execution and communication depends on the actual program, communication load, etc.



Phase 1: Read Inputs

Phase 2: Program Execution

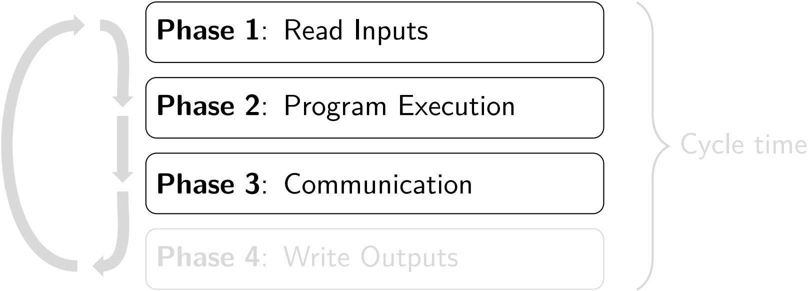
Phase 3: Communication

Phase 4: Write Outputs

Cycle time

Simplified PLC cycle time

- The time for program execution and communication depends on the actual program, communication load, etc.



Phase 1: Read Inputs

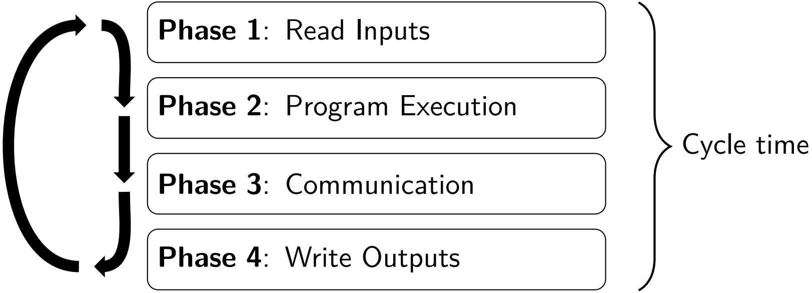
Phase 2: Program Execution

Phase 3: Communication

Phase 4: Write Outputs

Simplified PLC cycle time

- The time for program execution and communication depends on the actual program, communication load, etc.



Phase 1: Read Inputs

Phase 2: Program Execution

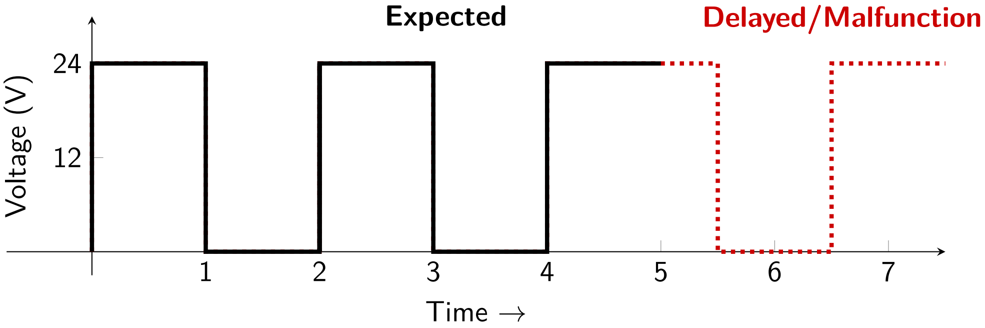
Phase 3: Communication

Phase 4: Write Outputs

Cycle time

Influences on the PLC cycle time

- Any delay in the cycle time of a PLC could influence the physical process
- Observation with a logic analyzer



Hypothesis: Network traffic/scanning could influence ICS and corresponding processes

Certification

There are already proprietary closed source certification programs for ICS components:

- Achilles Certification
  - Initially developed by Wurdtech Security Technologies, the Achilles Program was later bought by General Electric.
  - Relies on a proprietary test device called "Achilles Satellite".
  - Protocol fuzzing and packet storms.
  - Level 2 certification, the PLC has a cycle output of 1000ms (500ms high output and 500ms low output) with an acceptable tolerance of 4 percent.
- ISASecure EDSA Certification
  - With the exception of Ethernet, the requirements state that the device under test maintains its essential services under high load but can reduce or cease network communication during periods of high load.
- Mu Dynamics MUSIC Certification

→ Independent measurement of communication load influences is necessary.

Certification

There are already proprietary closed source certification programs for ICS components:

- Achilles Certification
  - Initially developed by Wurdtech Security Technologies, the Achilles Program was later bought by General Electric.
  - Relies on a proprietary test device called "Achilles Satellite".
  - Protocol fuzzing and packet storms.
  - Level 2 certification, the PLC has a cycle output of 1000ms (500ms high output and 500ms low output) with an acceptable tolerance of 4 percent.
- ISASecure EDSA Certification
  - With the exception of Ethernet, the requirements state that the device under test maintains its essential services under high load but can reduce or cease network communication during periods of high load.
- Mu Dynamics MUSIC Certification

→ Independent measurement of communication load influences is necessary.

