Technische Universiteit
Eindhoven
University of Technology

Where innovation starts

Security from IT to IoT

Sandro Etalle

(Prof. dr.) full professor,
head of the security group at the Technical University of Eindhoven
(faculty of Mathematics and Computer Science)
s.etalle@tue.nl

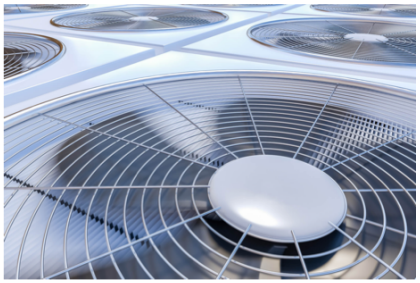
For the sake of transparency:
co-founder and chairman of the board at SecurityMatters

SECURITY MATTERS

IT -> ICS -> Smart Industry -> Smart Cities

IT

Industrial Control Systems

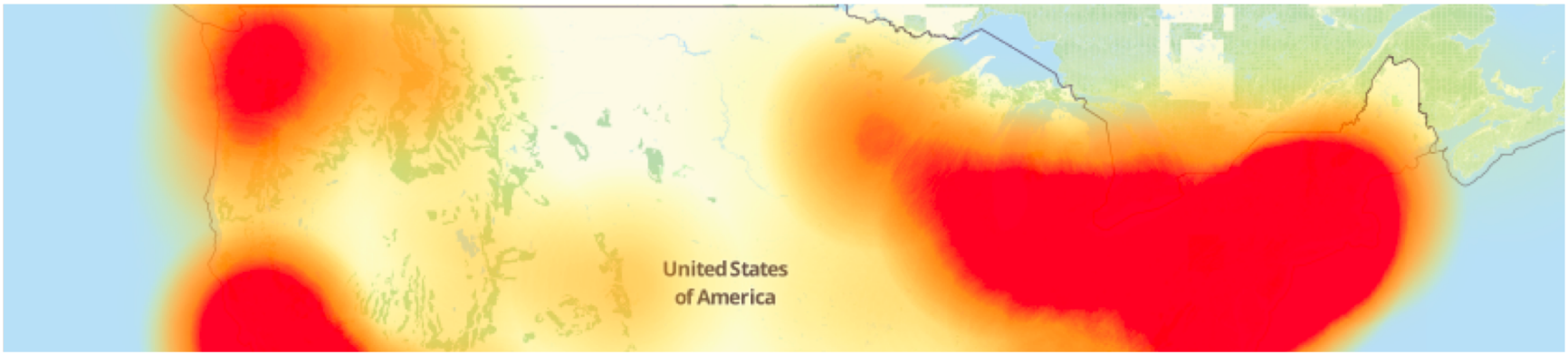


Smart Industry/building

Smart Cities (full IoT)

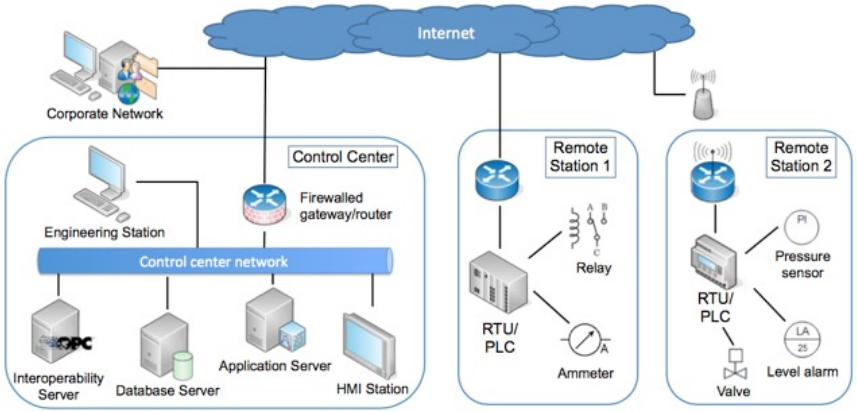
- Differences relevant to security
  - **DIVERSITY**: proprietary systems & protocols
  - **SCALE**
  - **GOVERNANCE**: Central/distributed/outsourced

