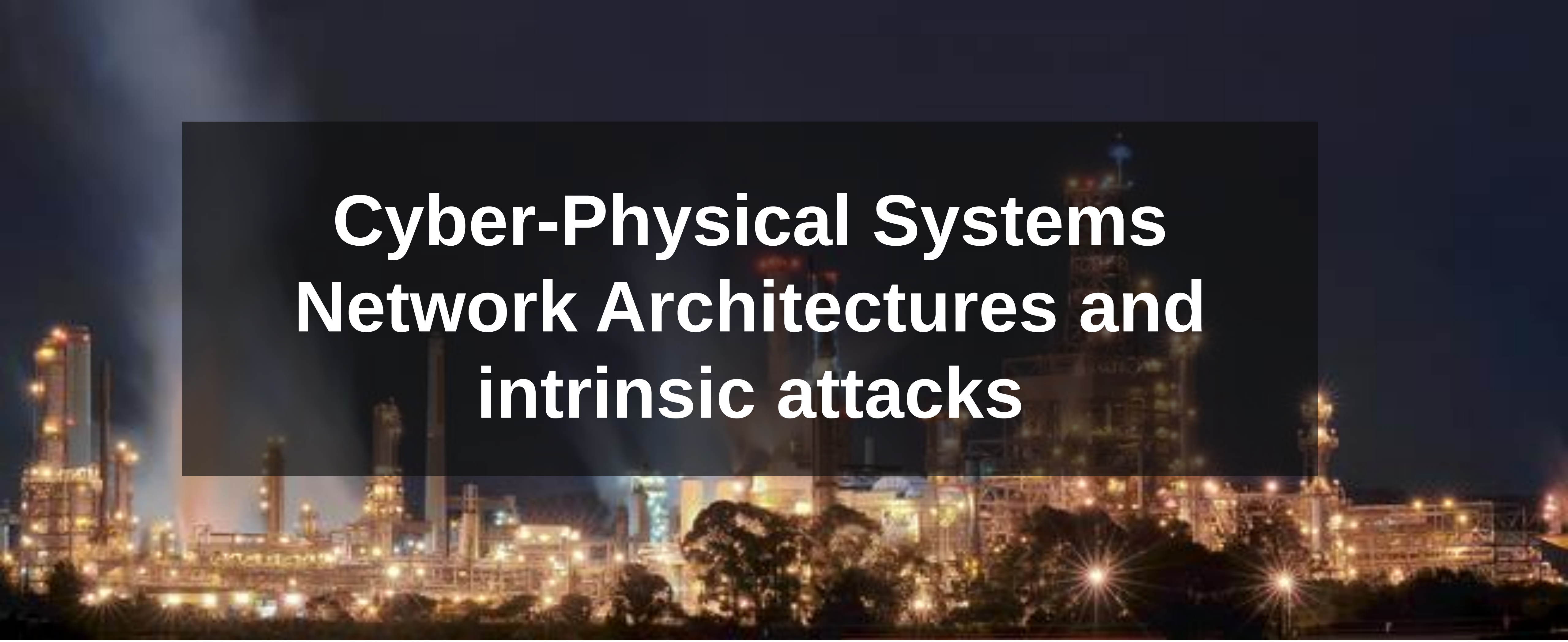


Cyber-Physical Systems Network Architectures and intrinsic attacks

Marina Krotofil

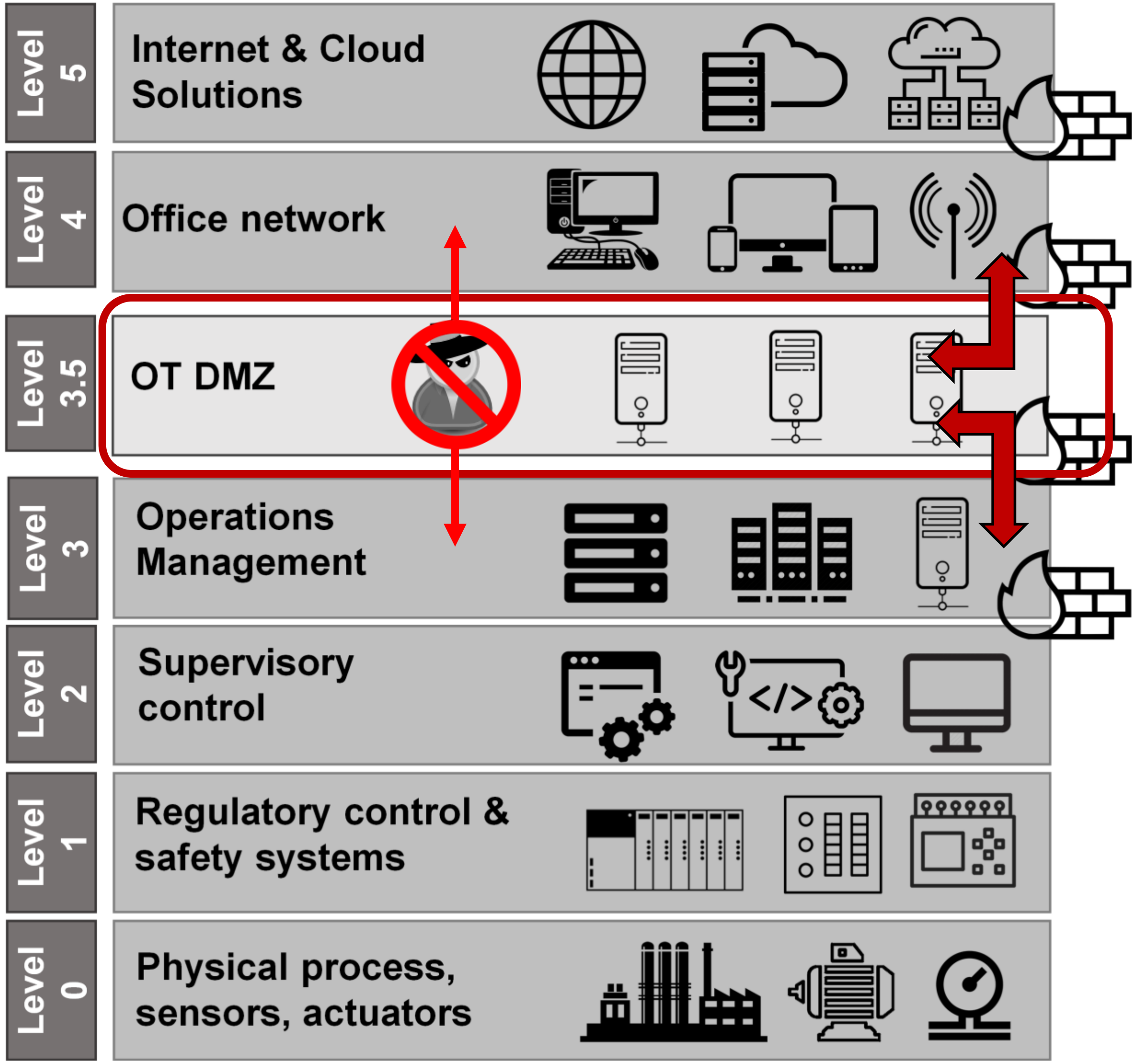
COINS summer school on Security Applications, Lesbos, Greece (online)
14-18.06.2021

Agenda

- **Security/network architectures**
  - **OT/ICS** – no or “strictly supervised” Internet
  - **IIoT** – “one-way” Internet
  - **IoT** – bidirectional Internet
  - **Edge computing**
- **CPS-specific attacks** (not preventable by any traditional IT security methods)
  - “Stale Data” attack
  - “Data Veracity” attack
  - Escaping security boundaries or “evil bubbles” attack

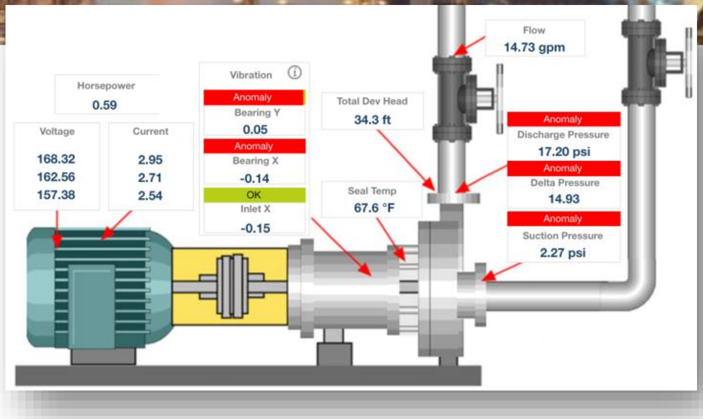
CPS network architectures

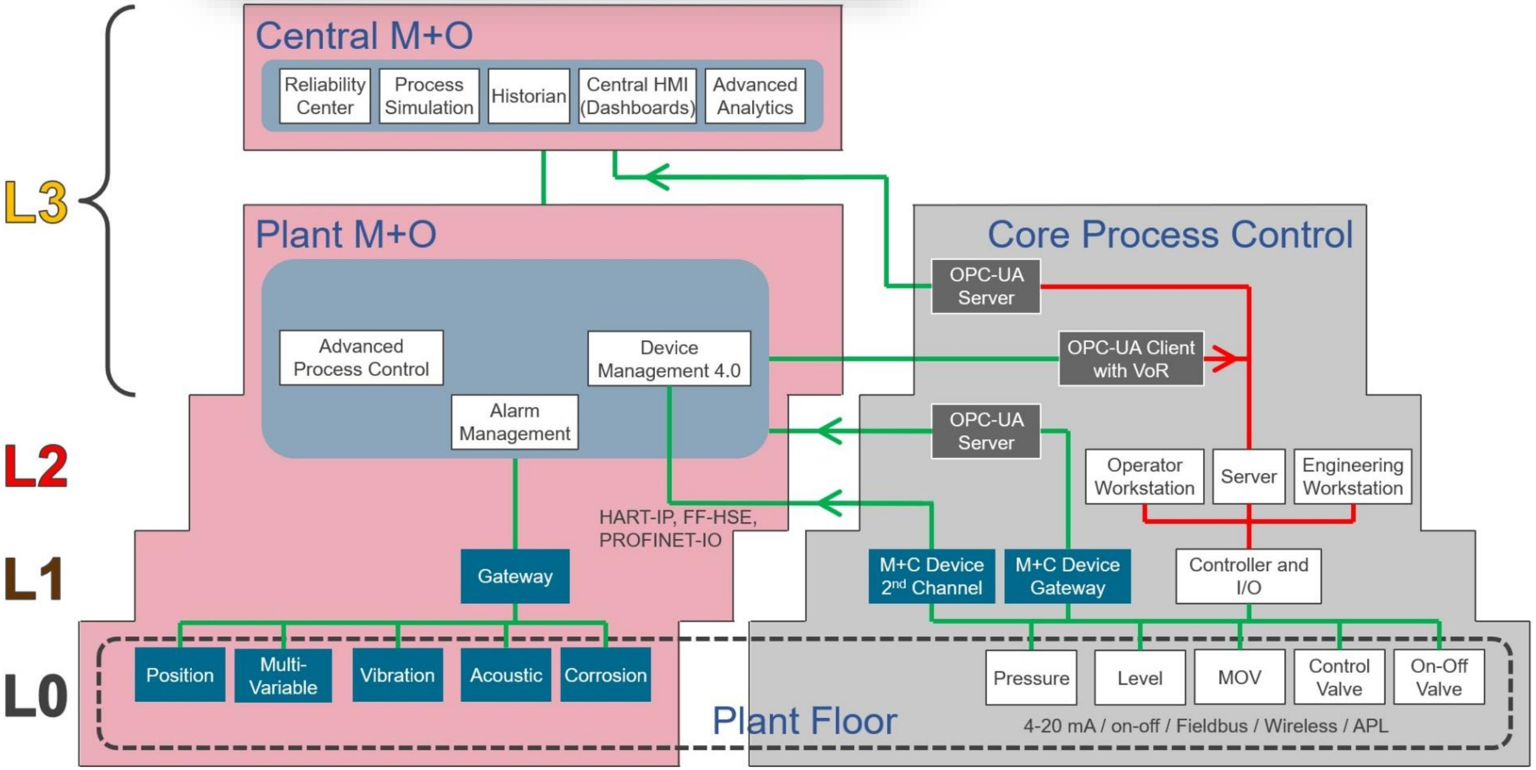
ICS/OT – typical architecture



- **Strong physical security**
- In rare cases air gapped
  - Data exchange over USB or similar
- **Limited and tightly configured** data exchange & communication flows through OT DMZ
  - Should prevent & detect >90% of automated & human-assisted intrusions/attacks
  - (Mostly) wired communication
- ***Lower requirement to security of end-points***

IIoT – independent reliable data infrastructure

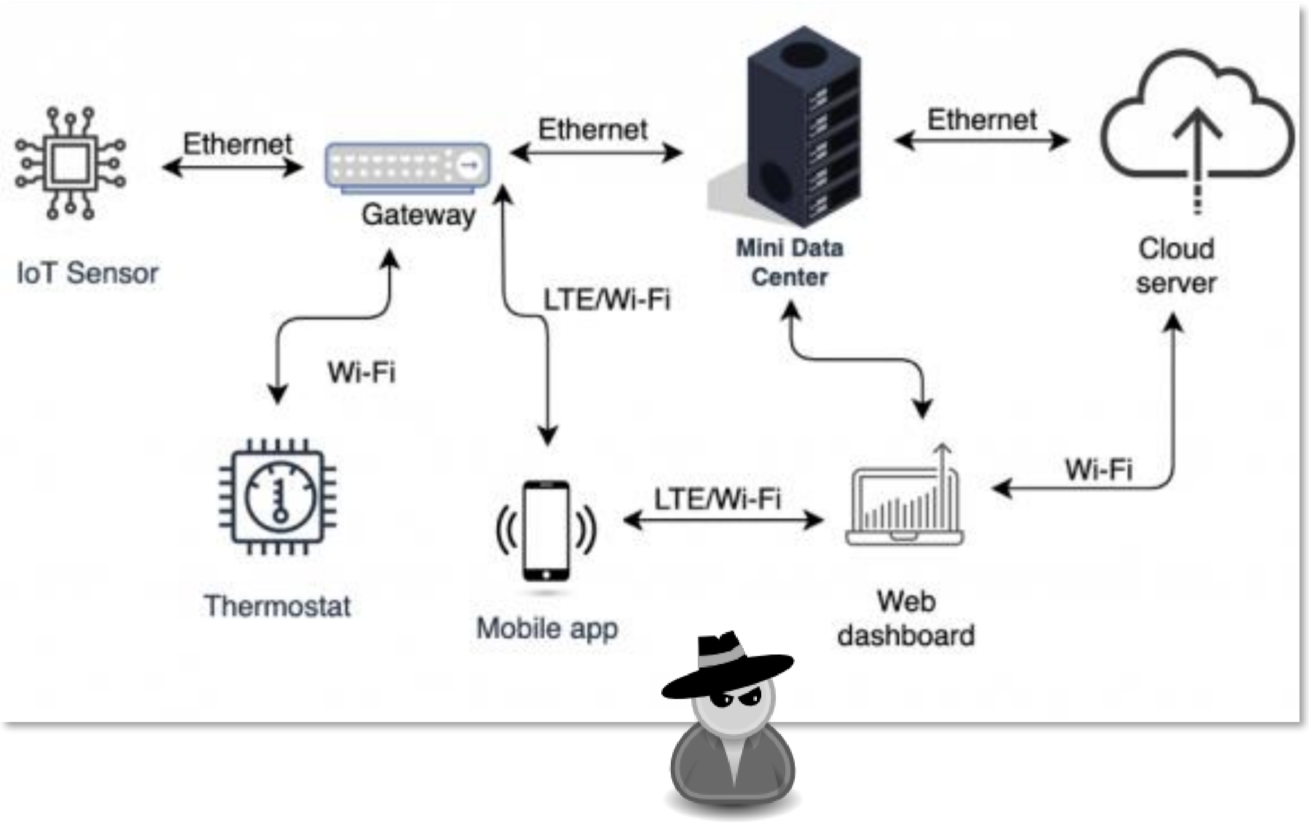




https://www.linkedin.com/pulse/implementing-namur-open-architecture-noa-jonas-berge/

- Strong physical security
- Typically <u>one way</u> communication, can be enforced with data diodes
- Data exchange between bore process control and IIoT is limited & securely provisioned
- **Lower requirement to security of end-points** (often simple analog sensors)

IoT – by definition is exposed to Internet

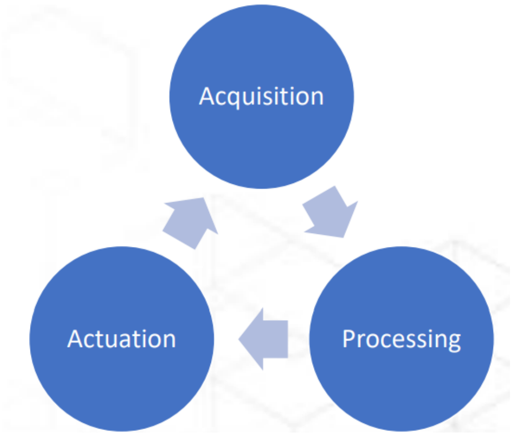


- **Physical security cannot be guaranteed**
- **Internet-connected:** directly or via some networking equipment (e.g. gateway)
- Predominately wireless communication
- **High requirement to security of end-point IoT devices**

Edge computing

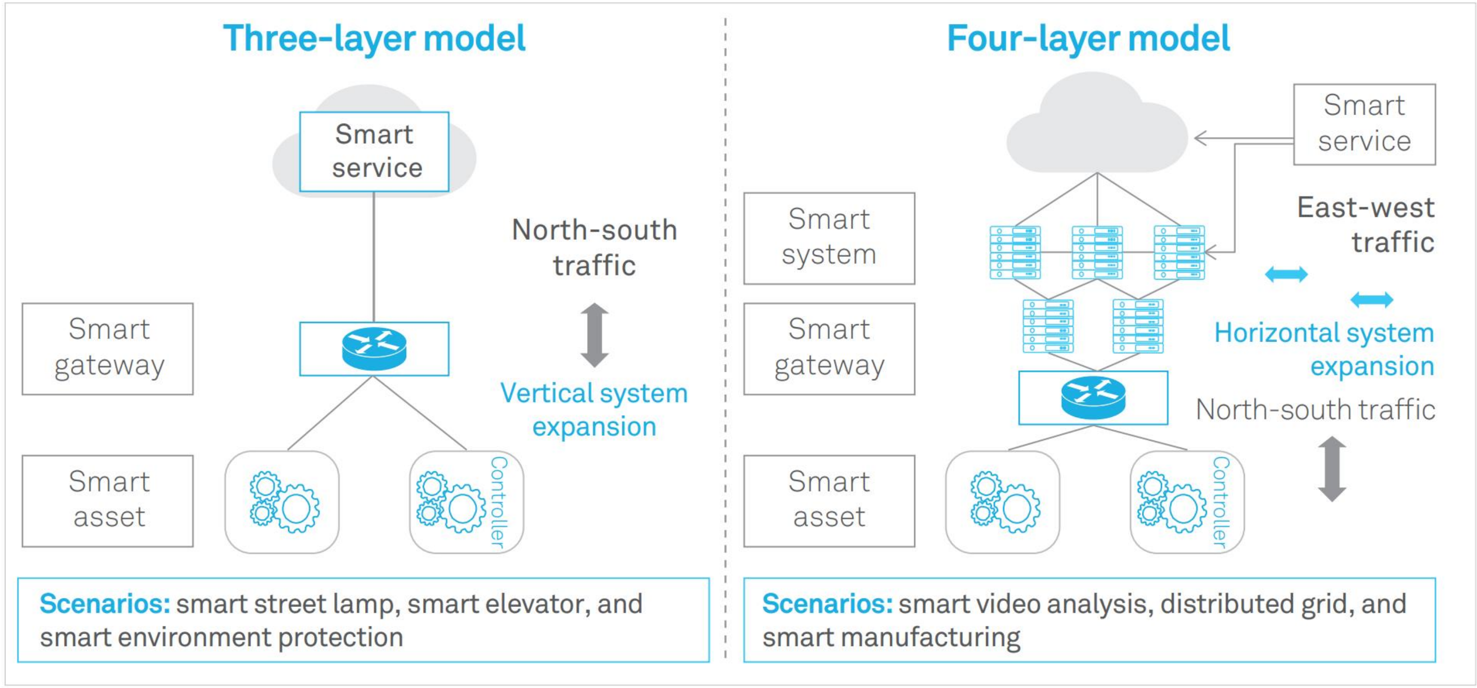
Advantages

- On premises data acquisition, processing & actuation
- Some resiliency
- Lower latency
- Less network traffic
- Data retention on premises



https://conference.hitb.org/hitb-lockdown002/sessions/the-fragile-art-of-edge-computing-walk-through-access-control-systems/

