Summer School AI 4 Industry
Keynote, 2020-07-30, 9h00

When **data** is the new **oil**, it is our role to **prevent** the **blowout**!

Marc-Oliver Pahl, IMT Atlantique Rennes

Chair holder **Chaire Cyber CNI**
Co-Directeur Equipe IRIS / UMR LAB-Sticc
Digital Teaching Coordinator German-French Academy for the Industry of the Future
Leader of the Smart Space Orchestration Team at TUM
Vice President German Chapter of the ACM

chairecyber-cni.org/

Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)

CHAIR OF CYBER CNI Critical National Infrastructures
Institut Mines-Télécom
AIRBUS
AMOSSYS
BNP PARIBAS
EDF
NOKIA Bell Labs

Structure

- Part I: Motivation
- Part II: Security in the Wild
- Part III: Where to use AI?

My goal:

Encourage you to **always consider security** when creating algorithms, software, or products.

The onogoing digitization in all areas of life **requires** it - from **each one of us!**

Cybersecurity of Critical Infrastructures

Some Methods

Blockchain

MACHINE LEARNING

Digital**Twin**

Prevent
Security-by-Design

Detect
Anomaly Detection

CHAIRE
CYBER CNI
Sécurité des infrastructures critiques
EST. 2016

Mitigate
Self-Defend Security Incidents
Self-Recover from Security Incidents

Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)


SHARING
DATA

Part I: Motivation

What data are we talking about and why is it relevant?

chairecyber-cni.org/

Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)

Two Use Cases

A. Self-Driving Cars

B. Industry 4.0

Self-Driving Cars

Tesla Autopilot 2.0 (Camera View) - Level 5 Autonomy. Full Self-Driving Hardware
Daniel
Published on 19 Nov 2016
https://www.youtube.com/watch?v=V4PDTD2VHSU

Tesla Autopilot 2.0 (Camera View) - Level 5 Autonomy. Full Self-Driving Hardware

Waymo 360° Experience: A Fully Self-Driving Journey
Waymo
Published on 28 Feb 2018
https://www.youtube.com/watch?v=B8R148hFxPw

How China is building an all-seeing surveillance state
Washington Post
Published on 7 Jan 2018
https://www.youtube.com/watch?v=uReVvICTrCM

