black hat®
USA 2019

AUGUST 3-8, 2019

MANDALAY BAY / LAS VEGAS

#BHUSA @BLACK HAT EVENTS

Sensor and Process Fingerprinting in Industrial Control Systems

Martín Ochoa
Cyxtera Technologies

Mujeeb Chuadhry
Singapore University of Technology and Design

Bio

Martín:

- Head of Research, Cyxtera TFP
- Previously Assistant Professor in Bogotá and SUTD, Singapore.
- Ph.D. in CS, background in Math and Systems Engineering.
- Interested in software and systems security applications to ICS, IoT.

Mujeeb:

- Ph.D. student at SUTD in Singapore.
- Thesis on sensor fingerprinting in ICS.
- Background in Electronic Engineering.

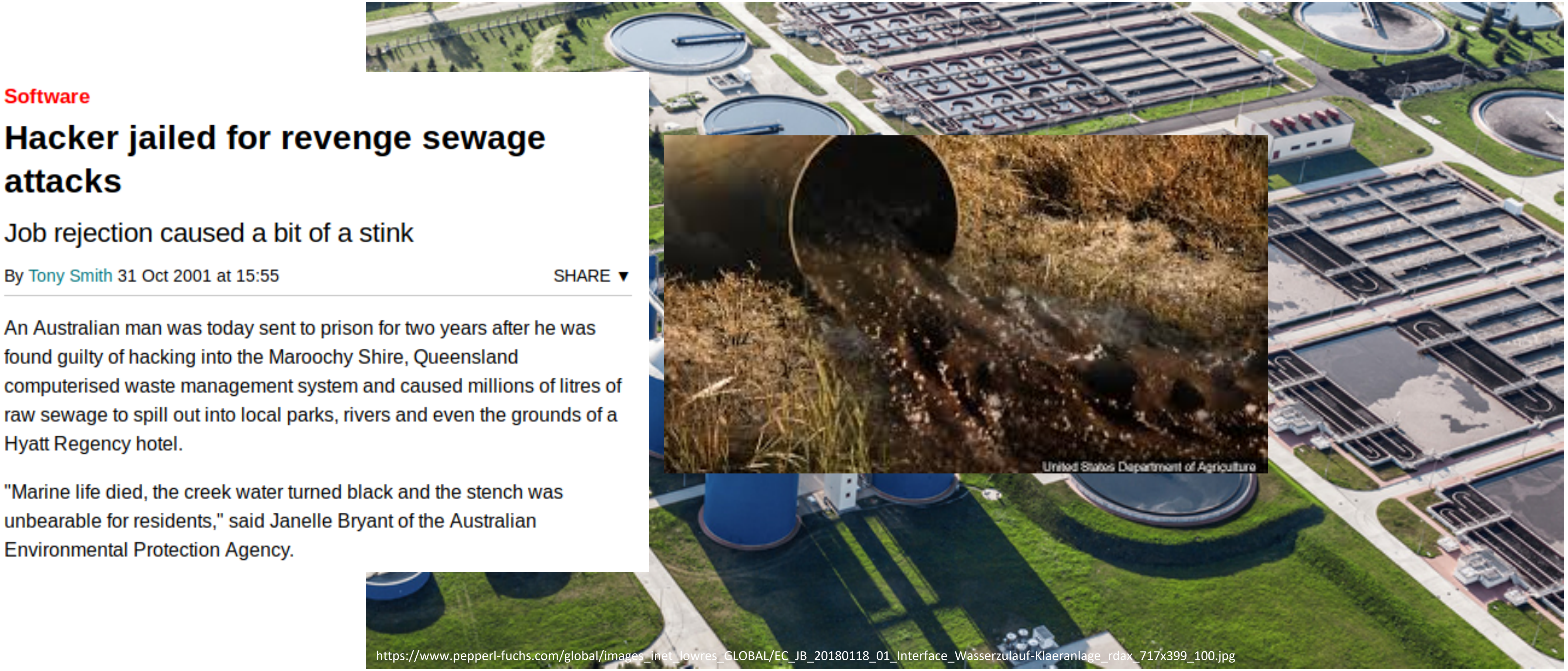
Cyxtera

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust Centre for Research in Cyber Security

ICS Security is important

Water also...



Software

Hacker jailed for revenge sewage attacks

Job rejection caused a bit of a stink

By Tony Smith 31 Oct 2001 at 15:55 SHARE ▼

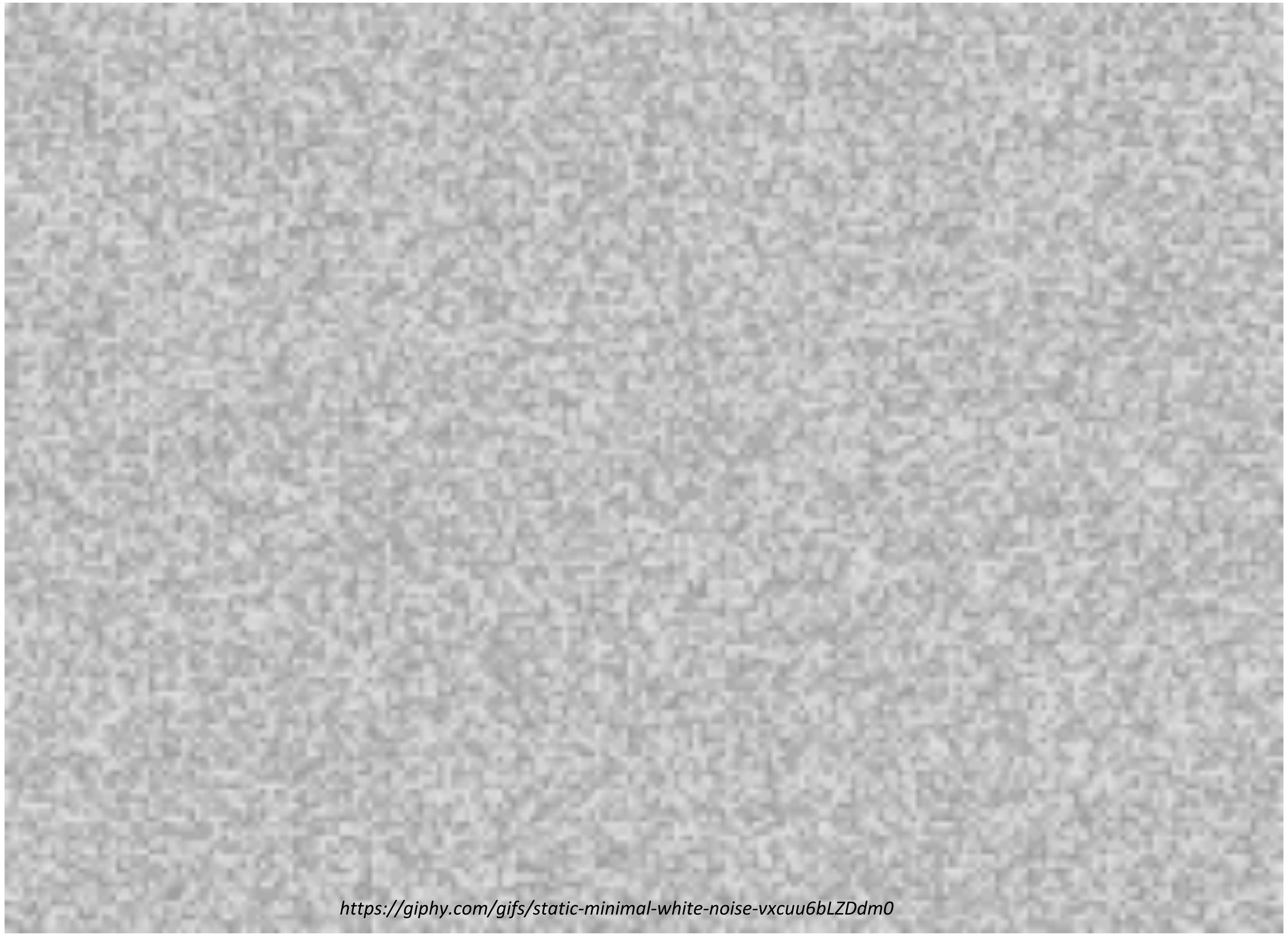
An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

"Marine life died, the creek water turned black and the stench was unbearable for residents," said Janelle Bryant of the Australian Environmental Protection Agency.

United States Department of Agriculture

https://www.pepperl-fuchs.com/global/images_inet_lowres_GLOBAL/EC_JB_20180118_01_Interface_Wasserzulauf-Klaeranlage_rdax_717x399_100.jpg

Noise is bad...

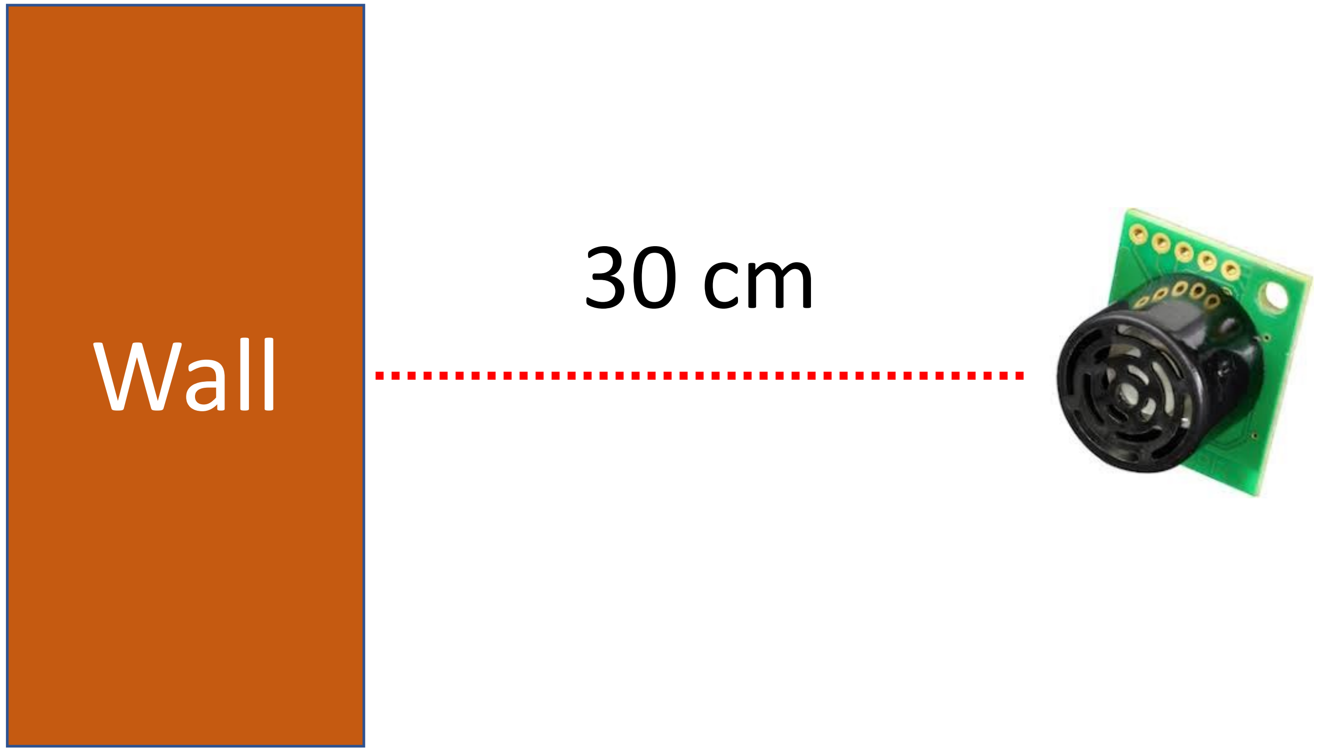


https://giphy.com/gifs/static-minimal-white-noise-vxcuu6bLZDdm0

Noise is good!

https://thewatchman.com.au/2018/05/20/deadpool-2-can-you-love-a-dumpster-fire/

What kind of noise?



Wall

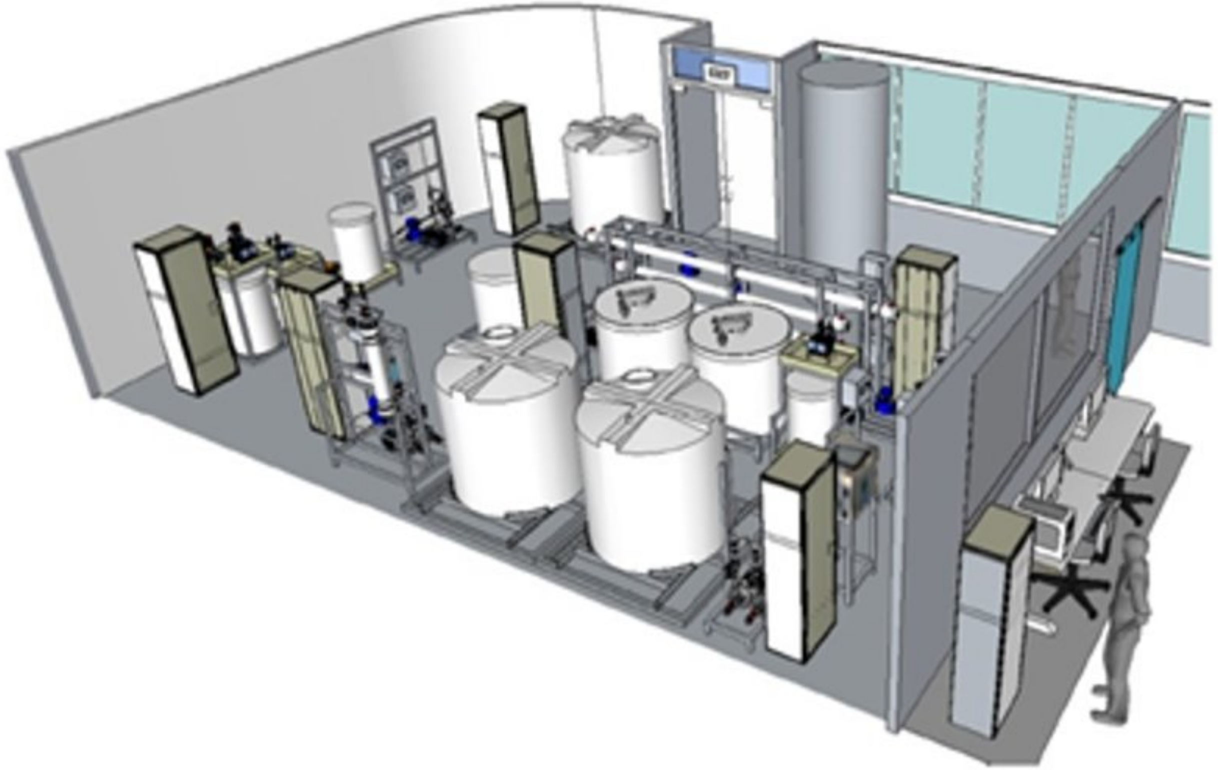
30 cm

Measured values

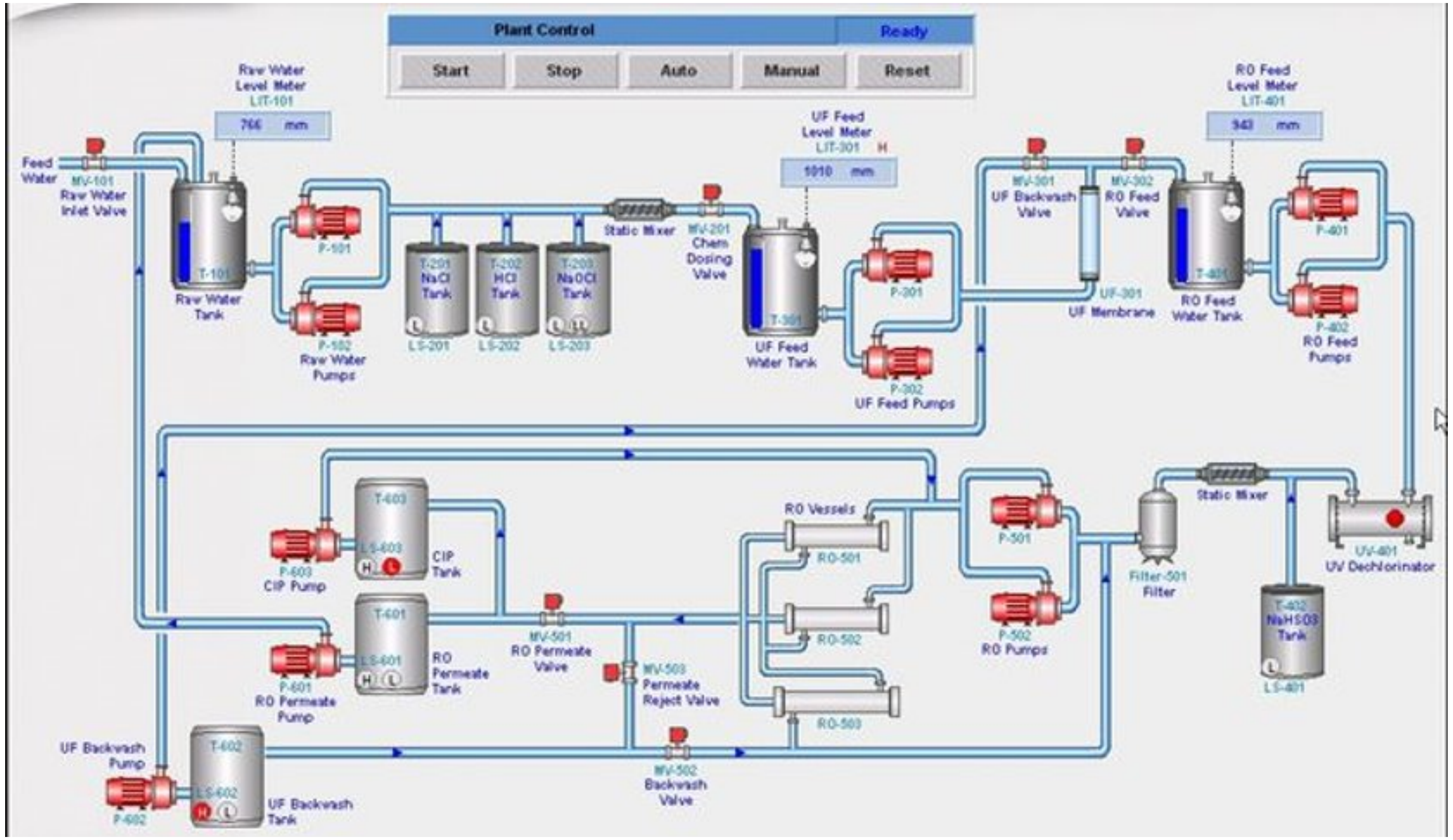
Timestamp	Values
0	30.541212341
1	30.481231303
2	30.521231290
3	30.342305190
4	30.560392148
5	30.531091240
6	30.494756191

Talk outline

1. An ICS testbed (SWaT)
2. Cyber/Physical attacks on SWaT
3. How to detect attacks?
4. How to detect attacks using sensor and process noise?
5. Discussion



Secure Water Treatment Testbed (SWaT)