Edge Computing Reference Architecture 2.0



Scenarios: smart street lamp, smart elevator, and smart environment protection

Scenarios: smart video analysis, distributed grid, and smart manufacturing

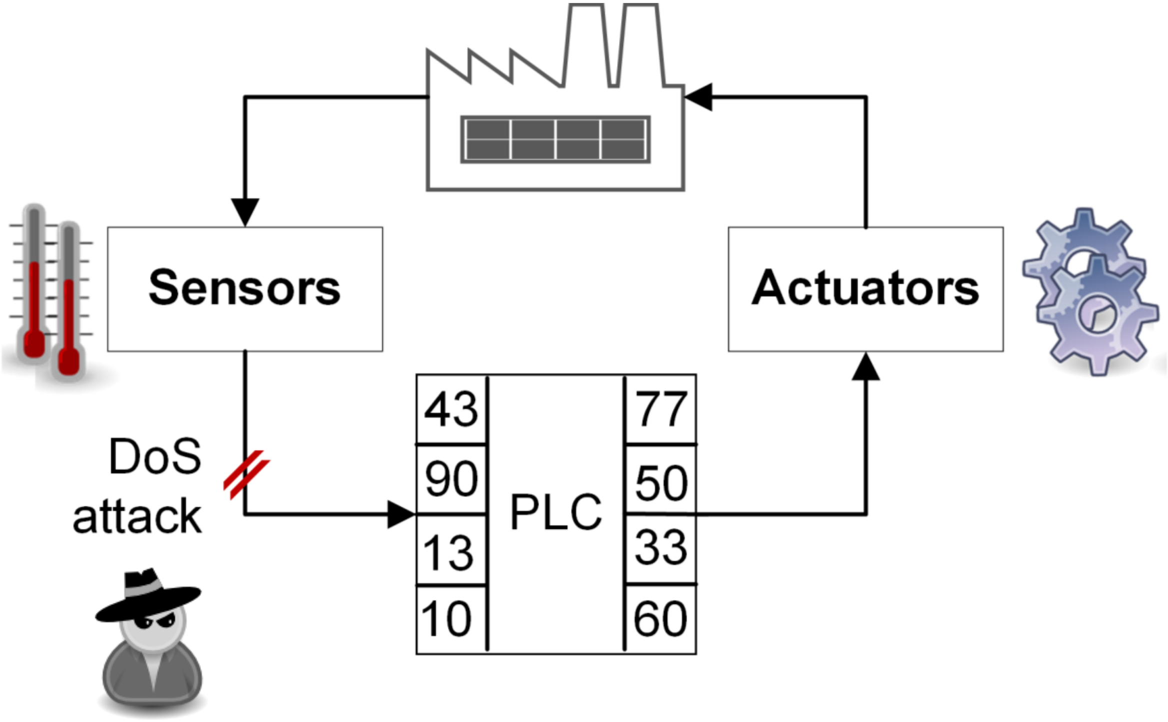
http://en.ecconsortium.net/Uploads/file/20180328/1522232376480704.pdf

Stale Data attack

Stale Data attack: Exploiting control features

- (Most) cyber-physical systems adhere to hard real-time control requirements
- Process data may only be valid for a short time & become irrelevant if arriving just few milliseconds too late
- Data timeliness must be protected and **"stale“ data** should be recognized & discarded

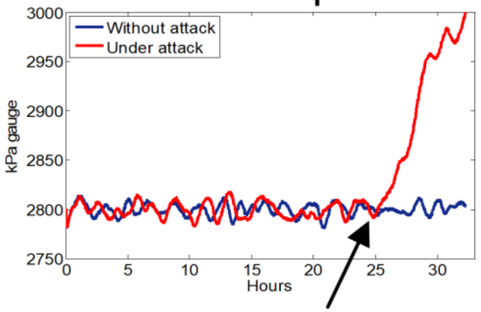
Giving “new life” to DoS attacks



Controller output

77	76	75	76	75	72	74	74	73
50	49	48	51	51	50	49	50	51
33	33	31	30	32	32	31	33	33
60	61	**62**	61	**56**	**51**	**46**	**41**	**35**

Overpressure



Attack time

PLC scan cycles

43	45	47	45	43	43	44	43	43
90	89	88	91	91	90	89	90	91
13	15	17	15	13	13	14	13	13
10	17	**10**	12	**10**	**10**	**10**	**10**	**10**

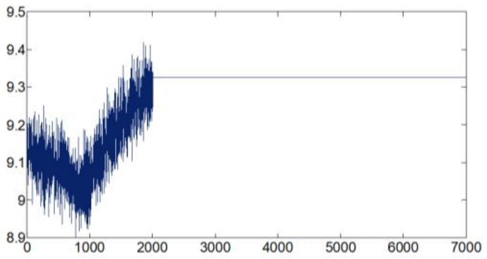
Stale data

Last stored value

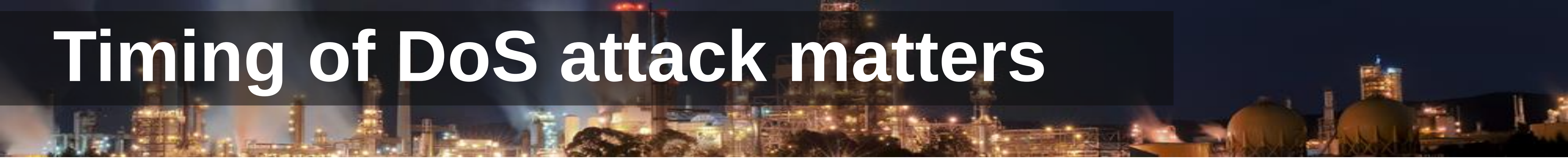
Attack time

Attack duration

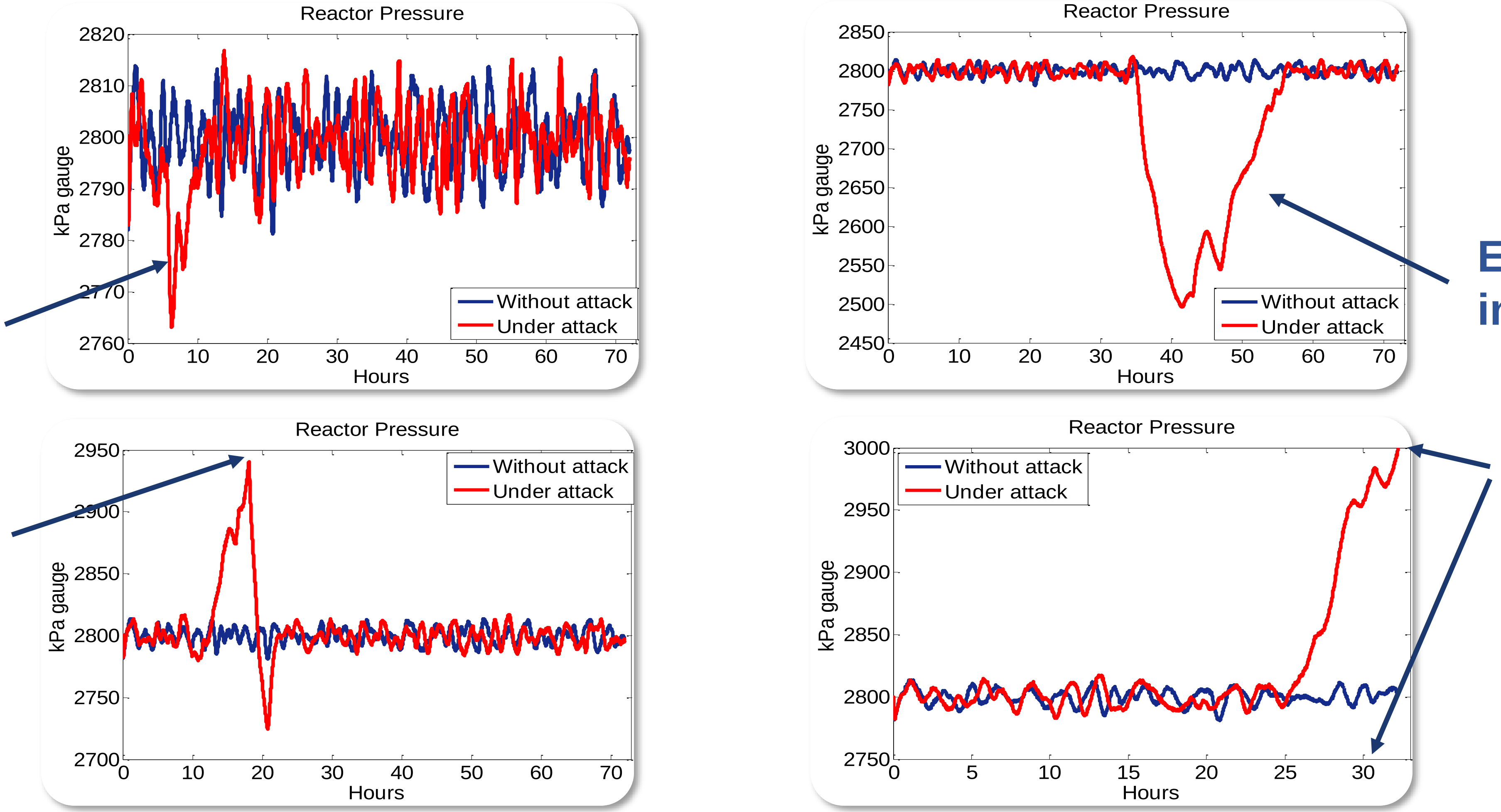
“Frozen” measurement



DoS / packet delay / packet drop / network congestion / etc.



Timing of DoS attack matters



Ordinary glitch

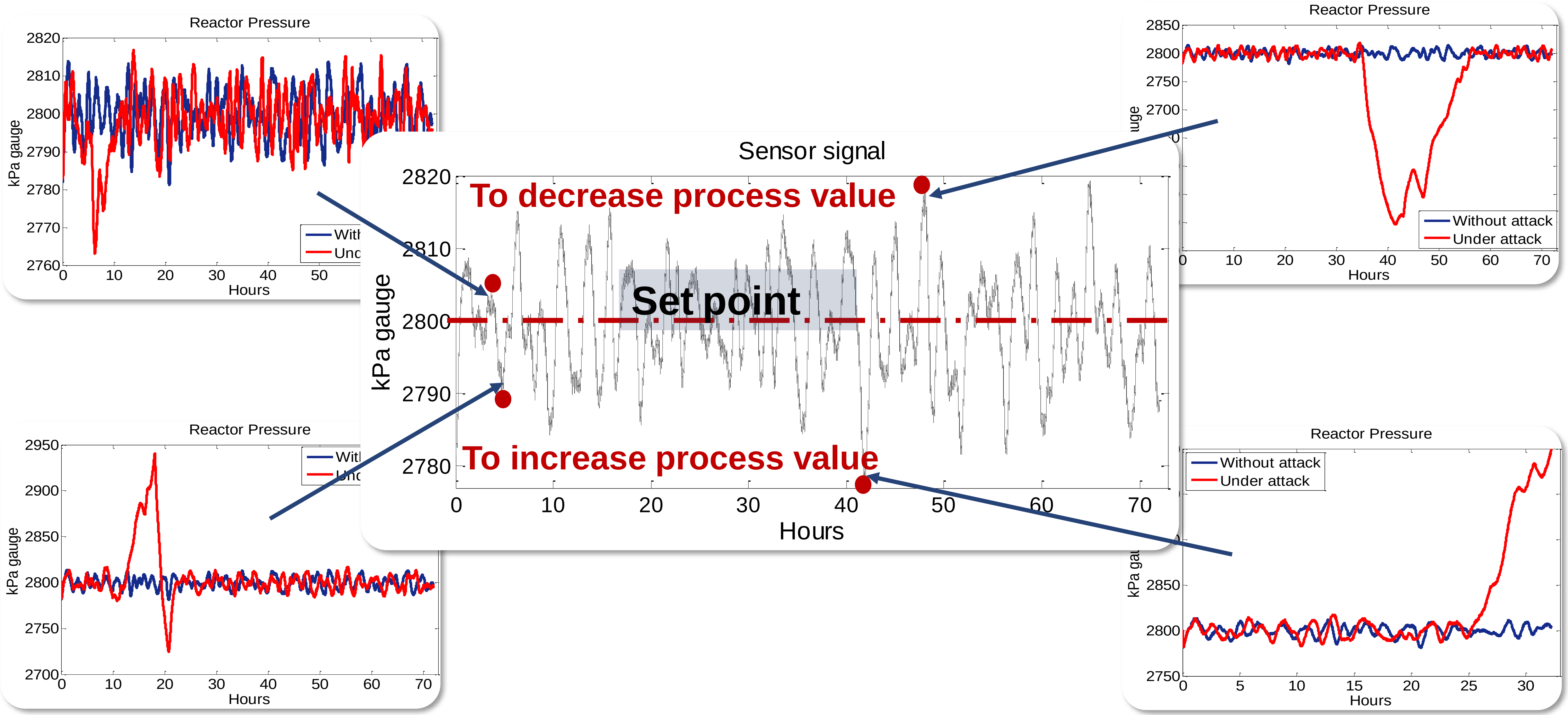
Economic inefficiency

Near miss (almost safety accident)

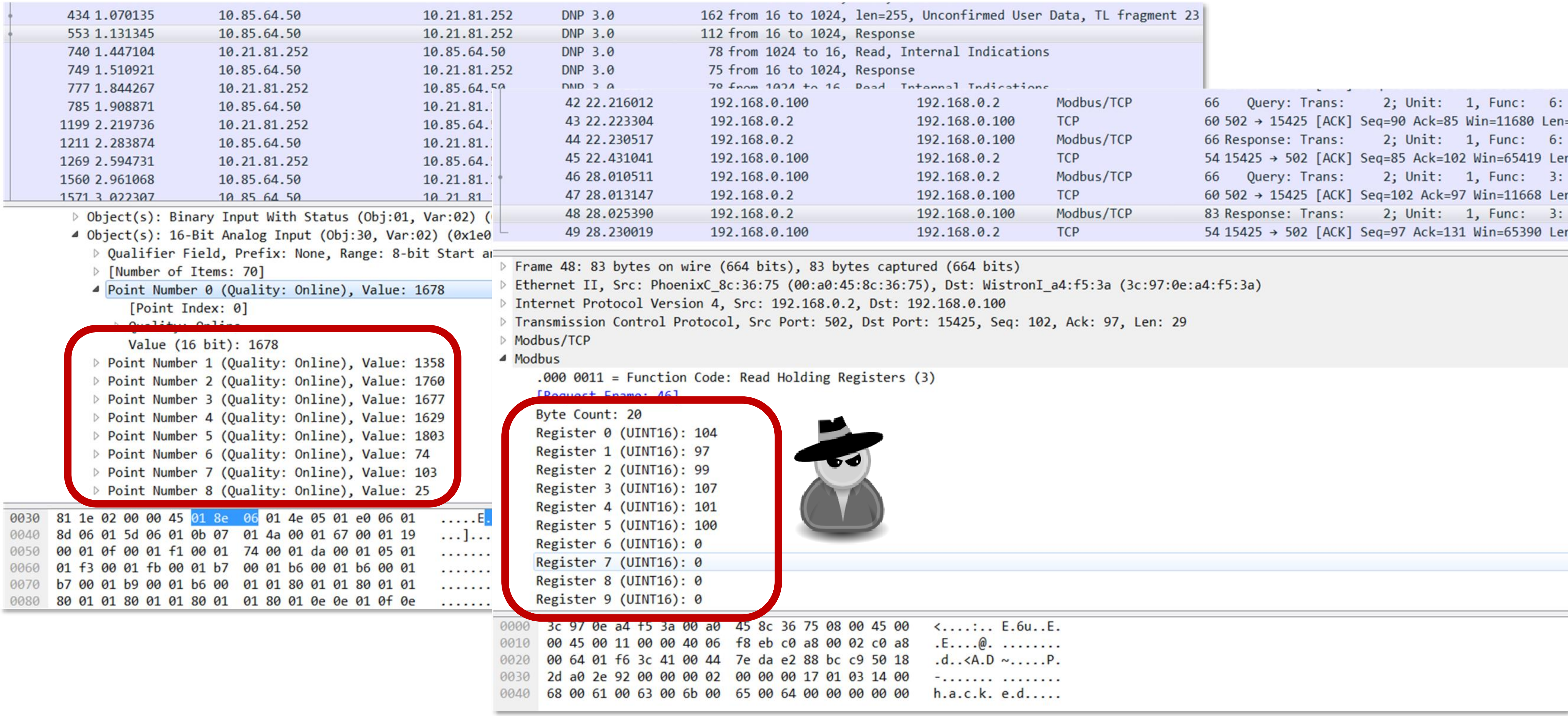
Safety shutdown

Impact of 8h long DoS attacks on reactor pressure sensor at random time

Process response depends on DoS value



Where this approach could be useful?



```
  434 1.070135   10.85.64.50    10.21.81.252   DNP 3.0   162 from 16 to 1024, len=255, Unconfirmed User Data, TL fragment 23
  553 1.131345   10.85.64.50    10.21.81.252   DNP 3.0   112 from 16 to 1024, Response
  740 1.447104   10.21.81.252   10.85.64.50    DNP 3.0    78 from 1024 to 16, Read, Internal Indications
  749 1.510921   10.85.64.50    10.21.81.252   DNP 3.0    75 from 16 to 1024, Response
  777 1.844267   10.21.81.252   10.85.64.50    DNP 3.0    78 from 1024 to 16, Read, Internal Indications
  785 1.908871   10.85.64.50    10.21.81.
 1199 2.219736   10.21.81.252   10.85.64.
 1211 2.283874   10.85.64.50    10.21.81.
 1269 2.594731   10.21.81.252   10.85.64.
 1560 2.961068   10.85.64.50    10.21.81.
 1571 3.022307   10.85.64.50    10.21.81.
```

```
▷ Object(s): Binary Input With Status (Obj:01, Var:02) (
◢ Object(s): 16-Bit Analog Input (Obj:30, Var:02) (0x1e0
  ▷ Qualifier Field, Prefix: None, Range: 8-bit Start a
  ▷ [Number of Items: 70]
  ◢ Point Number 0 (Quality: Online), Value: 1678
      [Point Index: 0]
    ▷ Quality: Online
      Value (16 bit): 1678
  ▷ Point Number 1 (Quality: Online), Value: 1358
  ▷ Point Number 2 (Quality: Online), Value: 1760
  ▷ Point Number 3 (Quality: Online), Value: 1677
  ▷ Point Number 4 (Quality: Online), Value: 1629
  ▷ Point Number 5 (Quality: Online), Value: 1803
  ▷ Point Number 6 (Quality: Online), Value: 74
  ▷ Point Number 7 (Quality: Online), Value: 103
  ▷ Point Number 8 (Quality: Online), Value: 25
```

