SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN
Established in collaboration with MIT

Legacy-Compliant Data Authentication for Industrial Control System Traffic

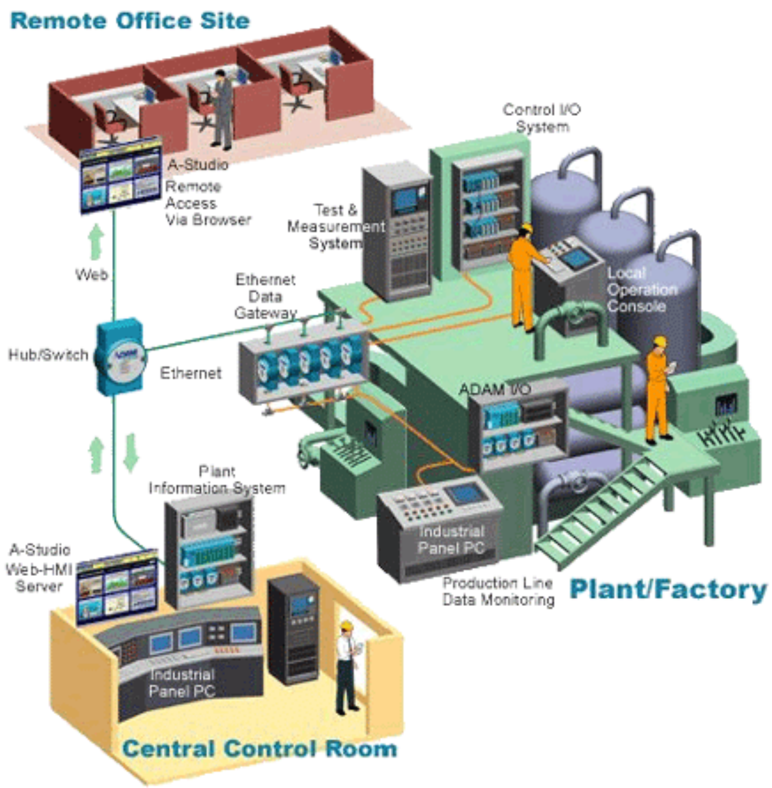
John Henry Castellanos, Daniele Antonioli, Nils Ole Tippenhauer and Martín Ochoa
Singapore University of Technology and Design

15th International Conference on Applied Cryptography and Network Security
Japan, Kanazawa, July 11, 2017.

iTrust
Center for Research in Cyber Security

Industrial Control Systems

What are ICSs?



Source: urvil.wordpress.com

Automatic control of Industrial Processes:

Manufacturing plants

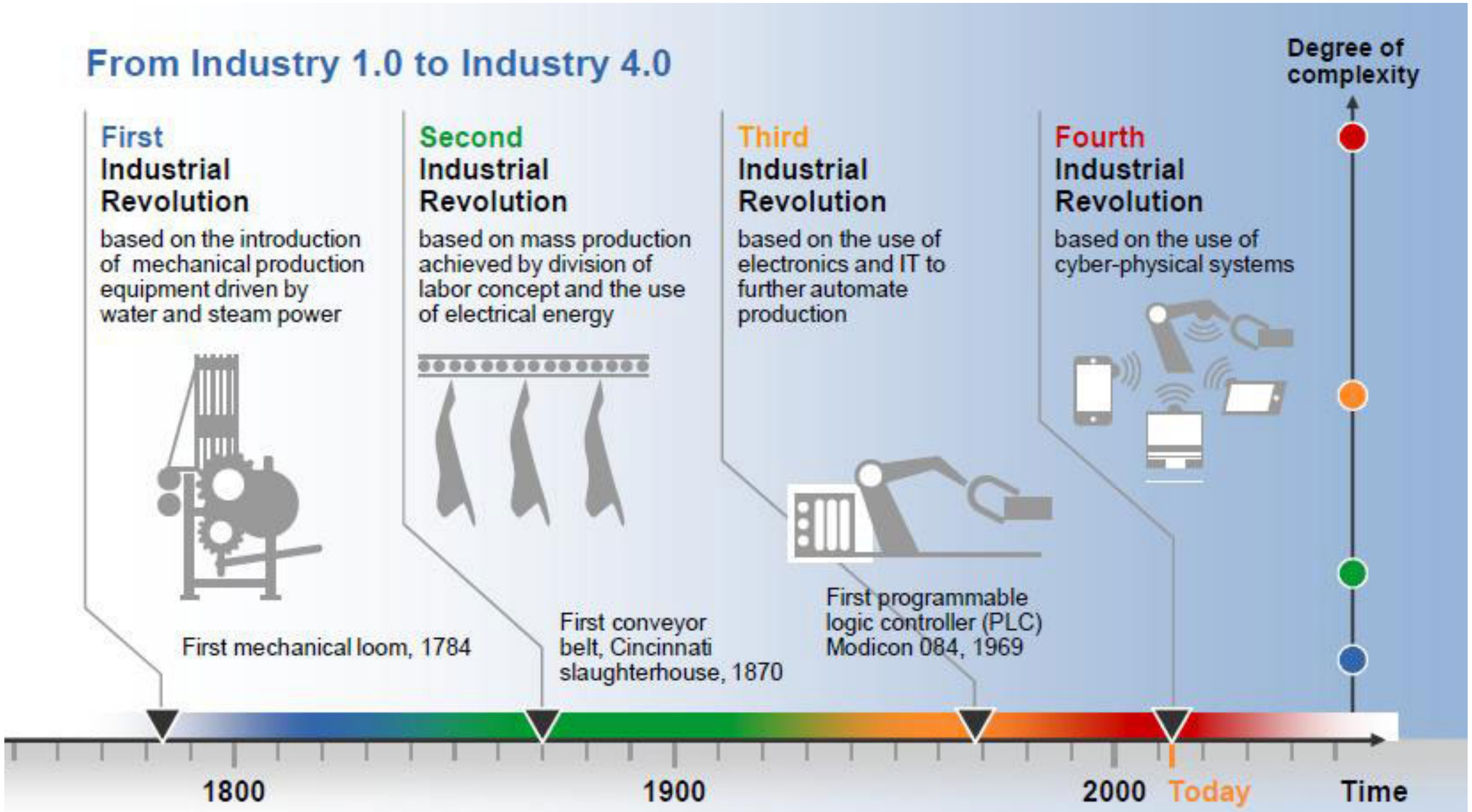
Power plants

Public transportation infrastructure

Utility infrastructure (water treatment, gas/oil, power generation)

Industrial Control Systems

Industry Evolution

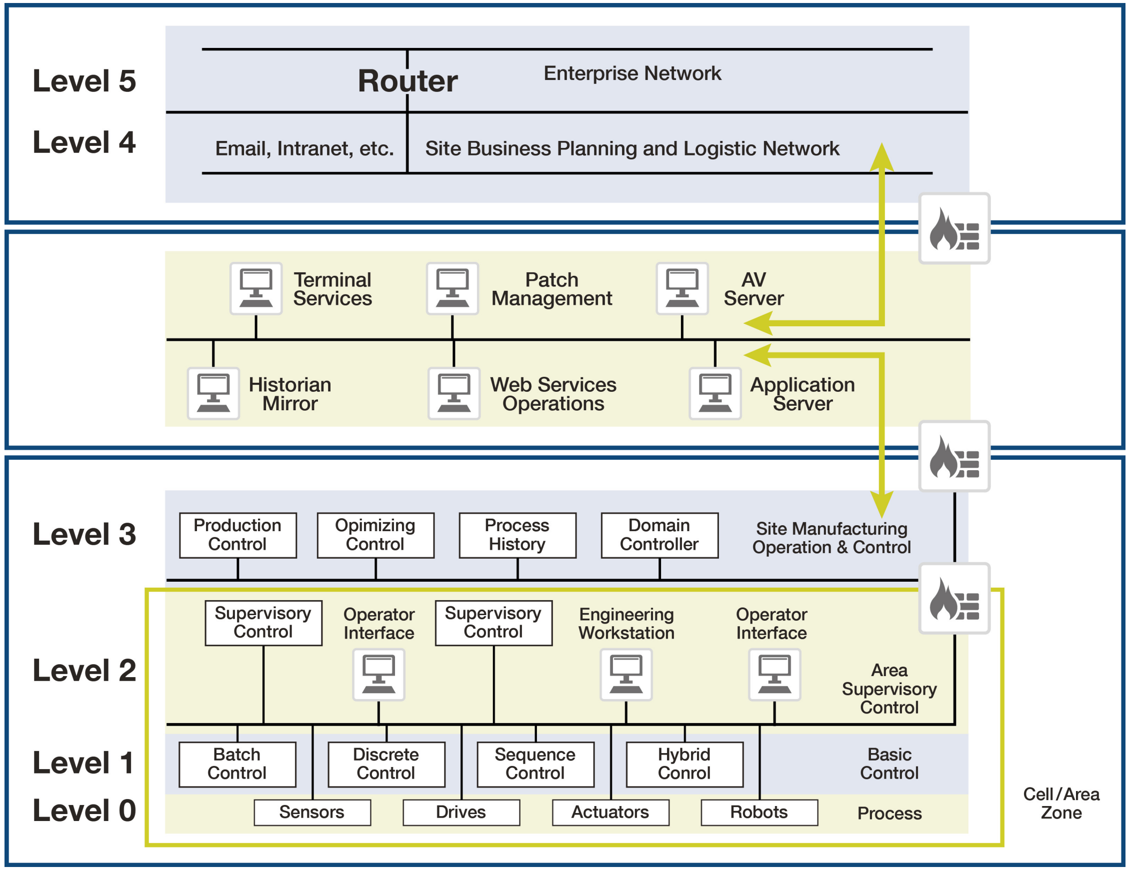


Source: http://bcmpublicrelations.com/

iTrust Center for Research in Cyber Security

Industrial Control Systems

IT meets OT (Purdue Model)



Source: https://pgjonline.com/

Information Technology:

Servers and Client PCs

Operational Technology:

Servers, PLCs, SCADA, HMI Devices, Actuators and Sensors

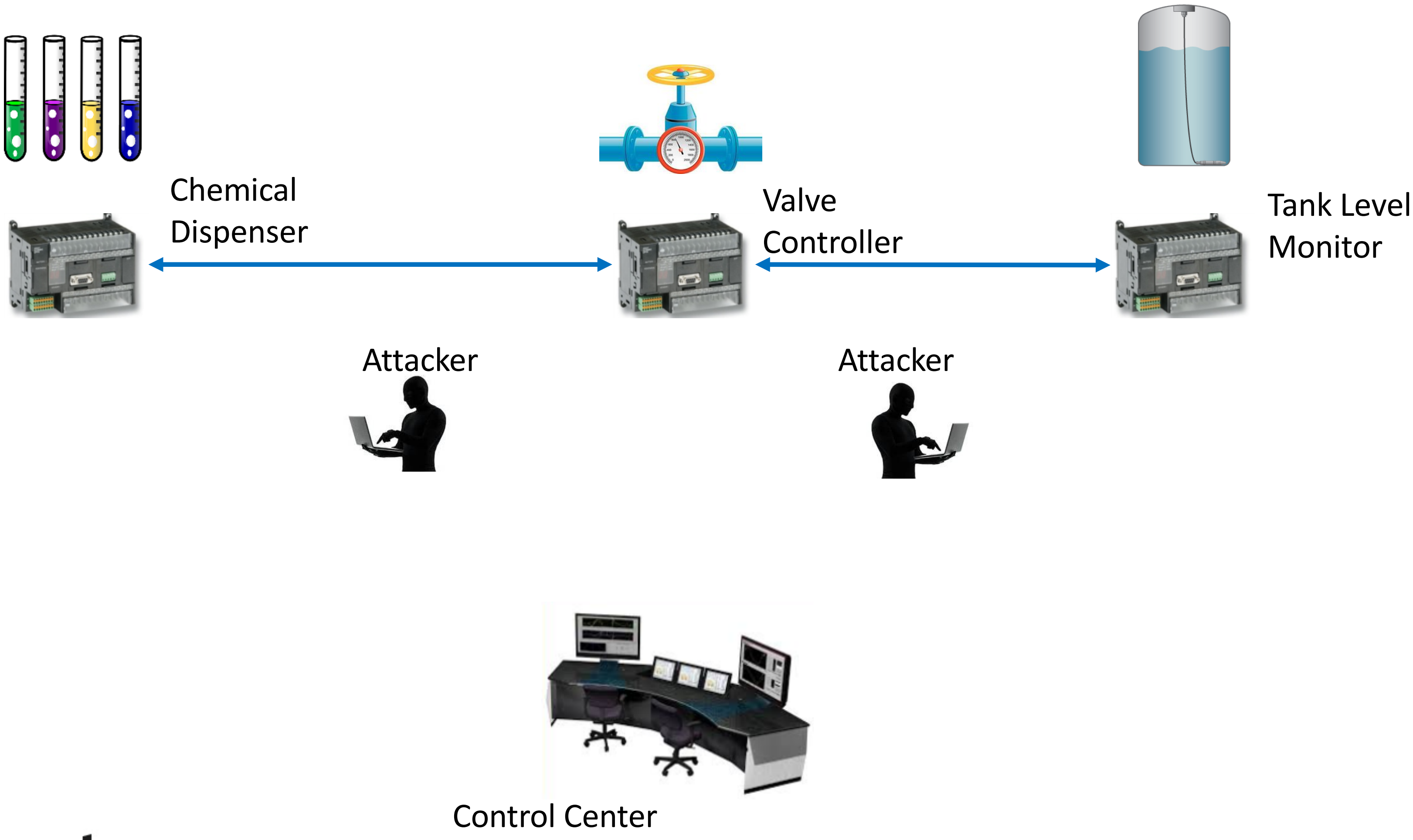
Integrity Attacks cause Operational Changes

