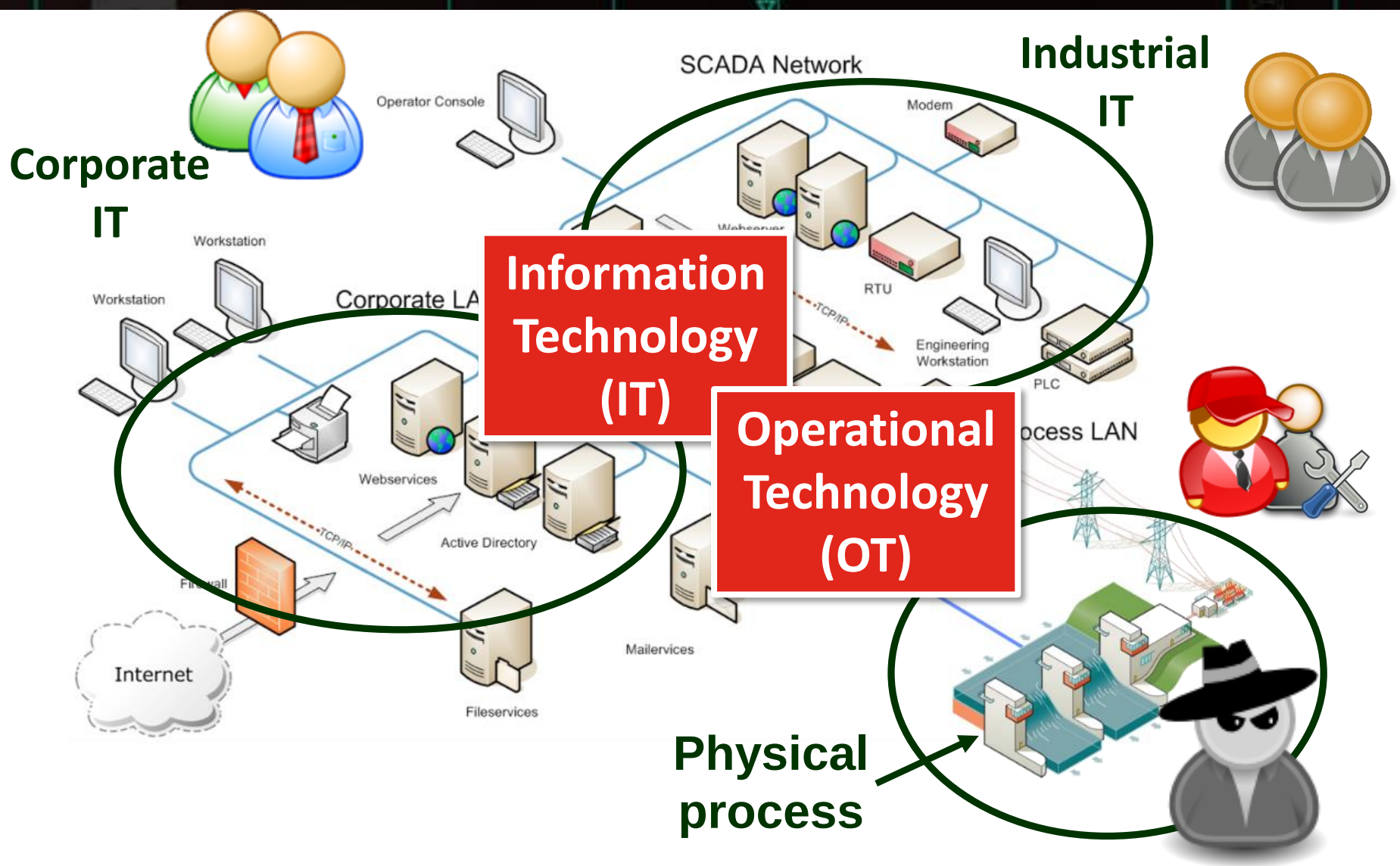
Deep Dive: Likely, Real and Unlikely Cyber-Physical Threats to ICS

Marina Krotofil

St. Petersburg
September 27-29, 2017

Just one of those opinionated opinions :-)