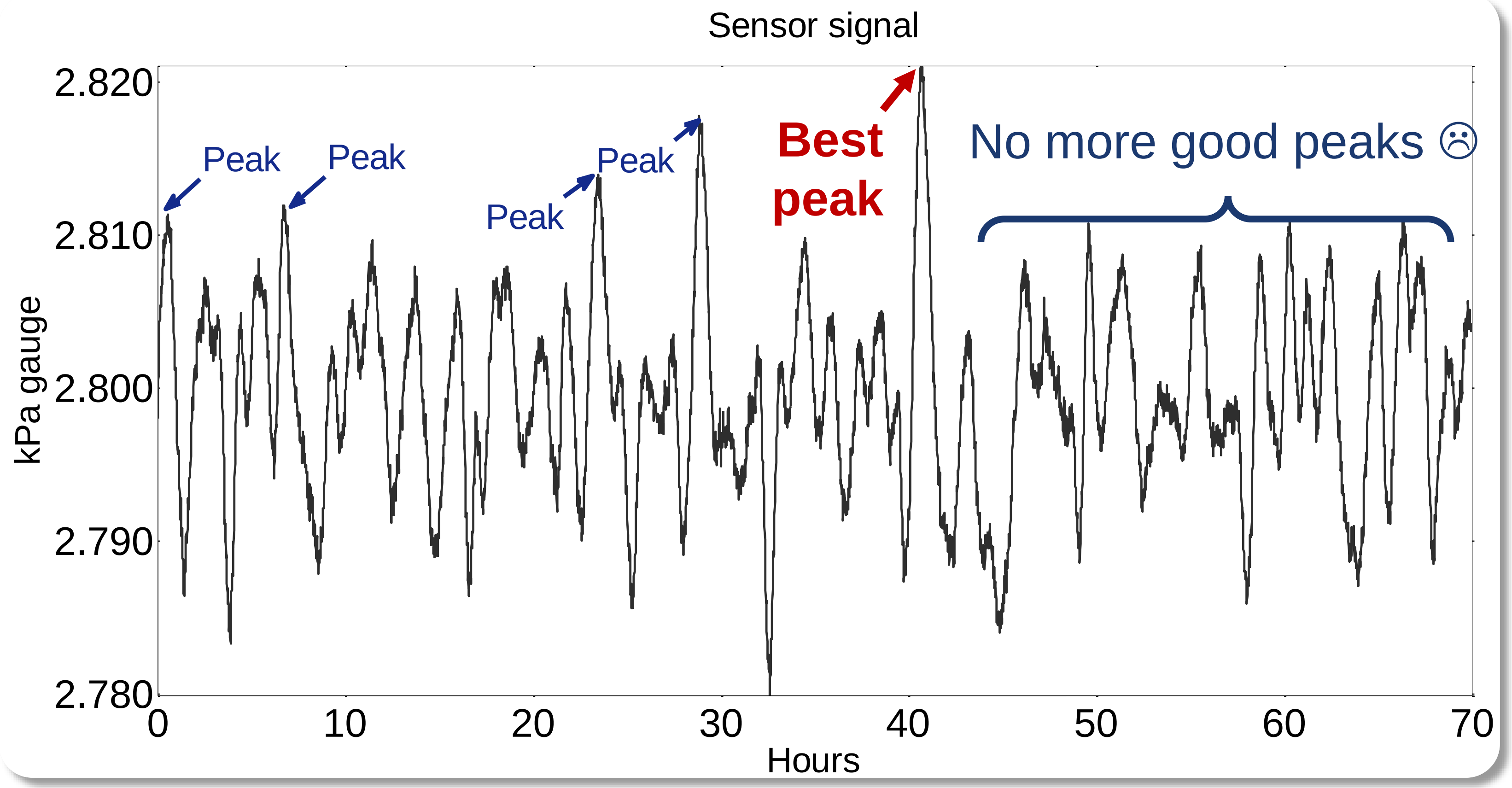
```
0030  81 1e 02 00 00 45 01 8e  06 01 4e 05 01 e0 06 01   .....E.
0040  8d 06 01 5d 06 01 0b 07  01 4a 00 01 67 00 01 19   ...]...
0050  00 01 0f 00 01 f1 00 01  74 00 01 da 00 01 05 01   .......
0060  01 f3 00 01 fb 00 01 b7  00 01 b6 00 01 b6 00 01   .......
0070  b7 00 01 b9 00 01 b6 00  01 01 80 01 01 80 01 01   .......
0080  80 01 01 80 01 01 80 01  01 80 01 0e 0e 01 0f 0e   .......
```

```
 42 22.216012   192.168.0.100   192.168.0.2     Modbus/TCP   66    Query: Trans:     2; Unit:   1, Func:   6:
 43 22.223304   192.168.0.2     192.168.0.100   TCP          60 502 → 15425 [ACK] Seq=90 Ack=85 Win=11680 Len=
 44 22.230517   192.168.0.2     192.168.0.100   Modbus/TCP   66 Response: Trans:     2; Unit:   1, Func:   6:
 45 22.431041   192.168.0.100   192.168.0.2     TCP          54 15425 → 502 [ACK] Seq=85 Ack=102 Win=65419 Len
 46 28.010511   192.168.0.100   192.168.0.2     Modbus/TCP   66    Query: Trans:     2; Unit:   1, Func:   3:
 47 28.013147   192.168.0.2     192.168.0.100   TCP          60 502 → 15425 [ACK] Seq=102 Ack=97 Win=11668 Len
 48 28.025390   192.168.0.2     192.168.0.100   Modbus/TCP   83 Response: Trans:     2; Unit:   1, Func:   3:
 49 28.230019   192.168.0.100   192.168.0.2     TCP          54 15425 → 502 [ACK] Seq=97 Ack=131 Win=65390 Len
```

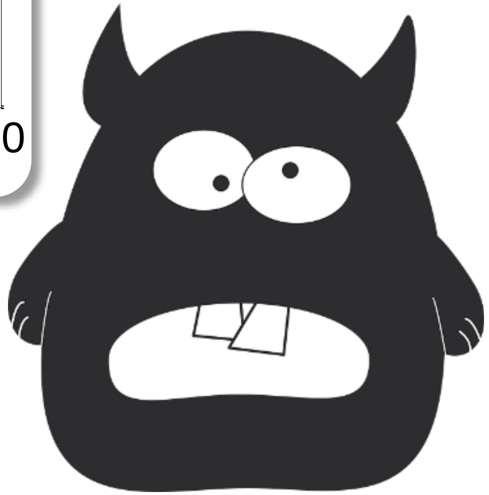
```
▷ Frame 48: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
▷ Ethernet II, Src: PhoenixC_8c:36:75 (00:a0:45:8c:36:75), Dst: WistronI_a4:f5:3a (3c:97:0e:a4:f5:3a)
▷ Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.100
▷ Transmission Control Protocol, Src Port: 502, Dst Port: 15425, Seq: 102, Ack: 97, Len: 29
▷ Modbus/TCP
◢ Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    [Request Frame: 46]
    Byte Count: 20
    Register 0 (UINT16): 104
    Register 1 (UINT16): 97
    Register 2 (UINT16): 99
    Register 3 (UINT16): 107
    Register 4 (UINT16): 101
    Register 5 (UINT16): 100
    Register 6 (UINT16): 0
    Register 7 (UINT16): 0
    Register 8 (UINT16): 0
    Register 9 (UINT16): 0
```

```
0000  3c 97 0e a4 f5 3a 00 a0  45 8c 36 75 08 00 45 00   <....:.. E.6u..E.
0010  00 45 00 11 00 00 40 06  f8 eb c0 a8 00 02 c0 a8   .E....@. ........
0020  00 64 01 f6 3c 41 00 44  7e da e2 88 bc c9 50 18   .d..<A.D ~.....P.
0030  2d a0 2e 92 00 00 00 02  00 00 00 17 01 03 14 00   -....... ........
0040  68 00 61 00 63 00 6b 00  65 00 64 00 00 00 00 00   h.a.c.k. e.d.....
```

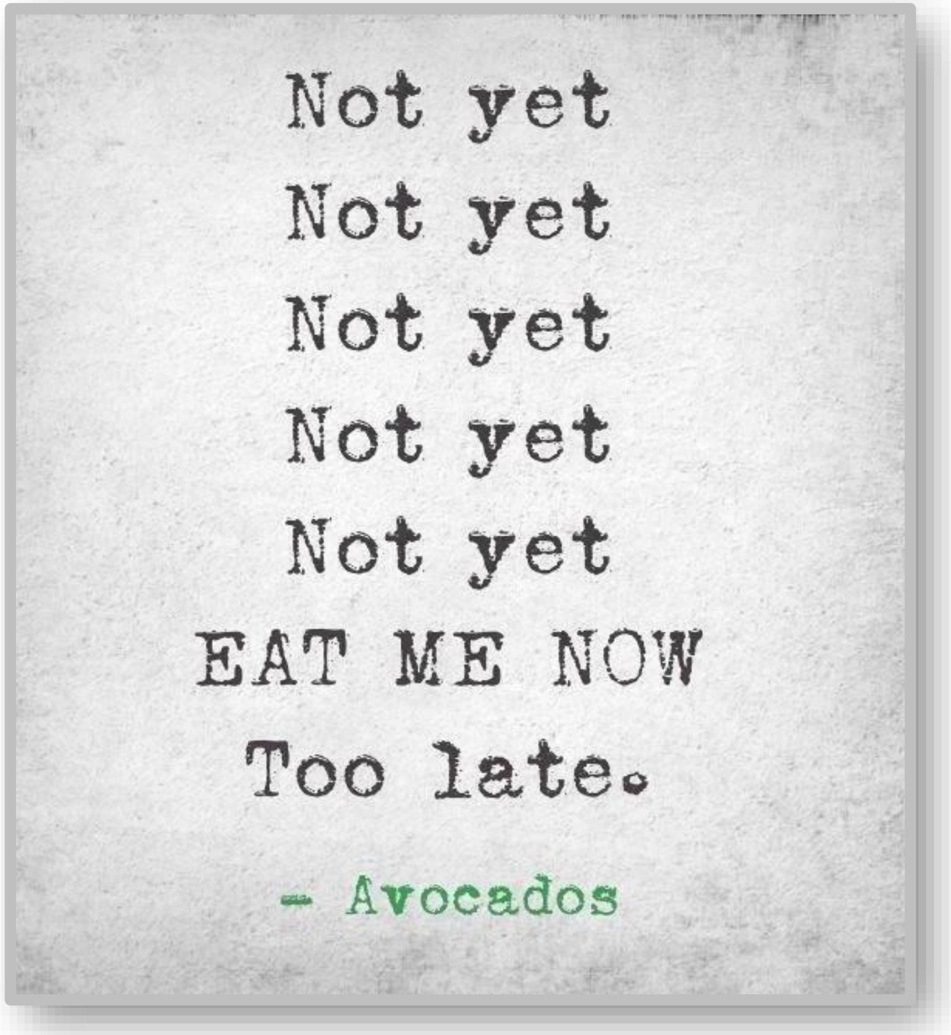
Quest for best peak



- **REAL TIME** decision making problem
- Searching for the **“BEST”** peak
- Achieving results within some time horizon



Avocado problem



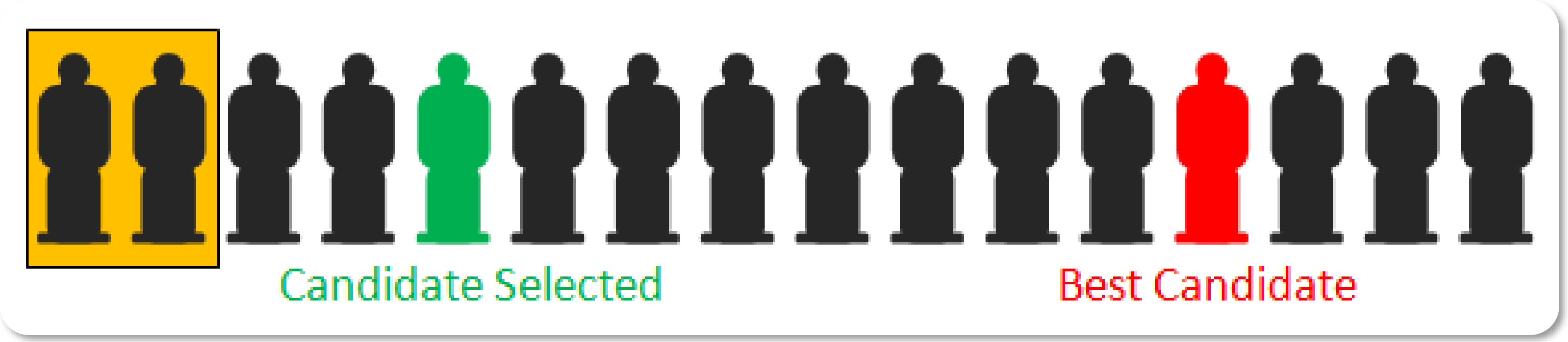
Not yet
Not yet
Not yet
Not yet
Not yet
EAT ME NOW
Too late.

– Avocados

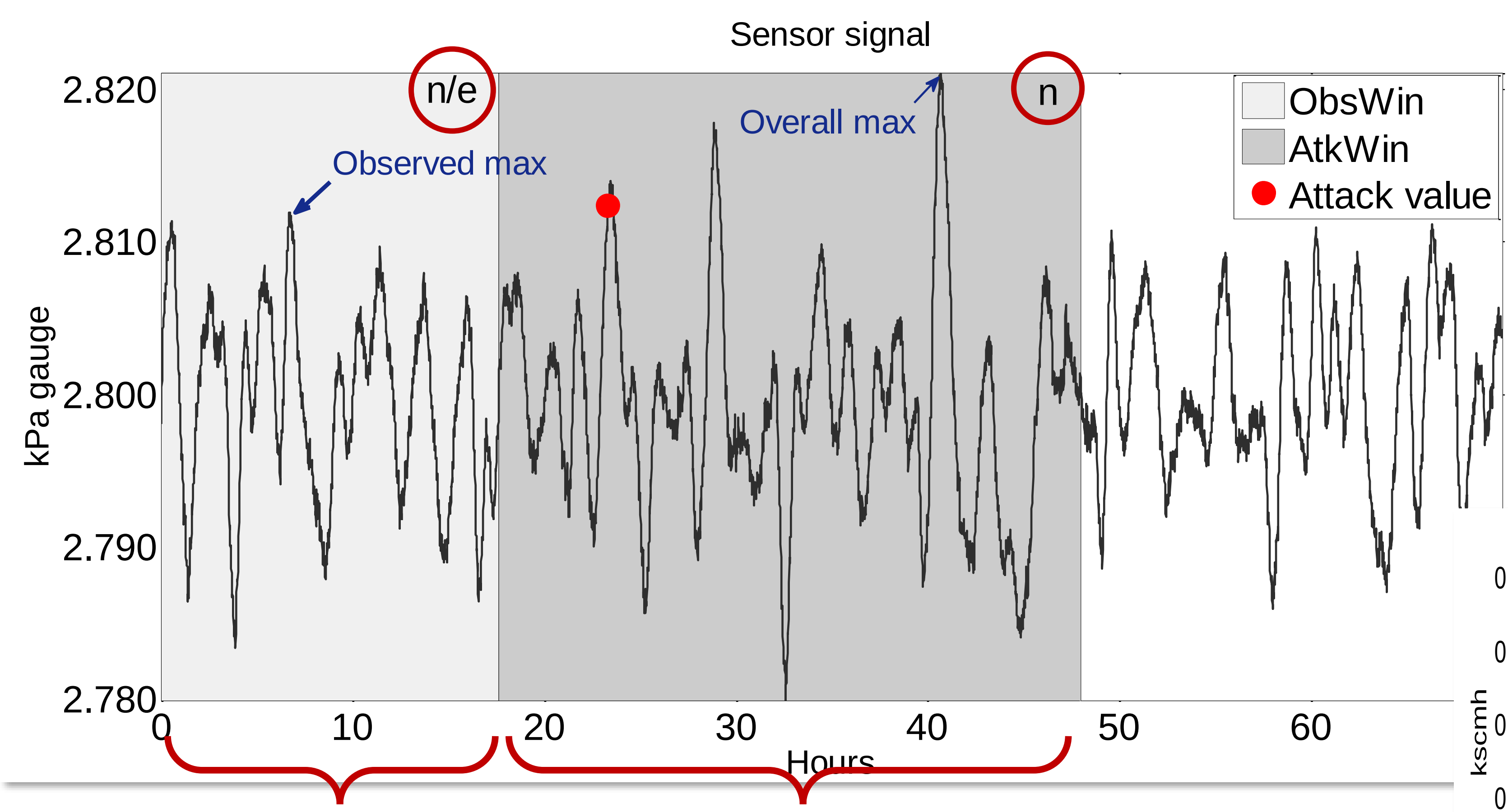
Avocado problem

- Problem of choosing the time to take a particular action
  - Based on sequentially observed random variables
  - In order to maximize an expected pay off
- Applied in a wide range of applications including financial
  - Best time to buy or sell stocks

Secretary Problem



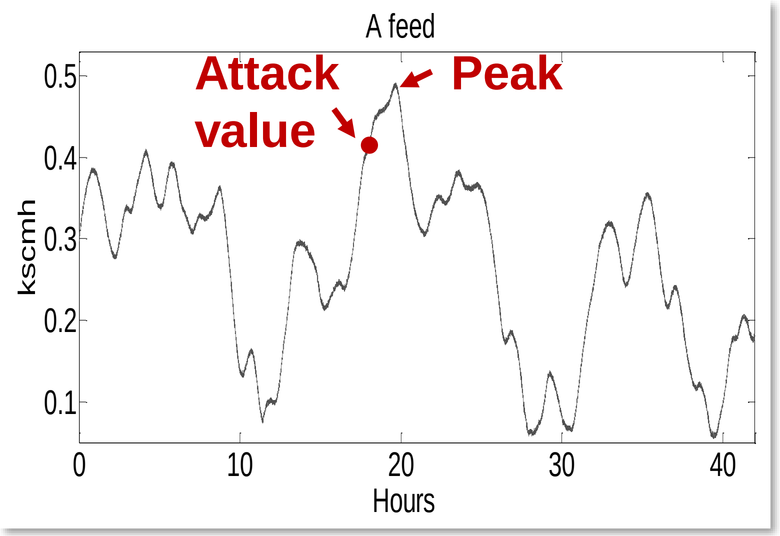
Secretary Problem applied to sensor signal