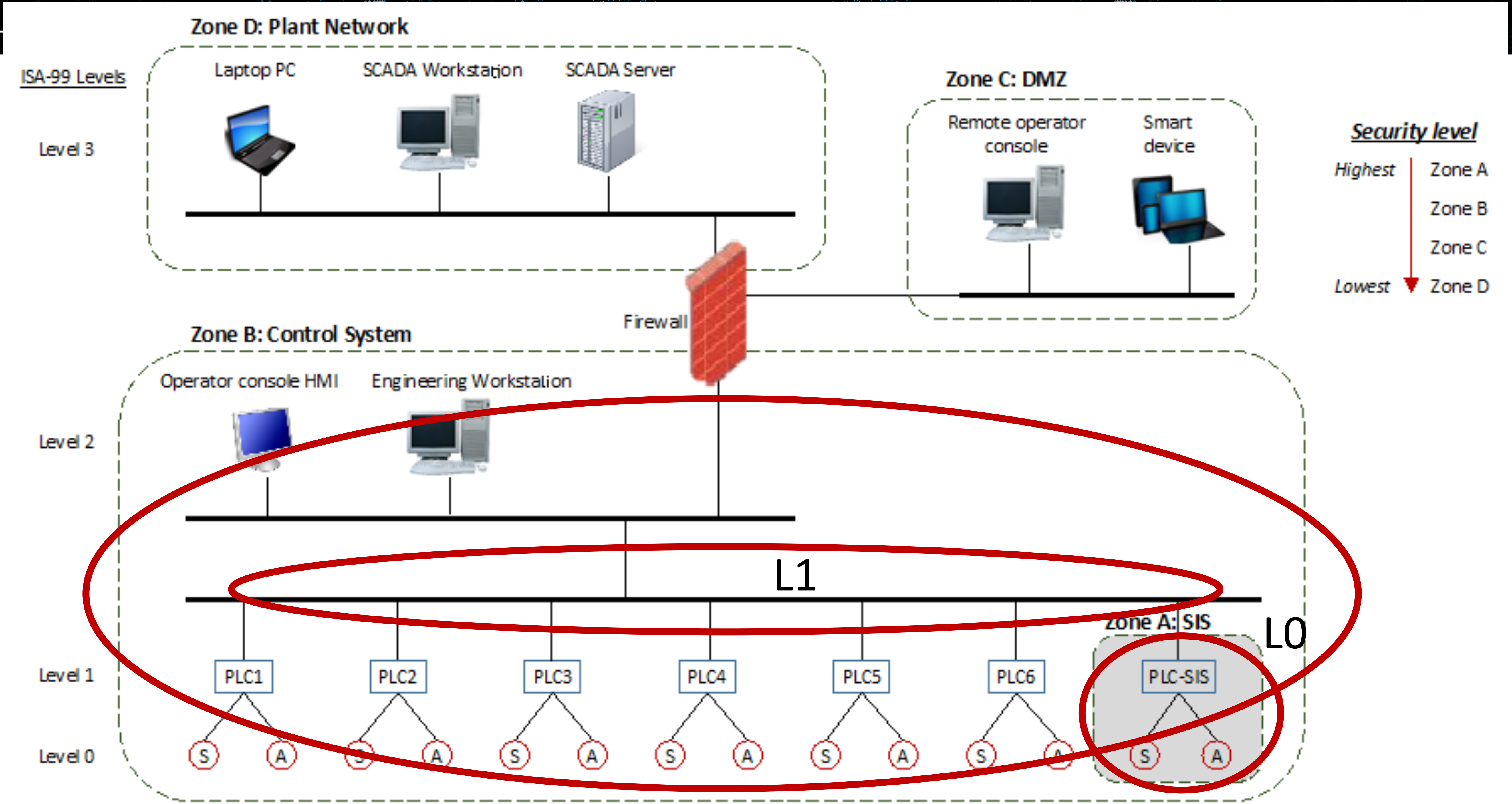


- Water treatment testbed for security research since 2015.
- 6 stages of processing (including UV, chemical treatment)

https://itrust.sutd.edu.sg/itrust-labs-home/itrust-labs_swat/

SWaT overview video

Network overview



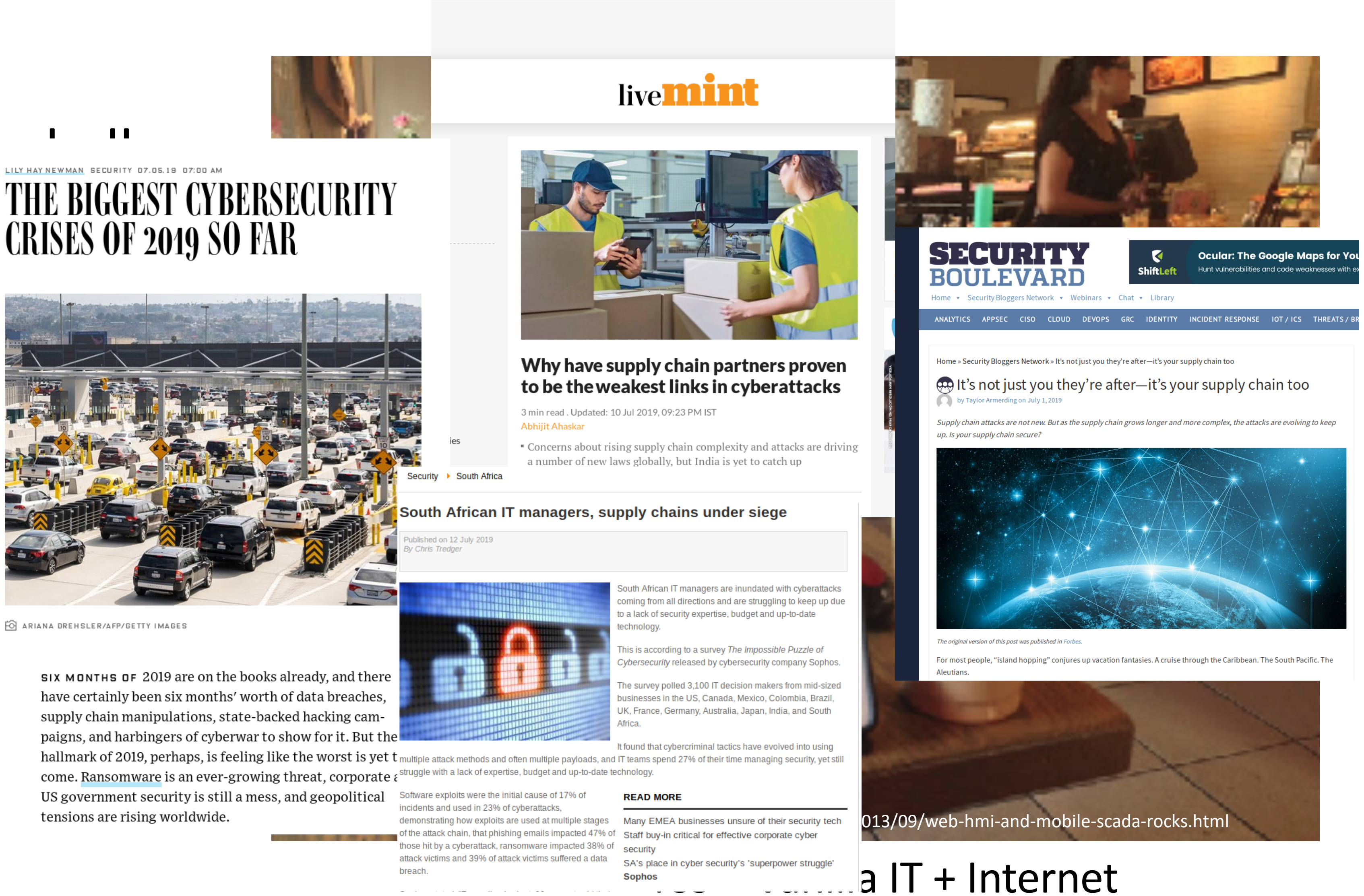
IF WE PROTECT THE PERIMETER
THAT'D BE GREAT
imgflip.com

https://looneytunes.fandom.com/wiki/That%27s_all_Folks

Thanks! Questions?

Why we need defense in depth in ICS

- Multiple advanced attack vectors tha
  traditional IT security views.
    - Insider threats
    - Insecure Updates
    - Supply chain attacks
- <u>Lack of authentication</u> in L1 and L0!
  (field network/protocols)



LILY HAY NEWMAN SECURITY 07.05.19 07:00 AM

THE BIGGEST CYBERSECURITY CRISES OF 2019 SO FAR

ARIANA DREHSLER/AFP/GETTY IMAGES

SIX MONTHS OF 2019 are on the books already, and there have certainly been six months' worth of data breaches, supply chain manipulations, state-backed hacking campaigns, and harbingers of cyberwar to show for it. But the hallmark of 2019, perhaps, is feeling like the worst is yet t come. Ransomware is an ever-growing threat, corporate a US government security is still a mess, and geopolitical tensions are rising worldwide.

livemint

Why have supply chain partners proven to be the weakest links in cyberattacks

3 min read . Updated: 10 Jul 2019, 09:23 PM IST

Abhijit Ahaskar

- Concerns about rising supply chain complexity and attacks are driving a number of new laws globally, but India is yet to catch up

Security ▸ South Africa

South African IT managers, supply chains under siege

Published on 12 July 2019
By Chris Tredger

South African IT managers are inundated with cyberattacks coming from all directions and are struggling to keep up due to a lack of security expertise, budget and up-to-date technology.

This is according to a survey *The Impossible Puzzle of Cybersecurity* released by cybersecurity company Sophos.

The survey polled 3,100 IT decision makers from mid-sized businesses in the US, Canada, Mexico, Colombia, Brazil, UK, France, Germany, Australia, Japan, India, and South Africa.

It found that cybercriminal tactics have evolved into using multiple attack methods and often multiple payloads, and IT teams spend 27% of their time managing security, yet still struggle with a lack of expertise, budget and up-to-date technology.

Software exploits were the initial cause of 17% of incidents and used in 23% of cyberattacks, demonstrating how exploits are used at multiple stages of the attack chain, that phishing emails impacted 47% of those hit by a cyberattack, ransomware impacted 38% of attack victims and 39% of attack victims suffered a data breach.

READ MORE

Many EMEA businesses unsure of their security tech
Staff buy-in critical for effective corporate cyber security
SA's place in cyber security's 'superpower struggle'
Sophos

SECURITY BOULEVARD

ShiftLeft Ocular: The Google Maps for You
Hunt vulnerabilities and code weaknesses with ex

Home • Security Bloggers Network • Webinars • Chat • Library

ANALYTICS APPSEC CISO CLOUD DEVOPS GRC IDENTITY INCIDENT RESPONSE IOT / ICS THREATS / BR

Home » Security Bloggers Network » It's not just you they're after—it's your supply chain too

It's not just you they're after—it's your supply chain too

by Taylor Armerding on July 1, 2019

Supply chain attacks are not new. But as the supply chain grows longer and more complex, the attacks are evolving to keep up. Is your supply chain secure?

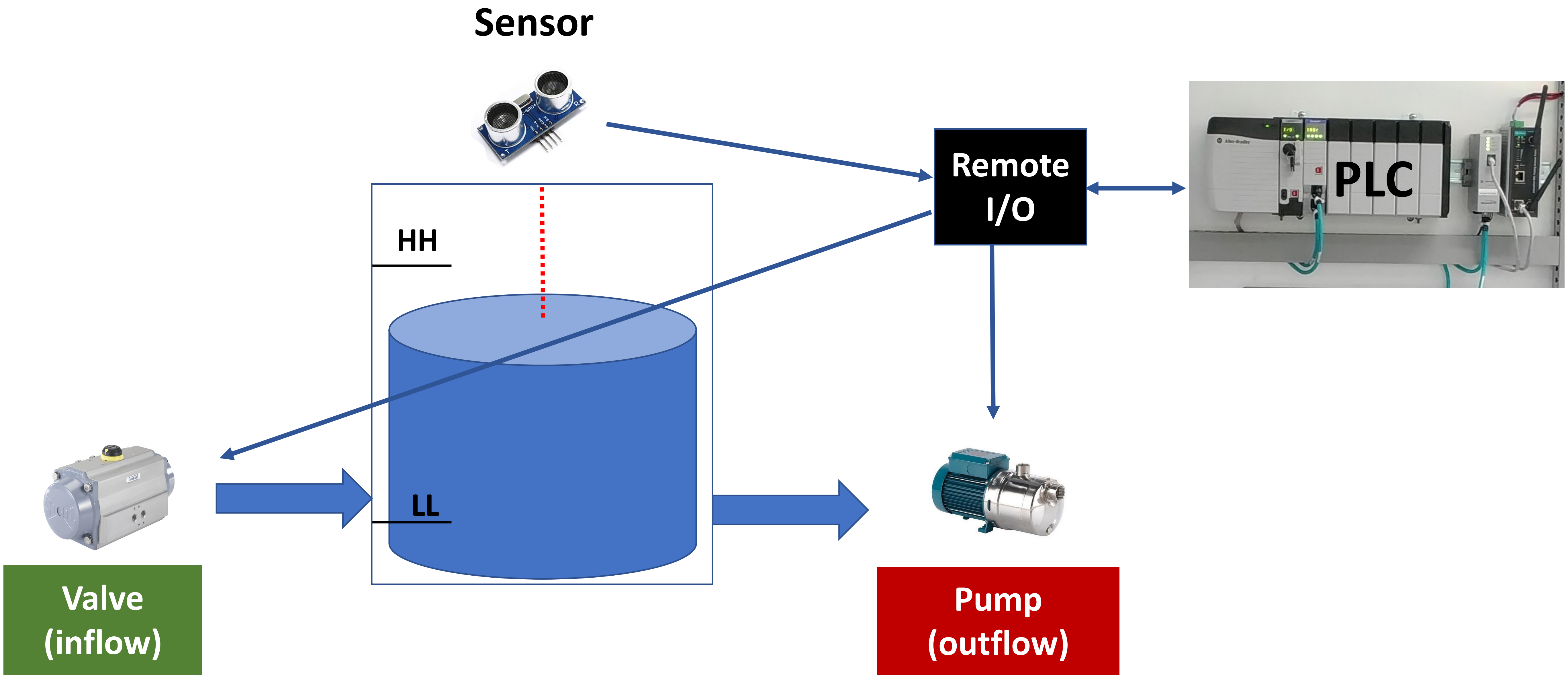
The original version of this post was published in Forbes.

For most people, "island hopping" conjures up vacation fantasies. A cruise through the Caribbean. The South Pacific. The Aleutians.

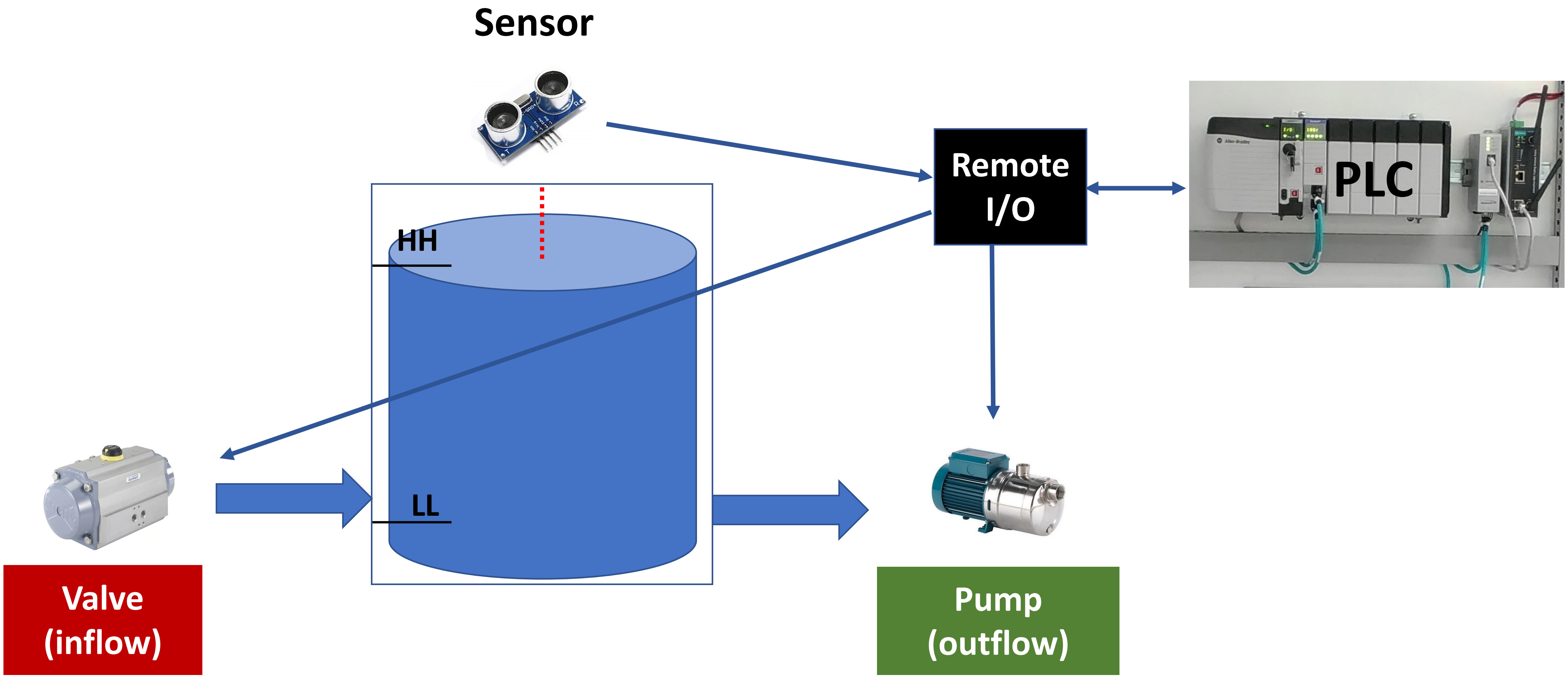
013/09/web-hmi-and-mobile-scada-rocks.html

a IT + Internet

How to control a water tank?

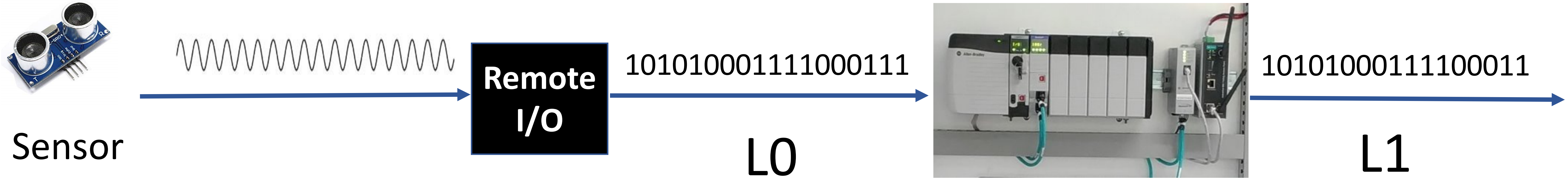


How to control a water tank?

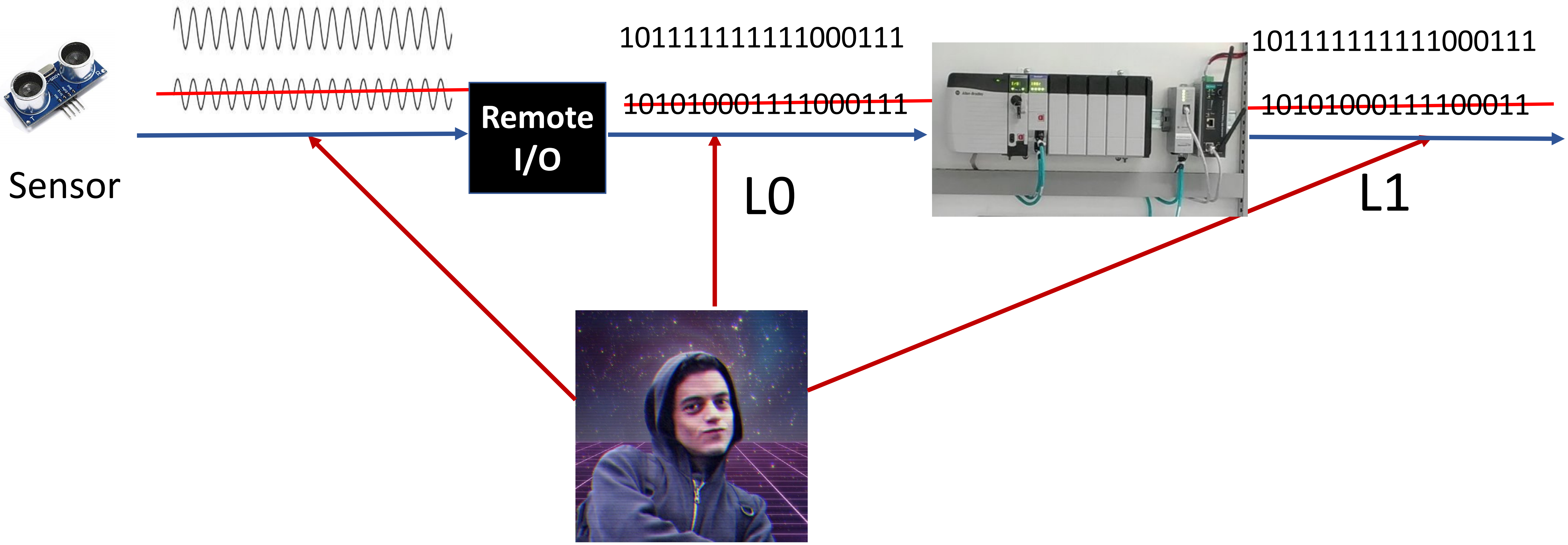


Attacks?

Authentication?



Authentication?



Sensor

Remote I/O

101111111111000111

~~101010001111000111~~

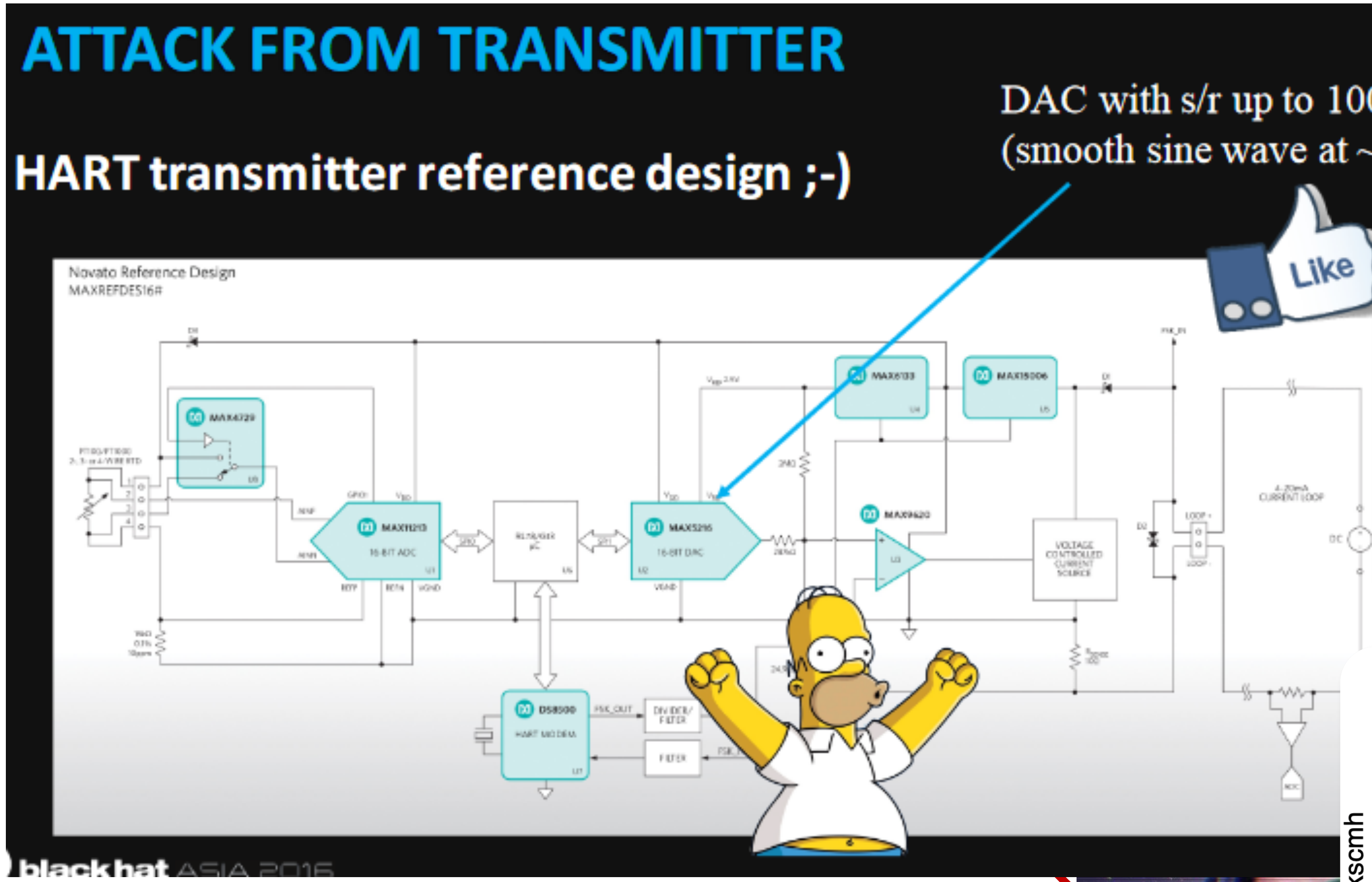
L0

101111111111000111

~~10101000111100011~~

L1

Attacker model



ATTACK FROM TRANSMITTER

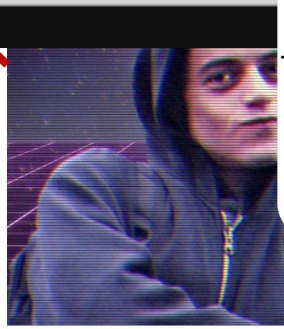
HART transmitter reference design ;-)