Industrial Control Systems



IT security vs. OT security

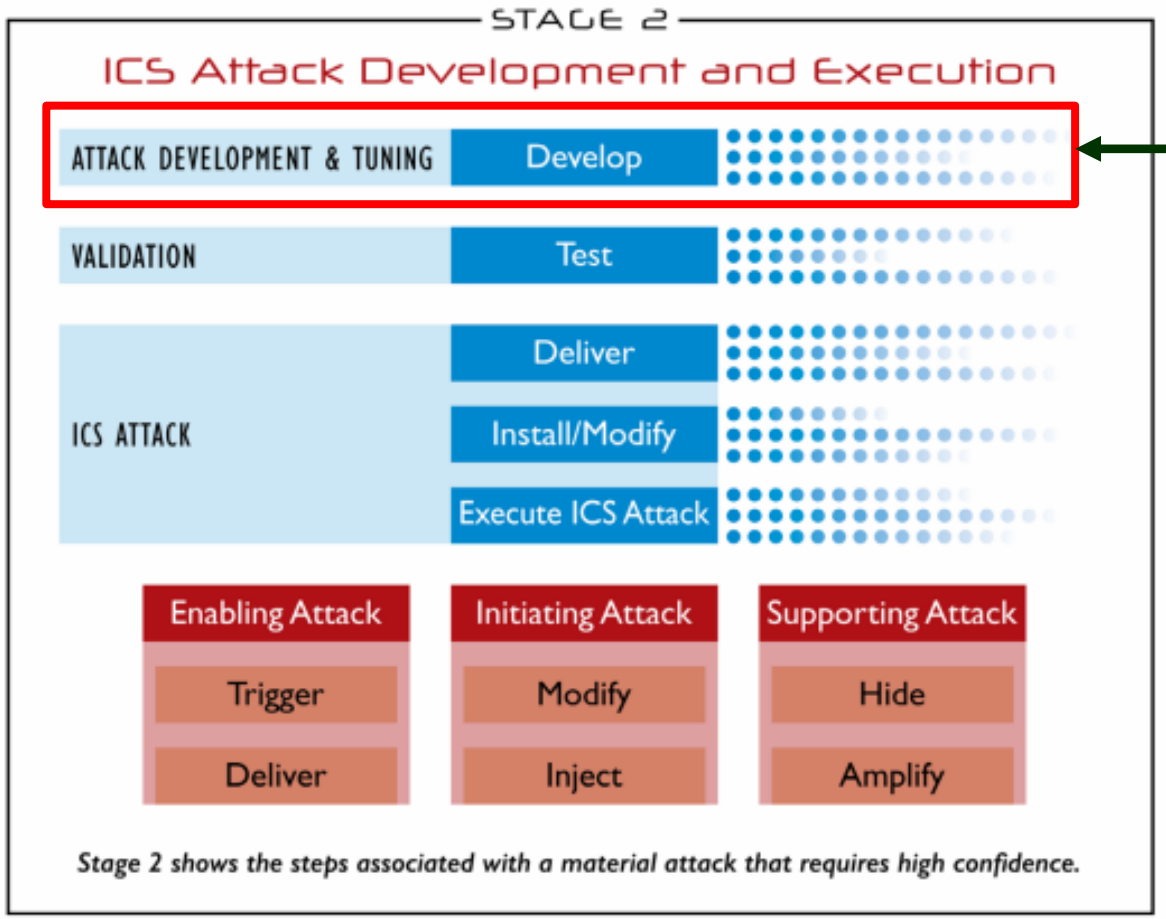
ICS security

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

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