Data Processing Pipeline

local | remote

Prevent
Security-by-Design

Detect
Anomaly Detection

Mitigate
Self-Defend Security Incidents
Self-Recover from Security Incid

data on my side | data with somebody else

Data Sharing

No mass-surveillance

Benefit from collaboration

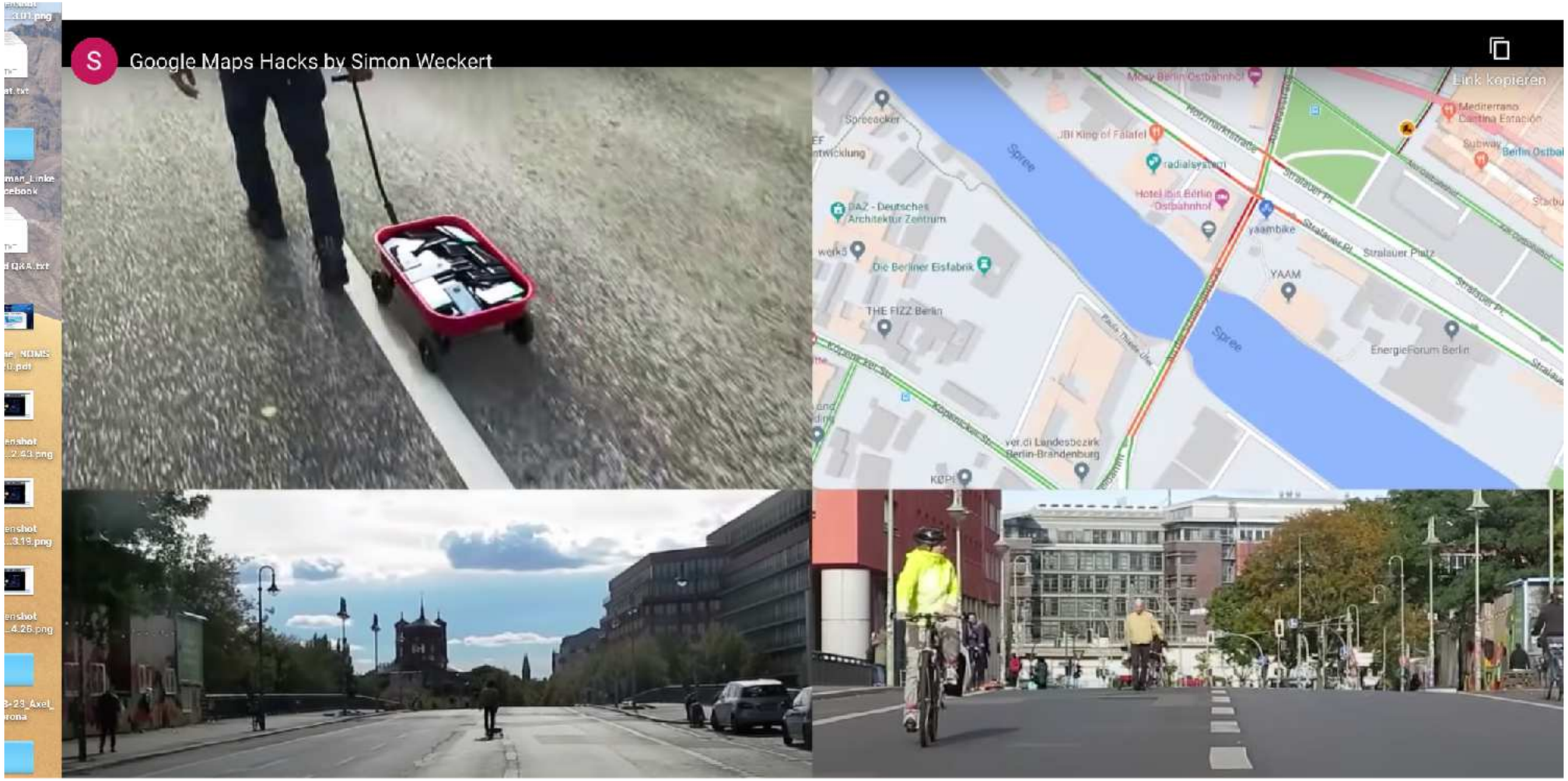
Versatility

Security

Local Processing in the car

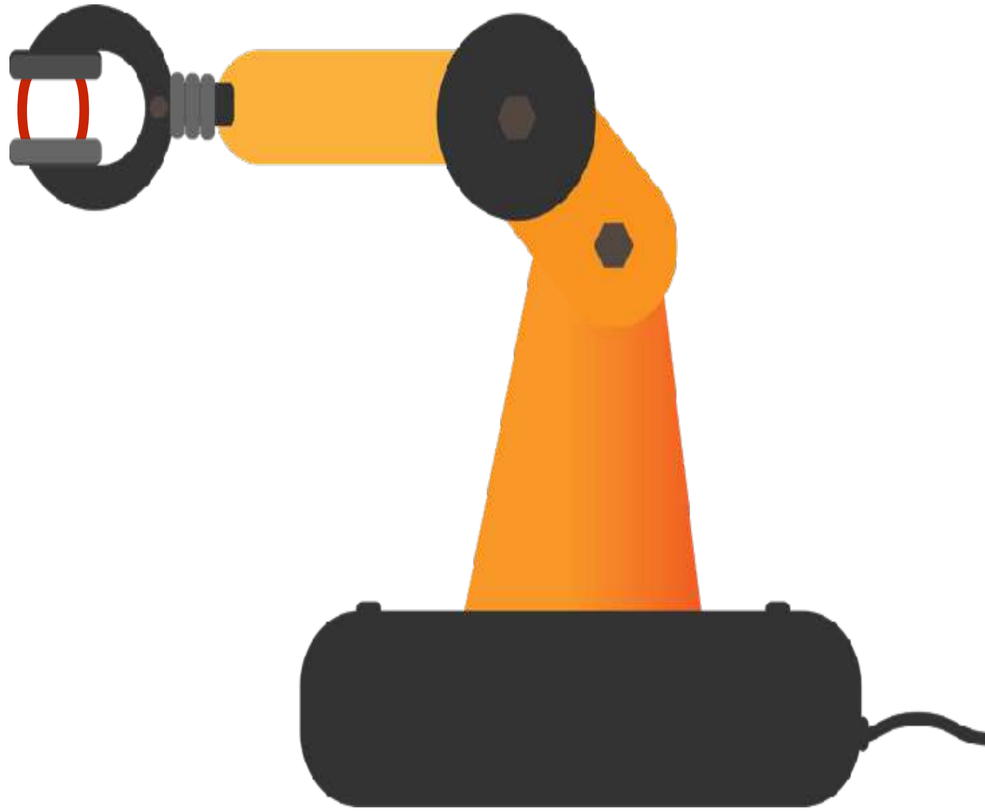
Remote Processing in the cloud

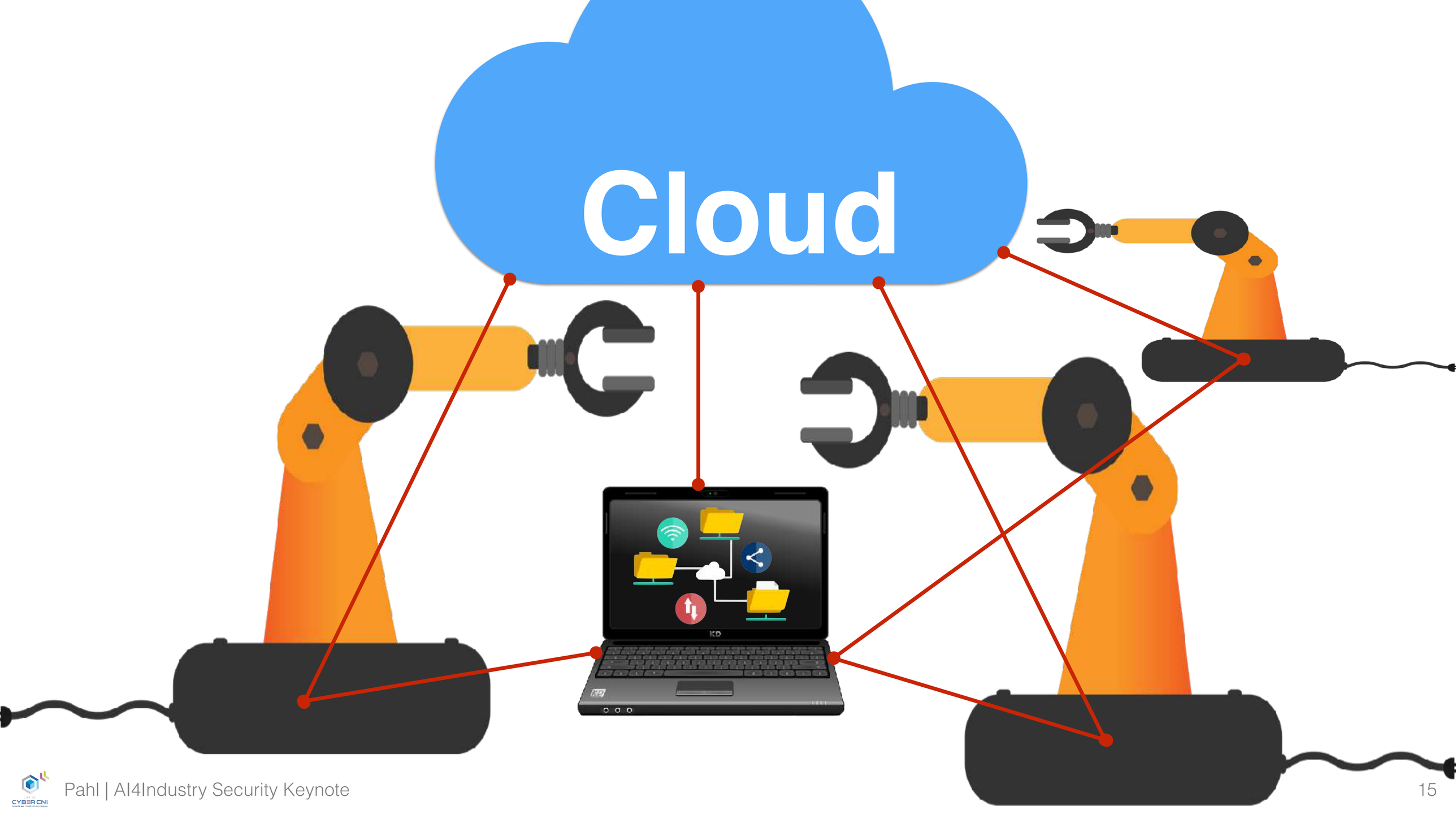
Lots of research challenges: Trust



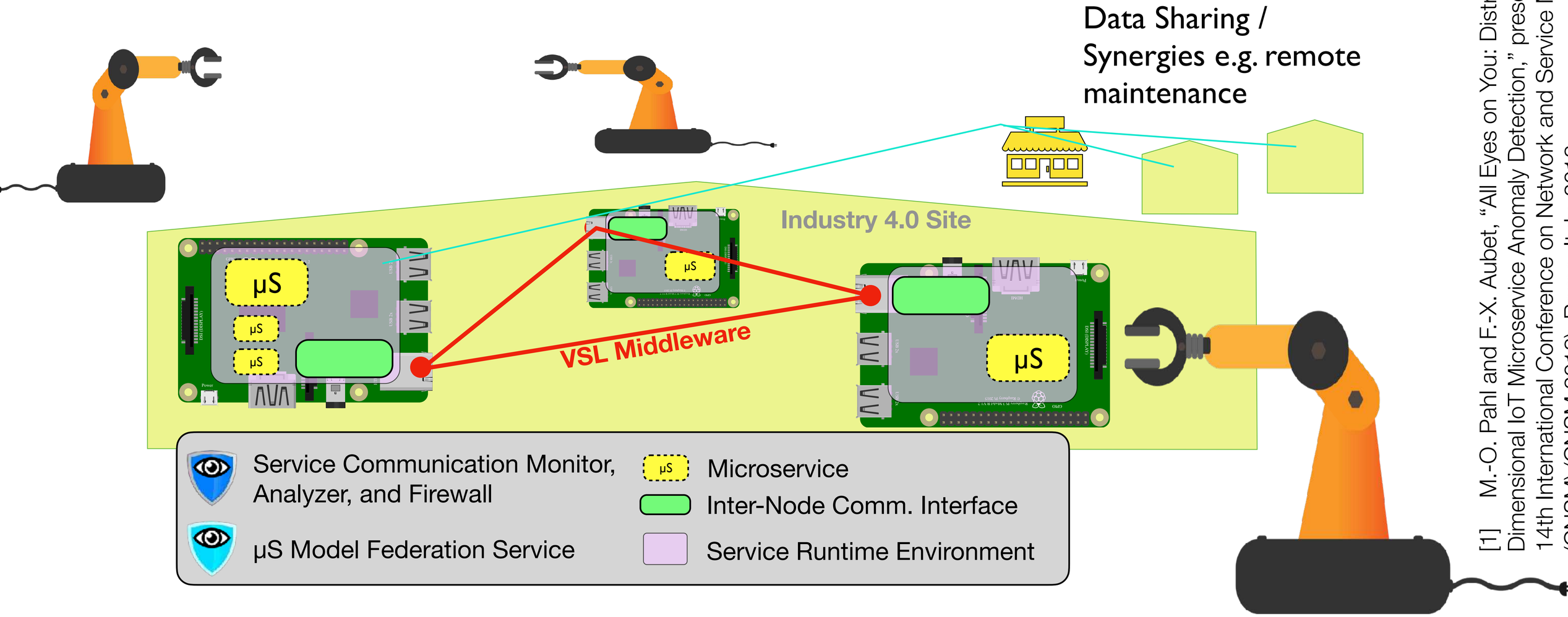
https://youtu.be/k5eL_aI_m7Q

Industry 4.0




Cloud

Synthesis of Distributed Observations



[1] M.-O. Pahl and F.-X. Aubet, "All Eyes on You: Distributed Multi-Dimensional IoT Microservice Anomaly Detection," presented at the 2018 14th International Conference on Network and Service Management (CNSM) (CNSM 2018), Rome, Italy, 2018.

Data Sharing

No unnecessary exposure

Benefit from collaboration

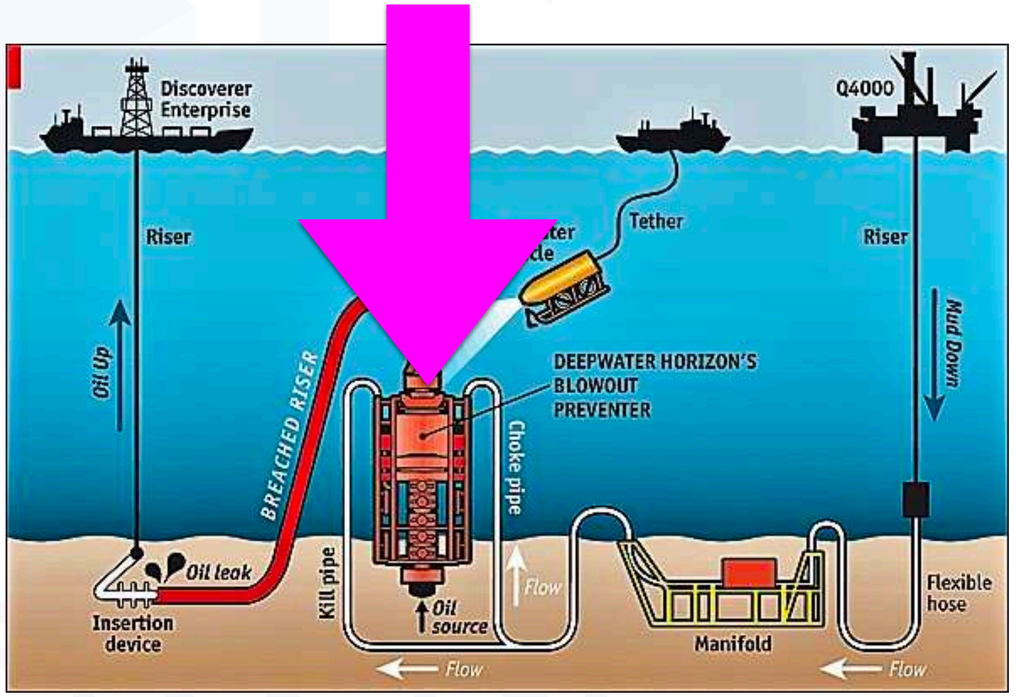
Versatility

Security

Local Processing in the factory

Remote Processing in the cloud

When **Data** is the new **Oil**, **Security** is the **Blowout Preventer**



https://www.seminarstopics.com/seminar/8096/blowout-preventer-seminar-report-pdf

We **need data sharing**. But it has to be **secure** = responsible, transparent, secured, …

Marc-Oliver Pahl, IMT Atlantique Rennes

Chair holder **Chaire Cyber CNI**
Co-Directeur Equipe IRIS / UMR LAB-Sticc
Digital Teaching Coordinator German-French Academy for the Industry of the Future
Leader of the Smart Space Orchestration Team at TUM
Vice President German Chapter of the ACM

chairecyber-cni.org/

Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)

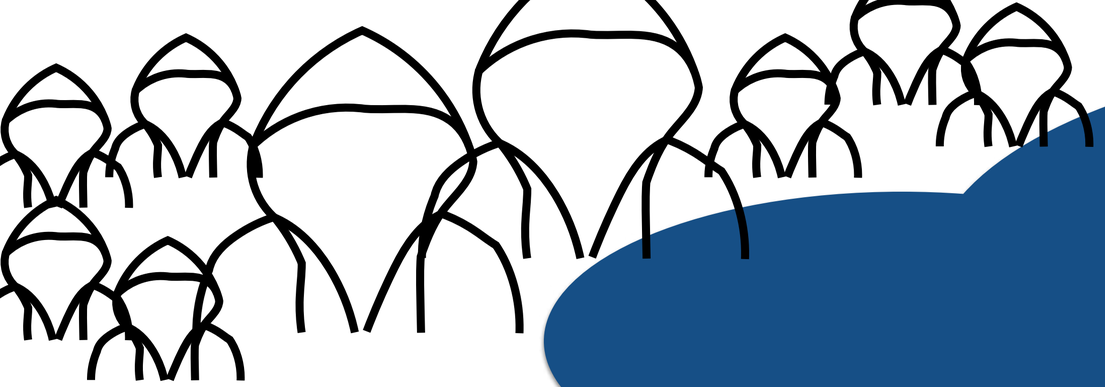
CHAIR OF CYBER CNI Critical National Infrastructures · Institut Mines-Télécom · AIRBUS · AMOSSYS · BNP PARIBAS · EDF · NOKIA Bell Labs

Part II: Security in the Wild

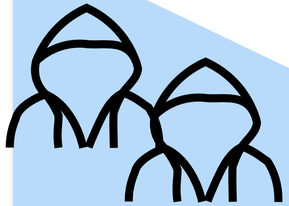
Terminology, goals

chairecyber-cni.org/

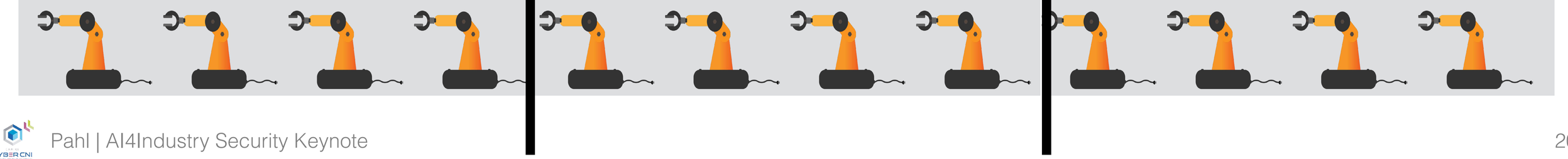
Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)



Cloud

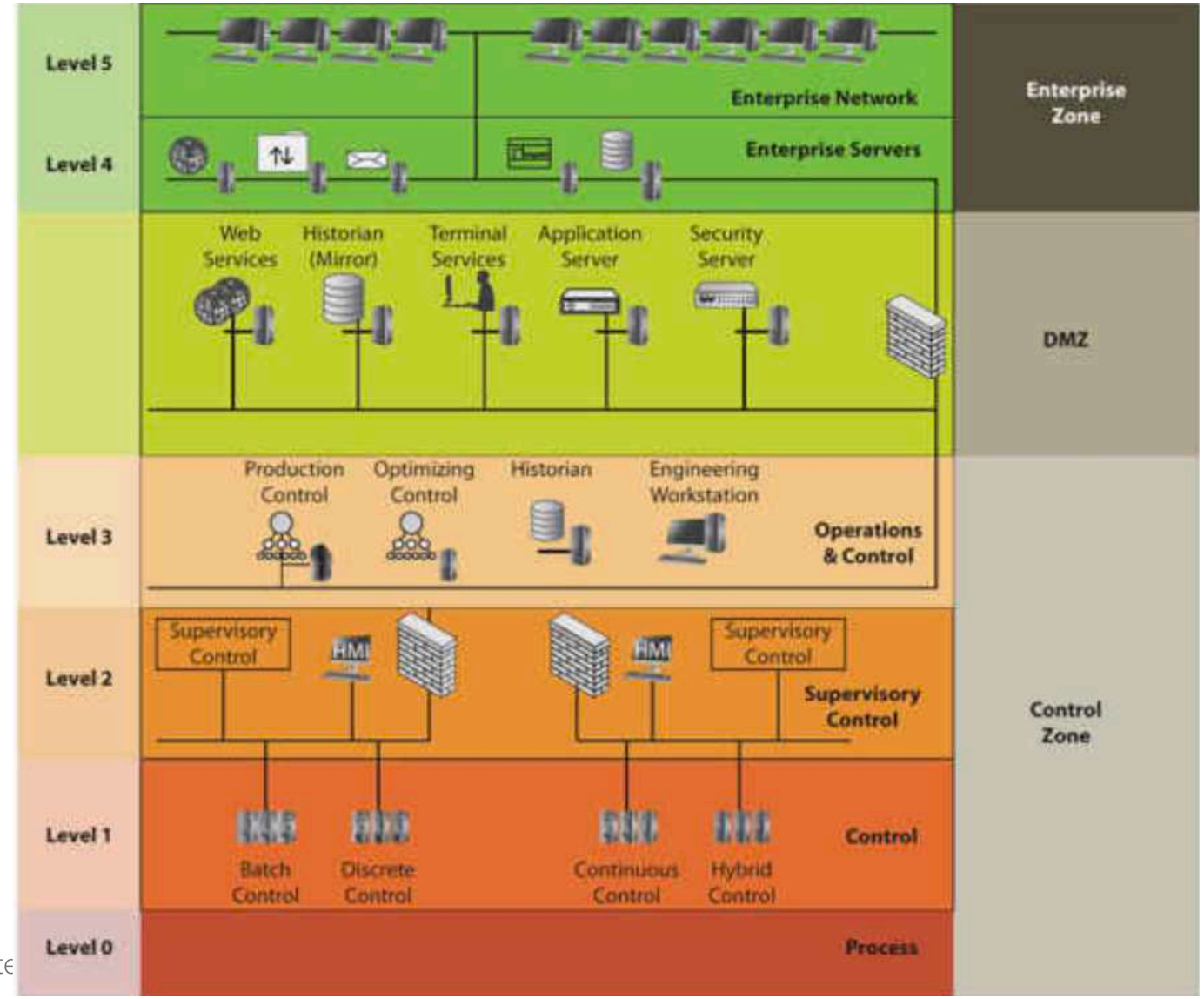


Edge / Fog



Purdue Enterprise Reference Model (PERA) [1]