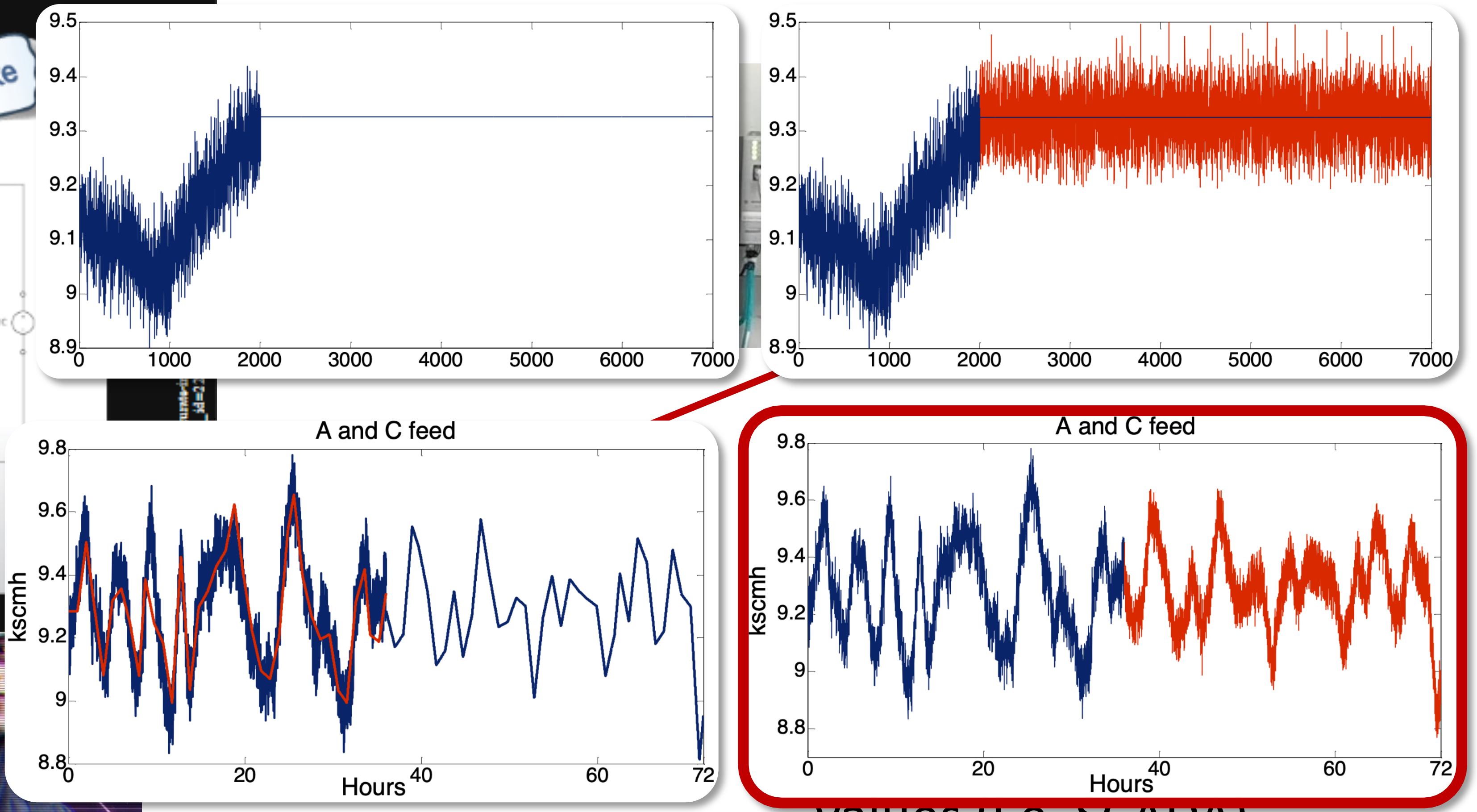
DAC with s/r up to 100kHz
(smooth sine wave at ~ 5kHz)

(hardware)

- Can manipulate analog/smart signal

[Bolshev et al. BH Asia 16]

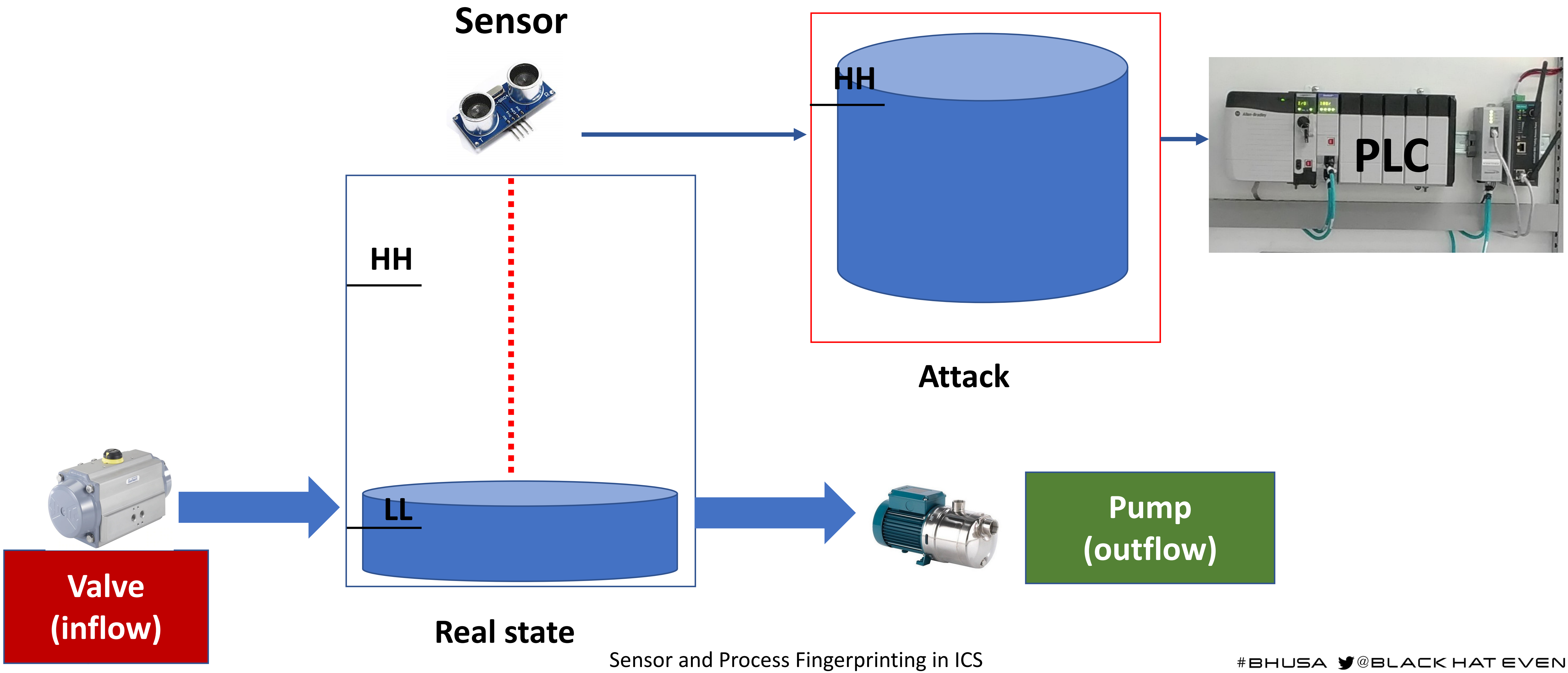




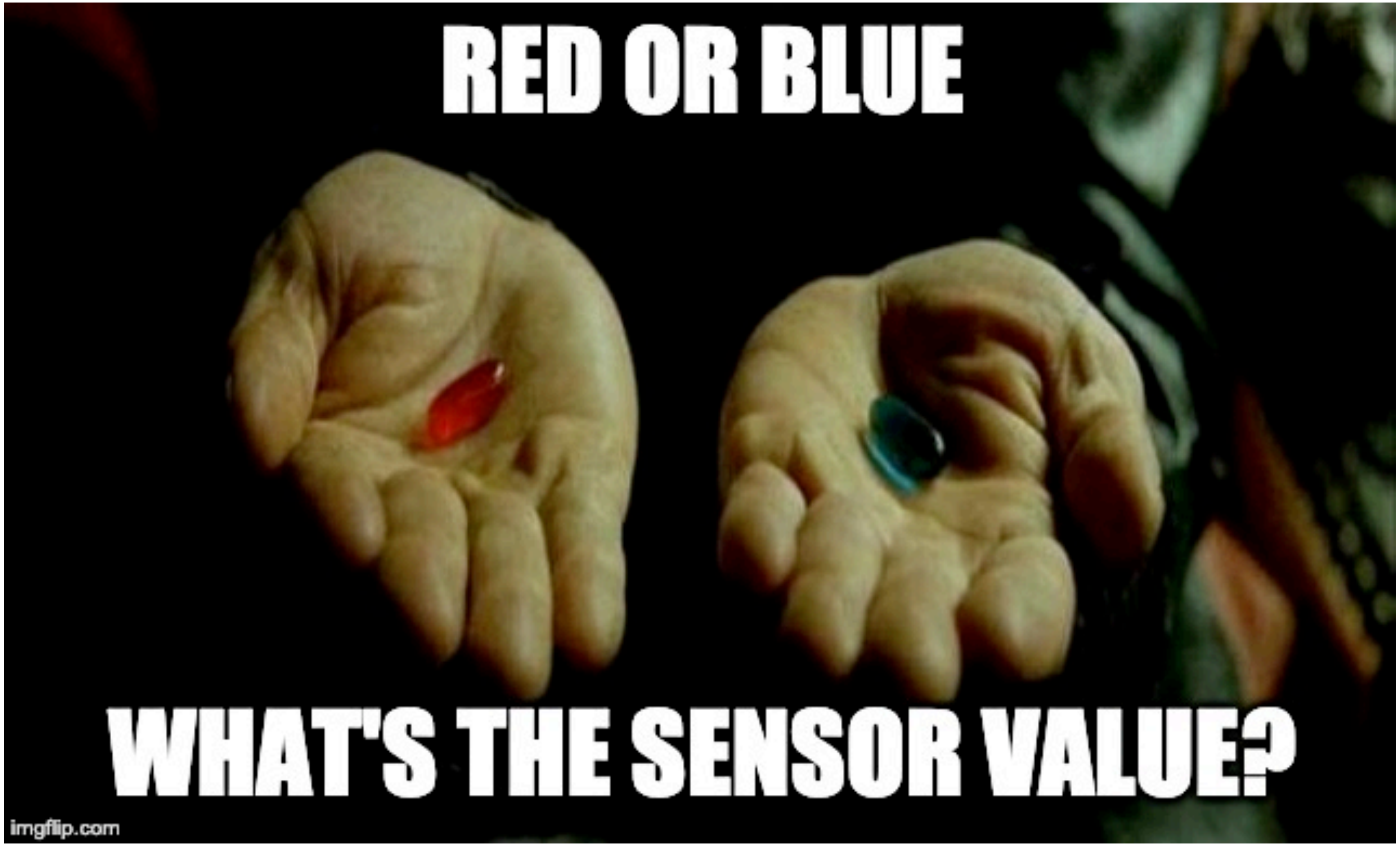
values (i.e. SCADA)

[Urbina et al. CCS 16]
[Krotofil et al. HITB 15]

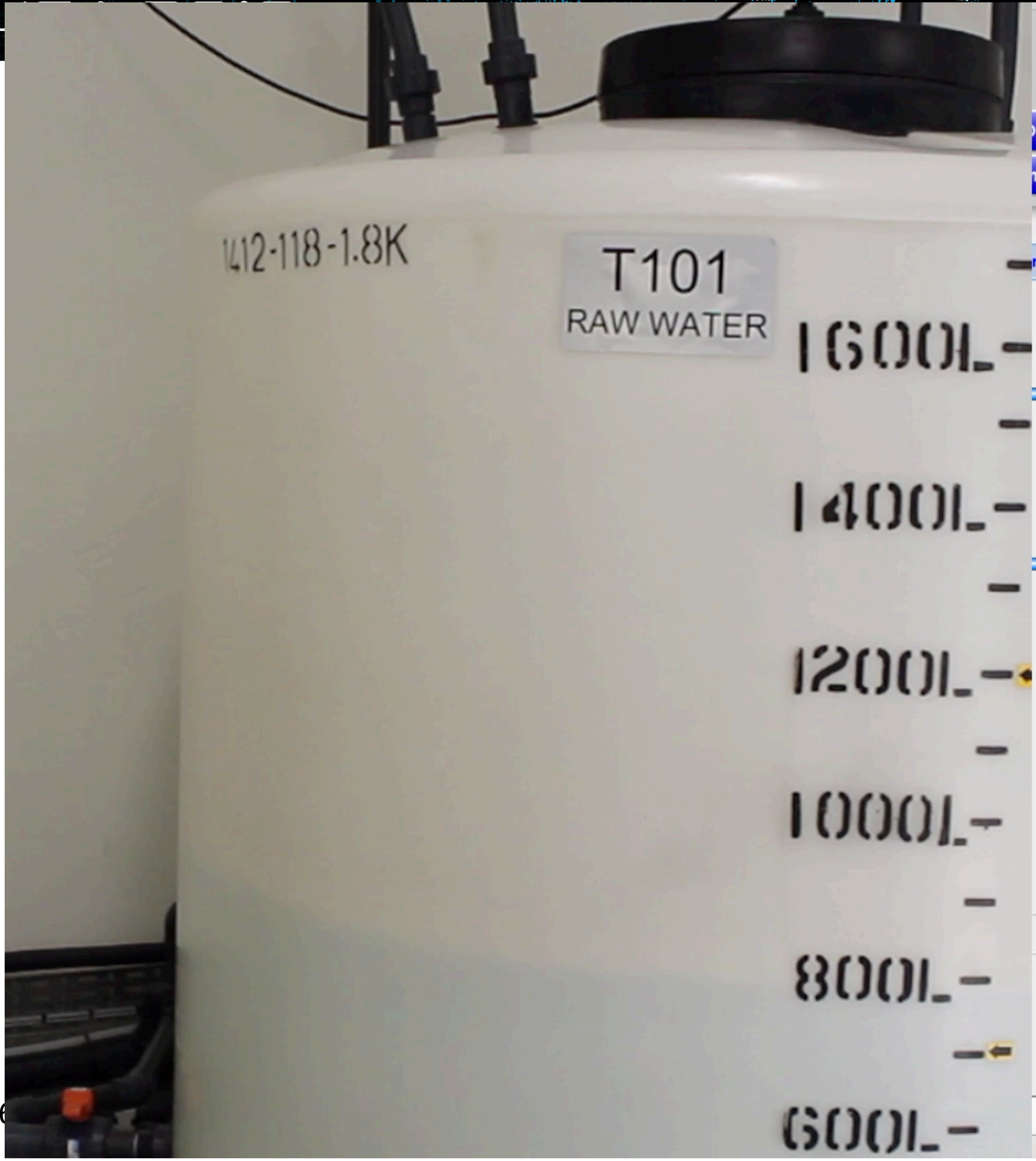
("Shameless") attack

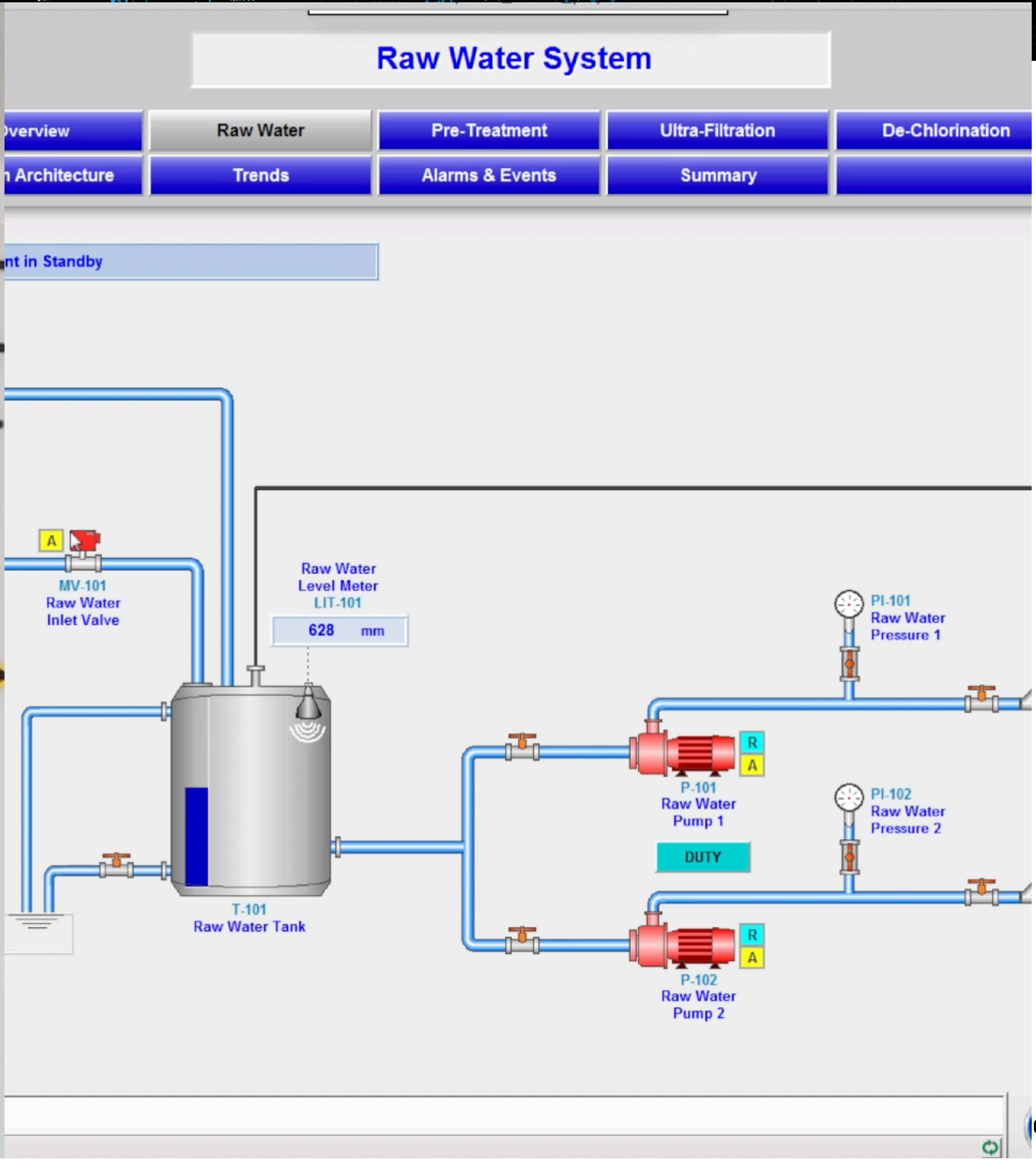


Data spoofing attacks



Video of data spoofing attack





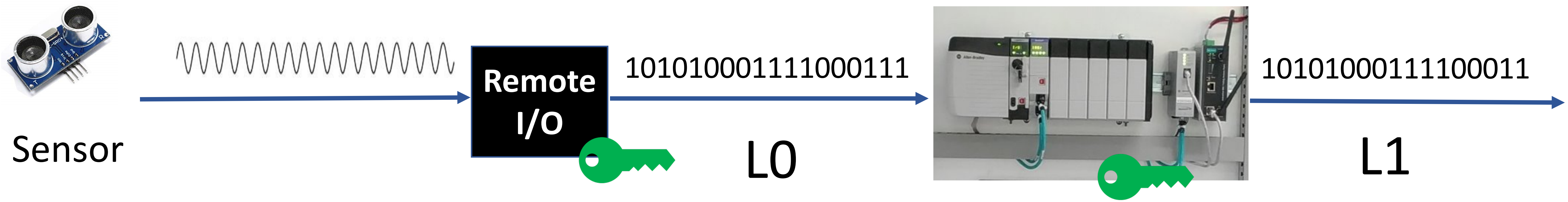
Defenses?

How to raise the bar against attacks?