Certification

There are already proprietary closed source certification programs for ICS components:

- Achilles Certification
  - Initially developed by Wurdtech Security Technologies, the Achilles Program was later bought by General Electric.
  - Relies on a proprietary test device called "Achilles Satellite".
  - Protocol fuzzing and packet storms.
  - Level 2 certification, the PLC has a cycle output of 1000ms (500ms high output and 500ms low output) with an acceptable tolerance of 4 percent.
- ISASecure EDSA Certification
  - With the exception of Ethernet, the requirements state that the device under test maintains its essential services under high load but can reduce or cease network communication during periods of high load.
- Mu Dynamics MUSIC Certification

→ Independent measurement of communication load influences is necessary.

Certification

There are already proprietary closed source certification programs for ICS components:

- Achilles Certification
  - Initially developed by Wurdtech Security Technologies, the Achilles Program was later bought by General Electric.
  - Relies on a proprietary test device called ”Achilles Satellite”.
  - Protocol fuzzing and packet storms.
  - Level 2 certification, the PLC has a cycle output of 1000ms (500ms high output and 500ms low output) with an acceptable tolerance of 4 percent.
- ISASecure EDSA Certification
  - With the exception of Ethernet, the requirements state that the device under test maintains its essential services under high load but can reduce or cease network communication during periods of high load.
- Mu Dynamics MUSIC Certification

→ Independent measurement of communication load influences is necessary.

Certification

There are already proprietary closed source certification programs for ICS components:

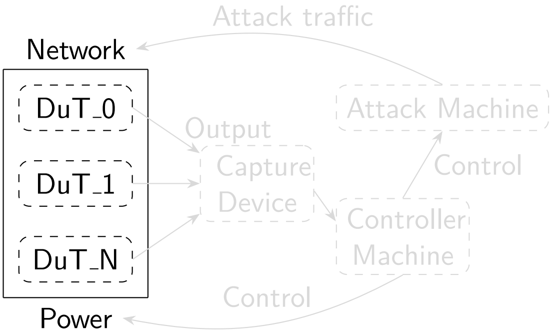
- Achilles Certification
  - Initially developed by Wurdtech Security Technologies, the Achilles Program was later bought by General Electric.
  - Relies on a proprietary test device called "Achilles Satellite".
  - Protocol fuzzing and packet storms.
  - Level 2 certification, the PLC has a cycle output of 1000ms (500ms high output and 500ms low output) with an acceptable tolerance of 4 percent.
- ISASecure EDSA Certification
  - With the exception of Ethernet, the requirements state that the device under test maintains its essential services under high load but can reduce or cease network communication during periods of high load.
- Mu Dynamics MUSIC Certification

→ Independent measurement of communication load influences is necessary.

Communication **R**obustness **T**estbed (**CoRT**)

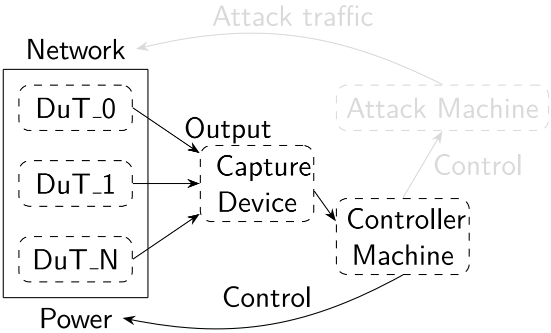
CoRT - Overview

- Fully automated measurment set-up.
- Easy integration.



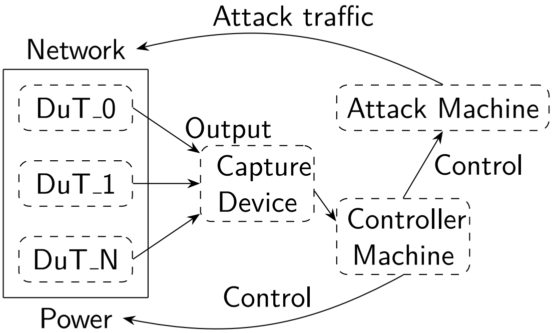
CoRT - Overview

- Fully automated measurment set-up.
- Easy integration.