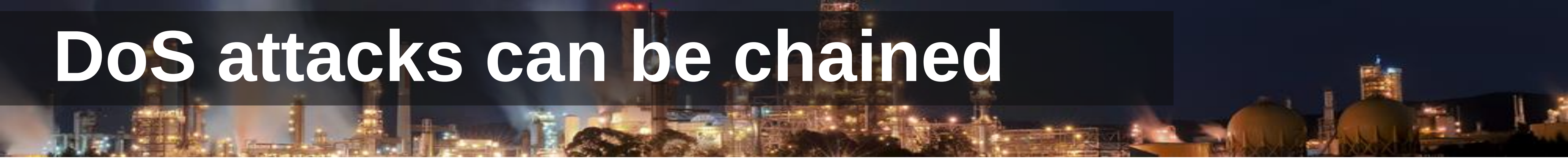


Observation window

Attack window

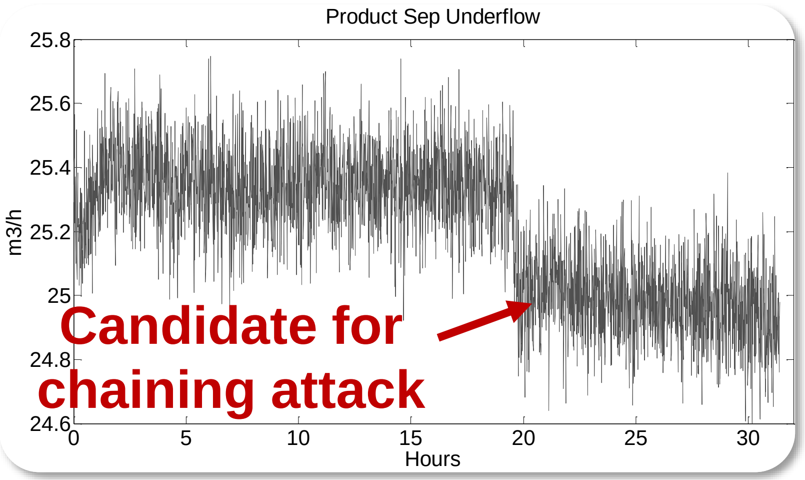
- **n** – number of hours (e.g. 24 hrs)
- **Number of candidates:** # sensor signal samples in 24 hrs



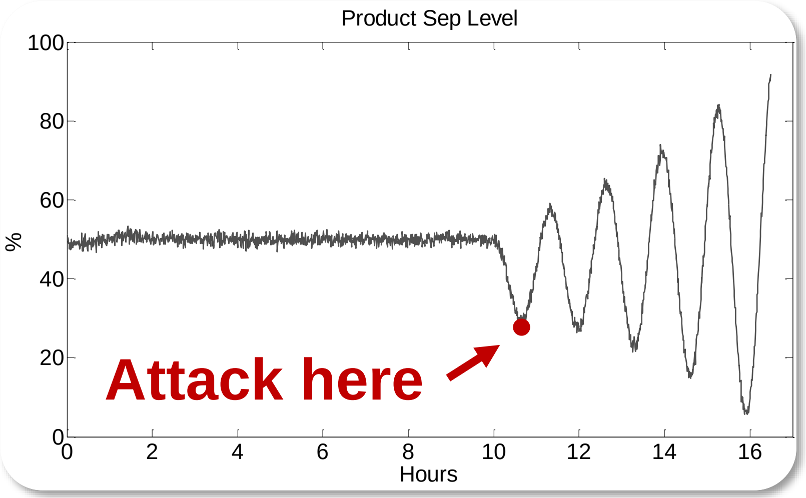


DoS attacks can be chained

- **Chain DoS attacks: on sensors**
- Use change detection algorithms (e.g. CUSUM) to detect state change

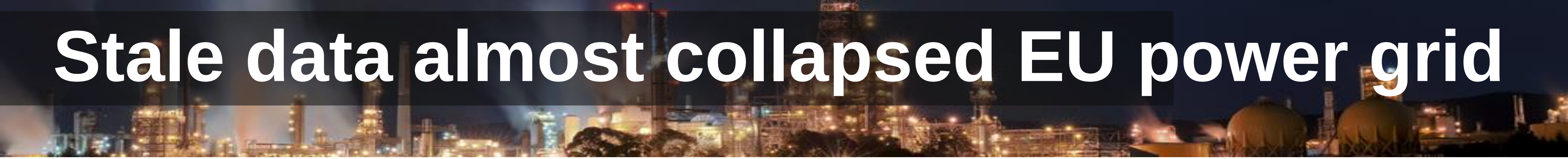


Candidate for chaining attack



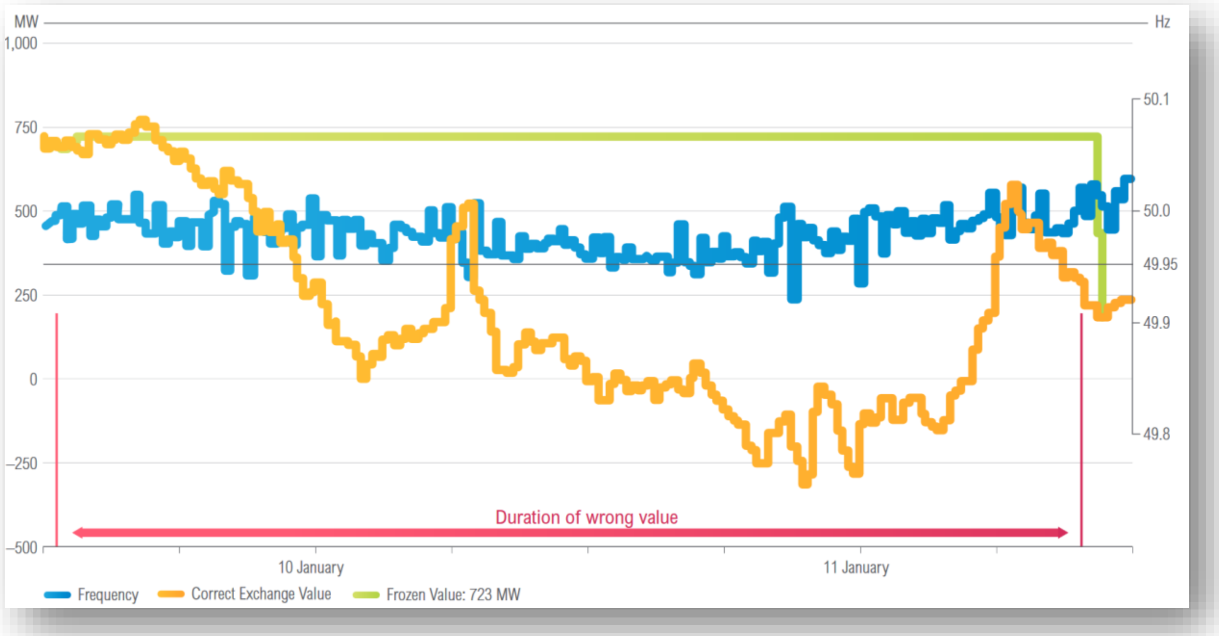
Attack here

- **Chain two DoS attacks:** on sensor & actuator
- Unsafe state achieved in **3.43 h** vs. **12.03 h** in case of direct attack



Stale data almost collapsed EU power grid

- On 10 January 2019, 21:02 CET, the Continental Europe Power System which stretches across 26 countries registered for nine seconds the largest absolute frequency deviation since 2006. Among the main causes of the incident was a failure of a communication line, which resulted in **stale data**

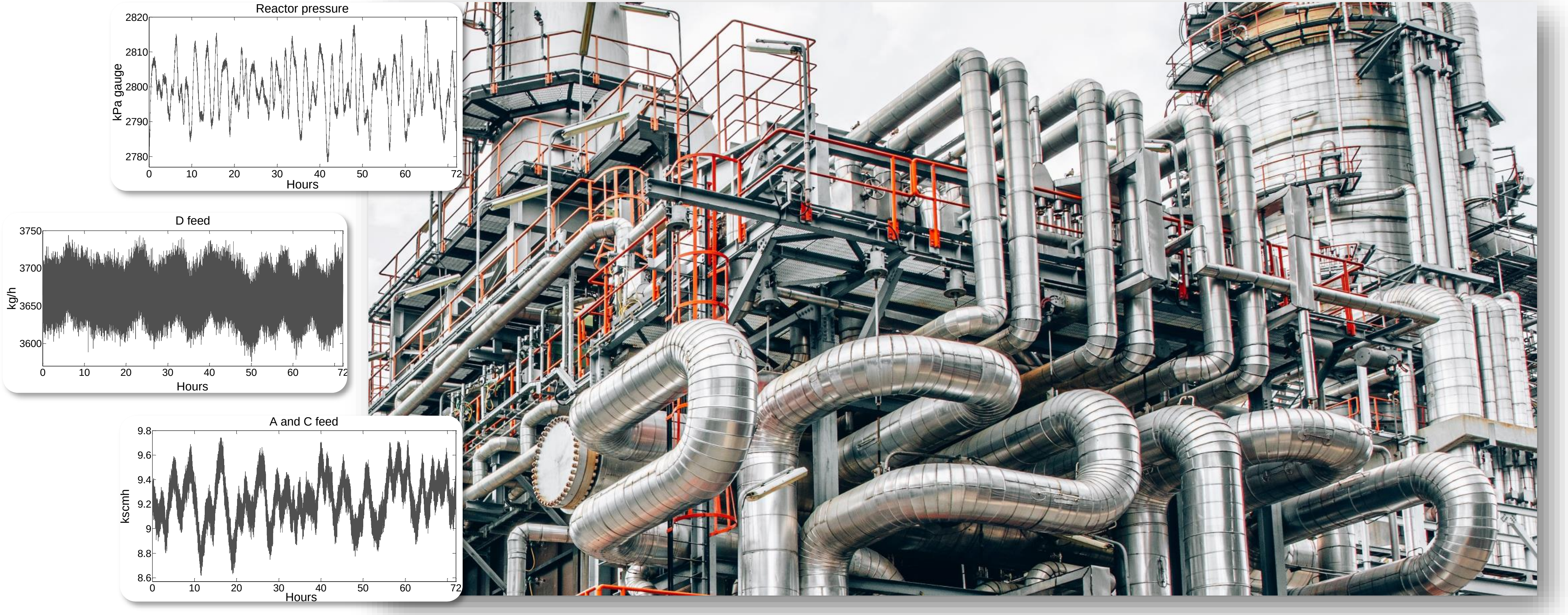


https://eepublicdownloads.entsoe.eu/clean-documents/news/2019/190522_SOC_TOP_11.6_Task%20Force%20Significant%20Frequency%20Deviations_External%20Report.pdf

Data Veracity attack

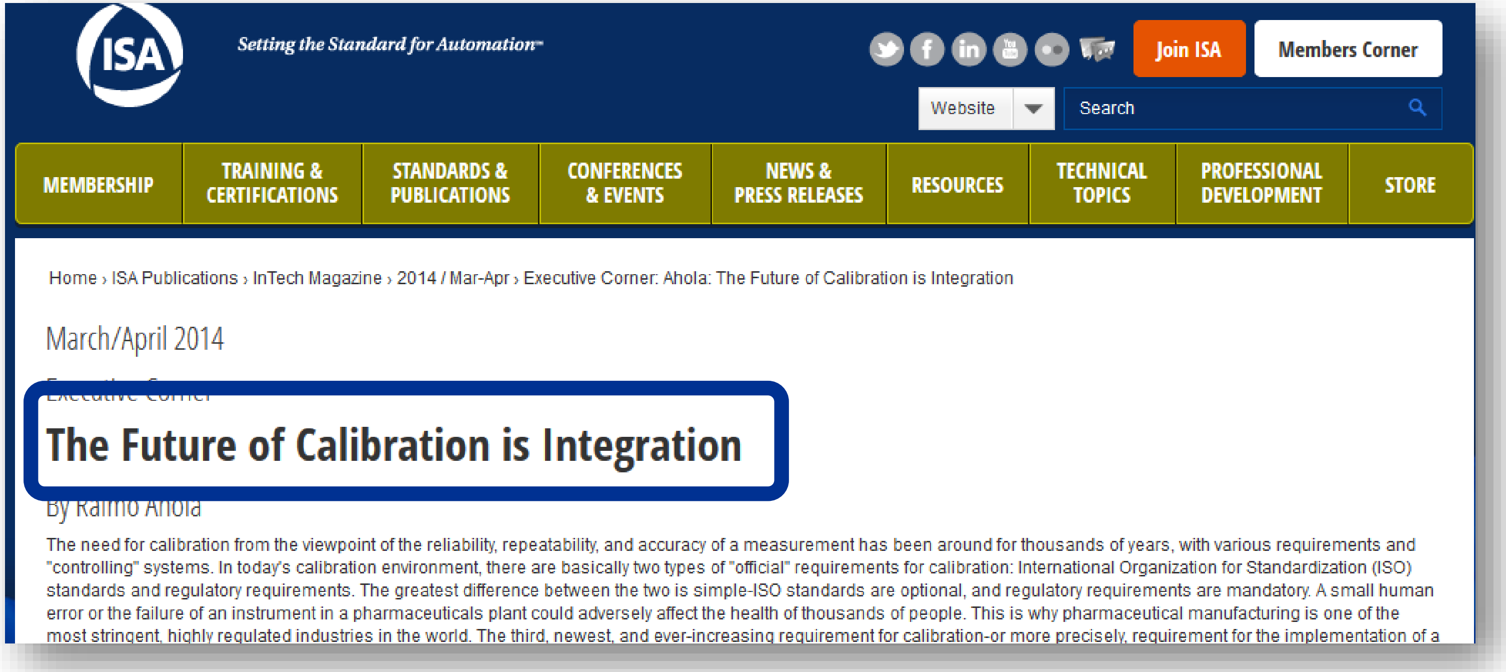
Process data security requirements

- Process data originate in physical world and their accuracy is paramount



Example: Instrument calibration

InTech, ISA magazine, April 2014



ISA Setting the Standard for Automation™

Home › ISA Publications › InTech Magazine › 2014 / Mar-Apr › Executive Corner: Ahola: The Future of Calibration is Integration

March/April 2014

Executive Corner

The Future of Calibration is Integration

By Raimo Ahola

The need for calibration from the viewpoint of the reliability, repeatability, and accuracy of a measurement has been around for thousands of years, with various requirements and "controlling" systems. In today's calibration environment, there are basically two types of "official" requirements for calibration: International Organization for Standardization (ISO) standards and regulatory requirements. The greatest difference between the two is simple-ISO standards are optional, and regulatory requirements are mandatory. A small human error or the failure of an instrument in a pharmaceuticals plant could adversely affect the health of thousands of people. This is why pharmaceutical manufacturing is one of the most stringent, highly regulated industries in the world. The third, newest, and ever-increasing requirement for calibration-or more precisely, requirement for the implementation of a

HIMA presentation, October 2014

- Due to a known bug at the engineering Software, all scaling of the SIS AI got altered to 0 to 100% automatically
- Altered values got loaded and activated automatically based on an unknown Bug at the same System

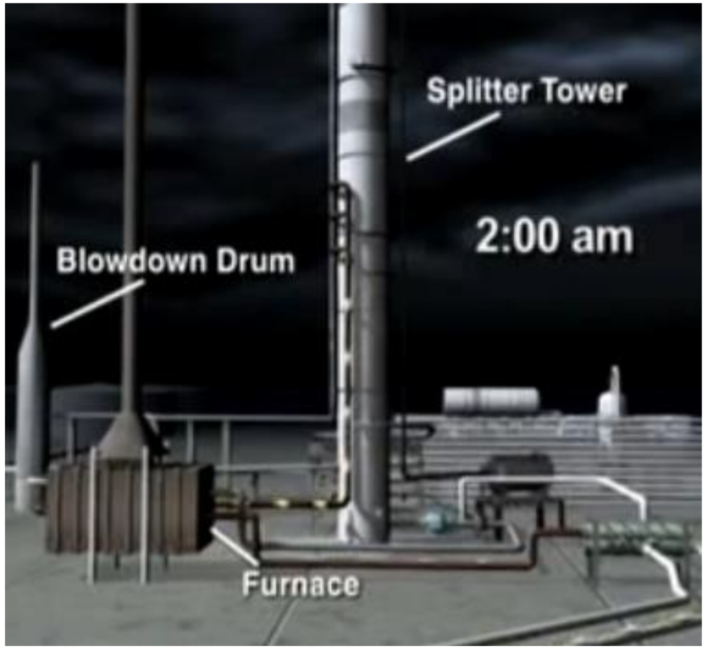
Core principle of application security

NEVER TRUST YOUR INPUTS

Veracity: data security property that a statement about an aspect relevant in a given application truthfully reflects reality

Process data security requirements

- Worst accident in the recent USA history (2005)
- 15 killed, 180 injured
- **Wrong calibration the splitter tower level indicator**
  - It showed that the tower level was declining when it was actually overfilling with flammable liquid hydrocarbons
- The further chain of events eventually led to an explosion

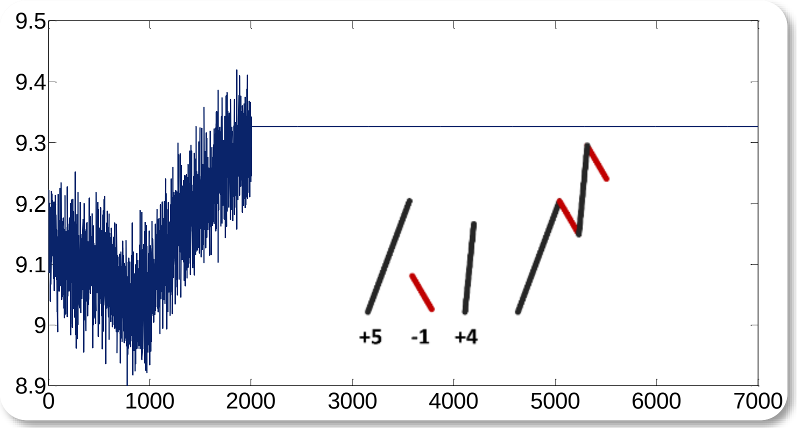


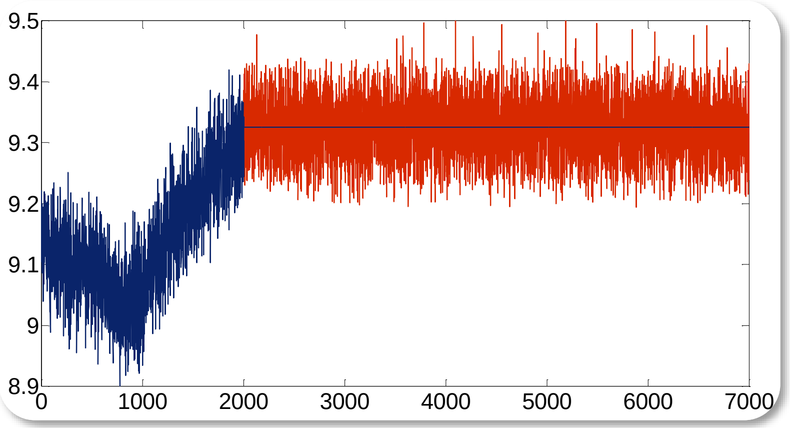
http://www.csb.gov/bp-america-refinery-explosion/

