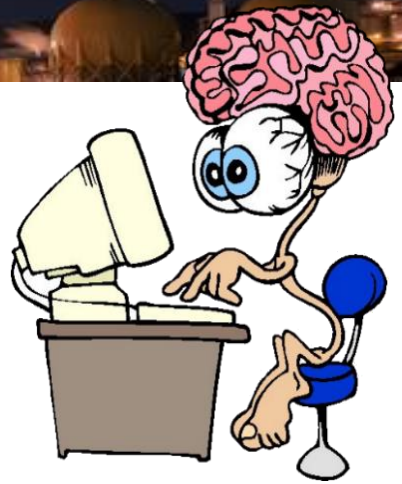
Industrial Control Systems Security: Introduction

Marina Krotofil

COINS summer school on Security Applications, Lesbos, Greece
26-27.07.2019

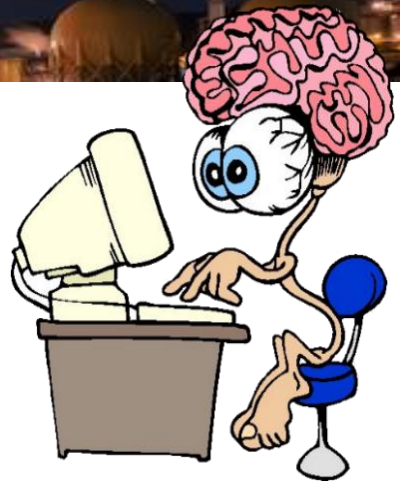
About myself

- Senior Automation Security Engineer at the large chemical company
- Specializing in offensive cyber-physical security in Critical Infrastructures
  - **Focus:** Physical damage or how to make something going bad, crash or blow up by means of cyber-attacks



About myself

- Ukrainian German who lived and worked in America
- Two engineering Masters and MBA , and almost PhD
- Previously worked as
  - Principal Analyst and Subject Matter Expert at FireEye (USA)
  - Lead Security Researcher at Honeywell (USA)
  - Senior Security Consultant at the European Network for Cyber Security (Netherlands)
  - Research assistant at Hamburg University of Technology (Germany) who had to teach



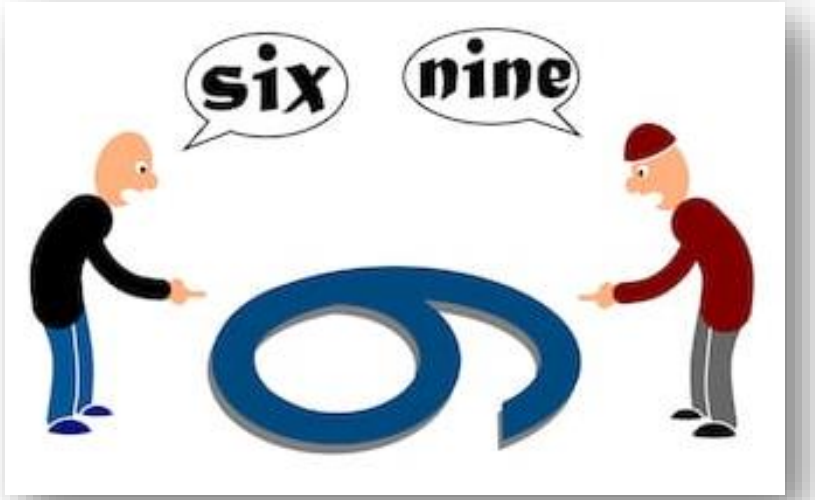
Introduction

Here is a Plant. What is your Plan?

http://www.amerpipe.com/sites/default/files/refinery-pipe.jpg

Two common views on cyber-physical attacks

- “Trivial! Look at the state of ICS security!”
- “Borderline impossible! These processes are extremely complex & engineered for safety!”



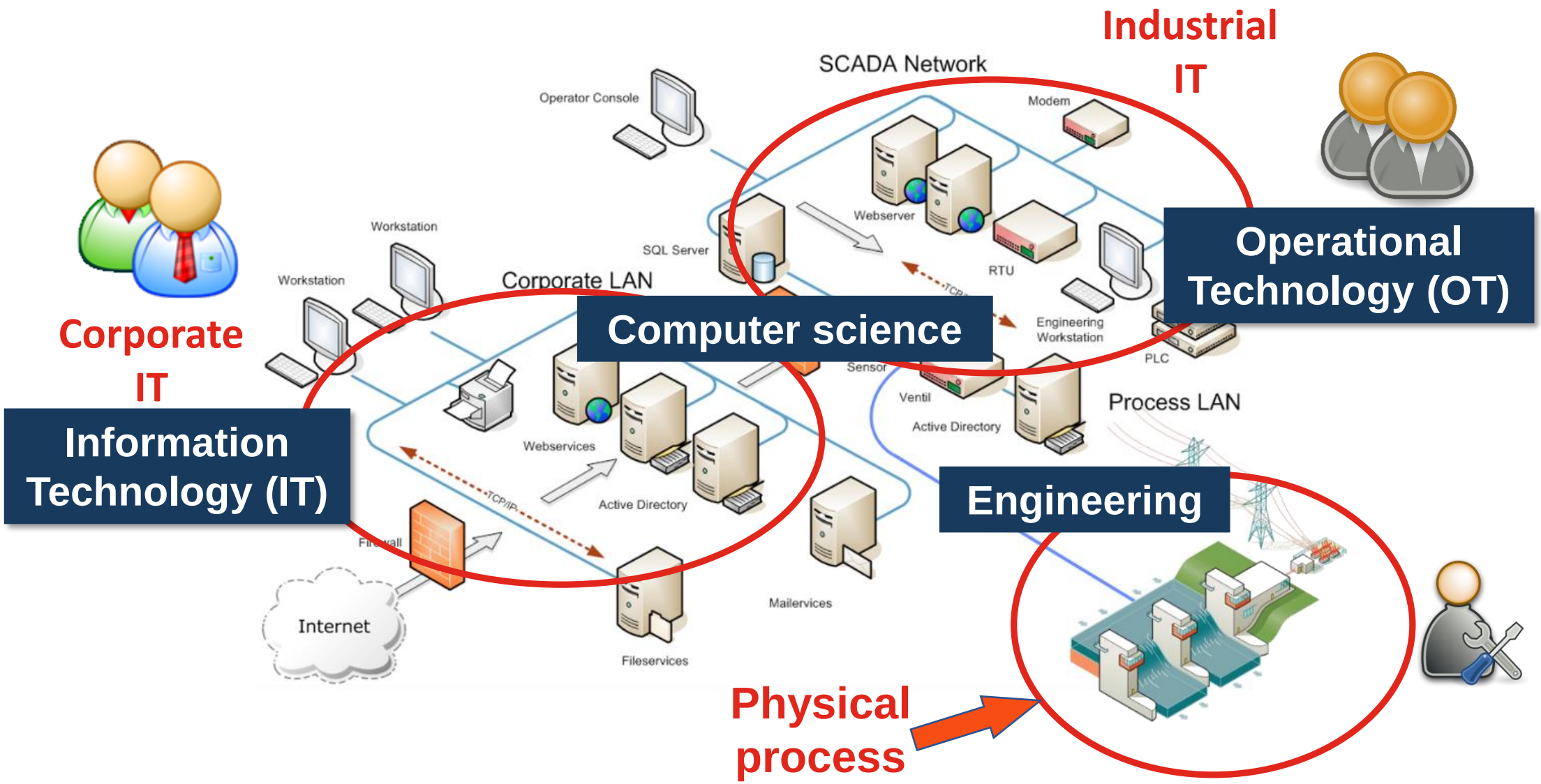
https://www.shutterstock.com/image-illustration/six-nine-matter-perspectives-1024980271

Typical expectation: MAGIC BUTTON

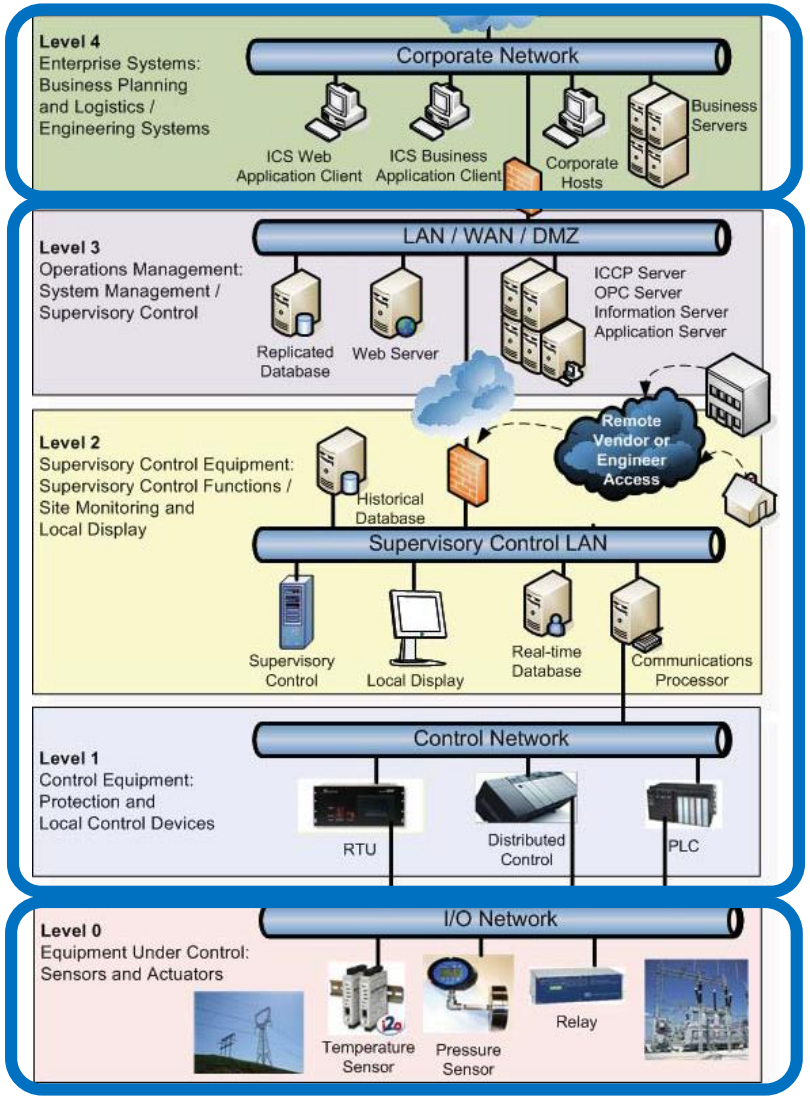
Attacks with strategic and long lasting effect

- Attacks with strategic, lasting damage will be process specific & require good process comprehension
- Wil require attacker to develop detailed '**damage scenario**'
  - What causes a pipeline to explode?
  - What causes the ***right*** pipeline to explode?
  - What causes the ***right*** pipeline to explode at the ***right*** moment?

Typical ICS architecture



Purdue network reference architecture

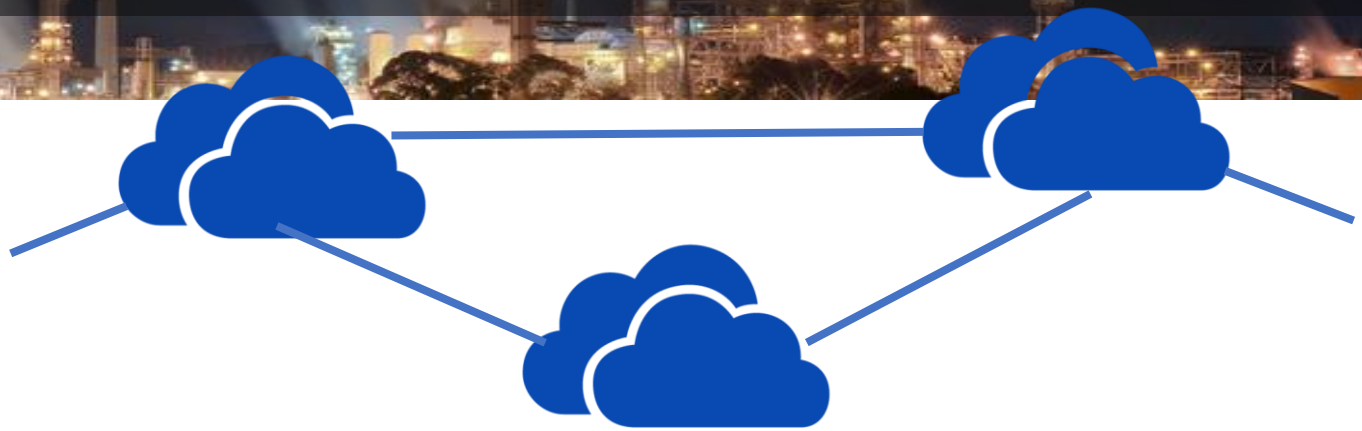


IT network

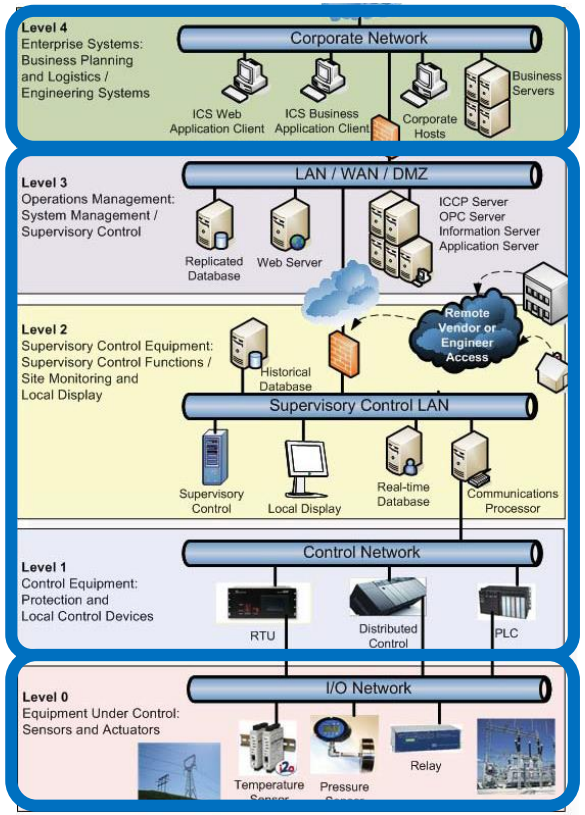
OT network

Physical process

Purdue reference architecture: recent trends



New trend: „Internet of Clouds“



Attacker goals

Traditionally:

- Espionage
- Persistence
- Reconnaisance

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

This campaign comprises two distinct categories of victims: staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks, referred to as "staging targets" throughout this alert. The threat actors used the staging targets' networks as pivot points and malware repositories when targeting their final intended victims. NCCIC and FBI judge the ultimate objective of the actors is to compromise organizational networks, also referred to as the "intended target."

https://www.us-cert.gov/ncas/alerts/TA18-074A

https://www.ncsc.gov.uk/news/hostile-state-actors-compromising-uk-organisations-focus-engineering-and-industrial-control

National Cyber Security Centre
a part of GCHQ

Advisory: Hostile state actors compromising UK organisations with focus on engineering and industrial control companies

The NCSC is aware of an ongoing attack campaign against multiple companies involved in the CNI supply chain. These attacks have been ongoing since at least March 2017. The targeting is focused on

Turla malware found in a German plant

Attacker goals

Emerging trends

- Physical damage
- Ransomware

TRITON Malware Targeting Critical Infrastructure Could Cause Physical Damage

December 15, 2017 Wang Wei

https://thehackernews.com/2017/12/triton-ics-scada-malware.html

Threat Research

TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers

October 23, 2018 | by FireEye Intelligence

MALWARE ICS RUSSIA CRITICAL INFRASTRUCTURE

https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

Hexion, Momentive and Norsk Hydro all hit by ransomware cyber attacks

BY EMMA STOYE

Aftermath

In the immediate aftermath of the incident Norsk was forced to switch to manual production at its plants. Staff at 40 offices and manufacturing facilities were told to disconnect devices from the network while security experts were brought in to fix the issue.

https://www.chemistryworld.com/news/hexion-momentive-and-norsk-hydro-all-hit-by-ransomware-cyber-attacks/3010328.article

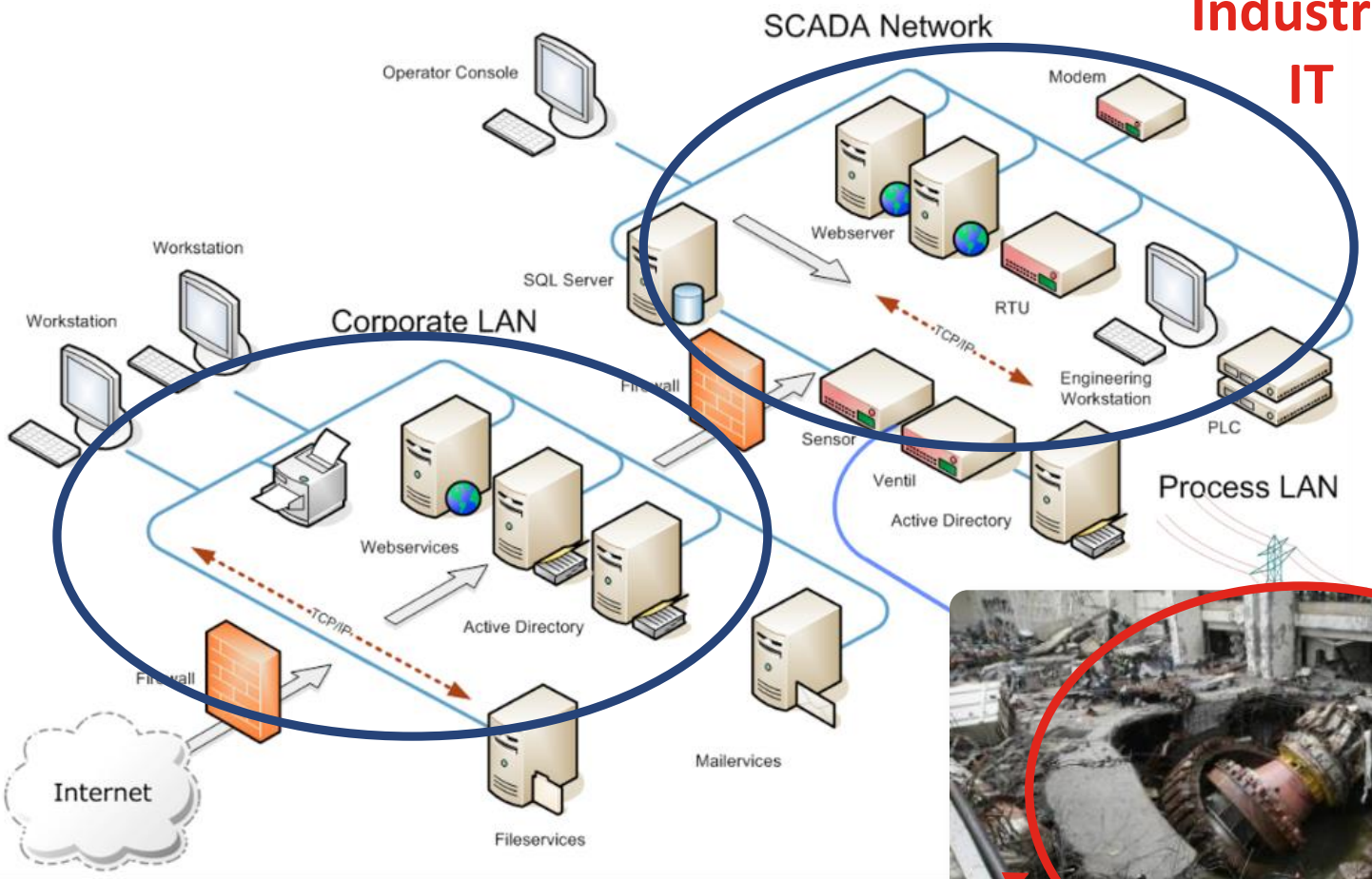
Ransomware Forces Two Chemical Companies to Order 'Hundreds of New Computers'

It appears that LockerGoga, the same ransomware that hit aluminum manufacturing giant Norsk Hydro this week, also infected American chemicals companies Hexion and Momentive, leaving employees locked out of their computers.

https://www.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers

Attack goal considered in this module

Corporate IT



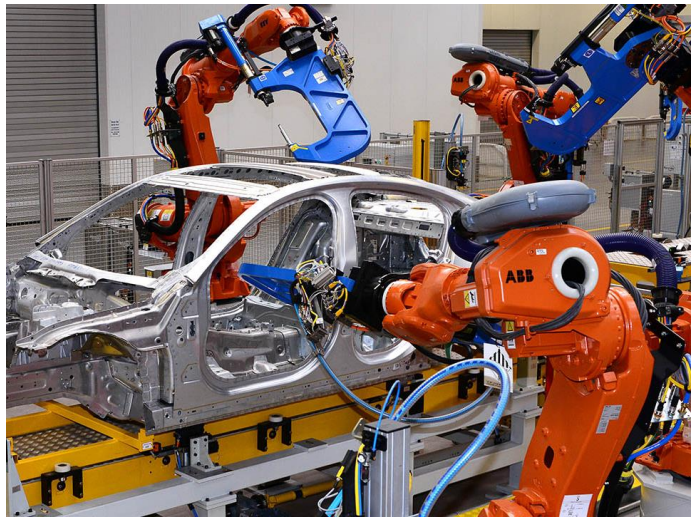
Industrial IT

Attacker goal

Embedded ICS systems

https://vecer.mk/files/article/2017/05/02/485749-saudiska-arabija-ja-kupi-najgolemata-naftena-rafinerija-vo-sad.jpg

http://www.jfwhite.com/Collateral/Images/English-US/Galleries/middleboro9115kvbreakers.jpg