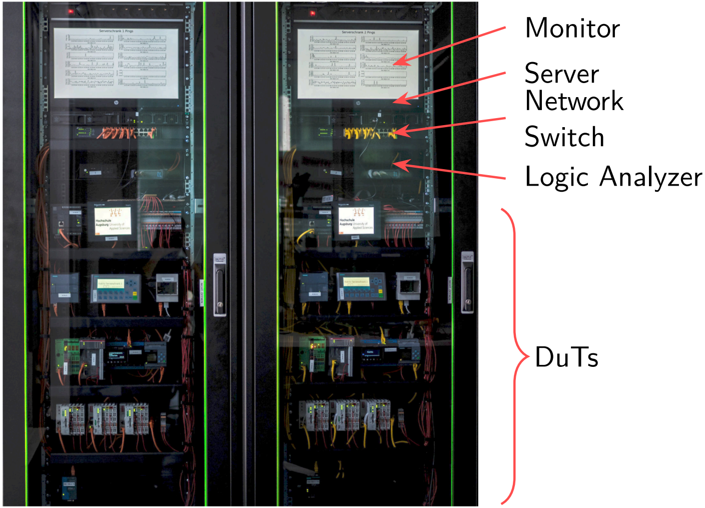


CoRT - Overview

- Fully automated measurment set-up.
- Easy integration.



CoRT - Overview



Monitor

Server Network

Switch

Logic Analyzer

DuTs

CoRT - Currently deployed devices in our test set-up

No.	Vendor	Manufacturer number	Name	Firmware
1	Wago	750-889	Controller KNX IP	01.07.13(10)
2	Wago	750-8100	Controller PFC100	02.05.23(08)
3	Wago	750-880	Controller ETH.	01.07.03(10)
4	Wago	750-831	Controller BACnet/IP	01.02.29(09)
5	Siemens	6ES7211-1AE40-0XB0	Simatic S7-1211*	V4.2.0
6	Siemens	6ES7212-1AE31-0XB0	Simatic S7-1212	V 3.0.2
7	Siemens	6ES7155-6AU00-0AB0	Simatic ET 200SP	V 3.3.0
8	Siemens	6ES7314-6EH04-0AB0	Simatic S7-314*	V 3.3.0
9	Siemens	6ES7516-3FN01-0AB0	Simatic S7-1516F*	V 2.0.5
10	Siemens	6ED1052-1CC01-0BA8	Logo! 8*	1.81.01
11	Phoenix	2700974	ILC 151 ETH	V.4.42.04
12	Phoenix	2985330	ILC 150 ETH	V.3.94.03
13	Phoenix	2700975	ILC 171 ETH 2TX	V.4.42.04
14	ABB	1SAP120600R0071	PM554-TP-ETH	2.5.4.15626
15	Crouzet	88981133	em4 Ethernet	1.2.75/1.0.27
16	Schneider	TM221CE16T	Modicon M221	1.5.1.0

* Achilles Level 2 Certified

CoRT - Currently deployed devices in our test set-up

No.	Vendor	Manufacturer number	Name	Firmware
1	Wago	750-889	Controller KNX IP	01.07.13(10)
2	Wago	750-8100	Controller PFC100	02.05.23(08)
3	Wago	750-880	Controller ETH.	01.07.03(10)
4	Wago	750-831	Controller BACnet/IP	01.02.29(09)
5	Siemens	6ES7211-1AE40-0XB0	Simatic S7-1211*	V4.2.0
6	Siemens	6ES7212-1AE31-0XB0	Simatic S7-1212	V 3.0.2
7	Siemens	6ES7155-6AU00-0AB0	Simatic ET 200SP	V 3.3.0
8	Siemens	6ES7314-6EH04-0AB0	Simatic S7-314*	V 3.3.0
9	Siemens	6ES7516-3FN01-0AB0	Simatic S7-1516F*	V 2.0.5
10	Siemens	6ED1052-1CC01-0BA8	Logo! 8*	1.81.01
11	Phoenix	2700974	ILC 151 ETH	V.4.42.04
12	Phoenix	2985330	ILC 150 ETH	V.3.94.03
13	Phoenix	2700975	ILC 171 ETH 2TX	V.4.42.04
14	ABB	1SAP120600R0071	PM554-TP-ETH	2.5.4.15626
15	Crouzet	88981133	em4 Ethernet	1.2.75/1.0.27
16	Schneider	TM221CE16T	Modicon M221	1.5.1.0

* Achilles Level 2 Certified

CoRT - Currently deployed devices in our test set-up

No.	Vendor	Manufacturer number	Name	Firmware
1	Wago	750-889	Controller KNX IP	01.07.13(10)
2	Wago	750-8100	Controller PFC100	02.05.23(08)
3	Wago	750-880	Controller ETH.	01.07.03(10)
4	Wago	750-831	Controller BACnet/IP	01.02.29(09)
5	Siemens	6ES7211-1AE40-0XB0	Simatic S7-1211*	V4.2.0
6	Siemens	6ES7212-1AE31-0XB0	Simatic S7-1212	V 3.0.2
7	Siemens	6ES7155-6AU00-0AB0	Simatic ET 200SP	V 3.3.0
8	Siemens	6ES7314-6EH04-0AB0	Simatic S7-314*	V 3.3.0
9	Siemens	6ES7516-3FN01-0AB0	Simatic S7-1516F*	V 2.0.5
10	Siemens	6ED1052-1CC01-0BA8	Logo! 8*	1.81.01
11	Phoenix	2700974	ILC 151 ETH	V.4.42.04
12	Phoenix	2985330	ILC 150 ETH	V.3.94.03
13	Phoenix	2700975	ILC 171 ETH 2TX	V.4.42.04
14	ABB	1SAP120600R0071	PM554-TP-ETH	2.5.4.15626
15	Crouzet	88981133	em4 Ethernet	1.2.75/1.0.27
16	Schneider	TM221CE16T	Modicon M221	1.5.1.0