Focus of the talk

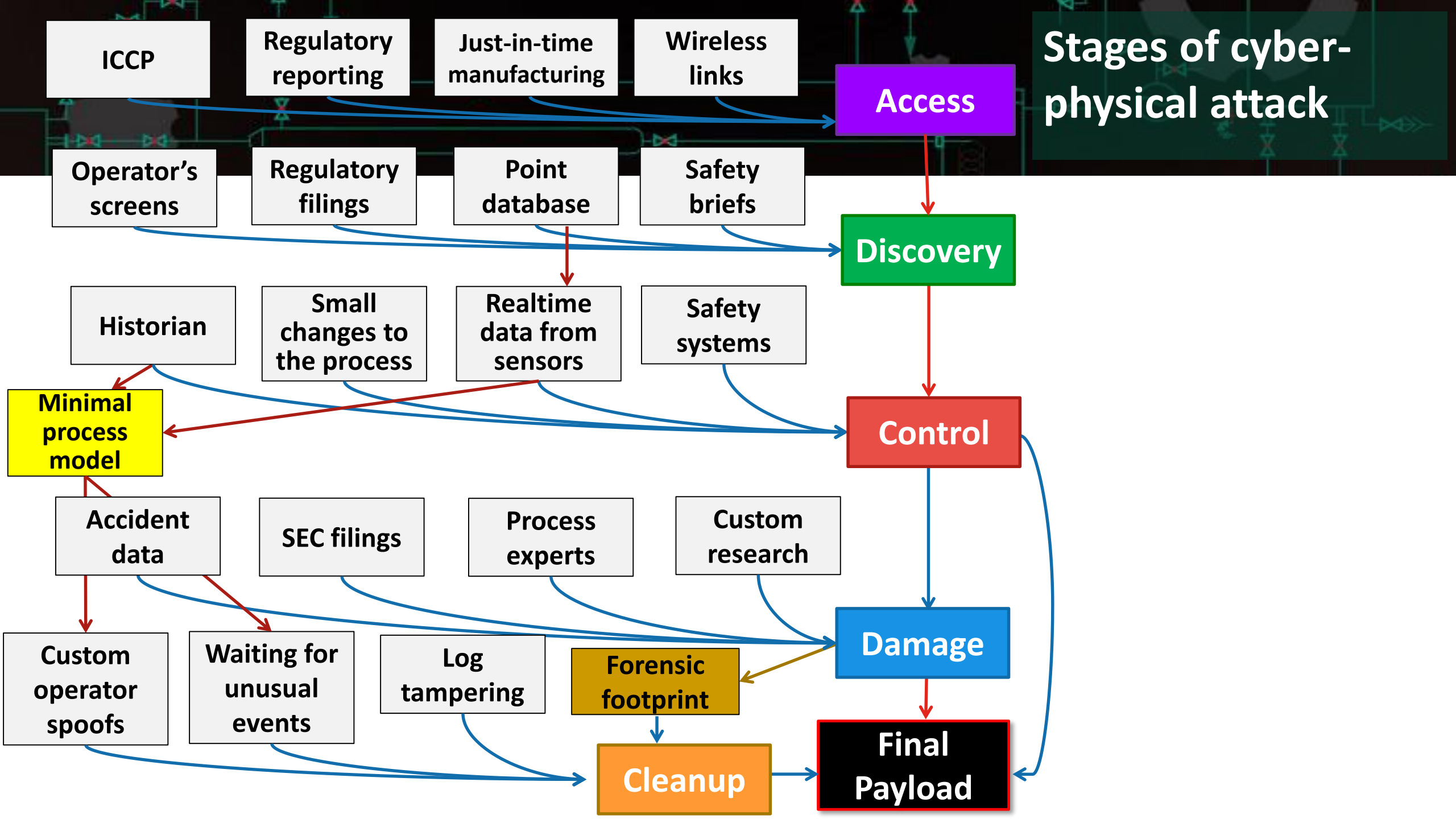
Attack Development stage in ICS kill chain



How?

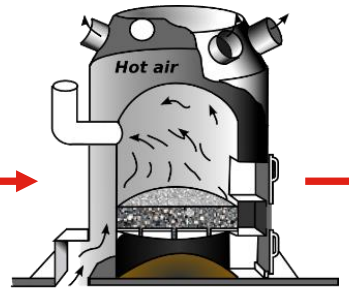
M. Assante, R. Lee. The Industrial Control System Cyber Kill Chain. SANS, 2015.

