Everything is Awesome or is It?
Cyber Security Risks in Critical Infrastructure

Awais Rashid

Professor of Cyber Security

Director, EPSRC Centre for Doctoral Training

@BristolCyberSec

University of BRISTOL

Bristol Cyber Security Group

Acknowledgements

Sylvain Frey
Pauline Anthonysamy
Ben Shreeve
Barney Craggs
Joe Gardiner
Matt Edwards
Joseph Hallett
Ben Green
Maria Pinto-Albuquerque
Syed Asad Naqvi
Alberto Zanutto
Karolina Follis
Jerry Busby
Anthony Mazeli
Rob Antrobus
William Jardine

Attack Technologies

Aircraft components
(Software Applications,
Operating Systems,
User interfaces)

Authentication
(Cryptography, Security protocols)

Attack sophistication

Partial-trust

New attack vectors

Multi-stakeholder

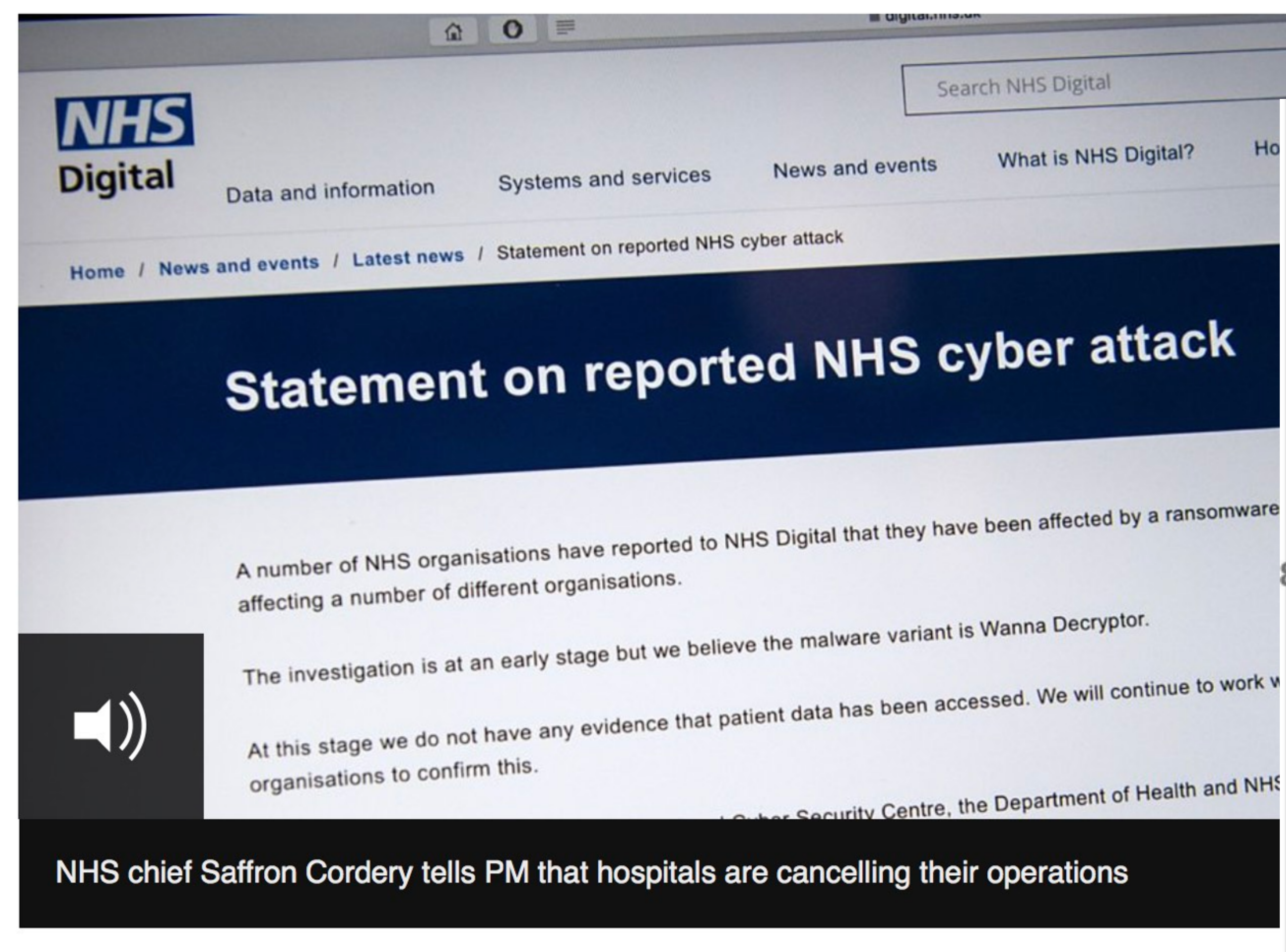
Longevity

Change

Ground interface
(Access control)

Ground components
(Software Applications,
Operating Systems,
User interfaces)

Ivano-Frankivsk



Statement on reported NHS cyber attack

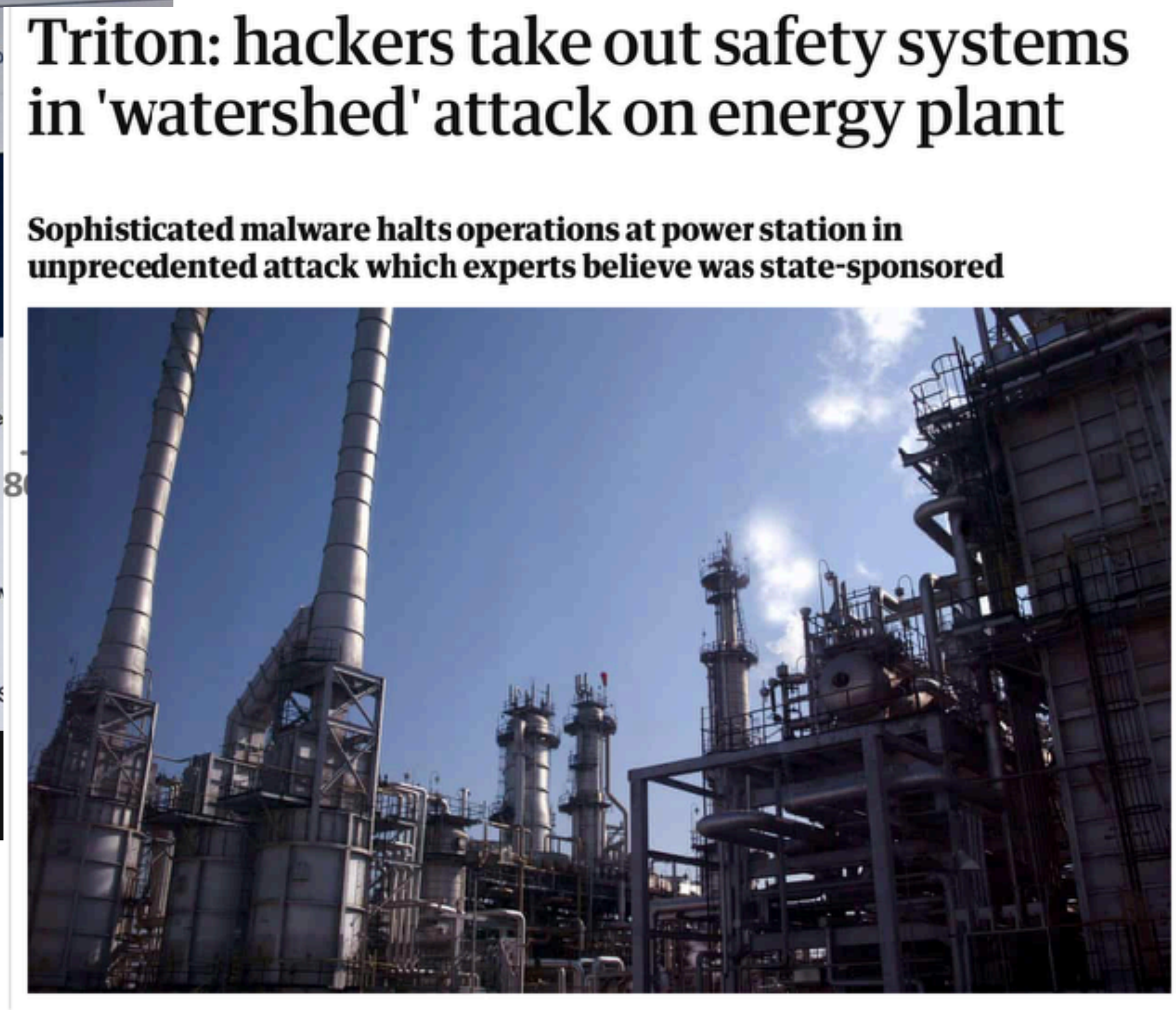
A number of NHS organisations have reported to NHS Digital that they have been affected by a ransomware affecting a number of different organisations.

The investigation is at an early stage but we believe the malware variant is Wanna Decryptor.

At this stage we do not have any evidence that patient data has been accessed. We will continue to work w organisations to confirm this.

Cyber Security Centre, the Department of Health and NHS

NHS chief Saffron Cordery tells PM that hospitals are cancelling their operations



Triton: hackers take out safety systems in 'watershed' attack on energy plant

Sophisticated malware halts operations at power station in unprecedented attack which experts believe was state-sponsored