* Achilles Level 2 Certified

CoRT - Currently deployed devices in our test set-up

No.	Vendor	Manufacturer number	Name	Firmware
1	Wago	750-889	Controller KNX IP	01.07.13(10)
2	Wago	750-8100	Controller PFC100	02.05.23(08)
3	Wago	750-880	Controller ETH.	01.07.03(10)
4	Wago	750-831	Controller BACnet/IP	01.02.29(09)
5	Siemens	6ES7211-1AE40-0XB0	Simatic S7-1211*	V4.2.0
6	Siemens	6ES7212-1AE31-0XB0	Simatic S7-1212	V 3.0.2
7	Siemens	6ES7155-6AU00-0AB0	Simatic ET 200SP	V 3.3.0
8	Siemens	6ES7314-6EH04-0AB0	Simatic S7-314*	V 3.3.0
9	Siemens	6ES7516-3FN01-0AB0	Simatic S7-1516F*	V 2.0.5
10	Siemens	6ED1052-1CC01-0BA8	Logo! 8*	1.81.01
11	Phoenix	2700974	ILC 151 ETH	V.4.42.04
12	Phoenix	2985330	ILC 150 ETH	V.3.94.03
13	Phoenix	2700975	ILC 171 ETH 2TX	V.4.42.04
14	ABB	1SAP120600R0071	PM554-TP-ETH	2.5.4.15626
15	Crouzet	88981133	em4 Ethernet	1.2.75/1.0.27
16	Schneider	TM221CE16T	Modicon M221	1.5.1.0

* Achilles Level 2 Certified

CoRT - Currently deployed devices in our test set-up

No.	Vendor	Manufacturer number	Name	Firmware
1	Wago	750-889	Controller KNX IP	01.07.13(10)
2	Wago	750-8100	Controller PFC100	02.05.23(08)
3	Wago	750-880	Controller ETH.	01.07.03(10)
4	Wago	750-831	Controller BACnet/IP	01.02.29(09)
5	Siemens	6ES7211-1AE40-0XB0	Simatic S7-1211*	V4.2.0
6	Siemens	6ES7212-1AE31-0XB0	Simatic S7-1212	V 3.0.2
7	Siemens	6ES7155-6AU00-0AB0	Simatic ET 200SP	V 3.3.0
8	Siemens	6ES7314-6EH04-0AB0	Simatic S7-314*	V 3.3.0
9	Siemens	6ES7516-3FN01-0AB0	Simatic S7-1516F*	V 2.0.5
10	Siemens	6ED1052-1CC01-0BA8	Logo! 8*	1.81.01
11	Phoenix	2700974	ILC 151 ETH	V.4.42.04
12	Phoenix	2985330	ILC 150 ETH	V.3.94.03
13	Phoenix	2700975	ILC 171 ETH 2TX	V.4.42.04
14	ABB	1SAP120600R0071	PM554-TP-ETH	2.5.4.15626
15	Crouzet	88981133	em4 Ethernet	1.2.75/1.0.27
16	Schneider	TM221CE16T	Modicon M221	1.5.1.0

* Achilles Level 2 Certified

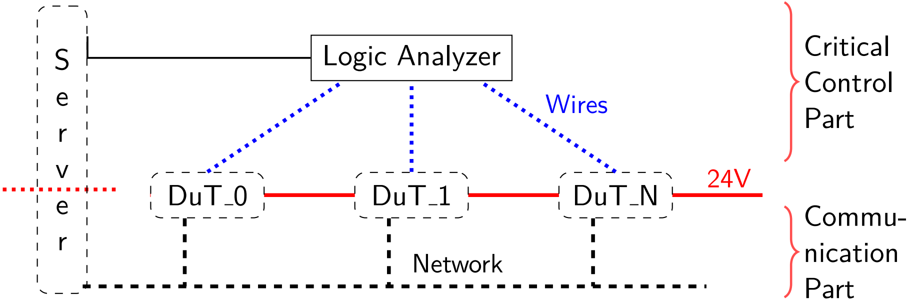
CoRT - Currently deployed devices in our test set-up