1990
Williams;
now
ISA-99
(ISA / IEC
62443)



Originally: ICS vs IIoT

- IoT = Things connected to the Internet
- ICS = Explicitly NOT connected to the Internet

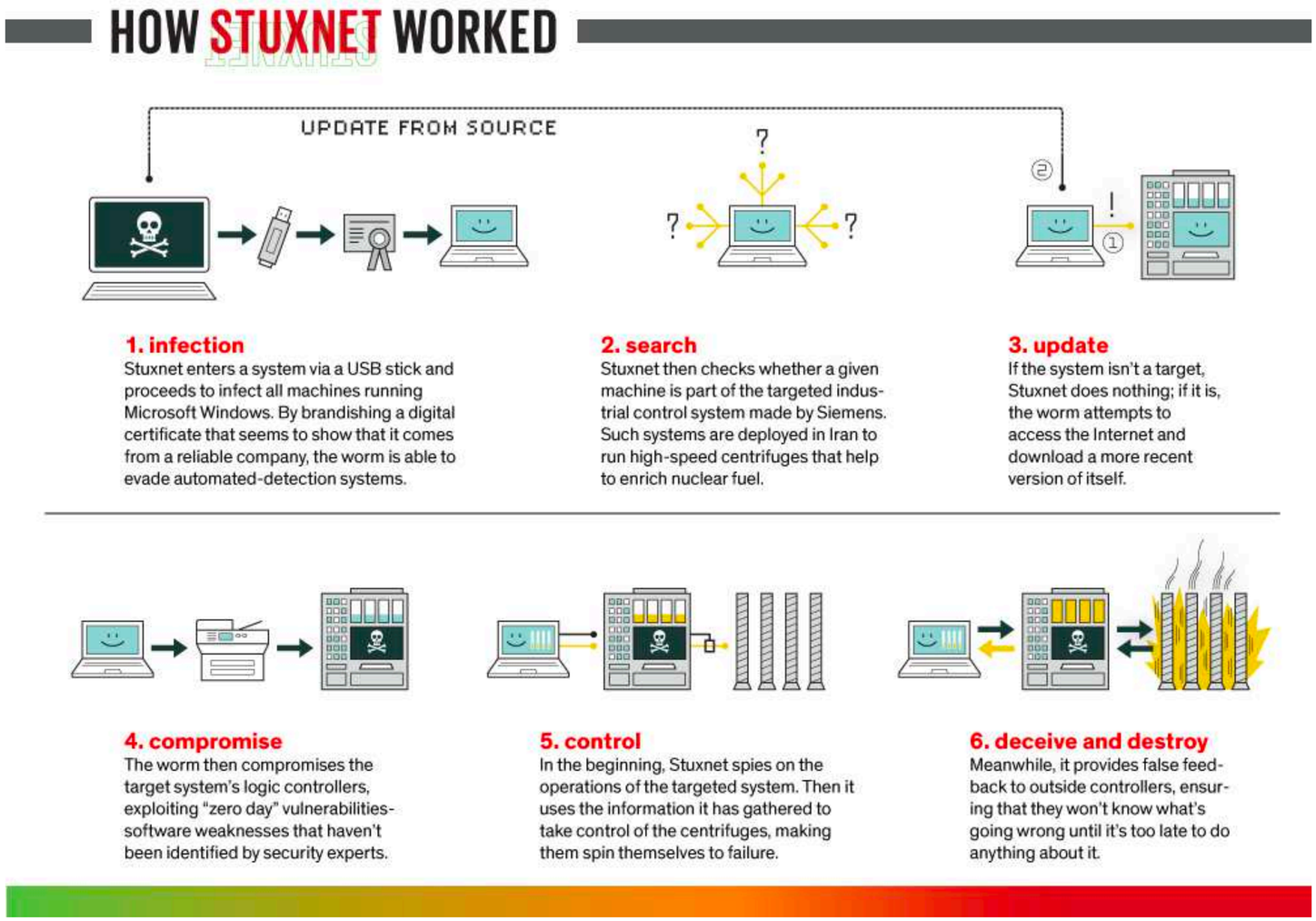
Why do we need Security?

- safety
- health
- welfare
- financial losses (production stop)
- lawsuit (non-compliance)
- environmental impact (oil spill)
- security (access control)
- …

Fundamental Problem

- Disconnected legacy systems get connected to the Internet
- Large attack potential
  - remote
  - script kids
  - hackers
  - stuxnet even over air gap

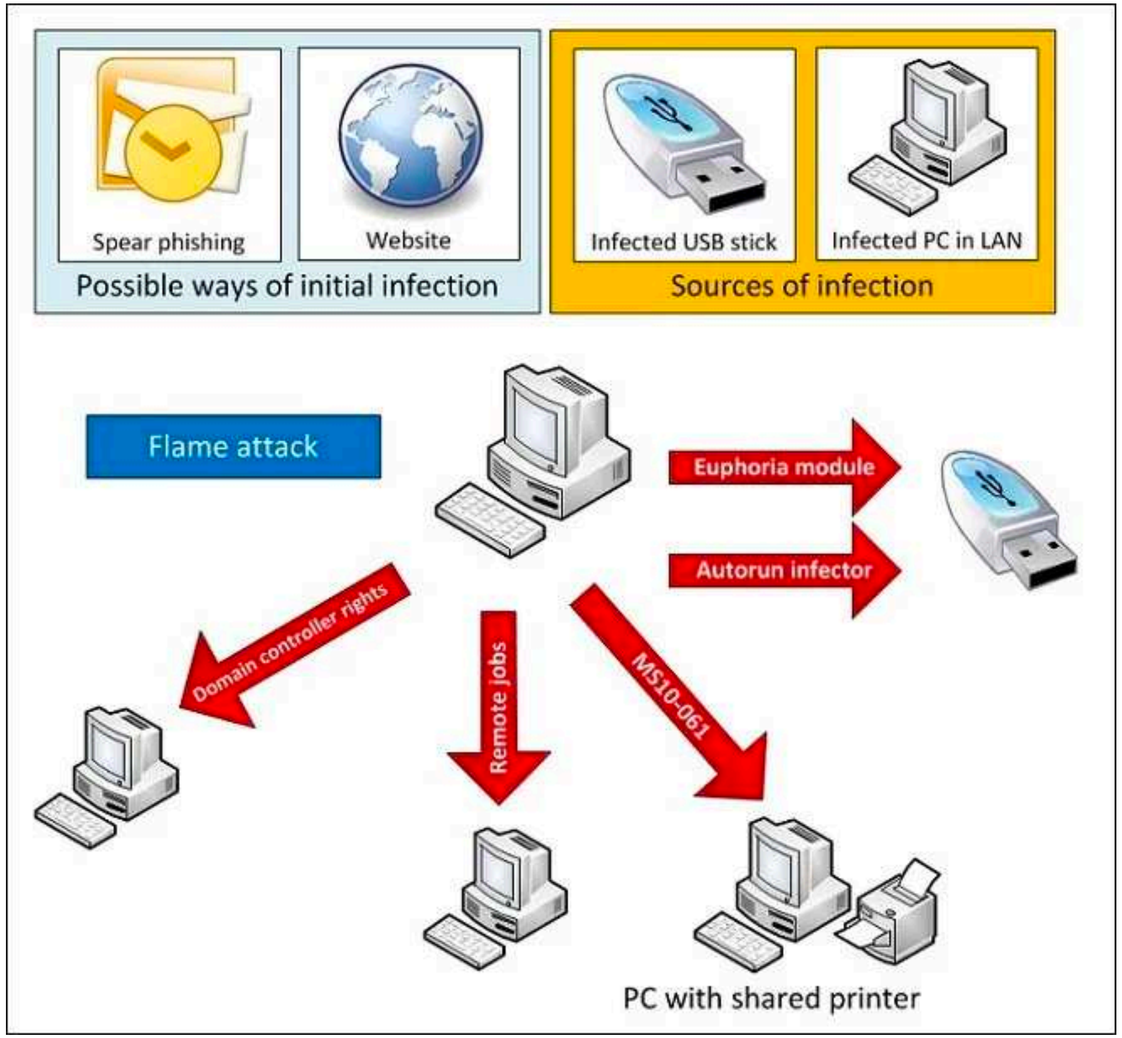
A. Stuxnet



- When?
- By whom?
- Where?
- Target?
- **How?**
  - What vulnerabilities are exploited?
  - How is the attack flow?
- Success rate?

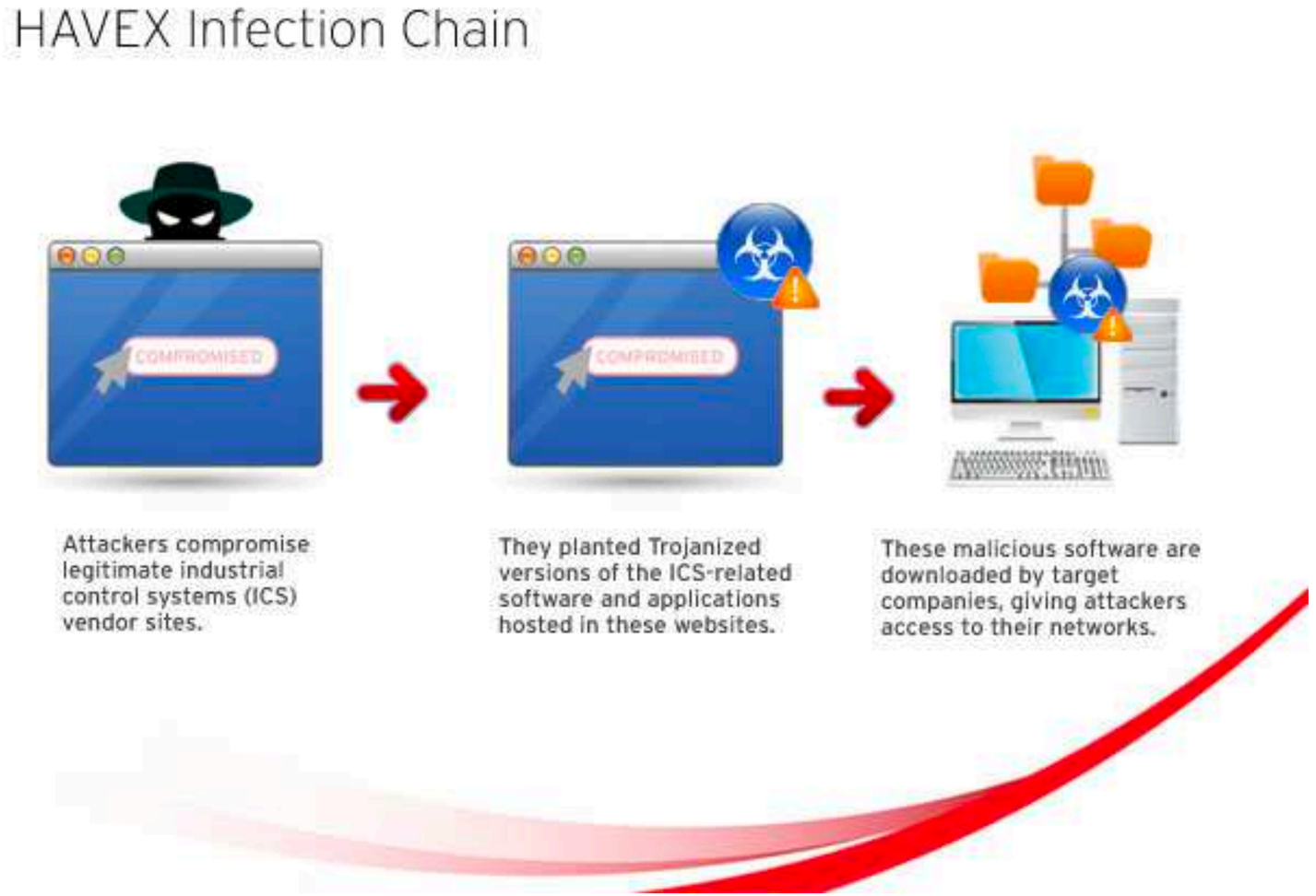
https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet

B. Flame



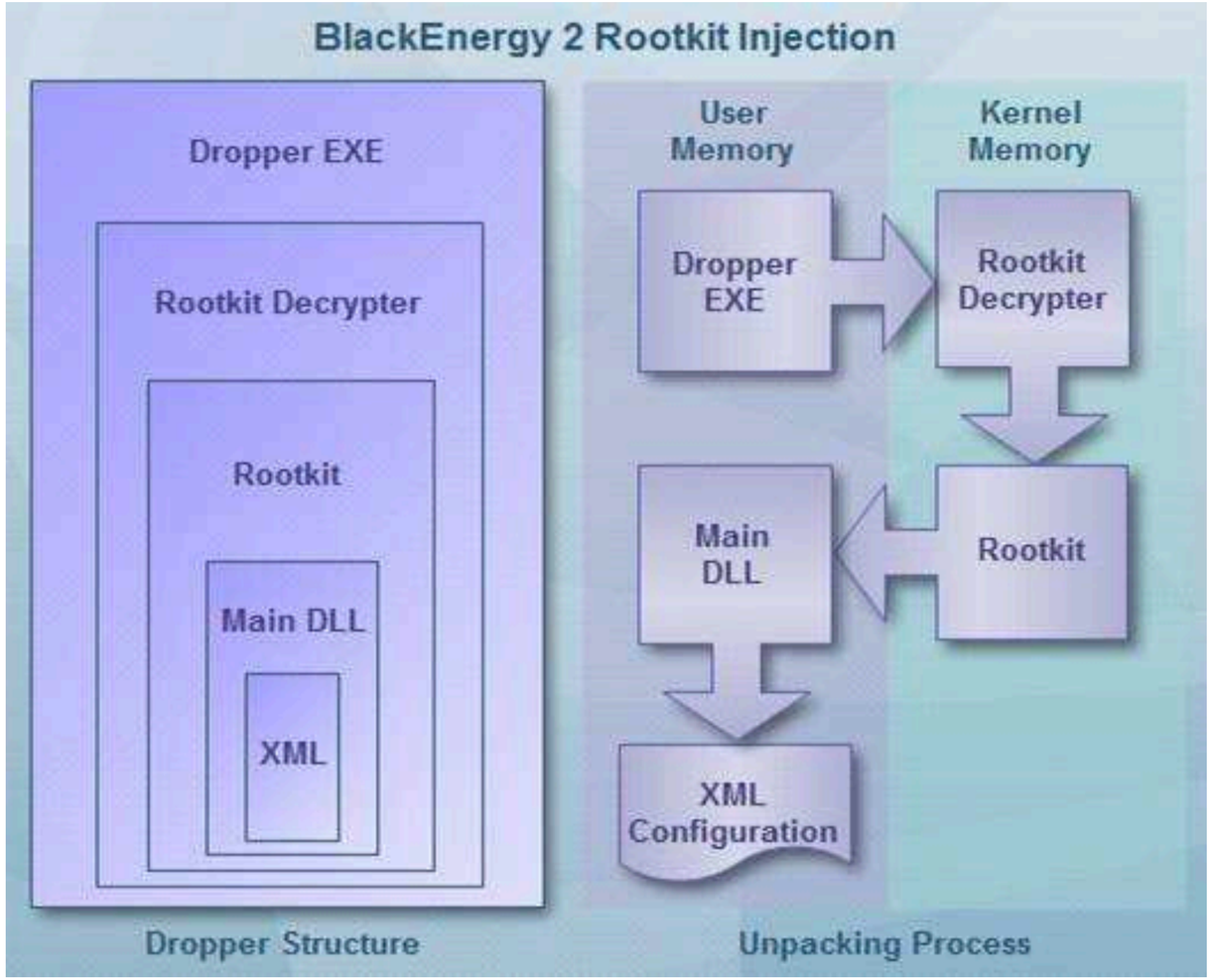
- When?
- By whom?
- Where?
- Target?
- **How?**
  - What vulnerabilities are exploited?
  - How is the attack flow?
- Success rate?

C. Havex



- When?
- By whom?
- Where?
- Target?
- **How?**
  - What vulnerabilities are exploited?
  - How is the attack flow?
- Success rate?

D. BlackEnergy



- When?
- By whom?
- Where?
- Target?
- **How?**
  - What vulnerabilities are exploited?
  - How is the attack flow?
- Success rate?

Skills for ICS Cybersecurity?

- Requires Multidisciplinary understanding
  - Cybersecurity: networking stack / OS stack
  - Functionality of ICS
  - Physics / Engineering requirements of industrial processes

What are **advantages** and disadvantages of having (networked) PLCs?

- Good
  - Software can easily be exchanged adapted
  - Mass production as “general purpose” -> cheaper
  - Flexible (can be adapted)

What are advantages and **disadvantages** of having (networked) PLCs?

- Bad
  - Software can easily be exchanged adapted (= modified by attack)
  - All software problems such as dead locks, overflows, timing issues, …
  - Much bigger attack surface
  - The weakest part in the chain defines the security level
  - Older devices were not designed with properties that spread from IT networks such as high traffic and fail or reset then
  - Human-factor: Knowledge in IT and OT rare -> common security standards are not taken into account

Goal for ICS security

- ensure the safe and reliable operation of the physical process [1]
  - Catastrophic safety failures
  - Environmental release of hazardous materials
  - Loss of production
  - Product recall
  - Regulatory fines
  - Sustained production inefficiency
  - Loss of public confidence”

ICS Security Standards

- ISA-84
- IEC 61508
- ISA-95
- ISA-99 (ISA-62443 / IEC 62443)
- NERC CIP
- 6 CFR 27
- Homeland Security's Chemical Facility Anti-Terrorism Statutes (CFATS)
- …

A. Worcester air traffic communications

Worcester air traffic communications In March 1997, a teenager in Worcester, Massachusetts, disabled part of the public switched telephone network using a dial-up modem connected to the system. This knocked out phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport. Also, the tower's main radio transmitter and another transmitter that activated runway lights were shut down, as well as a printer that controllers used to monitor flight progress. The attack also knocked out phone service to 600 homes and businesses in the nearby town of Rutland. (http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html)

- When?
- Who?
- What attacked?
- How?
- Impact

B. Maroochy Shire sewage spill

Maroochy Shire sewage spill In the spring of 2000, a former employee of an Australian organization that develops manufacturing software applied for a job with the local government, but was rejected. Over a two-month period, the disgruntled rejected employee reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks. (http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf and http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/)

- When?
- Who?
- What attacked?
- How?
- Impact

C. Davis-Besse Nuclear plant

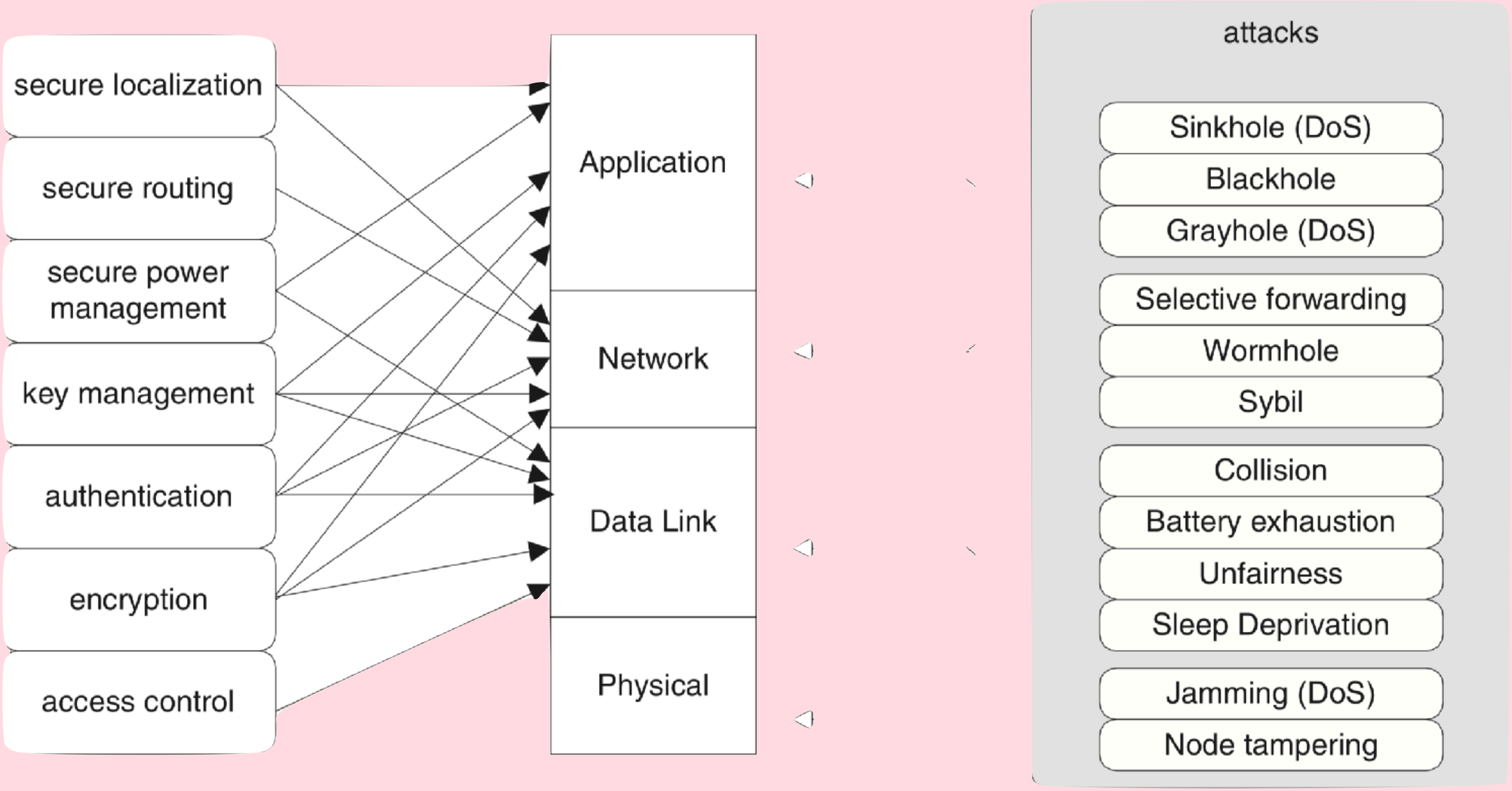
Davis-Besse In August 2003, the Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again. Slammer reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly that control system traffic was blocked. (http://www.securityfocus.com/news/6767)

- When?
- Who?
- What attacked?
- How?
- Impact

Some Literature to continue…

- Kim Zetter. 2014. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group, USA.
- Alex Gibney, Zero Days (2016) movie: https://youtu.be/2qaxJs8wYVw
- [1] Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit, Stephen Hilt. "Hacking Exposed: Industrial Control Systems".
- [2] Keith Stouffer (NIST), Suzanne Lightman (NIST), Victoria Pillitteri (NIST), Marshall Abrams (MITRE), Adam Hahn (WSU), "SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security," Mai 2015, NIST, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
- [3] Michael J. Assante and Robert M. Lee, "The Industrial Control System Cyber Kill Chain," October 2015, https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Security Mechanisms and Risks



from: Jelena Misic and Vojislav B. Misic, “Wireless personal area networks : performance, interconnections and security with IEEE 802.15.4,” 2007

Part III: Where to use AI?