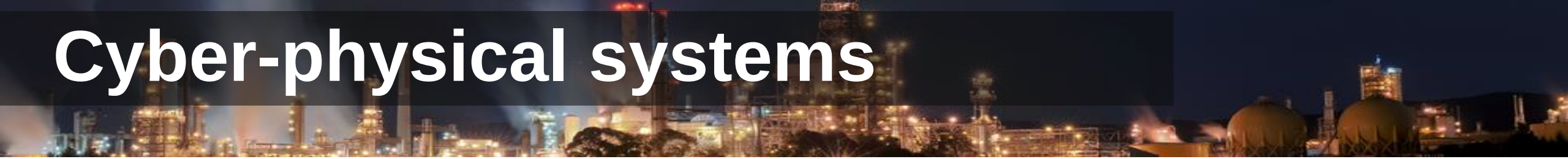
https://www.roboticsbusinessreview.com/wp-content/uploads/2016/05/jaguar-factory.jpg

https://www.oilandgasproductnews.com/files/slides/locale_image/medium/0089/22183_en_16f9d_8738_honeywell-process-solutions-rtu2020-process-controller.jpg

https://selinc.com/uploadedImages/Web/Videos/Playlists/Playlist_RTAC_1280x720.png?n=63584758126000

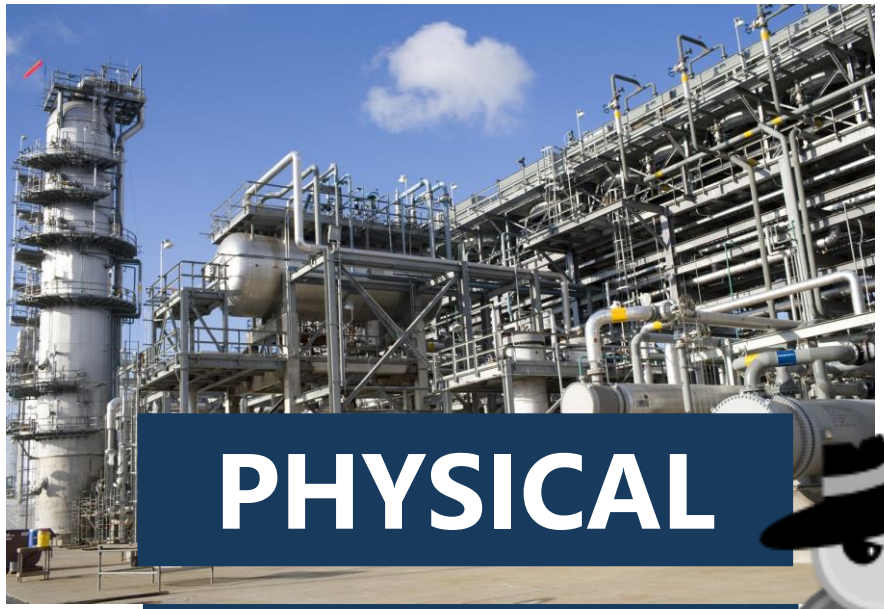
http://www02.abb.com/global/seitp/seitp202.nsf/0/0601d25ed243cfb0c1257d7e0043e50e/$file/7184_lvl2.jpg

Cyber-physical systems



Cyber-physical systems are IT systems “embedded” in an application in the physical world

Cyber-physical attack



PHYSICAL

CYBER

http://magazine.scientificmalaysian.com/wp-content/uploads/2013/12/Oil-refinery-explosion.png

ICS security

ICS security

IT security
(cyber-security -> taking over the infrastructure)

OT security
(causing impact on the operations -> process and equipment)

Focus of the session

Control equipment vulnerabilities

ICSA-15-099-01A: Siemens SIMATIC HMI Devices Vulnerabilities (Update A)

ICSA-13-274-01: Schneider Electric Telvent SAGE RTU DNP3 Improper Input Validation Vulnerability

ICSA-15-111-01: Emerson AMS Device Manager SQL Injection Vulnerability

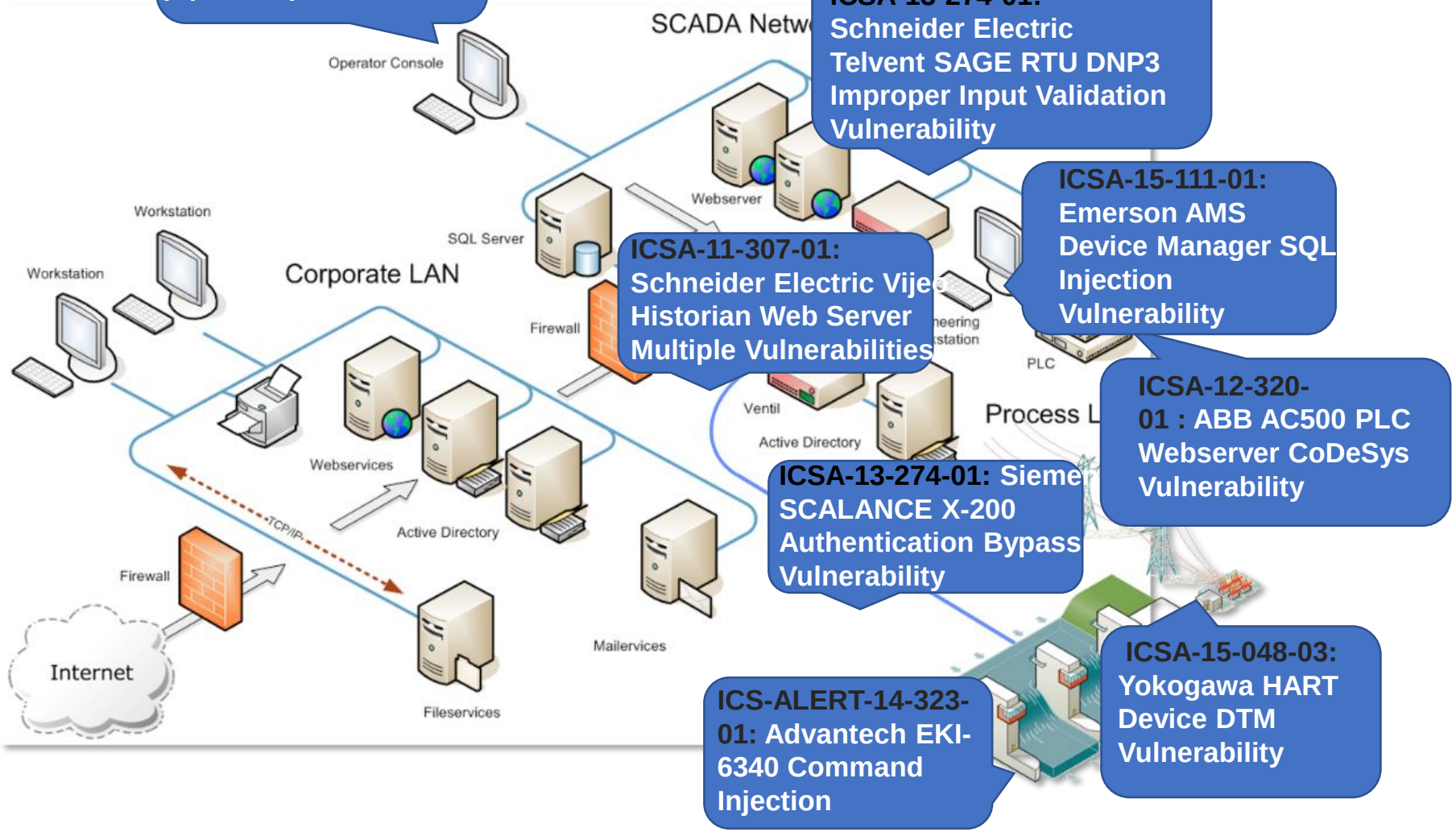
ICSA-11-307-01: Schneider Electric Vije Historian Web Server Multiple Vulnerabilities

ICSA-12-320-01 : ABB AC500 PLC Webserver CoDeSys Vulnerability

ICSA-13-274-01: Sieme SCALANCE X-200 Authentication Bypass Vulnerability

ICSA-15-048-03: Yokogawa HART Device DTM Vulnerability

ICS-ALERT-14-323-01: Advantech EKI-6340 Command Injection



ICS-CERT advisory

ICSA-13-274-01: Siemens SCALANCE X-200 Authentication Bypass Vulnerability

IMPACT

Successful exploitation of this vulnerability **may allow attackers to perform administrative operations** over the network without authentication.

***Impact to individual organizations depends on many factors that are unique to each organization**. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.*

Impact evaluation

- What exactly the attacker can do with the vulnerability?
- Any further necessary conditions required?
- How severe the potential physical impact?

Answering these questions requires understanding how the attacker interacts with the control system and the process

Control systems security

My research discoveries – how to attack cyber-physical systems even if the traditional IT security controls are in place

1 **Industrial systems can be controlled without modifying the contents of the messages**

- This can be effective even if the traffic is signed or even encrypted

Control system design flaw

2 **Process data can be spoofed to make it look like everything is normal**

- This can be done despite all traditional communication security put in place

Overlooked data security property

Stale data attack

Control system design flaw

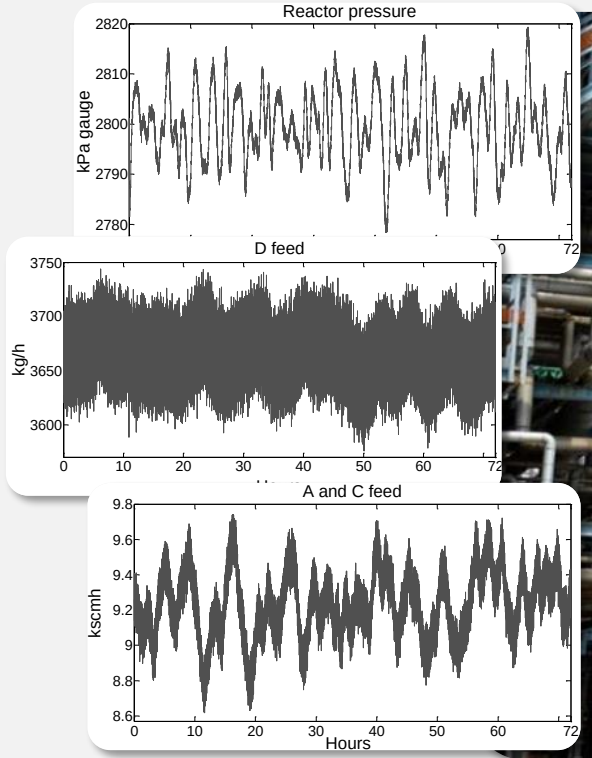
M. Krotofil, A. Cardenas, J. Larsen, D. Gollmann, Vulnerabilities of cyber-physical systems to stale data—Determining the optimal time to launch attacks, International Journal of Critical Infrastructure Protection, 2015

Data trustworthiness (veracity)

Overlooked data security property

Process data originates in the physical world and can be made wrong on purpose, before being handed into communication protocol stack (and securely delivered to the intended application)

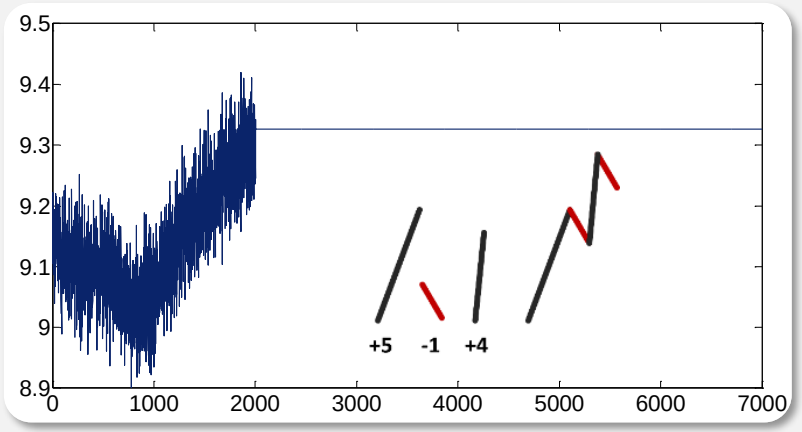
(Garbage in – garbage out)

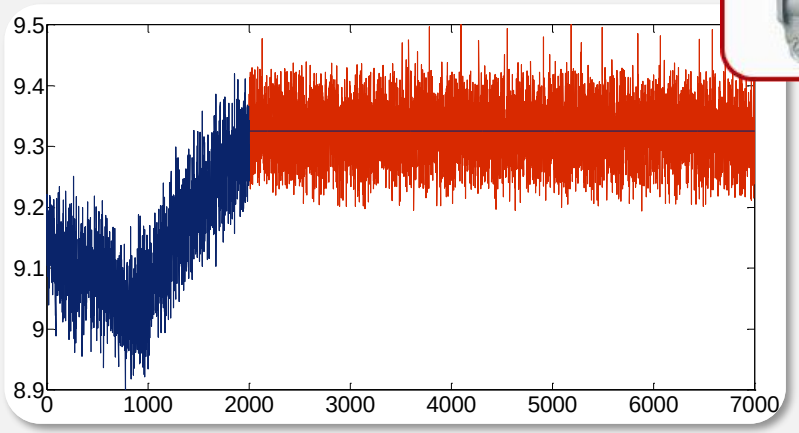


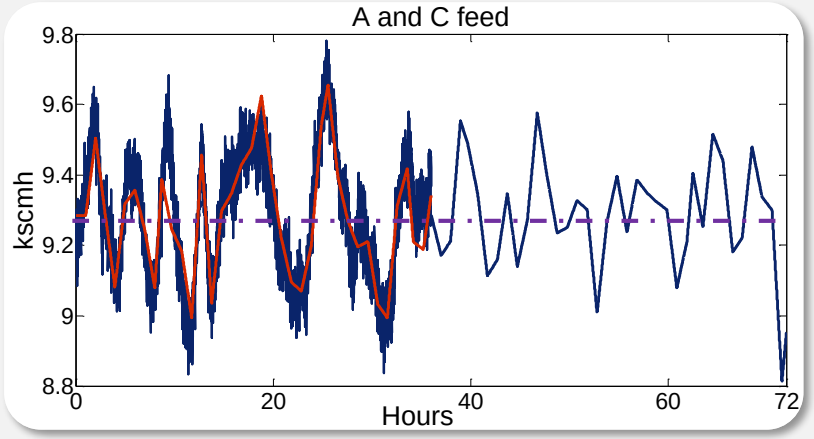
J. Larsen. Miniaturization. Black Hat USA (2014)

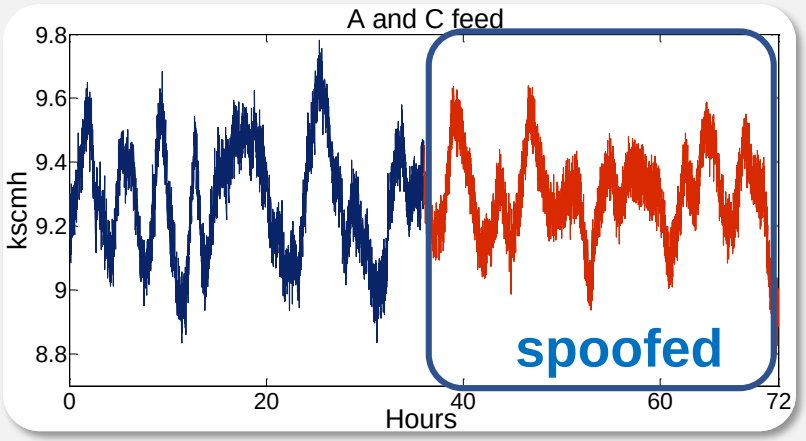
M. Krotofil, J. Larsen, D. Gollmann. Process Matters: Ensuring Data Veracity in Cyber-Physical Systems (ASIACCS'15)

Data trustworthiness (veracity)









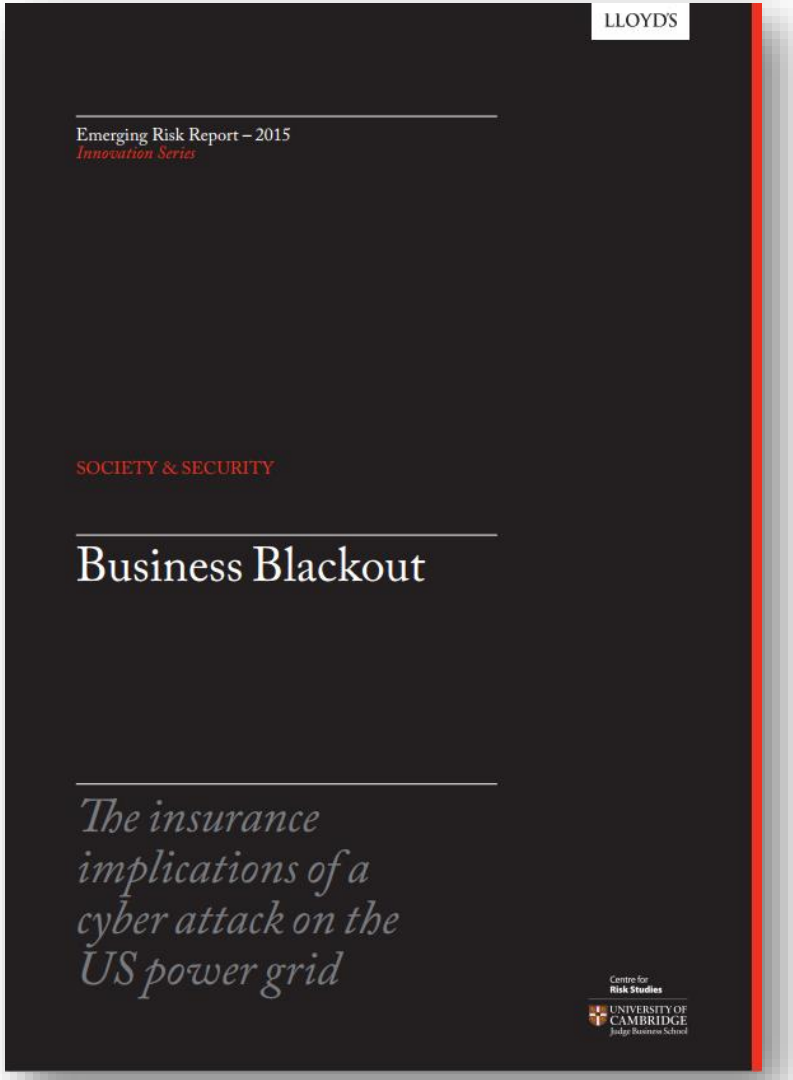
Find X differences

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

Incident data inavailability

- Due to various schemes for reputation management and data sharing laws, the majority of Operational Technology attacks over the last 20 years have not been made public, making even a catalogue of recent reference events difficult to assemble.
- A key requirement for an insurance response to cyber risks will be to enhance the quality of data available and to continue the development of probabilistic modelling.

We can and should conduct own research on cyber-physical exploitation



https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout

Cyber-physical security

1. After the attacker gets access to a control system/network, the attack still needs to be performed
   - This is where open literature falls short
   - Best attack strategies (?)