No.	Vendor	Manufacturer number	Name	Firmware
1	Wago	750-889	Controller KNX IP	01.07.13(10)
2	Wago	750-8100	Controller PFC100	02.05.23(08)
3	Wago	750-880	Controller ETH.	01.07.03(10)
4	Wago	750-831	Controller BACnet/IP	01.02.29(09)
5	Siemens	6ES7211-1AE40-0XB0	Simatic S7-1211*	V4.2.0
6	Siemens	6ES7212-1AE31-0XB0	Simatic S7-1212	V 3.0.2
7	Siemens	6ES7155-6AU00-0AB0	Simatic ET 200SP	V 3.3.0
8	Siemens	6ES7314-6EH04-0AB0	Simatic S7-314*	V 3.3.0
9	Siemens	6ES7516-3FN01-0AB0	Simatic S7-1516F*	V 2.0.5
10	Siemens	6ED1052-1CC01-0BA8	Logo! 8*	1.81.01
11	Phoenix	2700974	ILC 151 ETH	V.4.42.04
12	Phoenix	2985330	ILC 150 ETH	V.3.94.03
13	Phoenix	2700975	ILC 171 ETH 2TX	V.4.42.04
14	ABB	1SAP120600R0071	PM554-TP-ETH	2.5.4.15626
15	Crouzet	88981133	em4 Ethernet	1.2.75/1.0.27
16	Schneider	TM221CE16T	Modicon M221	1.5.1.0

* Achilles Level 2 Certified

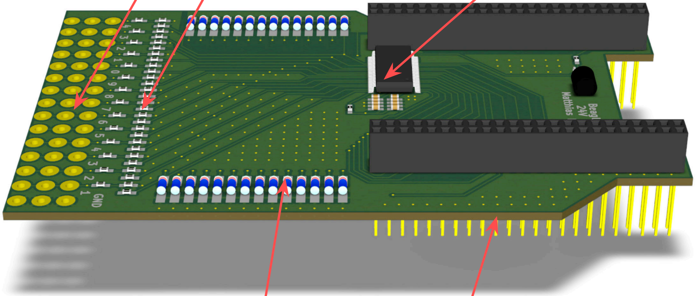
CoRT - Measurement schematic

- Separation in communication and critical part.
- Observation of the Device under Test (DuT) on both sides.
- Reproducible set-up.



CoRT - Measurement adapter

- Logic analyzer with the real-time processors on a **Beagle Bone Green**.
- 24V input voltage with up to 100 Megasamples/s.
- Continuous logging over Ethernet.



Digital Inputs

Resistor Dividers

Level Shifter

Protection Diodes

Pin Headers

Increasing SYN loads over all DUTs

Normalized deviation during hping3 flooding

The delays between the flooding was created by the wait parameter of hping3 (`hping3 -i u<wait for x microseconds> <IP>`). After each packet, hping3 waited *x* microseconds until the next packet is sent.

The mean cycle time of each segment was calculated as:

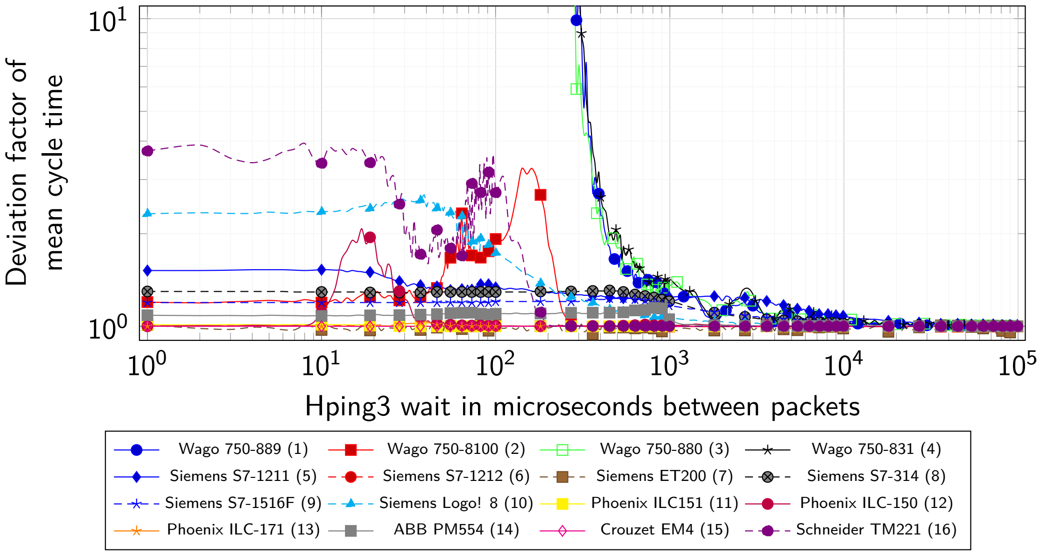
$$\bar{t} = \frac{1}{n} \cdot \sum_{i=1}^{n} t_i \qquad (1)$$

For better comparability, we normalized the results by dividing them by the mean idle time:

$$\Delta t = \frac{\bar{t}}{\bar{t}_{idle}} \qquad (2)$$

- Increasing SYN loads over all DUTs to get an overview.