iTrust Center for Research in Cyber Security

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

Cyber-security in ICS

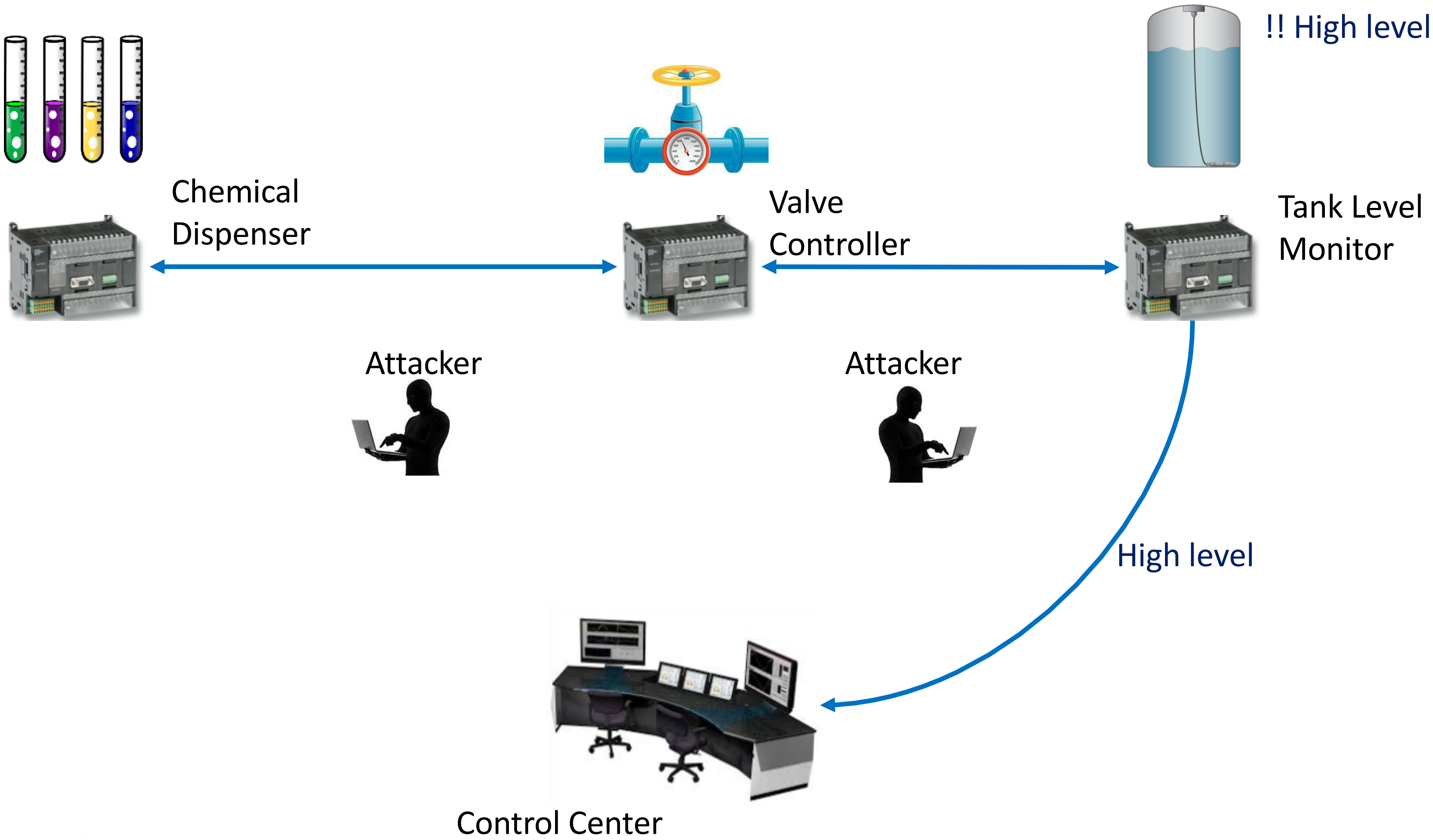
Motivation: Integrity Attacks



iTrust
Center for Research in Cyber Security

Cyber-security in ICS

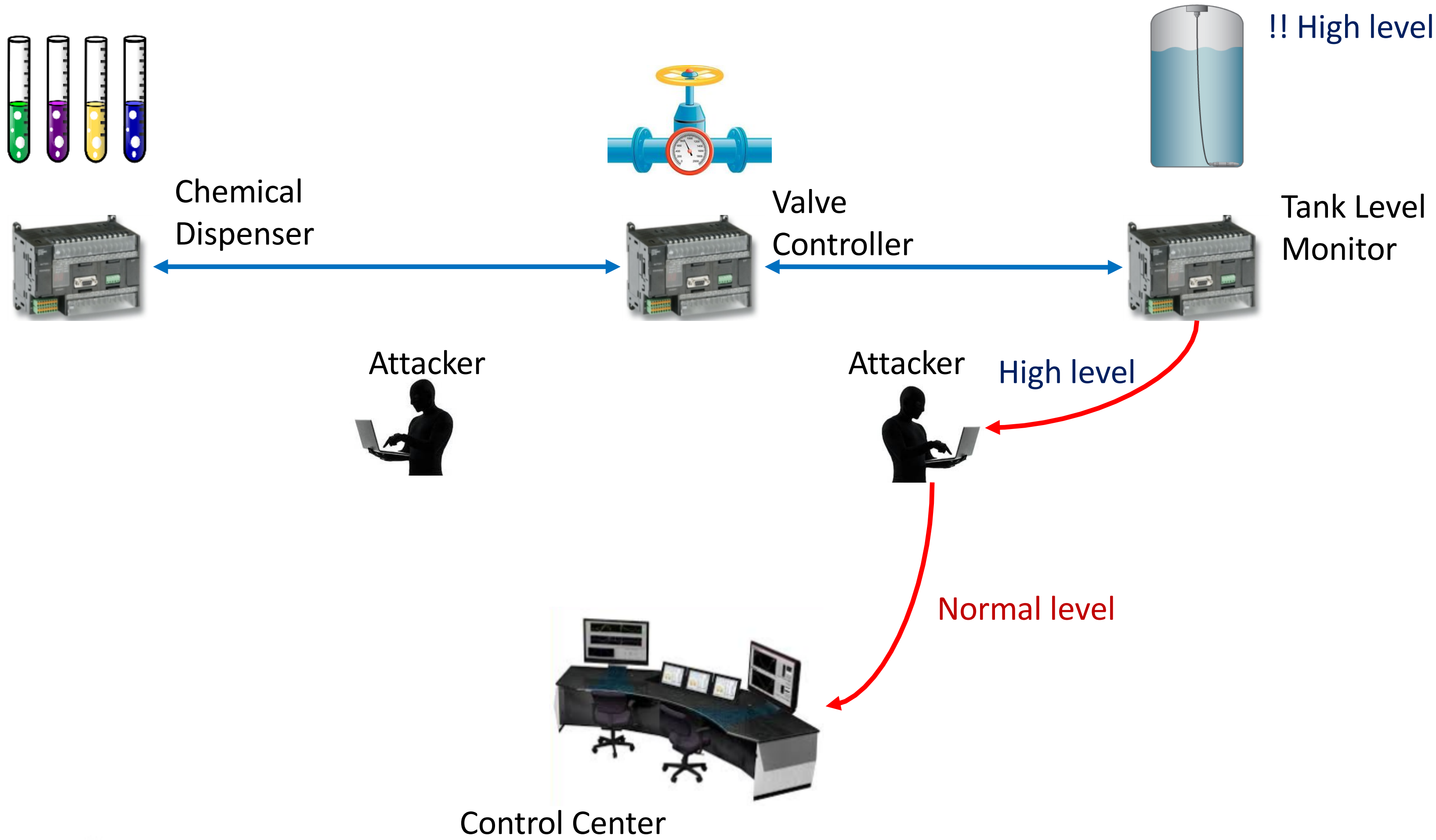
Motivation: Integrity Attacks



iTrust
Center for Research in
Cyber Security

Cyber-security in ICS

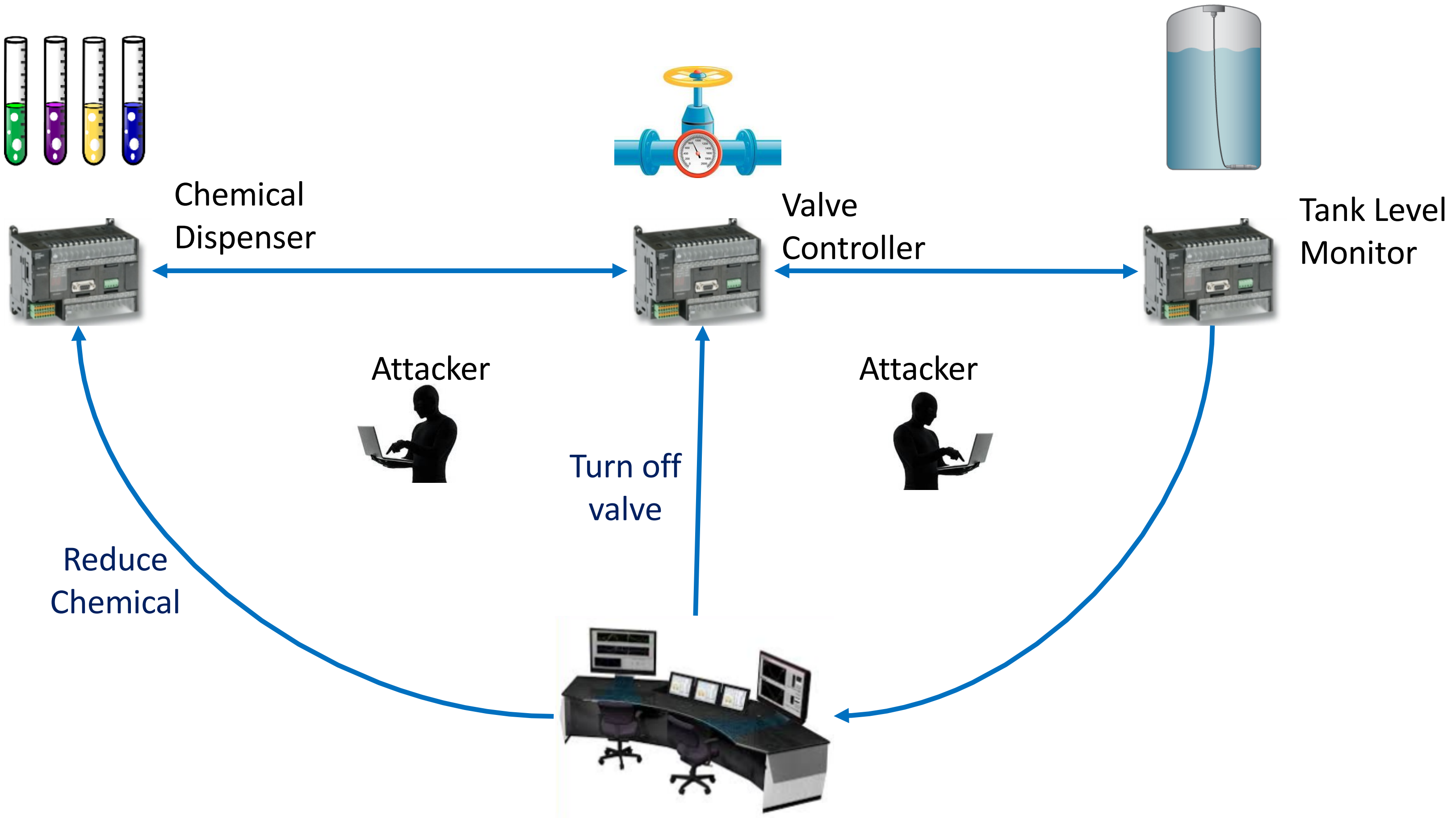
Motivation: Integrity Attacks



iTrust
Center for Research in
Cyber Security

Cyber-security in ICS

Motivation: Integrity Attacks

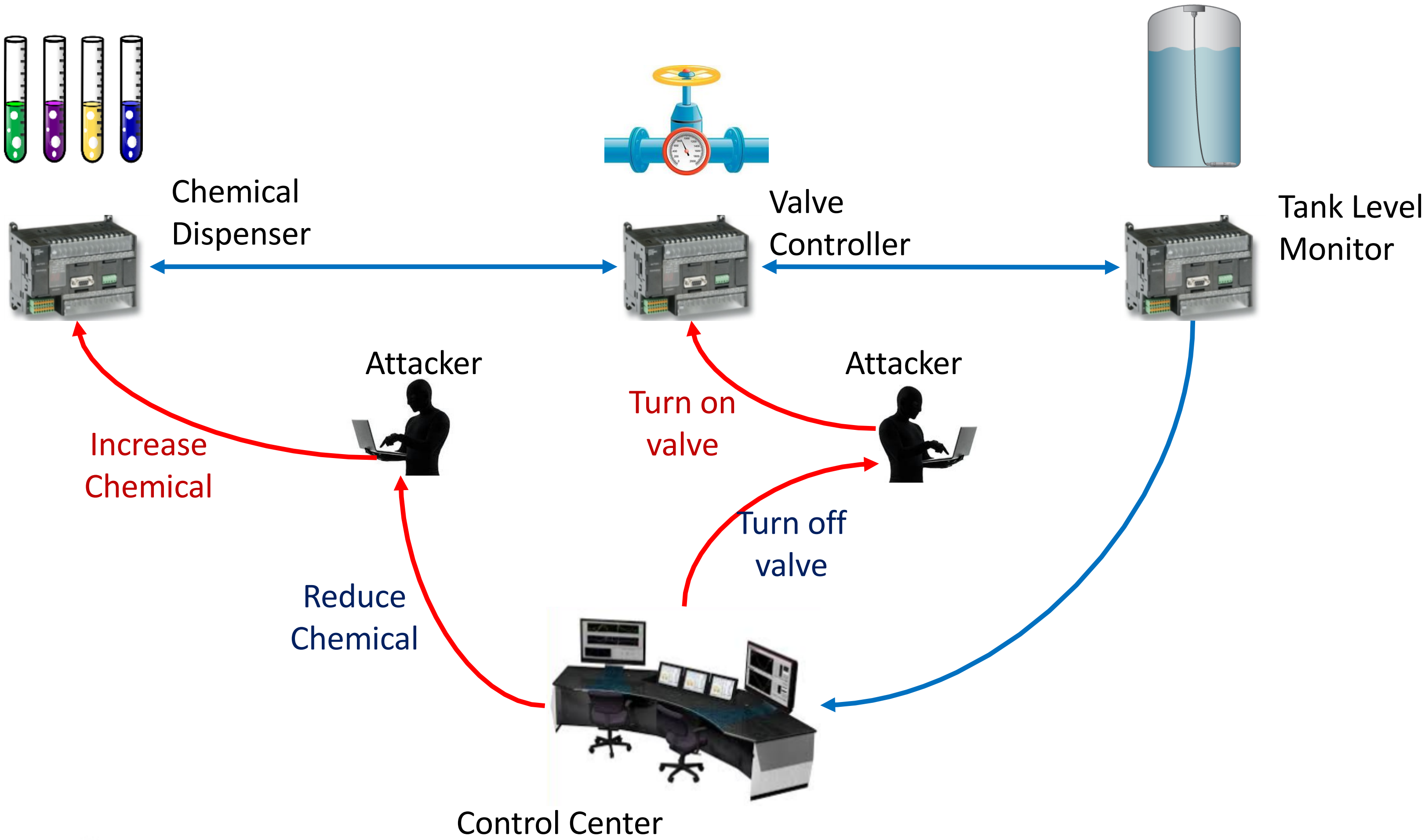


SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

iTrust
Center for Research in Cyber Security

Cyber-security in ICS

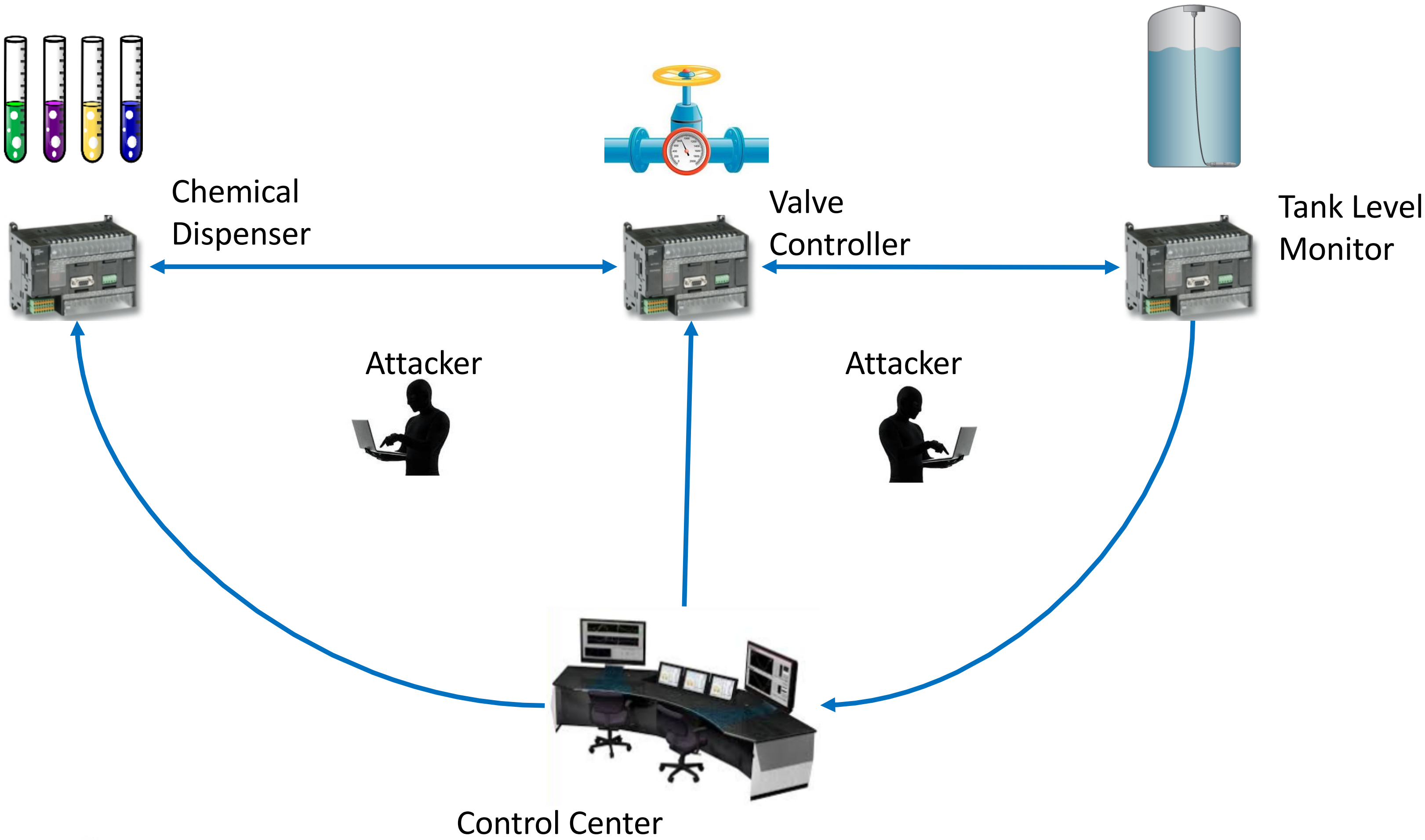
Motivation: Integrity Attacks



iTrust
Center for Research in Cyber Security

Cyber-security in ICS

Motivation: Integrity Attacks

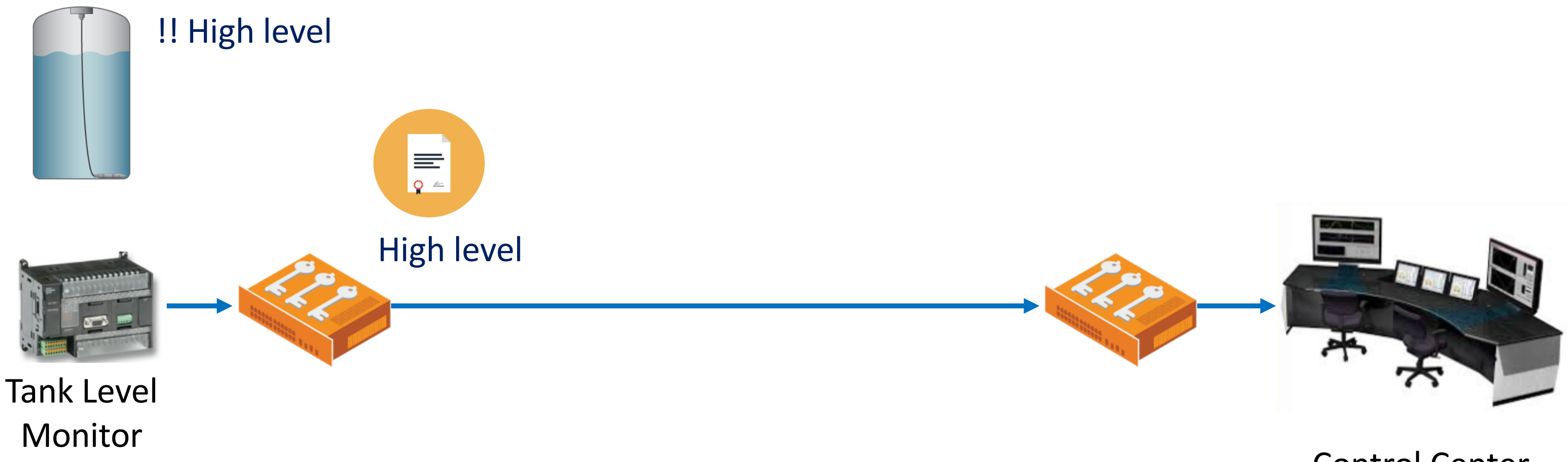


iTrust
Center for Research in
Cyber Security

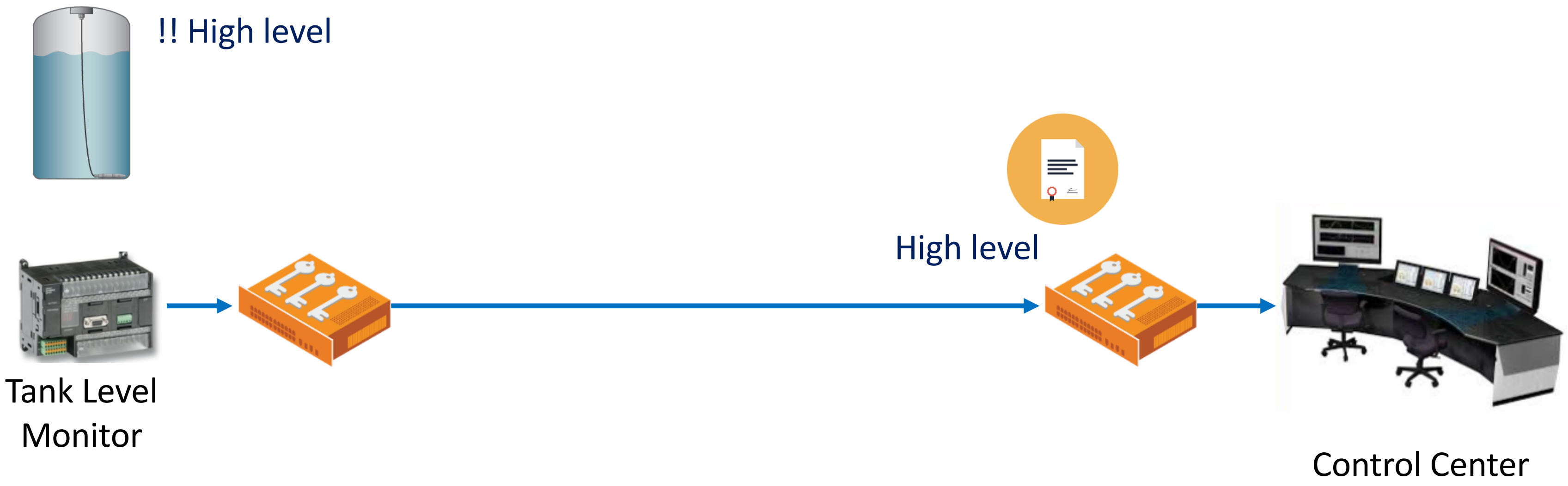
Countermeasures
Authenticity & Integrity checks

Countermeasures

Authenticity & Integrity checks



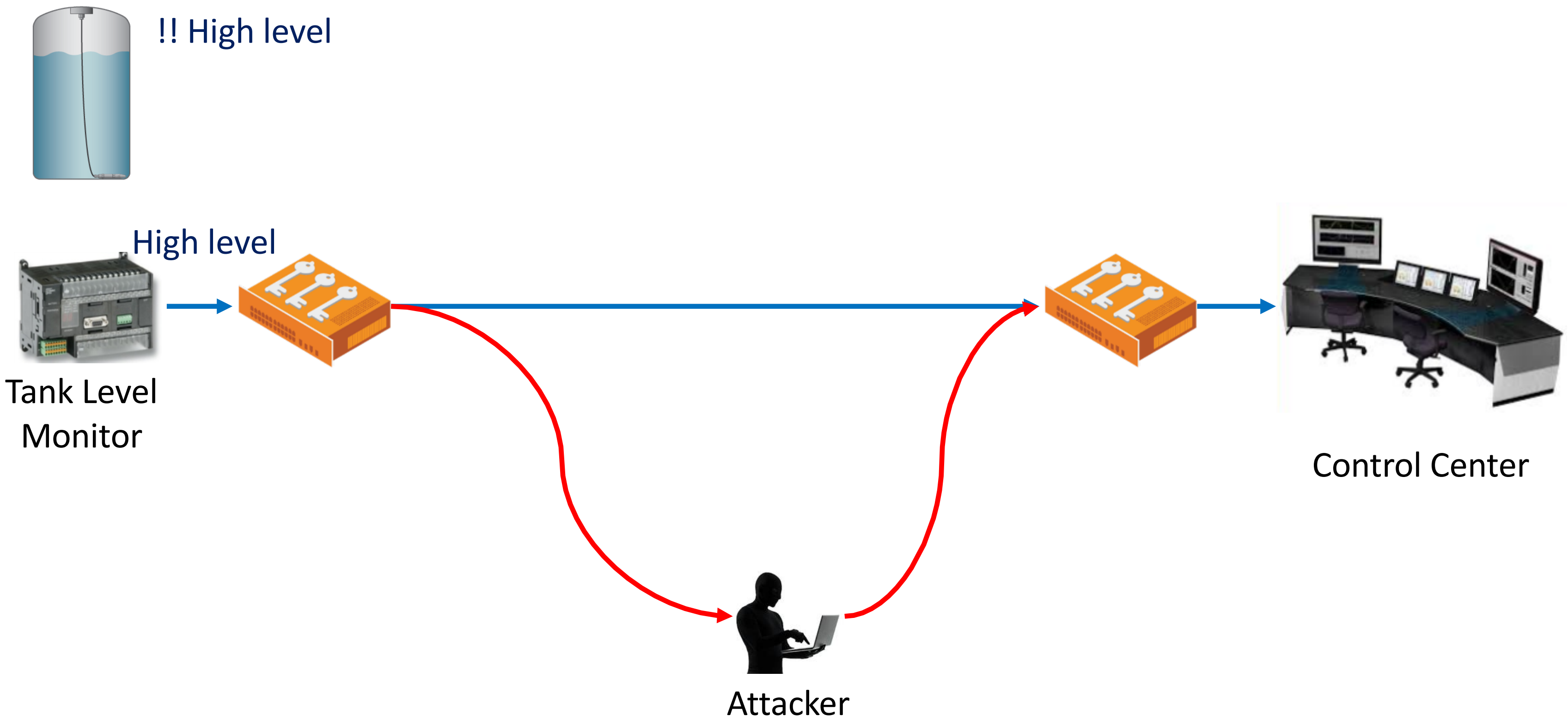
Countermeasures
Authenticity & Integrity checks