Scale

of complexity

of connectivity

of attacks

of impact

Attack sophistication

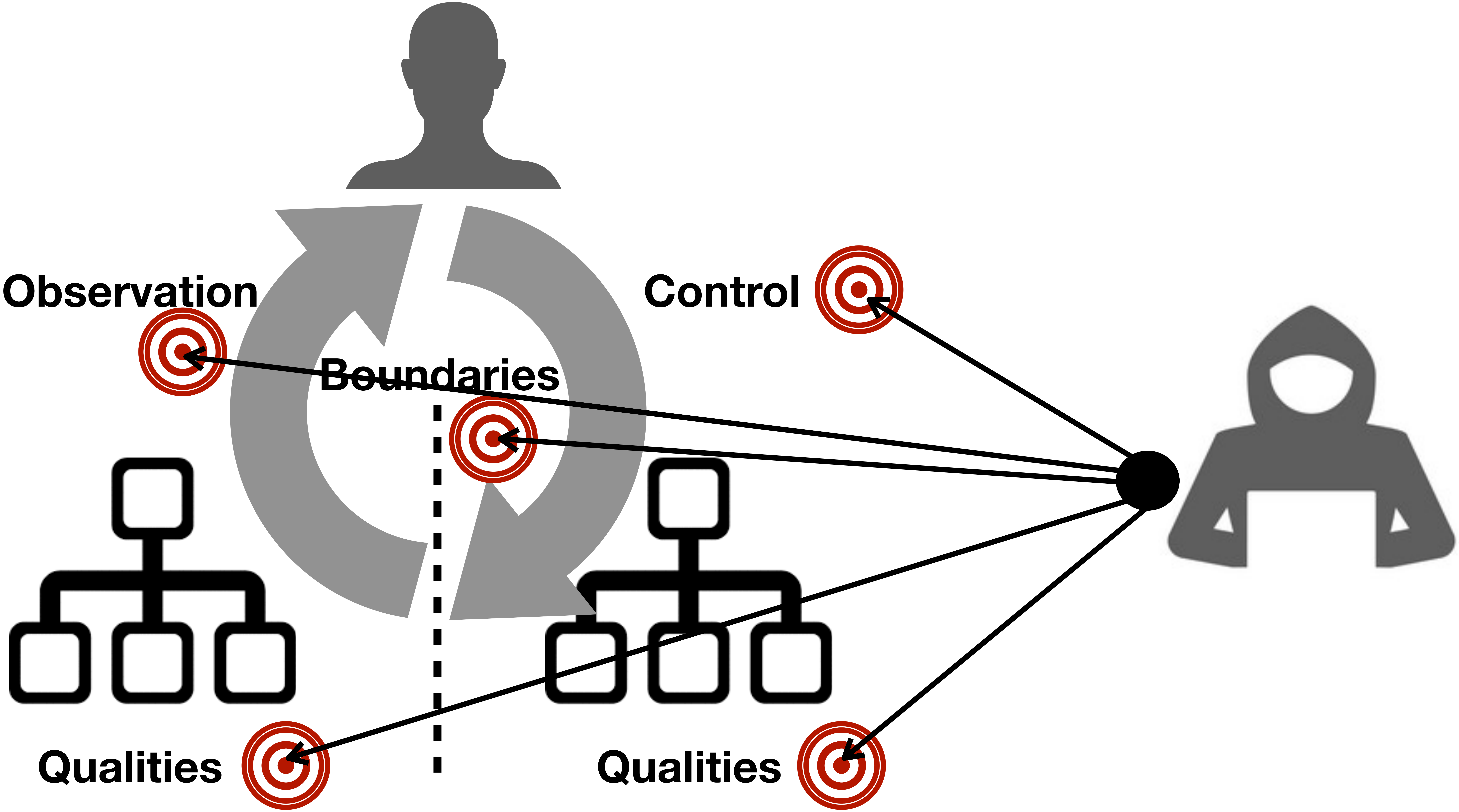
Partial-trust

New attack vectors

Multi-stakeholder

Longevity

Change



Observation

Control

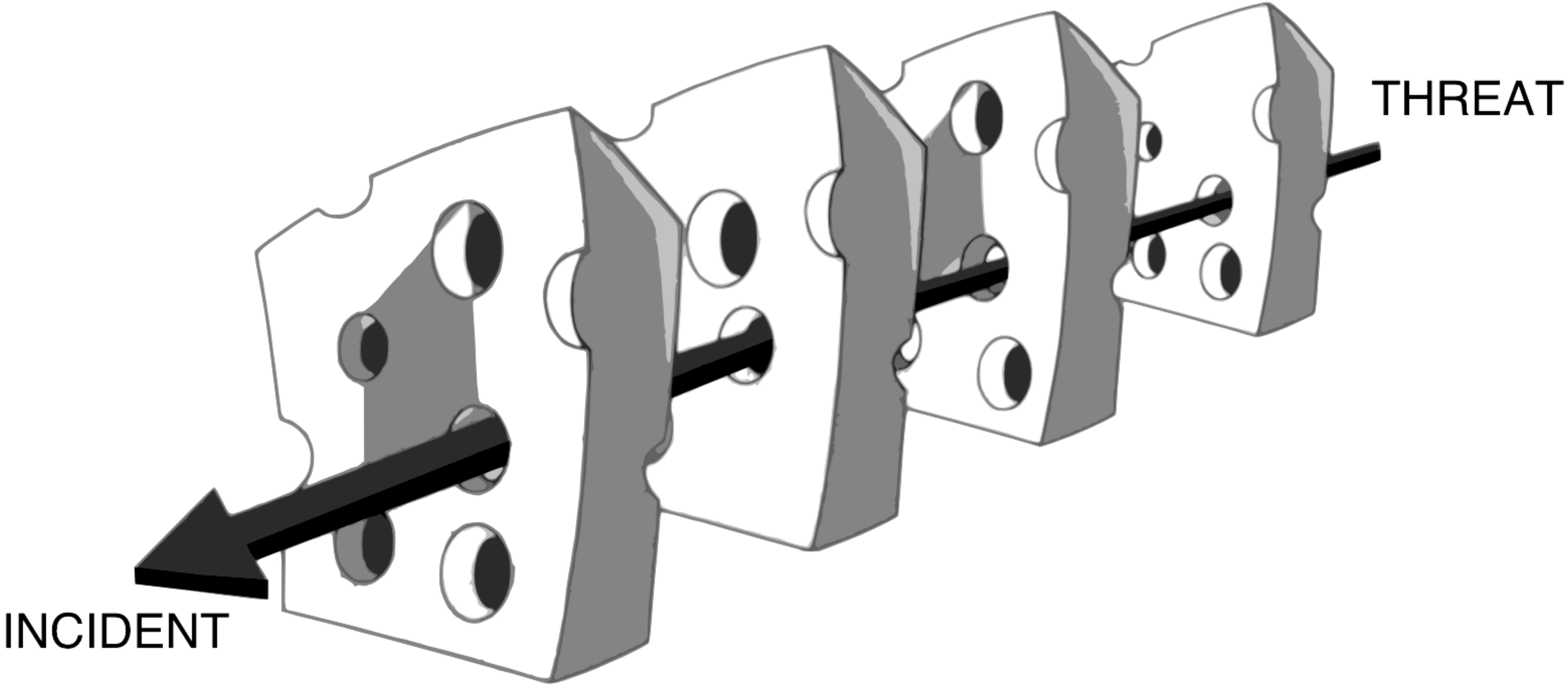
Boundaries

Qualities

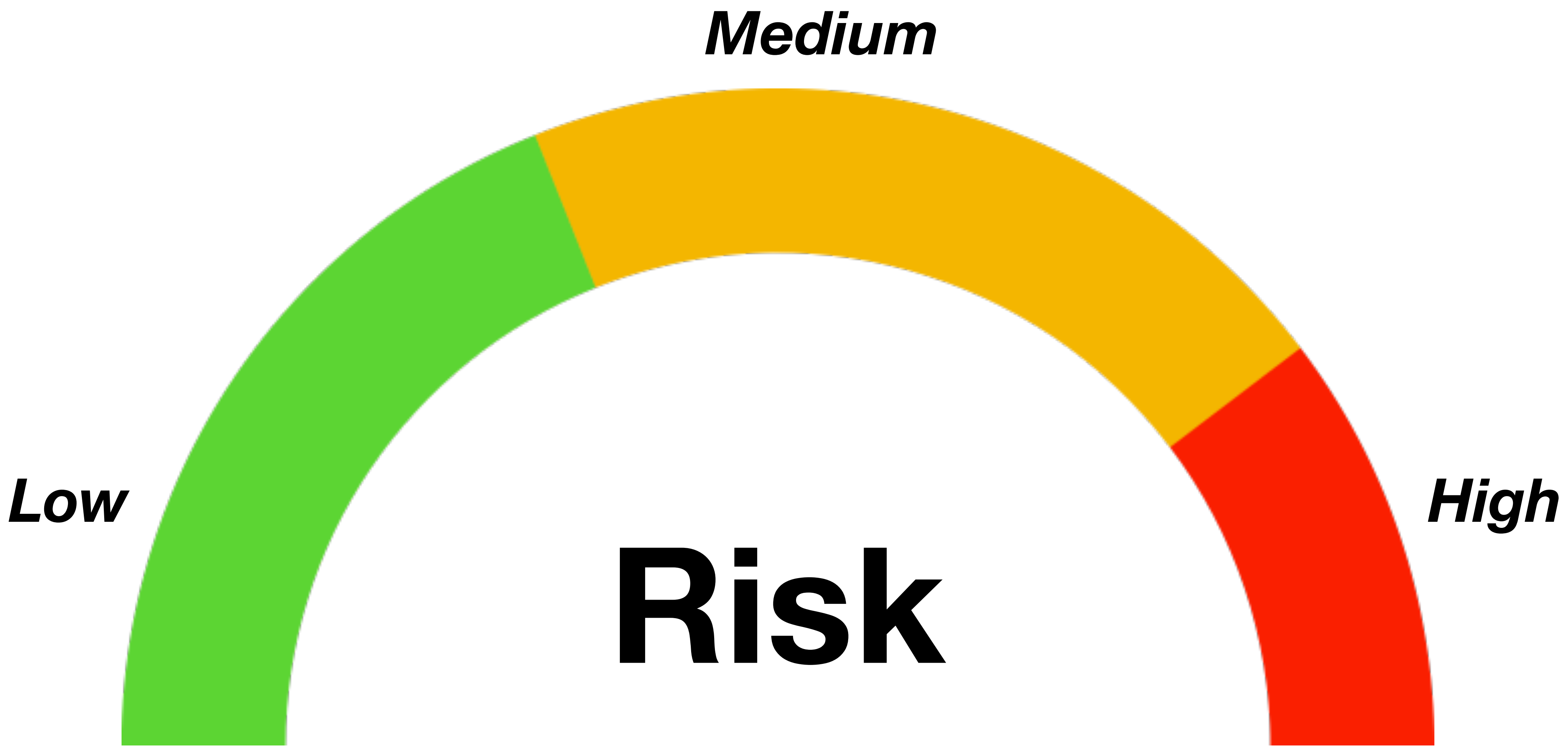
Qualities

Confidentiality
Integrity
Availability
Non-repudiation

Auditability
Safety
Resilience
...



Angela Sasse, Awais Rashid (2019). *Human Factors Knowledge Area*, Cyber Security Body of Knowledge. https://www.cybok.org/



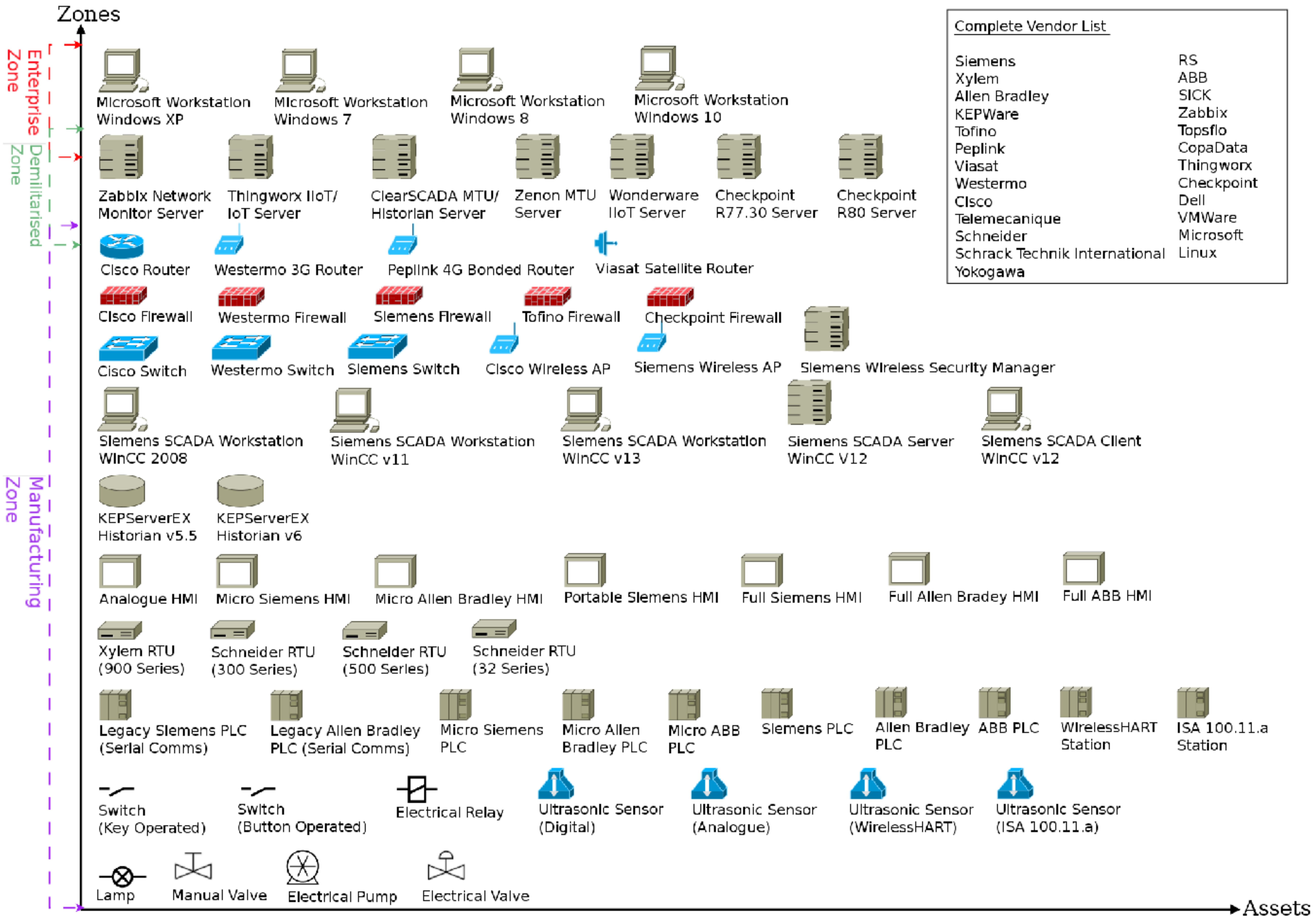
Medium

Low

High

Risk

Socio- technical



Complete Vendor List

Siemens
Xylem
Allen Bradley
KEPWare
Tofino
Peplink
Viasat
Westermo
Cisco
Telemecanique
Schneider
Schrack Technik International
Yokogawa
RS
ABB
SICK
Zabbix
Topsflo
CopaData
Thingworx
Checkpoint
Dell
VMWare
Microsoft
Linux

B. Green, A. Le, R. Antrobus, U. Roedig, D. Hutchison, A. Rashid (2017). *Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research*. Cyber Security Experimentation and Text @ USENIX Security Symposium 2017

The Bristol Cyber Security Group Testbed

- Multiple **physical** and virtual industrial **processes** each within distinct, centrally managed **field site**
- OT **vendor agnostic** design, with control equipment from **multiple** manufacturers
- Realistic corporate **OT / IT network environment**
- Real-world “**top-end**” software based SOC

J. Gardiner, B. Craggs, B. Green, A. Rashid (2019). Oops I Did it Again: Further Adventures in the Land of ICS Security Testbeds. Proc. ACM Workshop on Cyber-Physical Systems Security & Privacy, ACM Conference on Computers and Communications Security.

Realistic Physical Processes

Large scale or highly complex processes representative of multiple CNI verticals. Co-designed, specified and built with industrial input. Potential for batch and continuous running to investigate ICS vulnerabilities. Extensible where possible.

Reference Field-Sites

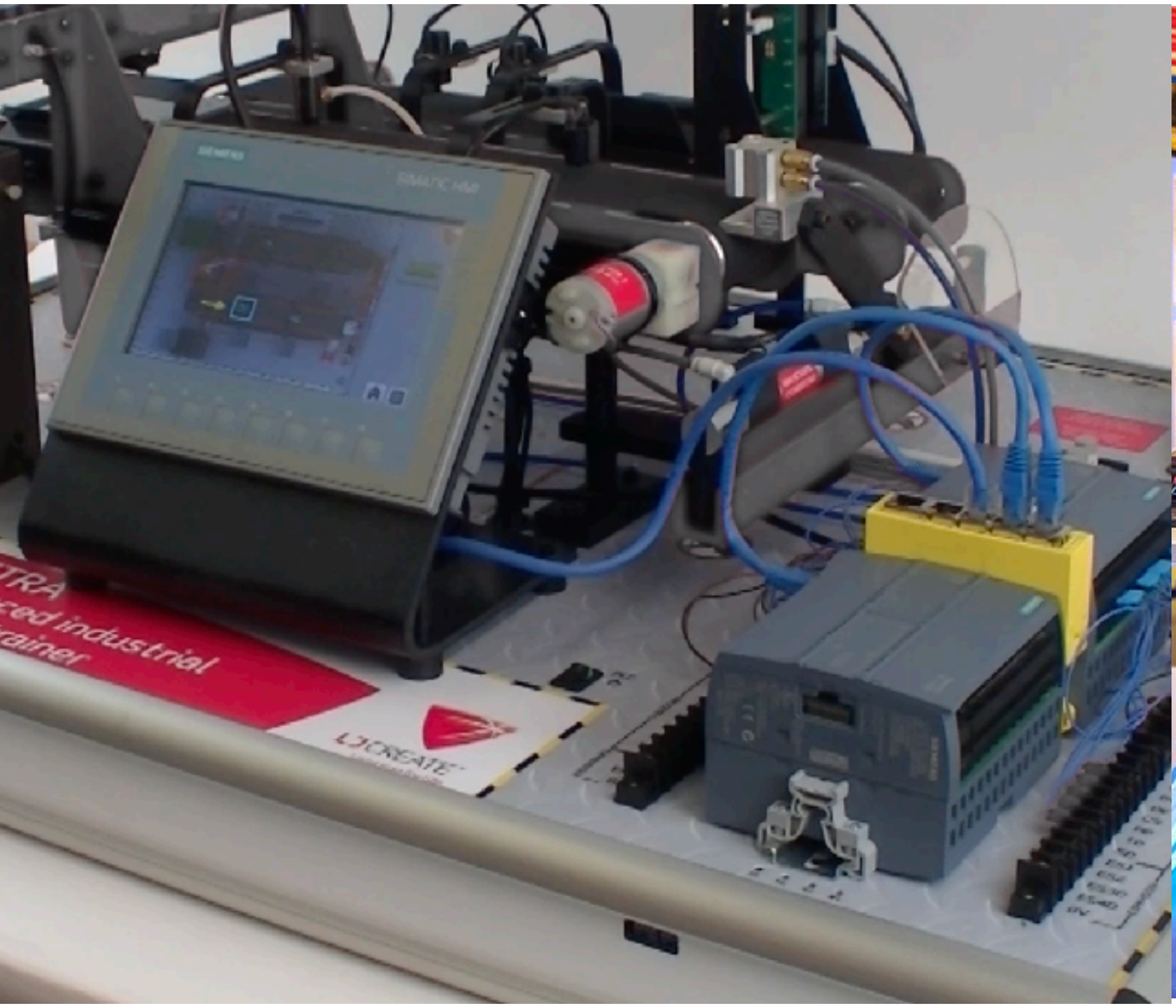
Reconfigurable control systems board built to reference architecture design, with ability to handle multiple legacy and contemporary PLC, RTU and datacomms components. One board per physical process, with discrete routed network into operational environment.

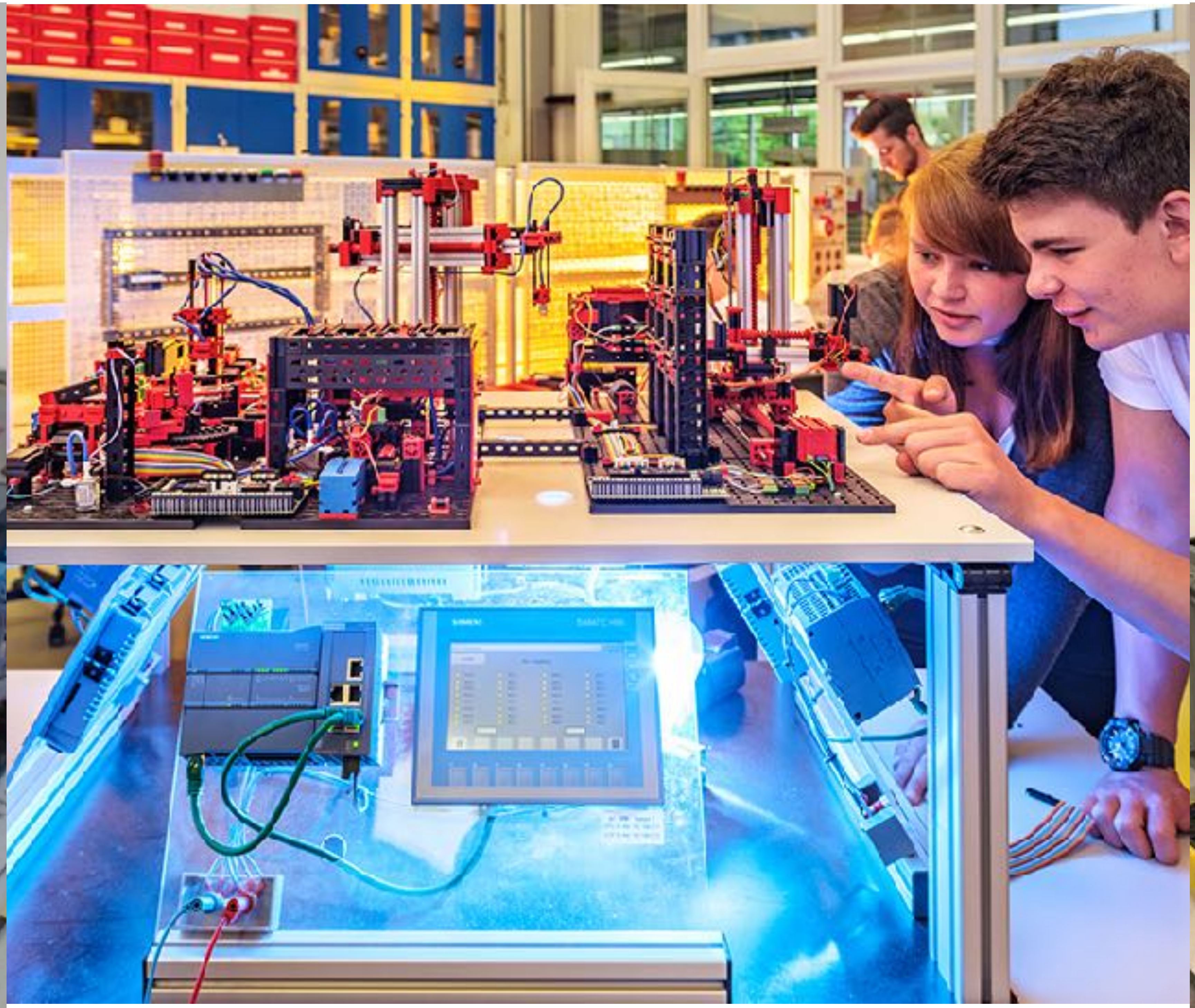
Converged Tech

Building management systems and industrial internet of things technologies for studying convergence issues with operational and informational technology environments.