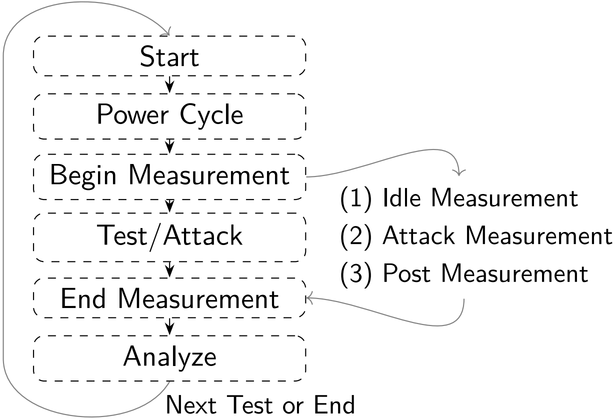
Normalized deviation during hping3 flooding



Detailed analysis with different attacks

Test cycle procedure

- Test cycle to compare ”normal” behavior with behavior during tests.
- Predefined and automatic testing for reproducibility and comparison is important.



(1) Idle Measurement
(2) Attack Measurement
(3) Post Measurement

Tools used for load generation

We used common tools to generate network loads and custom implementations, when necessary.

Program	Protocols	Parameters
ZGrab	S7comm / HTTP(S) / Modbus/TCP / Ethernet/IP / DNP3 / Bacnet/IP	`-s7 --port 102 / --port 80 --http="" / --port 443 --tls --http="" / -modbus --port 502 / -dnp3 --port 20000 / -enip --port 44818`
Vegata	HTTP	`attack`
hping3	SYN / UDP	`-c 1 -1 -C 17 / -S -P -U --flood`
syn_spam*	SYN	`-worker 20`
arp_spam*	ARP	`-worker 20`
gre_spam*	GRE	`-worker 20`
snmp_spam*	SNMP	`-worker 20`

- Every tool is running for 10 minutes, with an idle measurement before and after.

Tools used for load generation

We used common tools to generate network loads and custom implementations, when necessary.

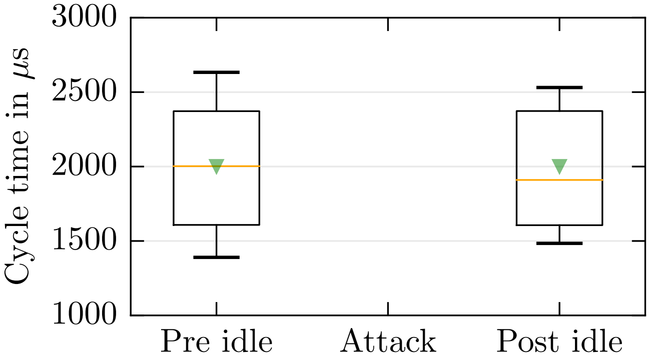
Program	Protocols	Parameters
ZGrab	S7comm / HTTP(S) / Modbus/TCP / Ethernet/IP / DNP3 / Bacnet/IP	`-s7 --port 102 / --port 80 --http="" / --port 443 --tls --http="" / -modbus --port 502 / -dnp3 --port 20000 / -enip --port 44818`
Vegata	HTTP	`attack`
hping3	SYN / UDP	`-c 1 -1 -C 17 / -S -P -U --flood`
syn_spam*	SYN	`-worker 20`
arp_spam*	ARP	`-worker 20`
gre_spam*	GRE	`-worker 20`
snmp_spam*	SNMP	`-worker 20`

- Every tool is running for 10 minutes, with an idle measurement before and after.

Measurement results in detail

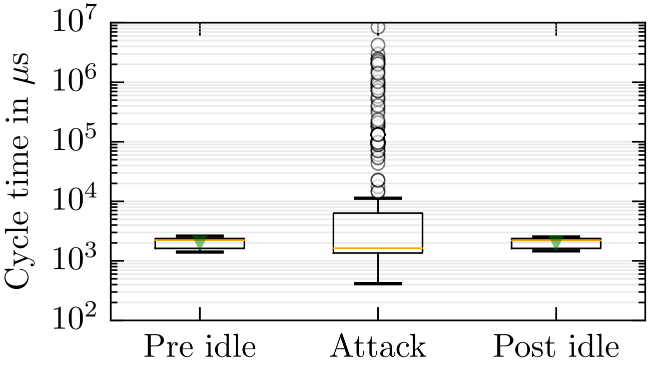
Class 1: PLC 'Stops'

- Boxplot of a Wago 750-831 (4), where the PLC stops during Address Resolution Protocol (ARP) flooding.