Stages of cyber-physical attack



Let’s dive into some specifics

In control world it is all about control loops



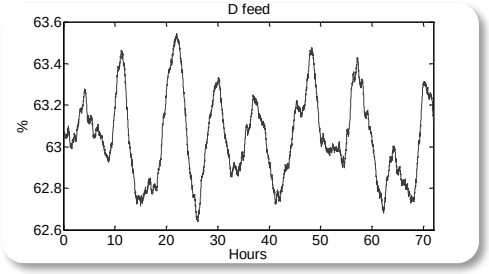
Physical process

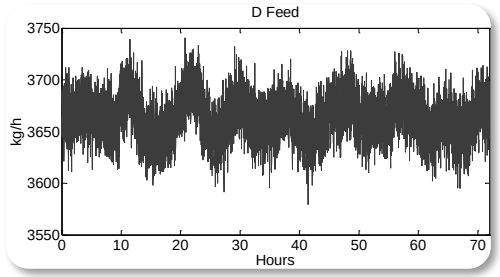
Actuators

Sensors

Setpoint

Control system





Cyber-Physical Attack

1

Cyber-Physical attack

2

3

Manipulate the process

Capture process feedback

Prevent response

Direct

Indirect

Direct

Estimated or Derived

Operators

Control system (including safety)

Set point change; manipulation of actuators

Deceiving controller/ operator about process state

Direct observation of process values

From existing measurements or calculations

Blind

Mislead

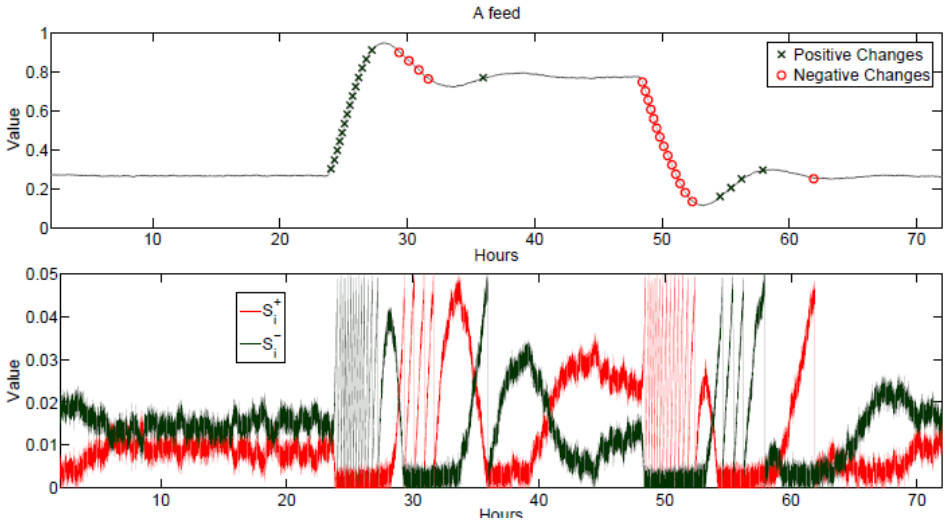
Modify operational/safety limits

Why feedback loop is so important?

- **In most scenarios involving process manipulation, attacker needs a feedback mechanism to know how well she is doing**
  - Is attack succeeding/ failing?
- **Attack effect propagation**
  - To monitor the extent of attack effect propagation
  - To monitor state in the neighboring systems
- **To calculate Time-to-Damage to plan for concealing activities**
  - When is the time to return control back to control system

Plant designs are attacker ufriendly

- So far I haven't ever worked with a scenario when feedback mechanism was easily or at all obtainable
- Typically values needed for attack are not measured
  - No readily available control methods exist
  - Multiple strategies to obtain feedback (but none is easy)



Mostly involves "non-glamorous" sensor data processing

Parameterization of cyber-physical attack

J. Larsen. Physical Damage 101: Bread and Butter Attacks. Black Hat USA, 2015.

- Vacuum collapse – Implosion attack
- "Generic" type of attacks – works across multiple industries
- The final payload still needs to be parameterized on facility-to-facility basis
- **This demo: 11 destroyed barrels**
- **$$$ in costs of equipment and man hours**