Do not Panic, but Think Ahead



- **Do not Panic**
  - Not everything that can be attacked will be attacked
  - Attackers have usually better things to do
- **But do worry**
  - IoT botnets are a fact
  - Attackers are finding ways to make money from IoT weaknesses
  - There will be liability issues

The attacker's view pt. 1 (Industrial Control Systems)



See Also: Michael J. Assante and Robert M. Lee, The Industrial Control System Cyber Kill Chain, Report, SANS Institute, 2015

IF you have an appropriate network segmentation THEN

- (If your device is on SHODAN, you have a bigger problem)

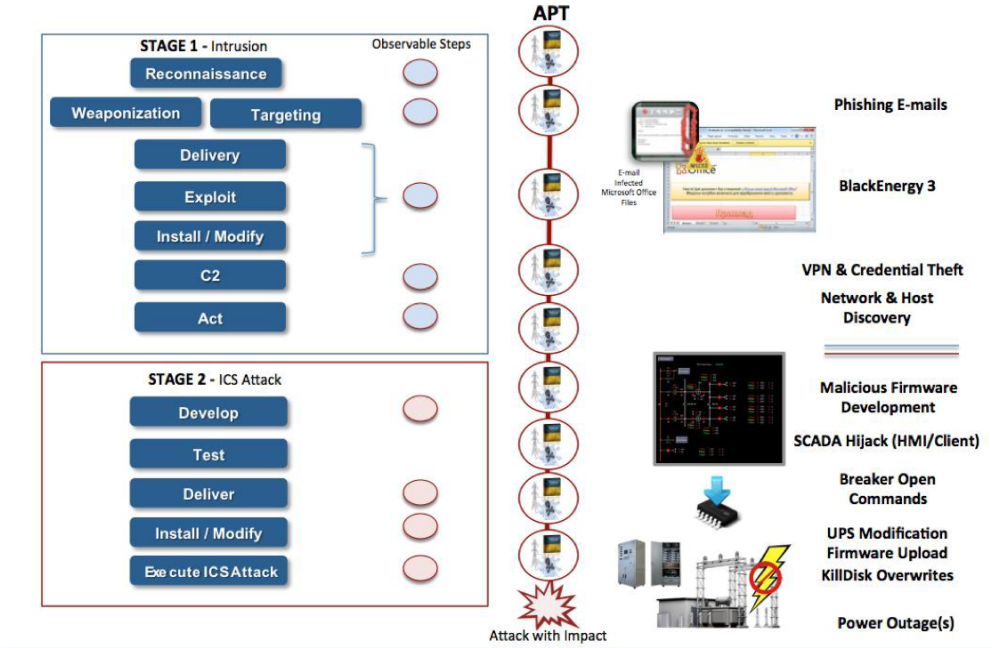
[GOOD] Expensive (but not difficult) for the attacker to get inside

[GOOD] Difficult for the attacker to *make money* (ransomware?)

[BUT] Segmentation is not Segregation

- Lots of people and devices getting in and out, vendors, maintenance, …

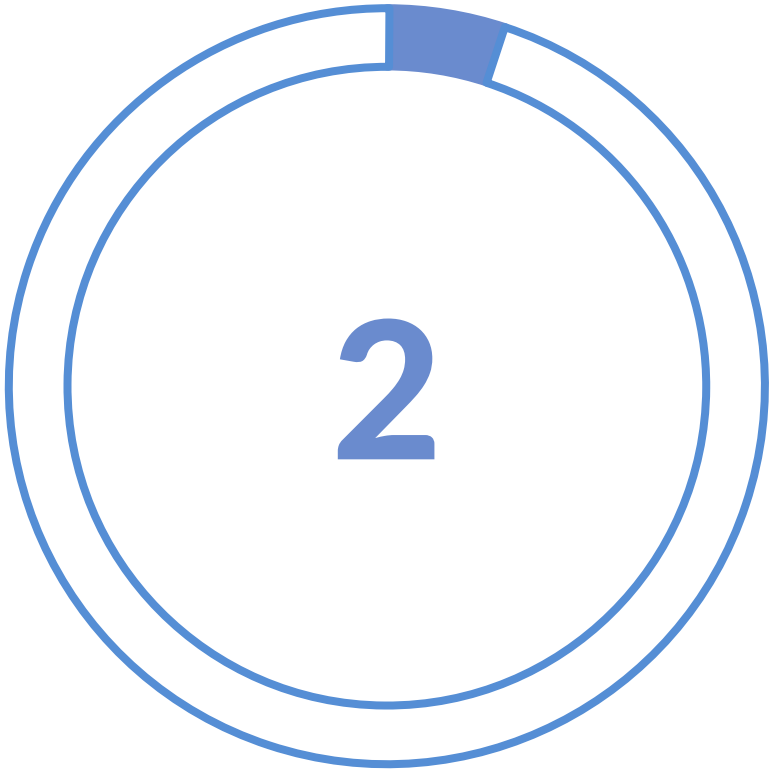
The attacker's view pt. 2 (Industrial Control Systems)