- Use cryptographic primitives to authenticate data?
  - Cumbersome in legacy systems.
    - Computational resources are limited.
    - Not supported by industrial protocols.
  - Doesn't entirely solve the problem.
    - Analog data could already be malicious.
    - Cryptographic keys can be stolen.

https://shadowlakemusic.com/shop/indoor-percussion/raising-the-bar/

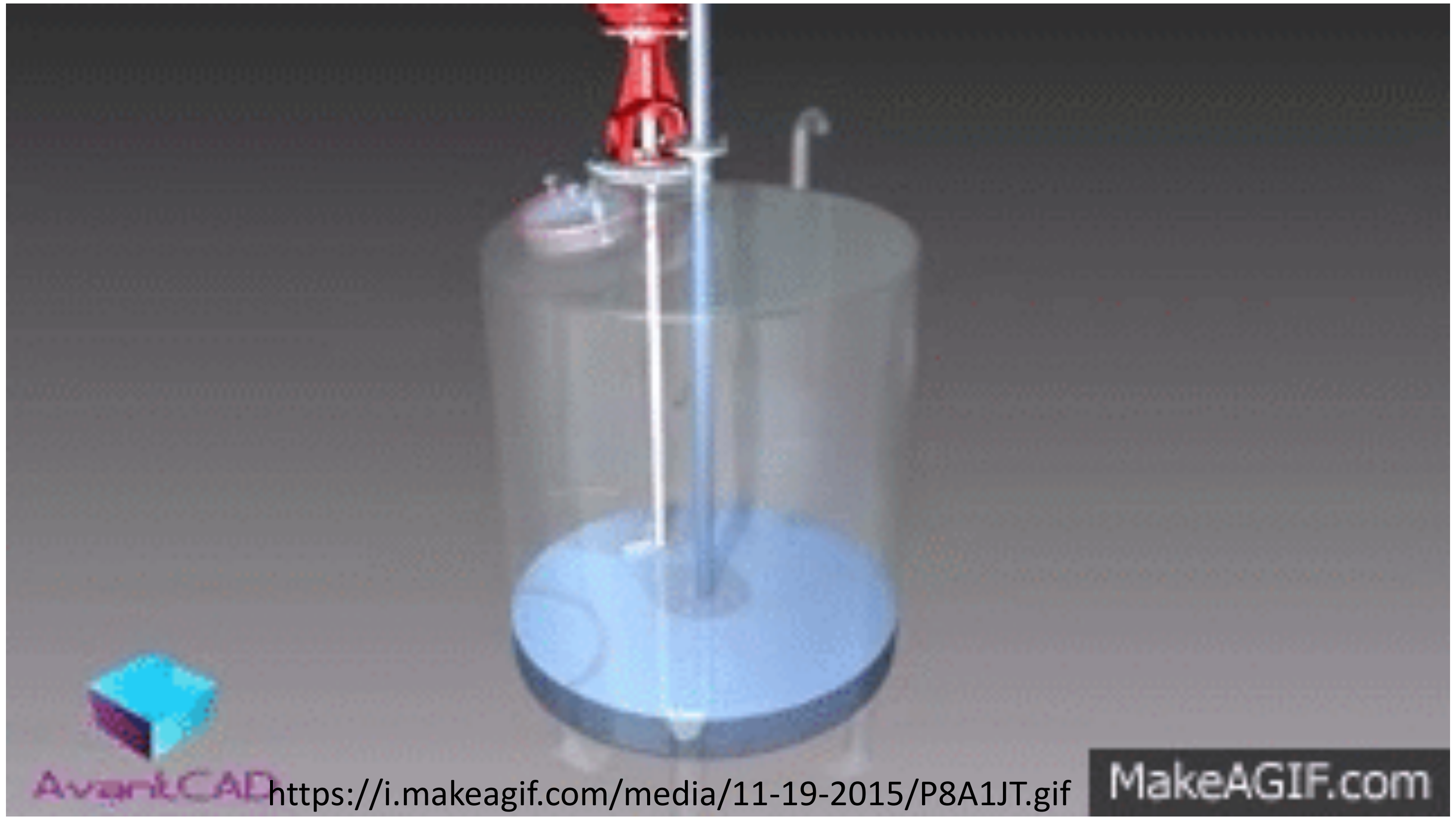
Authentication?



- Sensor data could already be malicious before authenticating.
- Keys can be stolen.

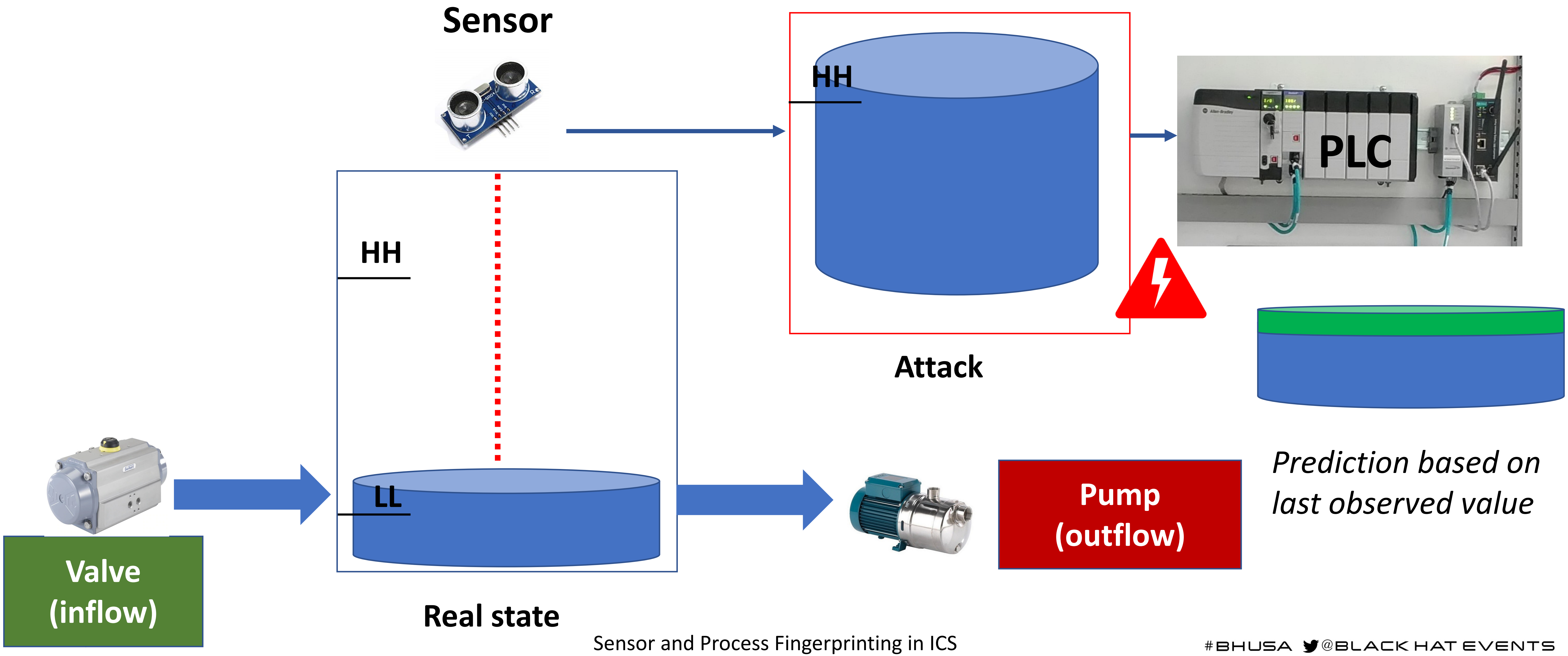
Model-based countermeasures

- Idea: a mathematical model of the process gives a "prediction" of future plant states.
  - If observation does not match the prediction, raise an alarm.



https://i.makeagif.com/media/11-19-2015/P8A1JT.gif

"Shameless" attack detection



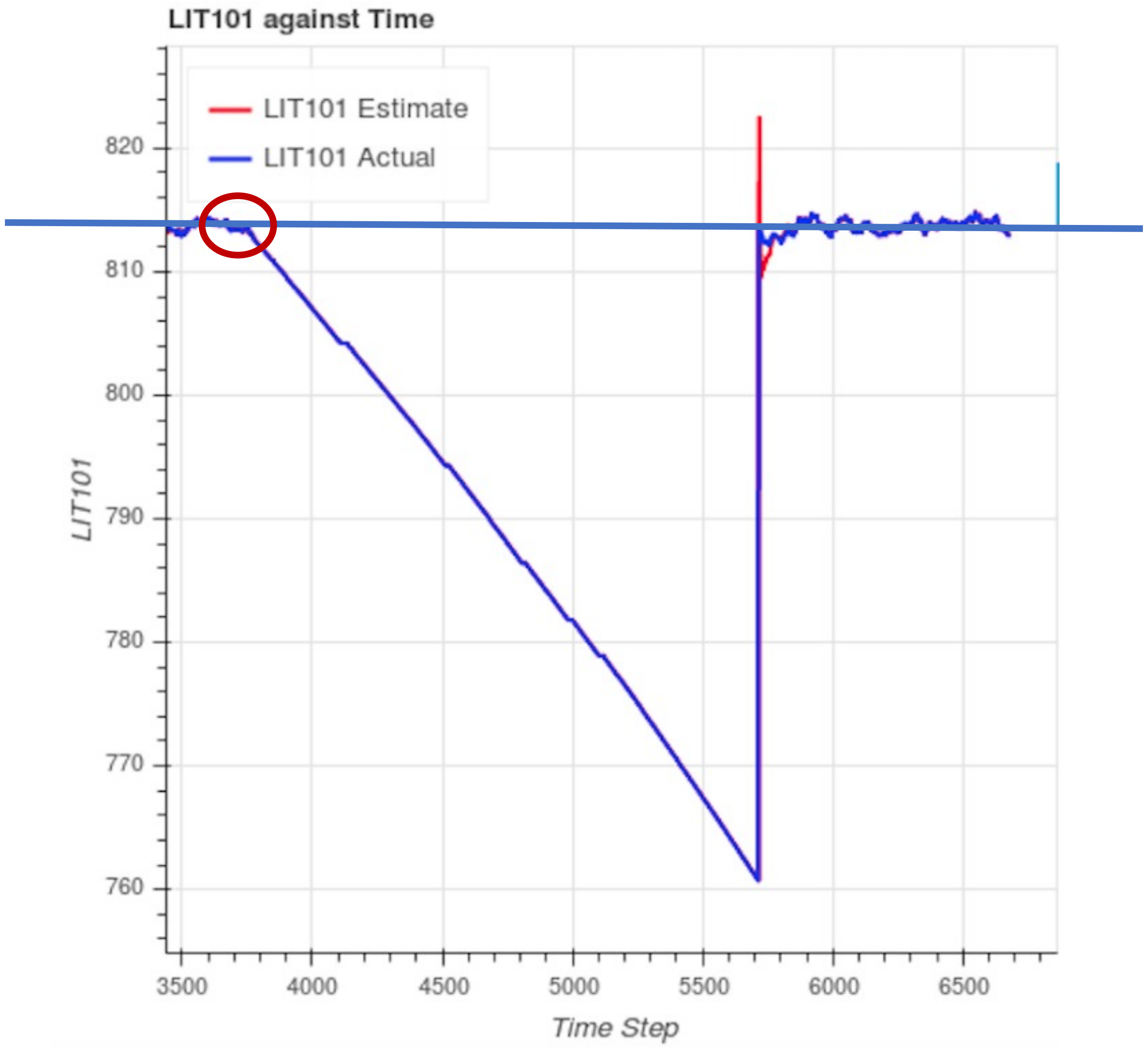
Prediction based on last observed value

Stealthy attacks

https://www.cinemaspartan.com/somewhere-oliver-stone-is-frowning-tropic-thunder/

Stealthy attacks

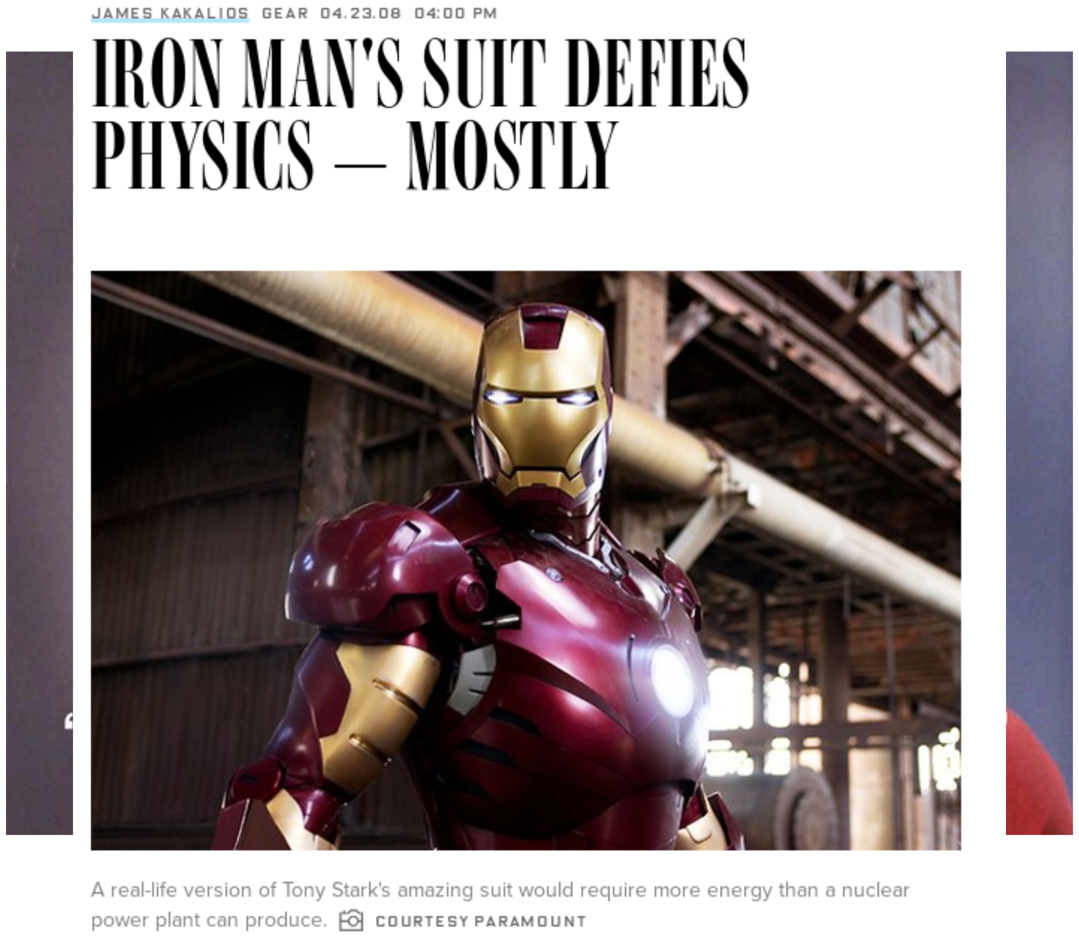
- Small deviations have a cumulative effect.
- Can bypass model-based countermeasures.



Physical invariants

- Idea: detect violations of laws of physics, i.e. pressure as a function of a water tank level. [Adepu et al. IFIP SEC 16]

- Shortcomings: hard to produce exhaustive invariant list for a system.



JAMES KAKALIOS GEAR 04.23.08 04:00 PM

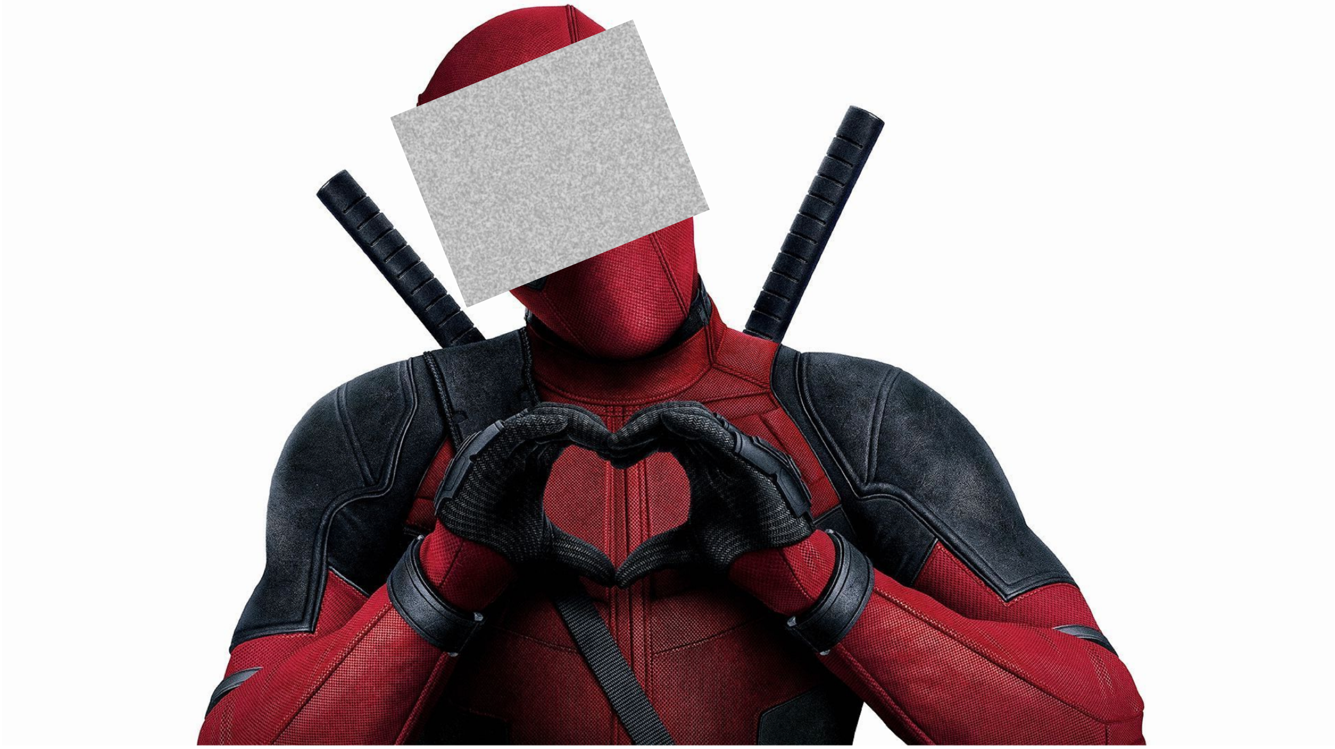
IRON MAN'S SUIT DEFIES PHYSICS — MOSTLY

A real-life version of Tony Stark's amazing suit would require more energy than a nuclear power plant can produce. COURTESY PARAMOUNT

Noise!

Come on, feel the noise

- Can we use sensor noise to fingerprint sensor values and address shortcomings of previous defenses?
  - Can we distinguish sensors of same type and brand?

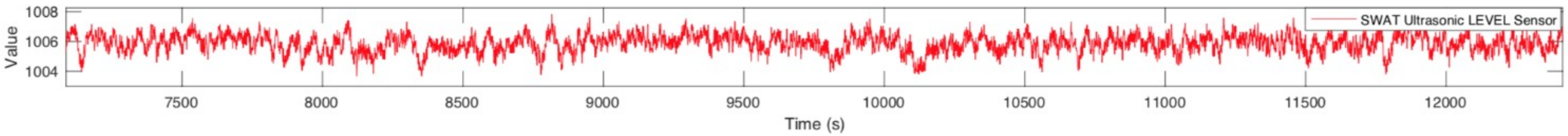


Our sensors

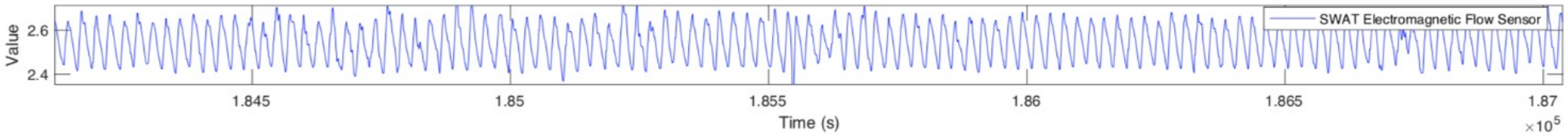
$1500 - $3000

Noise in different sensors

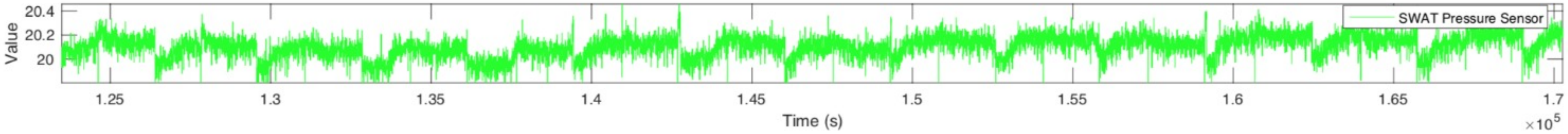
Ultrasonic Level Sensor (SWaT)



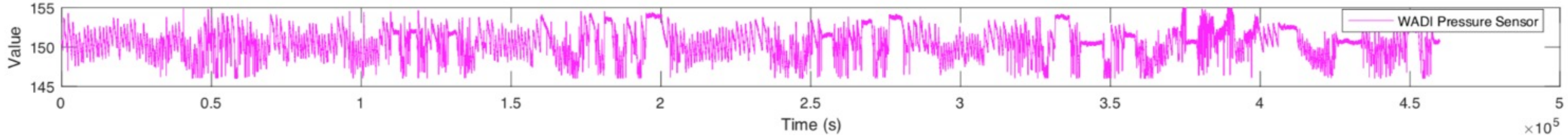
Electromagnetic Flow Sensor (SWaT)



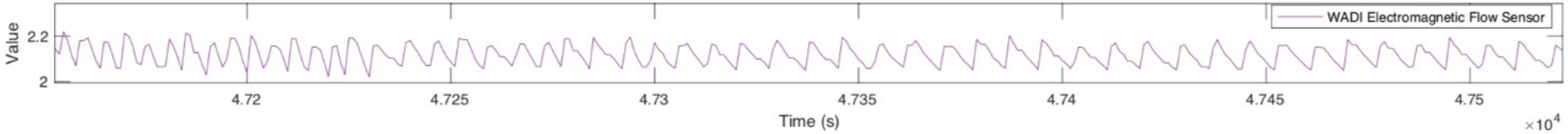
Pressure Sensor (SWaT)



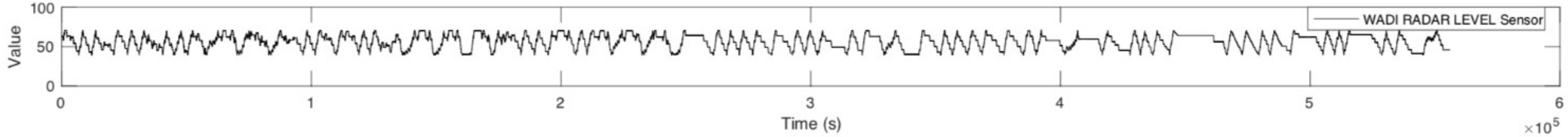
Pressure Sensor (WADI)