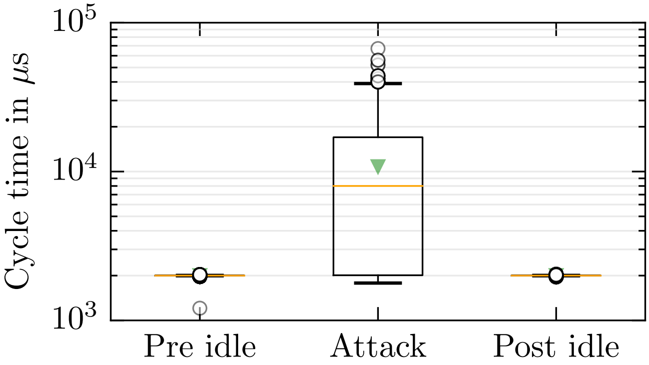
Class 2: High Deviation

- Boxplot of UDP flooding attack on a Wago 750-889 (1), resulting in a high deviation (>1000) of the cycle time.



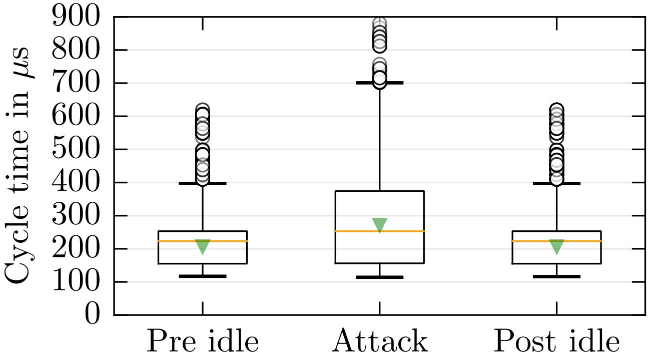
Class 3: Medium Deviation

- Boxplot with medium deviation (>10) during UDP flooding with hping3 of the Schneider TM221CE16T (16).



Class 4: Increased Variance of Cycle Times

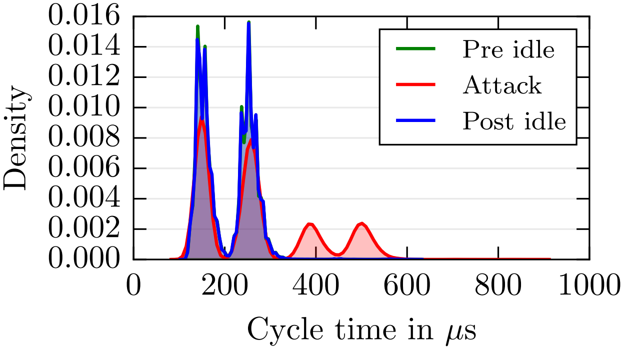
- Boxplot, while an attack on a Siemens S7-314 (8) is generating a high network load with the S7Com implementation of zgrab.



Other representation views distribution.

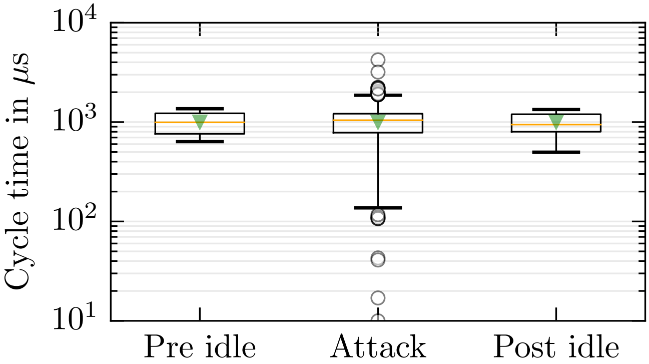
Class 4: Increased Variance of Cycle Times

- Probability Density Function, to view the distribution during the S7Com flooding of a Siemens S7-314 (8) with zgrab.



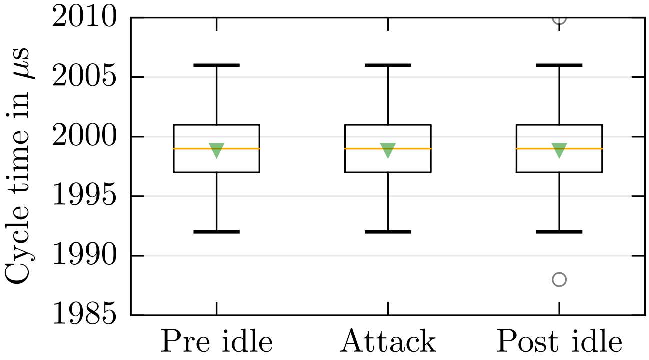
Class 5: Faster Cycle Time

- A boxplot representing a shorter cycle time of a Phoenix ILC151 (11) during Modbus/TCP flooding with zgrab.