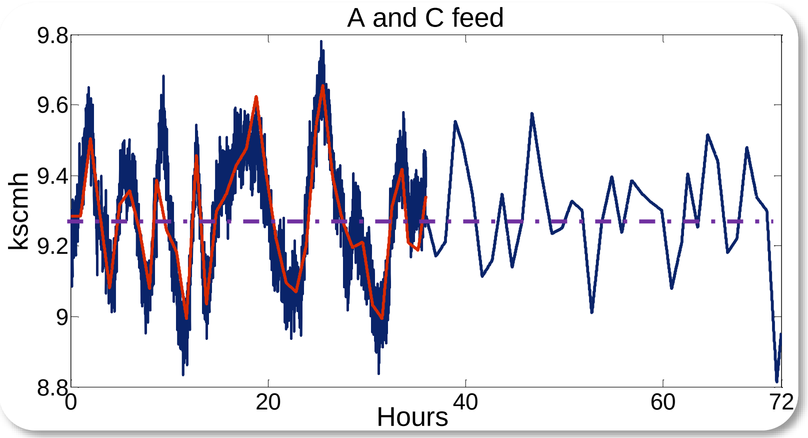
Attack concealment

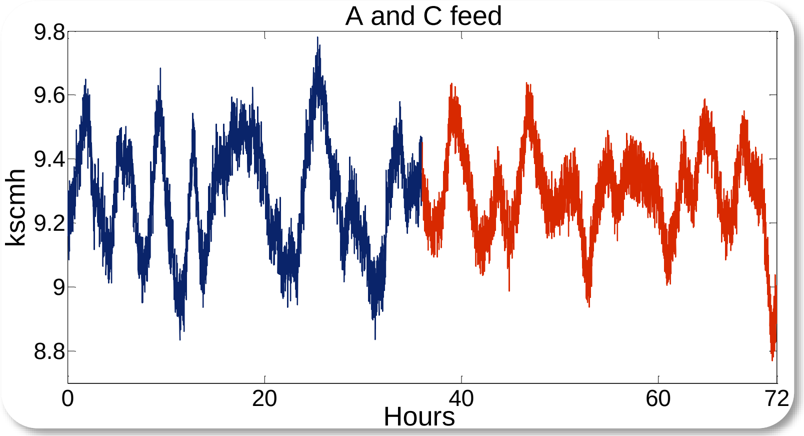
- „Record-and-play-back“
  - Used in Stuxnet ;-)
  - Storage requirements
- Derive process model
  - Requires knowledge, CPU cycles and storage
- Crafted sensor signals
  - Reconstruction of sensor data features

Spoofing sensor signals inside transmitter





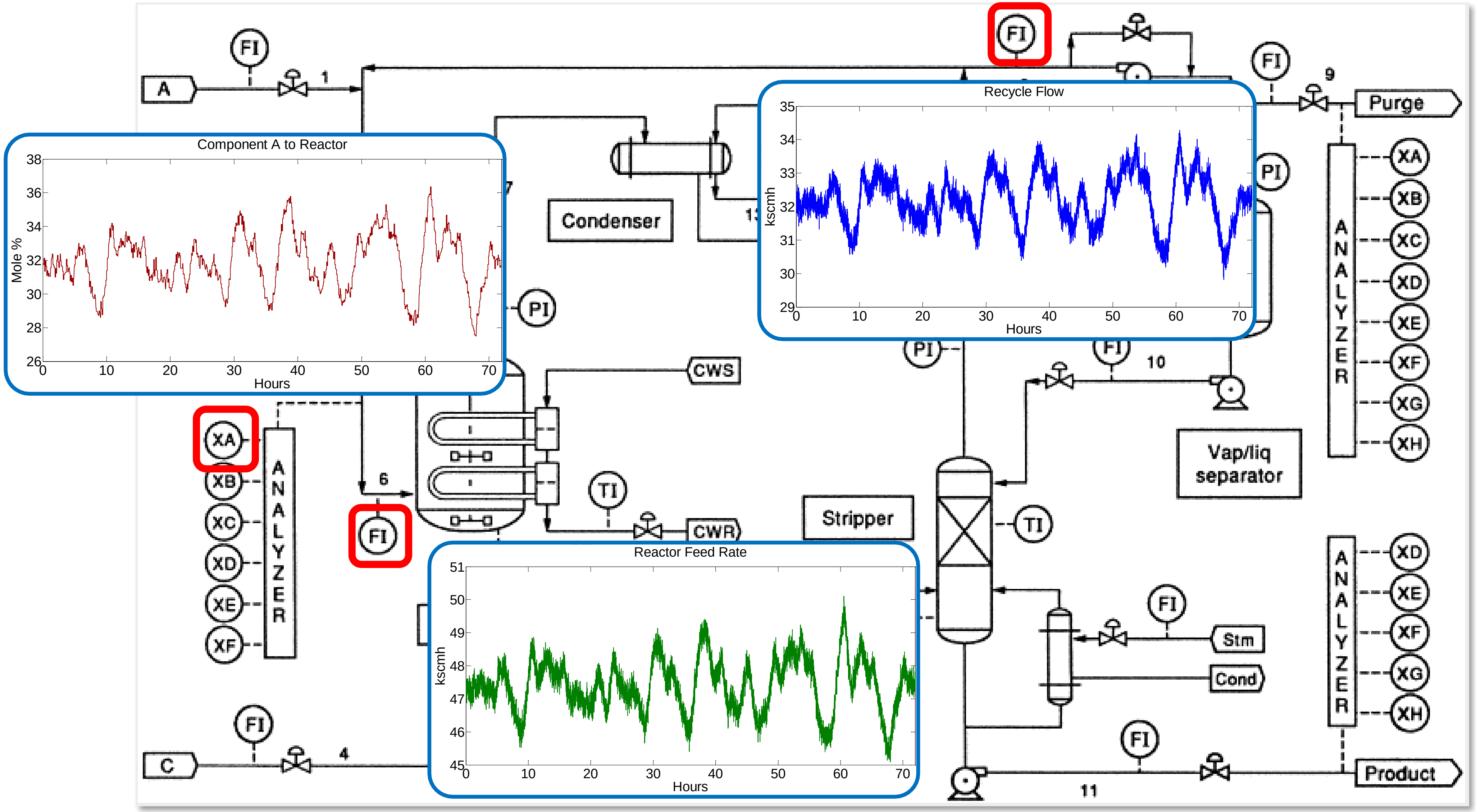




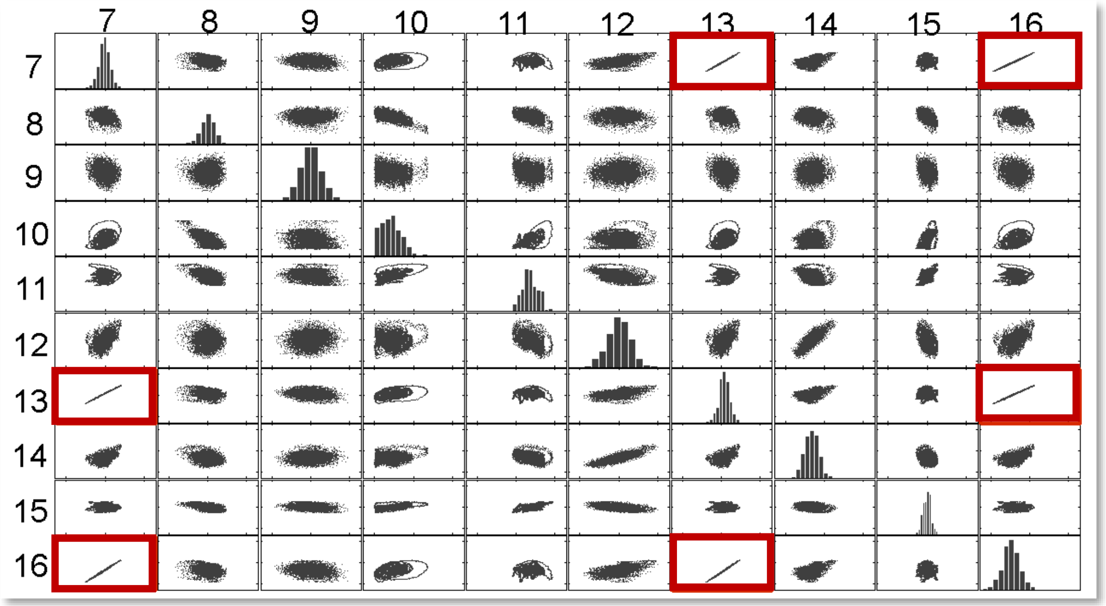
Find X differences ;-)

M. Krotofil, J. Larsen, D. Gollmann. The Process Matters: Ensuring Data Veracity in Cyber-Physical Systems (ASIACCS, 2015)

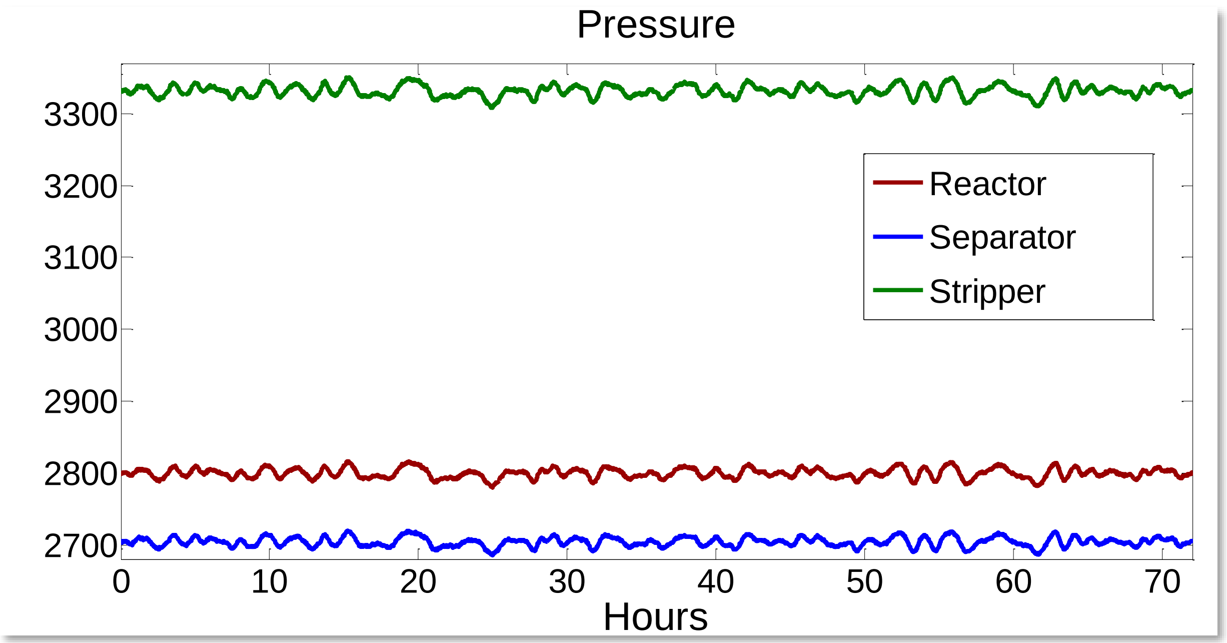
Correlated sensor signals



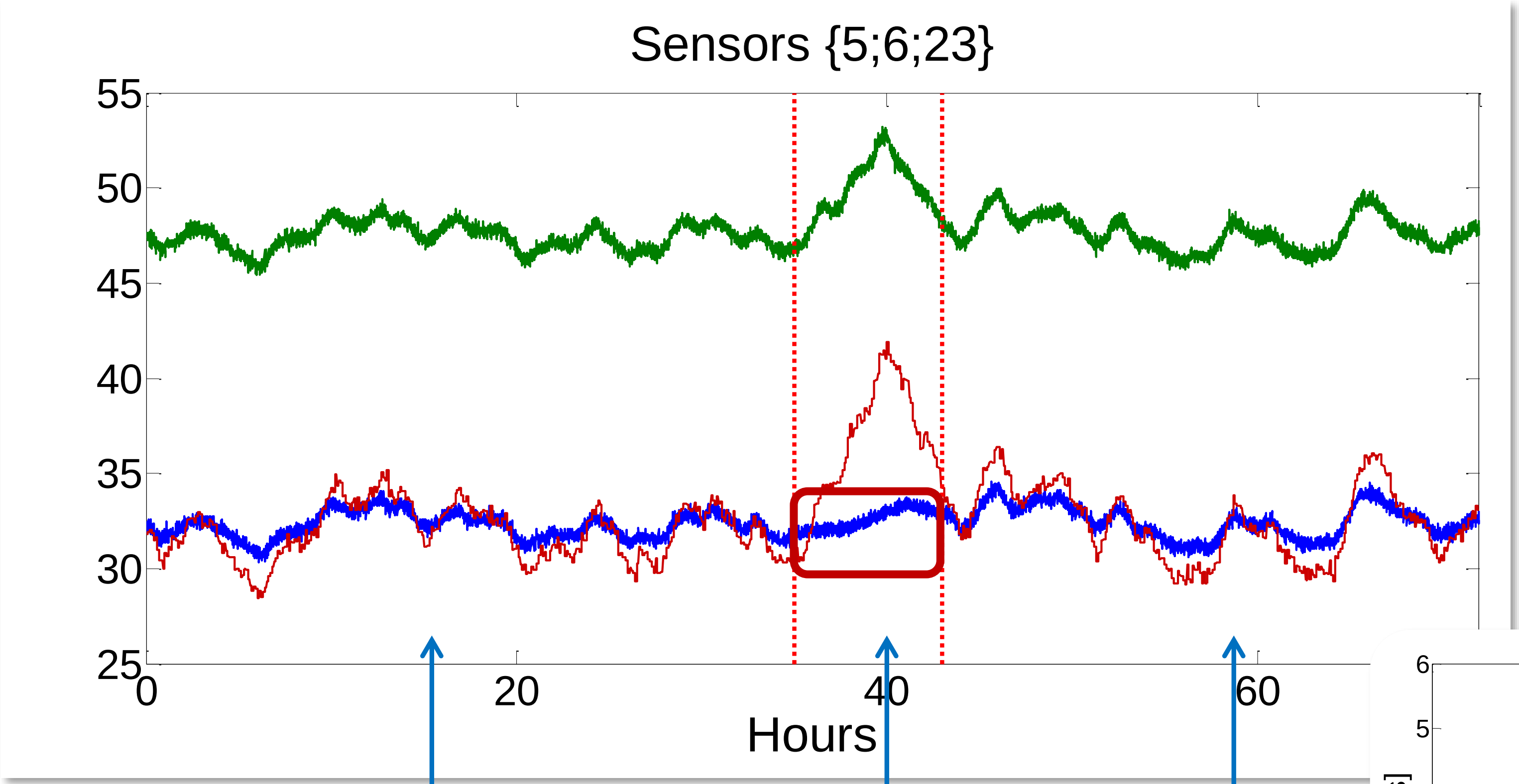
Spoofing sensor signals inside transmitter



- Scatter plot to visualize correlations between signals
- Metis tool kit: Graph partitioning for sensor clustering

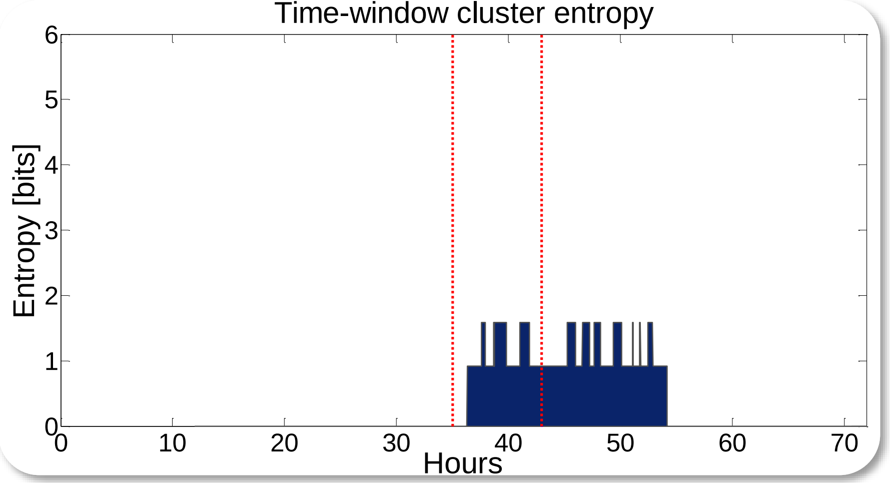


Correlation entropy



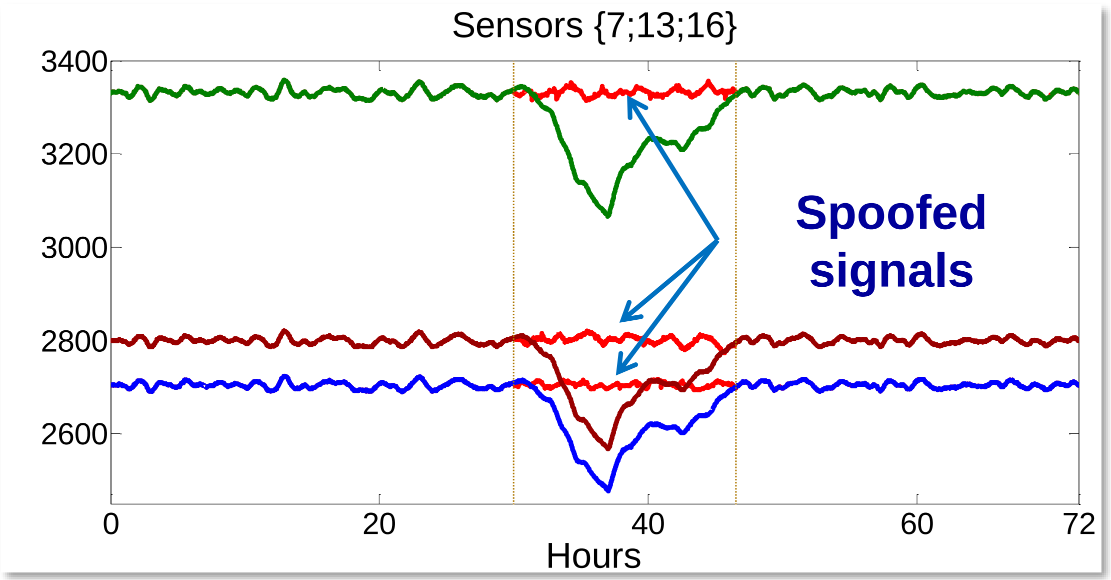
Signals correlation: + – +

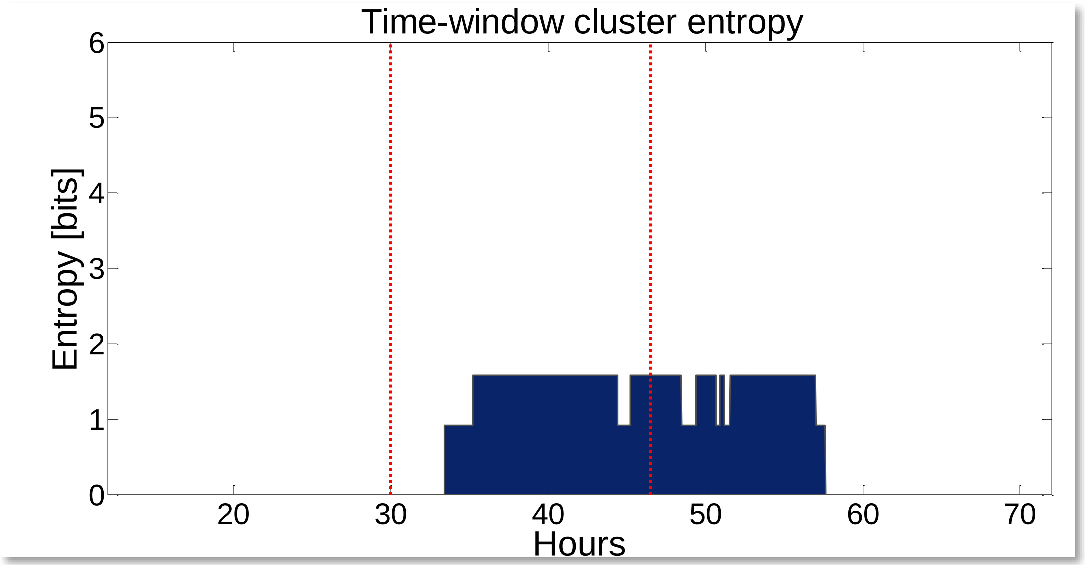
Correlation entropy: LOW HIGH LOW



Powerful attacker

He spoofed them all!!!