Countermeasures

Authenticity & Integrity checks

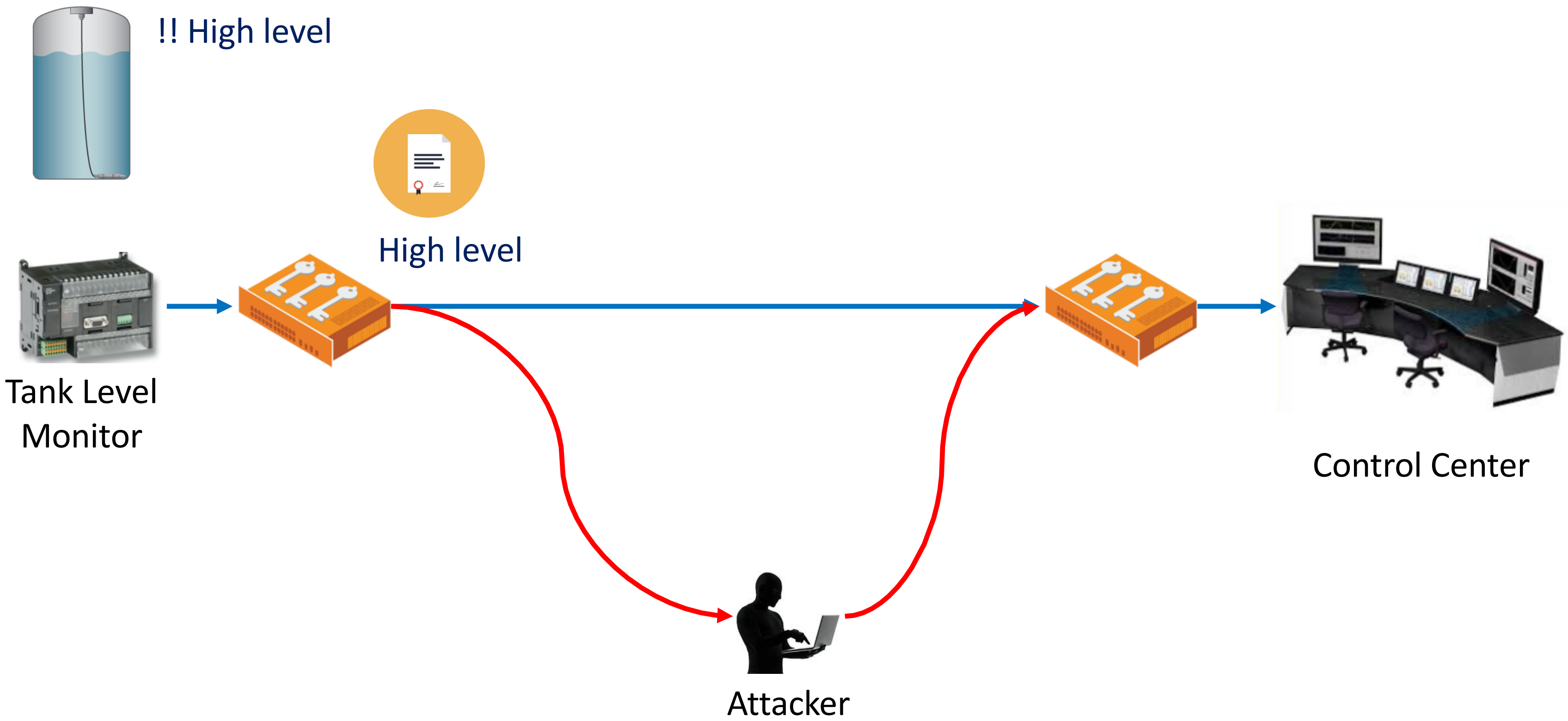
Countermeasures
Authenticity & Integrity checks



iTrust
Center for Research in Cyber Security

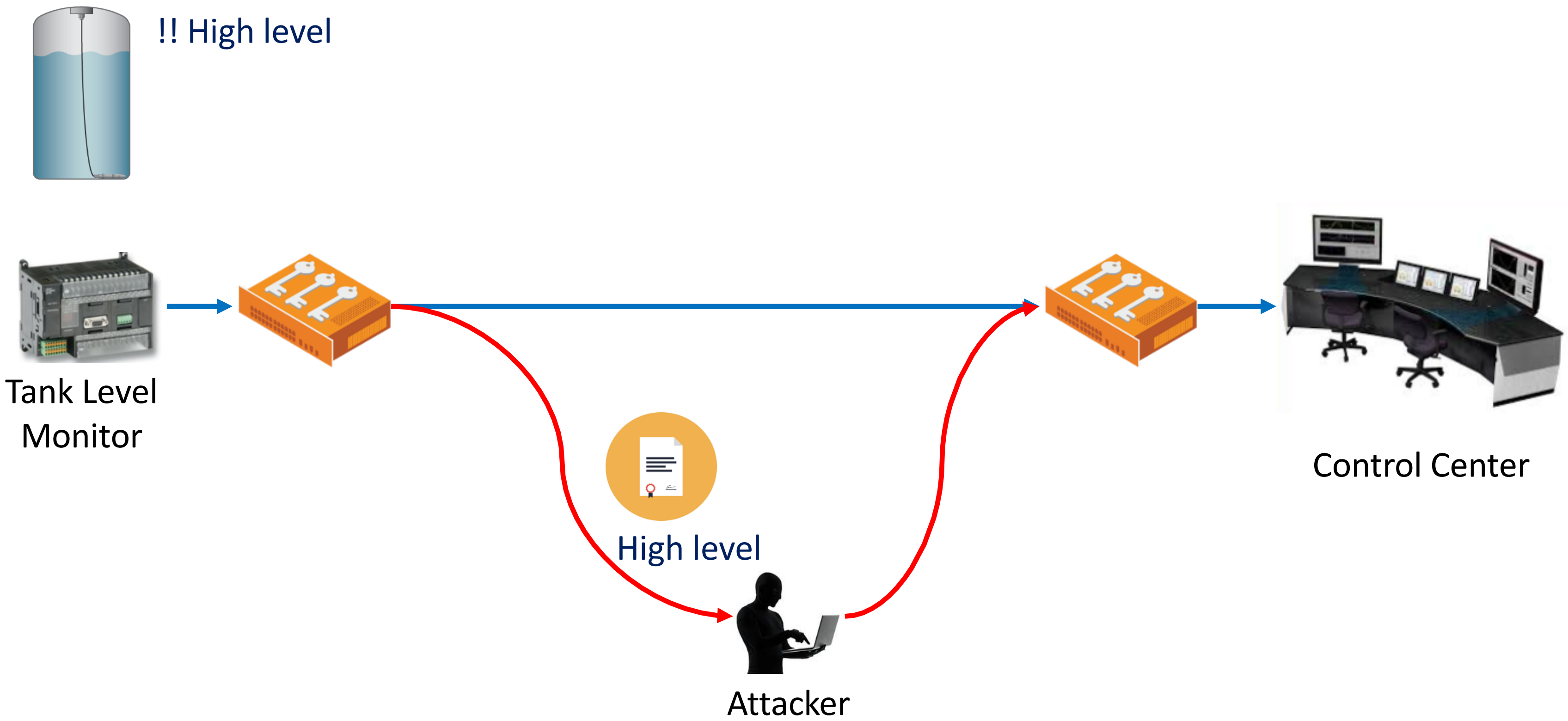
Countermeasures

Authenticity & Integrity checks



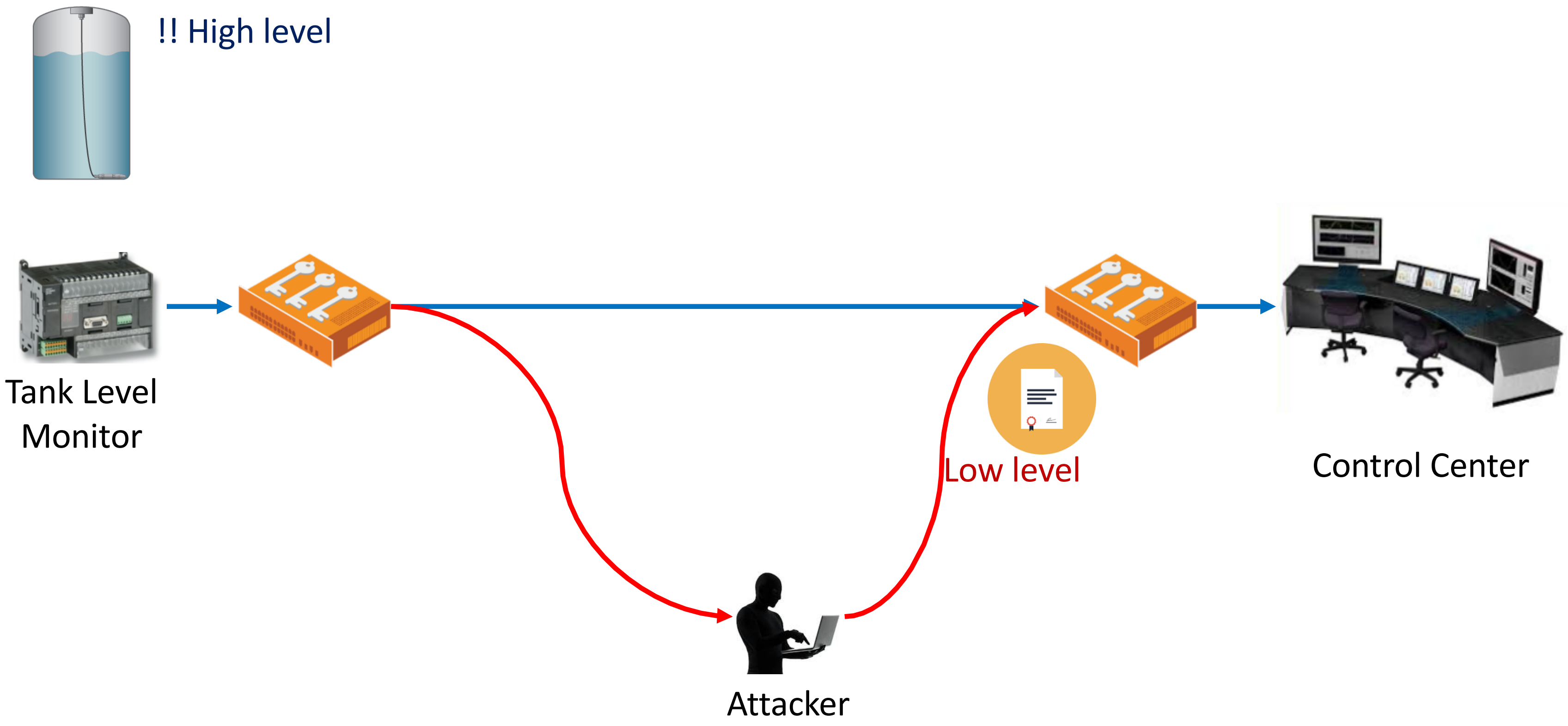
Countermeasures

Authenticity & Integrity checks



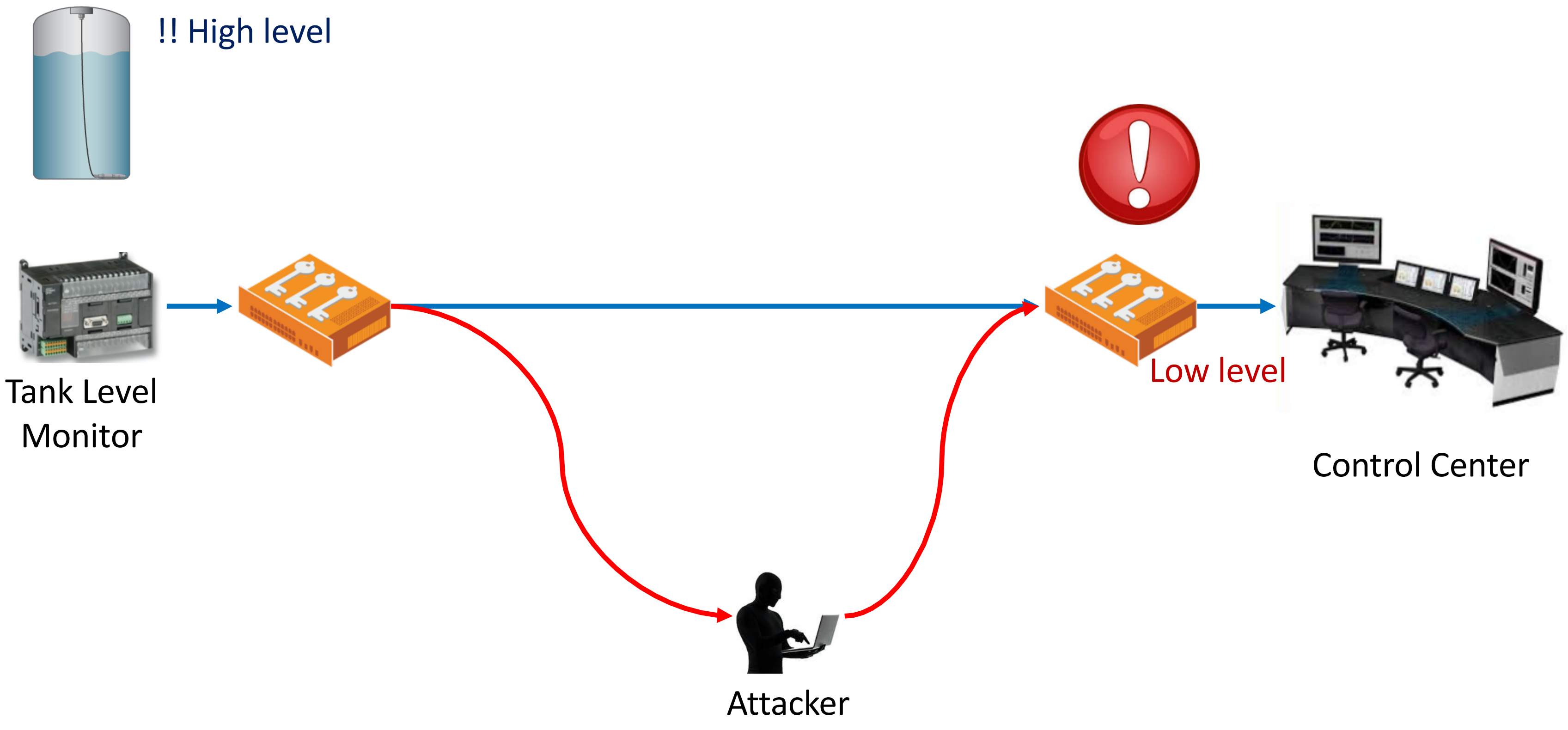
Countermeasures

Authenticity & Integrity checks



Countermeasures

Authenticity & Integrity checks



iTrust
Center for Research in Cyber Security

Industrial Control Systems

IT/OT Requirements

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

Attribute	Information Technology Systems (IT)	Industrial Control Systems (OT)
Component Lifetime	3 to 5 years	10 to 15 years
Connectivity	Corporate network, IP-based, standard protocols	Control Network, proprietary protocols
Performance Requirements	Non-real-time	Real-time