2. Security standards & guidelines require “knowing your system” prior performing risk assessment and subsequent implementation of security controls
   - No guidance on HOW to understand the system in a away to best understand where all the risks lie
   - Who should participate in risk assessment

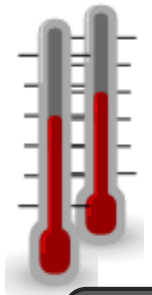
Fundamentals of cyber-physical exploitation

Industrial plants work on control loop concept

Process Optimization Applications

HMI

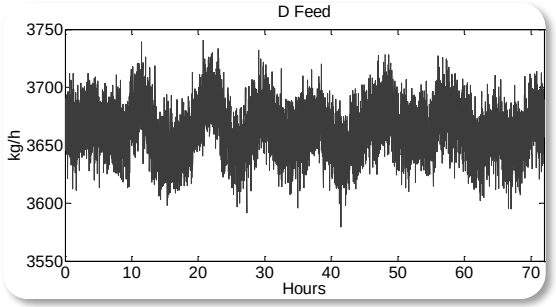
Control system

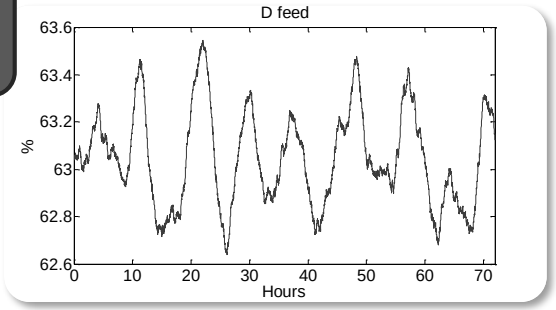


SET POINT

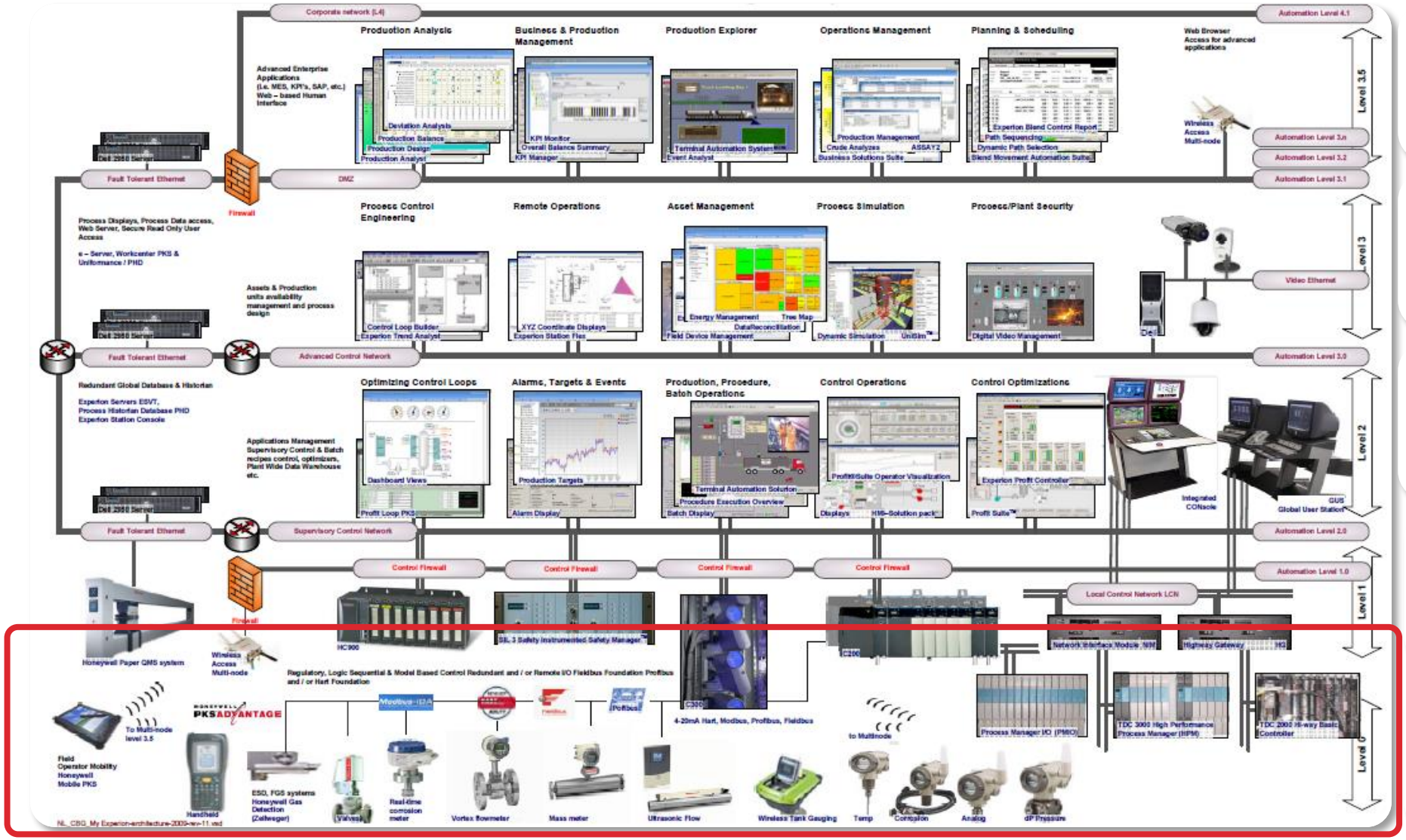
Sensors

Actuators





Industrial network architecture



Planning and management

Optimization Applications

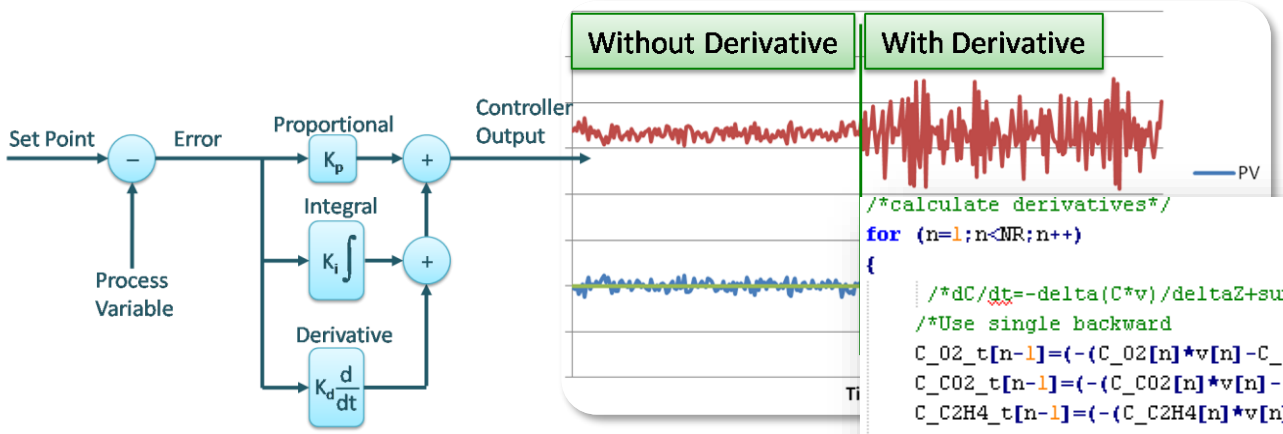
HMI (Supervisory control)

Controllers (Regulatory control)

Field Instrumentation

Definition of Real Time

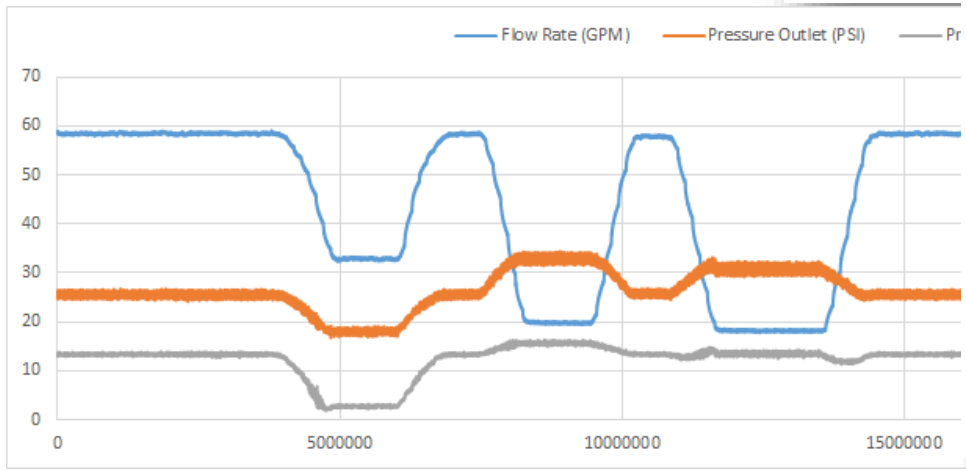
Process data

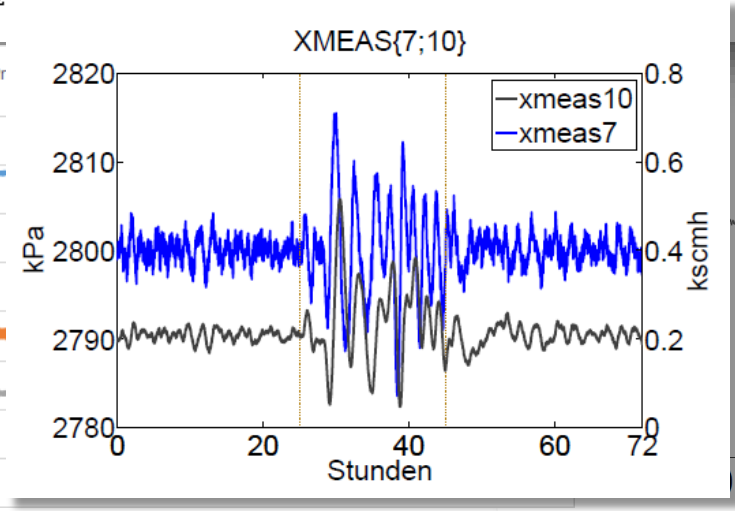


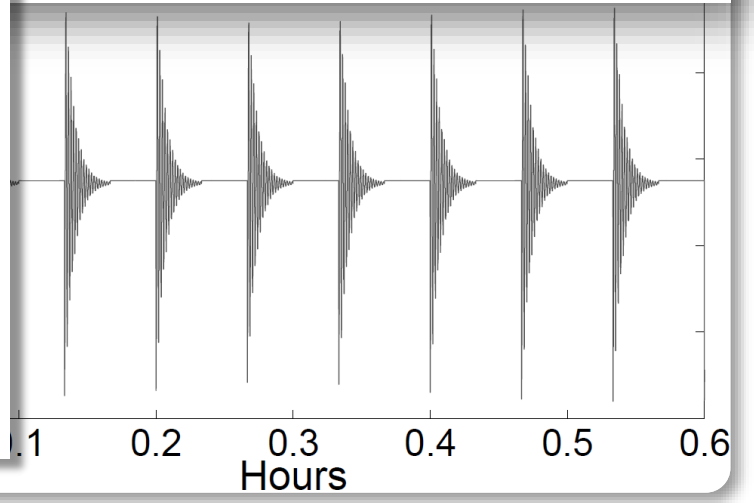
$$u(t) = K\left(e(t) + \frac{1}{T_i}\int_0^t e(\tau)d\tau + T_d\frac{de(t)}{dt}\right)$$

$$(\varepsilon\sum_{k=1}^{7} C_{i,k}Cp_{i,k} + \rho_b Cp_b)\frac{\partial T_i}{\partial t} = -\frac{\partial(v_i\sum_{k=1}^{7}(C_{i,k}Cp_{i,k})T_i)}{\partial z} - \phi_i\rho_b(r_{1,i}E_1 + r_{2,i}E_2) - Q_i^{RCT}$$

```
/*calculate derivatives*/
for (n=1;n<NR;n++)
{
    /*dC/dt=-delta(C*v)/deltaZ+sum(vij*rj)                    */
    /*Use single backward                                    */
    C_O2_t[n-1]=(-(C_O2[n]*v[n]-C_O2[n-1]*v[n-1])/dz + Coefficient1[0]*r_all[n][0]+Coefficient2[0]*r_all[n][1])/cata_porosity;
    C_CO2_t[n-1]=(-(C_CO2[n]*v[n]-C_CO2[n-1]*v[n-1])/dz + Coefficient1[1]*r_all[n][0]+Coefficient2[1]*r_all[n][1])/cata_porosity;
    C_C2H4_t[n-1]=(-(C_C2H4[n]*v[n]-C_C2H4[n-1]*v[n-1])/dz + Coefficient1[2]*r_all[n][0]+Coefficient2[2]*r_all[n][1])/cata_porosity;
    C_VAc_t[n-1]=(-(C_VAc[n]*v[n]-C_VAc[n-1]*v[n-1])/dz + Coefficient1[4]*r_all[n][0]+Coefficient2[4]*r_all[n][1])/cata_porosity;
    C_H2O_t[n-1]=(-(C_H2O[n]*v[n]-C_H2O[n-1]*v[n-1])/dz + Coefficient1[5]*r_all[n][0]+Coefficient2[5]*r_all[n][1])/cata_porosity;
    C_HAc_t[n-1]=(-(C_HAc[n]*v[n]-C_HAc[n-1]*v[n-1])/dz + Coefficient1[6]*r_all[n][0]+Coefficient2[6]*r_all[n][1])/cata_porosity;
    Q_rct[n]= UA*(Tg[n]-Shell_T); /*kcal/min m^3*/
    Tg_t[n-1]=1/(cata_porosity*CCP[n] + cata_heatcapacity *cata_bulk_density)*(-FCP[n]*(Tg[n]-Tg[n-1])/dz - r_all[n][0]*E_r1-r_all[
    n][1]*E_r2-0 rct[n]);
};
```

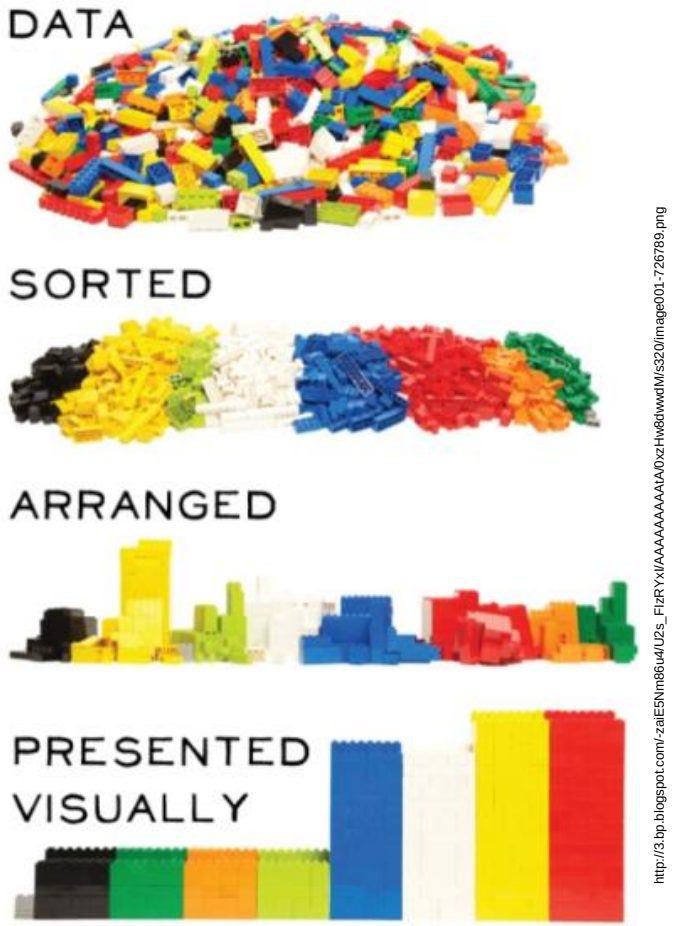






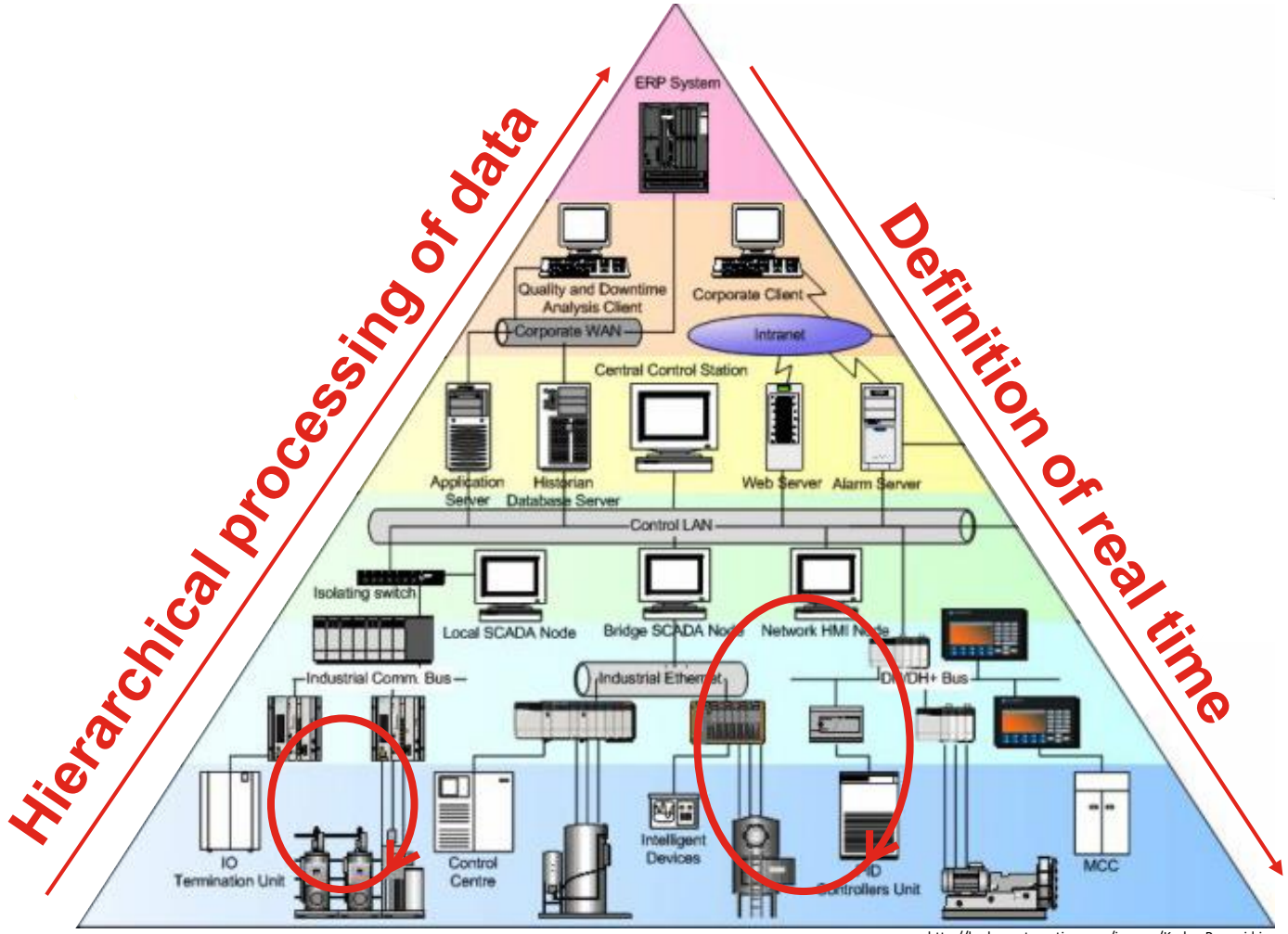
Information as an asset

- **Computer-Integrated Manufacturing** (CIM) concept in the 1970s
- The most essential constituent of modern automation is data, and processing this data into information is a substantial task in automation
- The key to handling information was the establishment of a transparent data flow inside an automation system with a strict subdivision of the data processing into a hierarchical model → **automation pyramid**



http://3.bp.blogspot.com/-zaiE5Nm86u4/U2s_FIzRYxI/AAAAAAAAAtA/0xzHw8dwwdM/s320/image001-726789.png