Class 6: No Measurable Influence

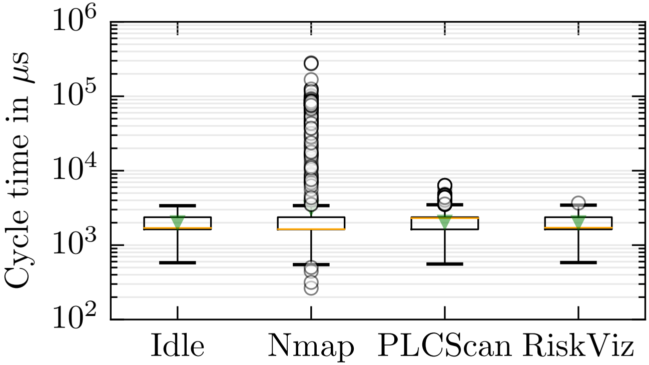
- Example of a boxplot with no measurable influence on the Crouzet em4 (15).



To scan, or not to scan: that is the question

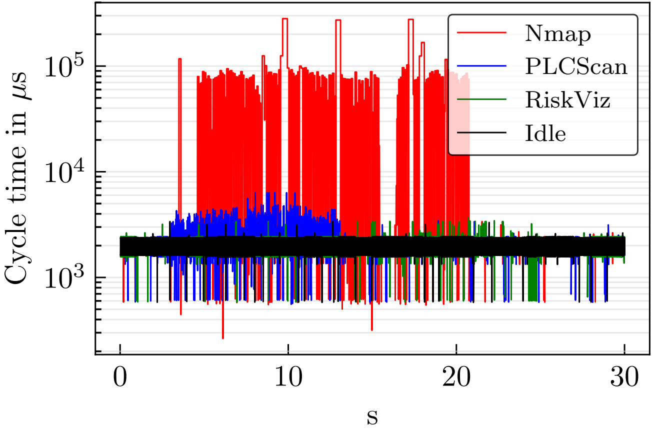
Cycle time influences during scanning

- Comparing standard network scanners with an influenceable Wago 750-880 PLC.



Cycle time influences during scanning

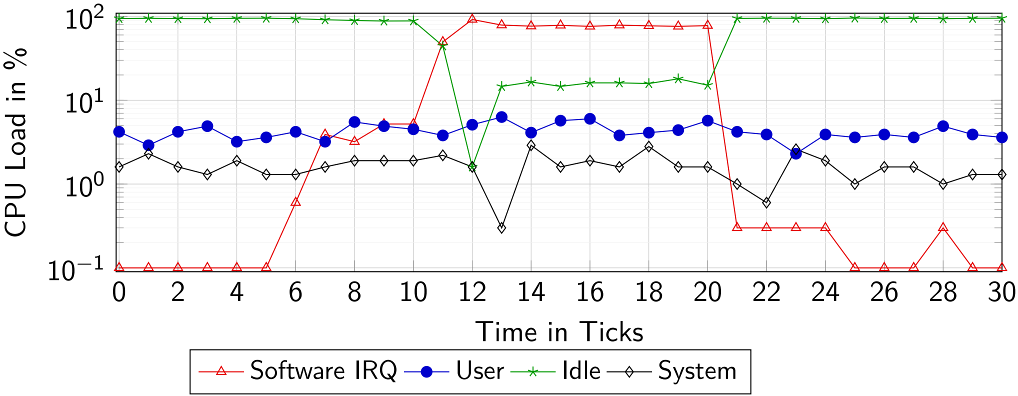
- Impact of scanners over the scan time of an influenceable Wago 750-880 PLC.



CPU load during SYN flooding attacks

CPU load during SYN flooding attacks

- CPU load during attacks on a Linux based Wago 750-8100 controller.



Mitigation

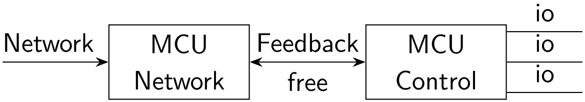
Mitigation

Operators and integrators:

- Implement and maintain a state-of-the-art industrial security concept.
- Data rate limitations on the network provide a possible software solution. This feature is already implemented by controllers from Wago (1,2,3,4). (Only working partially)

Vendors:

- Usage of a hard real-time OS.
- Usage of hardware separation, e.g. communication and control micro controller unit.



Conclusion and Outlook

Conclusion and Outlook

Conclusion

- Stable and extensible testbed for industrial components.
- A lot of measurement data, with unexpected results.
- Working in a close cooperation with vendors and CERTs to find solutions and fixes →many vendors do not see a security problem in this behavior.
- Secure PLC architectures are necessary.

Outlook

- Extending features for measurements.
- Observation of virtualized physical processes.
- Testing more devices and different vendors.

Hochschule Augsburg
University of Applied Sciences

HSA_innos
Institut für innovative Sicherheit 1

Freie Universität Berlin 2

Thank you all for listening. Any questions?

Matthias Niedermaier[1]
Matthias.Niedermaier@hs-augsburg.de