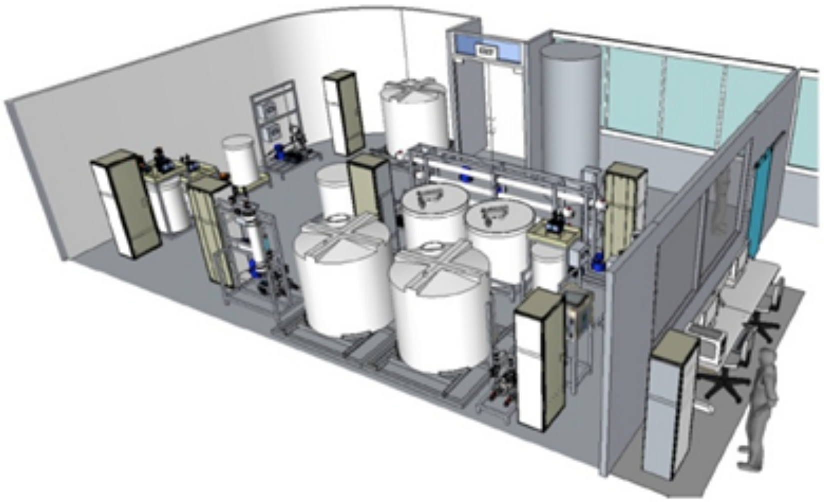
Sources:
NIST: Guide to Industrial Control Systems Security. 800-82 Rev2
http://www.wbdg.org/

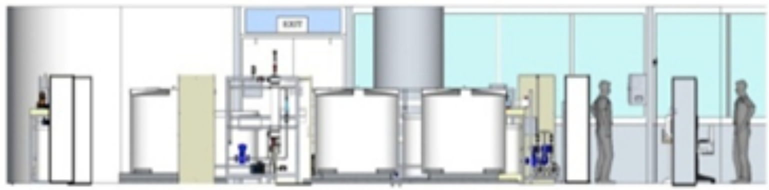
iTrust
Center for Research in Cyber Security

Data from a real ICS

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

SWaT Testbed





Secure Water Treatment (SWaT) is a testbed for research in the area of cyber security.

iTrust
Center for Research in Cyber Security

Data from a real ICS

Real-time requirements

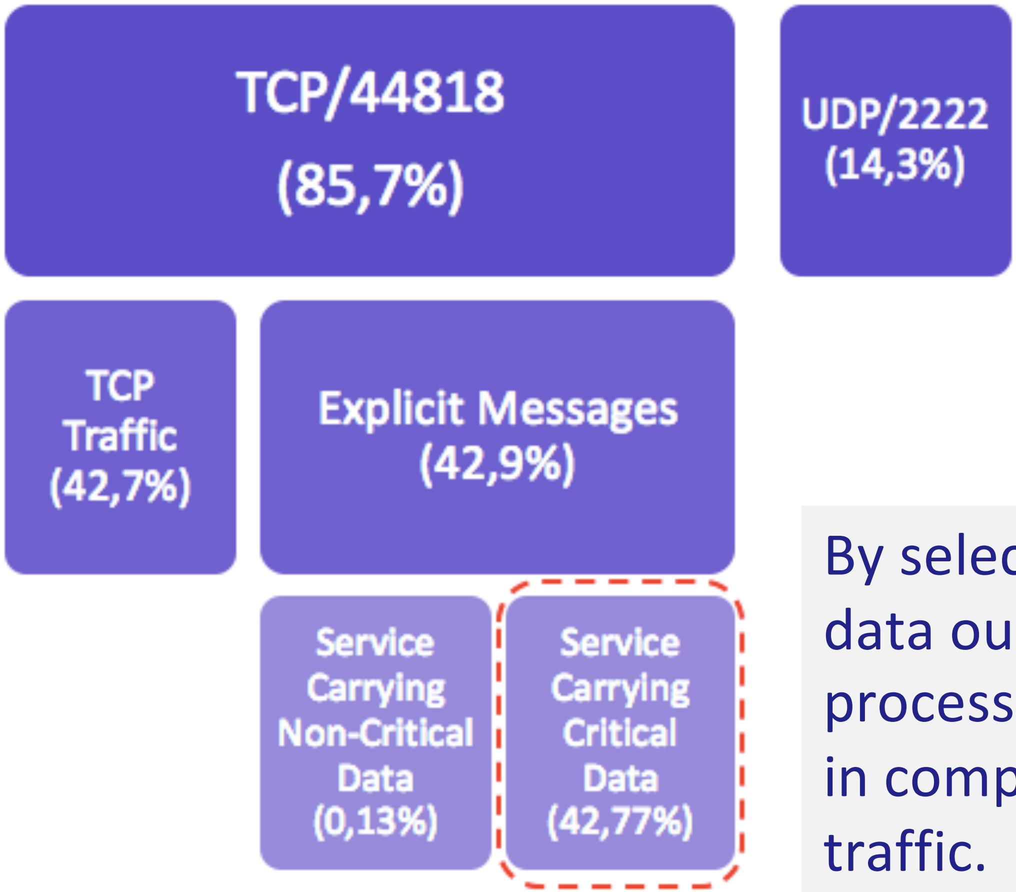
CIP Message Type		Sent	Received
	REQUEST	561 Pk/s Size (μ=63B, σ=3.36)	607 Pk/s Size (μ=69B, σ=5.32)
	RESPONSE	566 Pk/s Size (μ=75B, σ=58.16)	561 Pk/s Size (μ=86B, σ=9.42)
	TOTAL	**1127 Pk/s (Required Signing Performance)**	**1168 Pk/s (Required Verifying Performance)**

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

iTrust
Center for Research in Cyber Security

Data from a real ICS

Understanding ICS Data

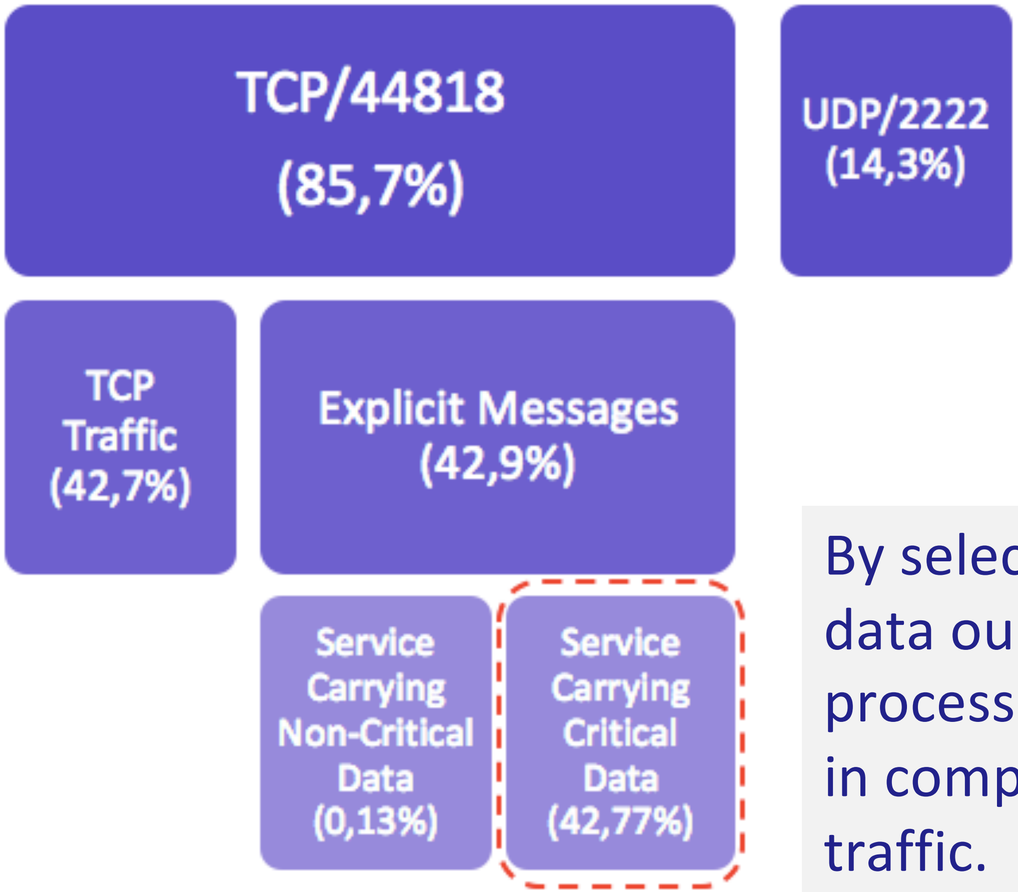


By selecting CIP services with critical data our proposal avoids additional processing and bandwidth overheads in comparison with signing all CIP traffic.

Data from a real ICS

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

Understanding ICS Data



CIP Services (Critical Data):

Read_Tag

Write_Tag

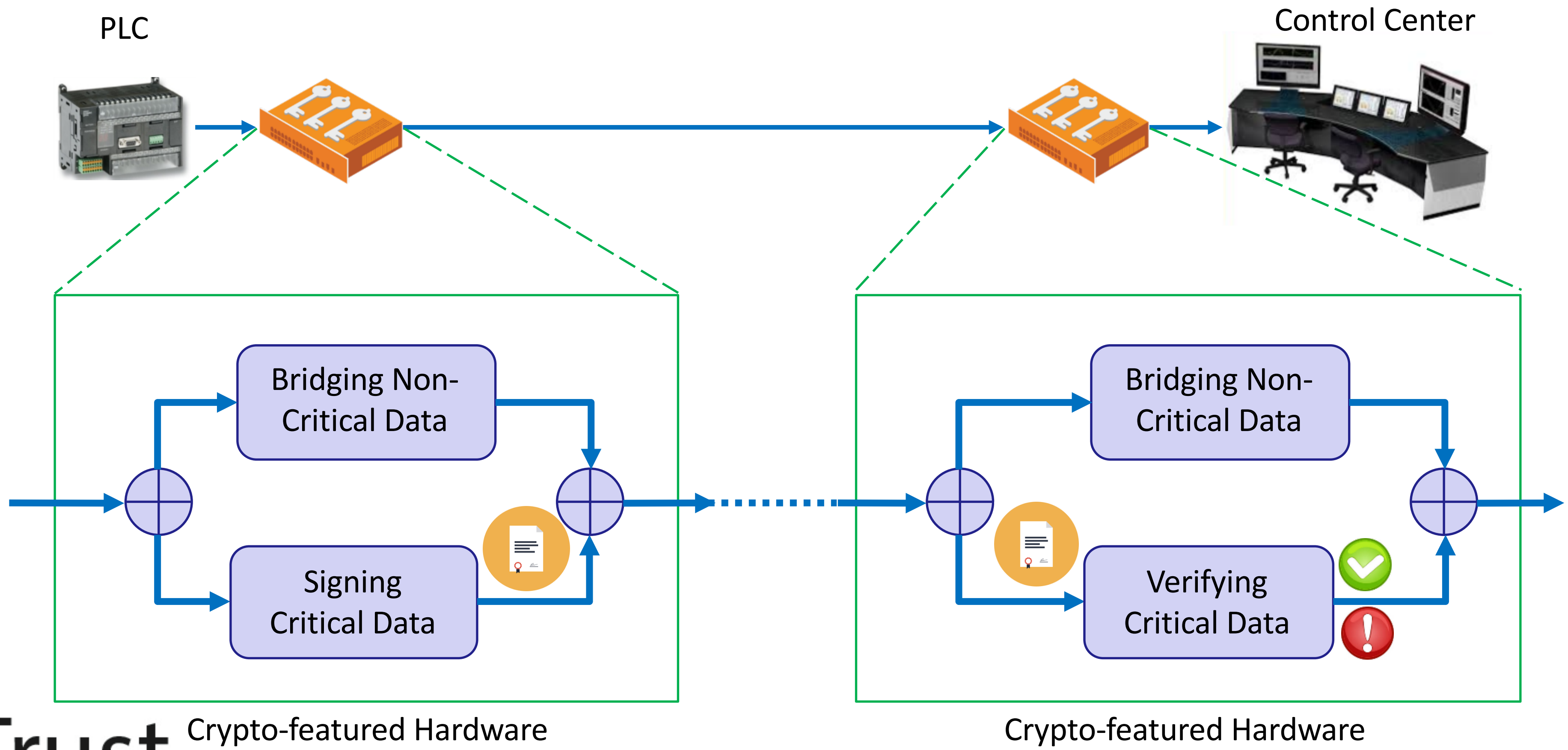
Read_Tag_Fragmented

By selecting CIP services with critical data our proposal avoids additional processing and bandwidth overheads in comparison with signing all CIP traffic.