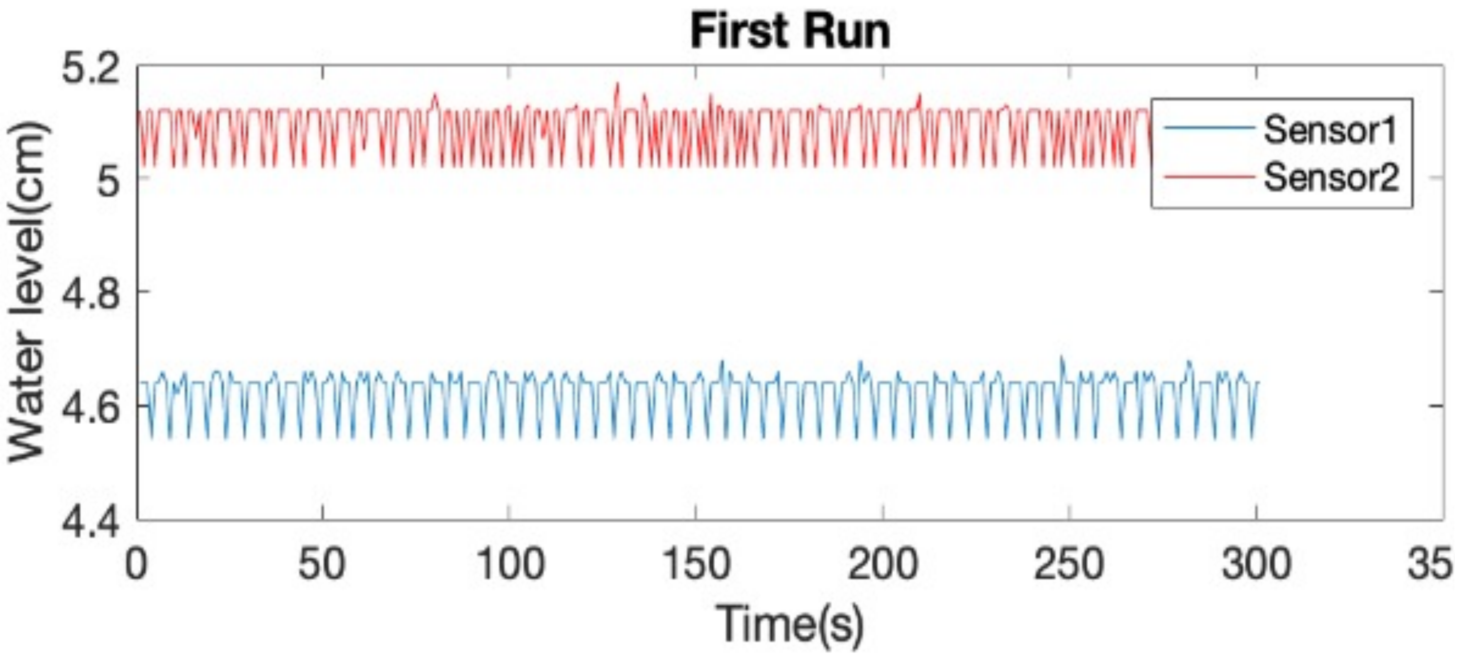
Electromagnetic Flow Sensor (WADI)

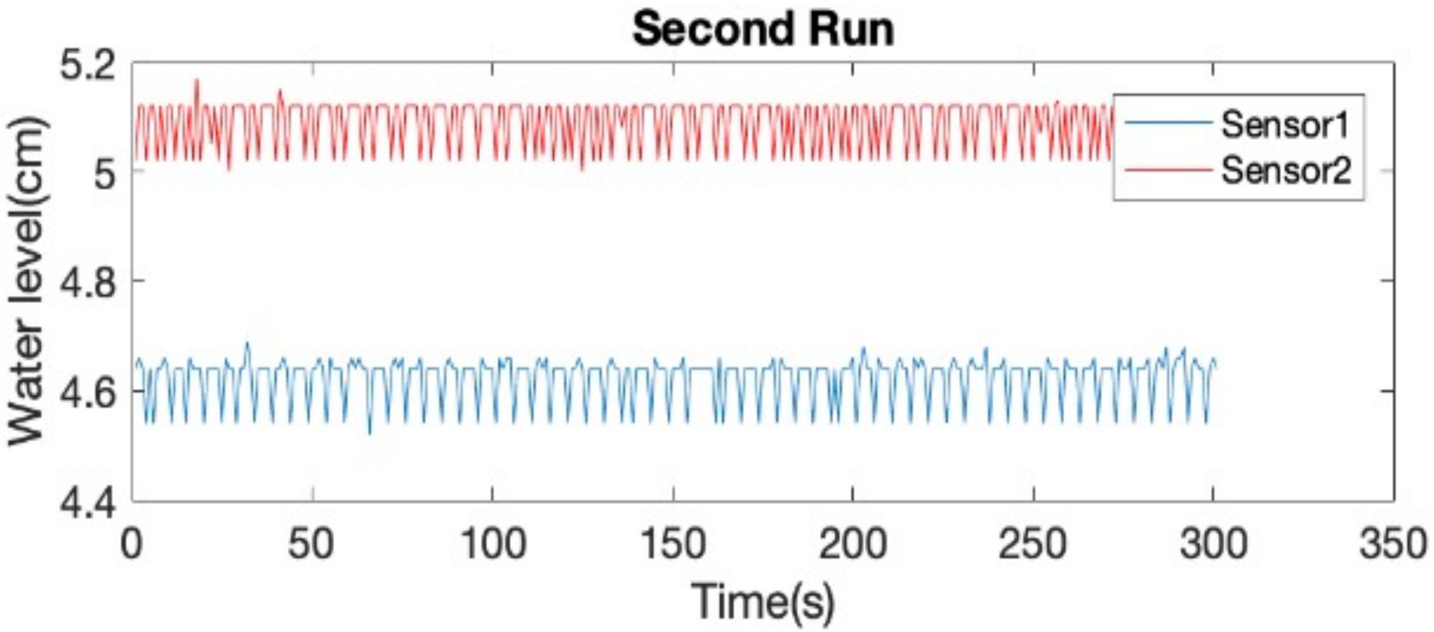


Radar Level Sensor (WADI)



Sensors vs Noise

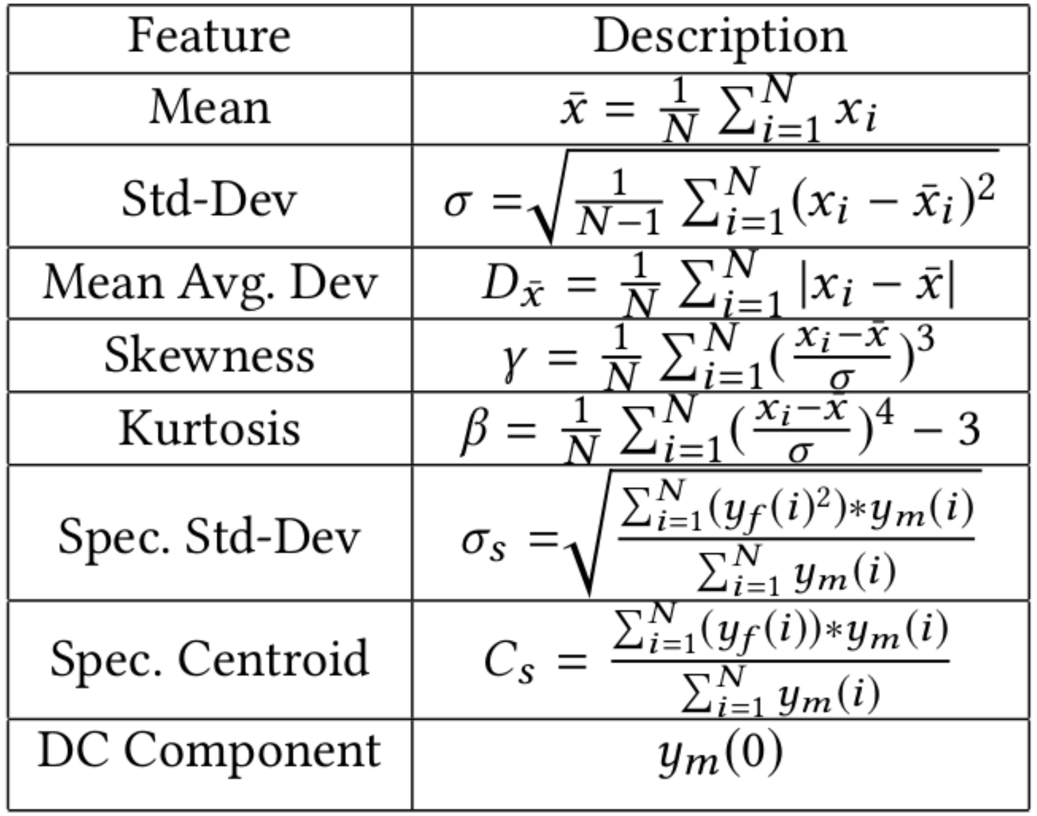




- Water level not changing.
- Stable behavior in two runs.
- Cannot really distinguish Sensor 1 from Sensor 2 visually but...

A bit of magic...

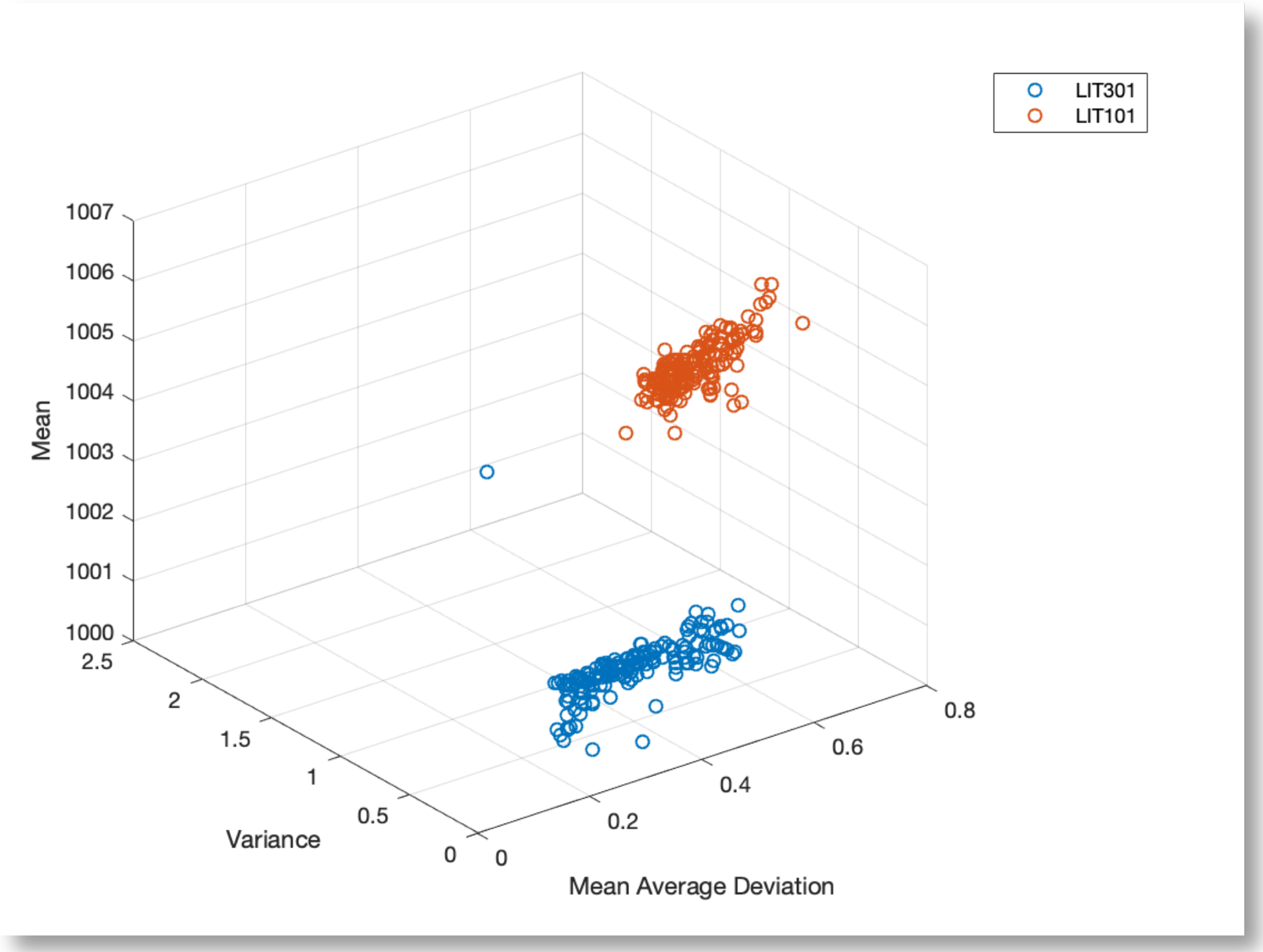
https://static.tvtropes.org/pmwiki/pub/images/technowizard.jpg

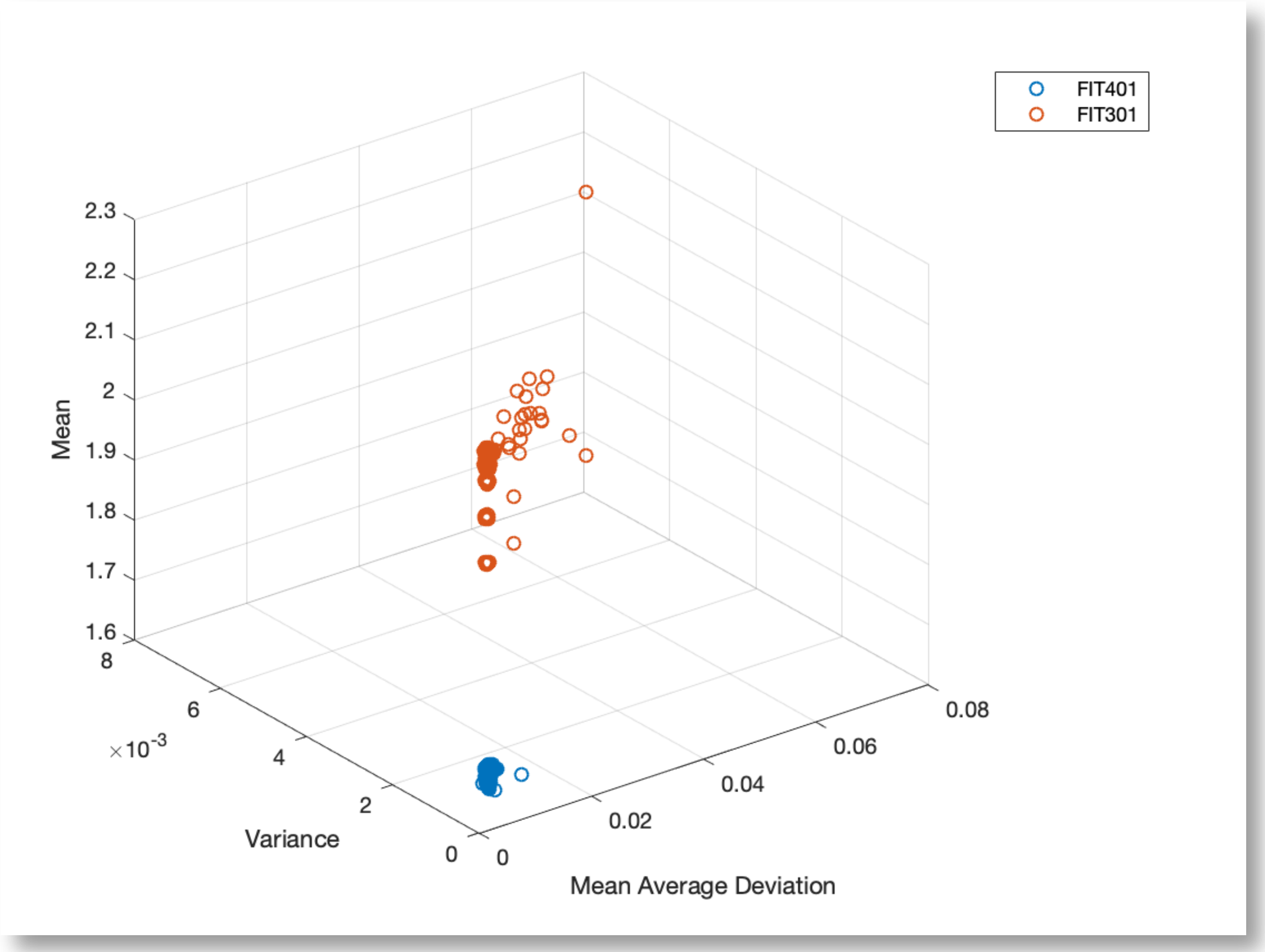


Feature	Description
Mean	$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$
Std-Dev	$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x}_i)^2}$
Mean Avg. Dev	$D_{\bar{x}} = \frac{1}{N}\sum_{i=1}^{N} \lvert x_i - \bar{x}\rvert$
Skewness	$\gamma = \frac{1}{N}\sum_{i=1}^{N}(\frac{x_i - \bar{x}}{\sigma})^3$
Kurtosis	$\beta = \frac{1}{N}\sum_{i=1}^{N}(\frac{x_i - \bar{x}}{\sigma})^4 - 3$
Spec. Std-Dev	$\sigma_s = \sqrt{\frac{\sum_{i=1}^{N}(y_f(i)^2)*y_m(i)}{\sum_{i=1}^{N} y_m(i)}}$
Spec. Centroid	$C_s = \frac{\sum_{i=1}^{N}(y_f(i))*y_m(i)}{\sum_{i=1}^{N} y_m(i)}$
DC Component	$y_m(0)$

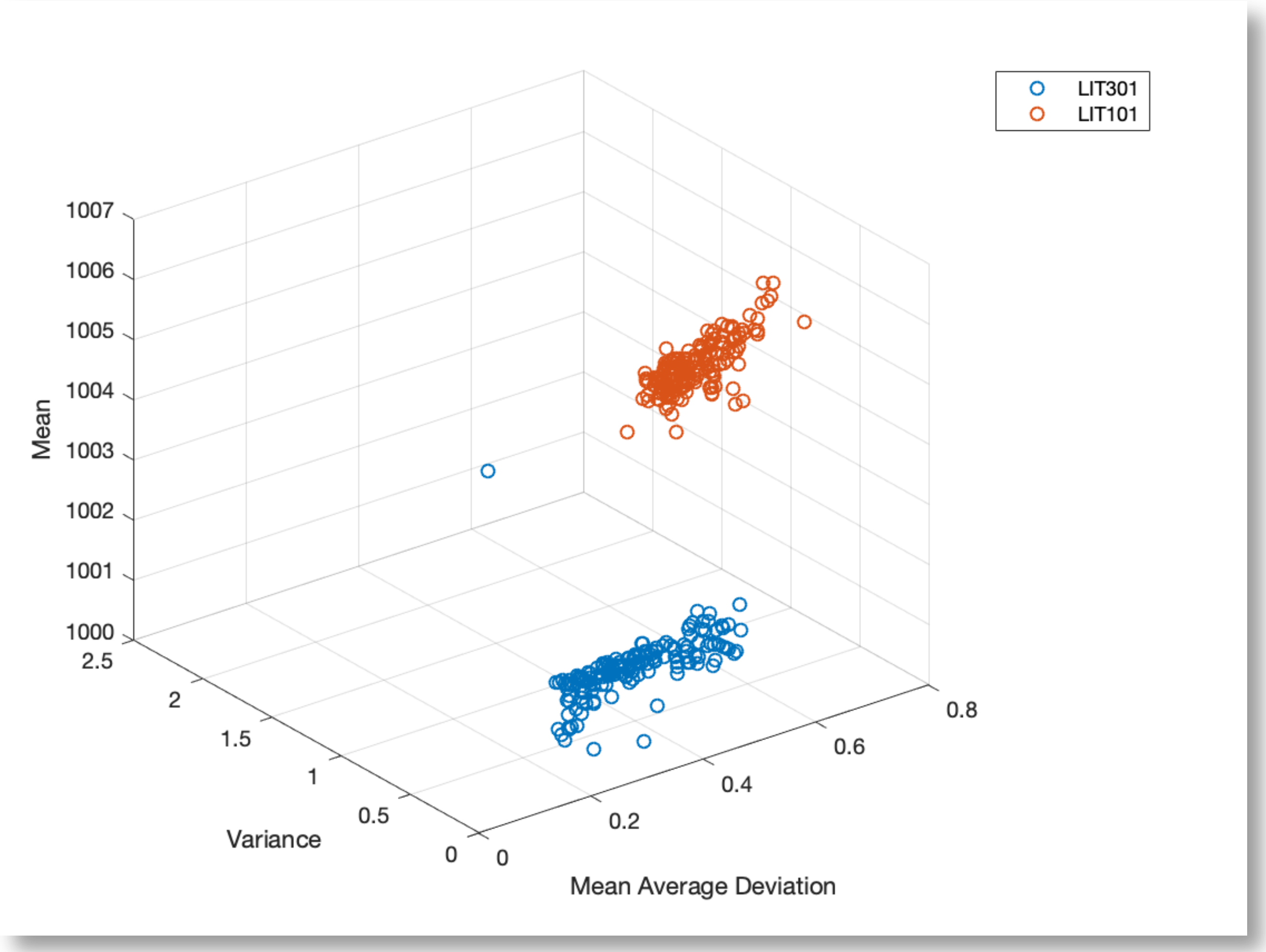
[Ahmed et al. ArxiV 17]