Process Based

Multiple **physical** and virtual industrial **processes** each within distinct, centrally managed **field sites**





Manufacturer Agnostic

OT **vendor agnostic** design, with control equipment from **multiple** manufacturers

SIEMENS

DELTA

TOFINO SECURITY
A BELDEN BRAND

YOKOGAWA

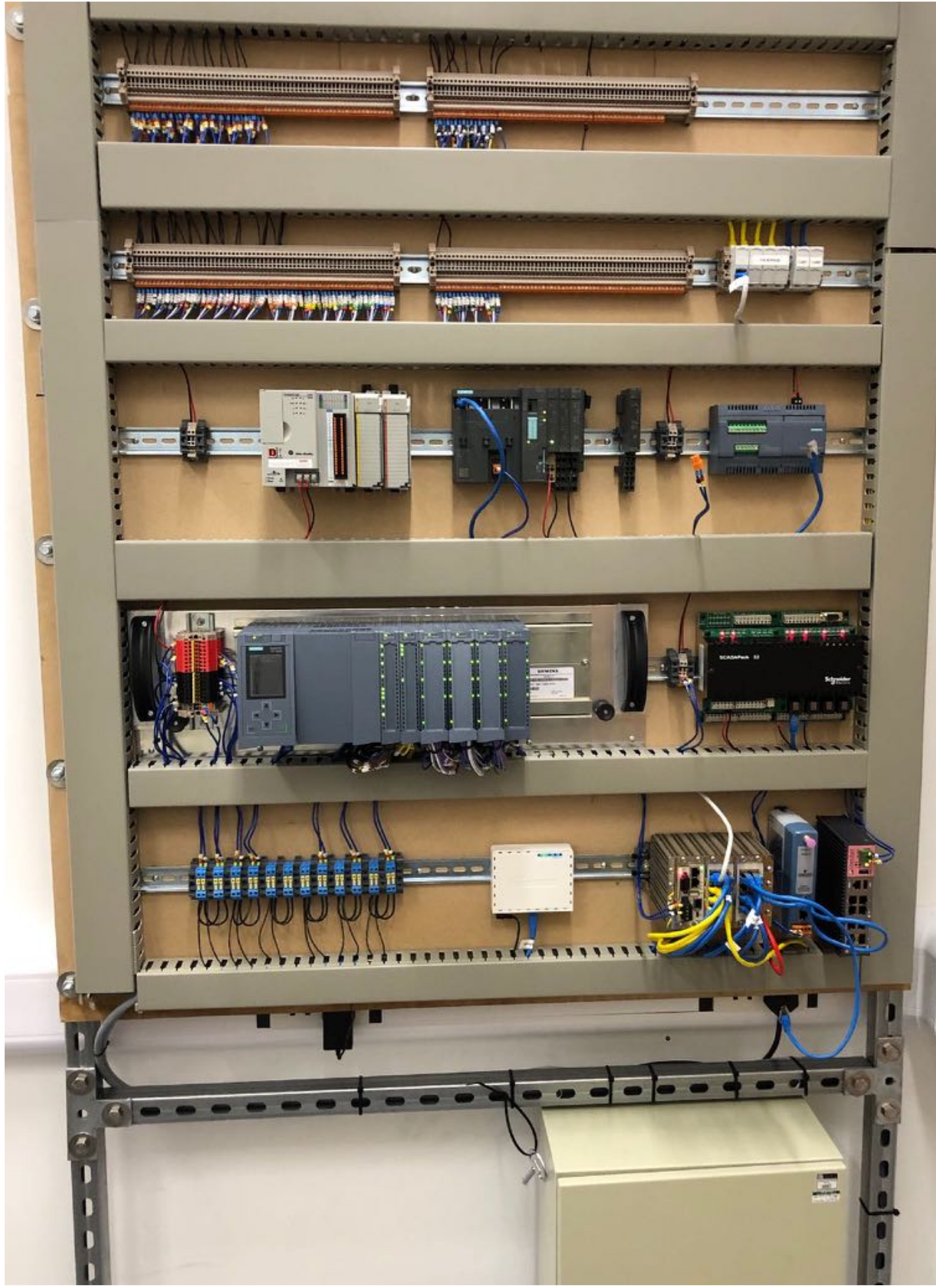
Honeywell

Check Point
SOFTWARE TECHNOLOGIES LTD.

Rockwell Automation
AB Allen-Bradley

Schneider Electric

westermo



Realistic Corporate Infrastructure

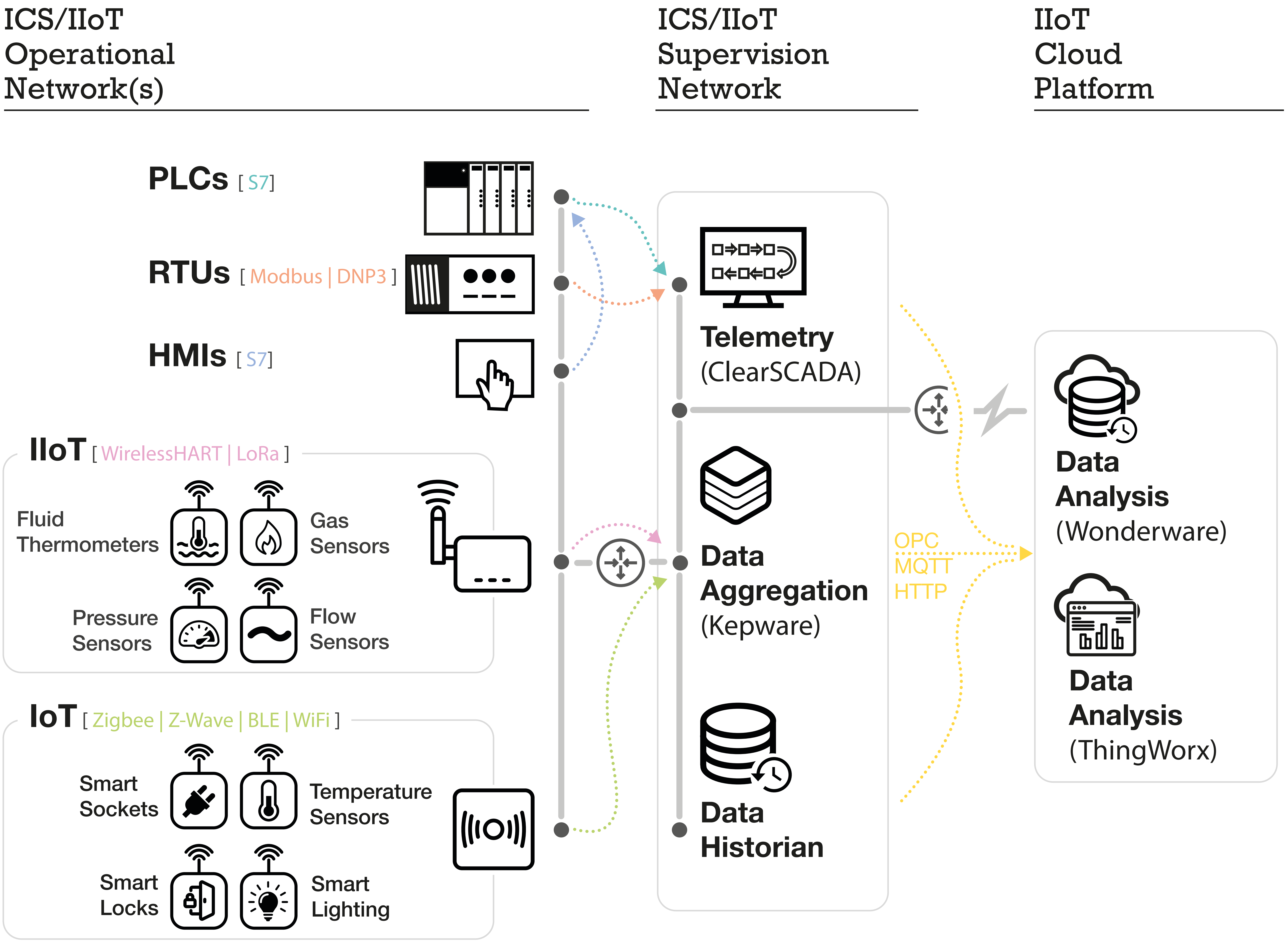
Designed upon industry knowledge, with multiple OT and IT VLANs, firewalls, boundary routers and field-sites. Secure VPN federation with partners.

CISCO DELL drobo

Wireless IIoT and IoT

To enable convergence studies we integrate industrial and deployed-consumer IoT, across a range of protocols.

Typical Converged ICS/IIOT Environment



ICS/IIoT Operational Network(s)

ICS/IIoT Supervision Network

IIoT Cloud Platform

PLCs [S7]

RTUs [Modbus | DNP3]

HMIs [S7]

IIoT [WirelessHART | LoRa]

Fluid Thermometers

Gas Sensors

Pressure Sensors

Flow Sensors

IoT [Zigbee | Z-Wave | BLE | WiFi]

Smart Sockets

Temperature Sensors

Smart Locks

Smart Lighting

Telemetry (ClearSCADA)

Data Aggregation (Kepware)

Data Historian

OPC
MQTT
HTTP

Data Analysis (Wonderware)

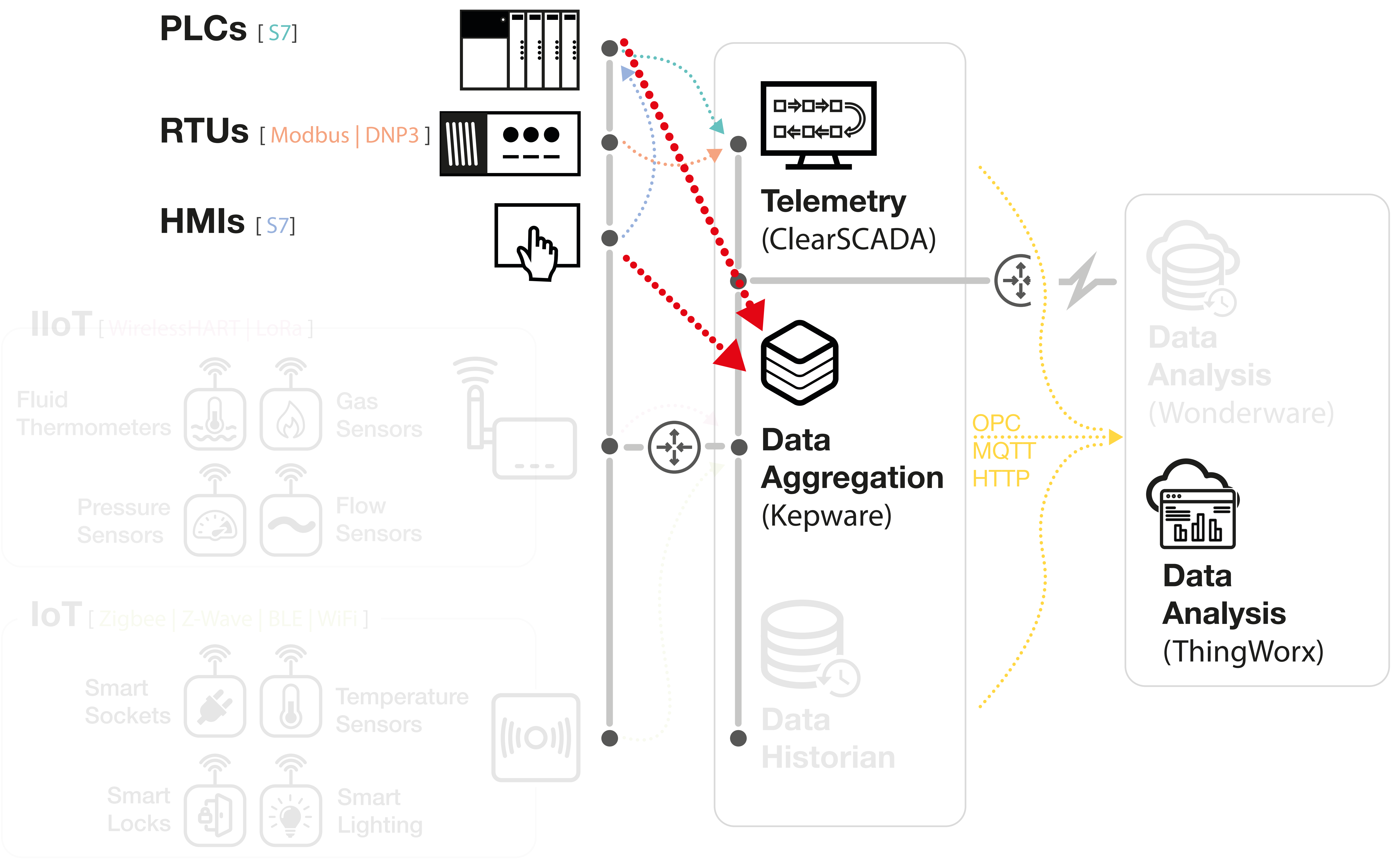
Data Analysis (ThingWorx)

Test Environment

ICS/IIoT
Operational
Network(s)

ICS/IIoT
Supervision
Network

IIoT
Cloud
Platform

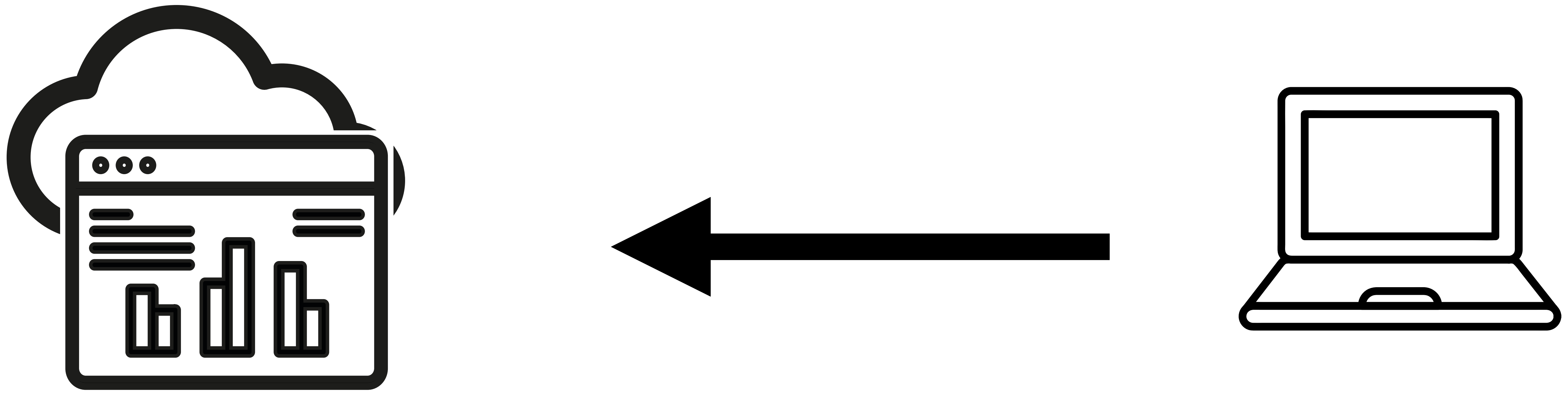


Attack Objectives

1. Compromise ThingWorx
2. Create network environment for staging attack
3. Undertake network & ICS reconnaissance
4. Mask attack
5. Manipulate process
6. Terminate process

Compromise ThingWorx

1



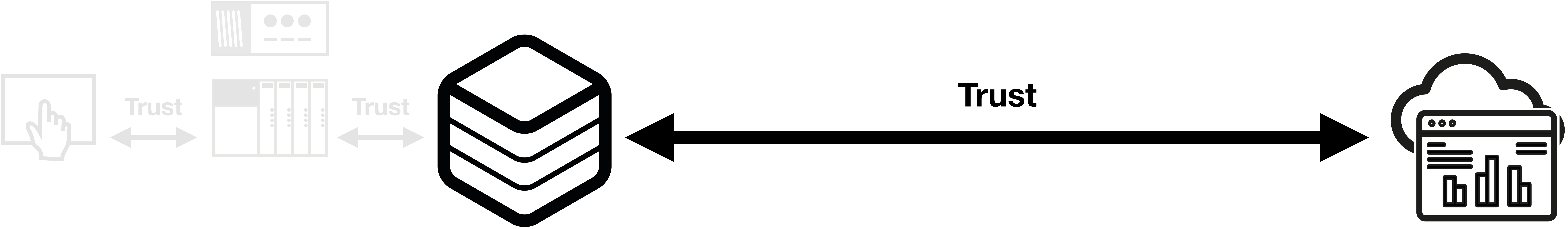
Our position is that ThingWorx has already been compromised due to it’s reliance upon Tomcat 8.5

P1 **of 2 !**

Critical	High		Medium	
CVE-2018-8014	CVE-2018-1136	CVE-2016-8745	CVE-2018-11784	CVE-2017-7674
CVE-2017-5651	CVE-2018-8034	CVE-2016-6817	CVE-2018-8037	CVE-2016-6794
	CVE-2017-12617	CVE-2016-6797	CVE-2018-1304	CVE-2016-0762
	CVE-2017-7675	CVE-2016-5018	CVE-2018-1305	
	CVE-2016-6796	CVE-2017-5664	CVE-2017-15706	