Automation pyramid

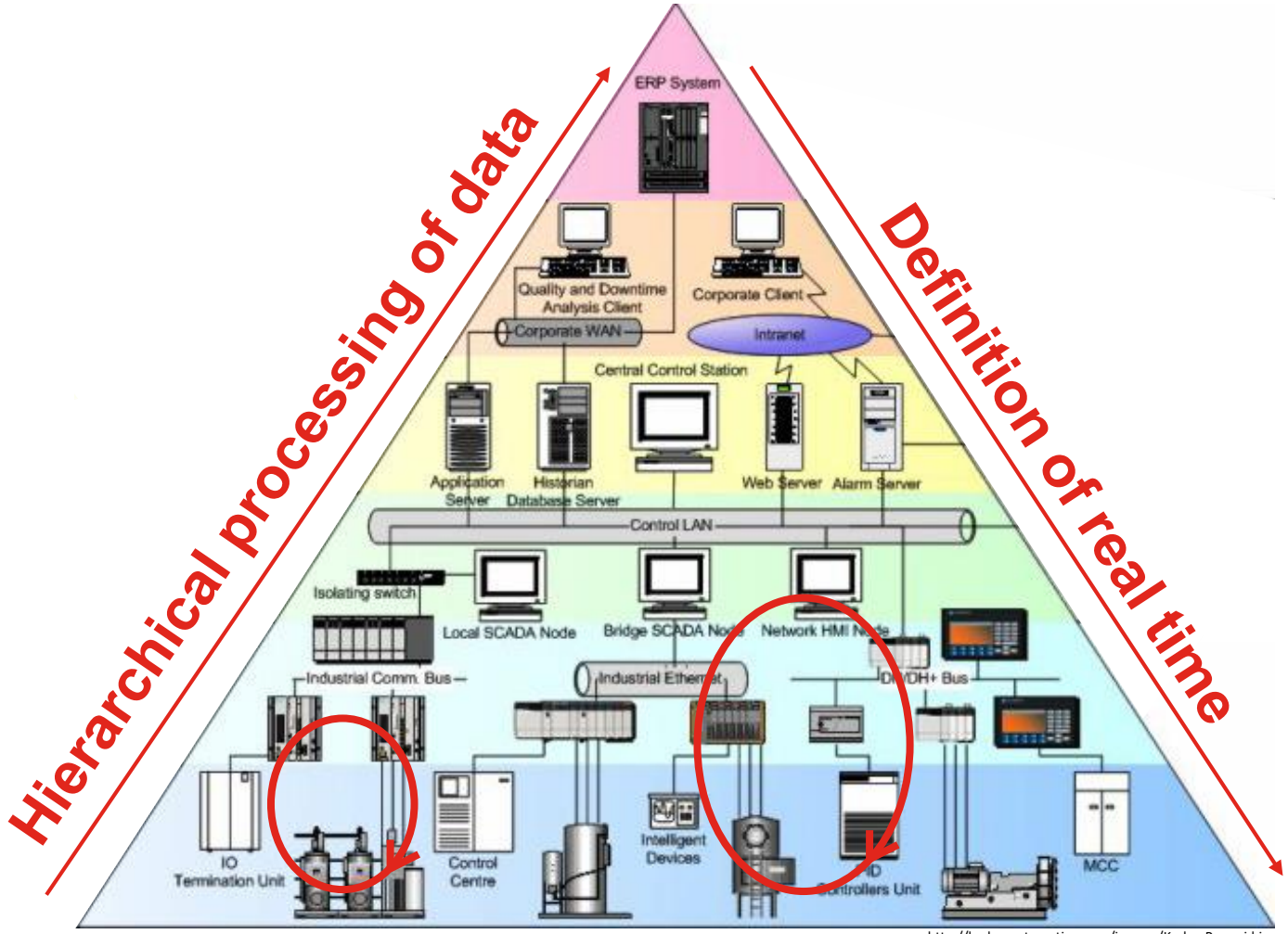


http://krakenautomation.com/images/KrakenPyramid.jpg

Loop in milli/nano seconds

Loop in seconds

Automation pyramid

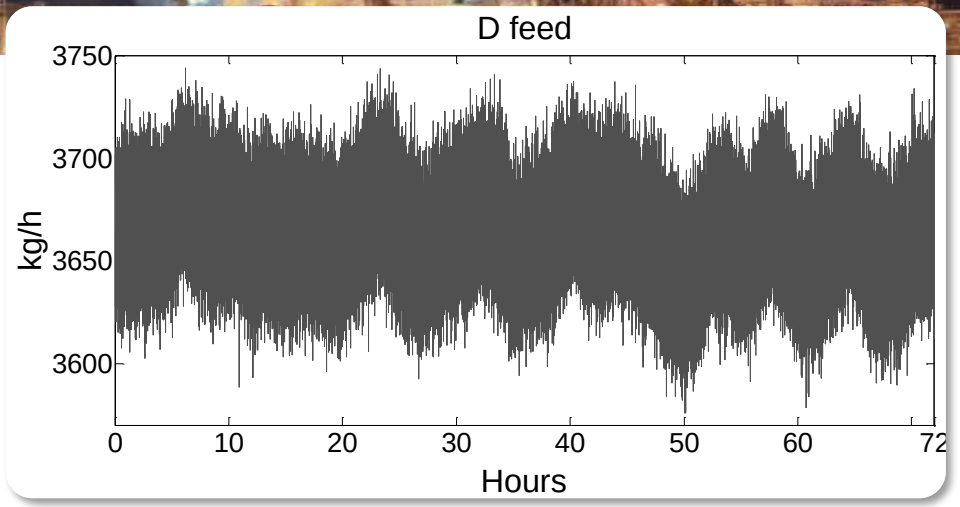


http://krakenautomation.com/images/KrakenPyramid.jpg

Operates on raw data

Operates on information

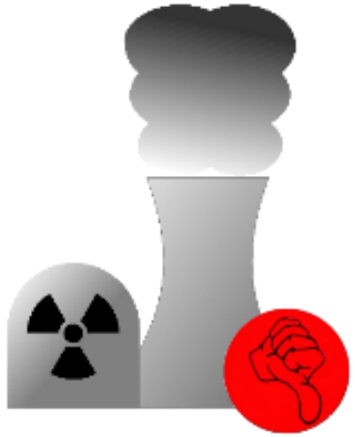
Data processing

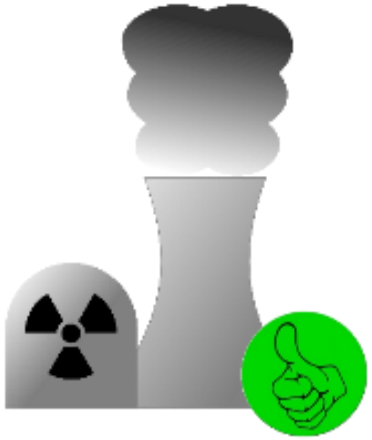


- Raw sensory data rarely can be used directly. The electrical output of a sensing element is usually small in value and has non-idealities such as offset, sensitivity errors, nonlinearities, noise, etc.
- Sensor signal is manipulated (processed) in a specific way to meet the requirements of data consuming circuits/devices/applications to produce meaningful information
  - **Data conditioning, conversion, aggregation, transformation, analysis…..**

Impact of data processing

Equipment damage at nuclear plant

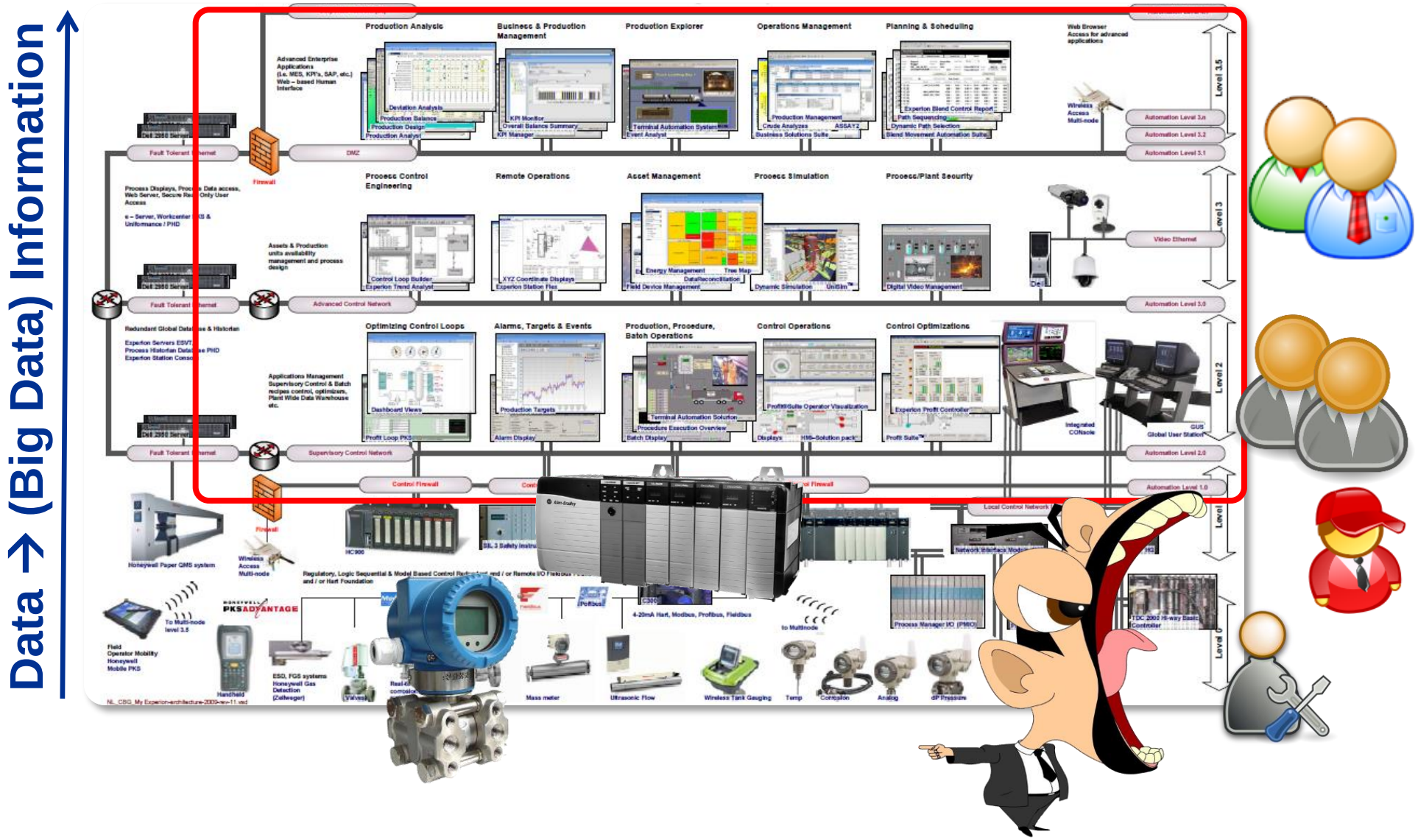




- Two identically built nuclear plants. One had flow induced vibration issue. And another did not.
- **The vibrations indication showed itself as a resonance (high-frequency) “noise”**
  - Field engineer has changed signal filtering parameter in the signal recorder to get rid of noise
  - Loss of view into vibration issue

http://www.controlglobal.com/blogs/unfettered/marina-krotofils-presentation-on-how-to-hack-a-chemical-plant-and-its-implication-to-actual-issues-at-a-nuclear-plant/

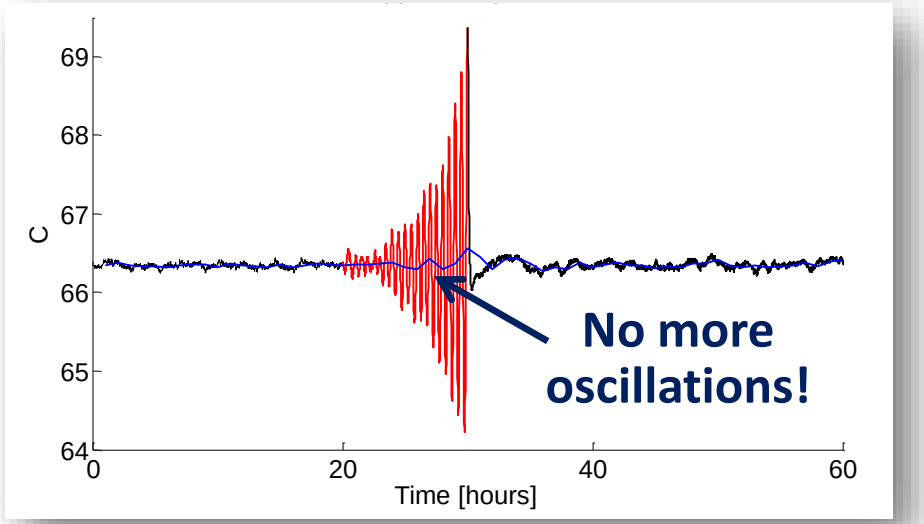
Process data reliability



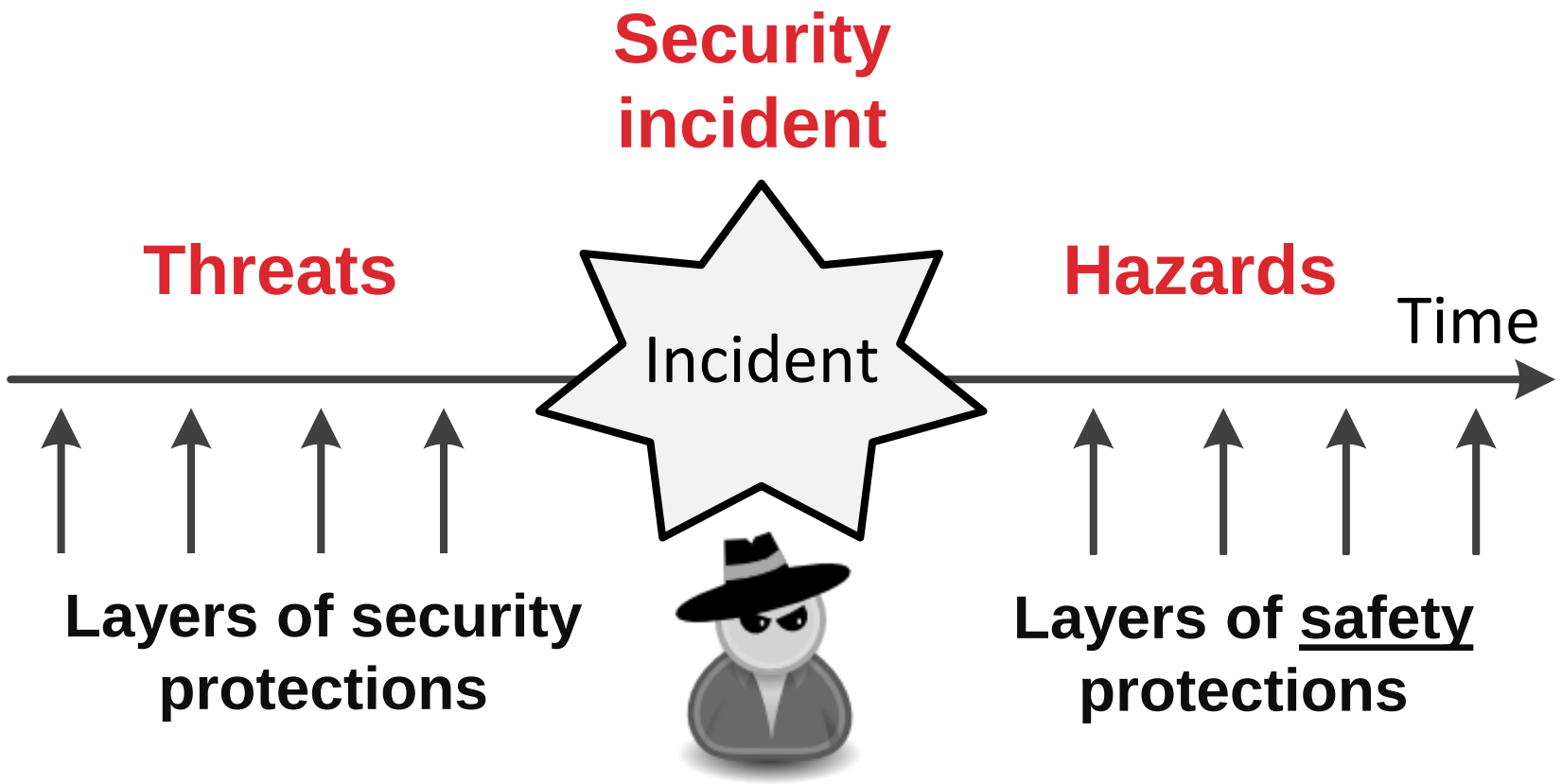
Signal/data processing points

Signal processing points is **an attack vector** in ICS / cyber-physical systems

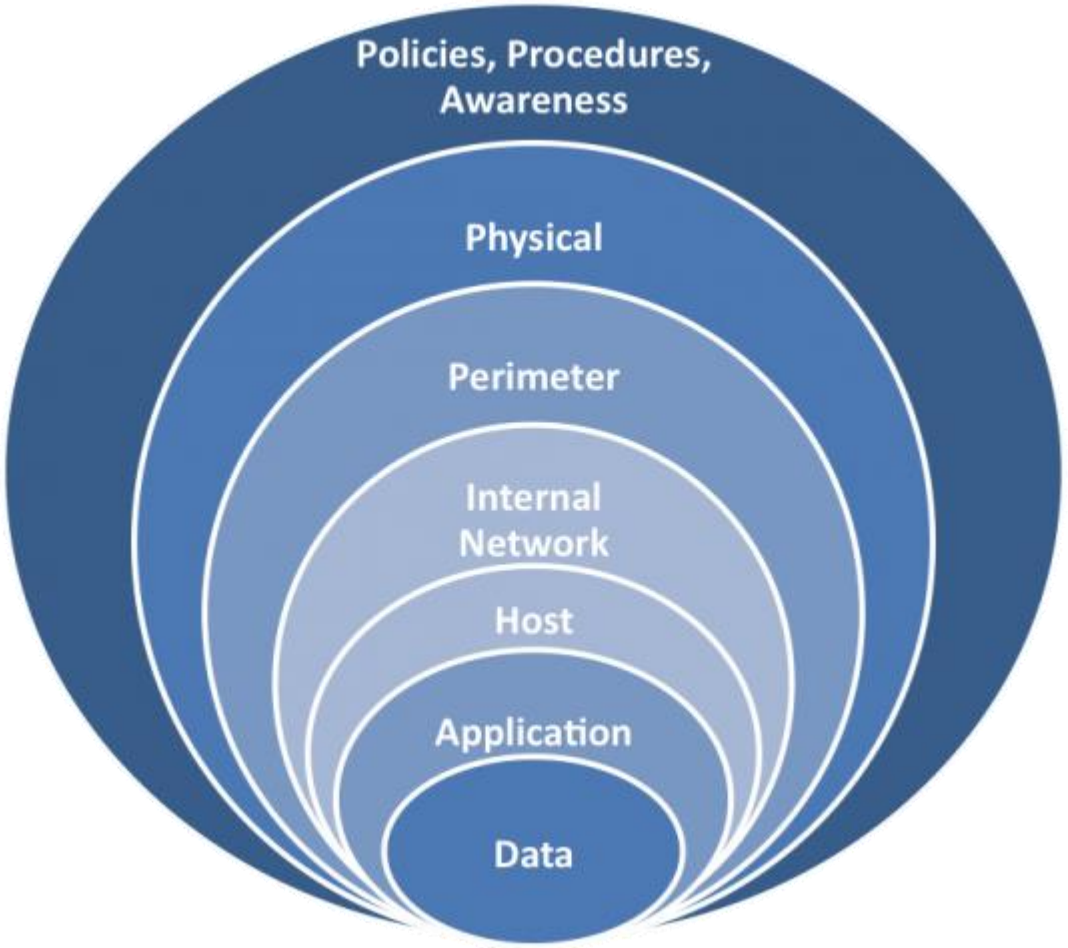
- Analyzing data processing points
  - Often “human friendly”
  - Tell you exactly how to make data out of spec
  - Allow for “educated guess” and granular manipulation
- Good for
  - Making data unusable; deceiving about process state
  - Removing attack traces (e.g. spikes, etc.)
  - Misleading forensics investigators
  - Etc., etc.



Security vs. Safety

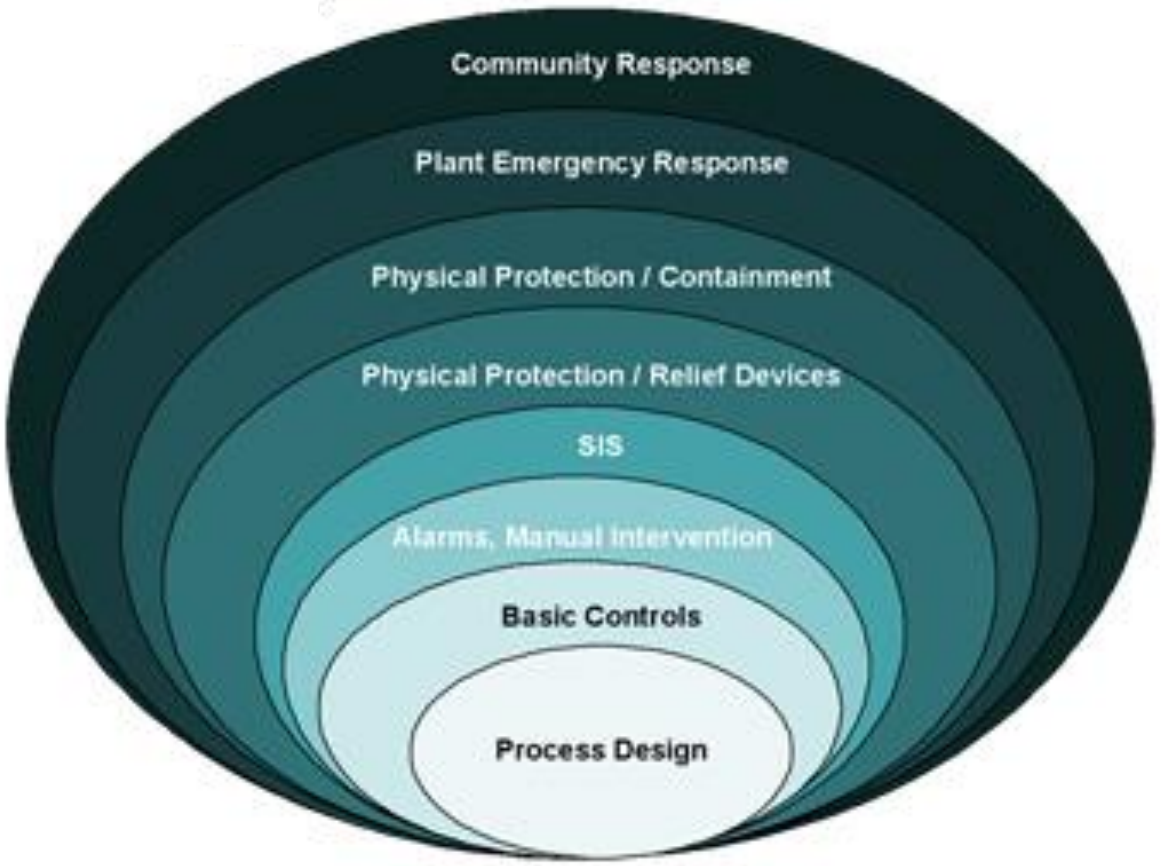


Security onion



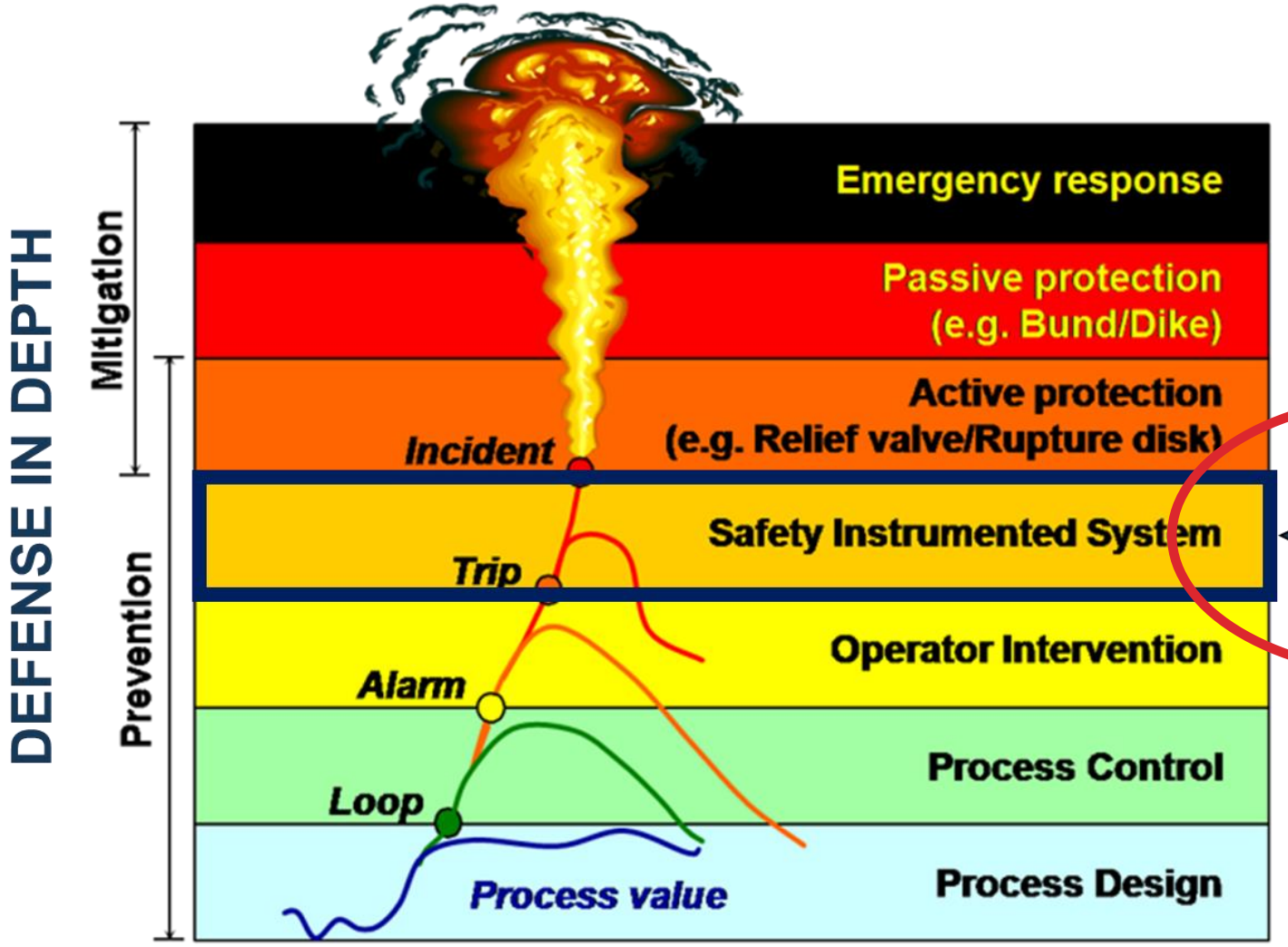
http://zentekconsulting.com/wp-content/uploads/2016/03/Defense-in-Depth-Graphic-e1478548099459.png