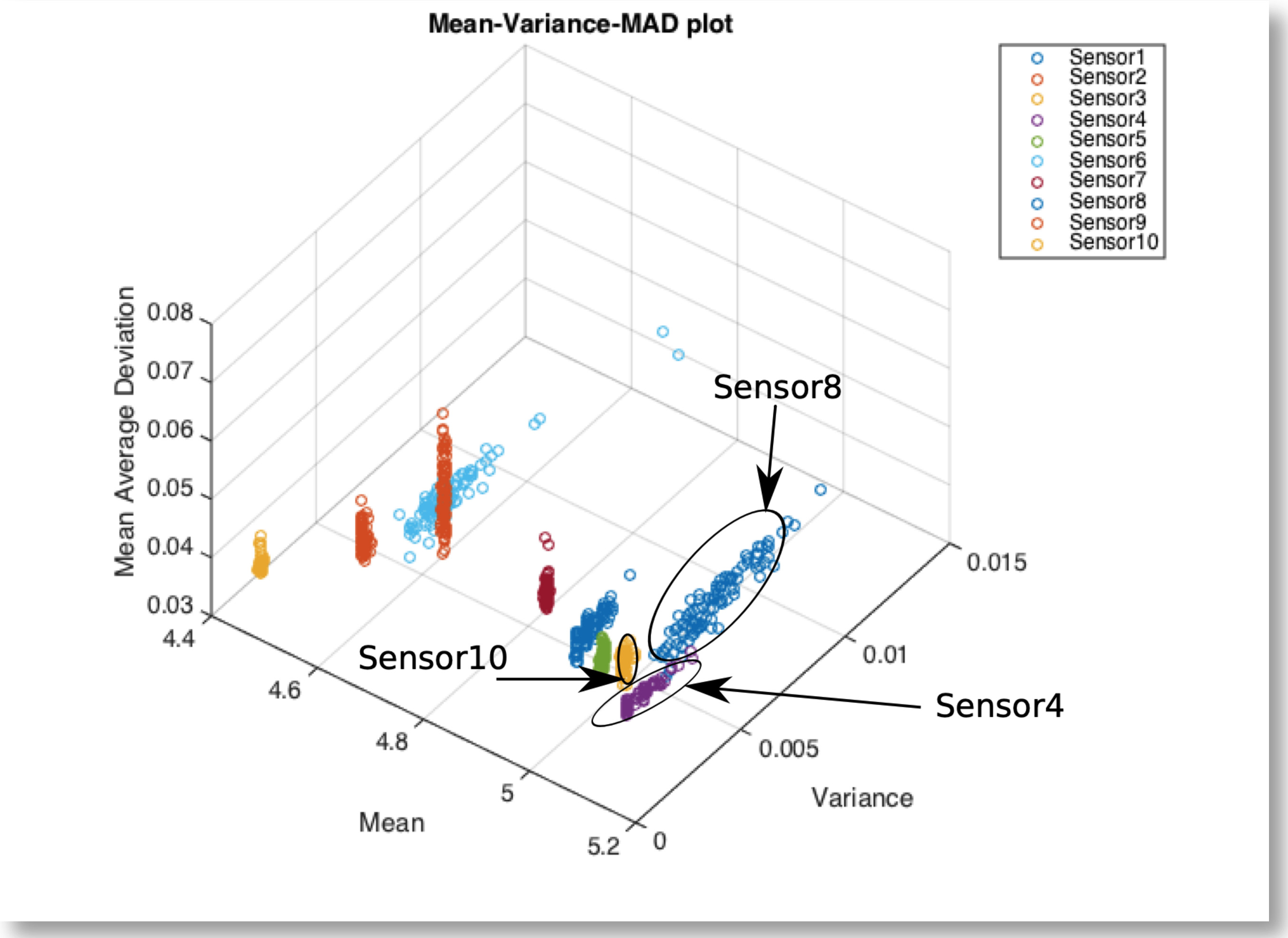
Sensors vs features





Sensors vs features



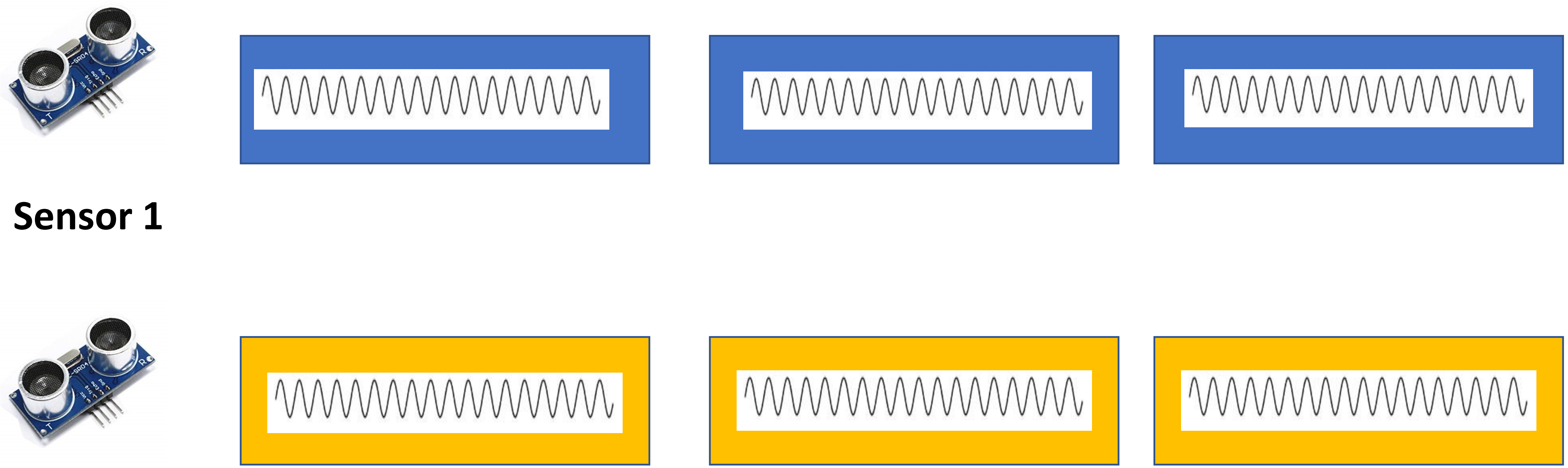


- Supervised Machine Learning can help distinguishing between the noise of different sensors!

[Ahmed et al. Arxiv 17, AsiaCCS 18]

Towards authentication

Can we distinguish data belonging to Sensor 1 from other sensors?

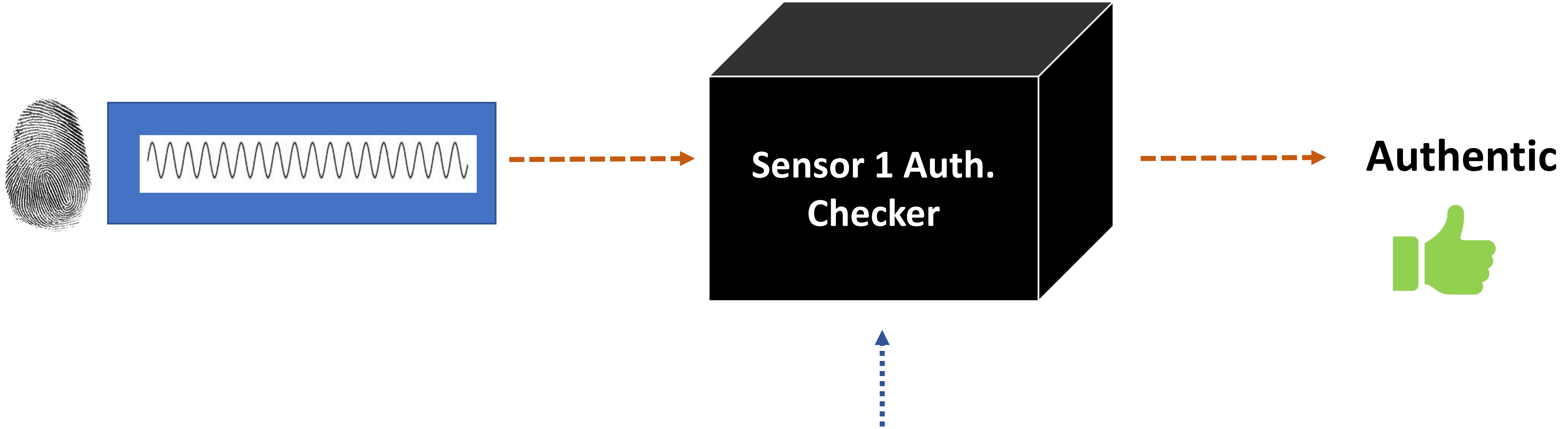


Sensor 1

Sensor 2

Towards authentication

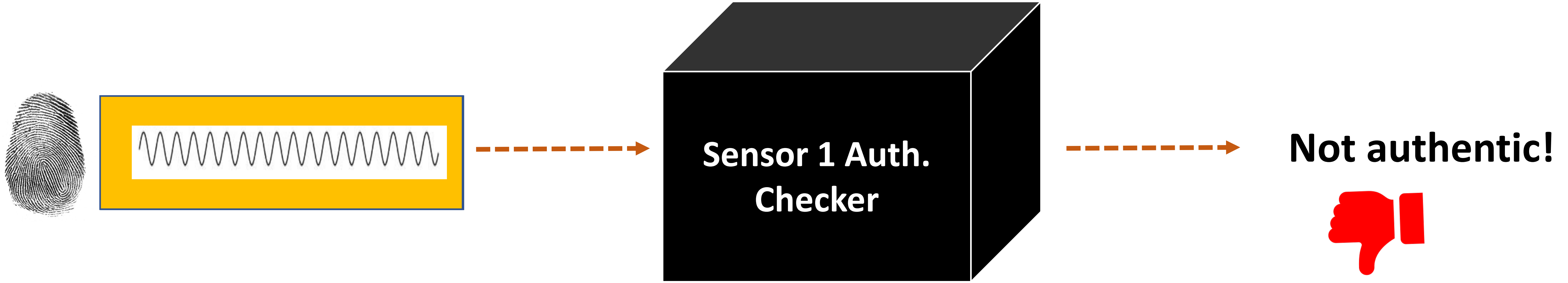
- Want to build a binary classifier (authentic/not authentic) to act as an authenticity verifier.
- Fingerprint check!



Trained with lots of data belonging to Sensor 1 and all other sensors in the plant!

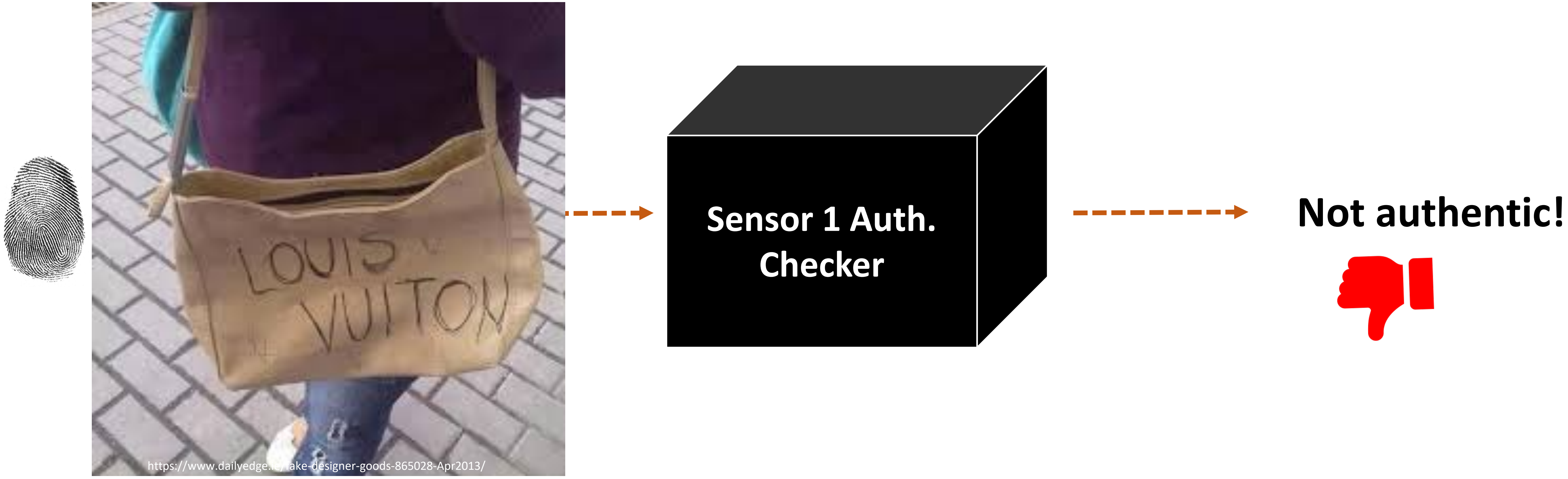
Towards authentication

- Chunks of observations from other sensors, even for similar values, brand, type etc. should not pass!



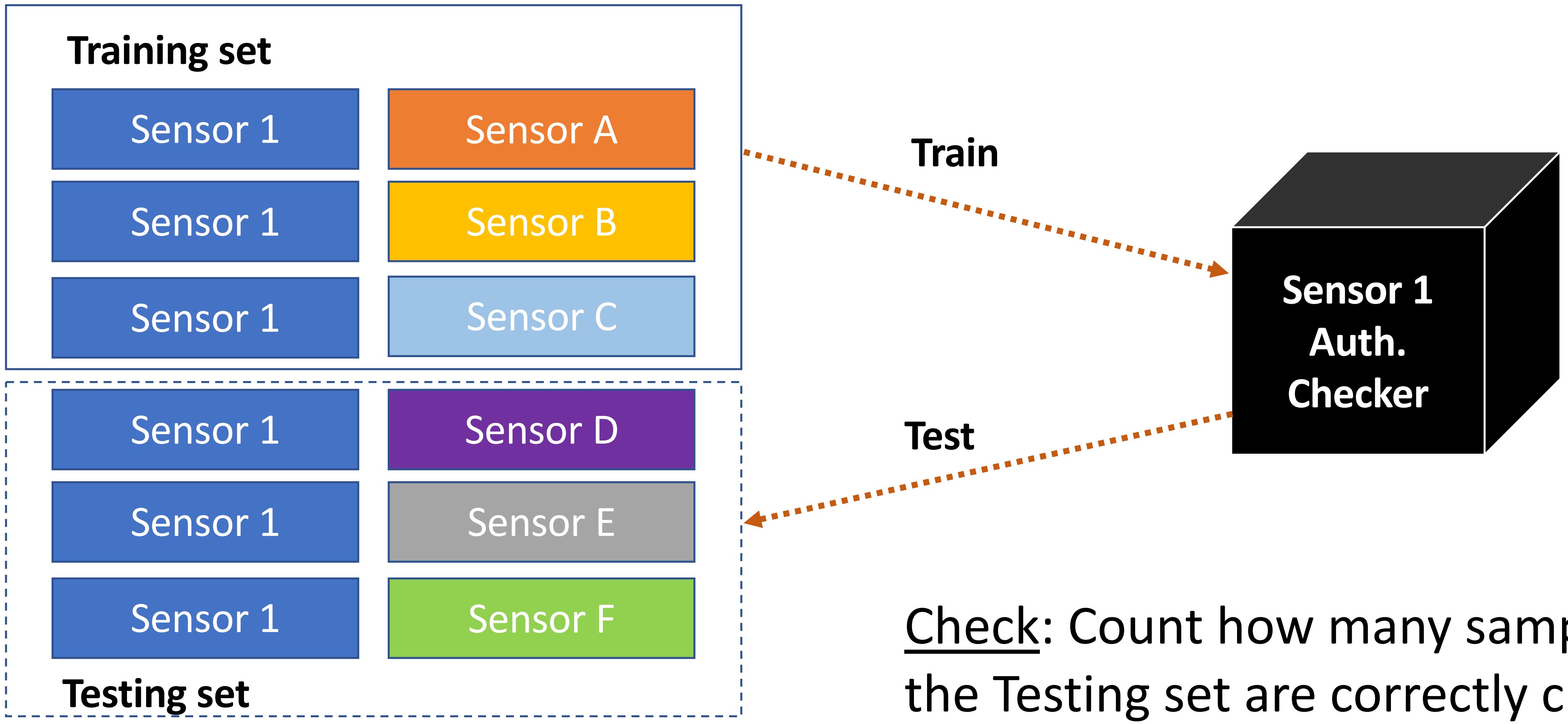
Careless (noise) attack

- An attacker using a constant value (no-noise) is easy to detect.



https://www.dailyedge.ie/fake-designer-goods-865028-Apr2013/

Does it work?



Training set

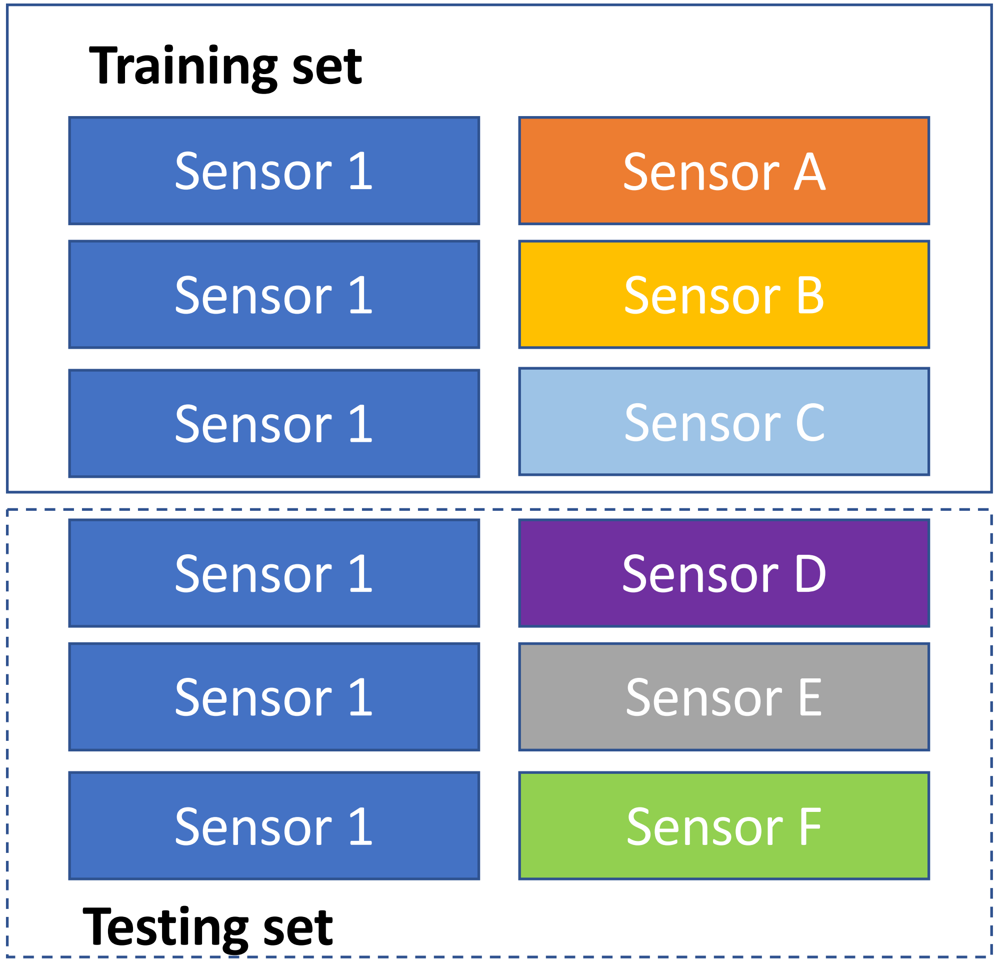
Sensor 1	Sensor A
Sensor 1	Sensor B
Sensor 1	Sensor C

Sensor 1	Sensor D
Sensor 1	Sensor E
Sensor 1	Sensor F

Testing set

<u>Check</u>: Count how many samples in the Testing set are correctly classified after training with the Training set.

Does it work?


Training set

Sensor 1	Sensor A
Sensor 1	Sensor B
Sensor 1	Sensor C
Sensor 1	Sensor D
Sensor 1	Sensor E
Sensor 1	Sensor F

Testing set

- Chunk size of about 2 minutes works best (120 samples).
- Tested on up to 60 sensors of the same class (cheap sensors).
- 99% accuracy in authentication test.

  [Ahmed et al. Arxiv 17, AsiaCCS 18]
- Fingerprints are still valid after 4 years at least.
- Tested in room temperature (20 to 35 ^{o}C)

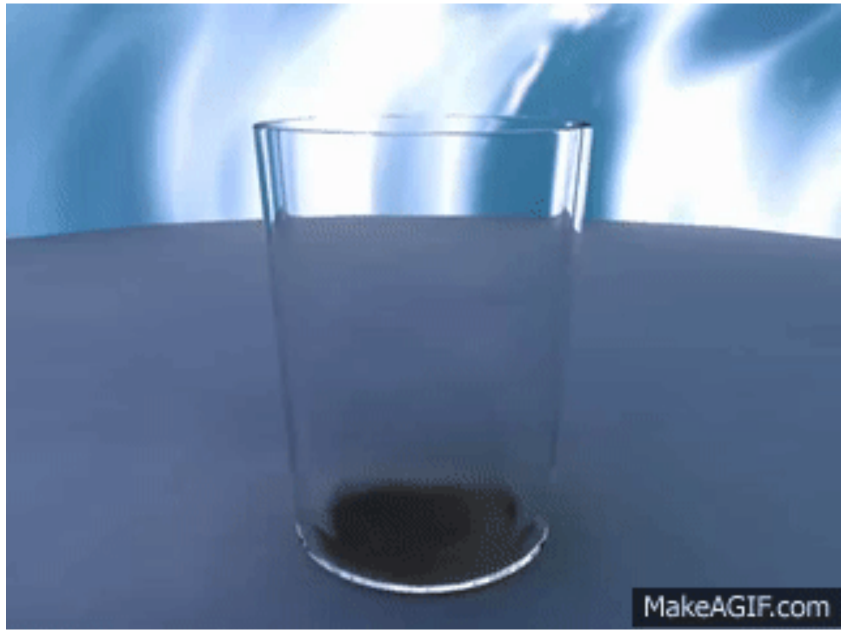
Note that this works when <u>physical quantity is constant!</u>

Attacks detected?