Create Network Environment

2



1 - Terminate ThingWorx

2 - Setup HTTP listener

3 - Engineer opens Kepware man .pdf

4 - Embedded exploit opens HTTP outbound request

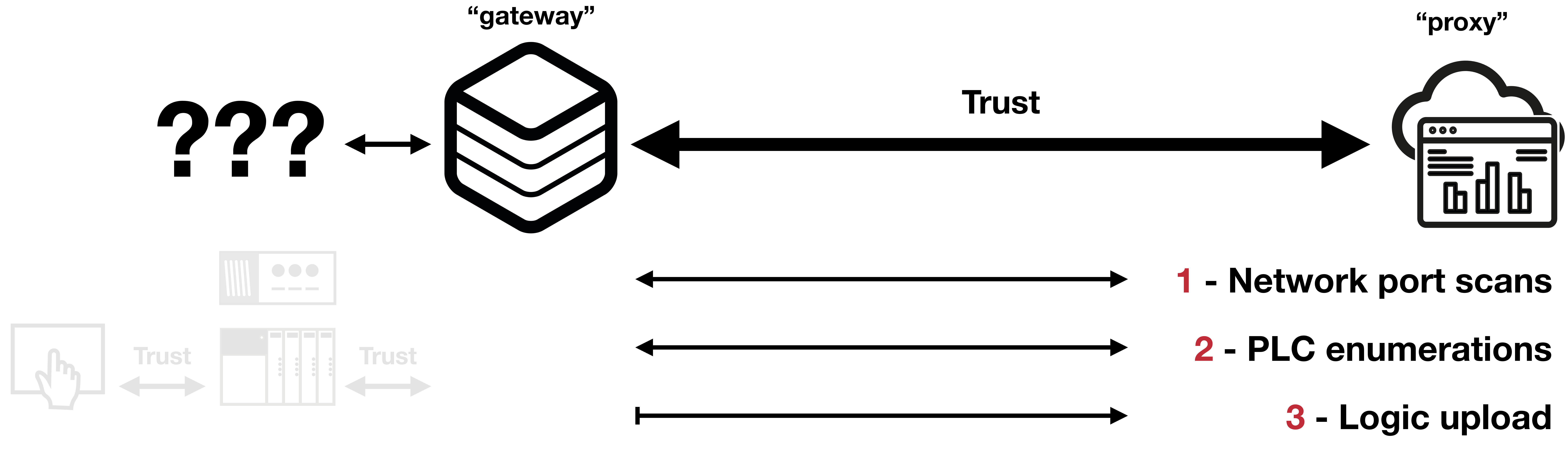
5 - HTTP session established

6 - Autoroute identifies available remote subnets

7 - Proxy setup via HTTP session

Generic Network / Specific ICS Recon

3



1 - Network port scans

2 - PLC enumerations

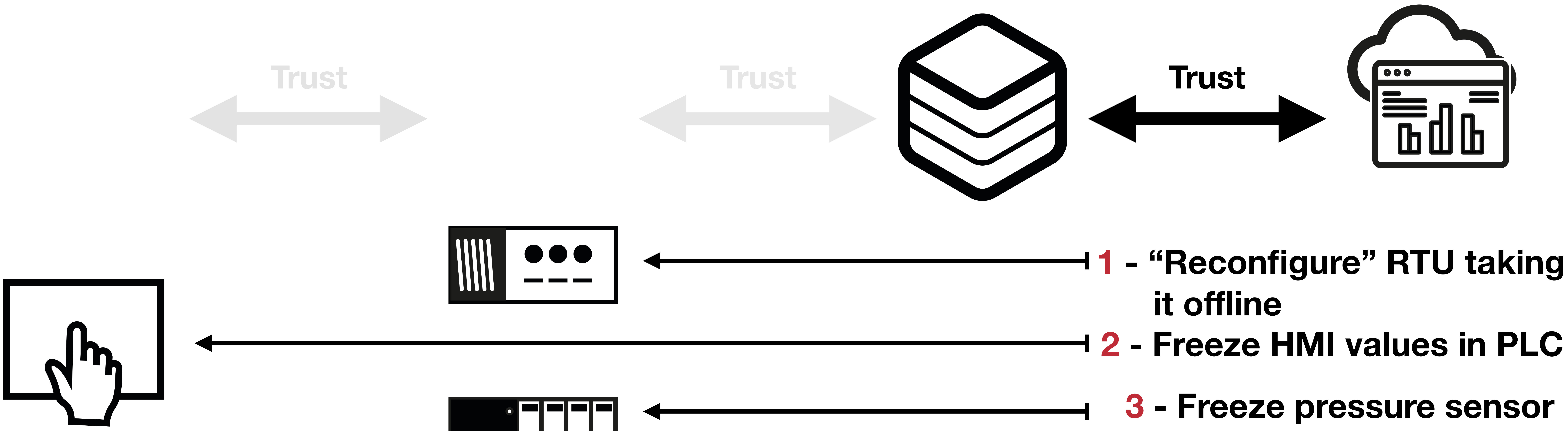
3 - Logic upload

Note: Whilst tags in PLC logic may contain descriptions reverse engineering logic is time consuming, and complex processes are hard to comprehend.

Verbose tags in ThingWorx can provide addition recon.

Mask Attack / Manipulate Process

4 5



1 - “Reconfigure” RTU taking it offline

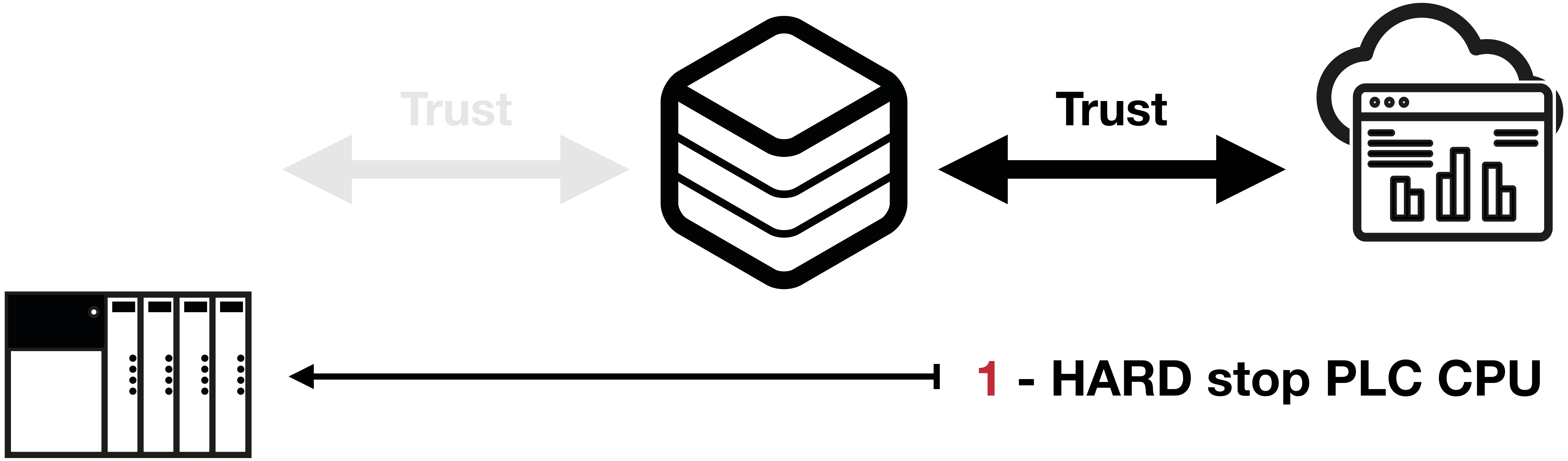
2 - Freeze HMI values in PLC

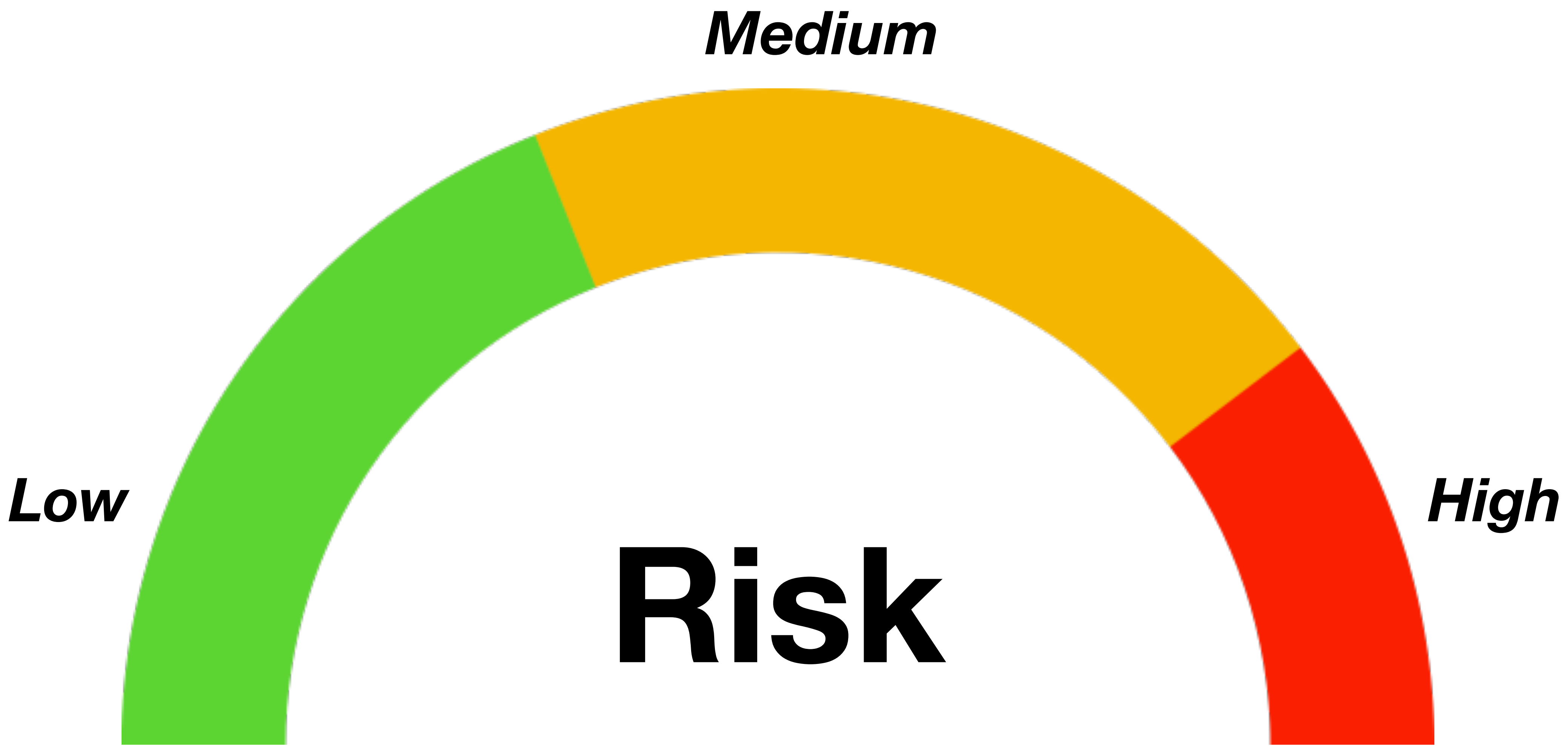
3 - Freeze pressure sensor values in PLC

4 - Push pump to run beyond safe limits

Terminate Process

6





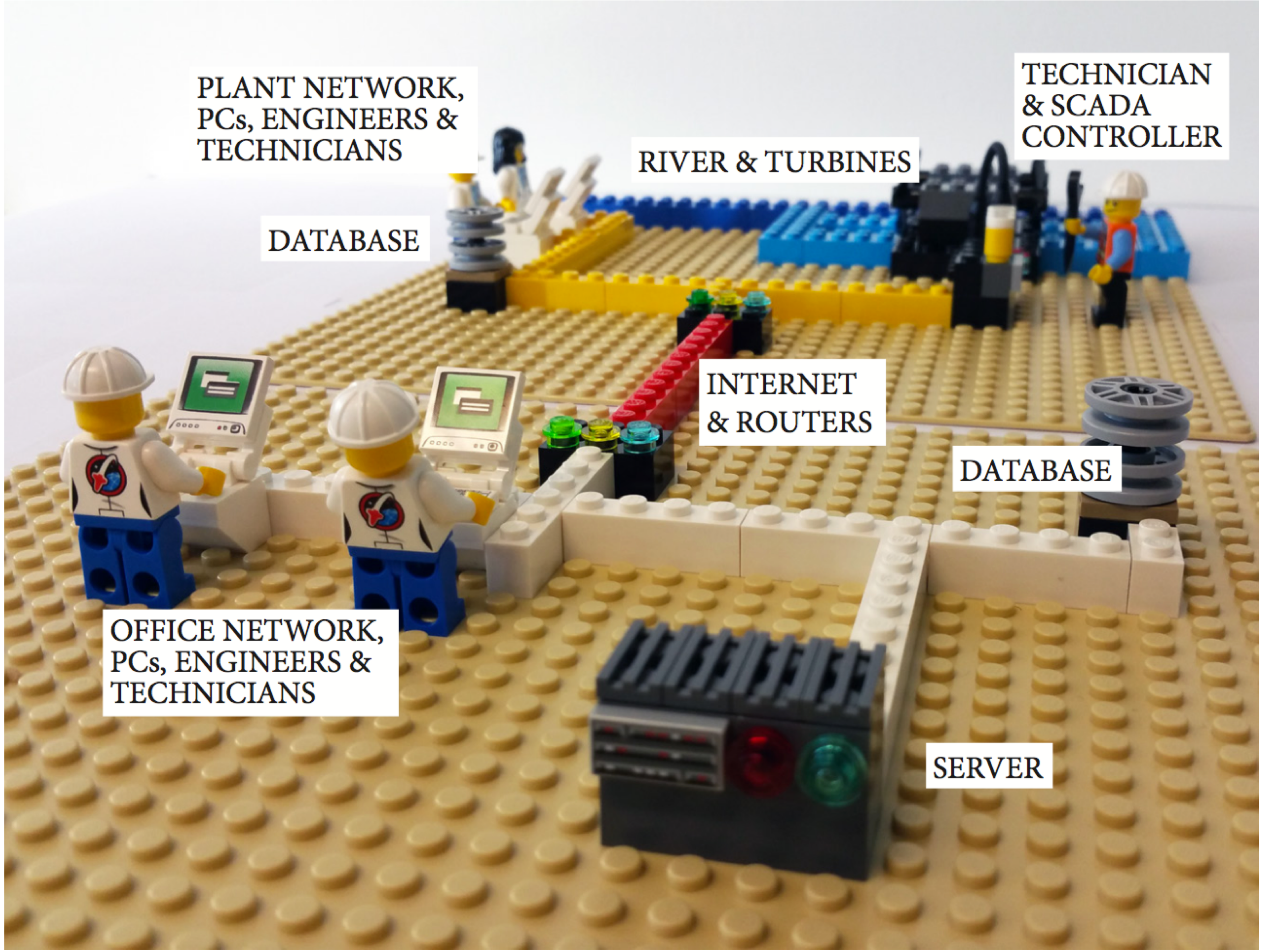
Medium

Low

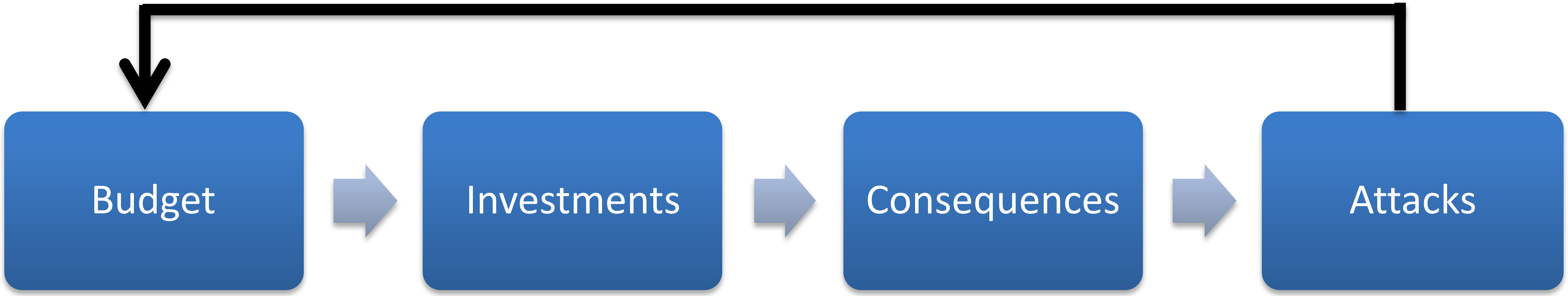
High

Risk

Socio- technical


PLANT NETWORK, PCs, ENGINEERS & TECHNICIANS
RIVER & TURBINES
TECHNICIAN & SCADA CONTROLLER
DATABASE
INTERNET & ROUTERS
DATABASE
OFFICE NETWORK, PCs, ENGINEERS & TECHNICIANS
SERVER

S. Frey, A. Rashid, P. Anthonysamy, M. Pinto-Albuquerque, S. A. Naqvi (2019). *The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game*. IEEE Trans. Software Eng. 45(5): 521-536.