iTrust
Center for Research in Cyber Security

SPA Protocol

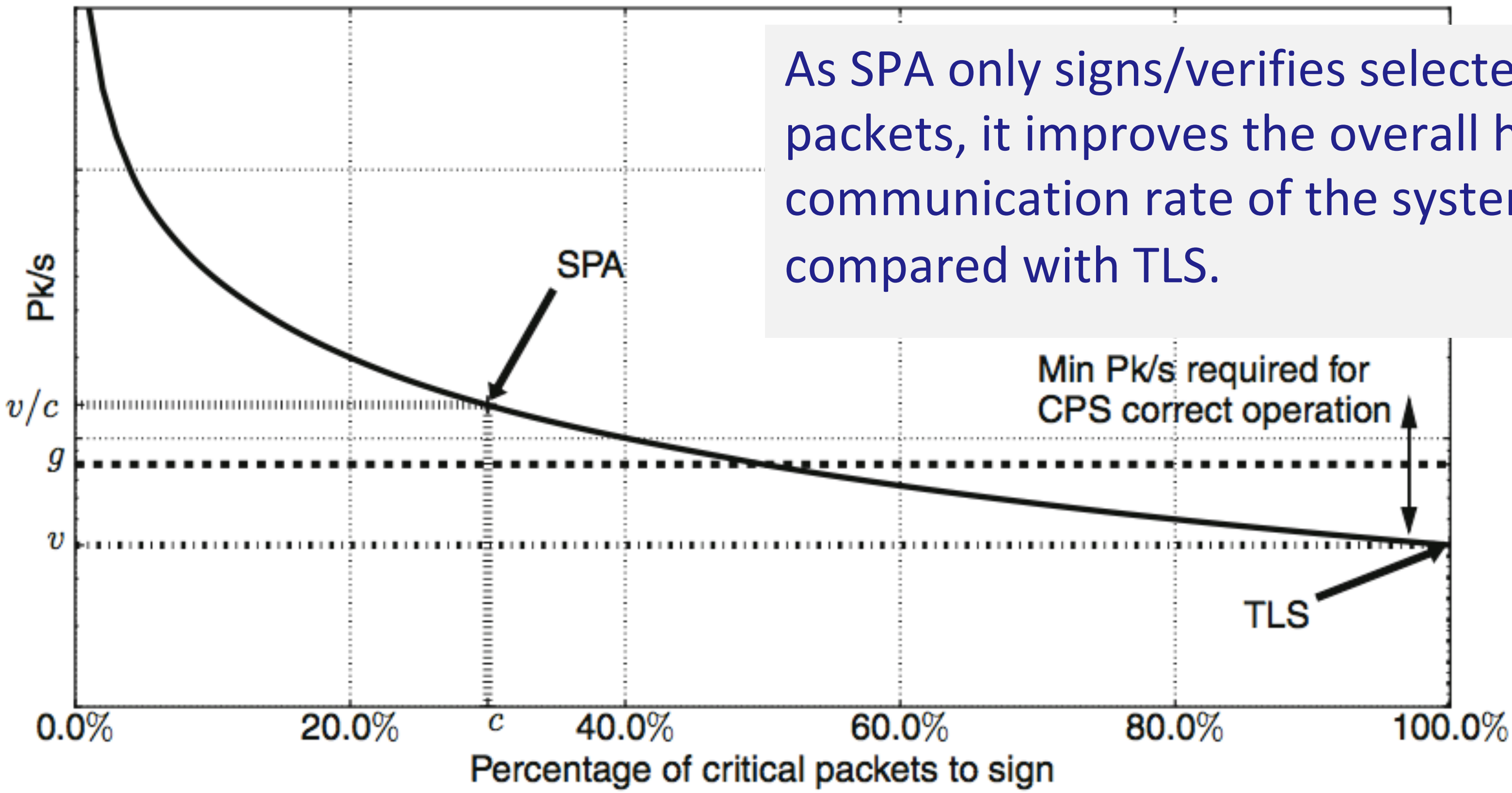
Selective Packet Authentication



iTrust Center for Research in Cyber Security

Comparison with TLS

SPA Evaluation



As SPA only signs/verifies selected critical packets, it improves the overall hardened communication rate of the system compared with TLS.

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

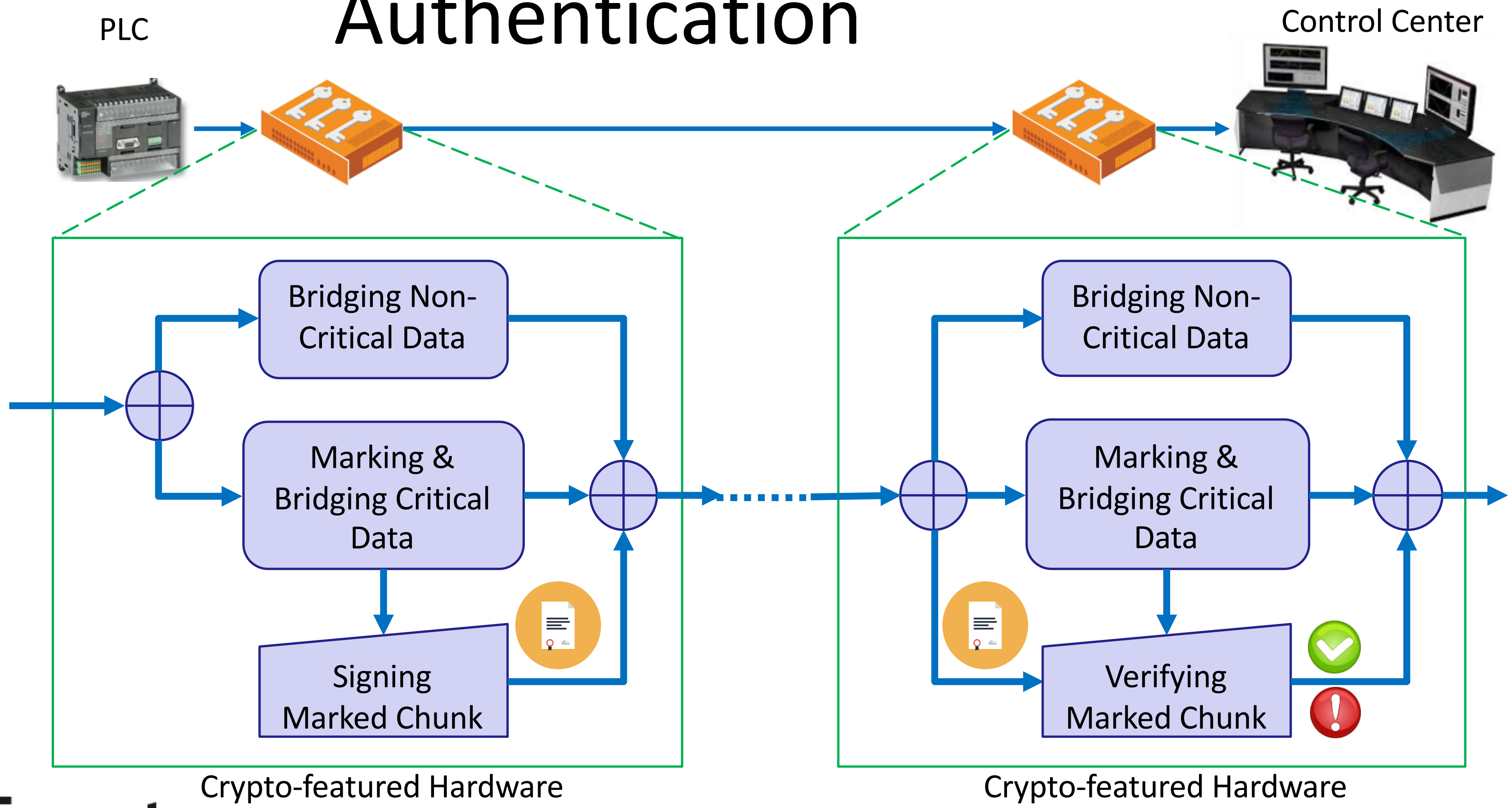
Established in collaboration with MIT

iTrust

Center for Research in Cyber Security

ASPA Protocol

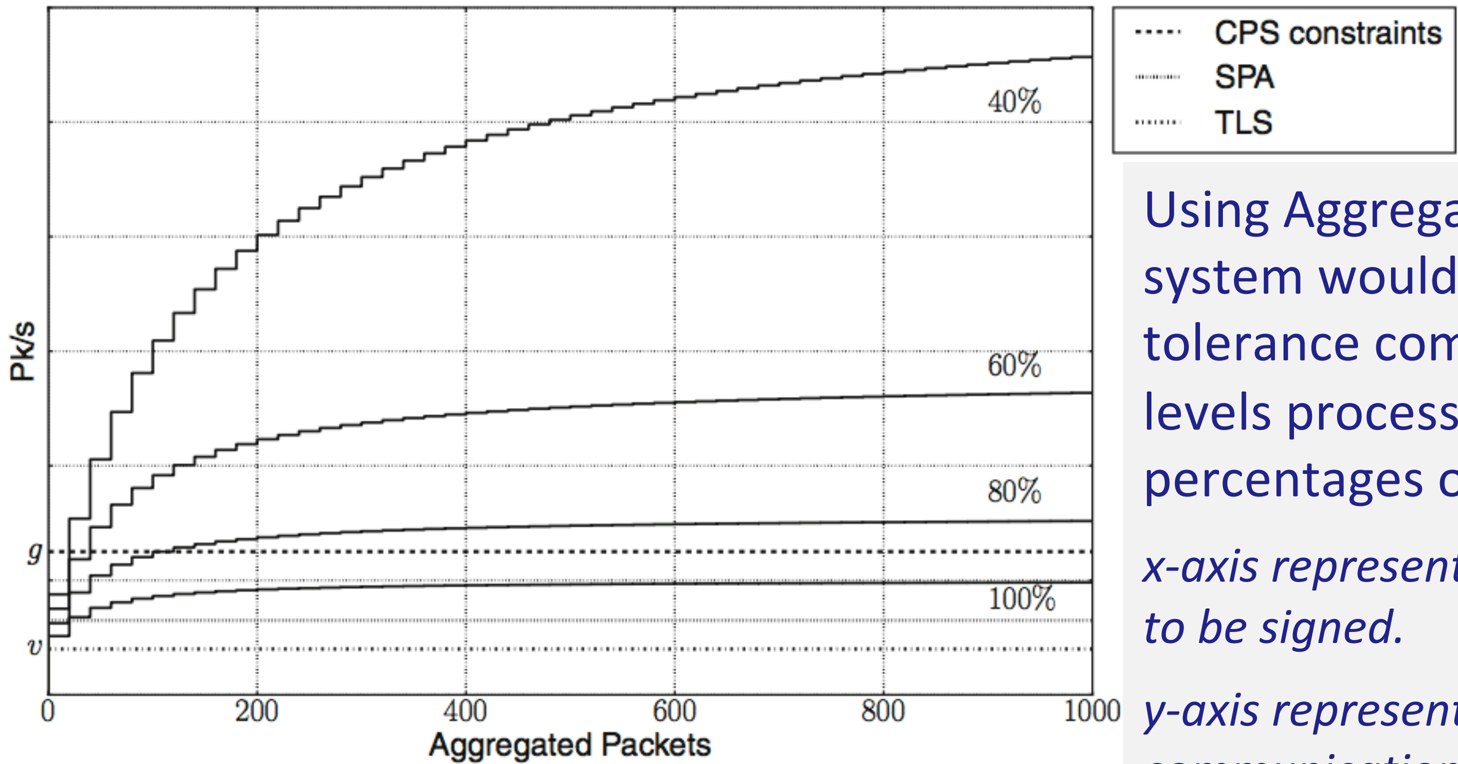
Aggregated Selective Packet Authentication



iTrust
Center for Research in Cyber Security

Comparison with TLS

ASPA Evaluation



Using Aggregated-SPA the system would achieve higher tolerance communication levels processing different percentages of critical data.

x-axis represents chunk of packets to be signed.

y-axis represents tolerance at communication level reached by the system.