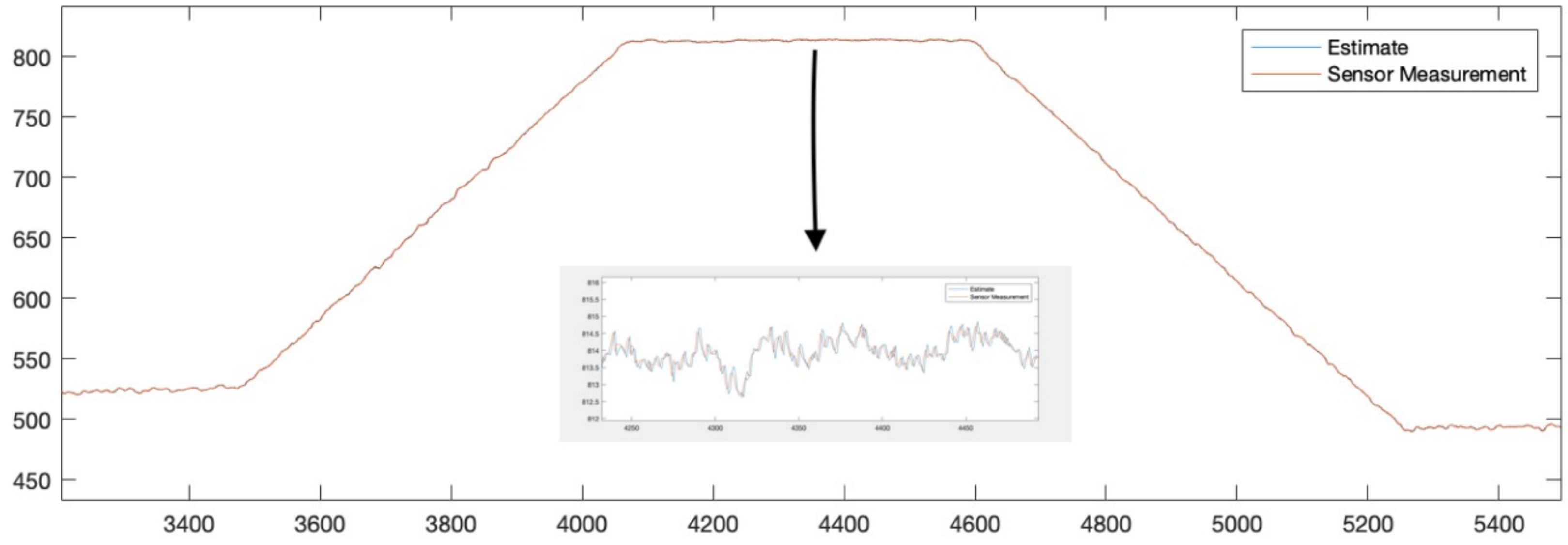
- "Shameless" attacks:
  - Abrupt jumps can be detected by Model-Based countermeasures.
  - "Flat" noise injections can be detected by noise patterns (even stealthy).
- Malicious sensors (hardware) can be detected.
  - Like [Bolshev et al. BH Asia 16]
- What about stealthy attacks that also try to inject coherent noise against a dynamic system?

Process and Sensor noise

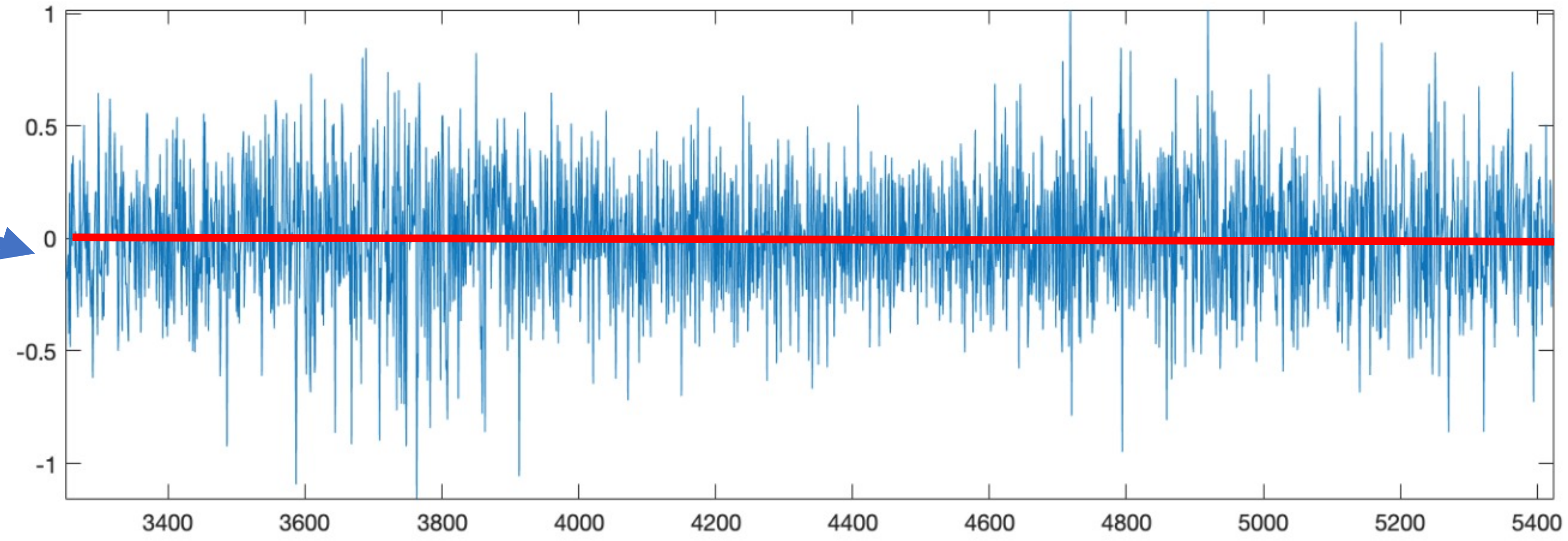
- In practice we have a combination of sensor plus process noise, I.e. water moving generates a certain characteristic "noise".
- I.e. even if sensor is perfect (no noise) measurement is "noisy".