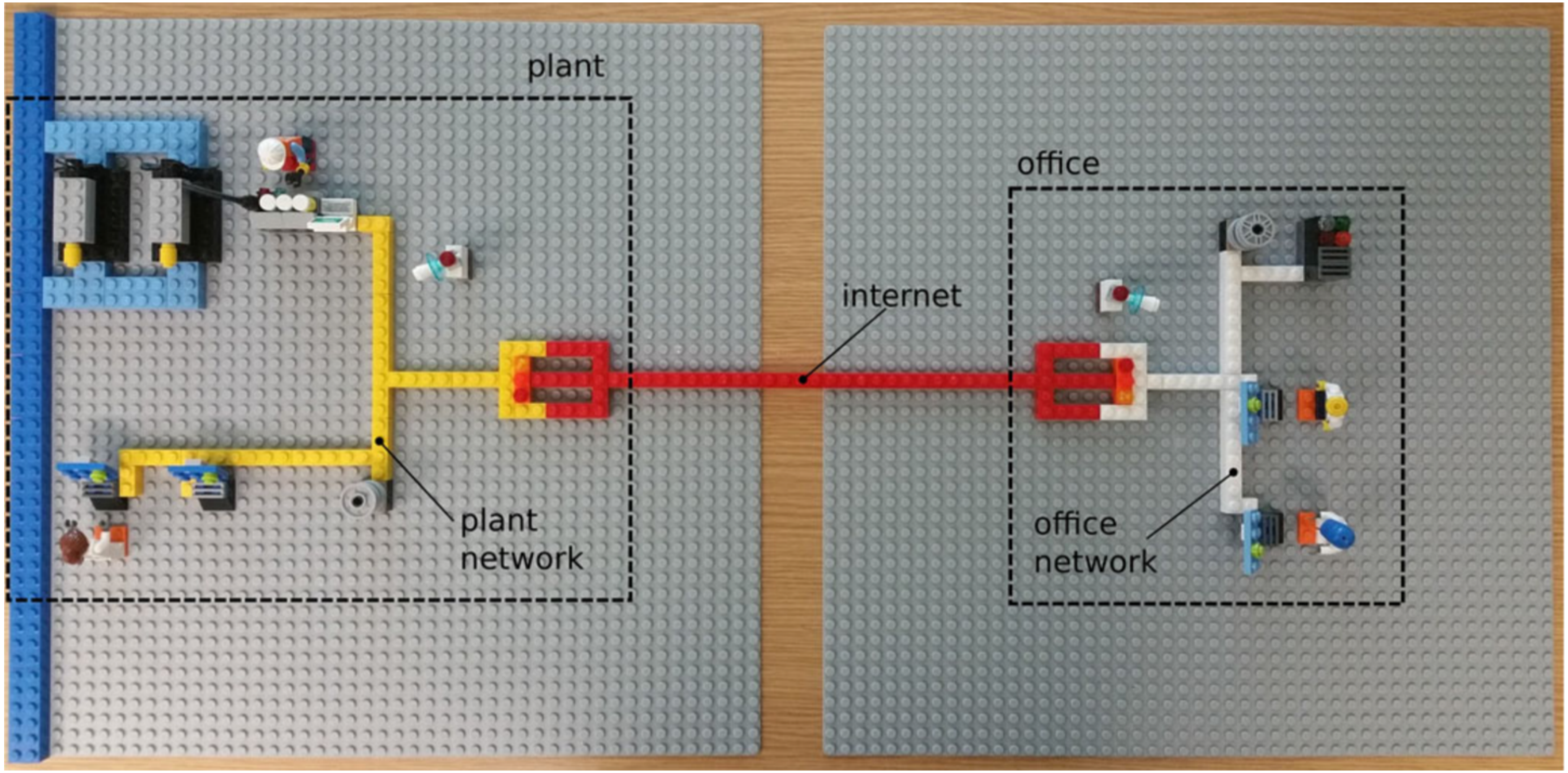


Budget

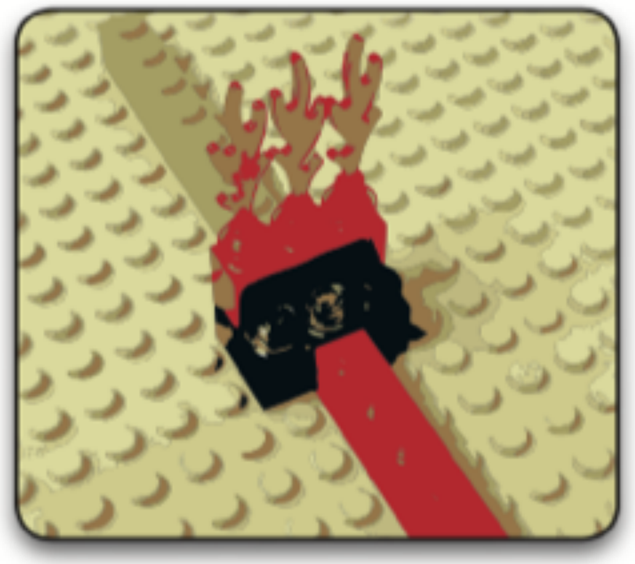
Investments

Consequences

Attacks



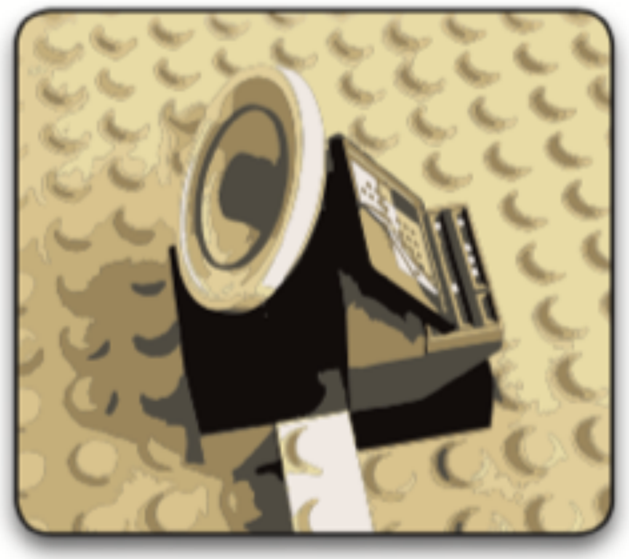
FIREWALL
(plant)



Firewall (plant) : 30k

A software and hardware solution that monitors and filters unauthorised traffic coming from the Internet to the plant network

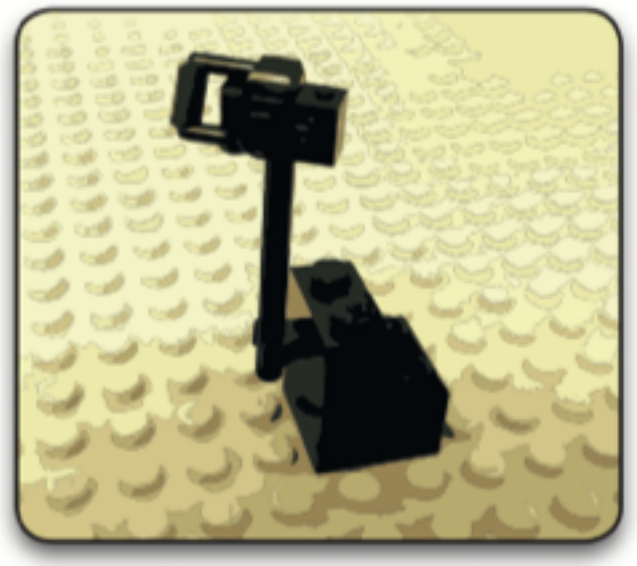
NETWORK MONITORING



Network Monitoring (plant) : 50k

This big, shiny piece of bleeding-edge technology is quite expensive but also very effective

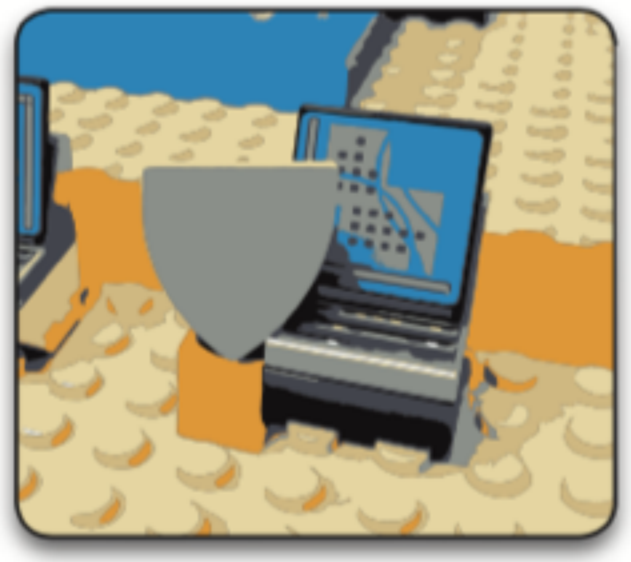
CCTV
(plant)



CCTV Surveillance : 50k

Surveillance camera and alarms that will automatically warn security guards of an intrusion

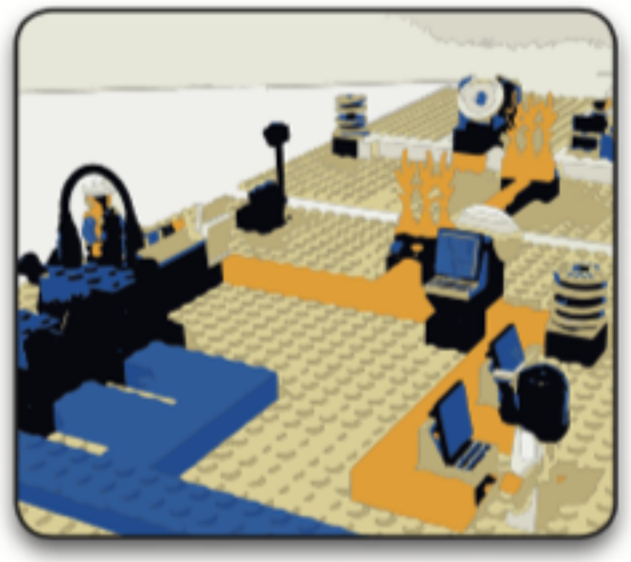
ANTIVIRUS
(plant & office)



Antivirus : 30k

A recent, decent professional anti-virus from a reputable provider

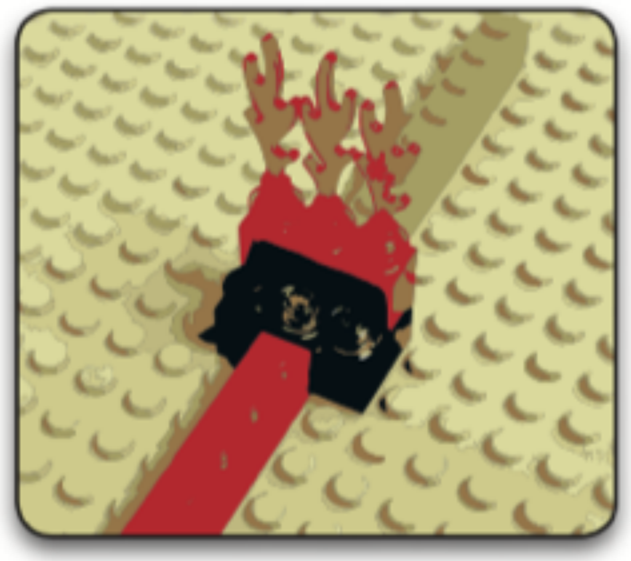
ASSET AUDIT



Asset Audit : 30k

The entire infrastructure is thoroughly assessed for vulnerabilities

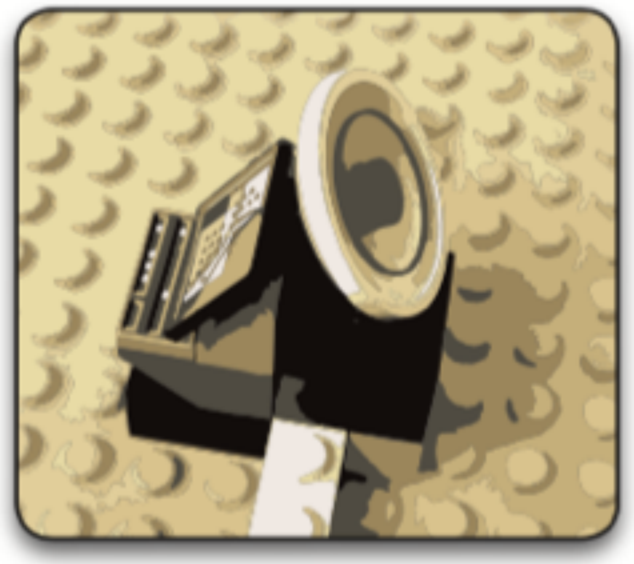
FIREWALL
(office)



Firewall (office) : 30k

A software and hardware solution that monitors and filters unauthorised traffic coming from the Internet to the office network

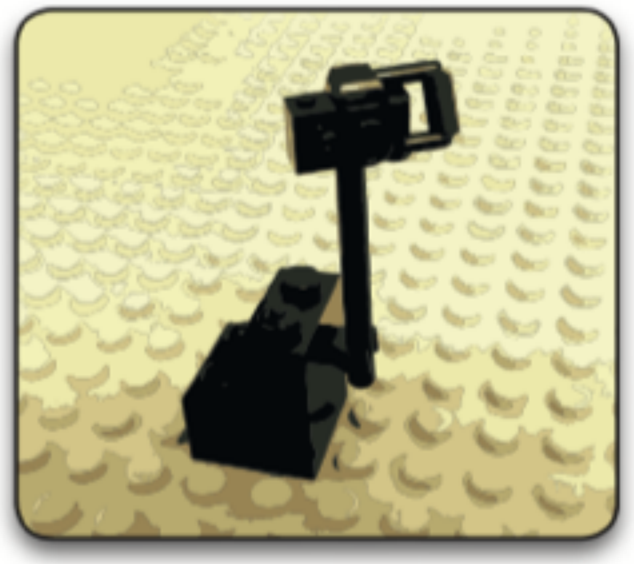
NETWORK MONITORING



Network Monitoring (office) : 50k

This big, shiny piece of bleeding-edge technology is quite expensive but also very effective

CCTV
(office)



CCTV Surveillance : 50k

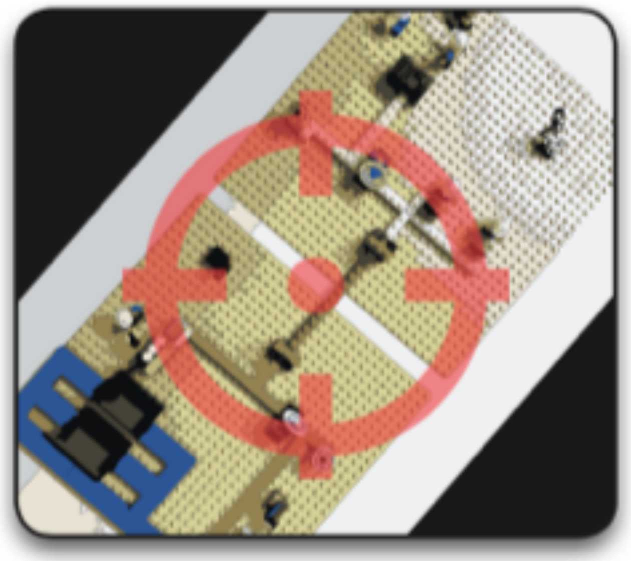
Surveillance camera and alarms that will automatically warn security guards of an intrusion

SECURITY TRAINING

Security Training : 30k

A quick yet thorough one-day formation on security essentials for all employees

THREAT ASSESSMENT

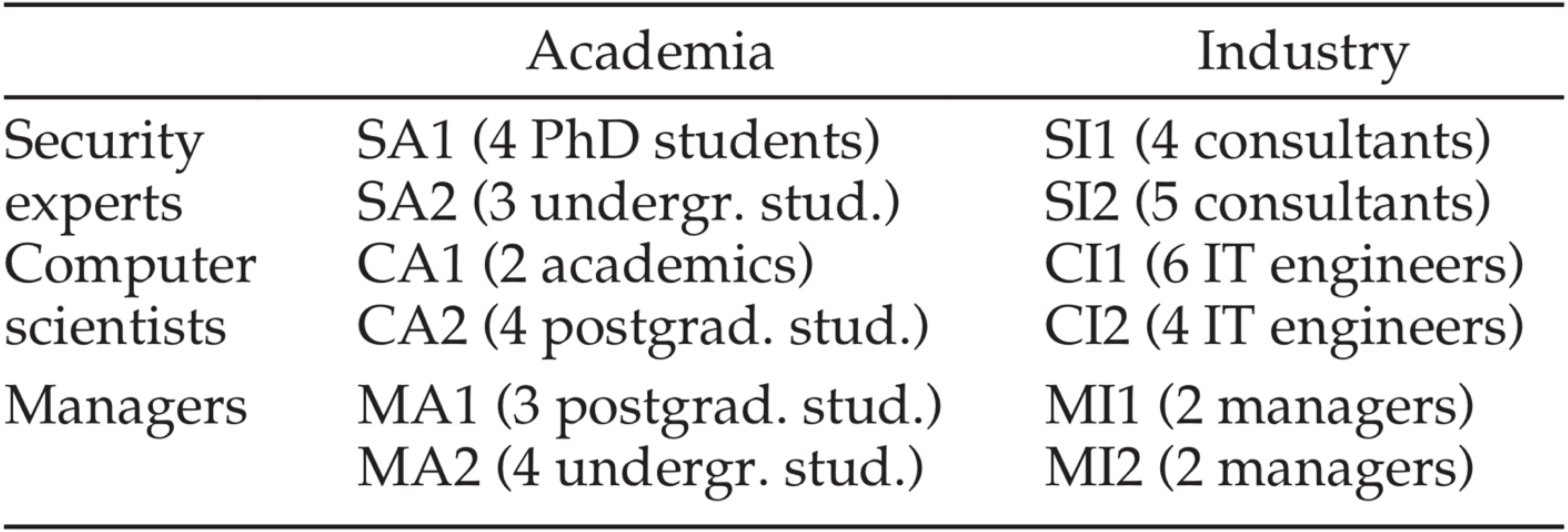


Threat Assessment : 20k

Reveals existing threats to the company, the attack vectors they use, and the possible effects of their attacks

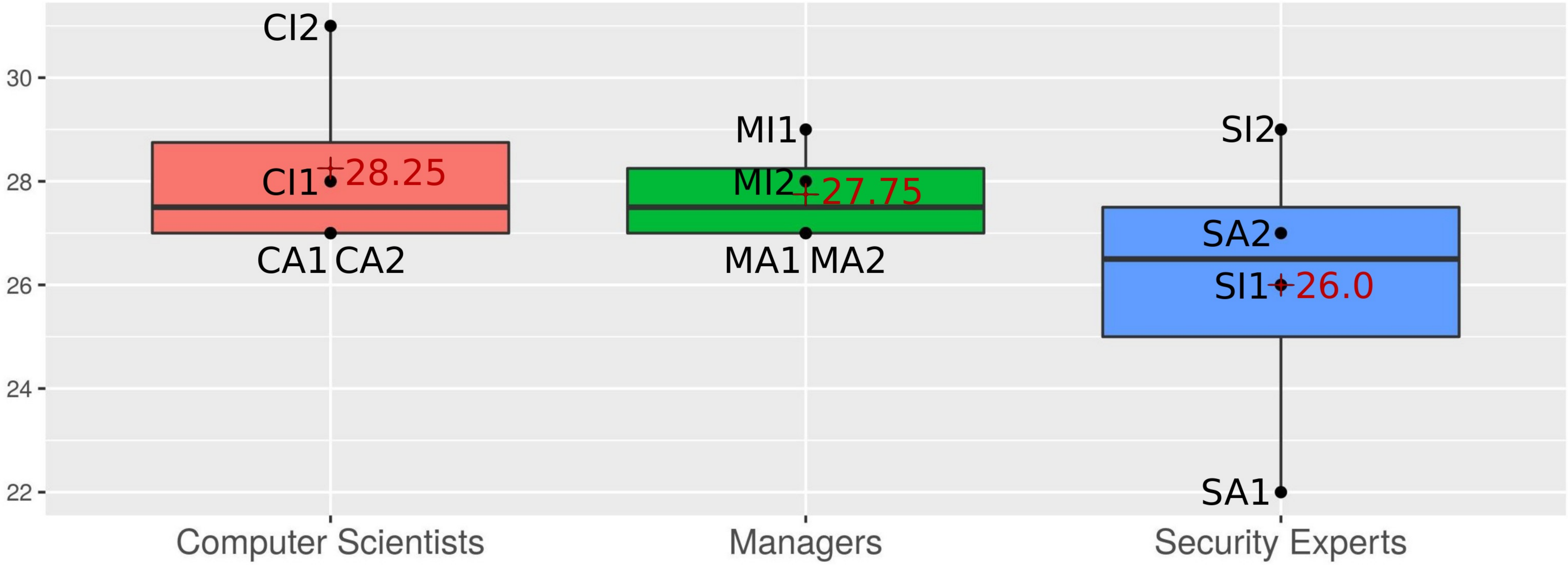
Patches - Controller ($30,000)	Upgrade to the firmware of the SCADA controller.
Patches - PCs ($30,000)	Upgrade to the operating system of all PCs (plant and offices).
Patches - Server & DBs ($30,000)	Upgrade to the operating system of the server and databases (plant and offices).
Encryption - PCs ($20,000)	Encryption for all PCs (plant and offices).
Encryption - databases ($20,000)	Encryption for all databases (plant and offices).