Examples where AI can help

chairecyber-cni.org/

Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)

Prevent
Security-by-Design

Detect
Anomaly Detection

Mitigate
Self-Defend Security Incidents
Self-Recover from Security Incidents

T7: Autoencoder
Integrity
Authentication

T8: Resilient Control Sys
Tolerance
Counter-maeasures
AI

T4: Non-Cooperative Game
Possibility for defense

T1: Time Series Analysis
Statistic Tests

T2: 3D Visualization
Virtual world
Log Data
AI

T3: CVE -> Graph
NLP
Semantic Processing
AI

T6: Resilience
Evaluation
Digital Twin
AI

T9: Share Incident Knowledge
Blockchain
AI

T5: SDN Security
Self-Security
Policy-based Security

Some Methods
Blockchain MACHINE LEARNING  DigitalTwin

chairecyber-cni.org/

Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)

CHAIR OF CYBER CNI Critical National Infrastructures
Institut Mines-Télécom
AIRBUS
AMOSSYS
BNP PARIBAS
EDF
NOKIA Bell Labs

Going to the full stack

S² labs

People

Interface Devices

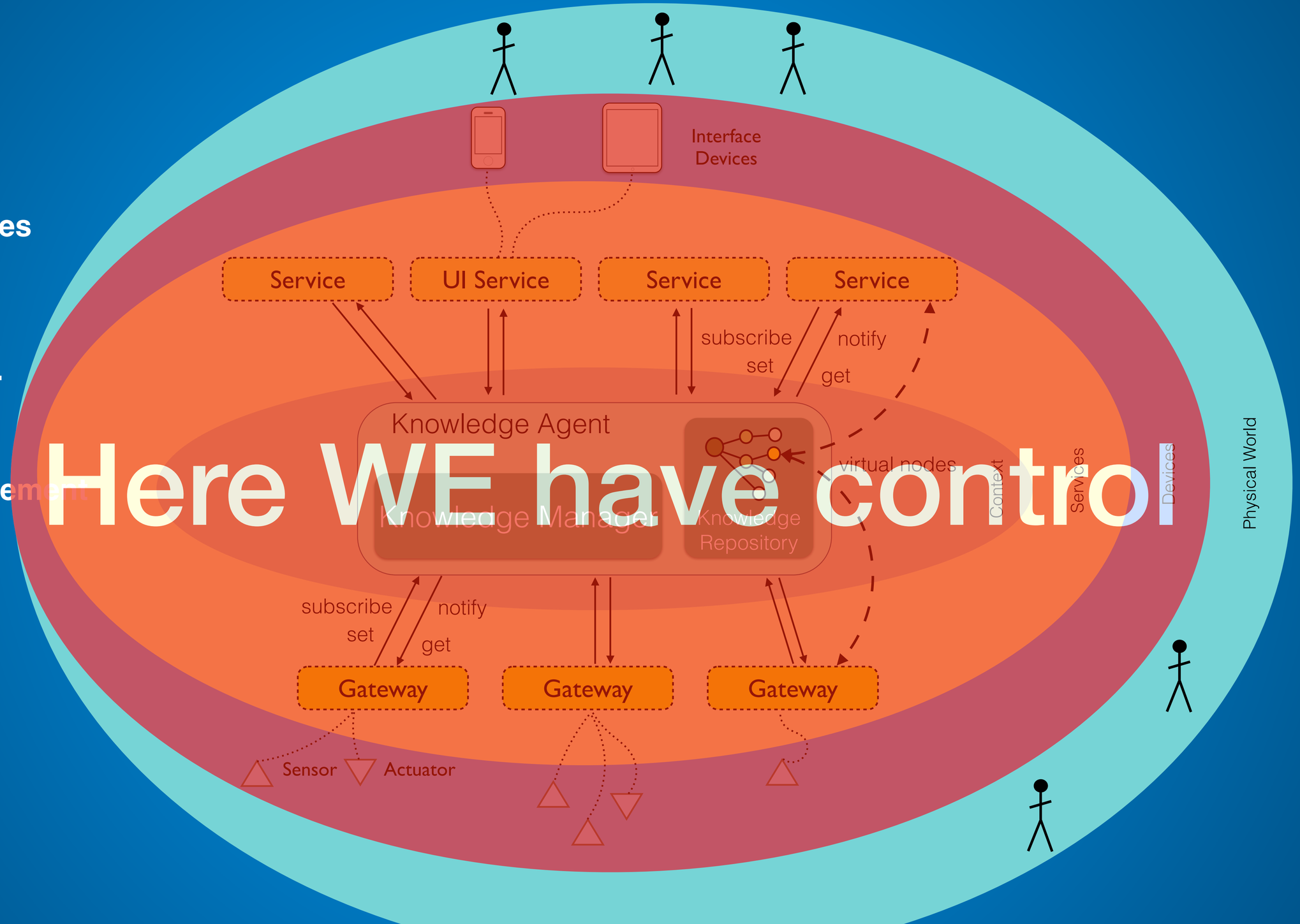
Orchestration
Workflows, etc.

Context Management

Bidirectional
Adaptation

Heterogeneous
Smart Devices

Physical World



Here WE have control

People

Interface Devices

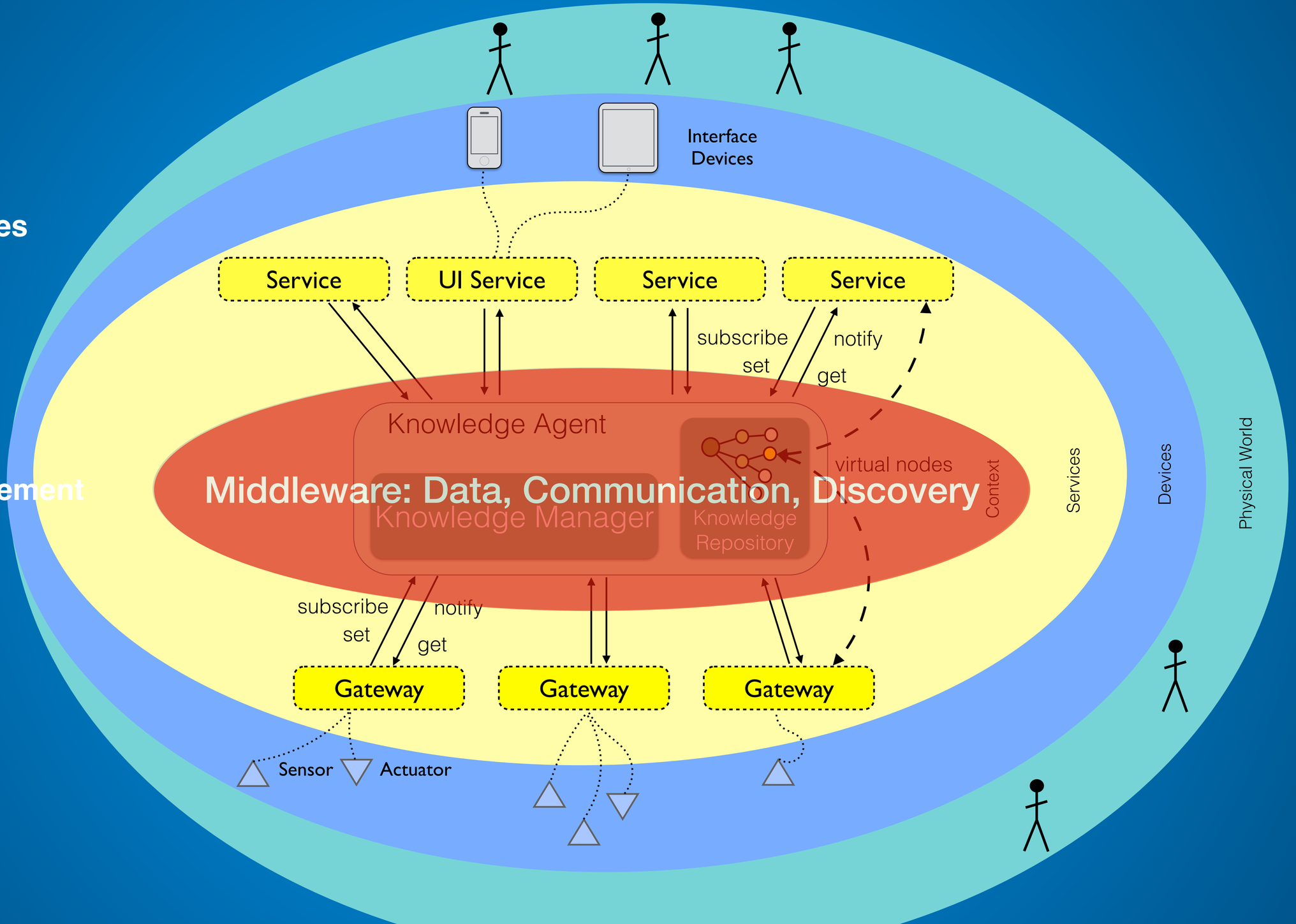
Orchestration
Workflows, etc.