Safety onion



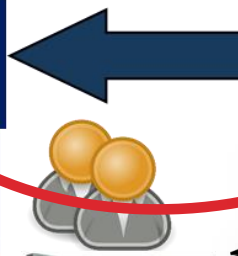
http://www.gmigasandflame.com/sil_info_layers.jpg

Hazards and layers of safety protections

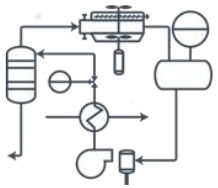


https://www.arcweb.com/sites/default/files/Images/blog-images/Layers-of-Protection.png

http://www.oseco.com/markets/processing/index.cfm?appID=23#23

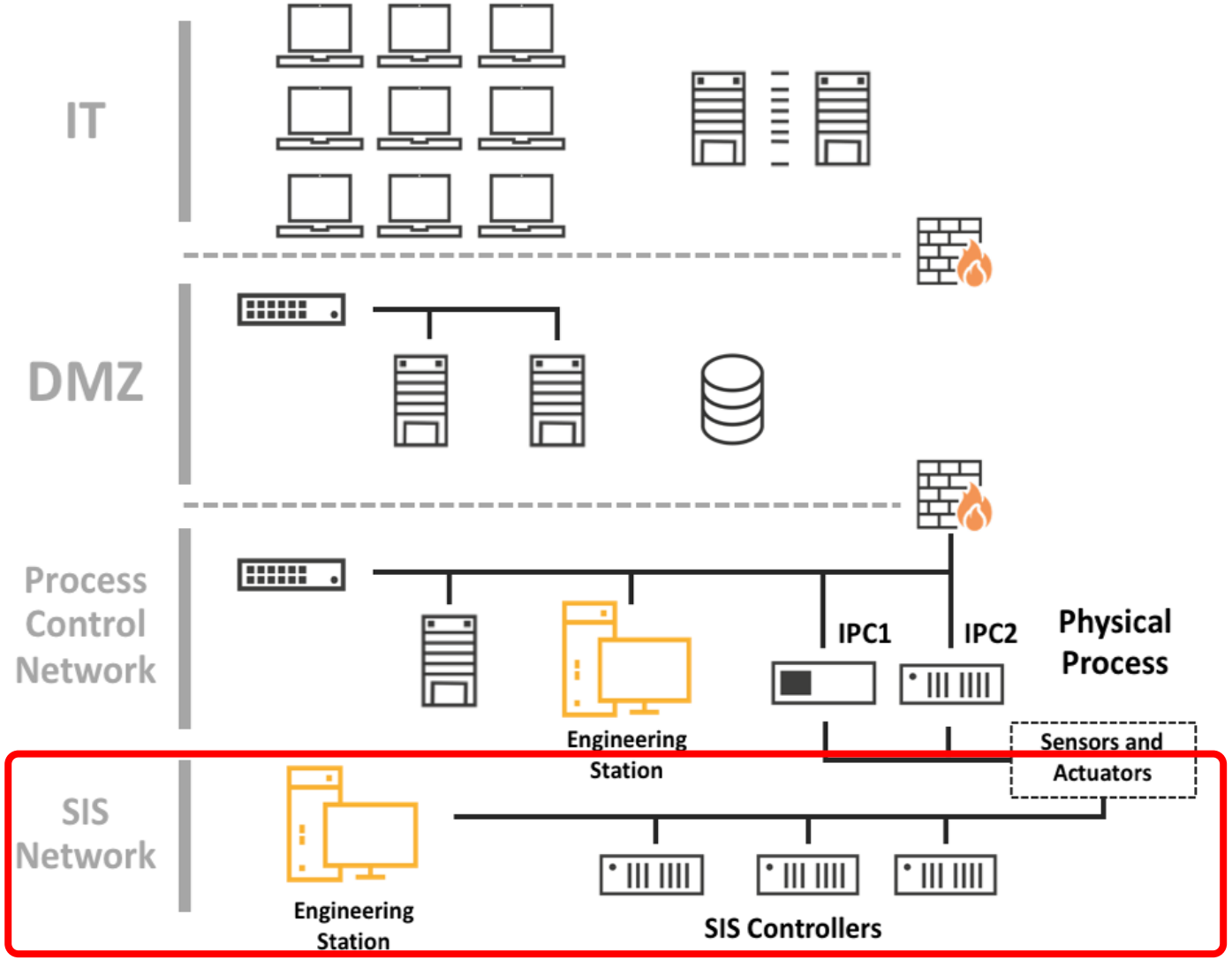


SIS



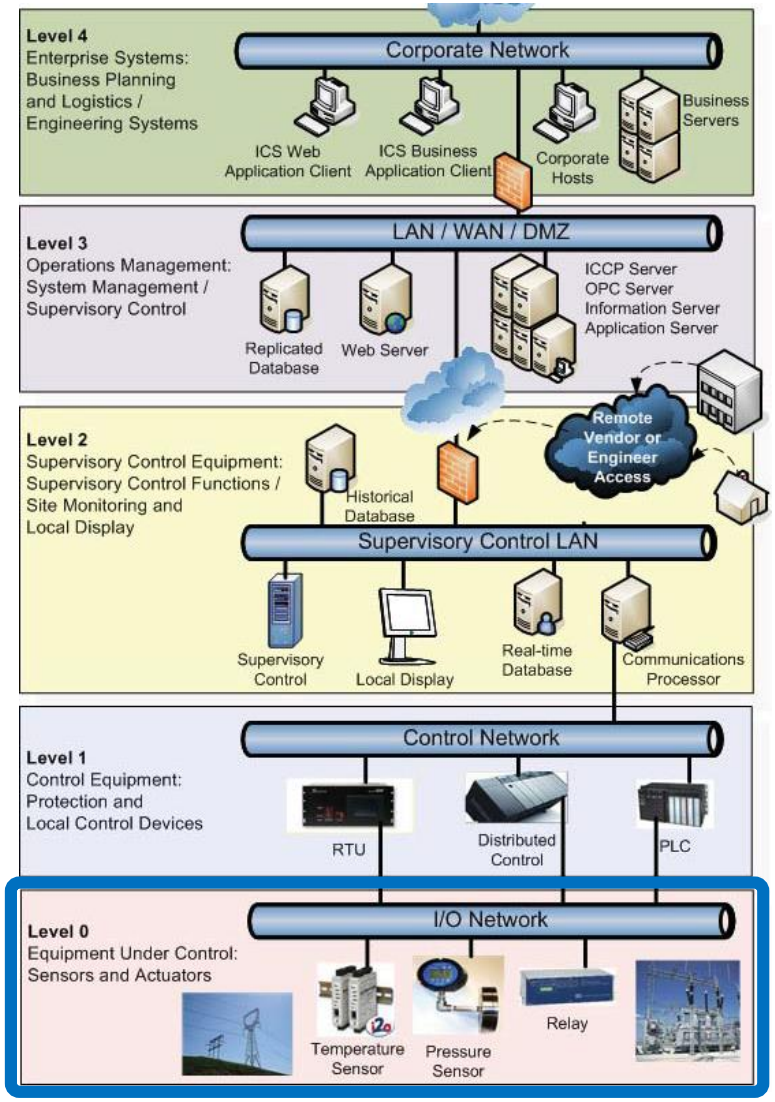
Worst case attack on ICS

An attack on a safety system can cause the MOST DAMAGING outcome of a cyber-physical attack



https://www.cyberark.com/threat-research-blog/anatomy-triton-malware-attack/

Process data as root of trust

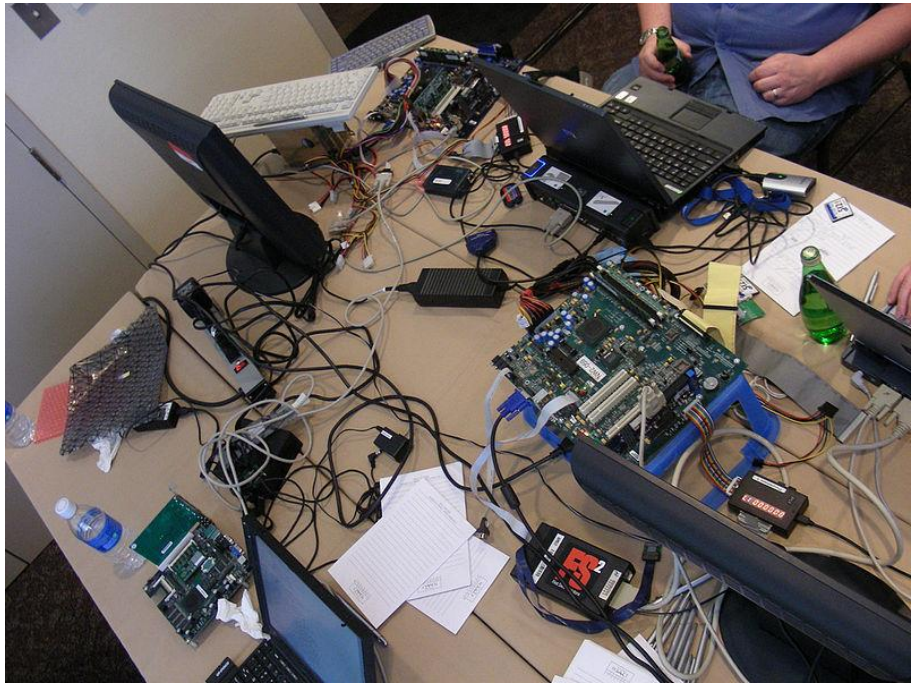


- If process data is incorrect, control algorithms, human operator and safety systems may take wrong (harmful) control decisions
- Ensuring **trustworthiness** of process data (**veracity** of data) is **the most crucial task** in cyber-physical security
  - Failed/misconfigured sensors or data processing points, mistakes in calculations and similar
  - Malicious tampering with process data
  - Process data is **root of trust** in ICS/cyber-physical security

Race-to-the-Bottom in ICS

Attackers vs. defenders

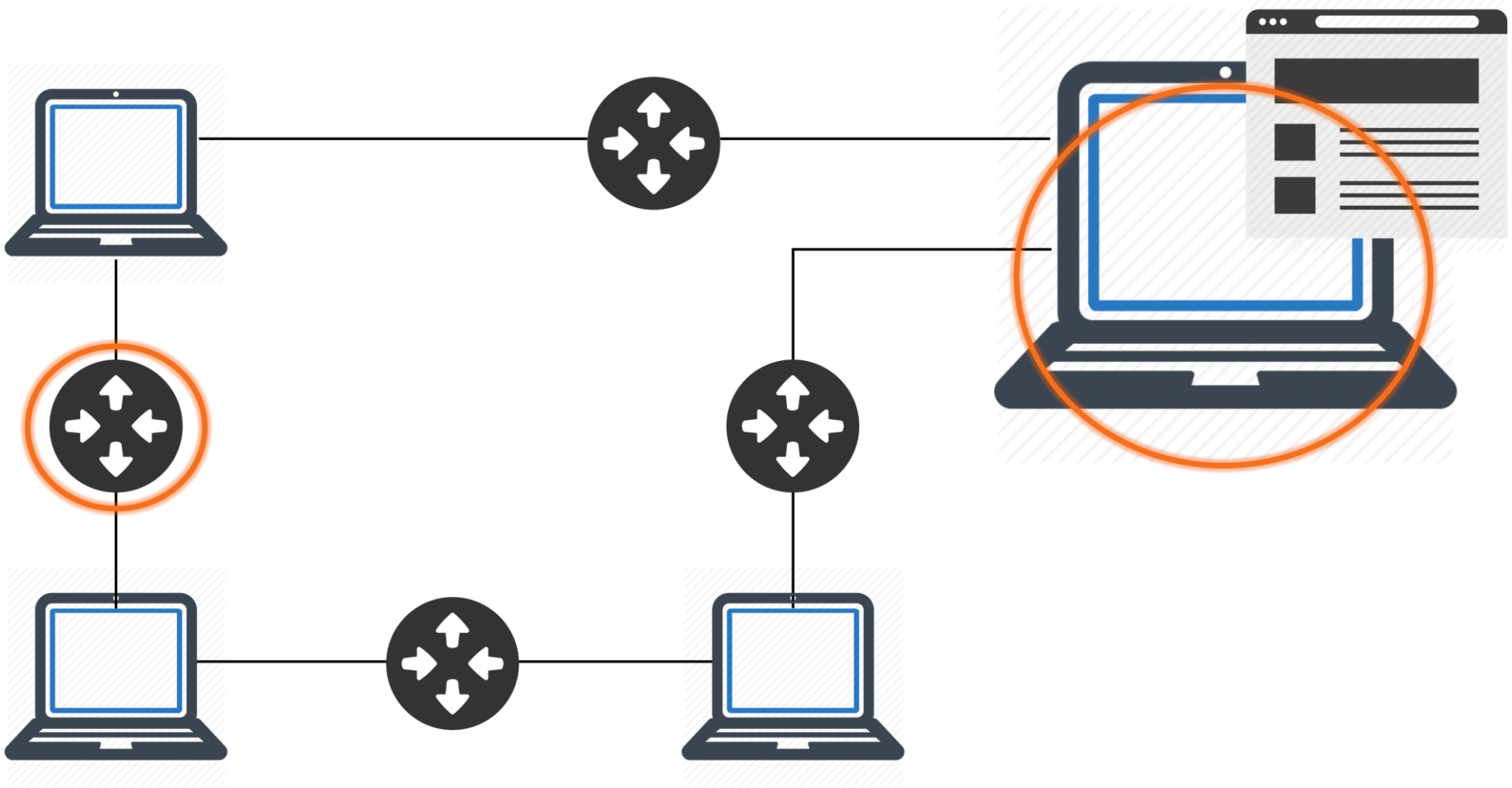
Attackers' vs. defenders skill sets



https://upload.wikimedia.org/wikipedia/commons/thumb/f/fb/Hacking_Coreboot.jpg/800px-Hacking_Coreboot.jpg

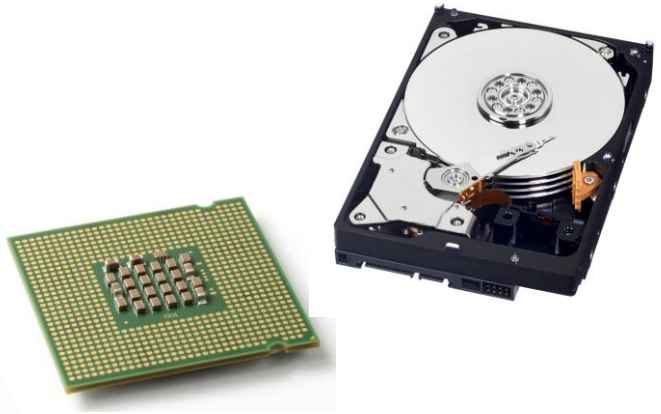
https://upload.wikimedia.org/wikipedia/commons/thumb/f/fb/Hacking_Coreboot.jpg/800px-Hacking_Coreboot.jpg

Security is a moving target



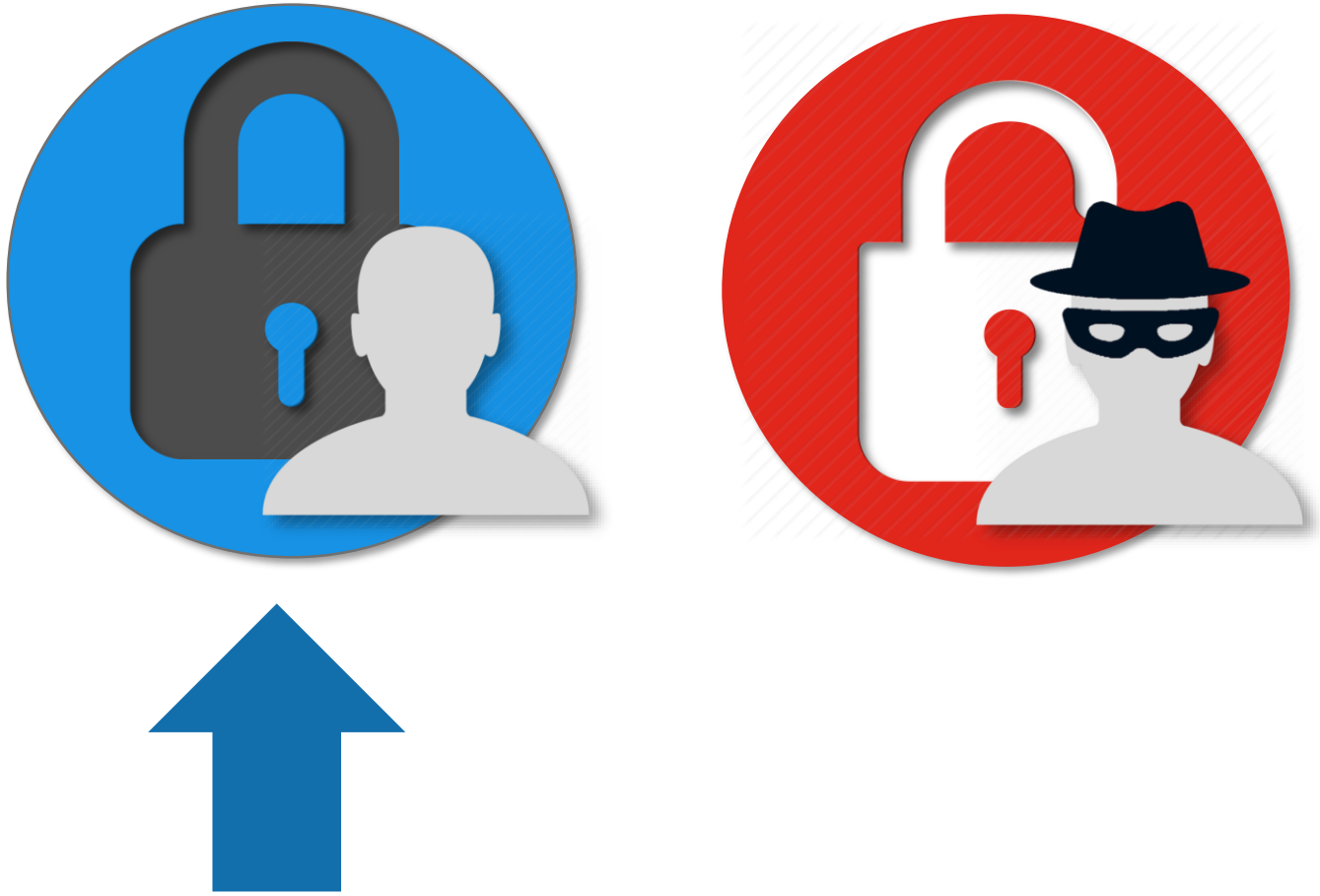
Your computer isn't a single computer

any more…..