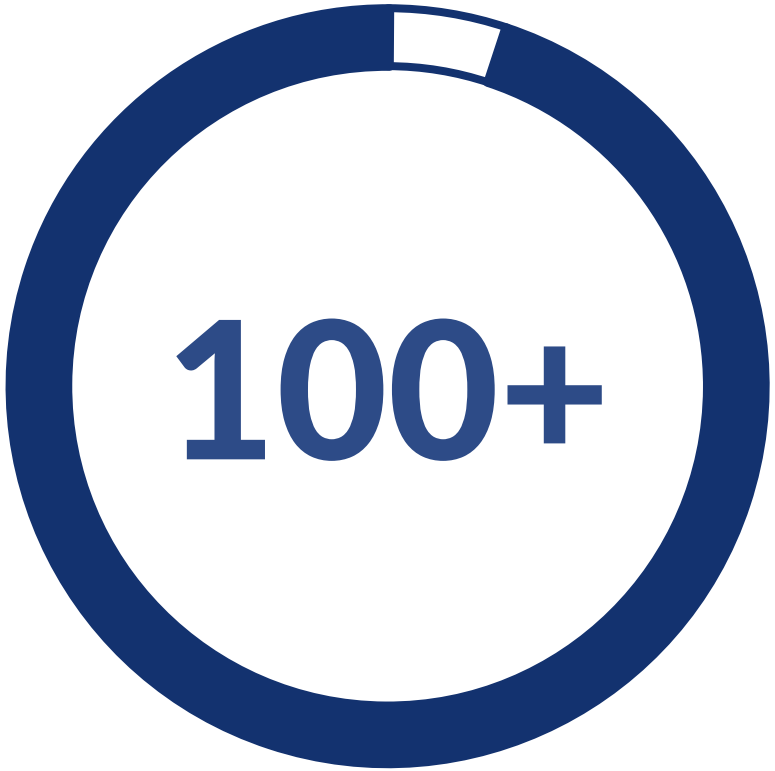
[GOOD] Attacks take time (at least so far). For the reconnaissance
[GOOD] The defender has a window of opportunity
[BAD] IPv6 Standardization of IoT will reduce this window

Security is not the only problem of IoT

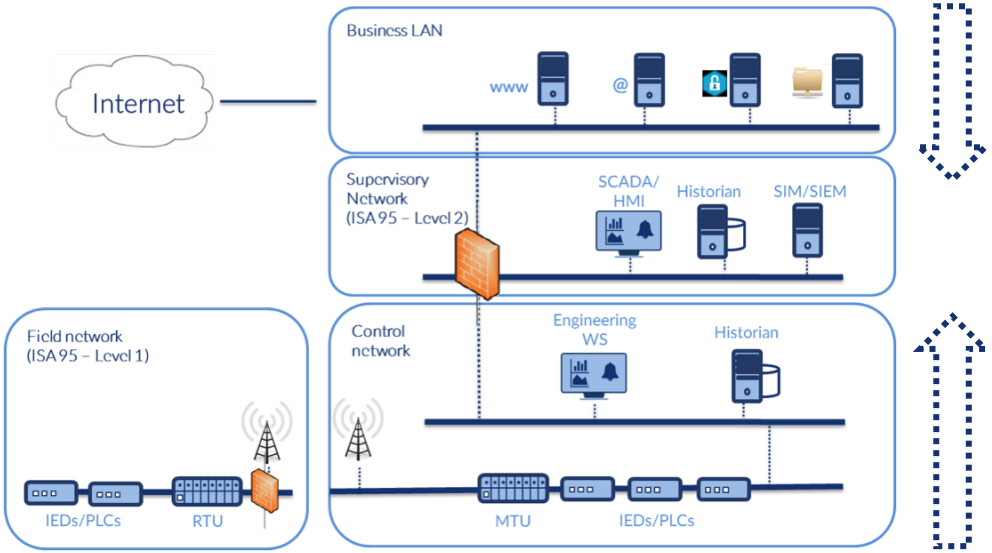
Reported events that can be classified as actual attacks and exploitation attempts