Bad luck ;-)

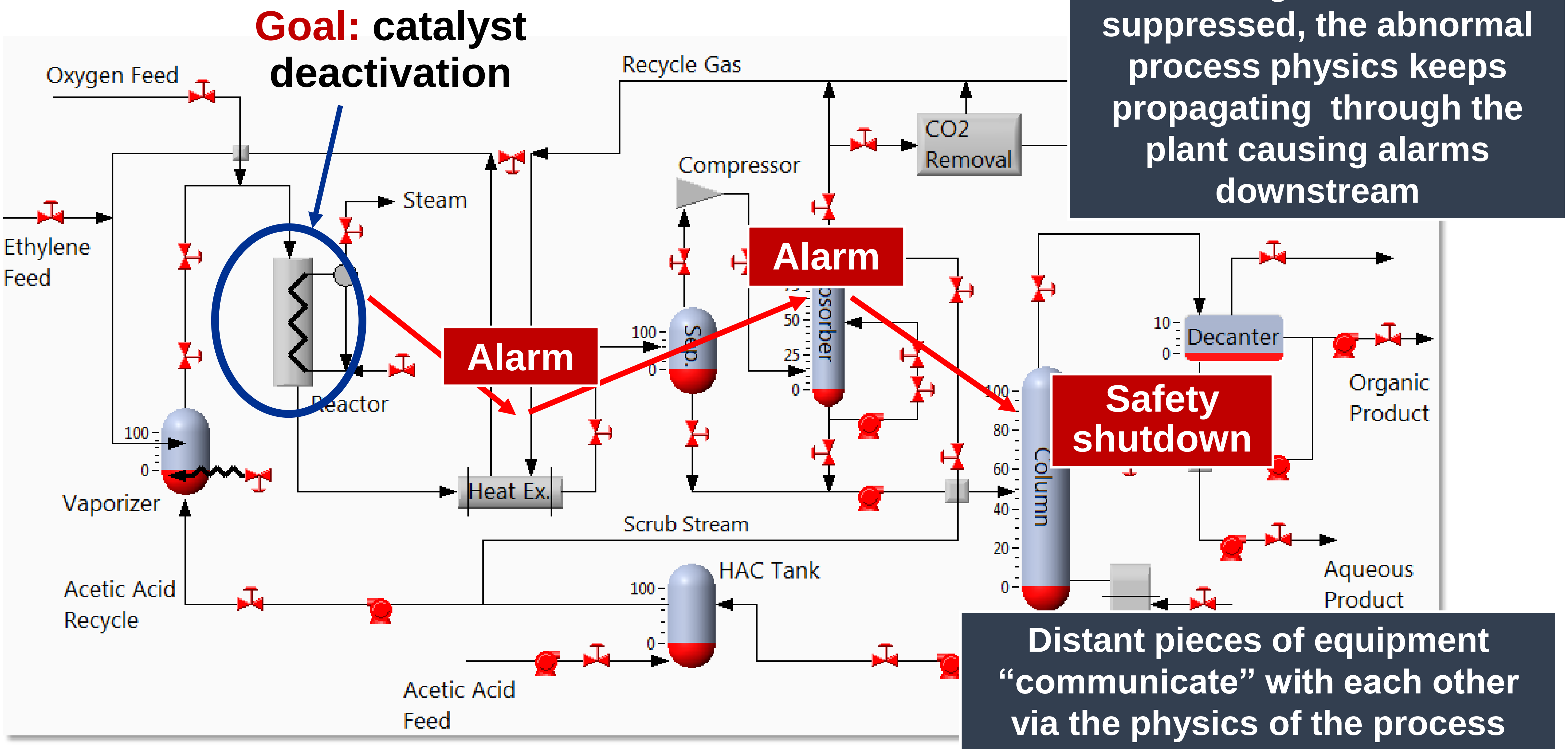
Spoofed signals will all look genuine but won't be correlated

Escaping security boundaries and Evil Bubbles attacks

Reminder: Persistent economic damage

Failed scenario: Alarm and physics propagation

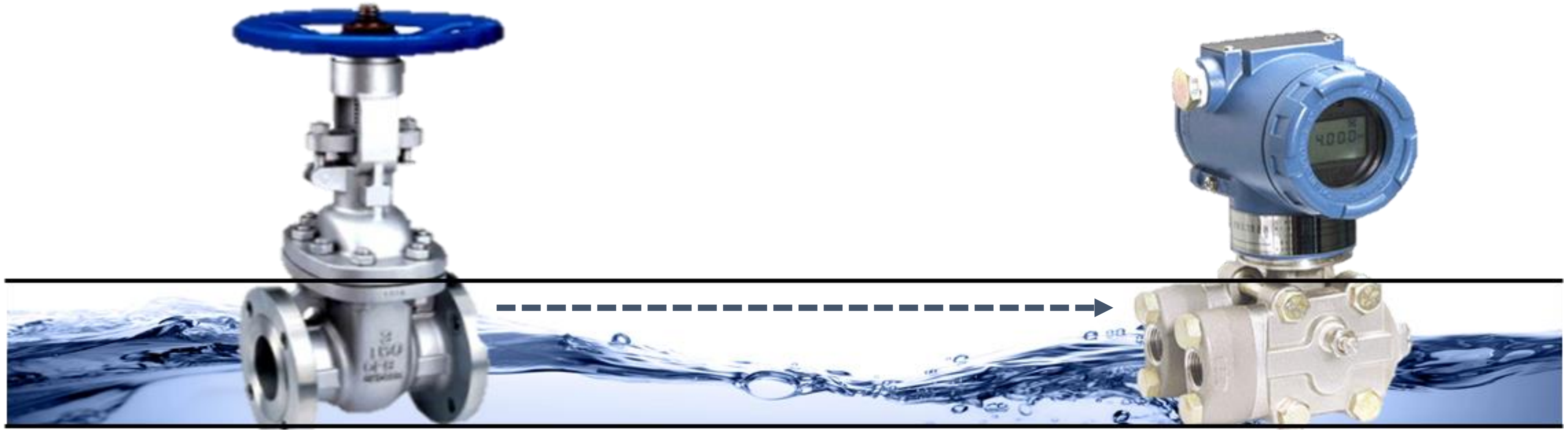
Goal: catalyst deactivation



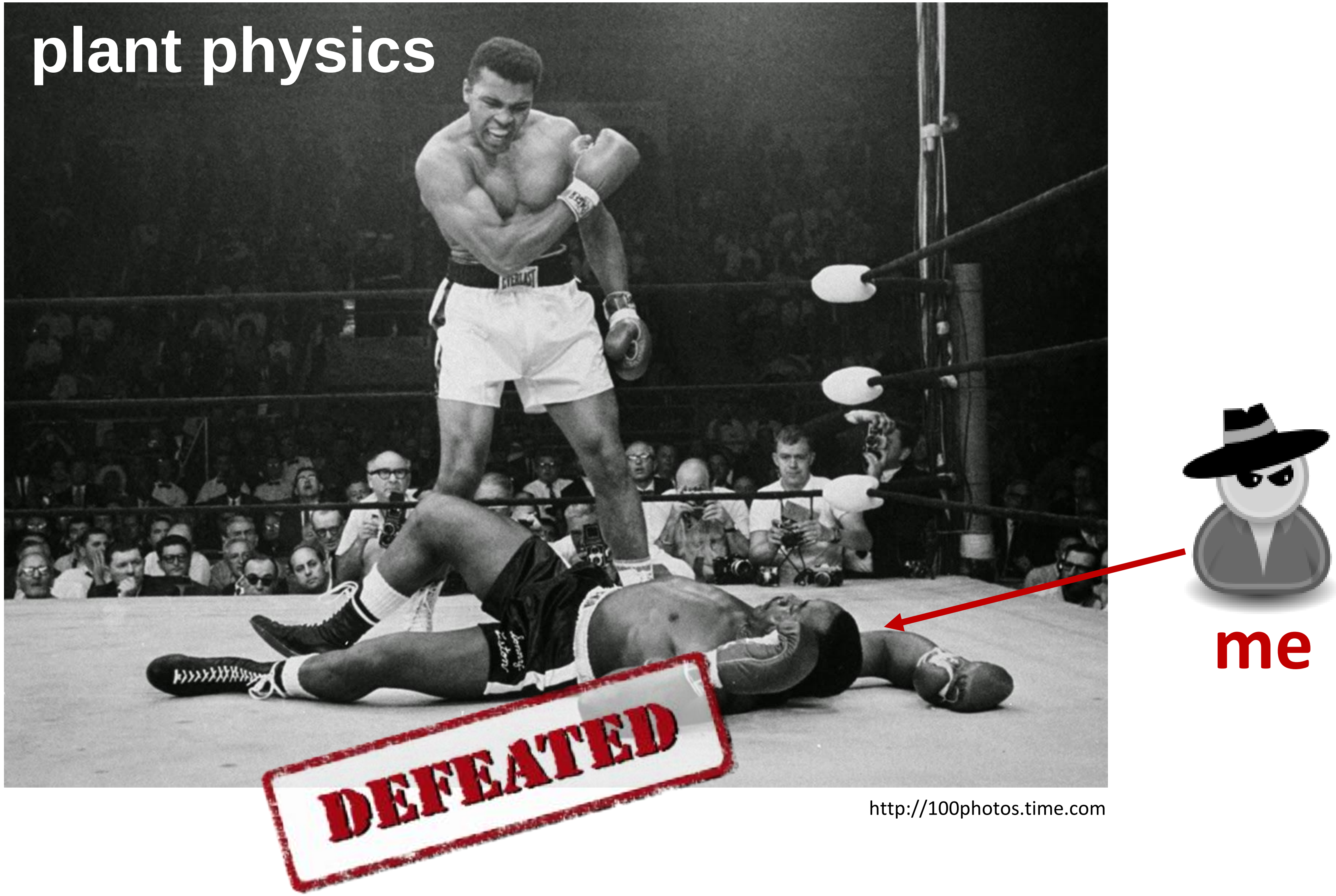
Even if digital alarms are suppressed, the abnormal process physics keeps propagating through the plant causing alarms downstream

Distant pieces of equipment "communicate" with each other via the physics of the process

Physical process is communication media



Process Physics vs. Attacker



http://100photos.time.com

I felt very angry

The attacker always wants to win!

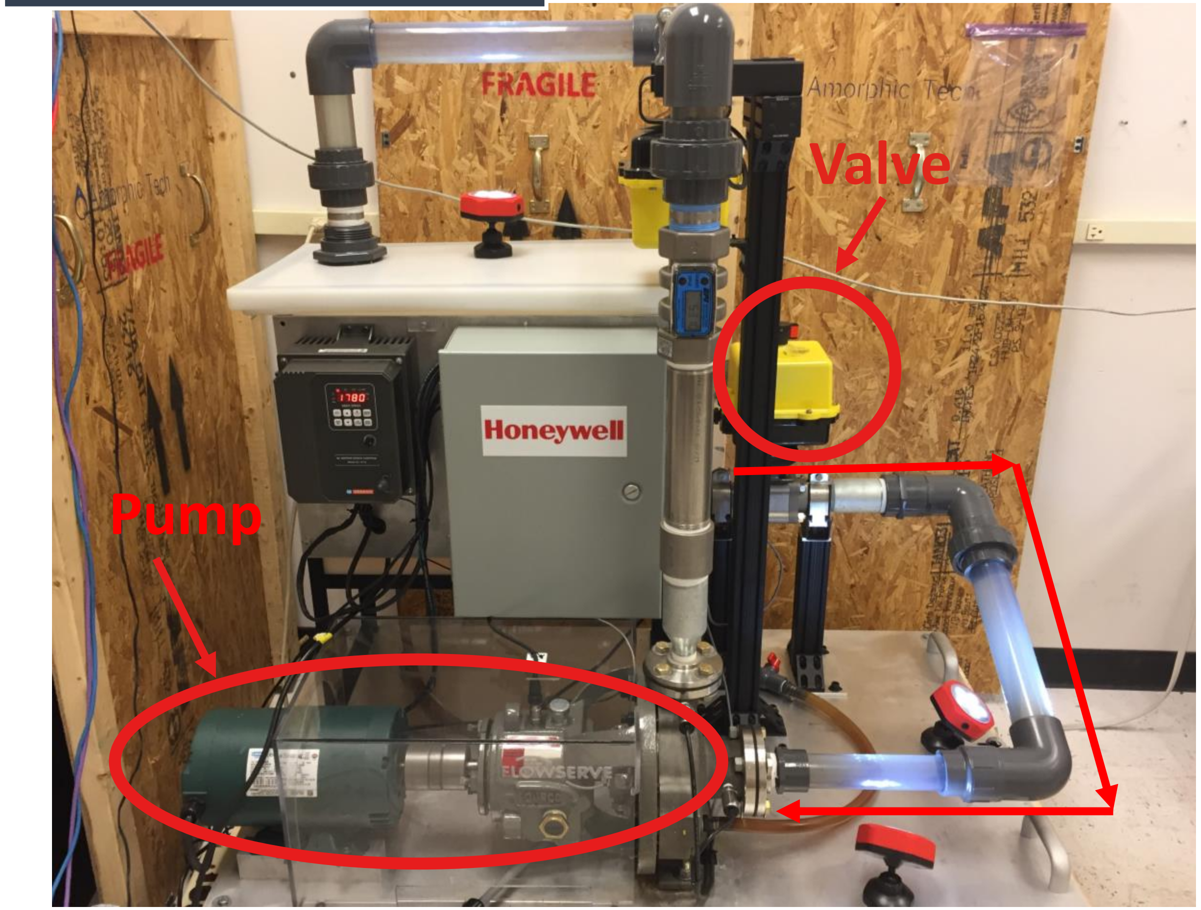
(wishfully)

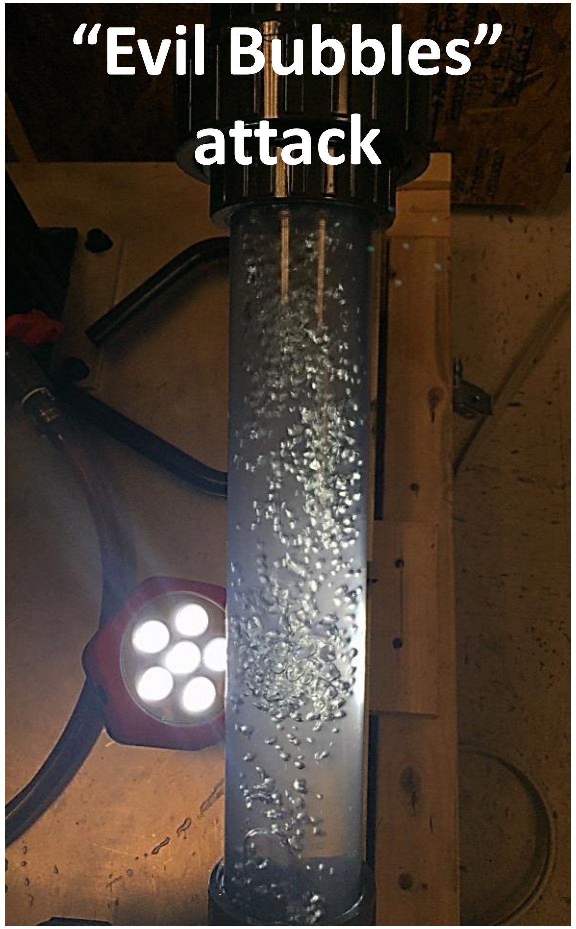
http://100photos.time.com

Delivery of Attack Payload via Process Physics

Valve and pump do not communicate electronically

The concept first formulated and described in 2013, practically demonstrated in 2017

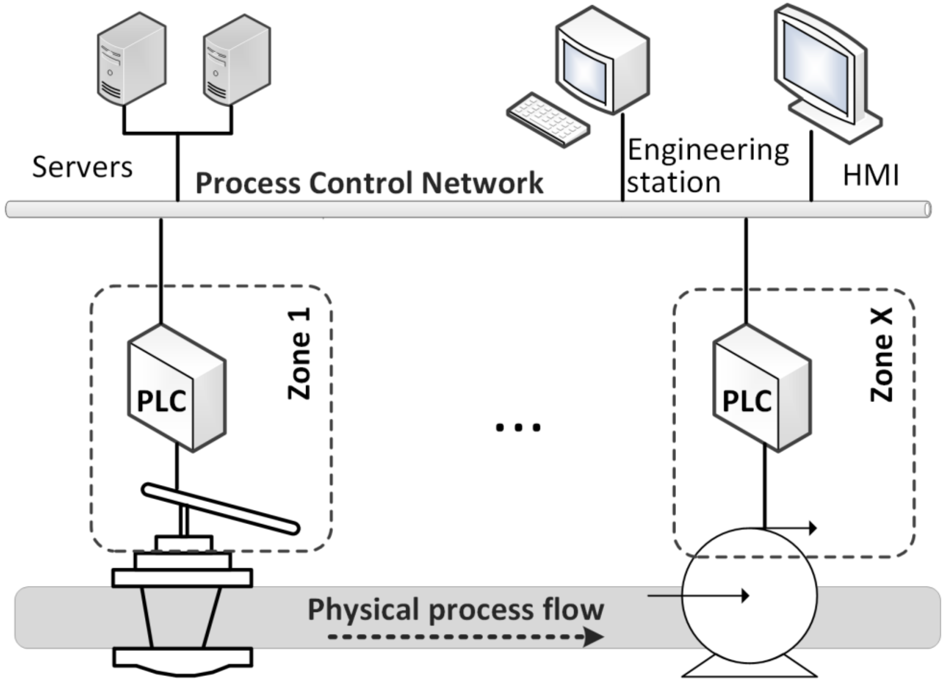



“Evil Bubbles” attack

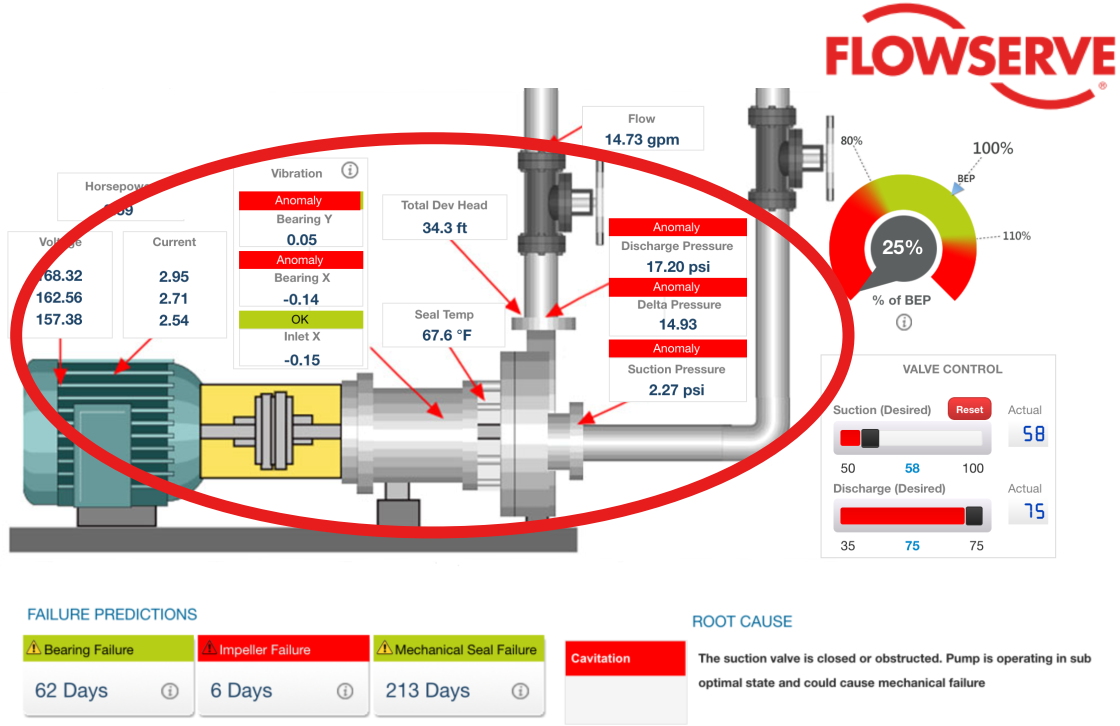
M. Krotofil. Evil Bubbles or How to Deliver Attack Payload via the Physics of the Process, Black Hat USA, 2017