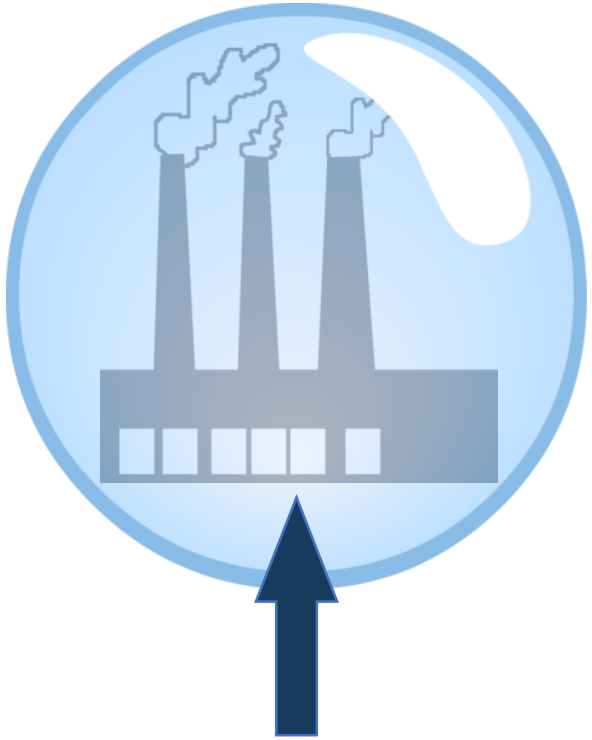


RACE TO THE BOTTOM

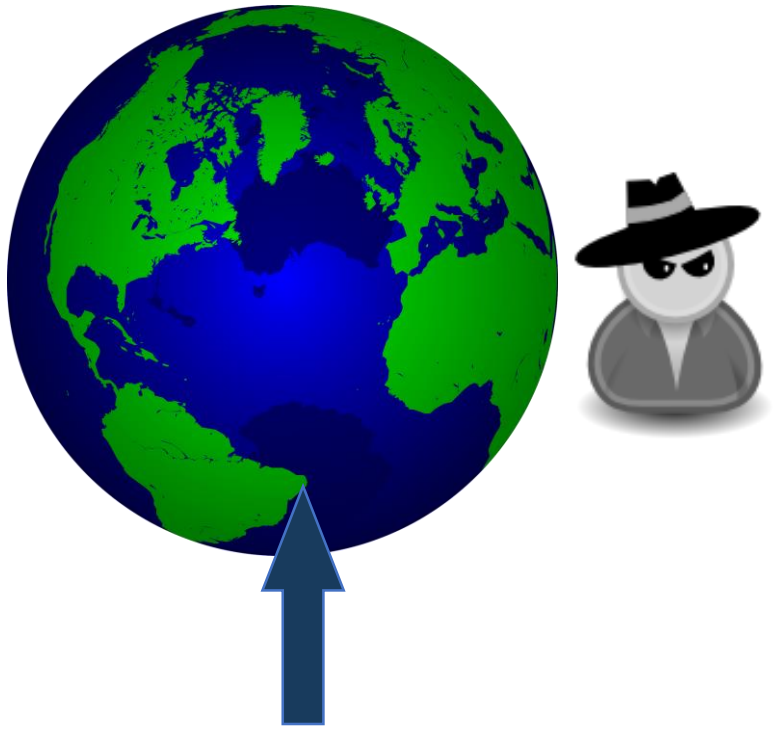
Advanced Persistent Threat (APT)



ICS landscape has changed



Nobody even knows about our existence



Crazy amount of hacking on a daily basis

Brief history of ICS attacks

Reconnaissance and weaponization of capabilities

It's happening: Publicly known cyber-physical attacks

1999

First active recon & initial intrusion attempts

Successful *cyber-physical* experiments

2010

Planned operation to hinder Iran's nuclear program (Stuxnet)

https://qph.fs.quoracdn.net/main-qimg-f741c6e5db32b87f282e54448a2129ce

2013

First publicly known OT recon activities (HAVEX)

2015

Ukraine power grid attack (BlackEnergy)

https://www.bankinfosecurity.com/ukrainian-power-grid-hacked-a-8779

2016

Ukraine power grid attack (Industroyer)

2017

TRITON

https://www.schneider-electric.com/ww/en/Images/tricon-IC-654x654.jpg

TRITON in the news

THE WALL STREET JOURNAL.

TECH

New Type of Cyberattack Targets Factory Safety Systems

Malicious software Triton was able to manipulate Schneider Electric devices' memory and run unauthorized programs by leveraging a previously unknown bug

The Washington Times

Industrial safety systems targeted by Triton malware meant to cause 'physical consequences': Reports

WIRED

ANDY GREENBERG SECURITY 12.14.17 10:00 AM

UNPRECEDENTED MALWARE TARGETS INDUSTRIAL SAFETY SYSTEMS IN THE MIDDLE EAST

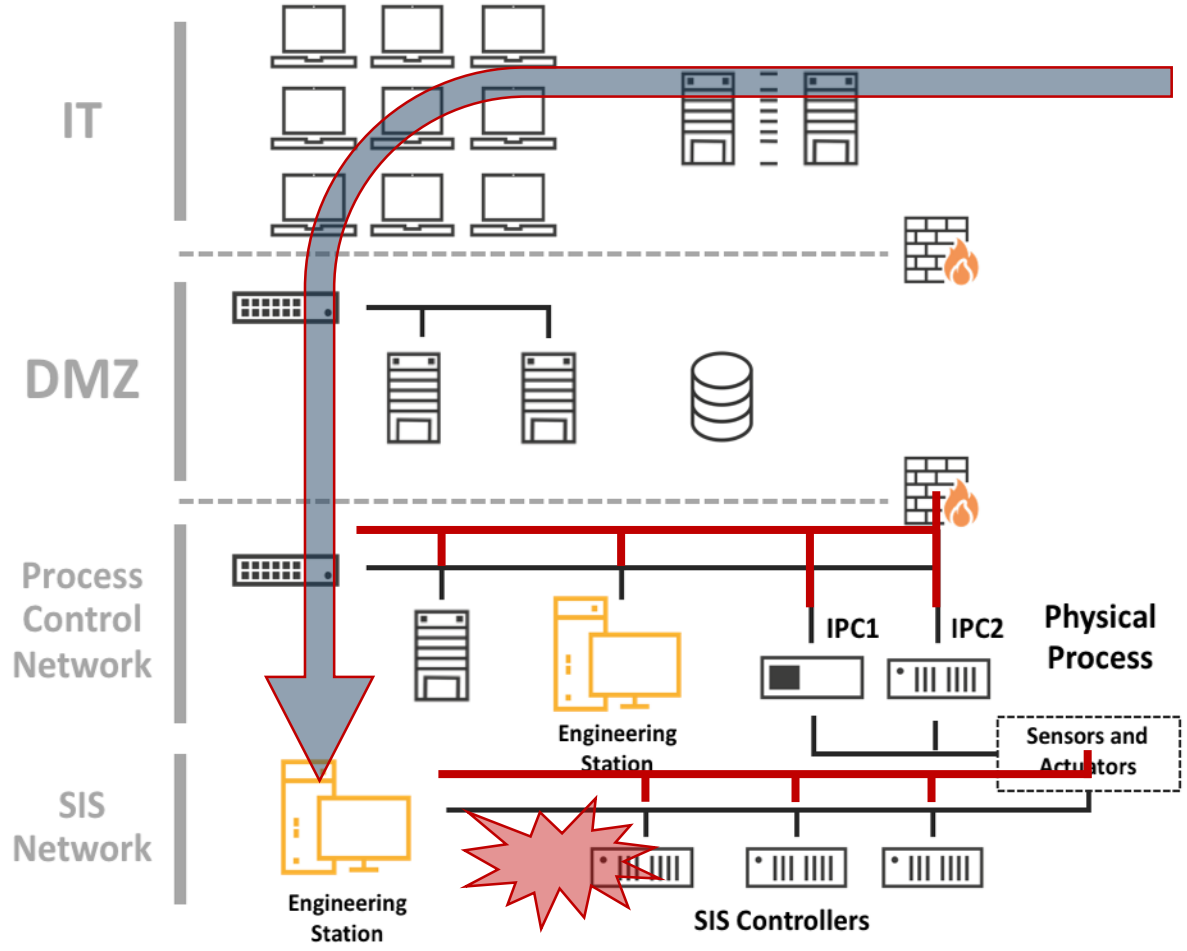
Hackers use Triton malware to shut down plant, industrial systems

The malware has been designed to target industrial systems and critical infrastructure.

By Charlie Osborne for Zero Day | December 15, 2017 -- 09:54 GMT (01:54 PST) | Topic: Security

ZDNet

TRITON incident description



Attacker obtained **remote access** to SIS communication network

Dual-homed SIS Eng. Workstation

TRITON implant capability

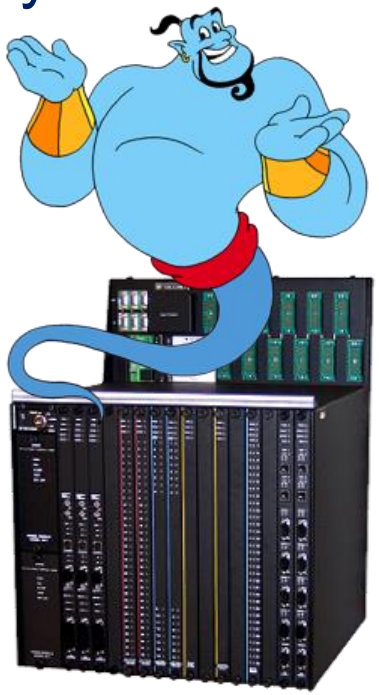
- Attacker attempted to inject passive implant into safety controller
  - Runs as user program on controller, activated by special network packet
  - Read / Write / Execute memory

trilog.exe
- script_test.py
- library.zip
- inject.bin
- imain.bin

TriStation protocol

imain.bin + inject.bin

"Your wish is my command"



Triconex safety controller

TRICONEX: Safety Integrity Level (SIL3)

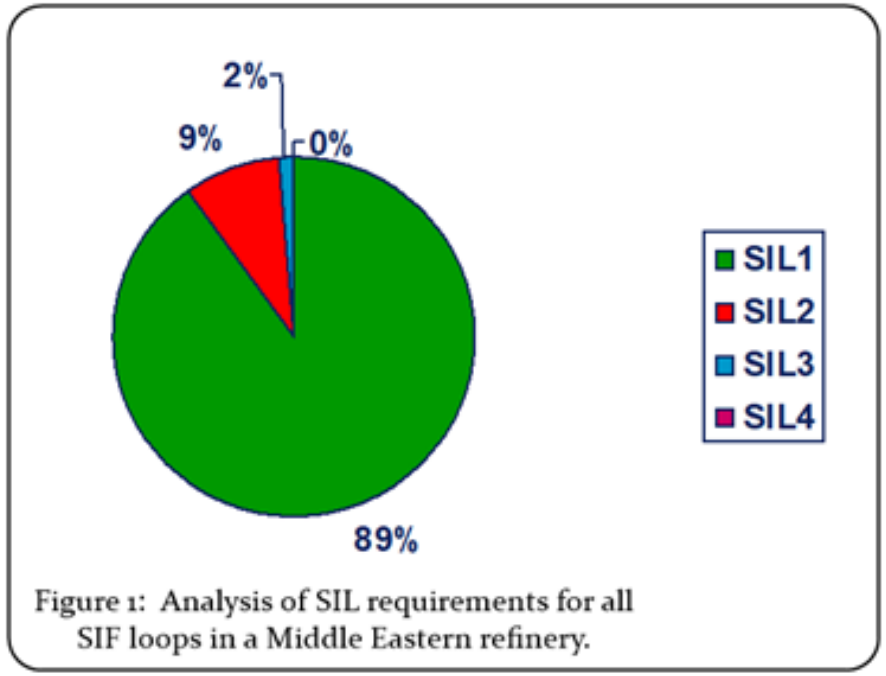
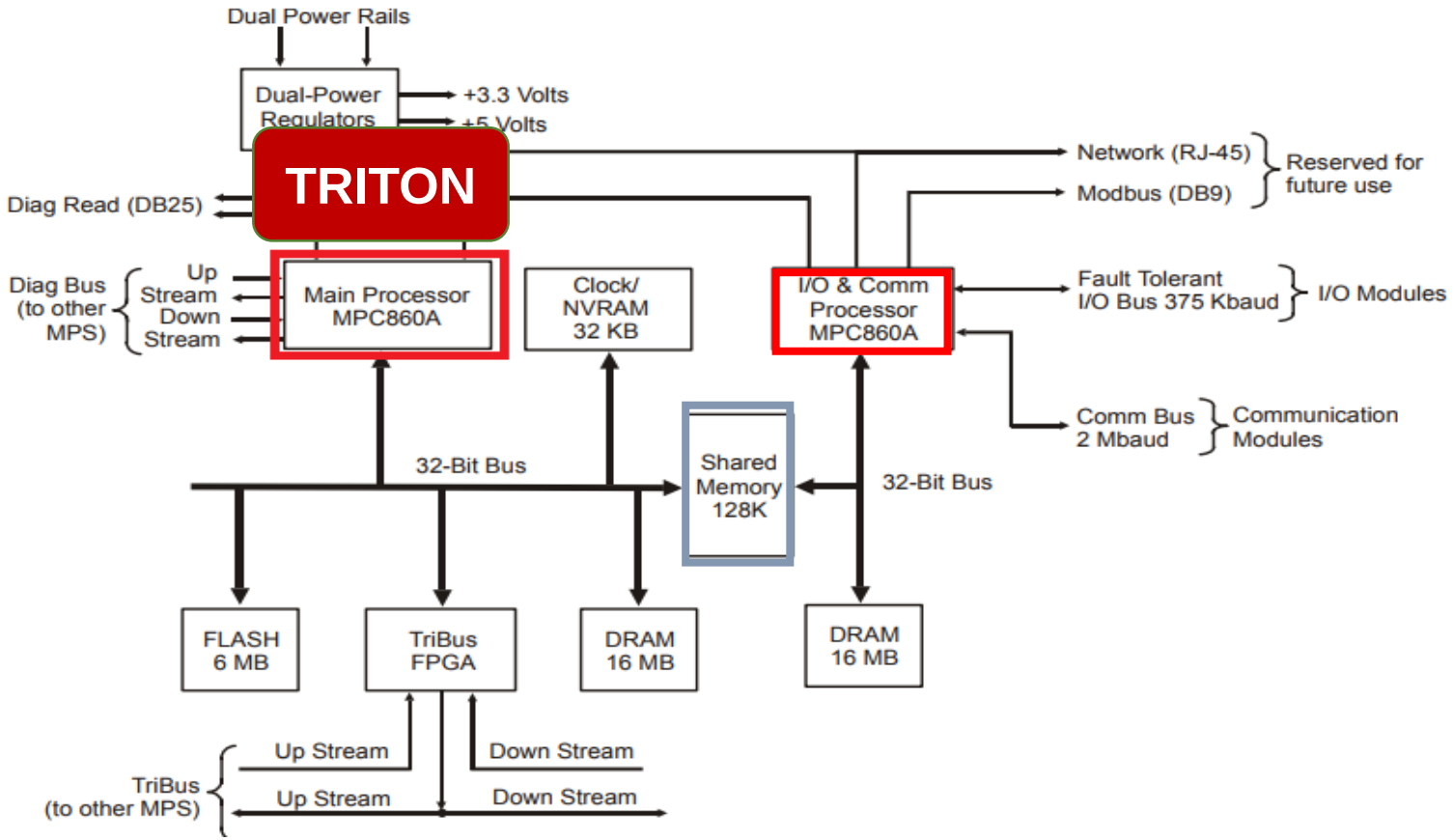


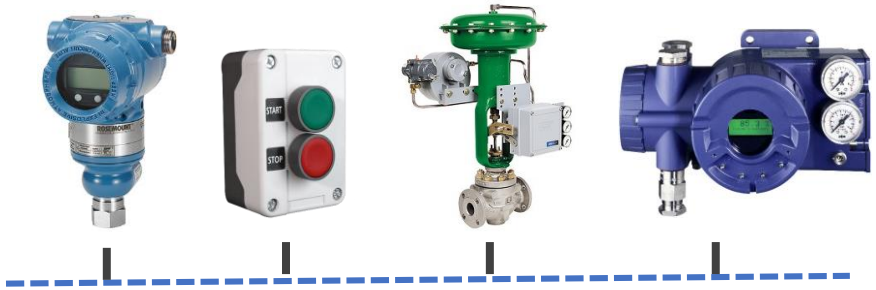
Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.

http://iom.invensys.com/EN/pdfLibrary/Datasheet_Triconex_TriconSIL3_06-11.pdf

TRITON worst case scenario



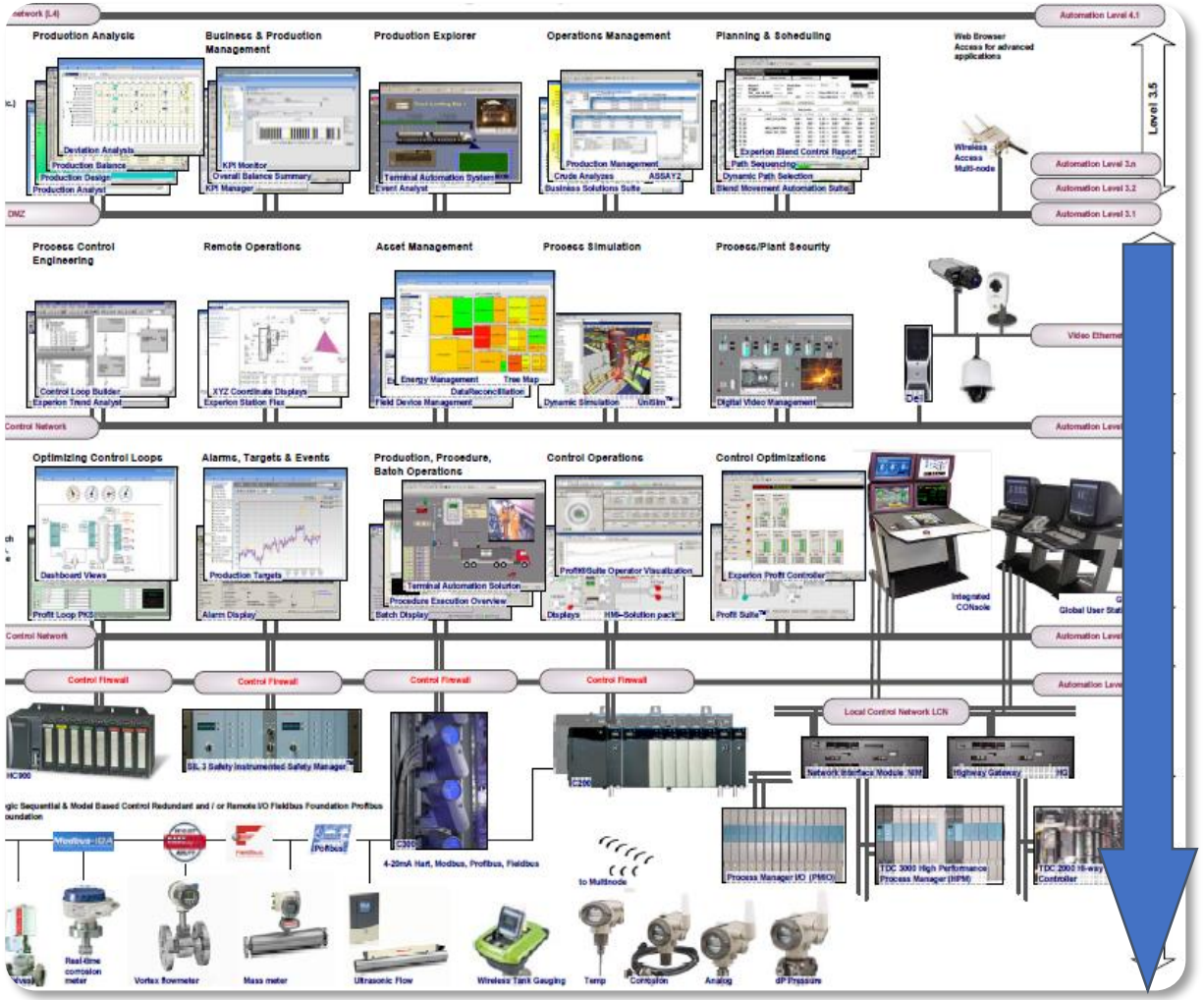
Architecture of model 3008 Main Processor