Reported events that could have seriously affected business continuity



Defender still has a few problems pt. 1



Information Technology (IT)

Operational Technology (OT)

DNP3, IEC 101/104 – ICCP - IEC 61850 (MMS, GOOSE, SV)- MODBUS, MODBUS/TCP - OPC DA/AE - EtherNet/IP,

- **[BAD] Standard "out-of-the-box" IT defenses do not work in OT/IoT**
  - Antivirus, WAF, vulnerability advisories
- **In IoT, SECURITY == UNDERSTANDING**
  - IoT Defenses have "running" (ongoing) costs, Someone has to *do* it

Defender still has a few problems pt. 2

- [BAD] The Defender usually has no idea what happens inside
  - Laptops & devices, Network misconfiguration, vendors ”messing around”. Internet-connected maintenance people

Defender still has a few problems pt. 3

- GOVERNANCE & LIABILITIES
- Combination of several vendors with competing goals

Stellingen

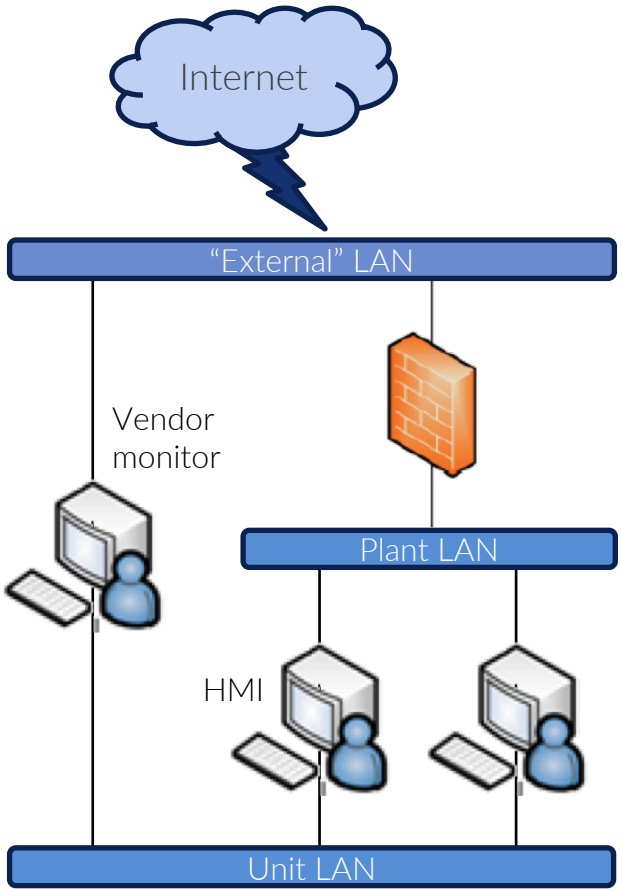
- In IoT, SEGMENTATION IS CRUCIAL
  - Not to block the attacker but to make the attack expensive, and contain mistakes
- In IoT, MONITORING WILL BECOME ROUTINE
  - In IoT, SECURITY == UNDERSTANDING
  - Monitoring would have actually detected: Stuxnet, Ukraine 2015/16, Havex, etc
- EVERY SMART DEVICE HAS A RUNNING “SECURITY” COST
  - IMHO: irresponsible to plan a smart . . . (city/plant/building, whatever) without thinking ahead about who/what is going to take care of its security
- LIABILITIES WILL BECOME AN ISSUE
  - Do not let the vendor/system integrator interfere with your choices

Questions?