43 Players, divided into 12 homogeneous groups



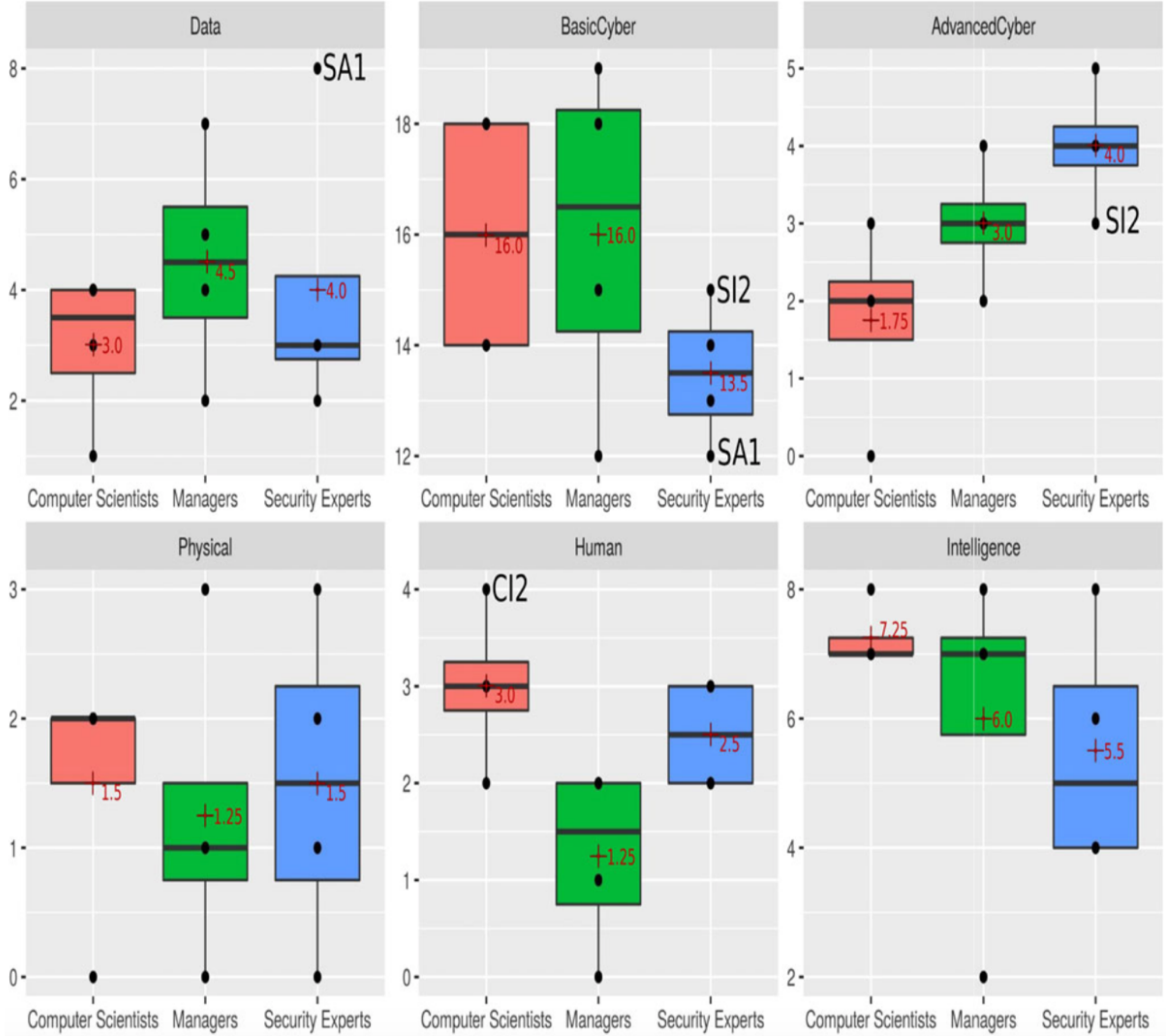
	Academia	Industry
Security experts	SA1 (4 PhD students)	SI1 (4 consultants)
	SA2 (3 undergr. stud.)	SI2 (5 consultants)
Computer scientists	CA1 (2 academics)	CI1 (6 IT engineers)
	CA2 (4 postgrad. stud.)	CI2 (4 IT engineers)
Managers	MA1 (3 postgrad. stud.)	MI1 (2 managers)
	MA2 (4 undergr. stud.)	MI2 (2 managers)

The best players are?



“We are security experts, we don’t need a threat assessment.” *Team SA1*

“You told us what we already knew.” *Team SI1*


Data
BasicCyber
AdvancedCyber
Physical
Human
Intelligence
SA1
3.0
4.5
4.0
16.0
16.0
SI2
13.5
SA1
4.0
SI2
3.0
1.75
1.5
1.25
1.5
CI2
3.0
1.25
2.5
7.25
6.0
5.5
Computer Scientists
Managers
Security Experts

Security Experts	+ +	Advanced cyber protection
	− −	Basic cyber protection
	− −	Intelligence gathering
Computer Scientists	+ +	Intelligence gathering
	+ +	Human factors
	− −	Advanced cyber protection
	− −	Data protection
Managers	+ +	Basic cyber protection
	+ +	Advanced cyber protection
	+ +	Data protection
	− −	Human factors

Procedure-driven

“We should start with an asset audit, then we can know what we are protecting and invest accordingly.”

Experience-driven

“I have never seen an IT infrastructure without a firewall.”, “Remember the news last week? They got owned by a phishing email, we should care about it.”

Scenario-driven

“What if someone got access to our database? We need to encrypt it.”

Intuition-driven

“I like the antivirus.”

Security Experts

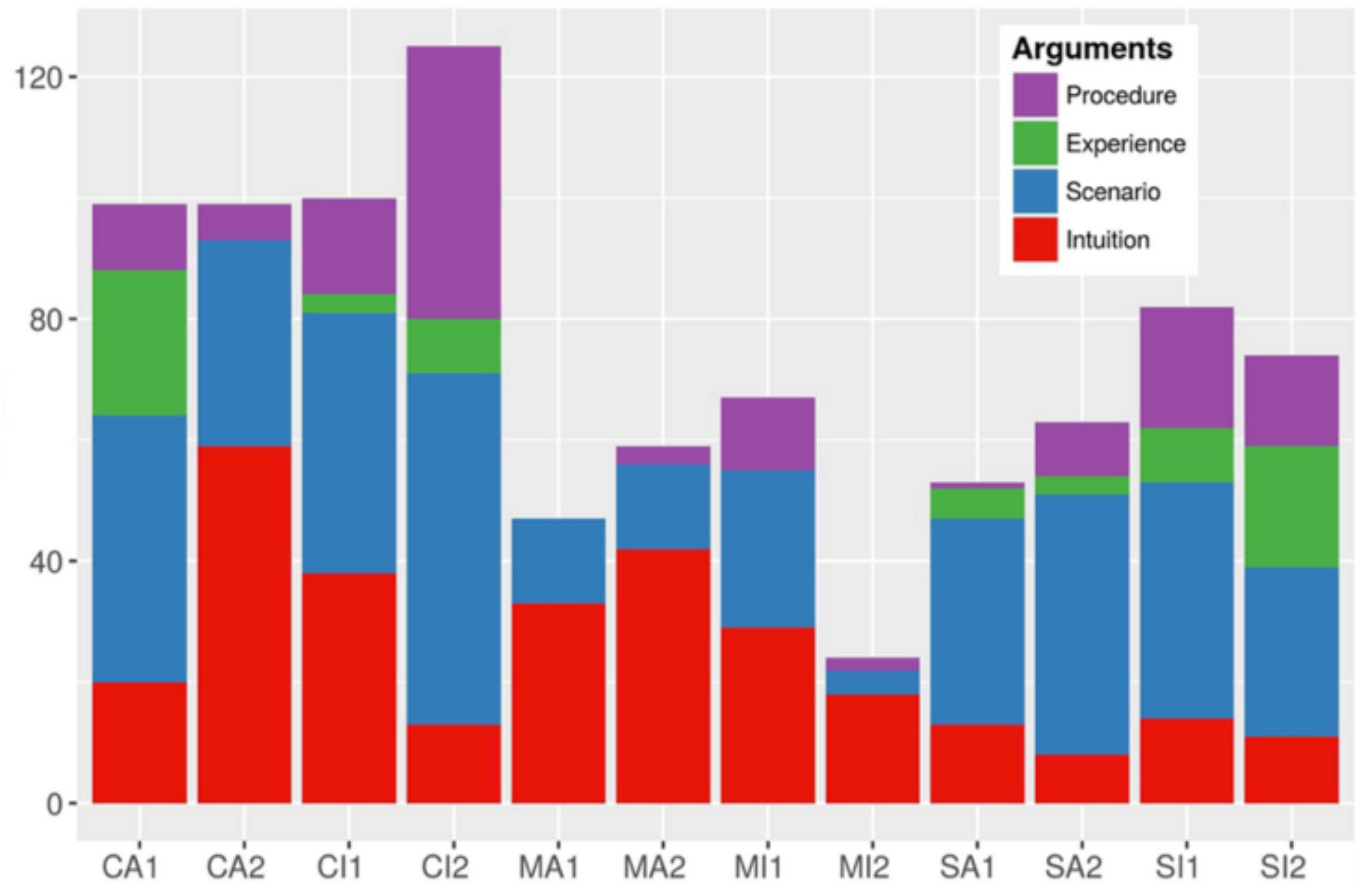
Scenario-driven
High confidence

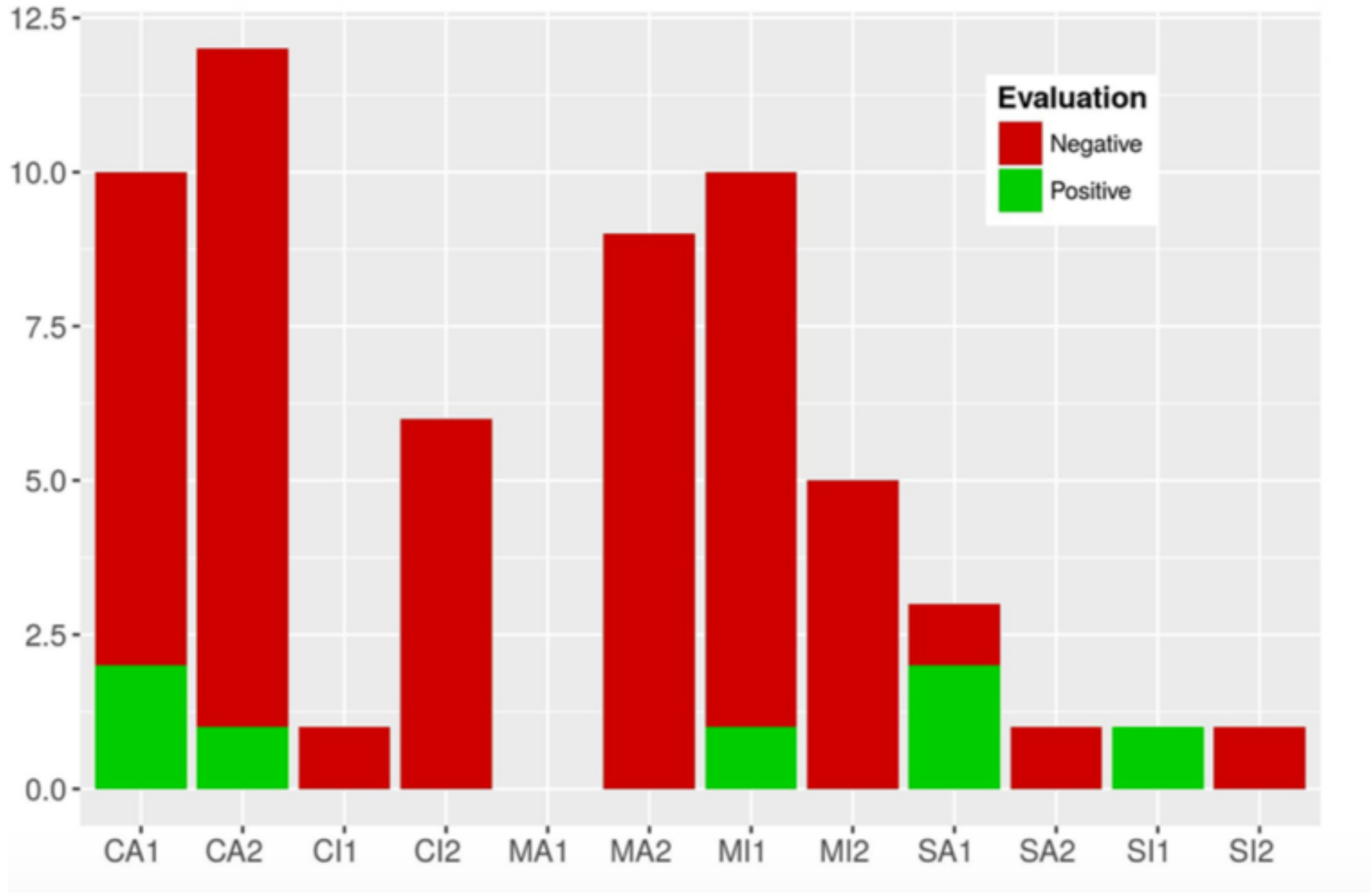
Managers

Intuition-driven
Low volume
Low confidence

Computer Scientists

Diverse
Higher volume
Low confidence





Balance is key

The Beginner’s Syndrome

A little knowledge is a dangerous thing

Beware of the champion!

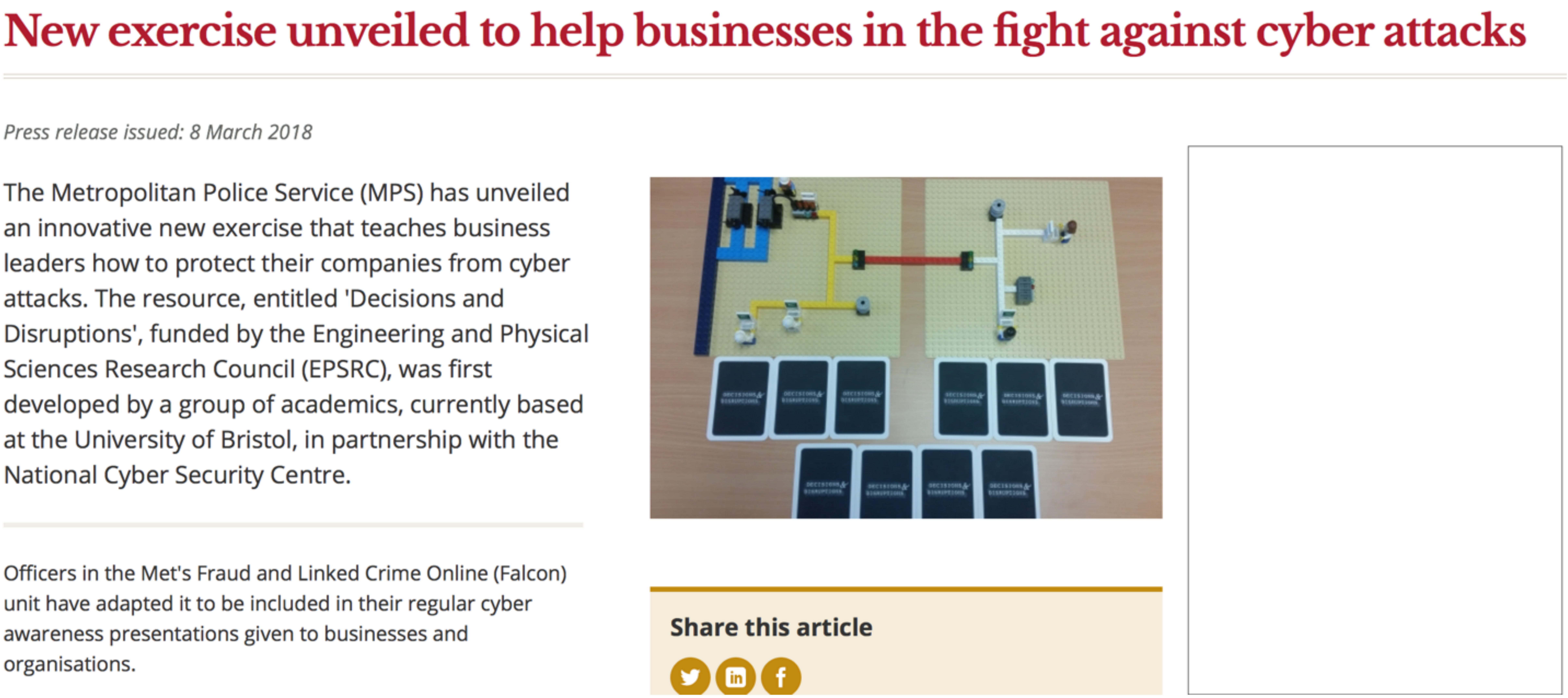
For better or worse

The “tunnel vision” syndrome

“This company’s data has little value: you could publish it all.”