Context Management

Bidirectional
Adaptation

Heterogeneous
Smart Devices

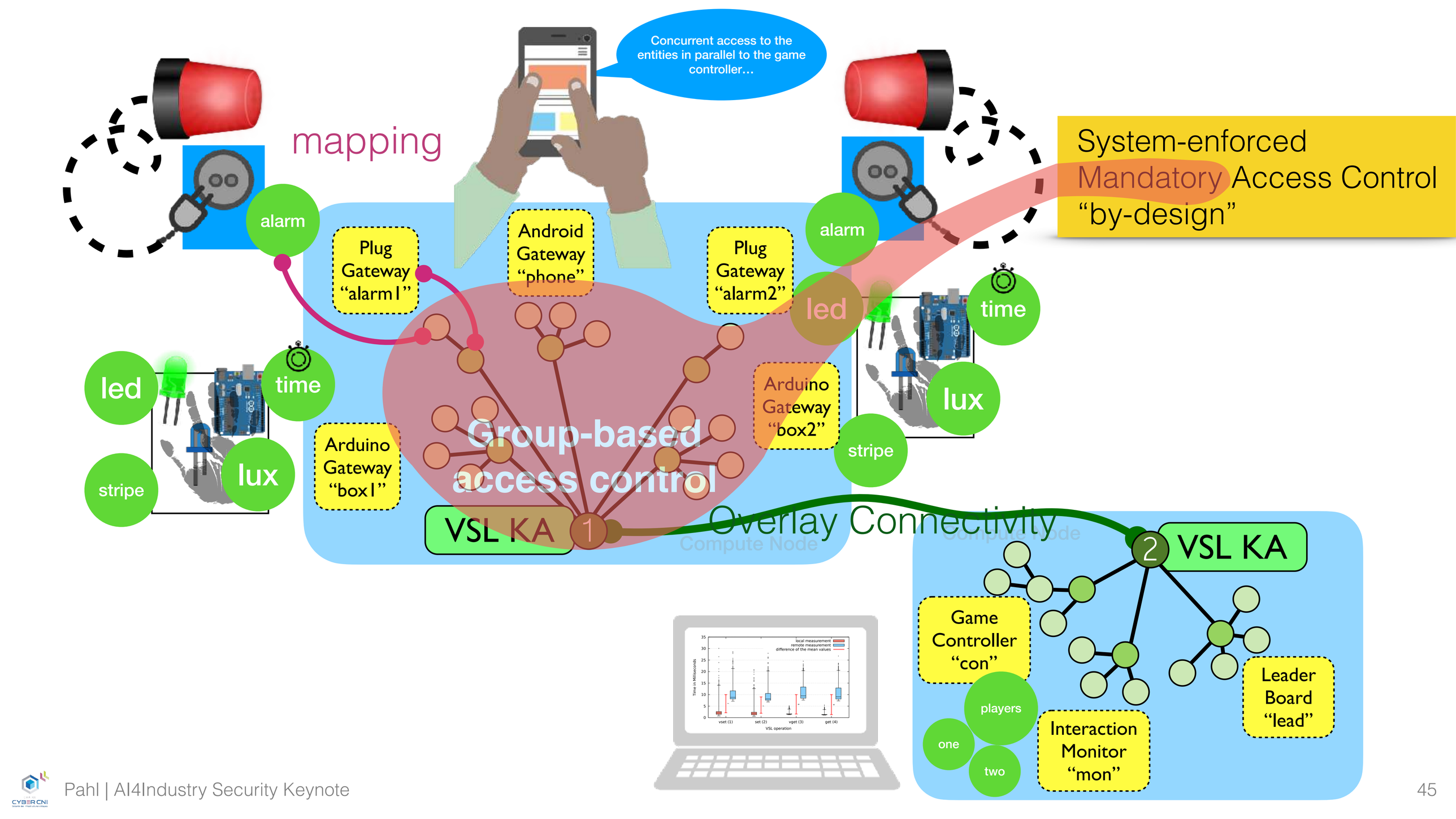
Physical World



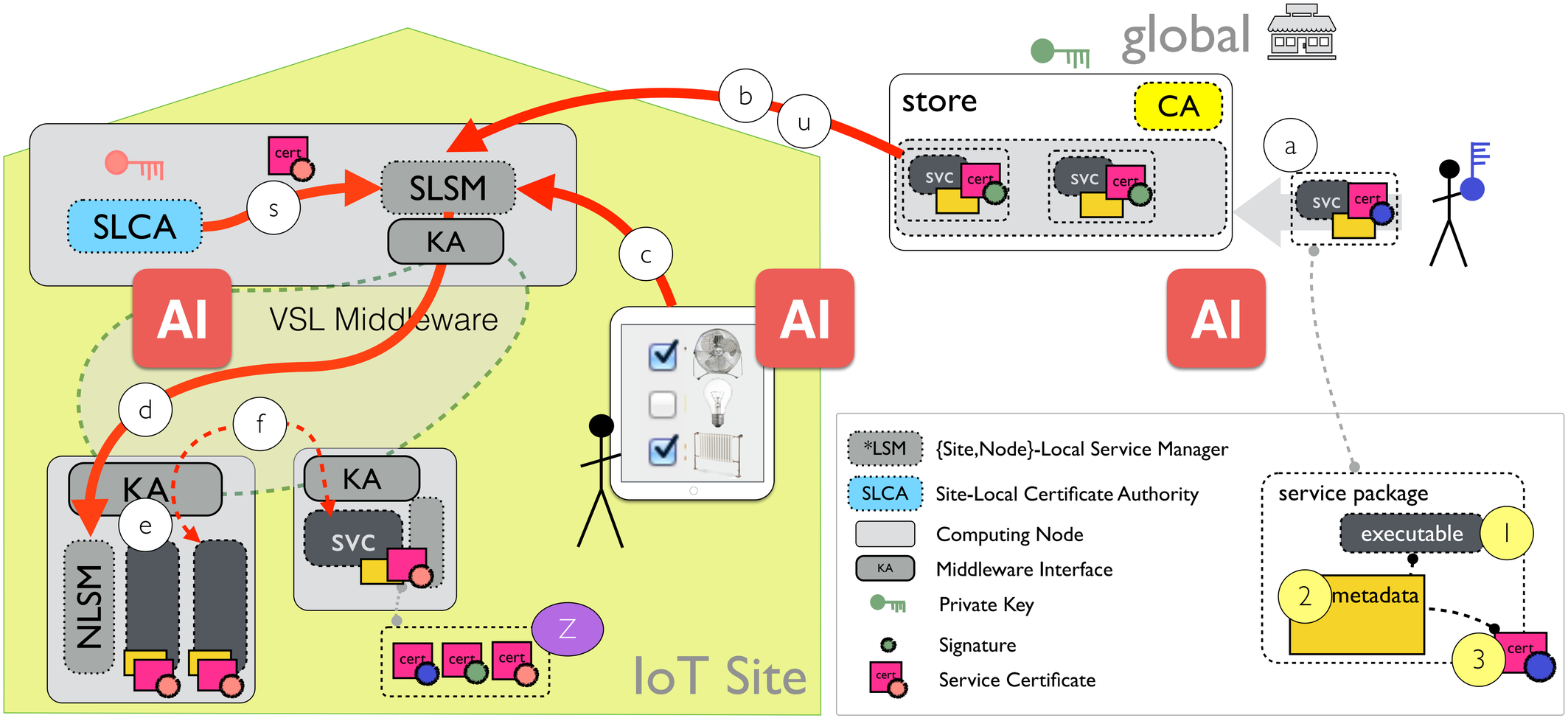
I. *Prevent*
Identities, Secure Metadata, Access Control

chairecyber-cni.org/

Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)


Concurrent access to the entities in parallel to the game controller…
mapping
System-enforced Mandatory Access Control “by-design”
alarm
Plug Gateway “alarm1”
Android Gateway “phone”
Plug Gateway “alarm2”
alarm
led
time
lux
stripe
led
time
lux
stripe
Arduino Gateway “box1”
Arduino Gateway “box2”
Group-based access control
VSL KA
1
Overlay Connectivity
Compute Node
Compute Node
2
VSL KA
Game Controller “con”
players
one
two
Interaction Monitor “mon”
Leader Board “lead”
local measurement
remote measurement
difference of the mean values
Time in Milliseconds
VSL operation
vset (1)
set (2)
vget (3)
get (4)

Distributed Smart Space Orchestration System



People

Interface Devices

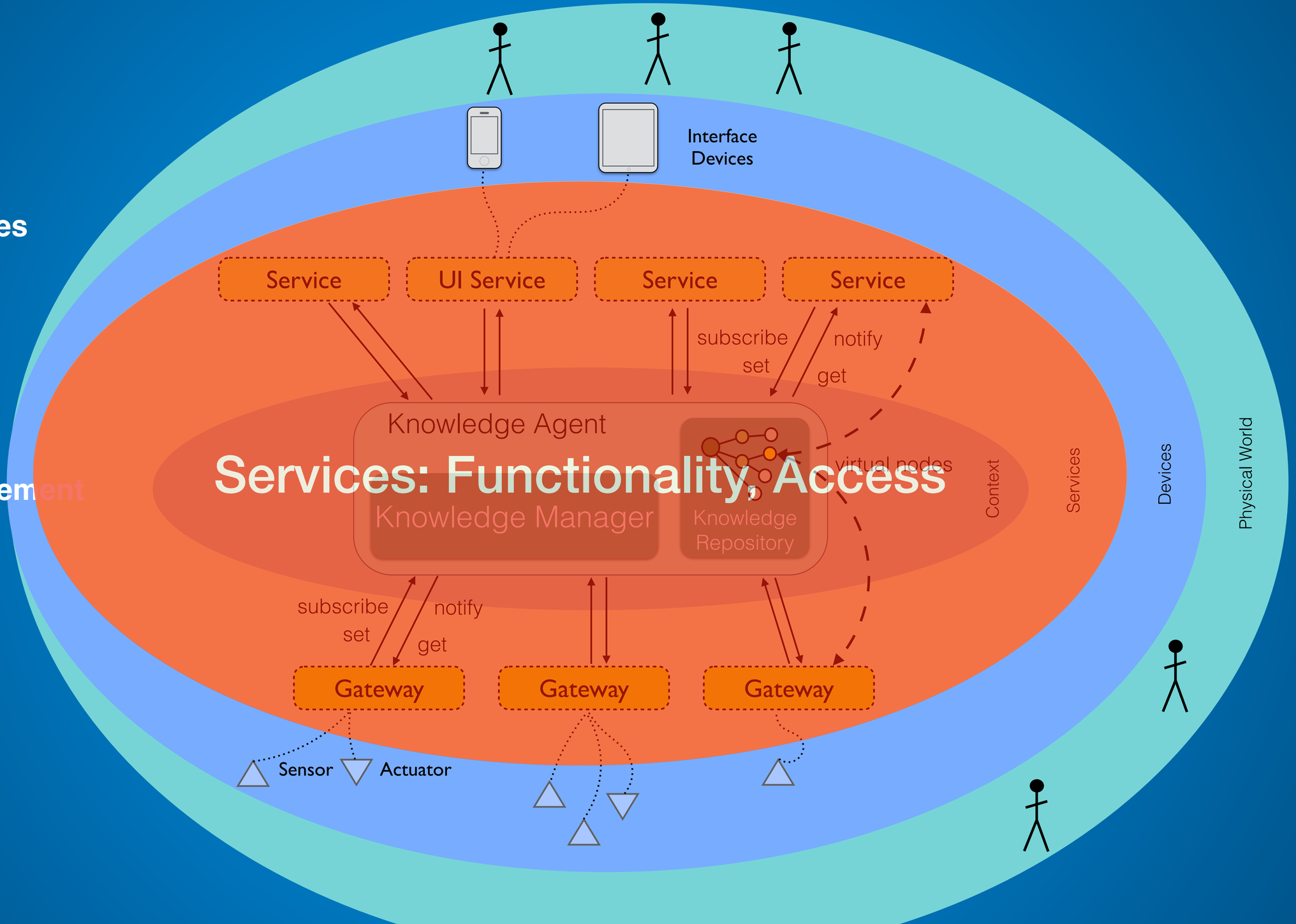
Orchestration
Workflows, etc.

Context Management

Bidirectional
Adaptation

Heterogeneous
Smart Devices

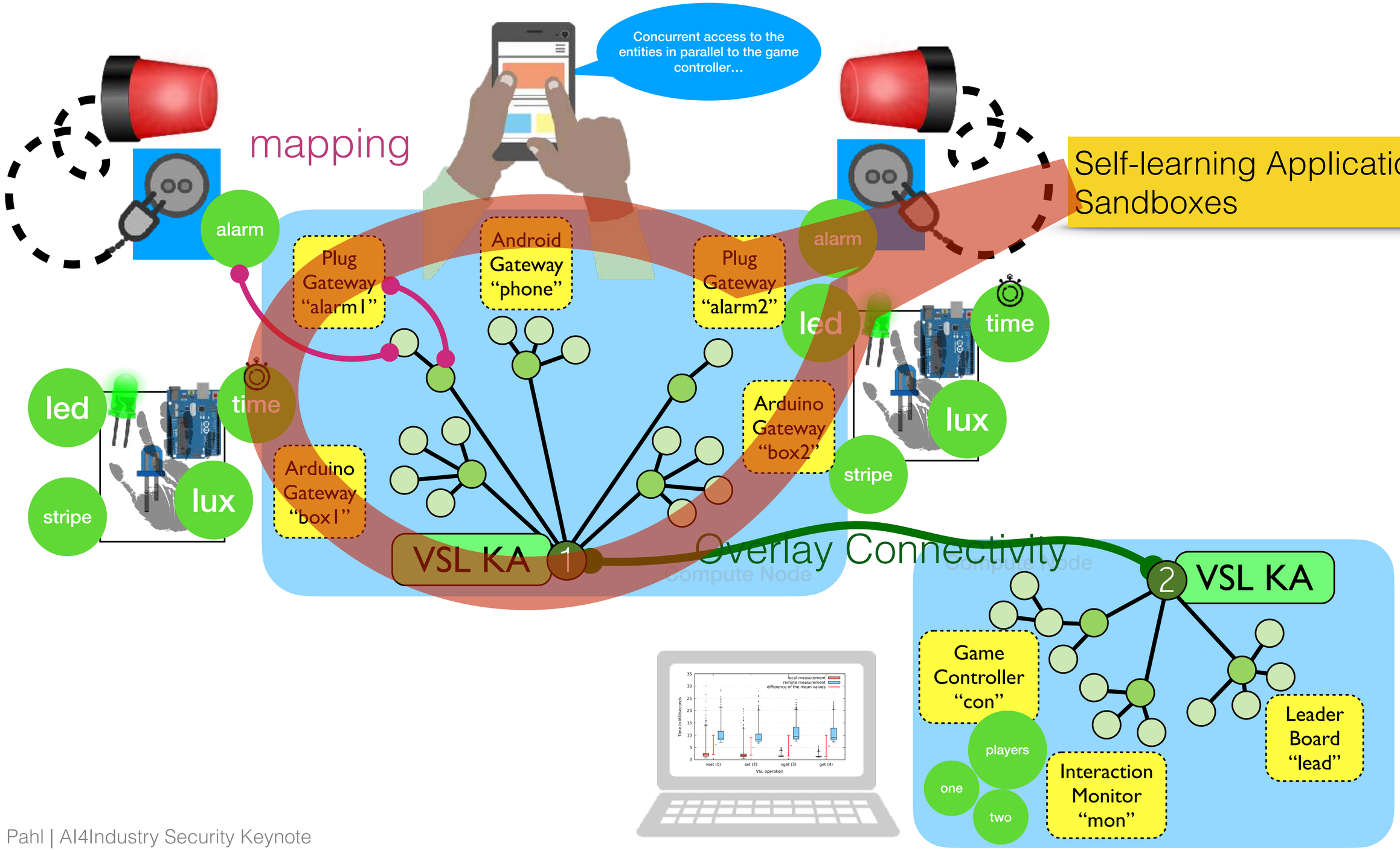
Physical World



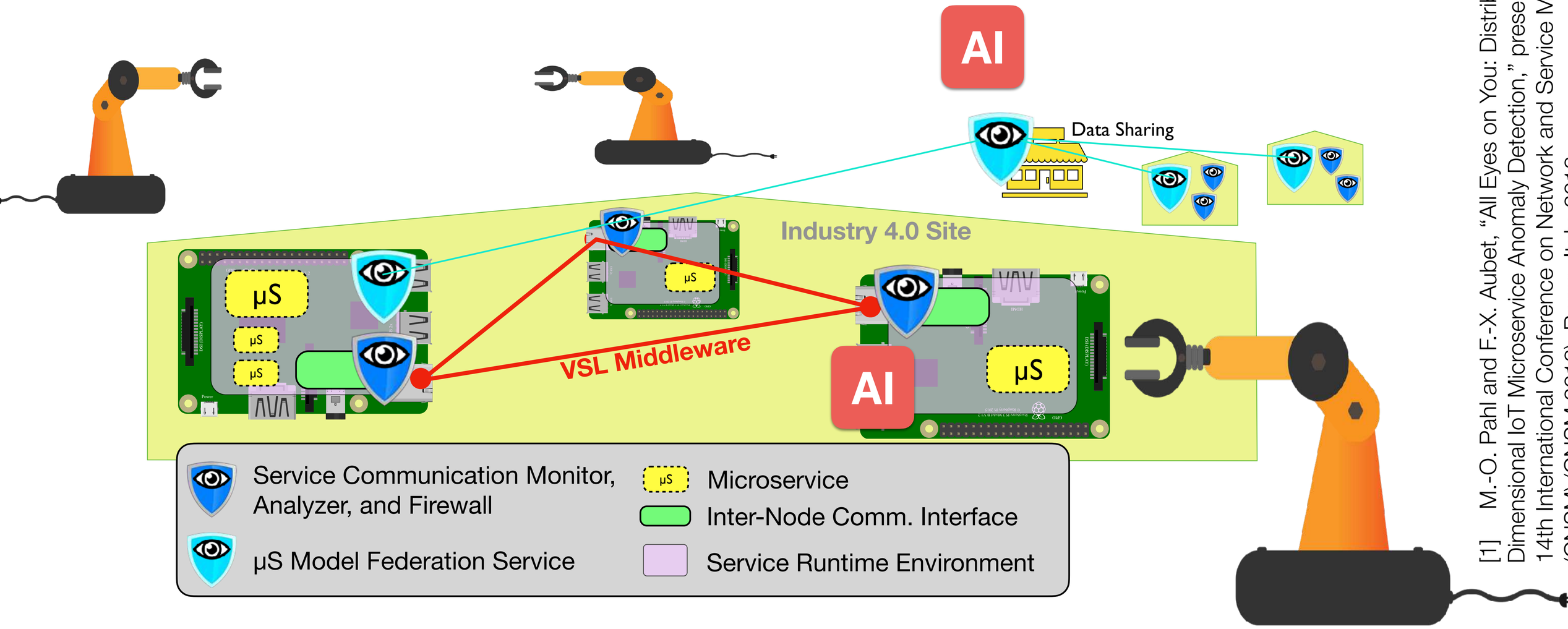
II. *Detect & Mitigate -> Prevent in the Future*
Machine-Learning-based **Modeling** and **Sandboxing** using **Anomaly Detection**