Small note for the LinkedIn users who are kindly connecting
please include a note about where we met.

“Insider-outsider” threat
Power generation company

- Maintenance contract with OEM
  - One person on-site
  - Remote connectivity for maintenance/support
  - Plant faced complete turbine shutdowns
  - No warning, no alarm
  - Actions not initiated by operators
  - No equipment failure
- Vendor monitor was not read-only
  - Connection not documented
  - 2 months of investigation
  - Cyber security now a management priority

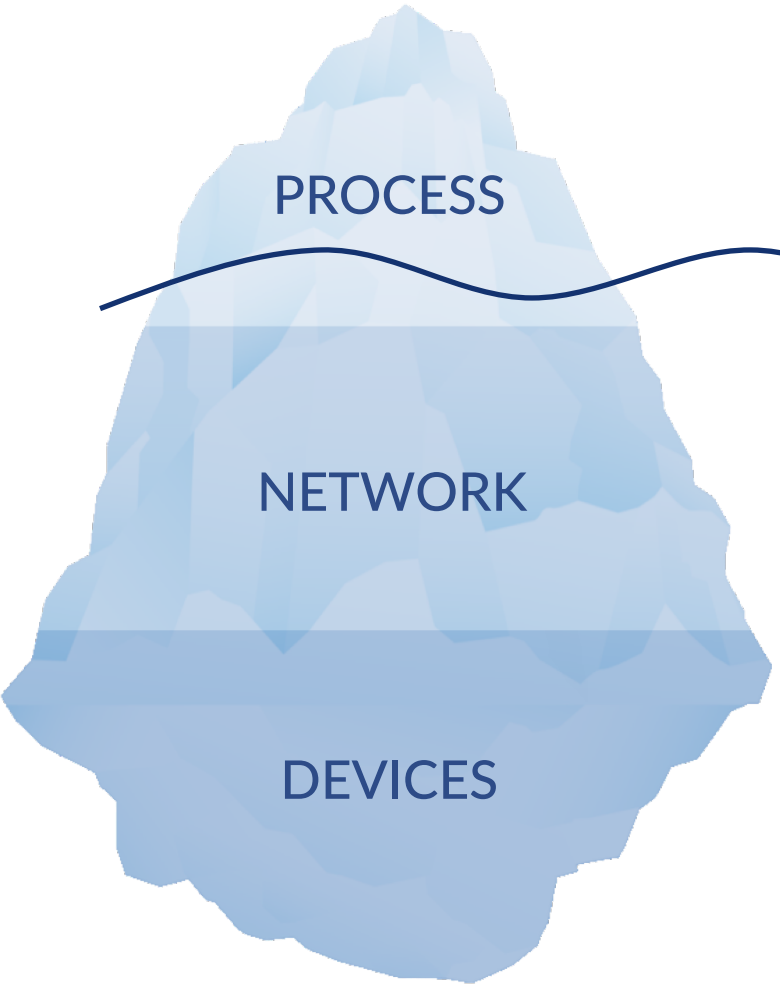


A tiny taxonomy of cyberattackers

- Interesting types
  1. Criminals (Cost < Benefit)
  2. Hacktivists (Cost < fixed limit)
  3. Nation states (no constraints)
  4. Occasional (typically: insiders)

- Not everything hackable will be hacked, see e.g. Where Do All The Attacks Go?, by Florencio and Herley

- Interesting for ICS is #2,3,4 (for the moment)
- When criminals will have found a way to a good ROI in attacking ICS, things will change completely.
  - IMHO: this is not going to happen very soon.
  - ”Ransomware for ICS” is possible but not as lucrative (yet?)



DCS/SCADA

- Standard monitoring systems (e.g. SCADA) show only the tip of the iceberg
- Missing most of what can affect business continuity
  - Laptops & devices
  - Network misconfiguration
  - Vendors ”messing around”
  - Internet-connected maintenance people
  - …
-