Escaping security boundaries

- Violation of security zones defined based on IEC 62443



- Detection with IIoT predictive maintenance solutions



Horsepow
59

Vol ge
68.32
162.56
157.38

Current
2.95
2.71
2.54

Vibration
Anomaly
Bearing Y
0.05
Anomaly
Bearing X
-0.14
OK
Inlet X
-0.15

Total Dev Head
34.3 ft

Seal Temp
67.6 °F

Flow
14.73 gpm

Anomaly
Discharge Pressure
17.20 psi
Anomaly
Delta Pressure
14.93
Anomaly
Suction Pressure
2.27 psi

VALVE CONTROL

Suction (Desired) Reset Actual 58
50 58 100

Discharge (Desired) Actual 75
35 75 75

FAILURE PREDICTIONS

Bearing Failure	Impeller Failure	Mechanical Seal Failure
62 Days	6 Days	213 Days

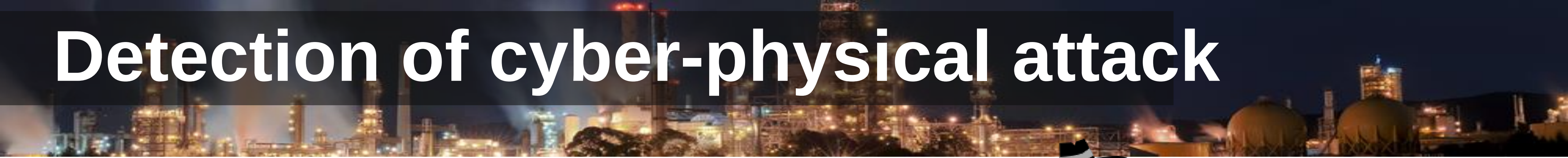
ROOT CAUSE

Cavitation

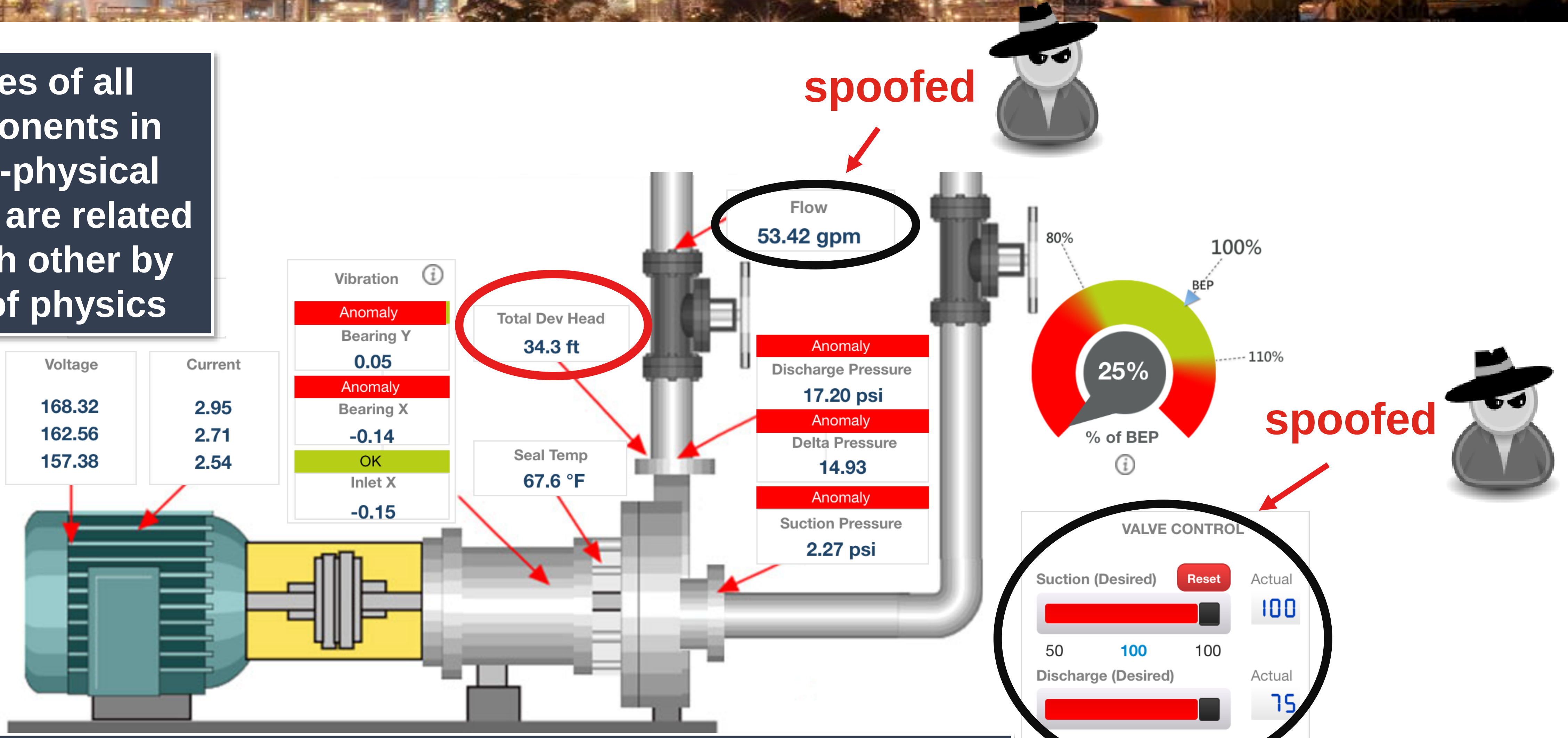
The suction valve is closed or obstructed. Pump is operating in sub optimal state and could cause mechanical failure

M. Krotofil. Evil Bubbles or How to Deliver Attack Payload via the Physics of the Process, Black Hat USA, 2017

Detection of cyber-physical attack



States of all components in cyber-physical system are related to each other by laws of physics



spoofed

spoofed

Flow
53.42 gpm

Total Dev Head
34.3 ft

Seal Temp
67.6 °F

Vibration
Anomaly
Bearing Y
0.05
Anomaly
Bearing X
-0.14
OK
Inlet X
-0.15

Voltage
168.32
162.56
157.38

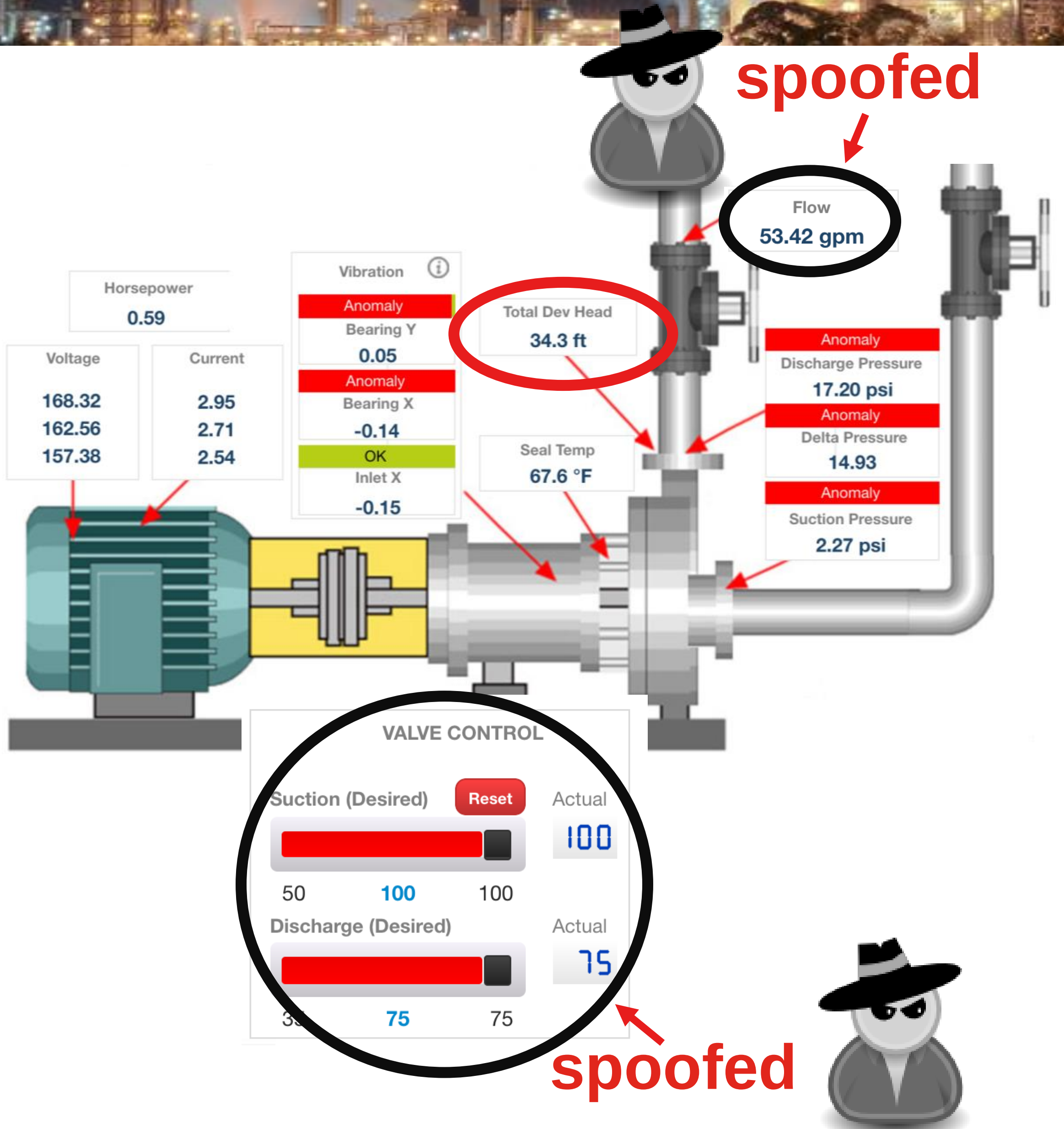
Current
2.95
2.71
2.54

Anomaly
Discharge Pressure
17.20 psi
Anomaly
Delta Pressure
14.93
Anomaly
Suction Pressure
2.27 psi

VALVE CONTROL
Suction (Desired) Reset Actual 100
50 100 100
Discharge (Desired) Actual 75
33 75 75

State of the pump can be used to validate the state of the process and detect spoofed/false process values

Verification of flow



spoofed

Horsepower
0.59

Voltage
168.32
162.56
157.38

Current
2.95
2.71
2.54

Vibration
Anomaly
Bearing Y
0.05
Anomaly
Bearing X
-0.14
OK
Inlet X
-0.15

Total Dev Head
34.3 ft

Seal Temp
67.6 °F

Flow
53.42 gpm

Anomaly
Discharge Pressure
17.20 psi
Anomaly
Delta Pressure
14.93
Anomaly
Suction Pressure
2.27 psi

VALVE CONTROL

Suction (Desired) Reset Actual
100
50 100 100

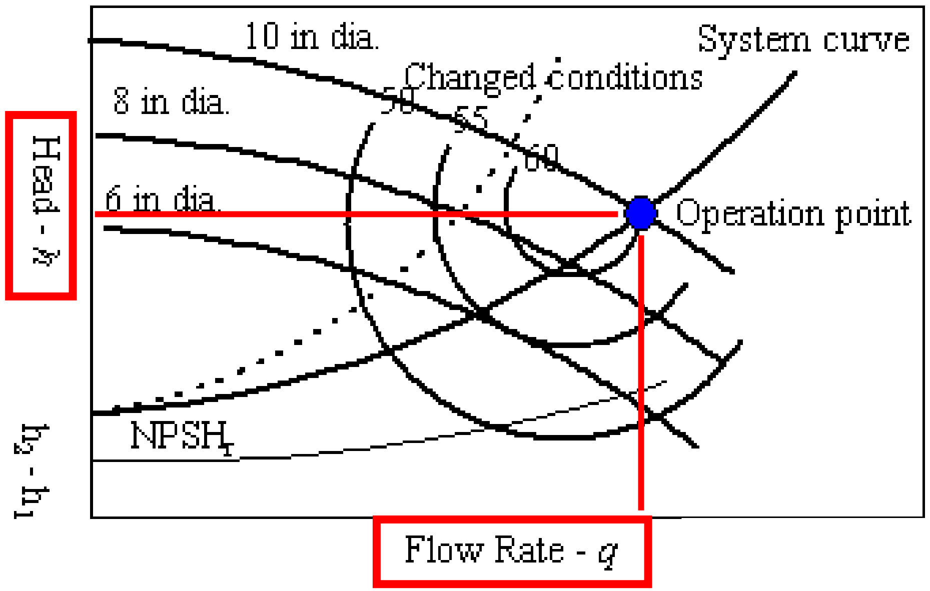
Discharge (Desired) Actual
75
3 75 75

spoofed

Pump curve would suggest:

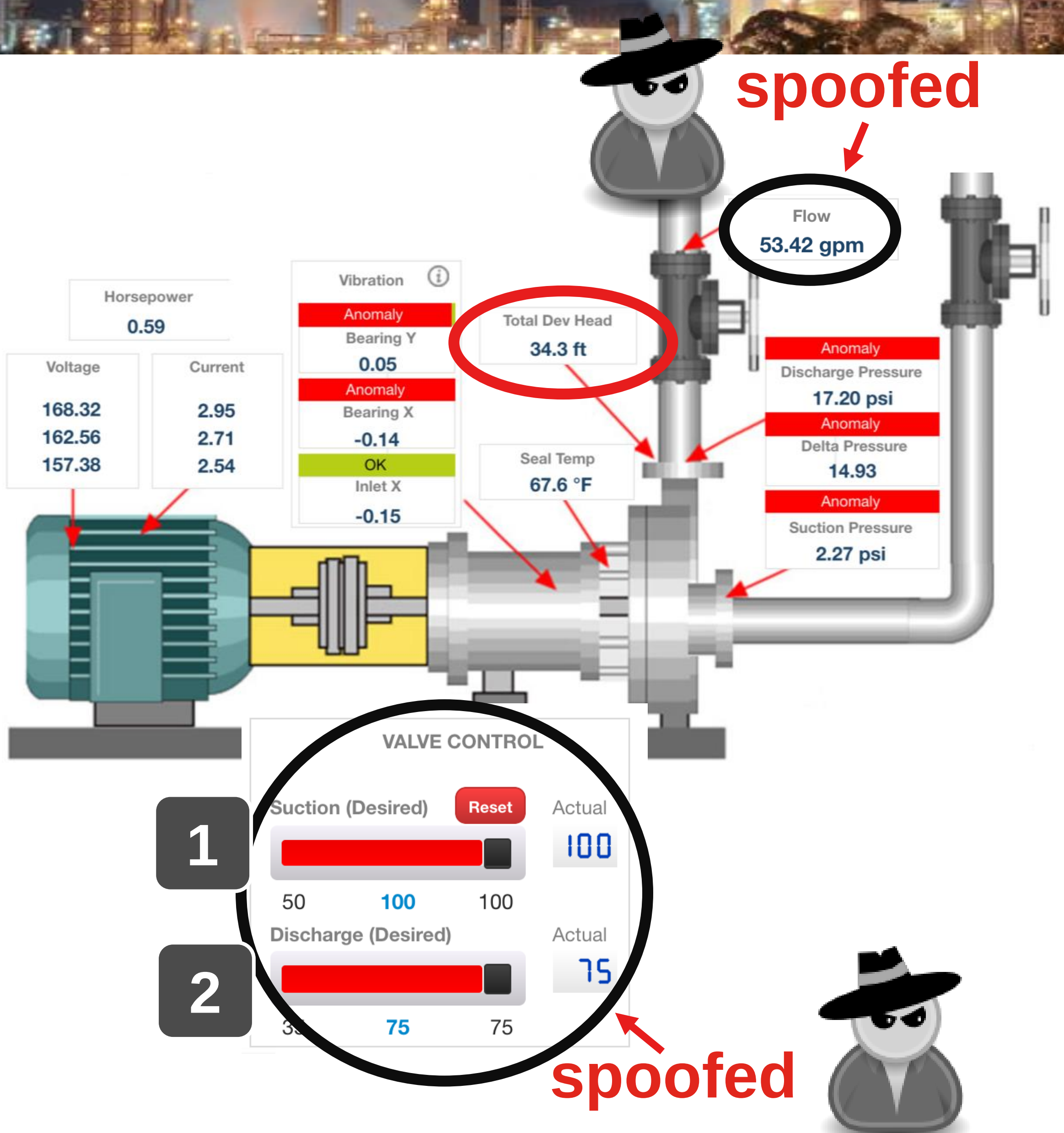
Head 34,3 ft ~ flow 21-22 gpm

Flow reading **53,42 gpm**
is <u>implausible</u>

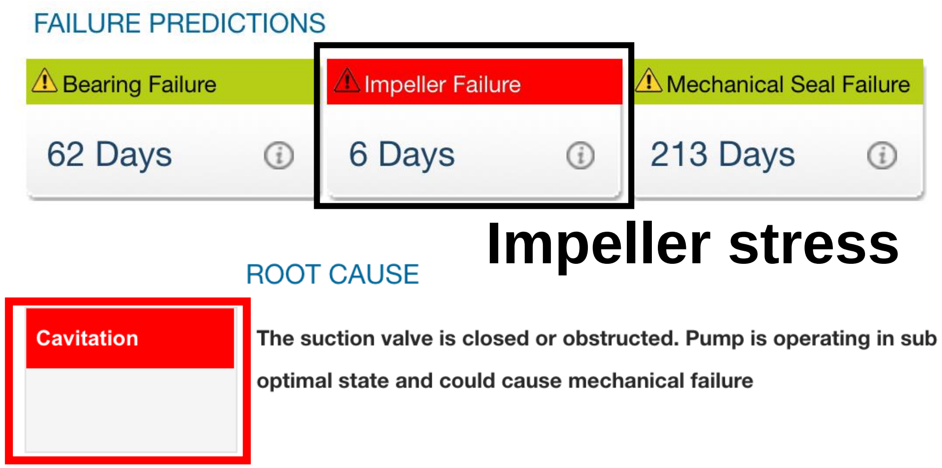


http://www.engineeringtoolbox.com/npsh-net-positive-suction-head-d_634.html

Verification of valve position



1



FAILURE PREDICTIONS

Bearing Failure	Impeller Failure	Mechanical Seal Failure
62 Days	6 Days	213 Days

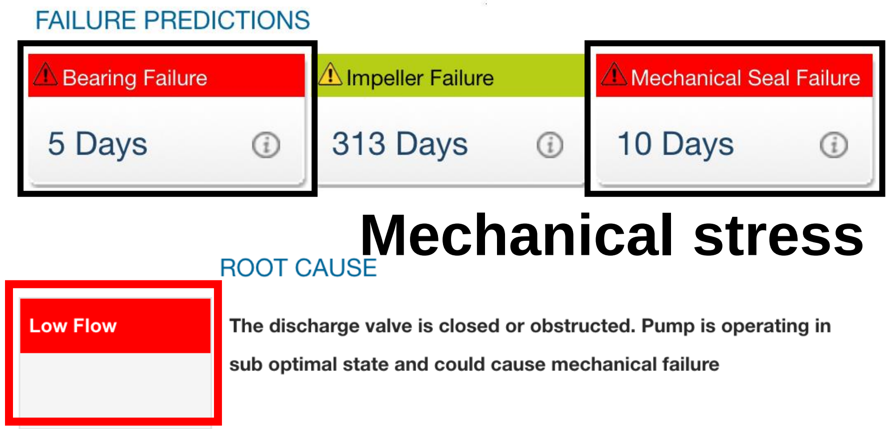
Impeller stress

ROOT CAUSE

Cavitation — The suction valve is closed or obstructed. Pump is operating in sub optimal state and could cause mechanical failure