chairecyber-cni.org/

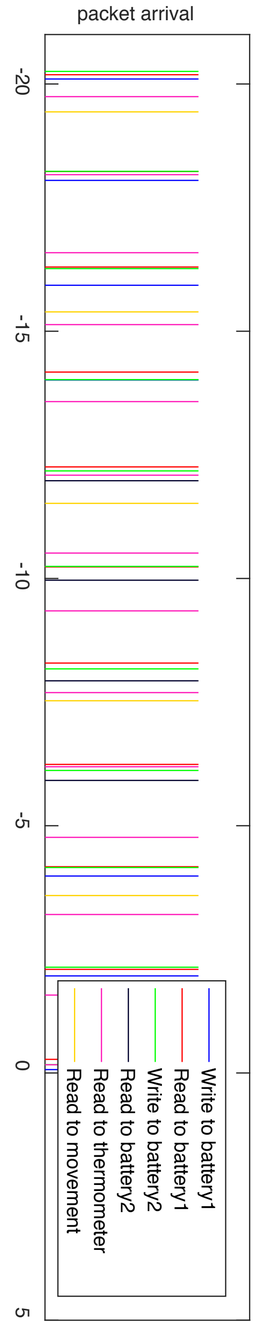
Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)


Concurrent access to the entities in parallel to the game controller…
mapping
Self-learning Application Sandboxes
alarm
Plug Gateway "alarm1"
Android Gateway "phone"
Plug Gateway "alarm2"
alarm
led
time
lux
stripe
led
time
lux
stripe
Arduino Gateway "box1"
Arduino Gateway "box2"
VSL KA
1
Overlay Connectivity
Compute Node
Compute Node
2
VSL KA
Game Controller "con"
players
one
two
Interaction Monitor "mon"
Leader Board "lead"
local measurement
remote measurement
difference of the mean values
Time in Milliseconds
VSL operation
vset (1)
set (2)
vget (3)
get (4)

Synthesis of Distributed Observations



[1] M.-O. Pahl and F.-X. Aubet, "All Eyes on You: Distributed Multi-Dimensional IoT Microservice Anomaly Detection," presented at the 2018 14th International Conference on Network and Service Management (CNSM) (CNSM 2018), Rome, Italy, 2018.



Approach in a 

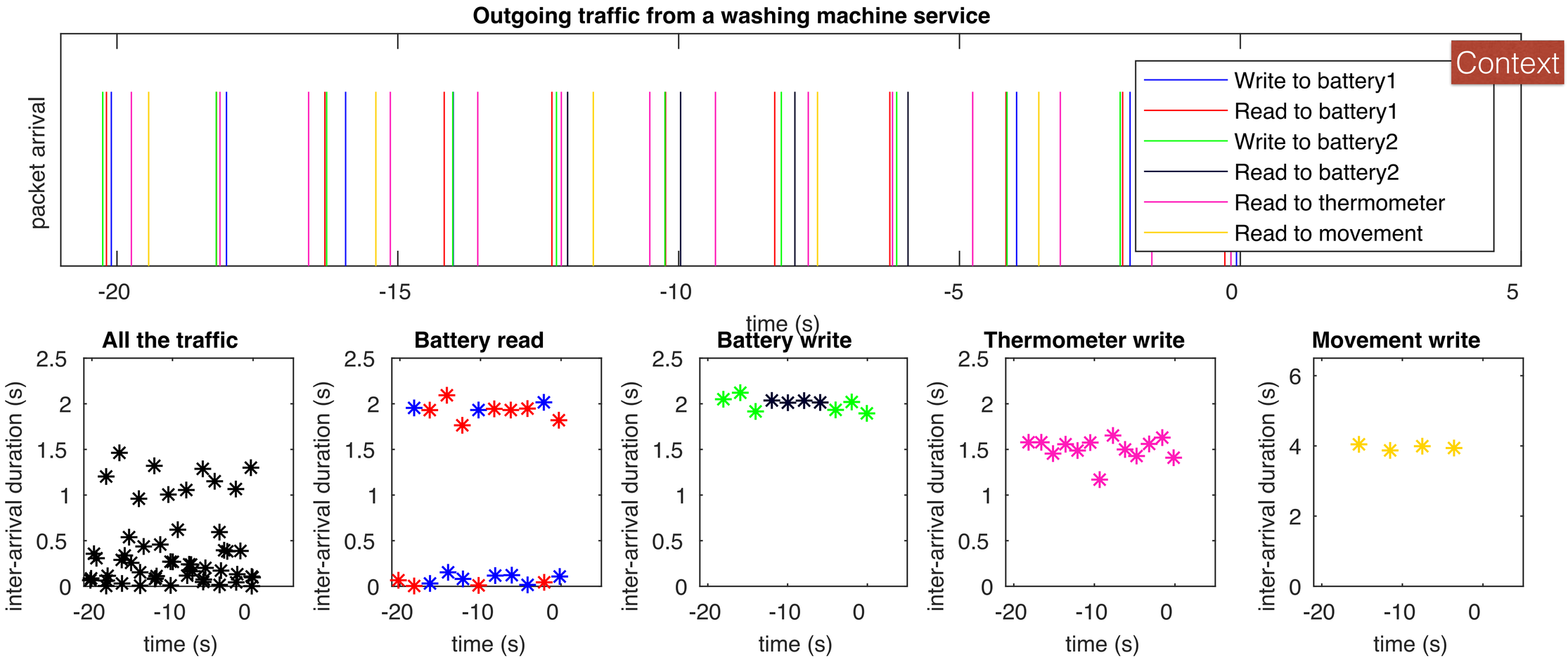
- Blackbox assumption
- Passive traffic monitoring
- Behavior modeling using Machine Learning
- Anomaly detection
- Firewalling

Prevent
Security-by-Design

Detect
Anomaly Detection

Mitigate
Self-Defend Security Incidents
Self-Recover from Security Incide

ML-Based Clustering of Periodicities



People

Interface Devices

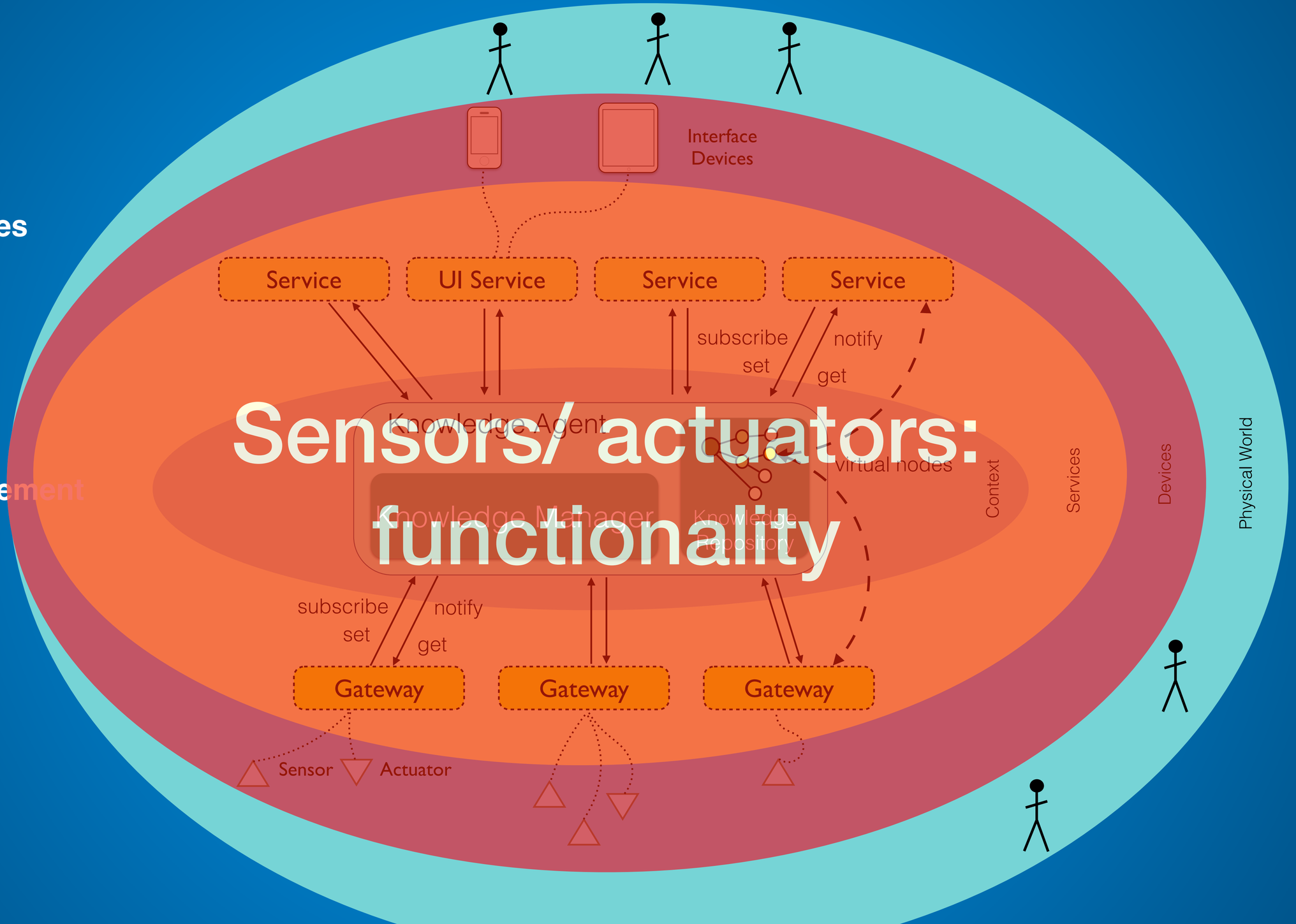
Orchestration
Workflows, etc.