I/O signals

https://www.nrc.gov/docs/ML0932/ML093290420.pdf

Race-to-the-Bottom in ICS



HMI

Industrial protocols

Controllers

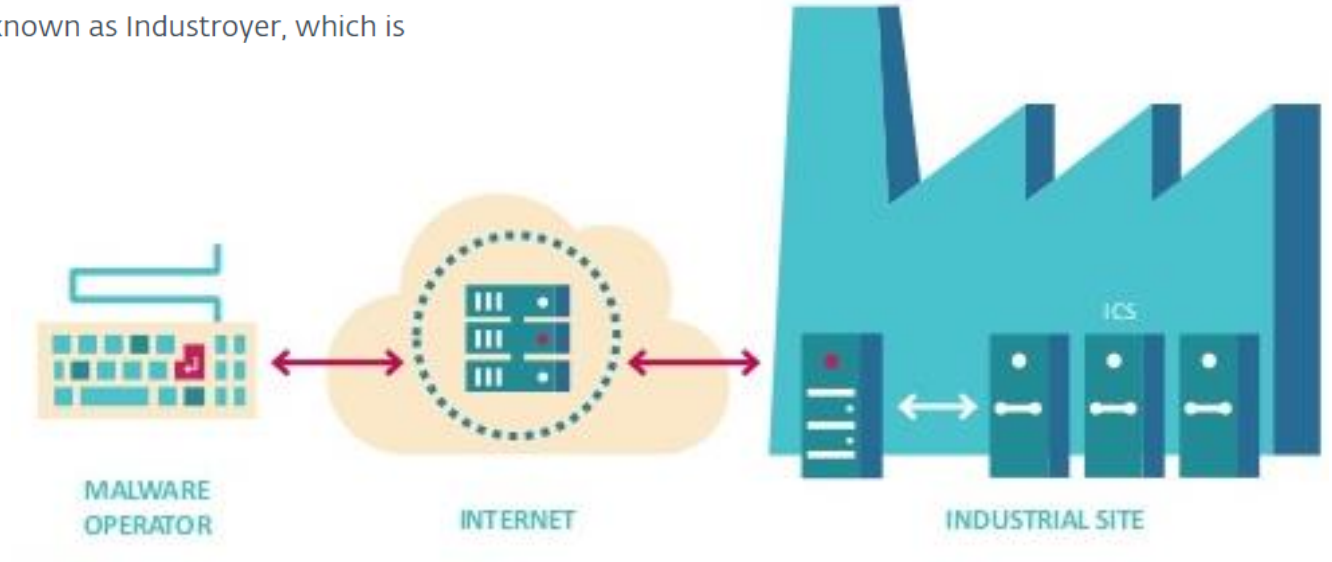
- Ukrainian power grid attack, 2015
- Ukrainian power grid attack, 2016 (Industroyer)
- TRITON, 2017

Application-driven nature of security science

Non-actionable threat intelligence

Industroyer: Biggest threat to industrial control systems since Stuxnet

ESET has analyzed a sophisticated and extremely dangerous malware, known as Industroyer, which is designed to disrupt critical industrial processes.



https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

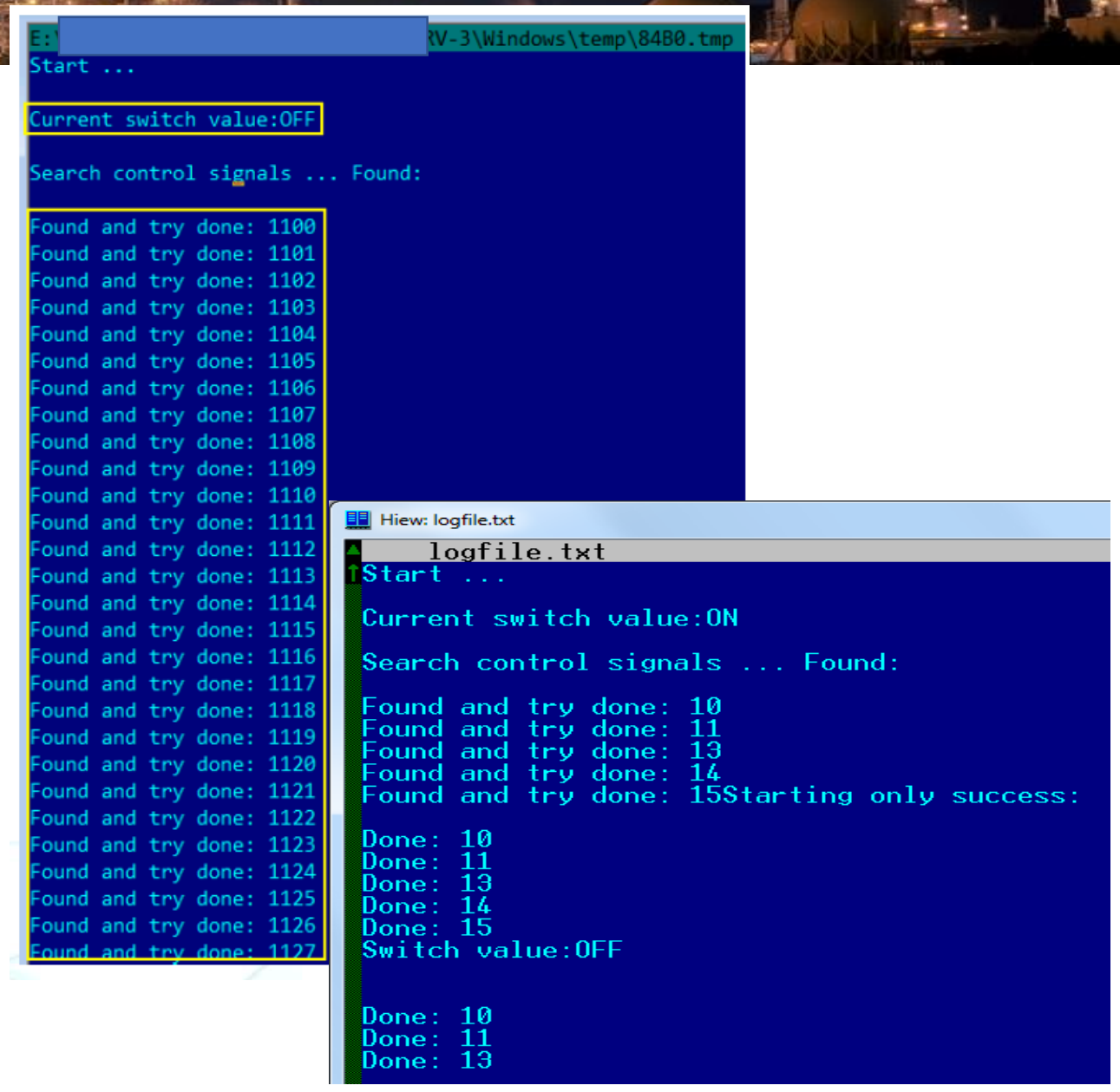
This is not a pragmatic threat intelligence

Pragmatic threat intelligence

Industroyer is substation configuration independent and can be seen as:

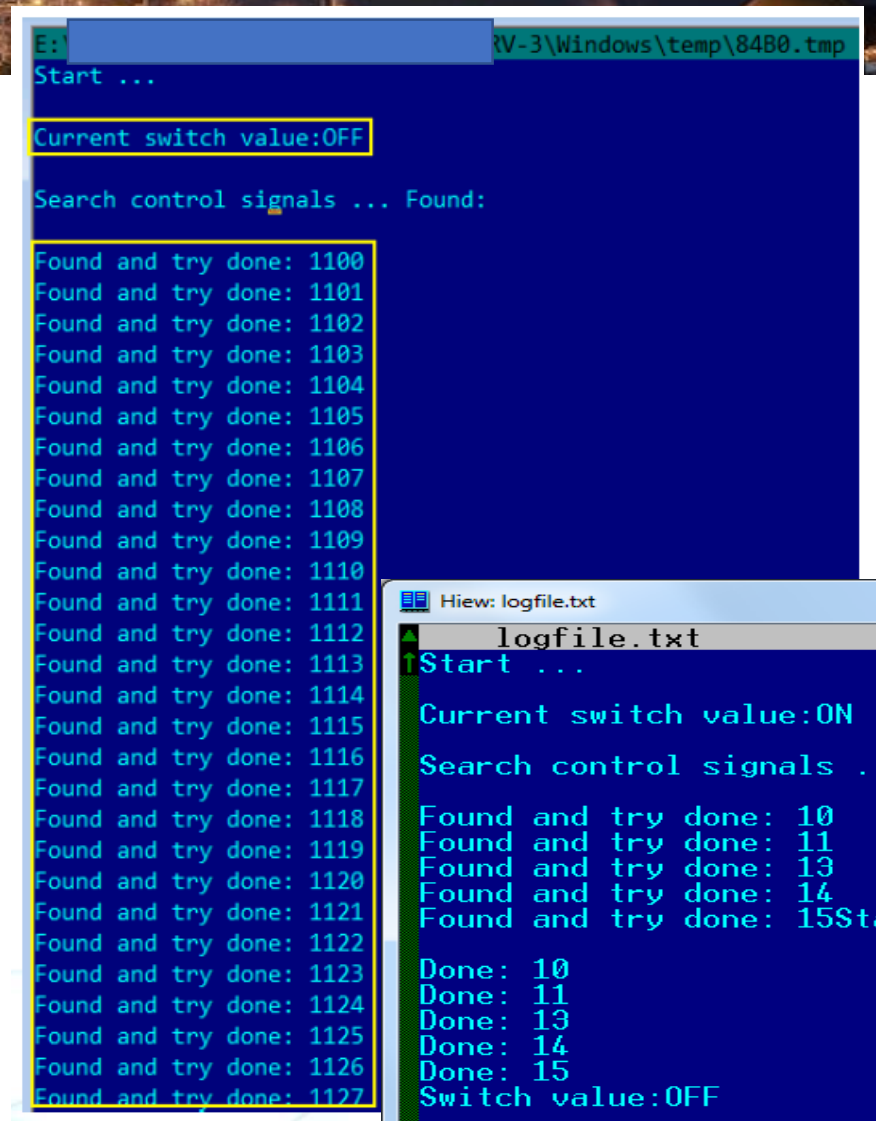
- Re-usable payload
- Lack or time/inability of attacker to conduct reconnaissance
- Lack of knowledge about electrical substations

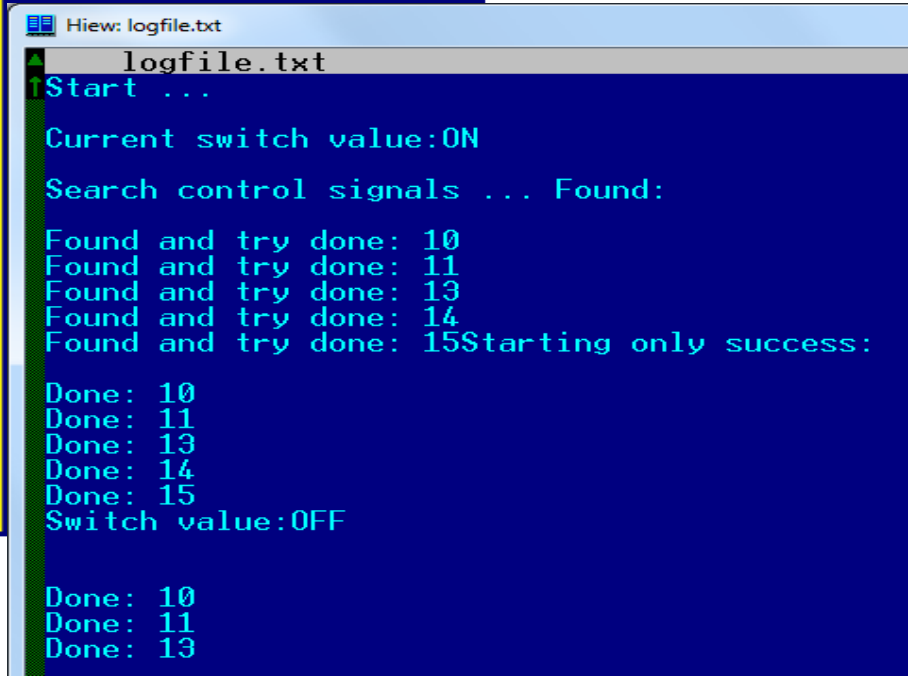
We can only evaluate this fact by considering other attributes of the attack and malware code



Pragmatic threat intelligence

While Industroyer was widely positioned as state-of-the-art destructive cyberweapon, it is a set of small utilities of limited capability and, seems like being not very valuable to the attacker





Pragmatic threat intelligence

While Industroyer was widely positioned as state-of-the-art destructive cyberweapon, it is a set of small utilities of little capability and, seems like, of not much value to the attacker

Germany Develops Offensive Cyber Capabilities Without A Coherent Strategy of What to Do With Them

AA FONT SIZE + PRINT AP PHOTO/MICHAEL PROBST

BY MATTHIAS SCHULZE
COUNCIL ON FOREIGN RELATIONS
READ BIO ›

SVEN HERPIG
COUNCIL ON FOREIGN RELATIONS
READ BIO ›

DECEMBER 3, 2018

TOPICS

Germany has traditionally prioritized defense over offense in cyberspace. That's now beginning to change.

There is a reoccurring debate in German national security and foreign policy whether Germany suffers from "Strategieunfähigkeit"—an inability to develop and implement strategy. The historic trauma of two lost World Wars created a

Security science

Security is not a fundamental science

It is application driven

Security solutions exist in the context of the application

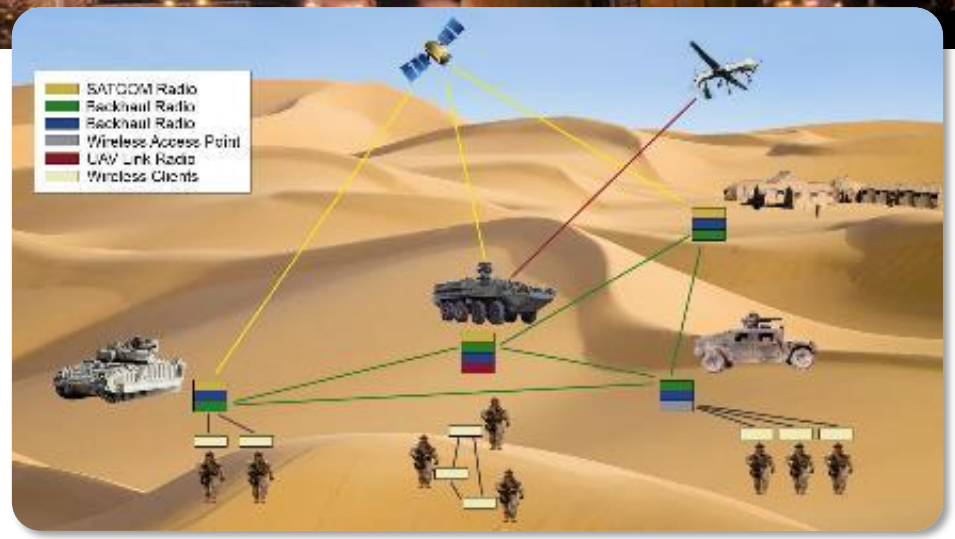
Early adopter: eCommerse

- **Security influences design decisions**
  - Attackers (mis)use functionality of web browsers
  - Novel approaches to designing web applications
  - Novel security controls in browsers

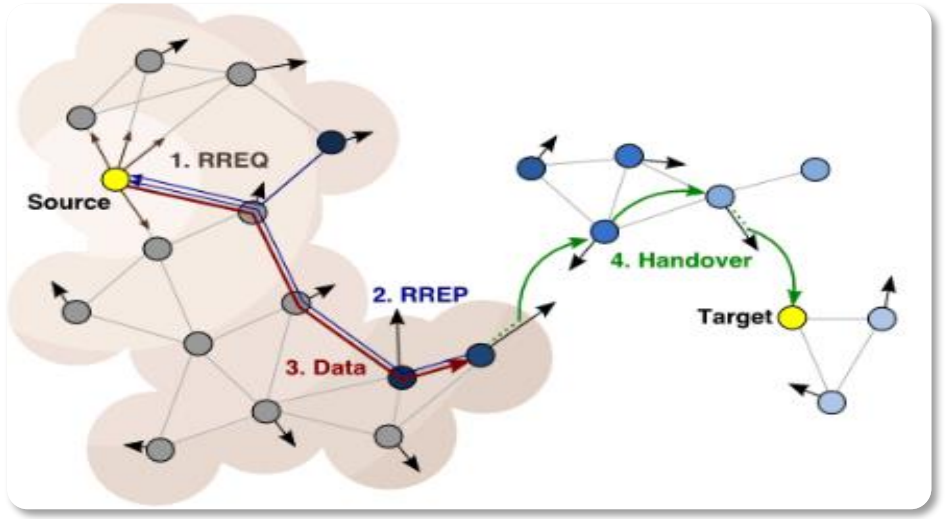
- **Application dictates security properties**
  - Information-theoretic security properties
  - CIA triad --> Parkerian hexad

Failed to adopt

- **Wireless sensor networks: Big hope**
  - A big hype for about a decade
  - Conferences, solutions, promising applications
  - Remained a “promising” technology with limited deployment
- **Wireless sensor networks: Big flop**
  - Deficiencies in the attacker models and security requirements
  - Unrealistic assumptions about physics of wireless communication



https://www.elprocus.com/wp-content/uploads/2014/12/Military-applications-based-on-wireless-sensor-networks.jpg



D. Gollmann, M. Krotofil, H. Sauff. Rescuing Wireless Sensor Networks Security from Science Fiction (WCNS’11)

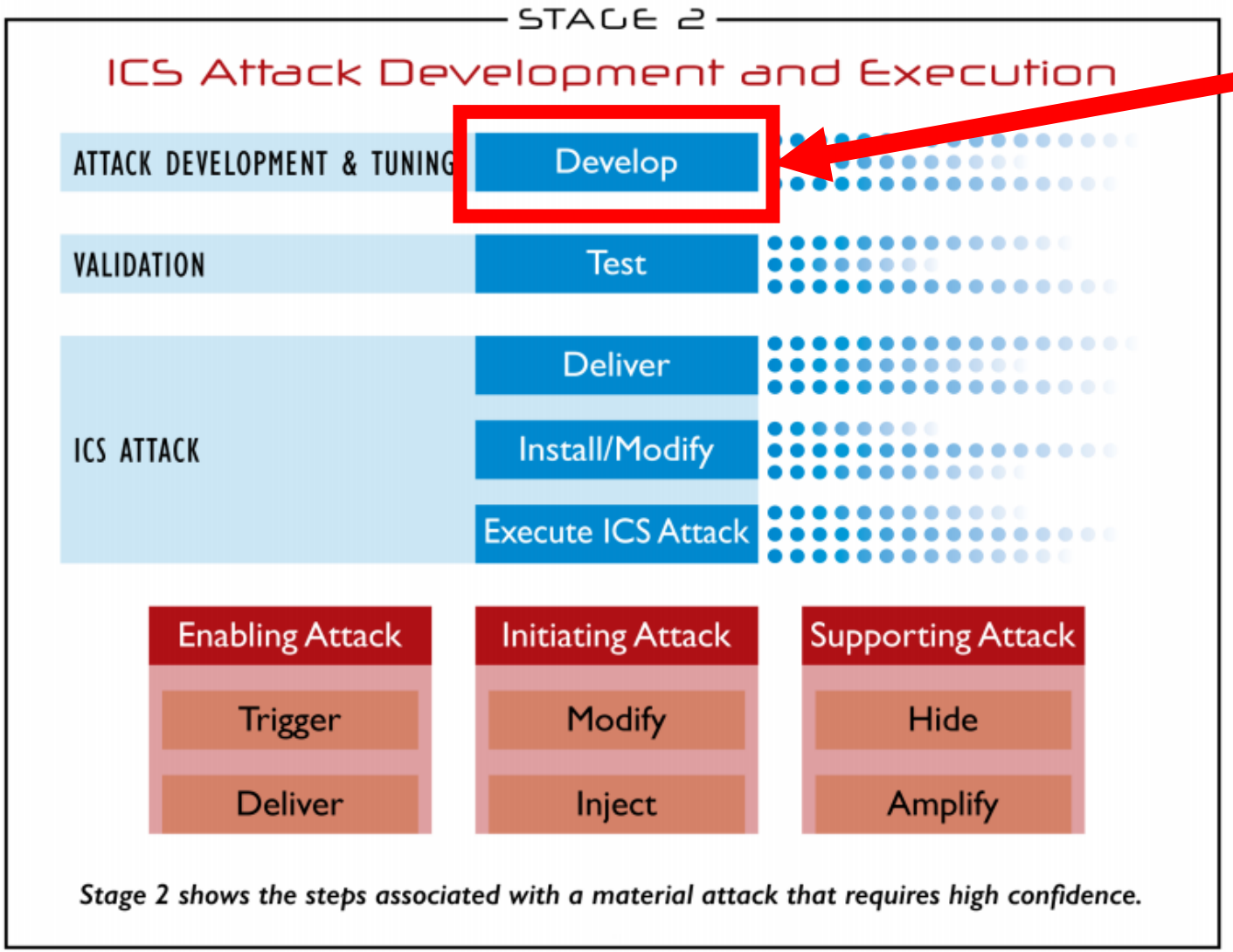
Experiment vs. assumptions

Tampering with Motes: Real-World Attacks on Wireless Sensor Networks

One of possible attacks on WSNs is called node capture where an adversary gains full control over sensor nodes through direct physical access. Many newer security mechanisms for WSNs take node capture into account. **It is usually assumed that node capture is "easy".** Some security mechanisms are verified with respect to being able to resist capture of 100 and more sensor nodes out of 10,000. **However, to the best of our knowledge, nobody ever tried to determine the actual cost to attack currently available sensor nodes**. Thus our project was set out to verify the assumption that node capture is easy.