Root cause: Cavitation

2



FAILURE PREDICTIONS

Bearing Failure	Impeller Failure	Mechanical Seal Failure
5 Days	313 Days	10 Days

Mechanical stress

ROOT CAUSE

Low Flow — The discharge valve is closed or obstructed. Pump is operating in sub optimal state and could cause mechanical failure

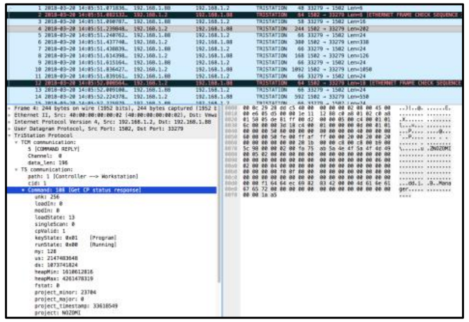
Root cause: Low flow

Another application of the attack vector

- Physical process is natural side-channel

- Process state detection algorithm and its implementation

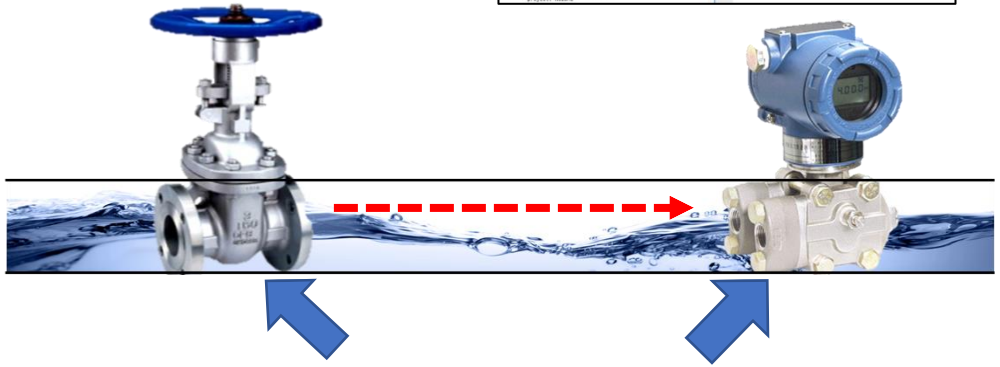
Might not see much electronic chatter after implantation



```
  1 2018-03-20 14:05:51.071836…  192.168.1.88   192.168.1.2    TRISTATION   48 33279 → 1502 Len=6
  2 2018-03-20 14:05:51.082132…  192.168.1.2    192.168.1.88   TRISTATION   64 1502 → 33279 Len=6 [ETHERNET FRAME CHECK SEQUENCE
  3 2018-03-20 14:05:51.090707…  192.168.1.88   192.168.1.2    TRISTATION   58 33279 → 1502 Len=16
  4 2018-03-20 14:05:51.239848…  192.168.1.2    192.168.1.88   TRISTATION  244 1502 → 33279 Len=202
  5 2018-03-20 14:05:51.240762…  192.168.1.88   192.168.1.2    TRISTATION   66 33279 → 1502 Len=24
  6 2018-03-20 14:05:51.437740…  192.168.1.2    192.168.1.88   TRISTATION  380 1502 → 33279 Len=338
  7 2018-03-20 14:05:51.438839…  192.168.1.88   192.168.1.2    TRISTATION   66 33279 → 1502 Len=24
  8 2018-03-20 14:05:51.614398…  192.168.1.2    192.168.1.88   TRISTATION  168 1502 → 33279 Len=126
  9 2018-03-20 14:05:51.615164…  192.168.1.88   192.168.1.2    TRISTATION   66 33279 → 1502 Len=24
 10 2018-03-20 14:05:51.836427…  192.168.1.2    192.168.1.88   TRISTATION 1092 1502 → 33279 Len=1050
 11 2018-03-20 14:05:51.839161…  192.168.1.88   192.168.1.2    TRISTATION   66 33279 → 1502 Len=24
 12 2018-03-20 14:05:52.000564…  192.168.1.2    192.168.1.88   TRISTATION   64 1502 → 33279 Len=18 [ETHERNET FRAME CHECK SEQUENCE
 13 2018-03-20 14:05:52.009100…  192.168.1.88   192.168.1.2    TRISTATION   66 33279 → 1502 Len=24
 14 2018-03-20 14:05:52.224378…  192.168.1.2    192.168.1.88   TRISTATION  592 1502 → 33279 Len=550
 15 2018-03-20 14:05:52.225078…  192.168.1.88   192.168.1.2    TRISTATION   66 33279 → 1502 Len=24
```

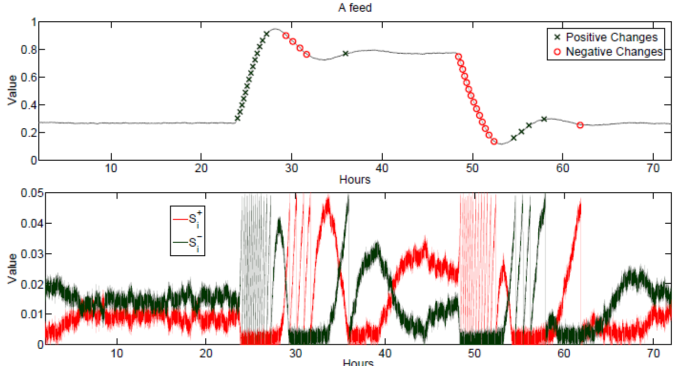
```
▸ Frame 4: 244 bytes on wire (1952 bits), 244 bytes captured (1952 b
▸ Ethernet II, Src: 40:00:00:00:00:02 (40:00:00:00:00:02), Dst: Vmwa
▸ Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.88
▸ User Datagram Protocol, Src Port: 1502, Dst Port: 33279
▾ TriStation Protocol
  ▾ TCM communication:
      5 [COMMAND REPLY]
      Channel: 0
      data_len: 196
  ▾ TS communication:
      path: 1 [Controller —> Workstation]
      cid: 1
    ▾ Command: 108 [Get CP status response]
        unk: 256
        loadIn: 0
        modIn: 0
        loadState: 13
        singleScan: 0
        cpValid: 1
        keyState: 0x01    [Program]
        runState: 0x00    [Running]
        my: 128
        us: 2147483648
        ds: 1073741824
        heapMin: 1610612816
        heapMax: 4261478319
        fstat: 0
        project_minor: 23704
        project_major: 0
        project_timestamp: 33618549
        project: NOZOMI
```

```
0000  00 0c 29 20 dd c5 40 00  00 00 00 02 08 00 45 00   ..) ..@. ......E.
0010  00 e6 05 d5 00 00 1e 11  12 88 c0 a8 01 02 c0 a8   ........ ........
0020  01 58 05 de 81 ff 00 d2  00 00 05 00 c4 00 01 01   .X...... ........
0030  6c 00 00 00 3d 18 c4 00  01 00 00 00 0d 00 01 01   l...=... ........
0040  00 00 00 50 80 00 00 00  00 00 00 00 40 00 00 00   ...P.... ....@...
0050  60 00 00 50 fe 00 ff af  ff 00 00 20 00 20 00 20   `..P.... ... . .
0060  00 00 00 00 00 00 20 1b  00 00 c8 00 c8 00 b9 00   ...... . ........
0070  5c 98 00 00 02 00 fa 75  ab 5a 4e 4f 5a 4f 4d 49   \......u .ZNOZOMI
0080  00 05 02 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 06 00   ........ ........
00a0  02 00 00 04 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 f0 0f 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 f1 64 64 ec 69 02  03 42 00 00 4d 61 6e 61   ...dd.i. .B..Mana
00e0  67 65 72 00 00 00 00 00  00 00 00 00 00 00 00 00   ger..... ........
00f0  00 00 1a a5                                        ....
```



These can be in completely different parts of the process, on different networks

Observation of state A in component B needs to trigger payloads X, Y, Z



$$S_i^+ = \max(0, |X_{i-1} - X_i| + S_{i-1}^+)$$
$$S_i^- = \max(0, |X_i - X_{i-1}| + S_{i-1}^-)$$

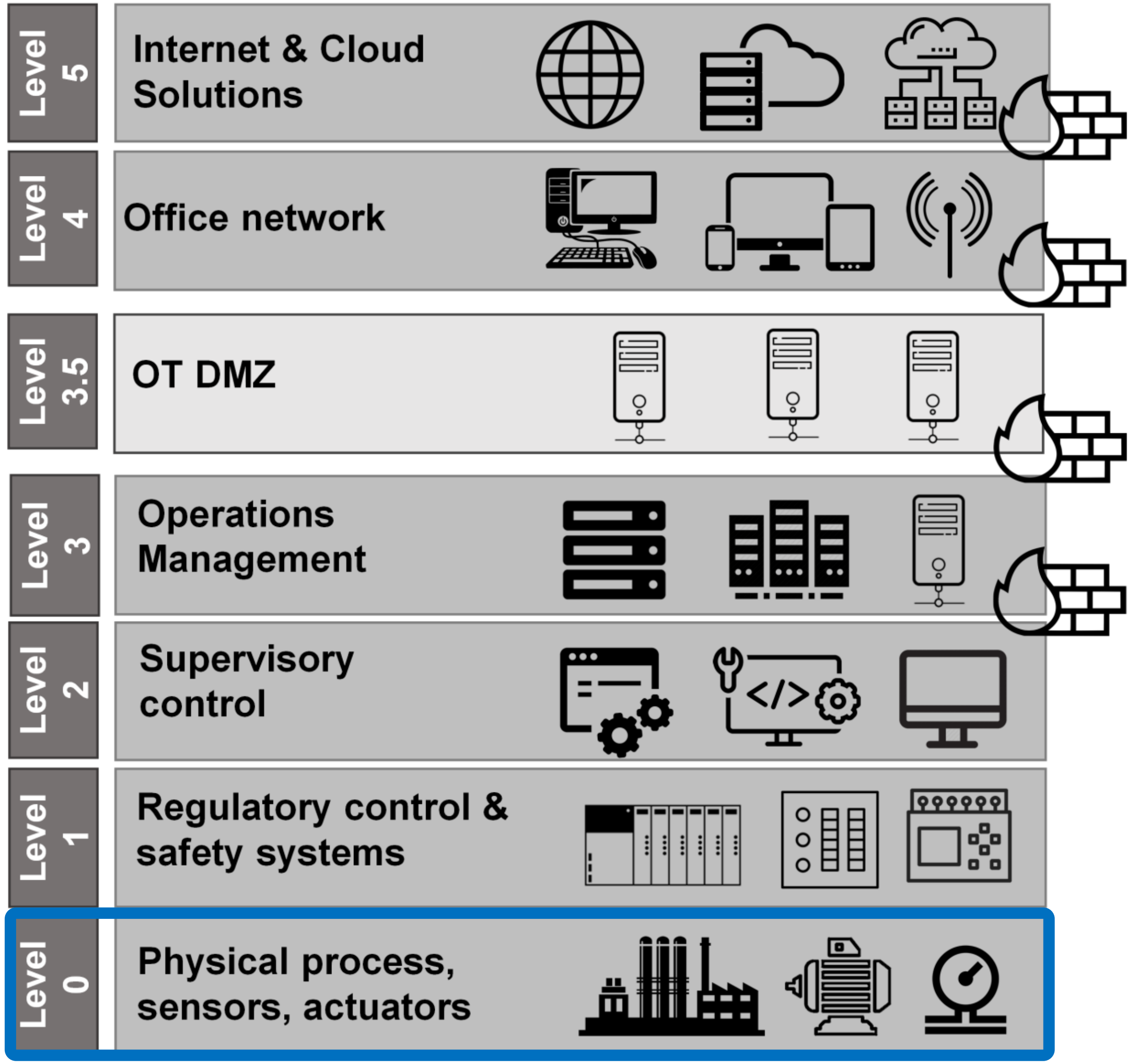
Non-Parametric Cumulative Sum (NCUSUM)

```
check(double):
        stwu 1,-48(1)
        mflr 0
        stw 0,52(1)
        stw 31,44(1)
        mr 31,1
        stfd 1,24(31)
        lfd 1,24(31)
        bl compute_score(double)
        stfd 1,8(31)
        lis 9,m_current_sum@ha
        lfd 12,m_current_sum@l(9)
```

17640 bytes ~= 0.11% of DRAM
(unoptimized)

Conclusions

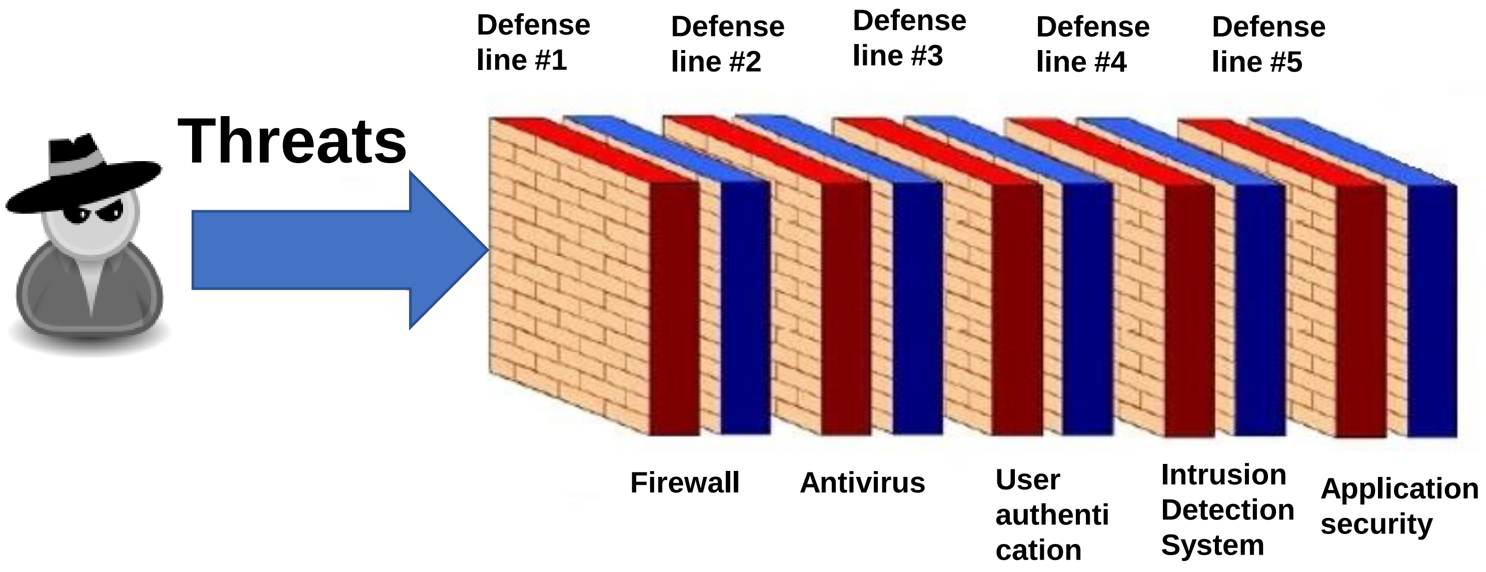
Process data as root of trust



- Process data is **root of trust** in ICS/ cyber-physical security
- If process data is incorrect/invalid, control algorithms, human operator and safety systems may take wrong (harmful) control decisions
- Ensuring **timeliness** and **trustworthiness** of process data is **a crucial task** in cyber-physical security:
  - Methods to detect missing/delayed or implausible readings are needed to ensure reliable and safe process control

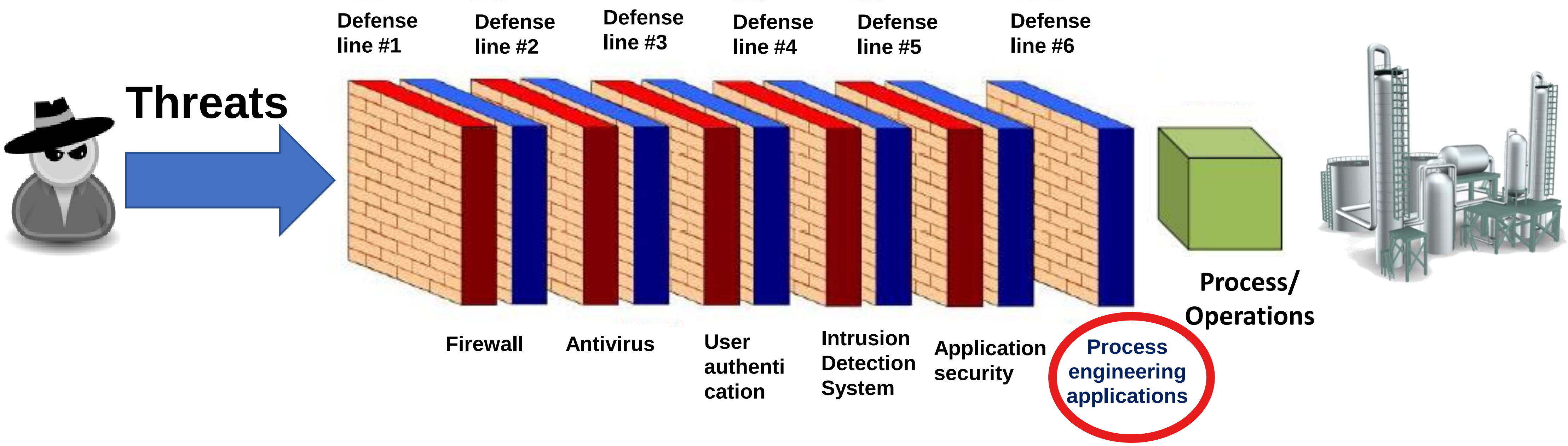
Defence-in-Depth in CPS domain

- *Defense-in-depth* concept suggest multiple layers of security
  - If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system



Defence-in-Depth in CPS domain

- In cases when the attacker manages to bypass all traditional IT security defenses and/or attacker executed a CPS-specific attack not covered by IT security defenses:
  - Engineering security controls should be in place to prevent and detect unwanted/malicious process manipulations



Q & A

Marina Krotofil
@marmusha
marmusha@gmail.com