“I don’t feel the encryption is any priority even though there has been a data breach.”

www.decisions-disruptions.org

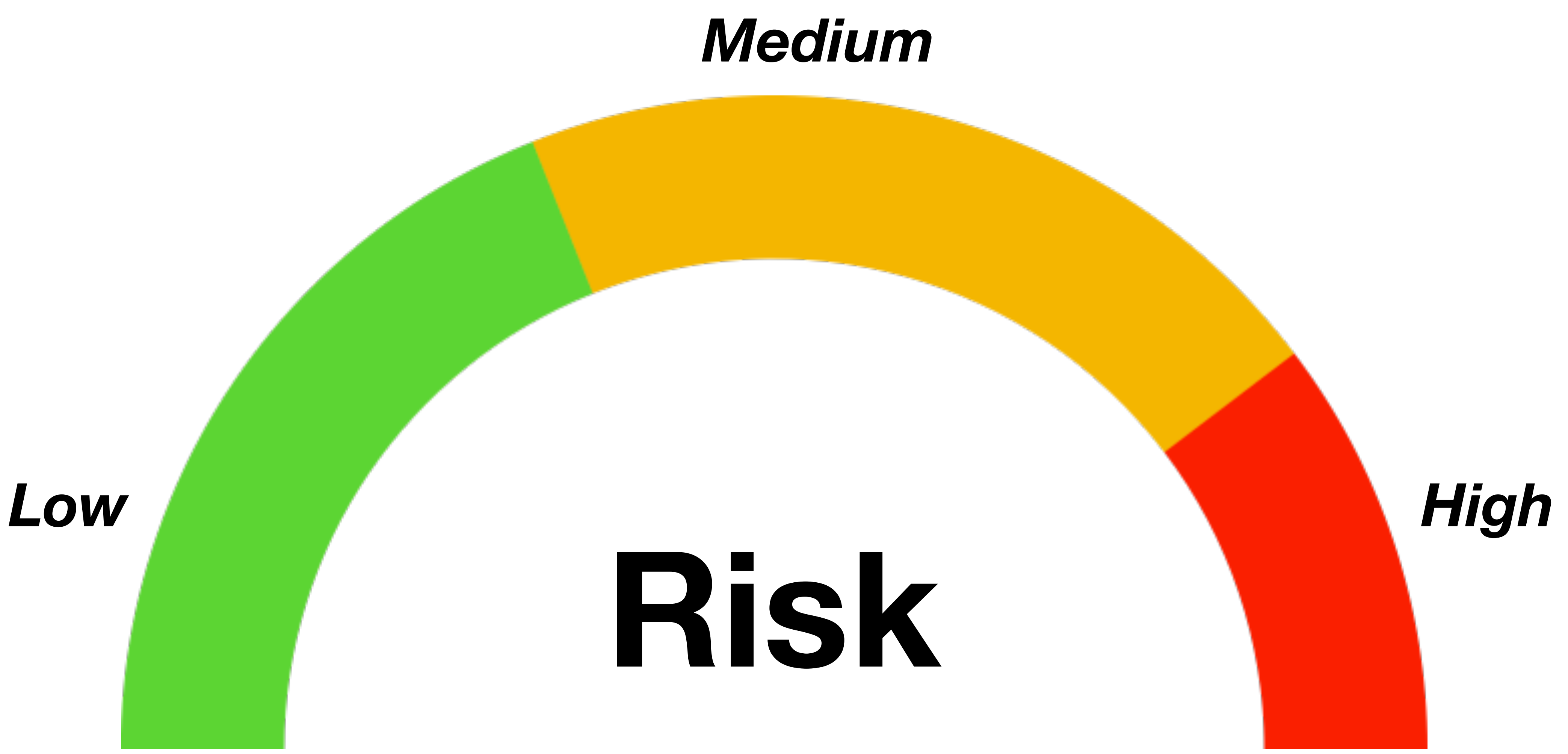


New exercise unveiled to help businesses in the fight against cyber attacks

Press release issued: 8 March 2018

The Metropolitan Police Service (MPS) has unveiled an innovative new exercise that teaches business leaders how to protect their companies from cyber attacks. The resource, entitled 'Decisions and Disruptions', funded by the Engineering and Physical Sciences Research Council (EPSRC), was first developed by a group of academics, currently based at the University of Bristol, in partnership with the National Cyber Security Centre.

Officers in the Met's Fraud and Linked Crime Online (Falcon) unit have adapted it to be included in their regular cyber awareness presentations given to businesses and organisations.



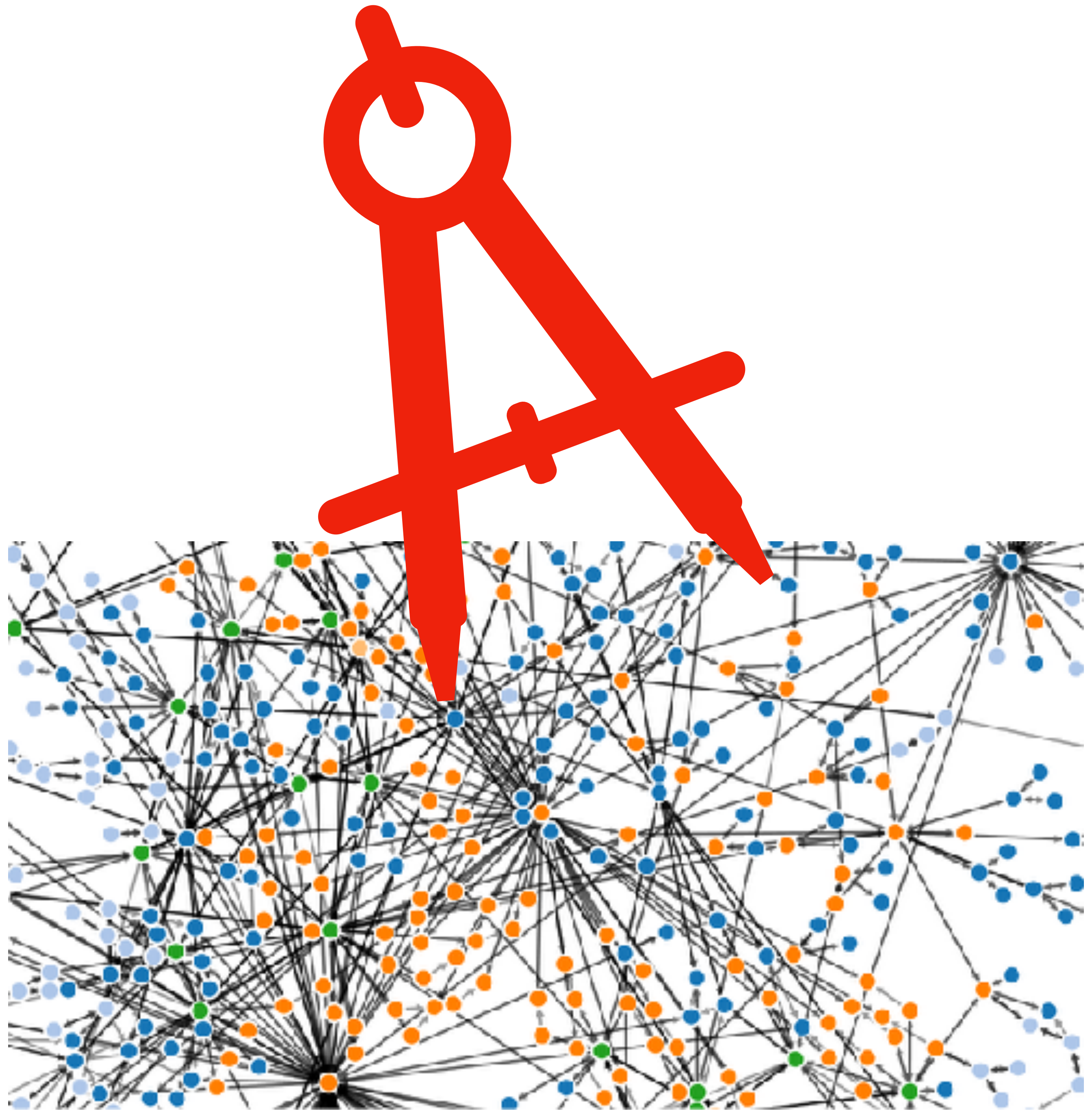
Medium

Low

High

Risk

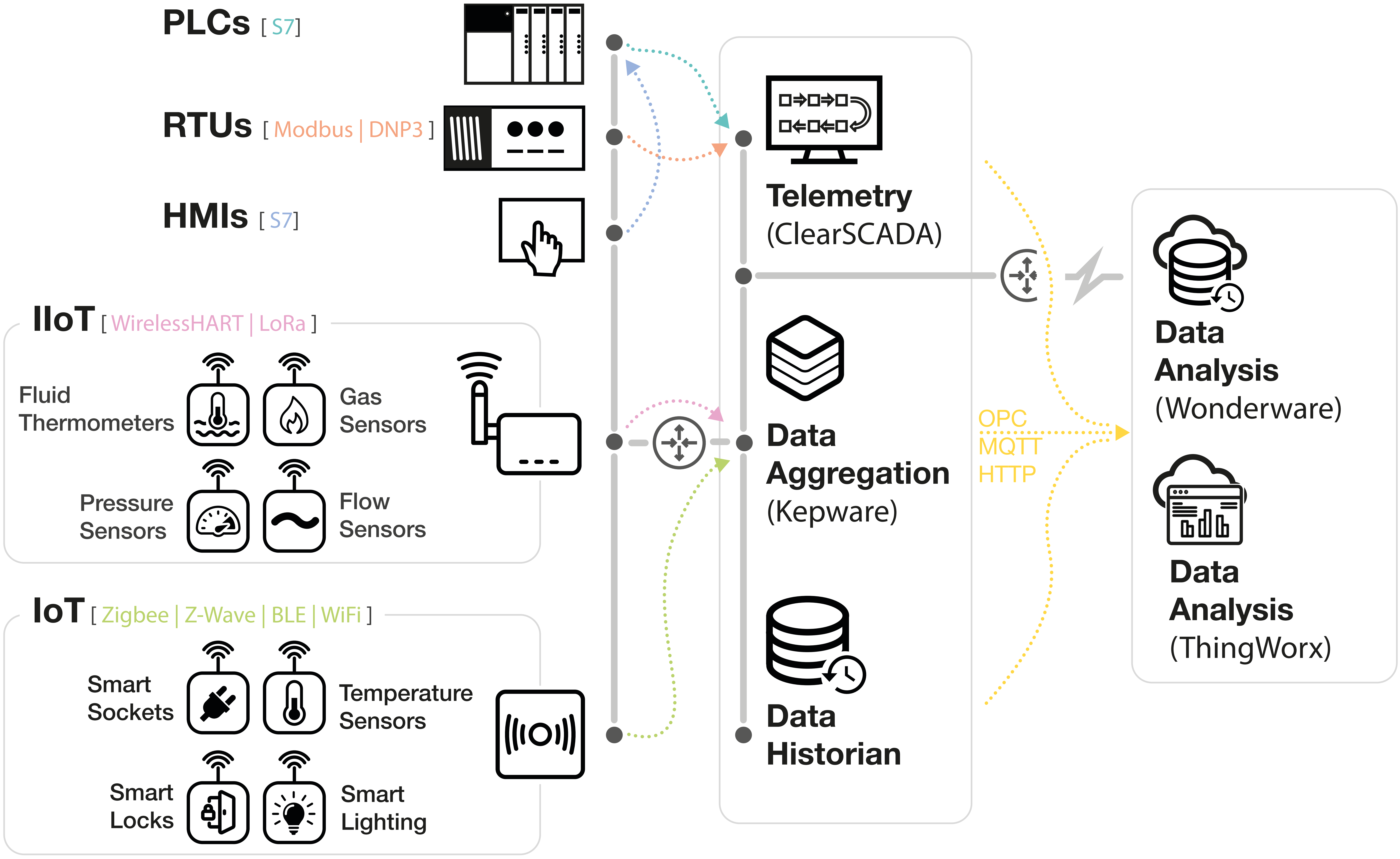
Socio- technical



ICS/IIoT Operational Network(s)

ICS/IIoT Supervision Network

IIoT Cloud Platform



PLCs [S7]

RTUs [Modbus | DNP3]

HMIs [S7]

IIoT [WirelessHART | LoRa]

Fluid Thermometers

Gas Sensors

Pressure Sensors

Flow Sensors

IoT [Zigbee | Z-Wave | BLE | WiFi]

Smart Sockets

Temperature Sensors

Smart Locks

Smart Lighting

Telemetry (ClearSCADA)

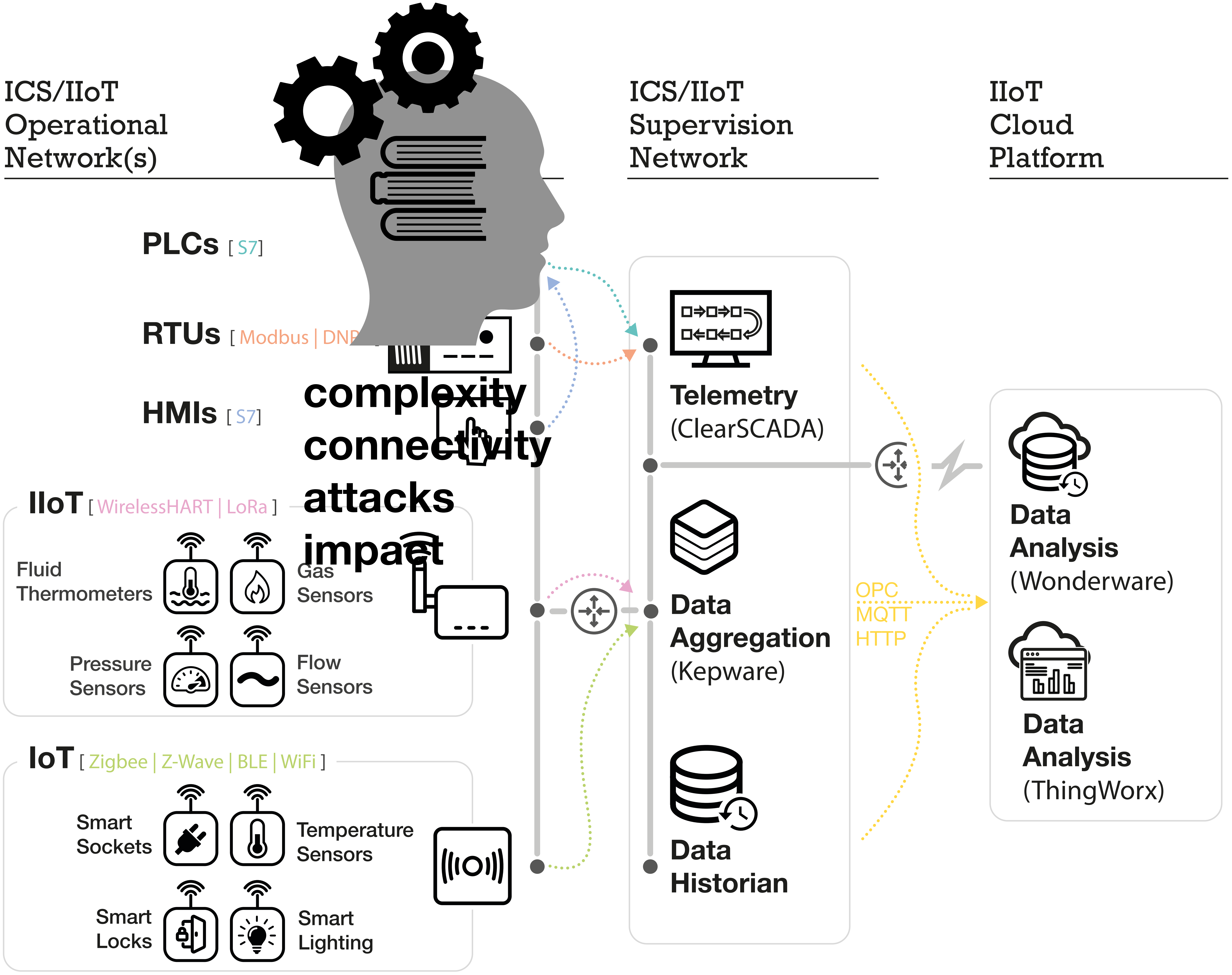
Data Aggregation (Kepware)