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

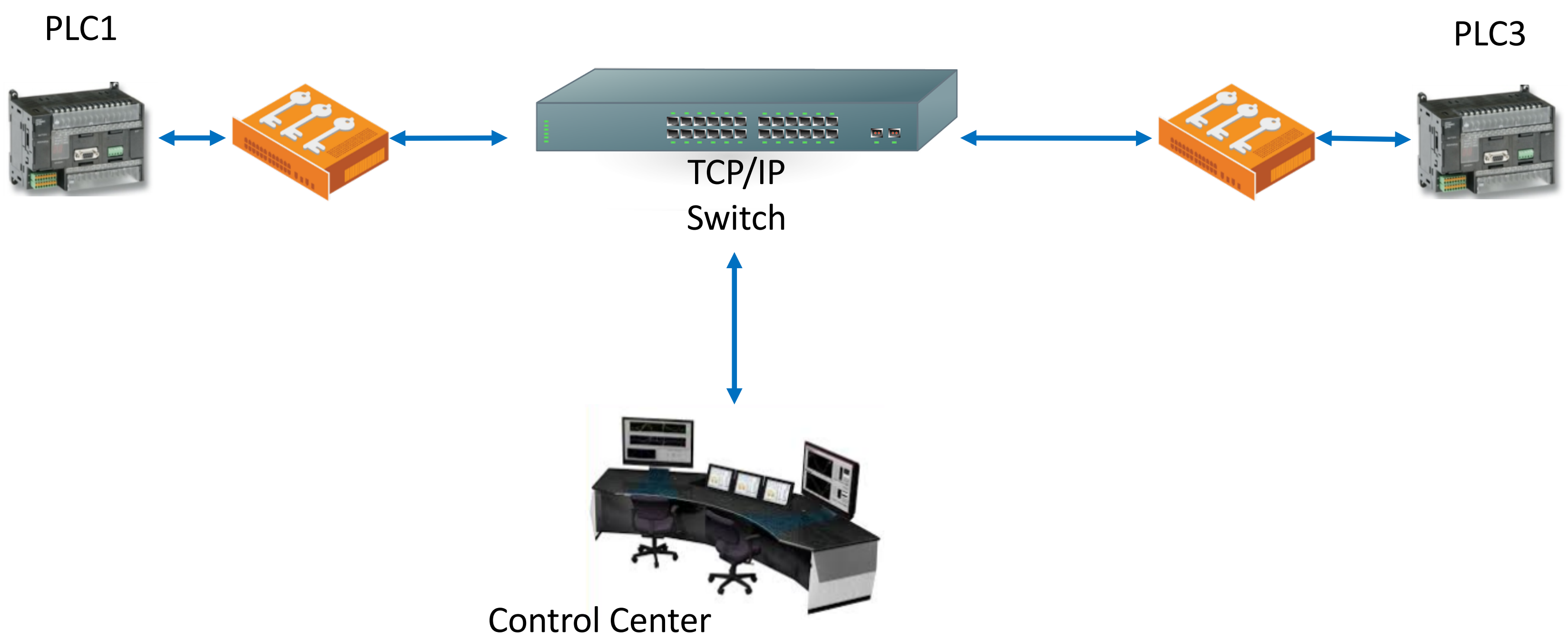
Established in collaboration with MIT

iTrust

Center for Research in Cyber Security

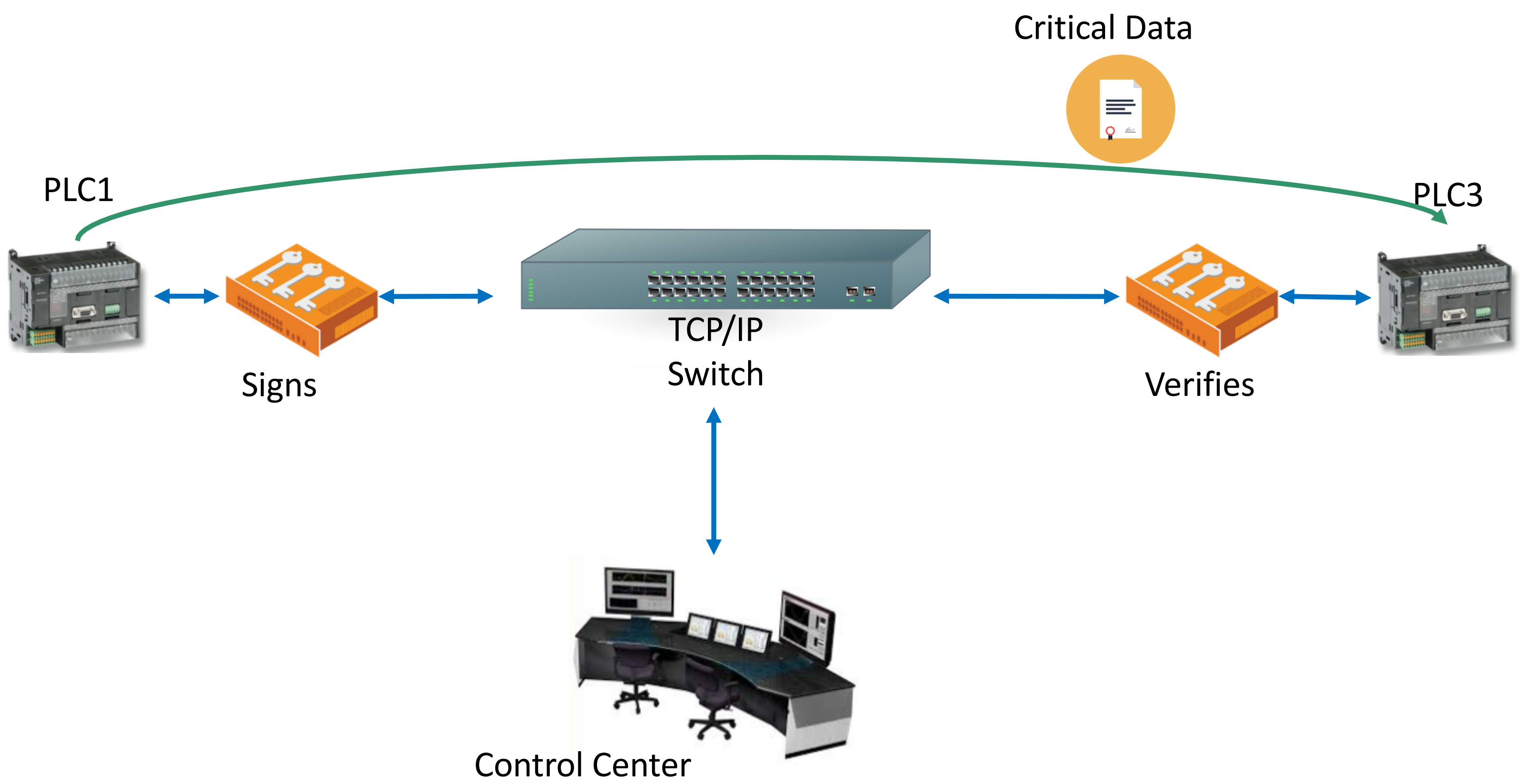
Implementation

Real Scenario on SWaT Testbed



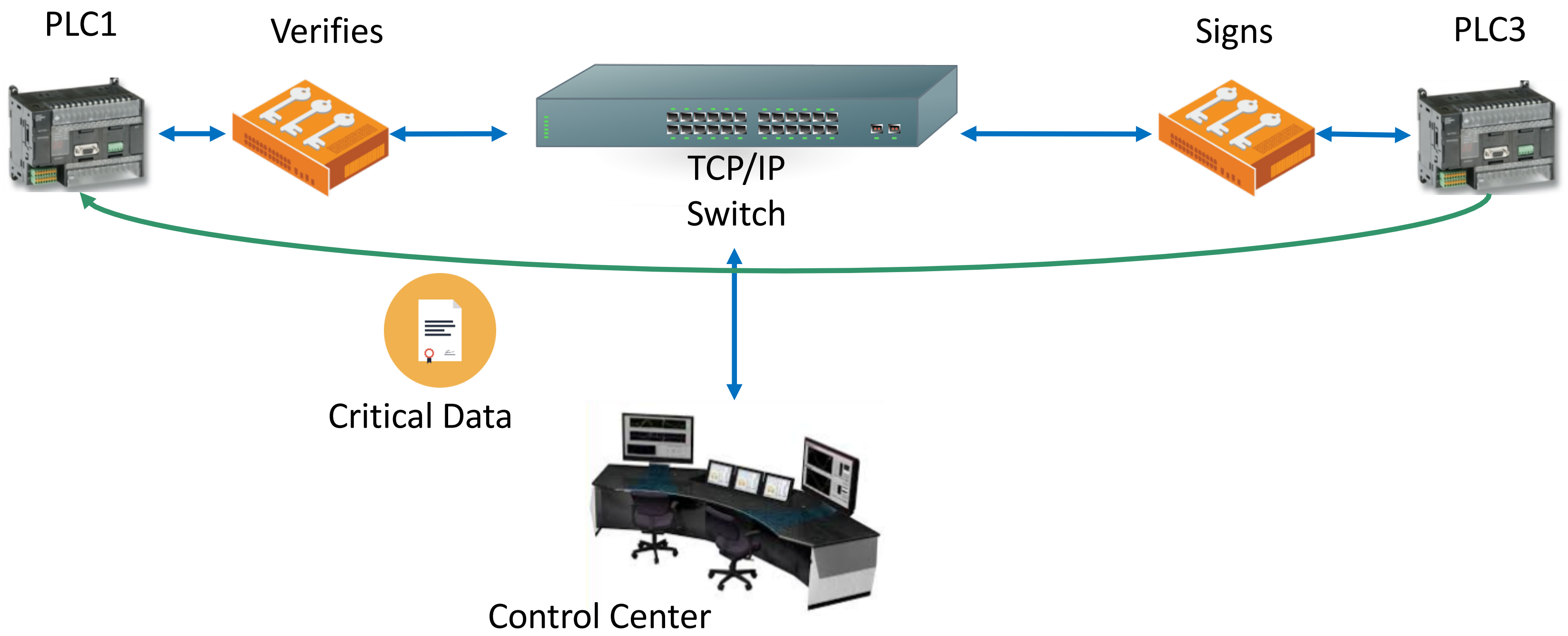
Implementation

Real Scenario on SWaT Testbed



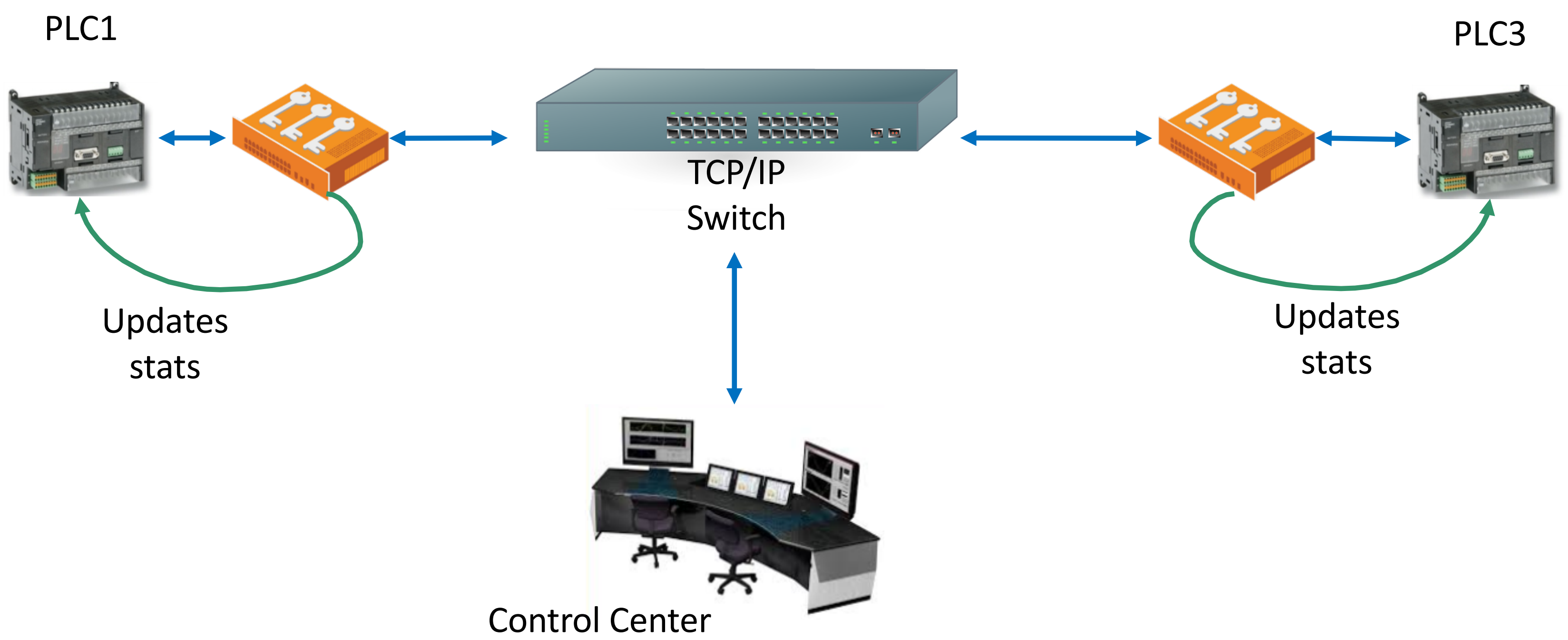
Implementation

Real Scenario on SWaT Testbed



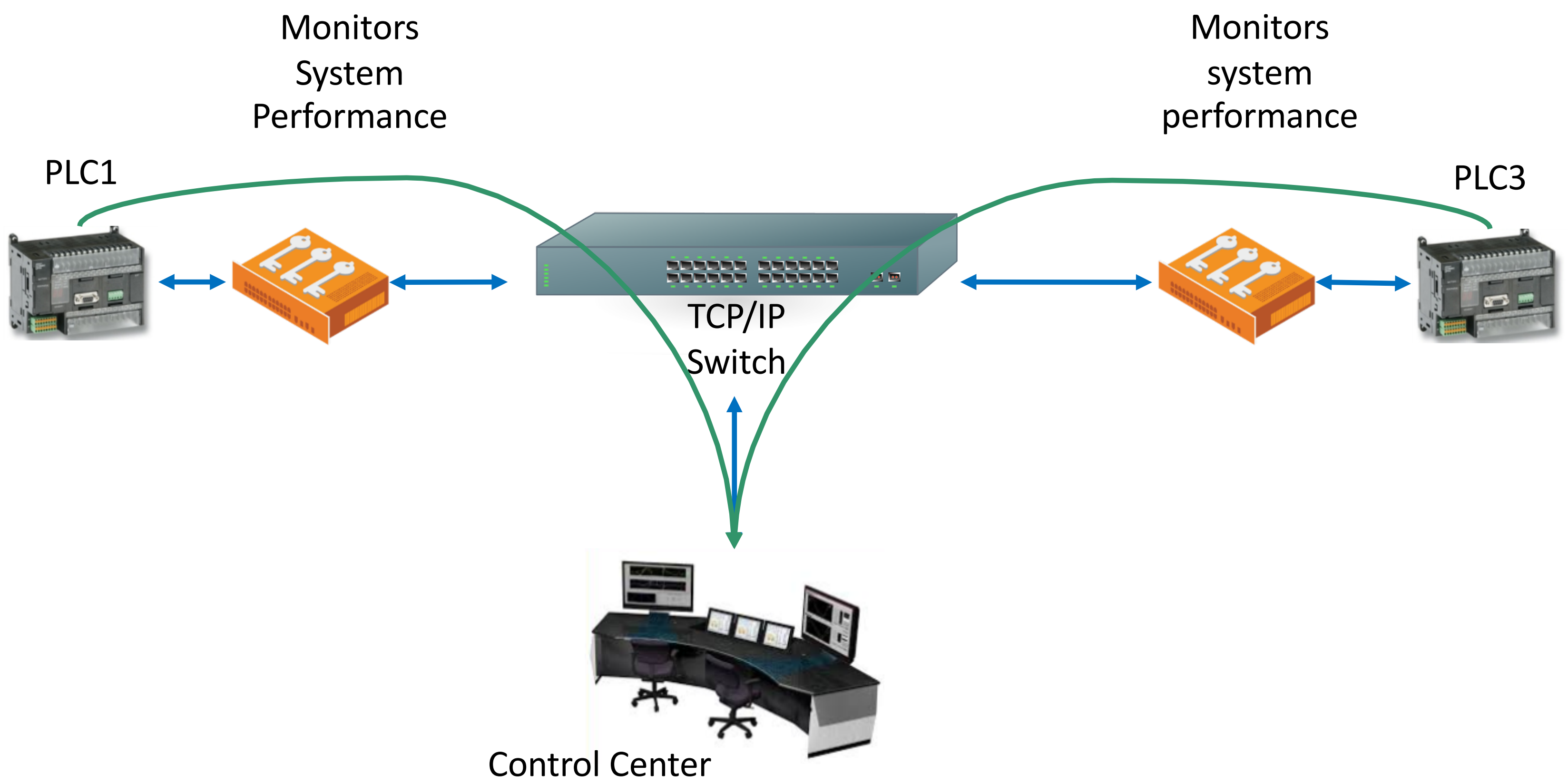
Implementation

Real Scenario on SWaT Testbed



Implementation

Real Scenario on SWaT Testbed



iTrust
Center for Research in
Cyber Security

Benchmark

Hardware Selection

Hardware	Processor	CPU	Memory
Controllino	ATmega2560 Microcontroller	16 MHz	256 KB
ARM (VM*)	ARM926EJ-S	540 MHz	256 MB
Raspberry PI 2	Quad-core ARM Cortex-A7	900 MHz	1 GB
Raspberry PI 3	Quad-core ARM Cortex-A53	1200 MHz	1 GB
PC (VM*)	Intel Core i5-5300 U	2300 MHz	2 GB