A. Becher, Z. Benenson, M. Dornseif. Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks, SPC 2006.

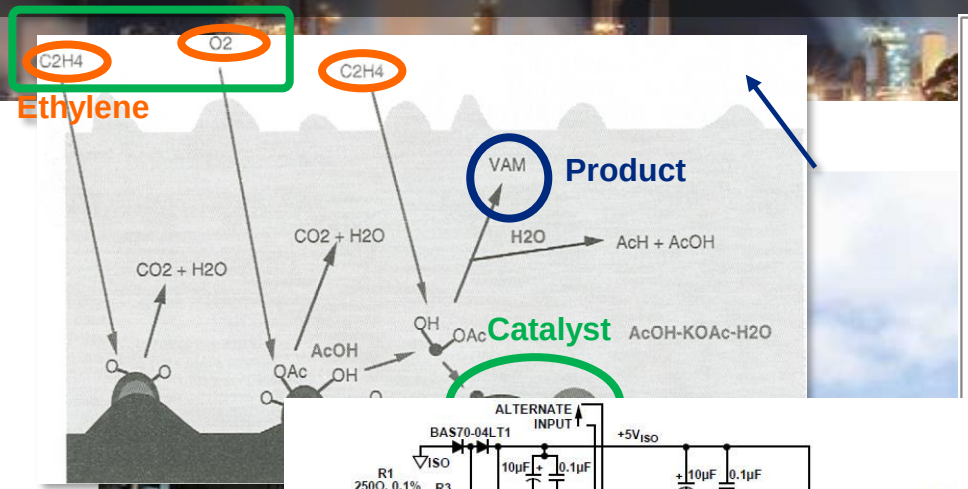
SANS: ICS cyber-kill chain

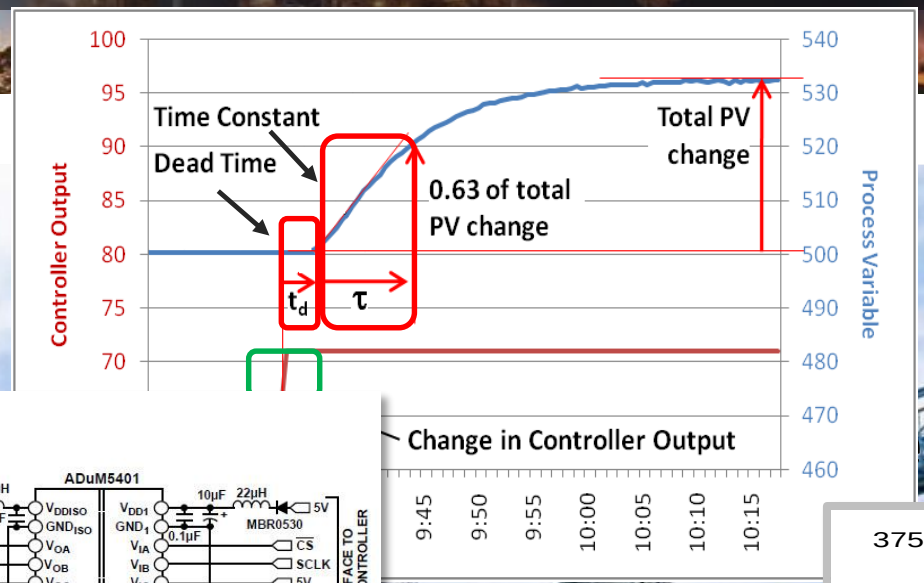


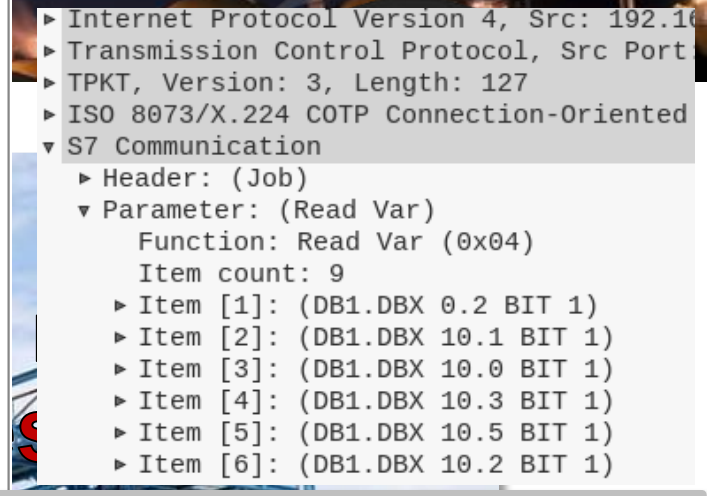
WHAT HAPPENS HERE??

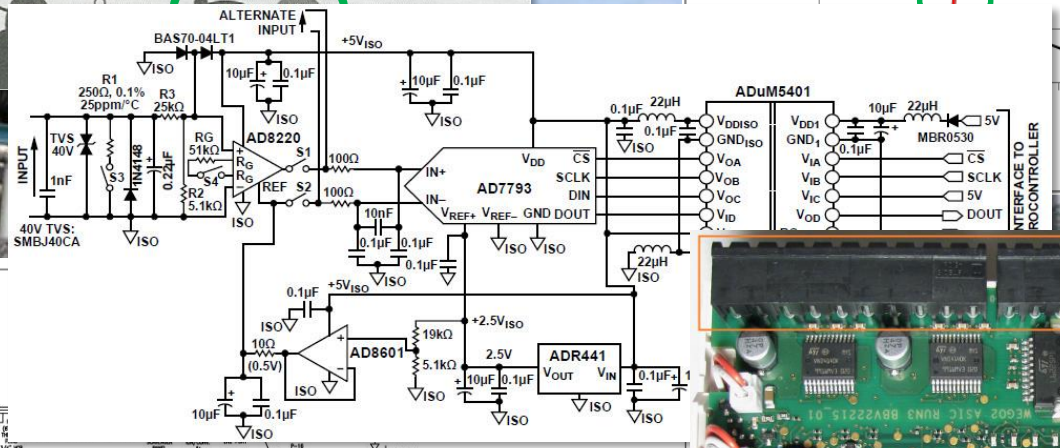
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

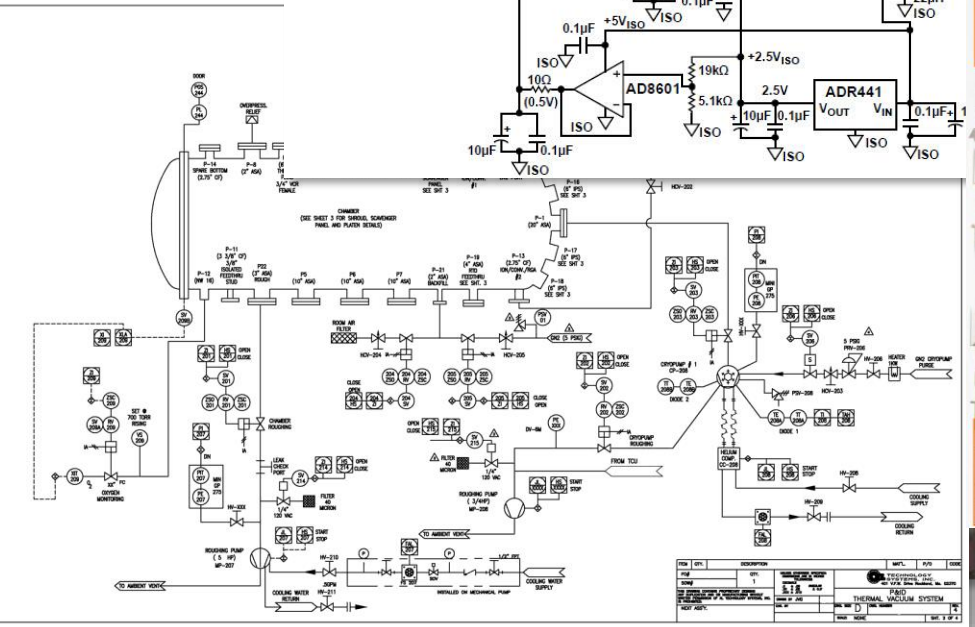
Knoweldge involved into exploit development

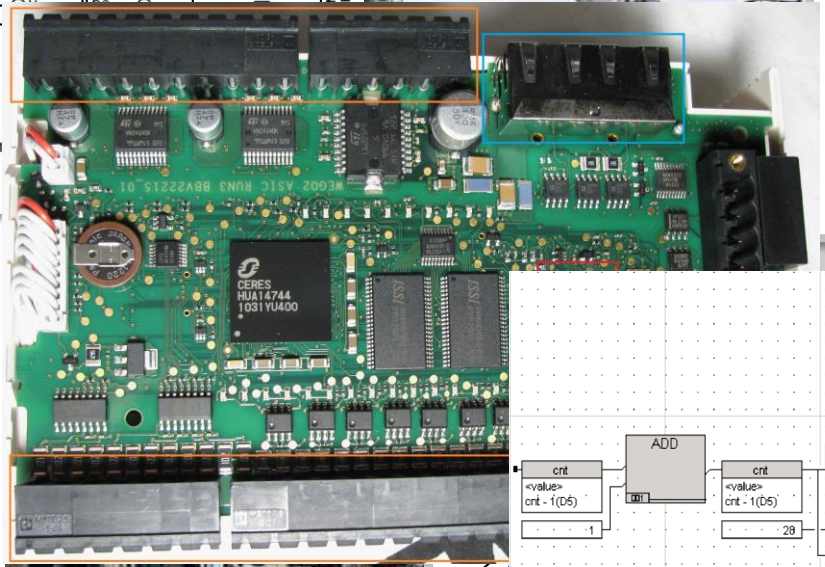


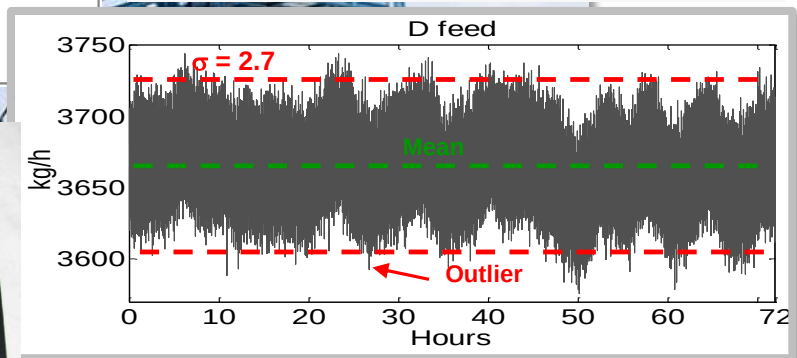


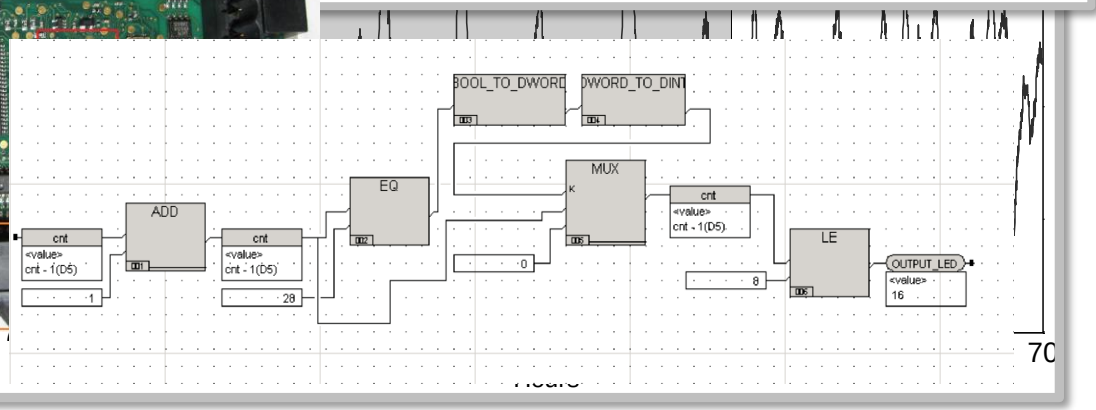




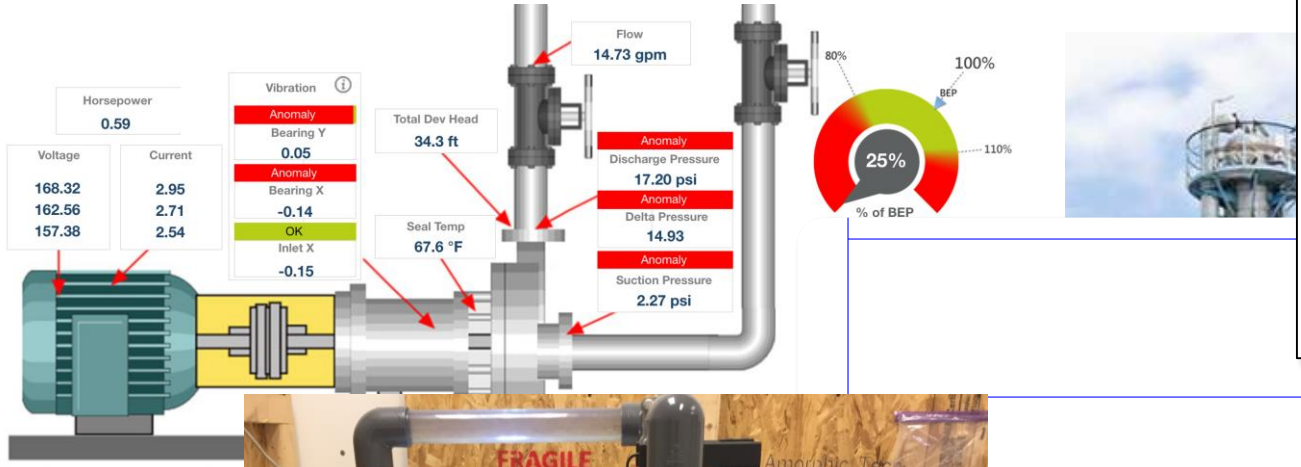






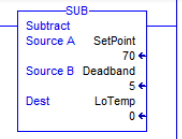


Knoweldge involved into exploit development

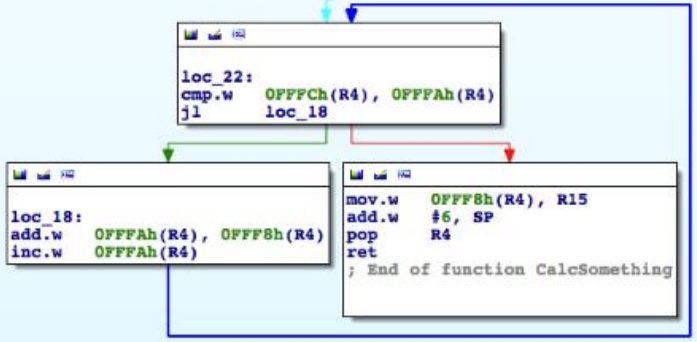


Algorithm 1 Runs Analysis

```
1: procedure EXPLORE                                   ▷ 1: analyse phase
2:     signal ← signal to analyse
3:     while not an end of signal do
4:         while moving up do
5:             runs++                                  ▷ count positives moves
6:             value = sum(changes)                    ▷ positive steps change
7:             if direction change then                ▷ save results
8:                 positivesruns(runs)++
9:                 positivesvalues(runs) = value
10:        while moving down do
11:            runs++                                  ▷ count negatives moves
12:            value = sum(changes)                    ▷ negative steps change
13:            if direction change then                ▷ save results
14:                negativesruns(runs)++
15:                negativesvalues(runs) = value
16:        if no change then
17:            nils++                                  ▷ count nils
18:    return runs, values, nils
```




```
.def CalcSomething
CalcSomething:
push.w   R4
mov.w    SP, R4
incd.w   R4
add.w    #0FFFAh, SP
mov.w    R15, 0FFFCh(R4)
clr.w    0FFF8h(R4)
clr.w    0FFFAh(R4)
jmp      loc_22
```



Algorithm 2 Triangles

```
1: procedure EXPLORE
2:     signal ← signal to analyse
3:     window ← learning window
4:     noiselvl ← noise parameter
5:     step = window ∗ 10
6:     topslope = −999.99
7:     bottomslope = 999.99
8:     while not an end of signal do
9:         if first elements then
10:            current = value
11:            index = 1
12:        while index < window do                     ▷ learning phase of i−th bucket
13:            upperslope = (current − (last + noiselvl))/index
14:            lowerslope = (current − (last − noiselvl))/index
15:            if upperslope > topslope then
16:                topslope = upperslope
17:            if lowerslope < bottomslope then
```

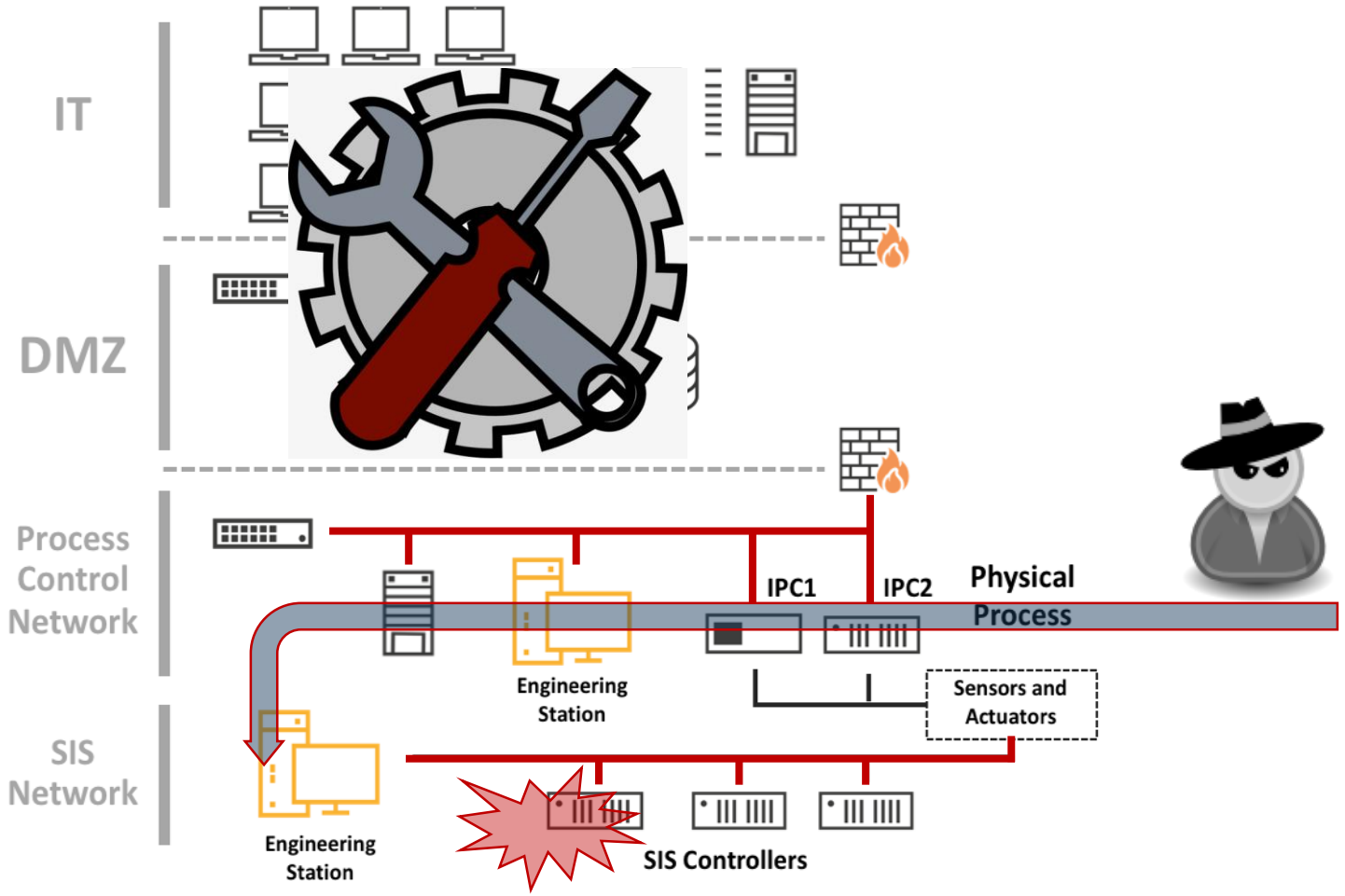
Designing cyber-physical payload

https://bloximages.newyork1.vip.townnews.com/hannapub.com/content/tncms/assets/v3/editorial/e/00/e00b6032-b883-11e9-863f-3f8704327902/5d49dabf0e770.image.jpg

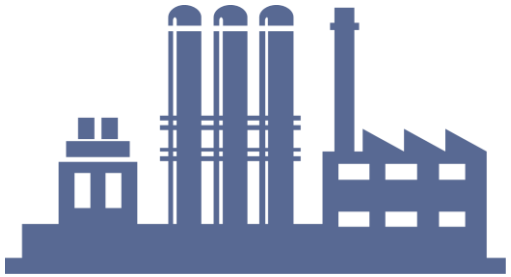
Evil Motivation

Cyber-physical Payload

Intrusion via trusted third-parties



Trusted third-party service providers



Q & A

Marina Krotofil
@marmusha
marmusha@gmail.com