Context Management

Bidirectional
Adaptation

Heterogeneous
Smart Devices

Physical World



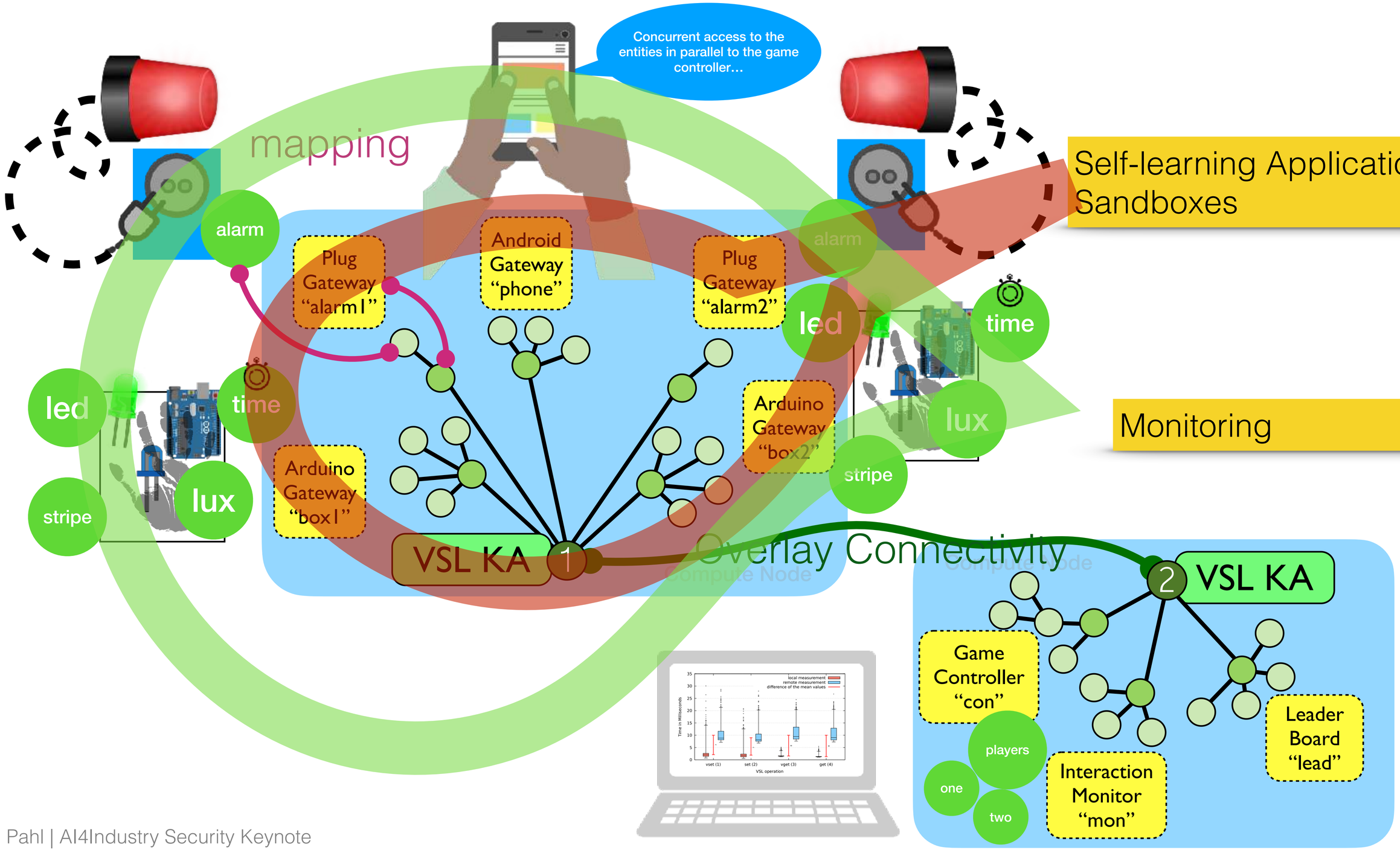
Sensors/ actuators: functionality

III. *Protect SW & HW*

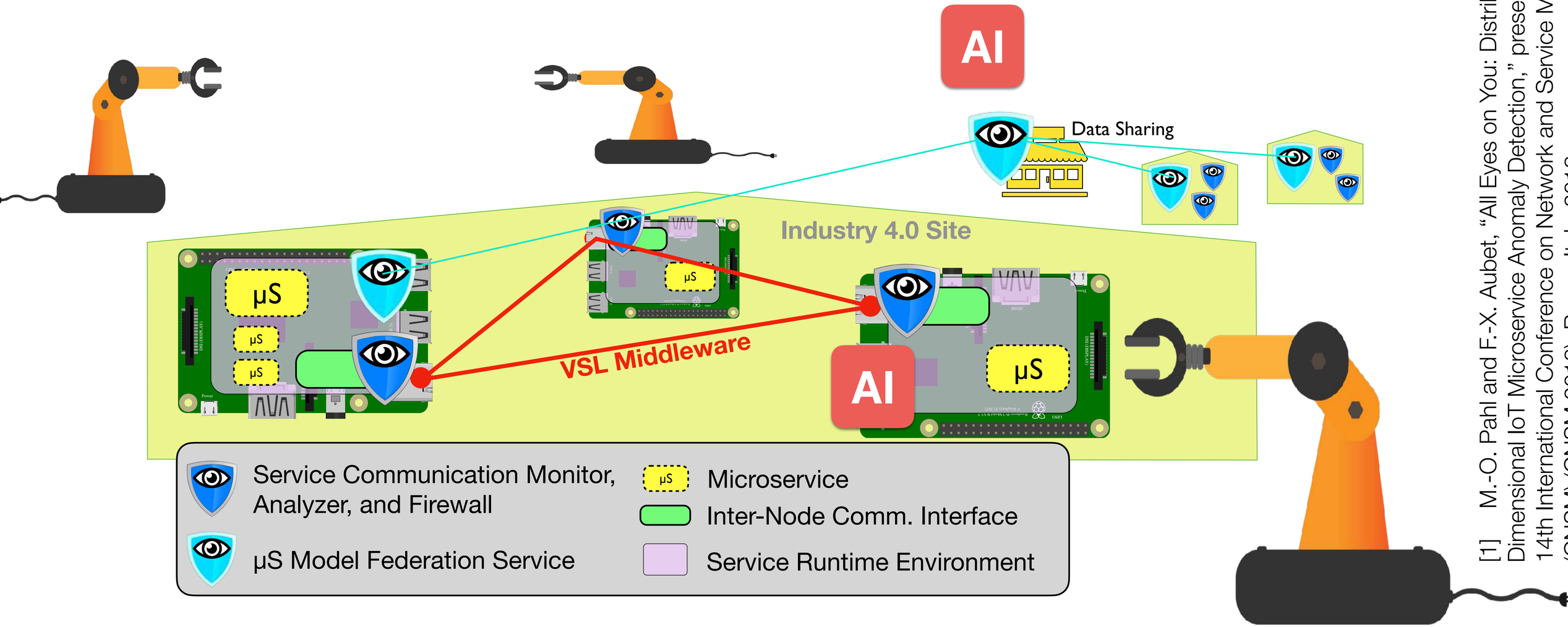
Anomaly Detection and Sandboxing, Watermarking

chairecyber-cni.org/

Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)


Concurrent access to the entities in parallel to the game controller…
mapping
alarm
Plug Gateway "alarm1"
Android Gateway "phone"
Plug Gateway "alarm2"
alarm
led
time
lux
stripe
led
time
lux
stripe
Arduino Gateway "box1"
Arduino Gateway "box2"
VSL KA
1
Overlay Connectivity
Compute Node
Compute Node
2
VSL KA
Game Controller "con"
players
one
two
Interaction Monitor "mon"
Leader Board "lead"
local measurement
remote measurement
difference of the mean values
Time in Milliseconds
vset (1)
set (2)
vget (3)
get (4)
VSL operation
Self-learning Application Sandboxes
Monitoring

Synthesis of Distributed Observations



[1] M.-O. Pahl and F.-X. Aubet, "All Eyes on You: Distributed Multi-Dimensional IoT Microservice Anomaly Detection," presented at the 2018 14th International Conference on Network and Service Management (CNSM) (CNSM 2018), Rome, Italy, 2018.

People

Interface Devices

Orchestration
Workflows, etc.

Context Management

Bidirectional
Adaptation

Heterogeneous
Smart Devices

Physical World

How China is building an all-seeing surveillance state
Washington Post
Published on 7 Jan 2018
https://www.youtube.com/watch?v=uReVvICTrCM

“We knew the world would not be the same. A few people laughed, a few people cried. Most people were silent. I remembered the line from the Hindu scripture, the Bhagavad-Gita; Vishnu is trying to persuade the Prince that he should do his duty, and to impress him, takes on his multi-armed form and says, '**Now I am become Death, the destroyer of worlds.**' I suppose we all thought that, one way or another.”

— J. Robert Oppenheimer (Researcher/ Head Manhatten Project)

Picture Openheimer: Department of Energy, Office of Public Affairs - Taken from a Los Alamos publication (*Los Alamos: Beginning of an era, 1943-1945*, Los Alamos Scientific Laboratory, 1986)

CHAIR OF

CYBERCNI

Critical National Infrastructures

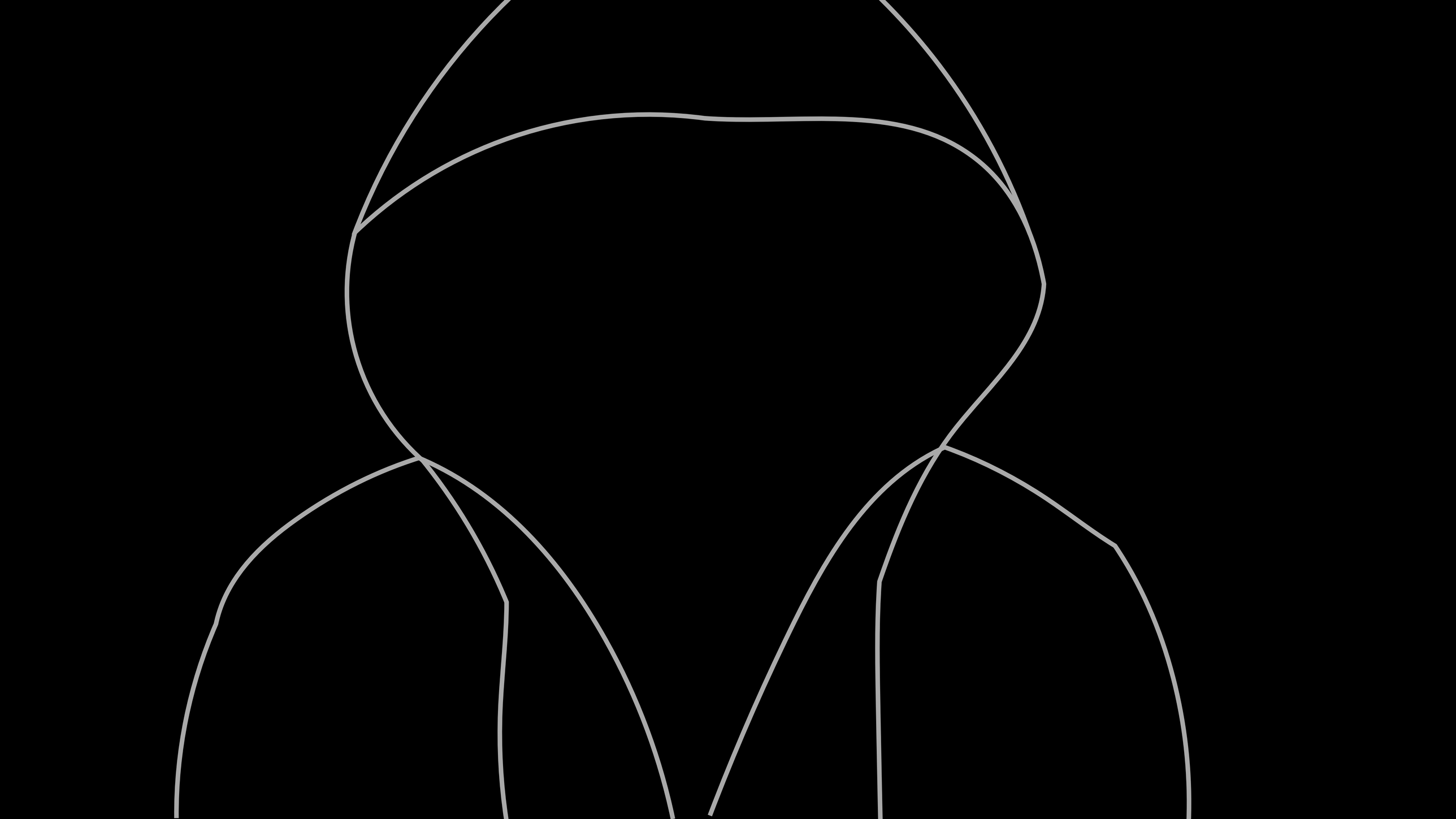
You are always welcome to contact us
for joint research / internship / speaker series / …

Unique concept with keynotes and challenges from our industry partners!

Oct 5-9, 2020
Strasbourg
Application open!

3rd Summer School Future-IoT: IoT meets Security

Oct 5-9, 2020, Strasbourg -> school.future-iot.org




Unique concept with keynotes and challenges from our industry partners!
Oct 5-9, 2020
Strasbourg
Application open!
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom
Technical University of Munich
german-french academy for the industry of the future
founded by IMT and TUM
INSTITUT CARNOT
Télécom & Société numérique
Université franco-allemande
Deutsch-Französische Hochschule
AIRBUS
DEFENCE & SPACE
amazon
arianeGROUP
Atos
elm.leblanc
SIEMENS
Ingenuity for life
Apply now!
school.future-iot.org

Cybersecurity of Critical Infrastructures

Some Methods

Blockchain

MACHINE LEARNING

Digital**Twin**

Prevent
Security-by-Design

Detect
Anomaly Detection

CHAIRE
CYBER CNI
Sécurité des infrastructures critiques
EST. 2016

Mitigate
Self-Defend Security Incidents
Self-Recover from Security Incidents

Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)

AIRBUS AMOSSYS BNP PARIBAS EDF NOKIA Bell Labs