*VM: Virtual Machine

Benchmark

Hardware Performance

Data Size (Bytes)	Controllino	ARM	Raspberry PI2	Raspberry PI3	PC
64	2.2×10^4	76	53	15	2
128	3.3×10^4	78	58	16	2
256	5.5×10^4	84	69	18	3
512	1×10^5	117	89	32	4
1K	1.8×10^5	171	130	35	6
2K	3.6×10^5	252	211	58	10
4K	7×10^5	474	374	104	18
ECDSA	N/A	1.5×10^5	1×10^5	3.2×10^4	3.1×10^3

All data in µs

Cryptographic Algorithms:

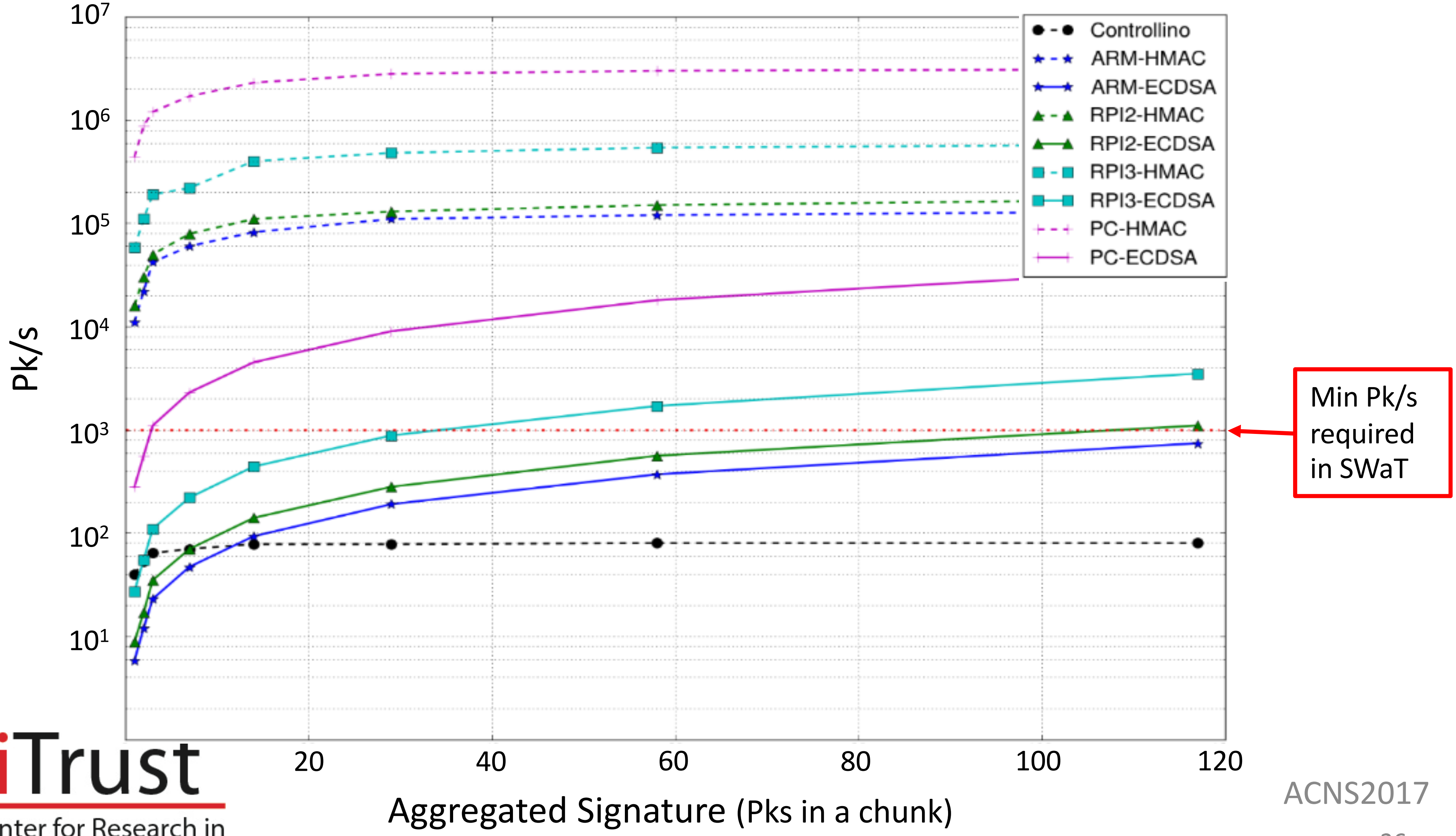
- Symmetric: HMAC-SHA256
- Asymmetric: ECDSA

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

iTrust
Center for Research in Cyber Security

ASPA Protocol

Performance Evaluation (Speed)



iTrust
Center for Research in Cyber Security

Conclusions

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

- Our protocols are backward compatible, as they transmit authentication data as payload in legacy industrial protocols.
- With inexpensive and fast hardware (Raspberry PI), it is feasible to enhance legacy plants with authentic channels for strong signature algorithms with simple protocols.
- It is feasible to significantly raise the bar against attackers of ICS by including authentication based on modern cryptography without compromising efficiency or cost.
- We plan to compare the real-time constraints of SWaT with constraints in other ICS Testbeds (Smart Grid).

iTrust
Center for Research in Cyber Security

Thank you

Q & A

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Established in collaboration with MIT

Backup Slides

iTrust

Center for Research in Cyber Security

Industrial Control Systems

IT/OT Requirements

Attribute	Information Technology Systems (IT)	Industrial Control Systems (OT)
Purpose	Process transaction, provide information	Controls and monitor physical processes
Role	Support people	Control machines
Architecture	Enterprise wide infrastructure and applications	Event-driven, real-time, embedded hardware and customized software
Component Lifetime	3 to 5 years	10 to 15 years
Interfaces	GUI, Web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays
Connectivity	Corporate network, IP-based, standard protocols	Control Network, proprietary protocols
Performance Requirements	Non-real-time	Real-time
Major risk impacts	Delay of business operations	Environmental impacts, loss of life, equipment, or production

Sources:
NIST: Guide to Industrial Control Systems Security. 800-82 Rev2
http://www.wbdg.org/

Injecting data into Ethernet IP Protocol

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

Ethernet Frame

Ethernet Header	IP Header	TCP/UDP Header	Encapsulation Header	Encapsulation Data	CRC
14 Bytes	*20 Bytes*	*20 Bytes*	*Encapsulation Packet*		

Encapsulation Header

Command	Length	Session Handle	Status	Sender Context	Options
2 Bytes	*2 Bytes*	*4 Bytes*	*4 Bytes*	*8 Bytes*	*4 Bytes*

Encapsulation Data (Common Packet Format)

	Address Item			*Data Item*		
Item Count *(Usual =2)*	Type ID	Length (*l1*)	Data (Connection ID)	Type ID	Length (*l2*)	Data (CIP Data)
2 Bytes	*2 Bytes*	*2 Bytes*	*l1 Bytes*	*2 Bytes*	*2 Bytes*	*l2 Bytes*

iTrust
Center for Research in Cyber Security

Injecting data into Ethernet IP Protocol

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

Ethernet Frame

Ethernet Header	IP Header	TCP/UDP Header	Encapsulation Header	Encapsulation Data	CRC
14 Bytes	*20 Bytes*	*20 Bytes*	*Encapsulation Packet*		

Encapsulation Header

Command	Length	Session Handle	Status	Sender Context	Options
2 Bytes	*2 Bytes*	*4 Bytes*	*4 Bytes*	*8 Bytes*	*4 Bytes*

Encapsulation Data (Common Packet Format)

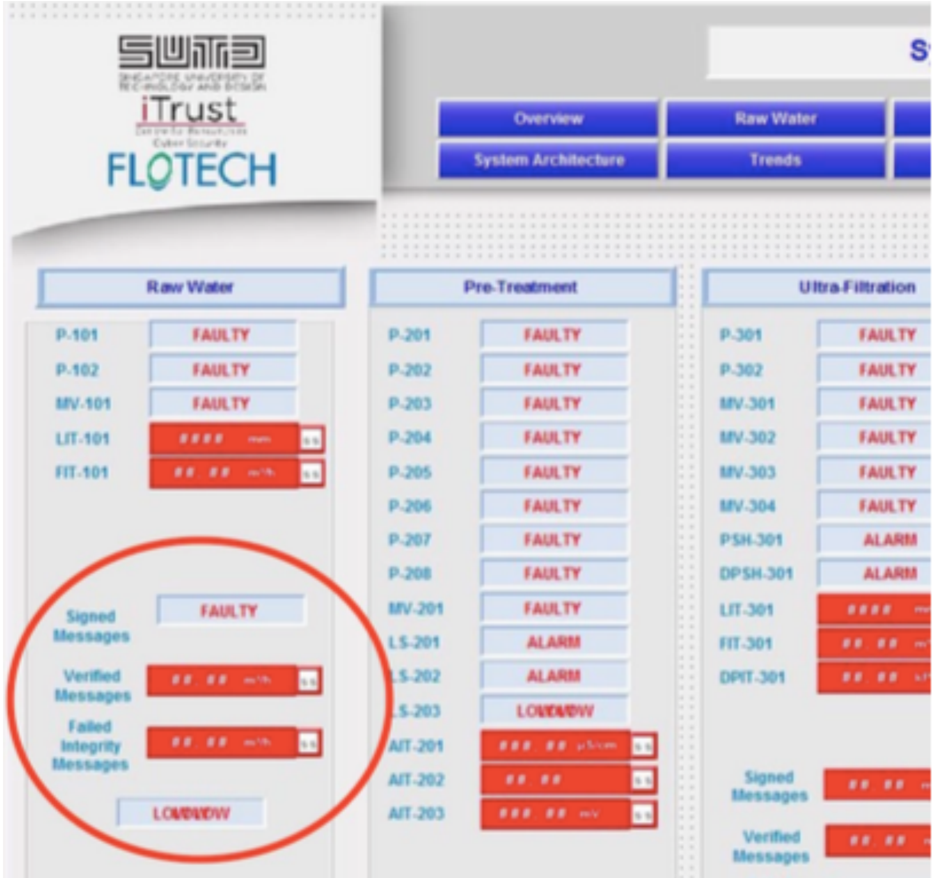
	Address Item			*Data Item*			*Signature Item*		
Item Count *(Usual = ~~2~~ 3)*	Type ID	Length (l_1)	Data (Connection ID)	Type ID	Length (l_2)	Data (CIP Data)	Type ID	Length (l_3)	Data (Signature)
2 Bytes	*2 Bytes*	*2 Bytes*	*l_1 Bytes*	*2 Bytes*	*2 Bytes*	*l_2 Bytes*	*2 Bytes*	*2 Bytes*	*l_3 Bytes*

iTrust
Center for Research in Cyber Security

Authentication Protocols Implementation:

Real Scenario on SWaT Testbed

- SCADA's supervisory reads PLC variables of signing-verification process.
- Statistics about integrity checks might be summarize.
- In case of integrity violations happen an alarm will trigger.



iTrust
Center for Research in Cyber Security

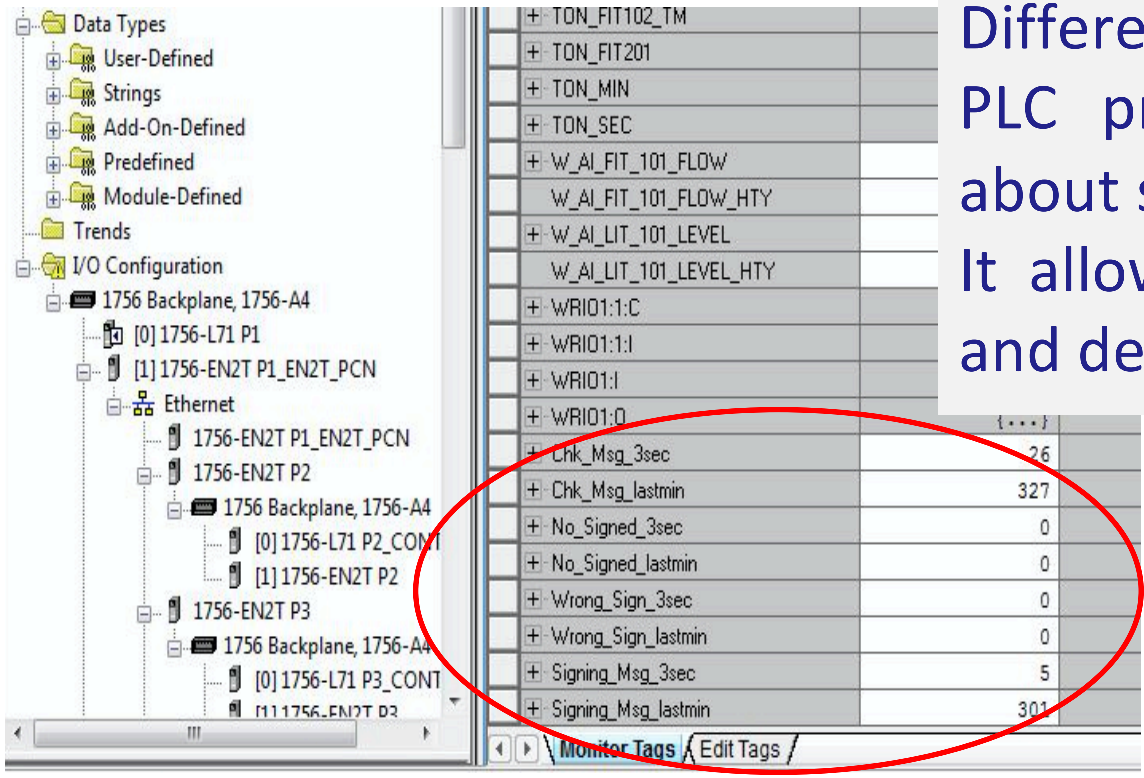
Implementation

Real Scenario on SWaT Testbed

A Raspberry PI is directly connected between the hardened PLC and its closest switch. It bridges communication between the PLC and the rest of the system.

Implementation

Real Scenario on SWaT Testbed



Different tags were configured at PLC program to store statistics about signing/verification process. It allows to monitor the process and debug it.