Data Historian

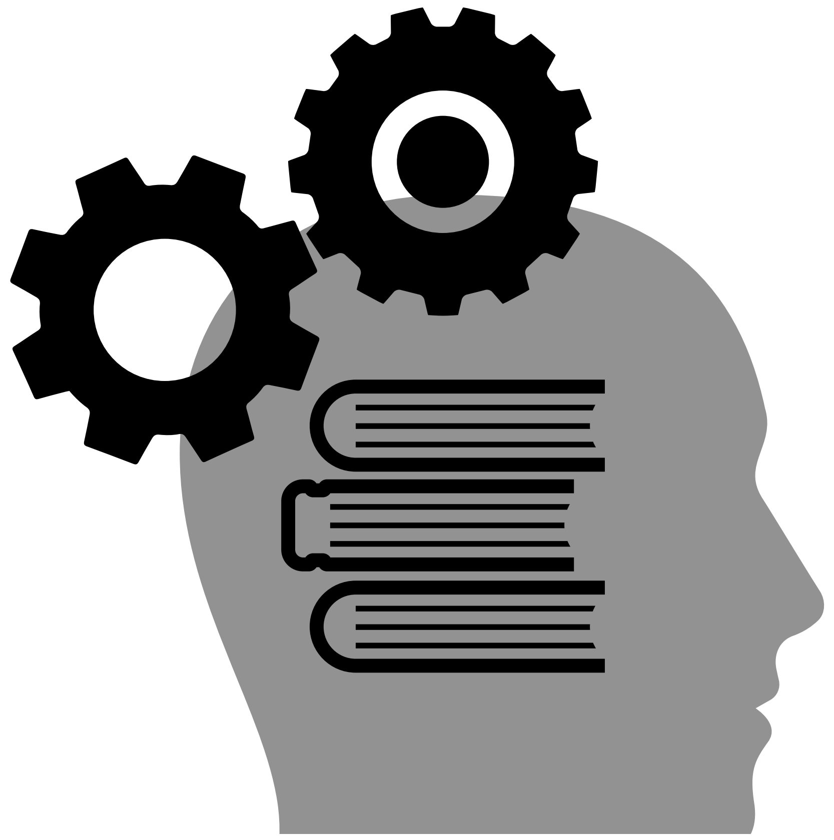
OPC
MQTT
HTTP

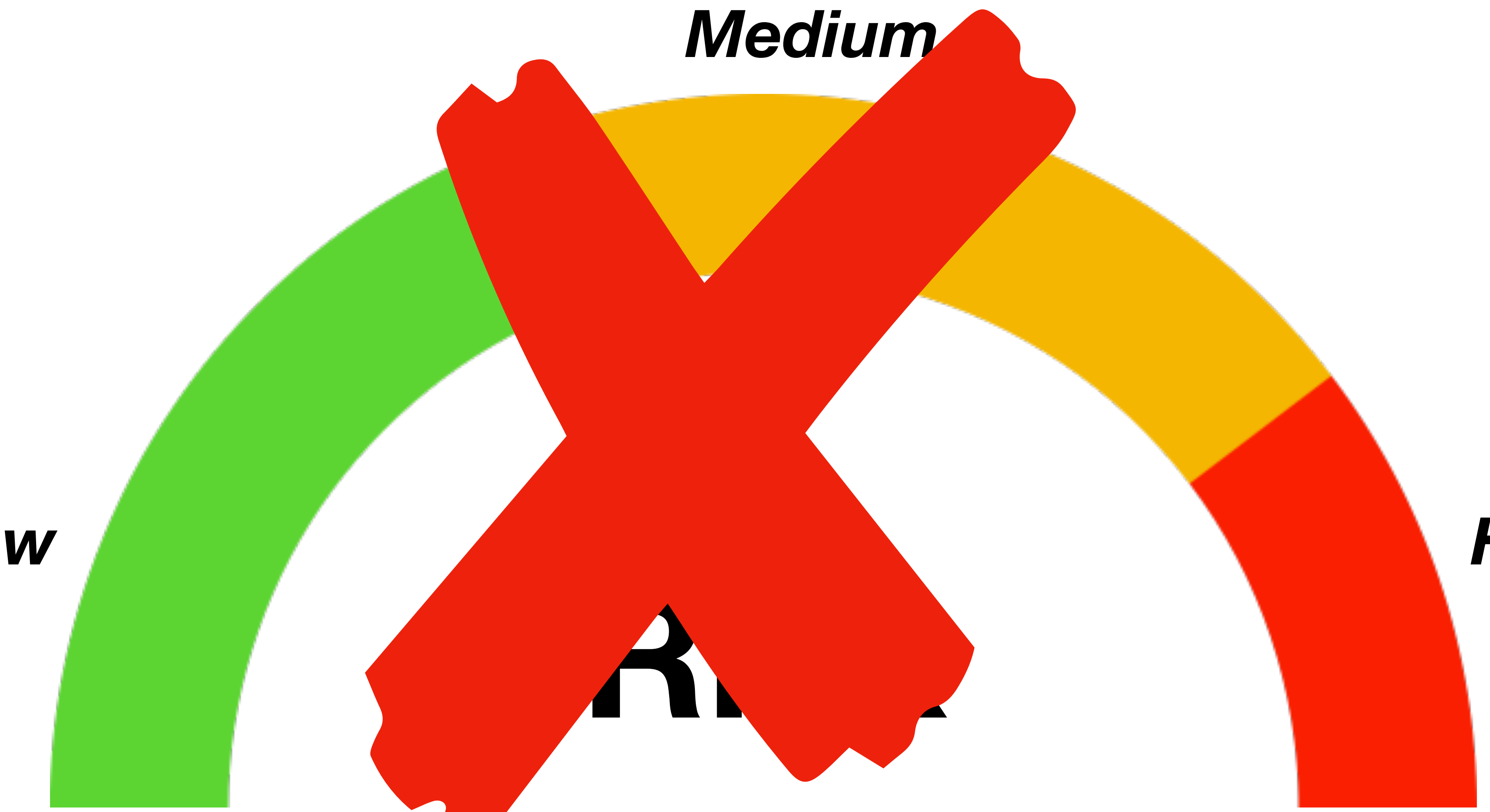
Data Analysis (Wonderware)

Data Analysis (ThingWorx)

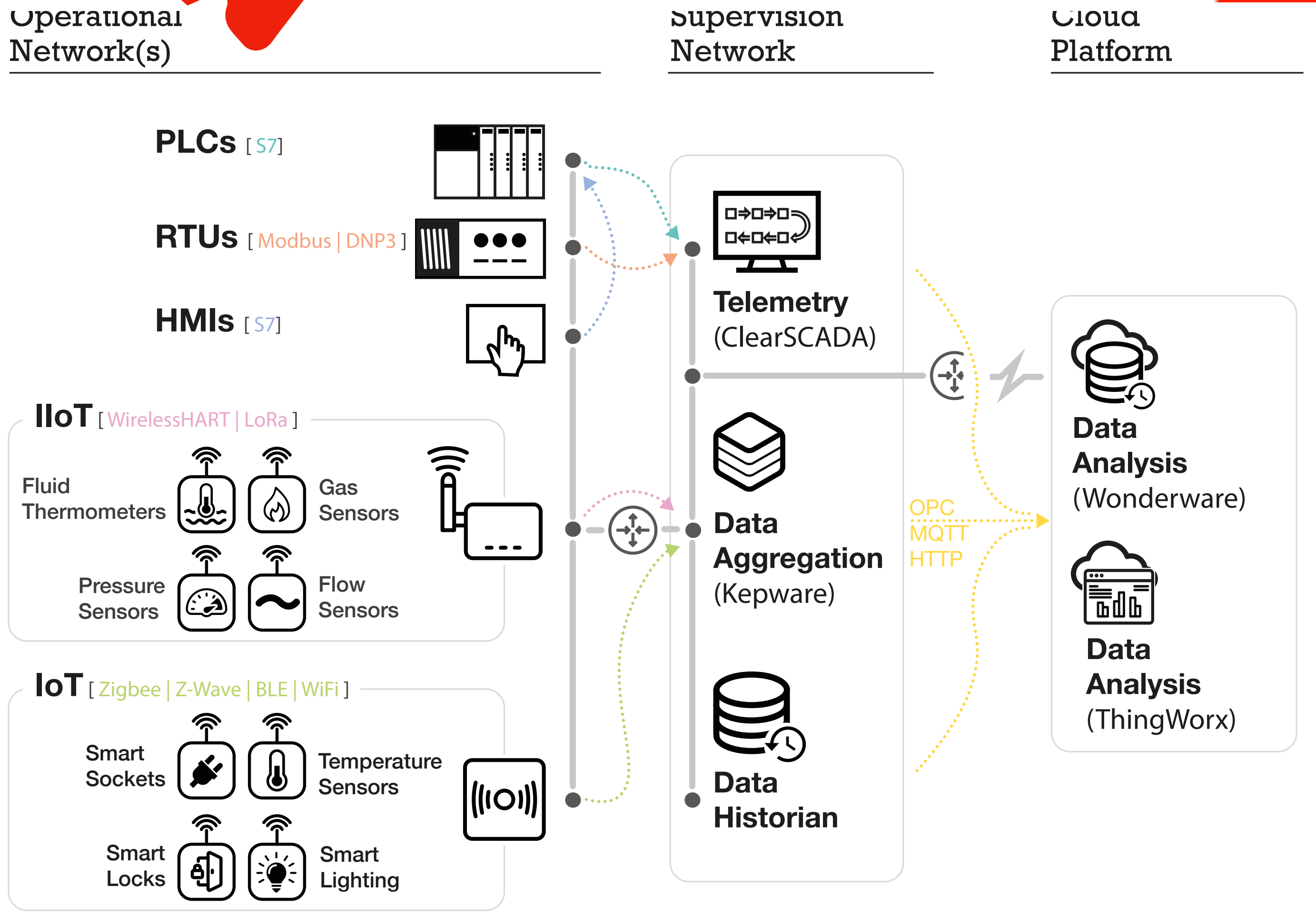


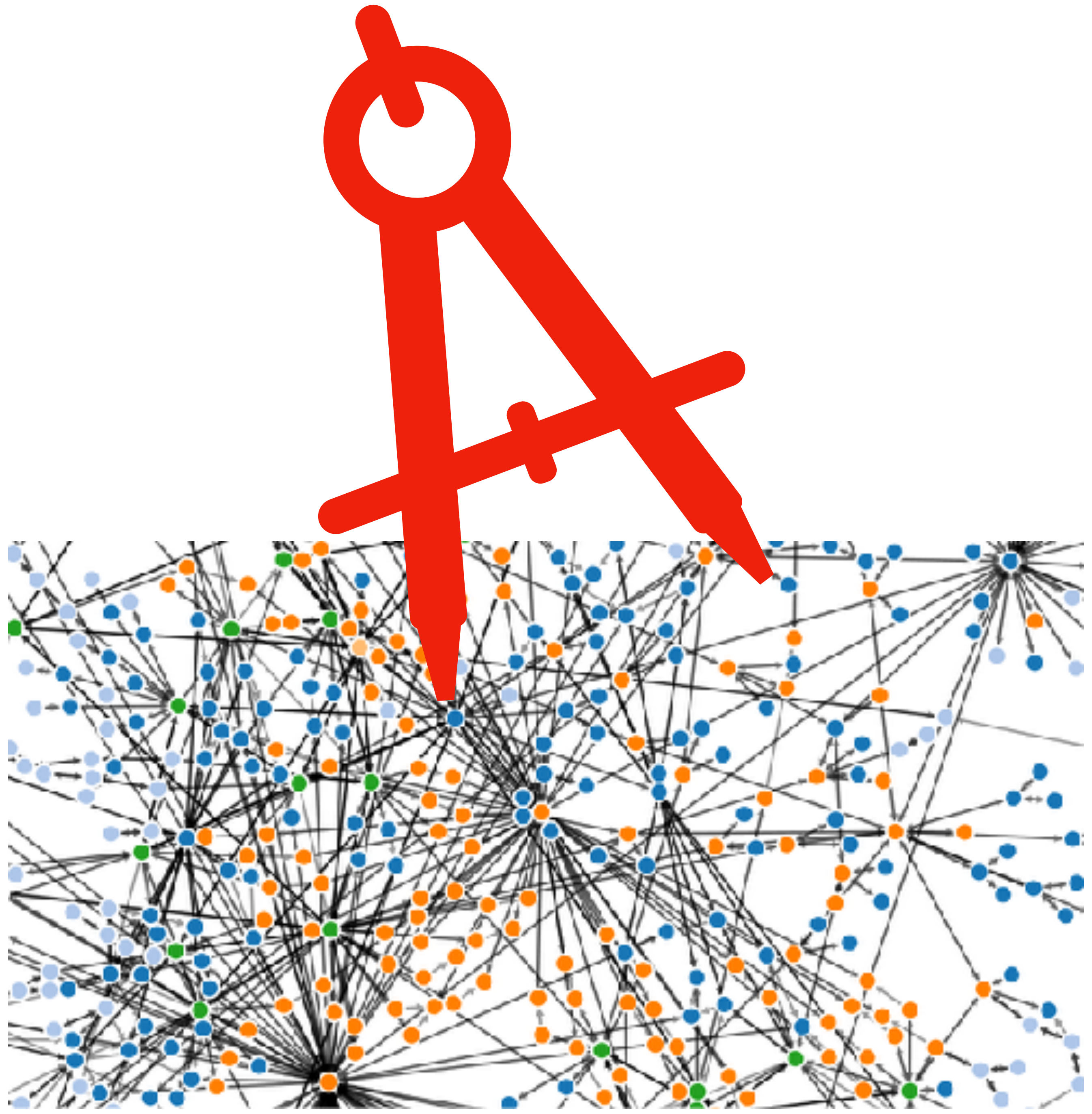
complexity
connectivity
attacks
impact

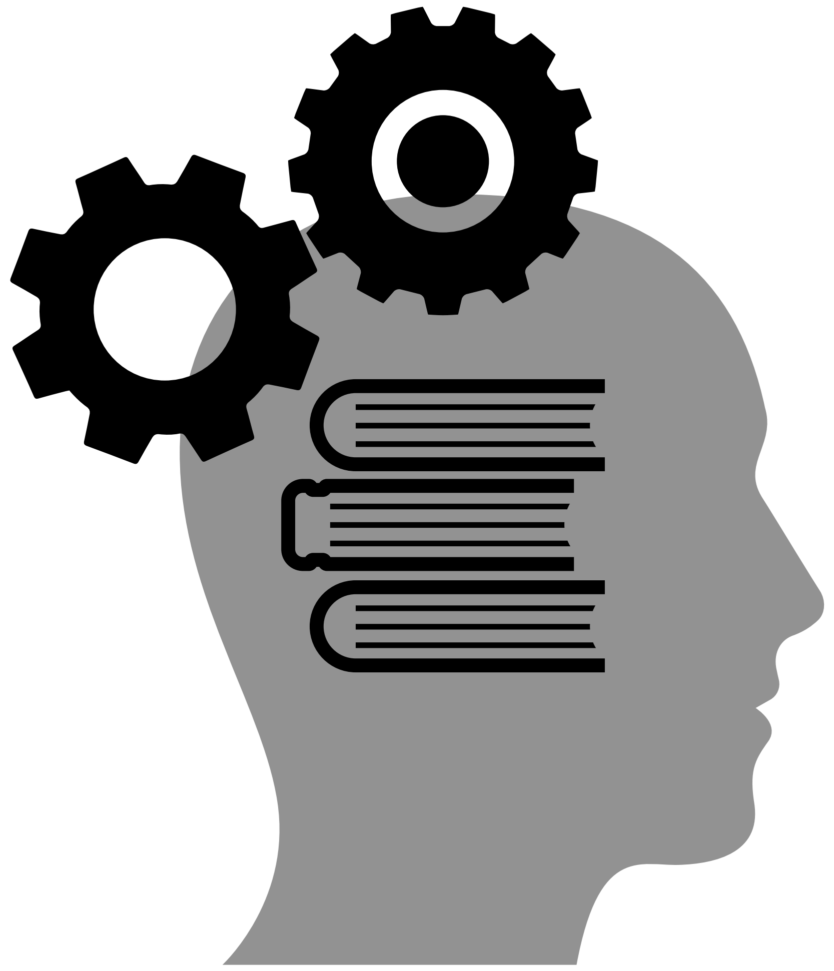



Medium
Low
High

Metrics


Operational Network(s)
Supervision Network
Cloud Platform
PLCs [S7]
RTUs [Modbus | DNP3]
HMIs [S7]
IIoT [WirelessHART | LoRa]
Fluid Thermometers
Gas Sensors
Pressure Sensors
Flow Sensors
IoT [Zigbee | Z-Wave | BLE | WiFi]
Smart Sockets
Temperature Sensors
Smart Locks
Smart Lighting
Telemetry (ClearSCADA)
Data Aggregation (Kepware)
Data Historian
OPC
MQTT
HTTP
Data Analysis (Wonderware)
Data Analysis (ThingWorx)





complexity
connectivity
attacks
impact

Metrics

Or is it?