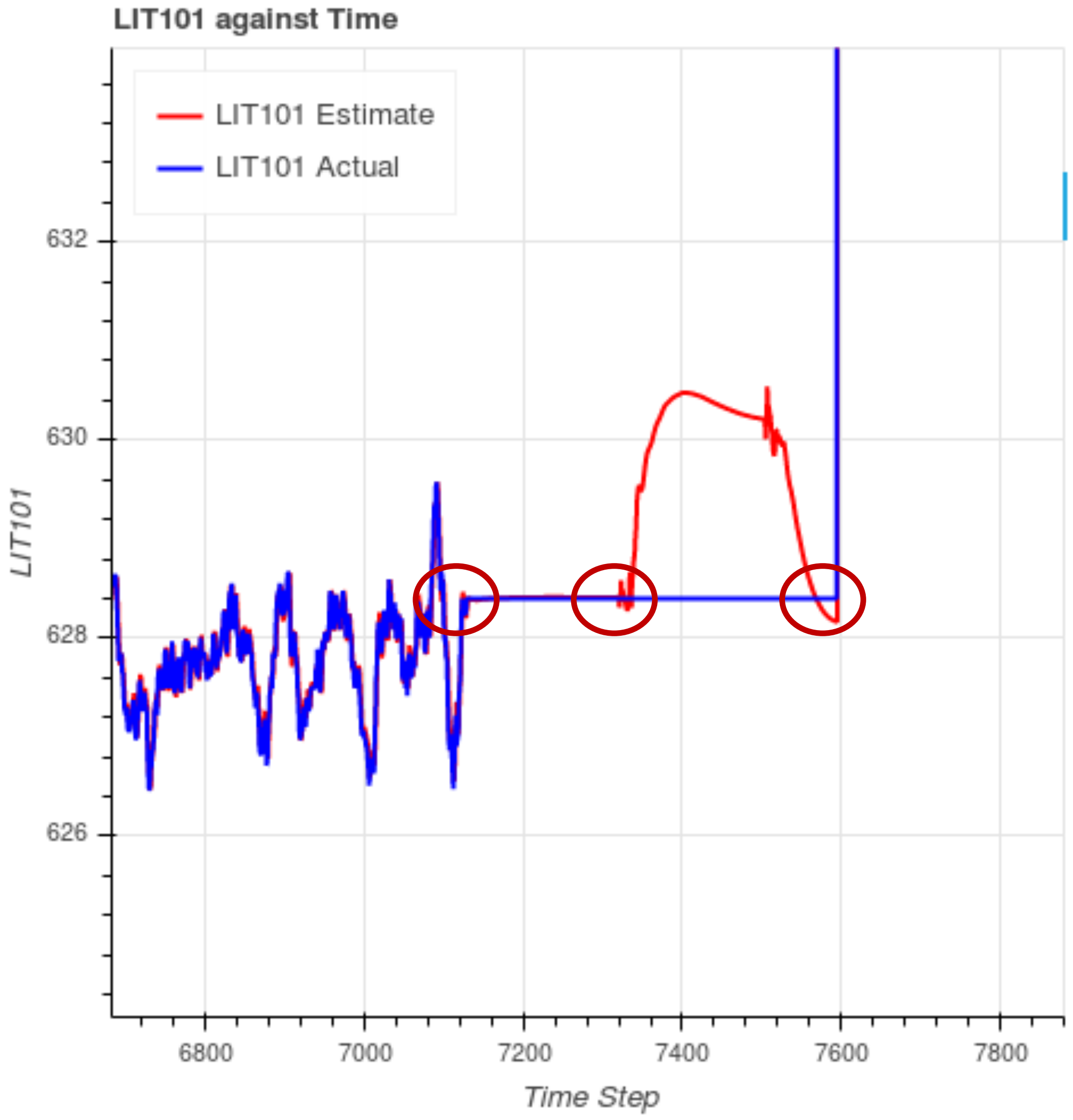
Process and Sensor noise

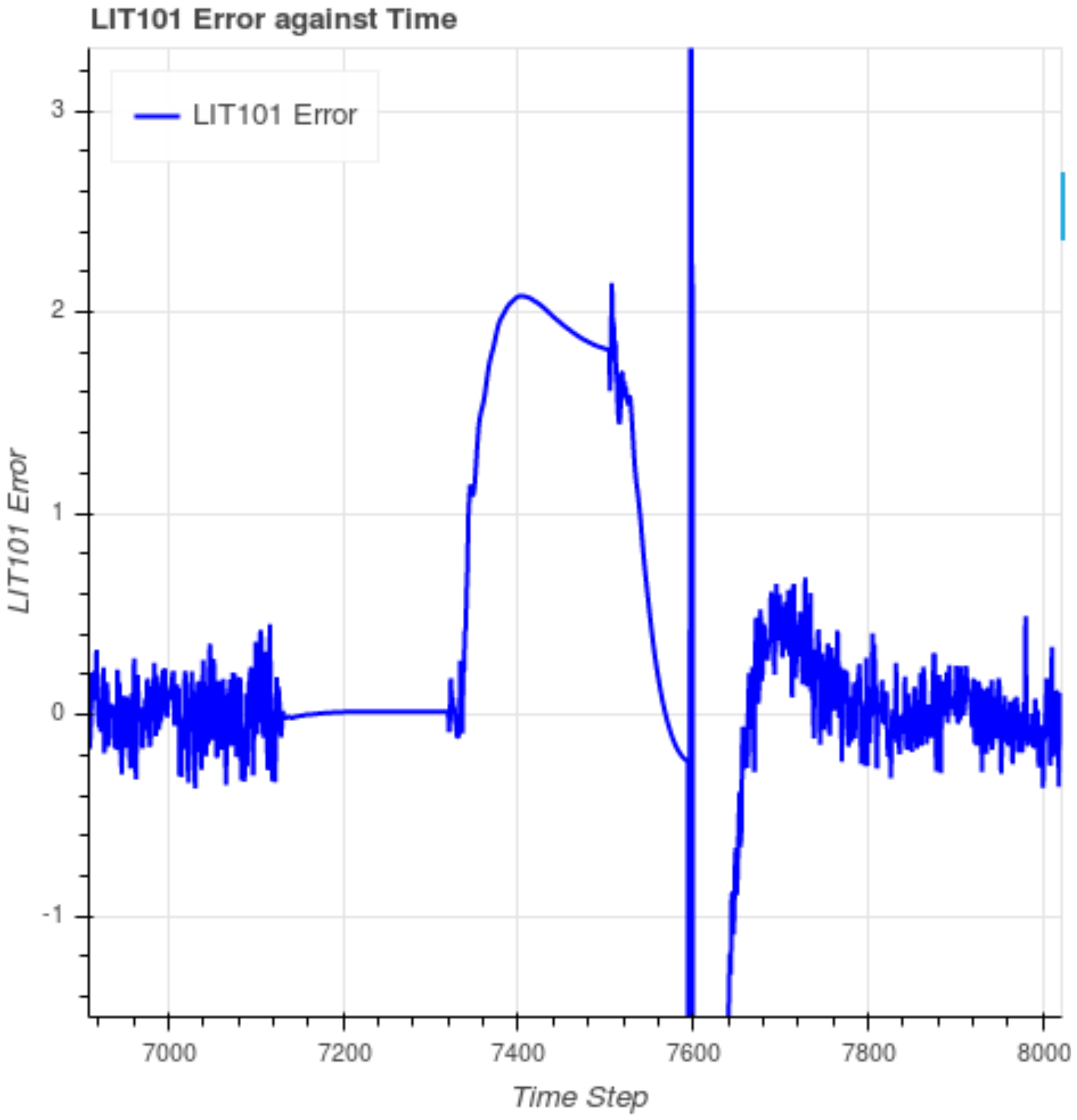


Residual =
Observation - Prediction

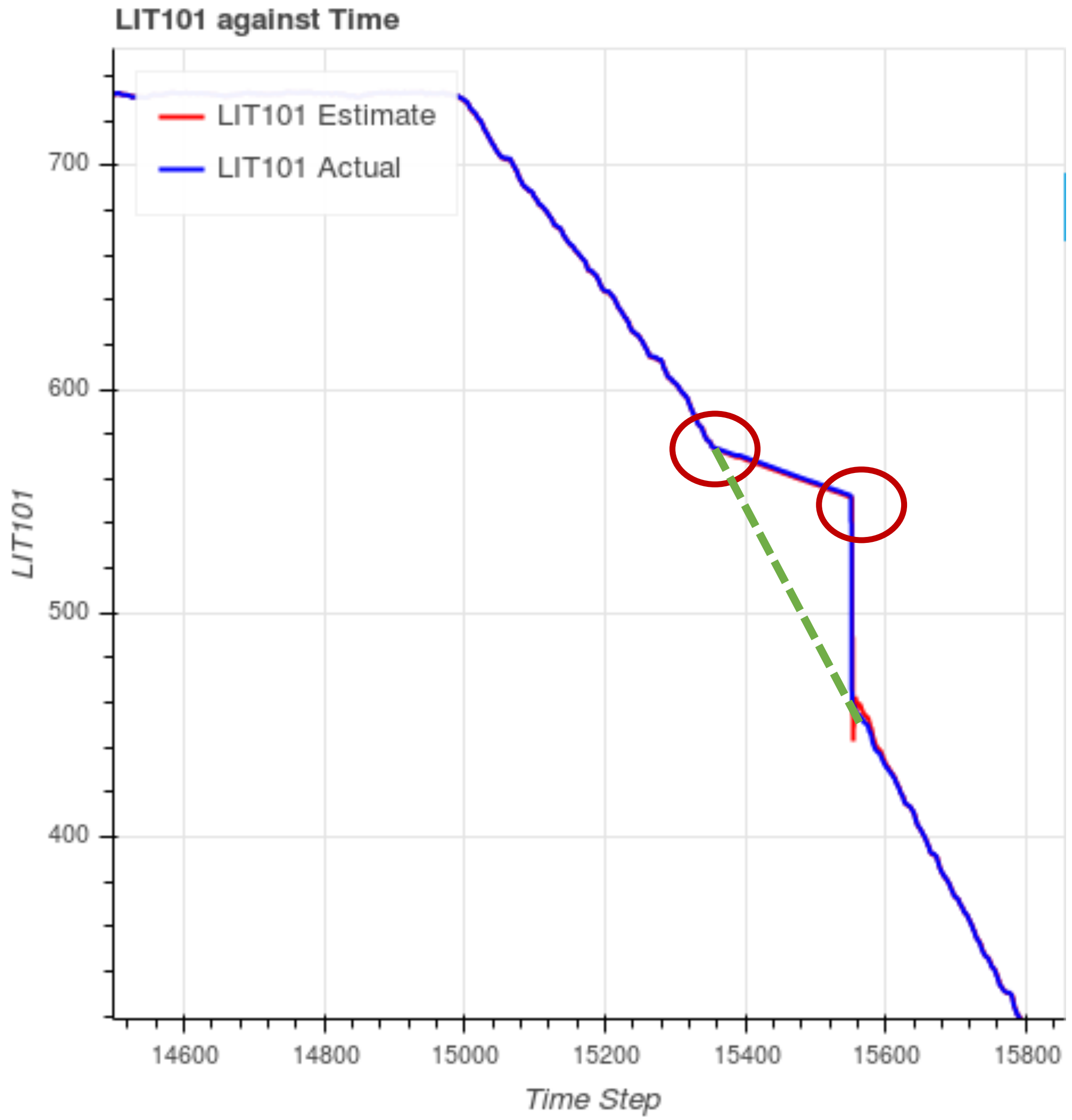


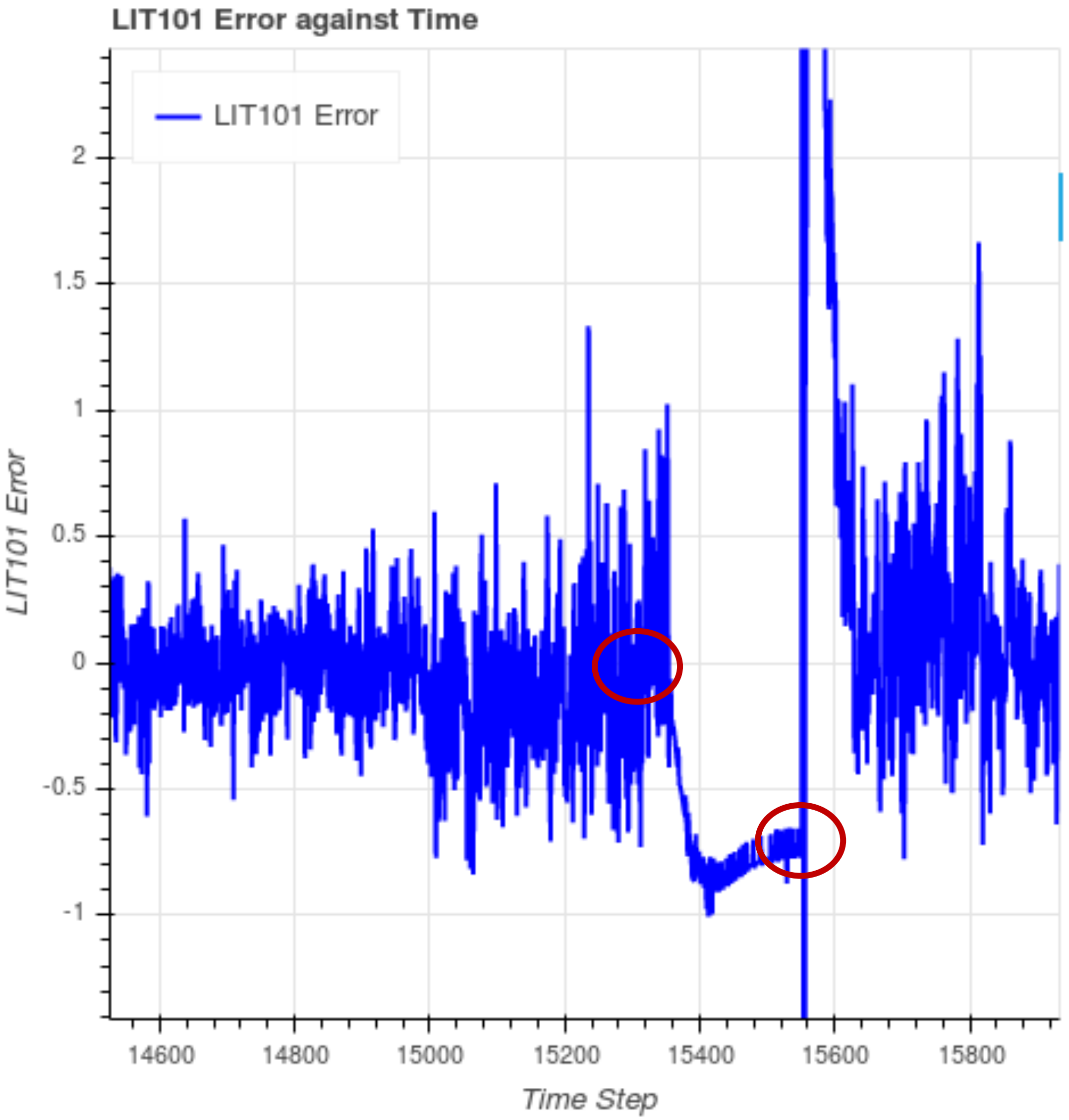
Detecting flat noise





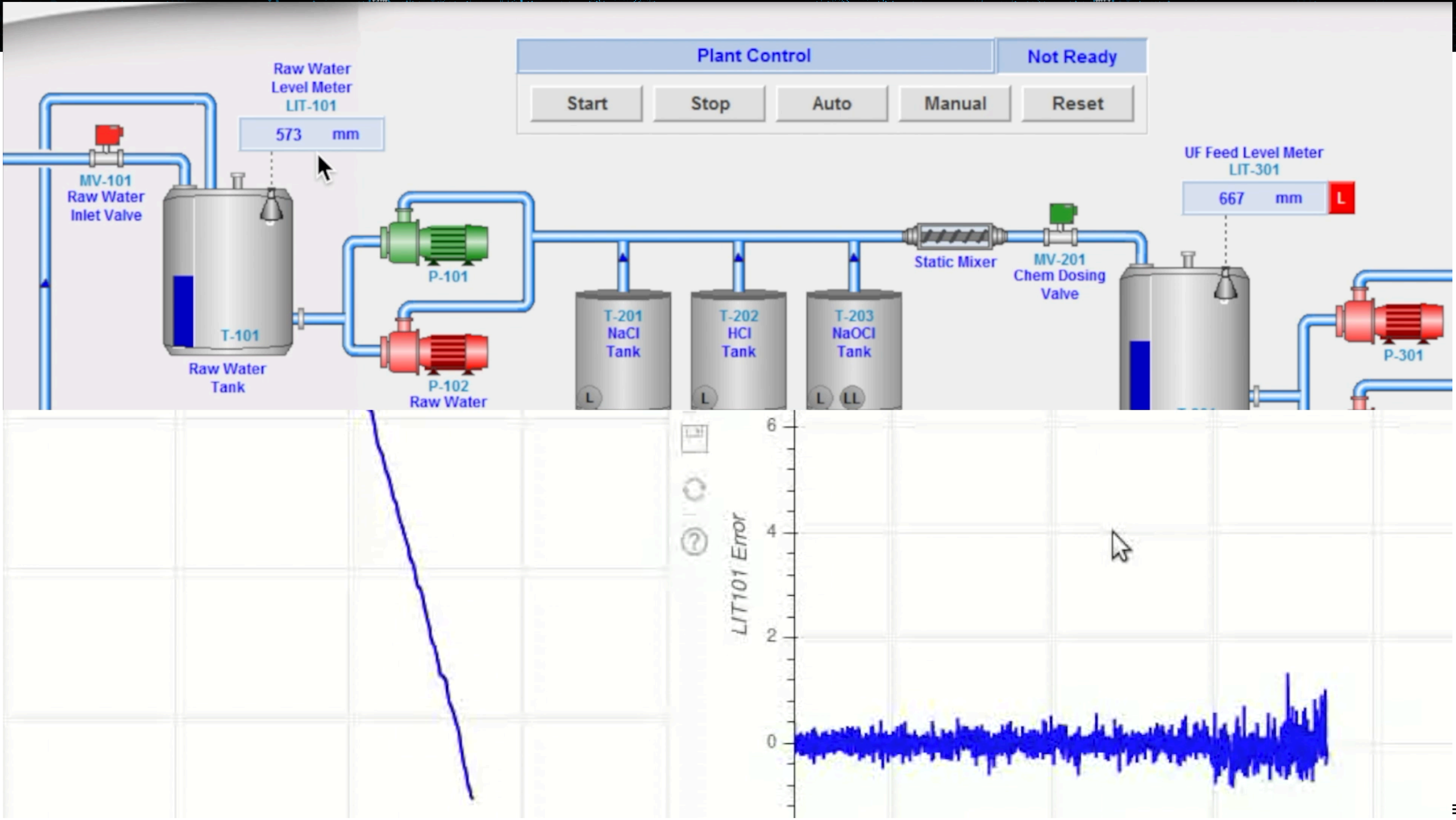
Noise vs. Stealthy attacks



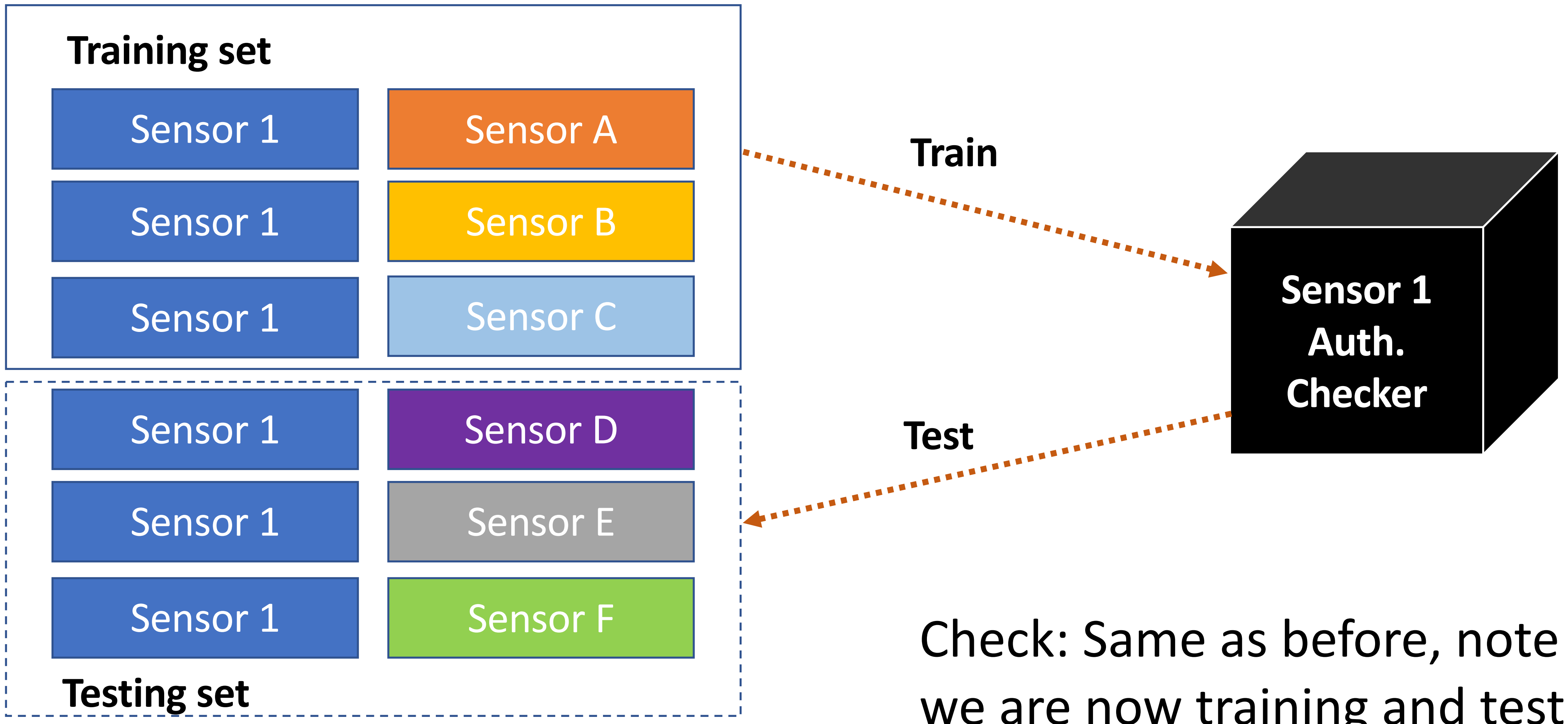


[Ahmed et al. ACSAC 18]

Video of attack detection

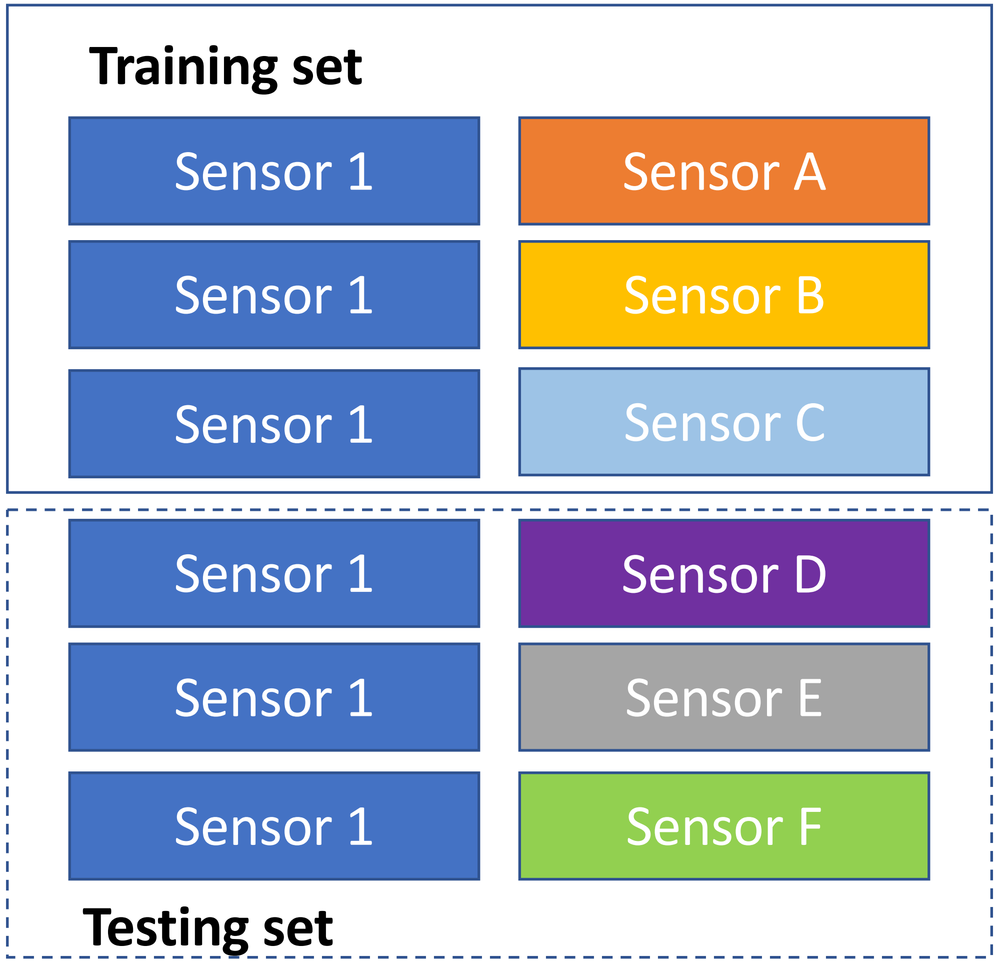


Does it work?



Check: Same as before, note that we are now training and testing against the residual!

Does it work?



Training set

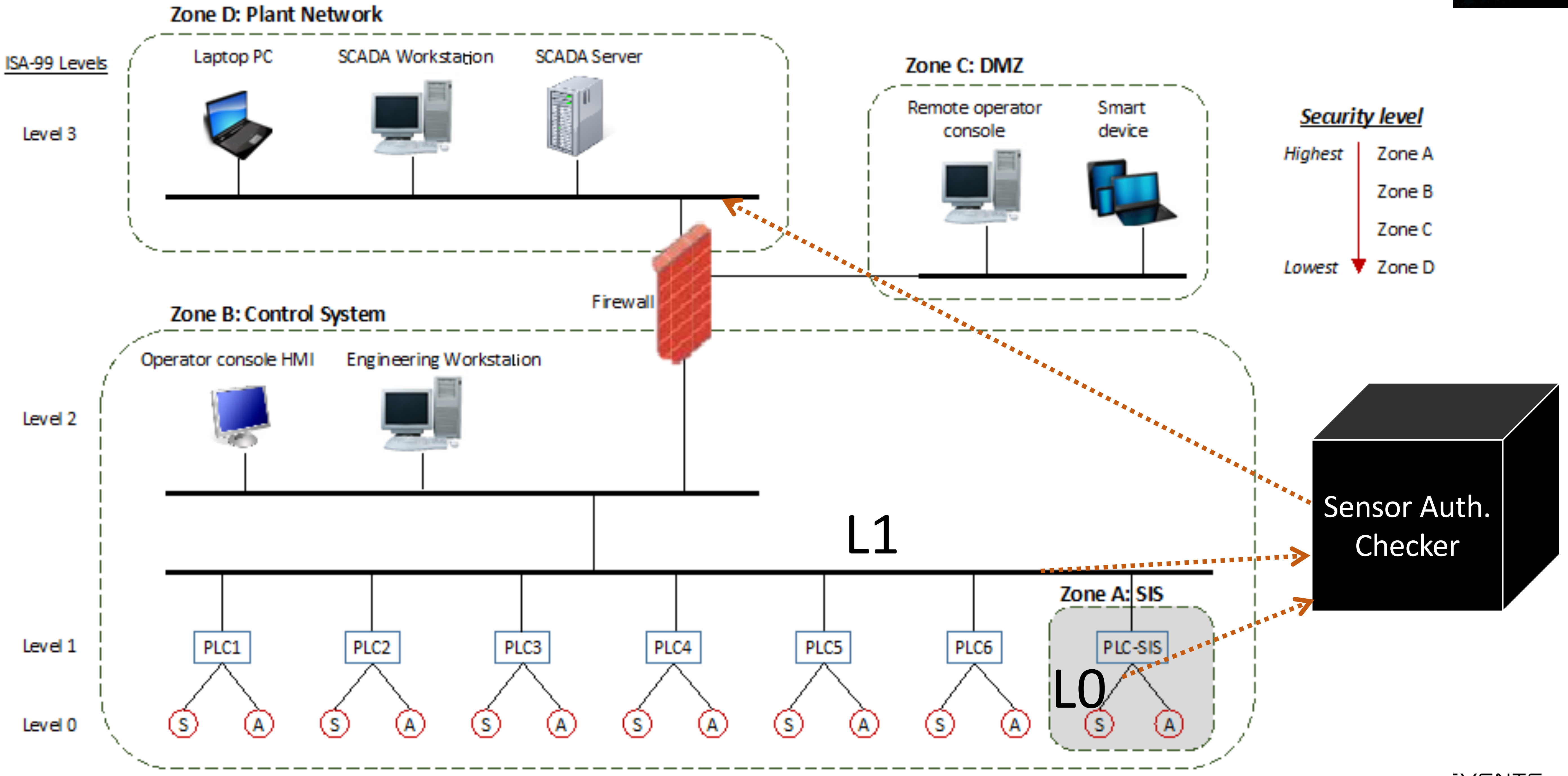
Sensor 1	Sensor A
Sensor 1	Sensor B
Sensor 1	Sensor C
Sensor 1	Sensor D
Sensor 1	Sensor E
Sensor 1	Sensor F

Testing set

- Chunk size of about 2 minutes (120 samples) works best (again).
- Tested on up to 18 sensors and respective process on SWaT.
- 96% accuracy in authentication test.

  [Ahmed et al. ACSAC 18]
- Considered several "stealthy" strategies.
  - But CPS are different! [Krotofil et al. HITB 15]

Architecture

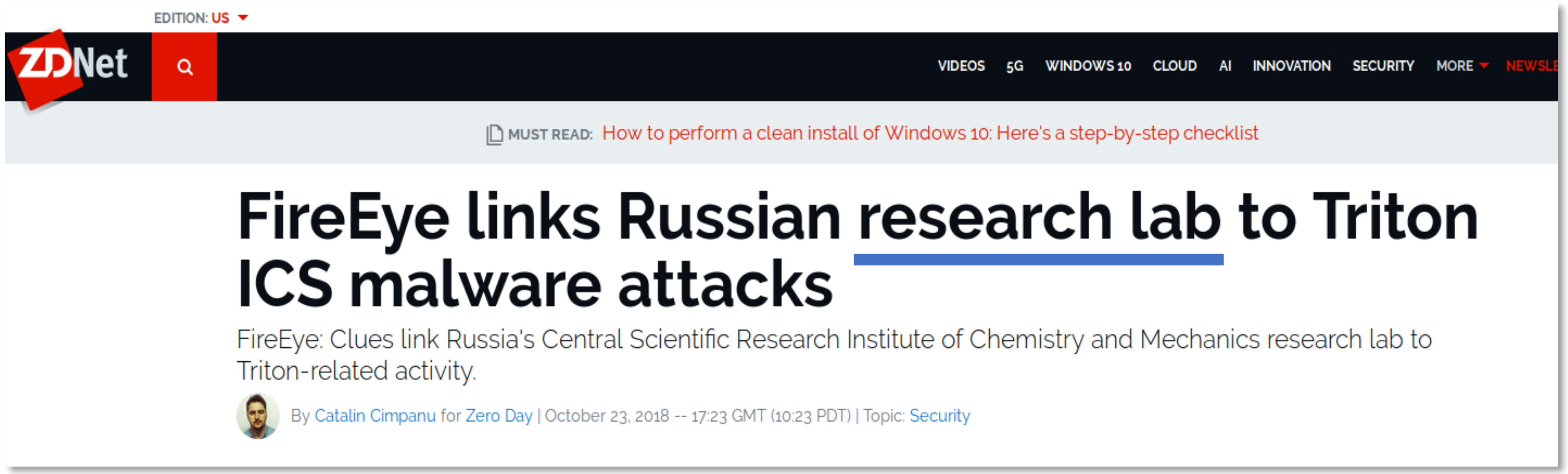


Summary

- We have shown empirical evidence of existence of sensor fingerprint in real-world ICS.
  - Over 10 sensor types, up to 60 sensors for each type.
- We have shown how this fingerprint, together with a process fingerprint, can help in authenticating sensor readings.
  - High detection/authentication accuracy (96%-99%).

Next steps?

- On the other hand, this is just the beginning!
- What if threat actor has an entire research institute at their disposal?



MUST READ: How to perform a clean install of Windows 10: Here's a step-by-step checklist

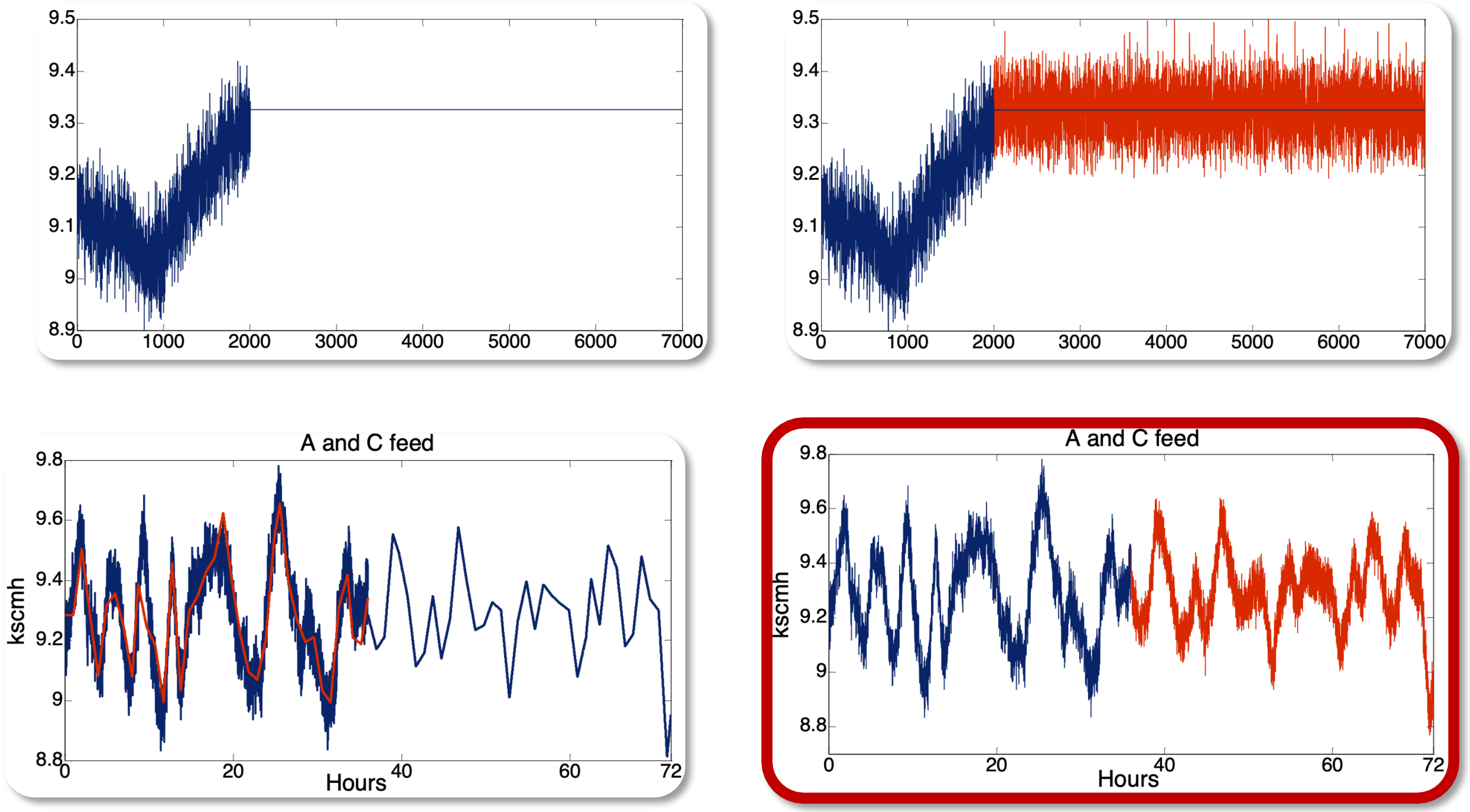
FireEye links Russian research lab to Triton ICS malware attacks

FireEye: Clues link Russia's Central Scientific Research Institute of Chemistry and Mechanics research lab to Triton-related activity.

By Catalin Cimpanu for Zero Day | October 23, 2018 -- 17:23 GMT (10:23 PDT) | Topic: Security

Next steps?

- A lack of model makes things challenging, under advanced attacks.
- Case of super powerful attacker (Ironman + PhD)
  - We have ideas on how to deal with this using a challenge-response protocol [Ahmed et al, ArxiV 17]



[Krotofil et al. HITB 15]

Sound Bytes

- In most real-world ICS sensor data is not authenticated at L0 and/or L1 levels.
- Sensor noise can be useful to authenticate sensors without using cryptography.
- Process + Sensor noise results in a more robust fingerprint.

Thanks!

martin.ochoa@cyxtera.com

chuadhry@mymail.sutd.edu.sg

Cyxtera

SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust Centre for Research in Cyber Security

- **[Adepu et al. IFIP SEC 16]** S. Adepu, A. Mathur *Using Process Invariants to Detect Cyber Attacks on a Water Treatment System.* IFIP SEC 2016.
- **[Ahmed et al. AsiaCCS 18]** C. Ahmed, M. Ochoa, J. Zhou, A. Mathur, R. Qadeer, C. Murguia, J.Ruths *NoisePrint: Attack Detection Using Sensor and Process Noise Fingerprint in Cyber Physical Systems*. AsiaCCS 2018
- **[Ahmed et al. Arxiv 17]** C. Ahmed, A. Mathur, M. Ochoa *NoiSense: Detecting Data Integrity Attacks on Sensor Measurements using Hardware based Fingerprints.* ArxiV 2017
- **[Ahmed et al. ACSAC 18]** C. Ahmed, J. Zhou, A. Mathur *Noise Matters: Using Sensor and Process Noise Fingerprint to Detect Stealthy Cyber Attacks and Authenticate sensors in CPS*. ACSAC 2018
- **[Bolshev et al. BH Asia 16]** A. Bolshev and M. Krotofil *Never trust your inputs: causing 'catastrophic physical consequences' from the sensor (or how to fool ADC).* Black Hat Asia 2016.
- **[Krotofil et al. HITB 15]** M. Krotofil and J. Larsen *What You Always Wanted and Now Can: Hacking Chemical Processes.* Hack In The Box 2015.
- **[Urbina et al. CCS 16]** D. Urbina, J. Giraldo, A. Cardenas, N. Tippenhauer et al. *Limiting the Impact of Stealthy Attacks on Industrial Control Systems.* CCS 2016.