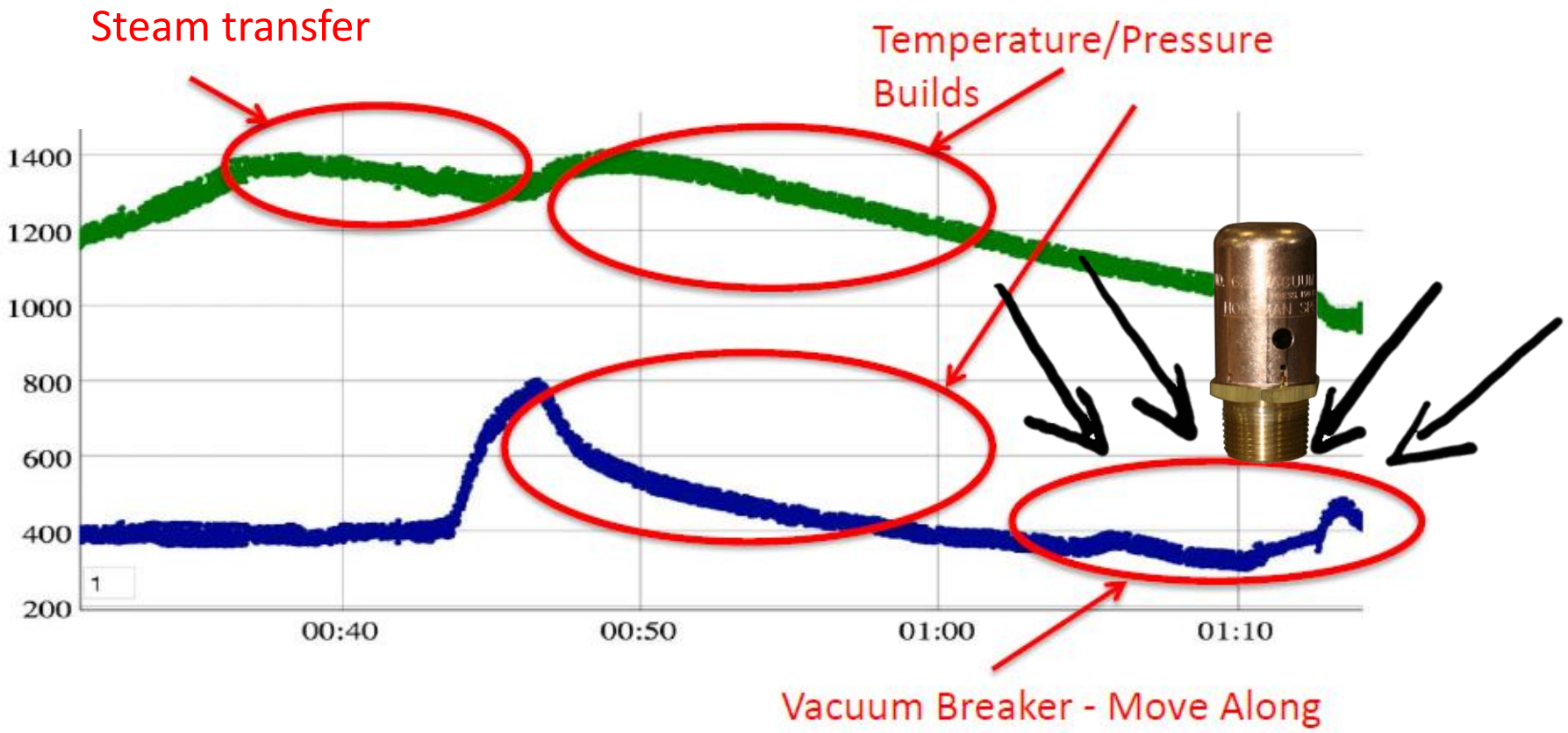
How to measure SUCCESS of implosion attack?

http://www.stgeorgeutah.com/news/archive/2013/12/17/jek-washington-countys-main-water-pipeline-collapses-district-urges-wise-water-use

http://www.folsomtelegraph.com/article/water-supply-folsom-restored

There is no sensor measuring “roundness” of the pipe

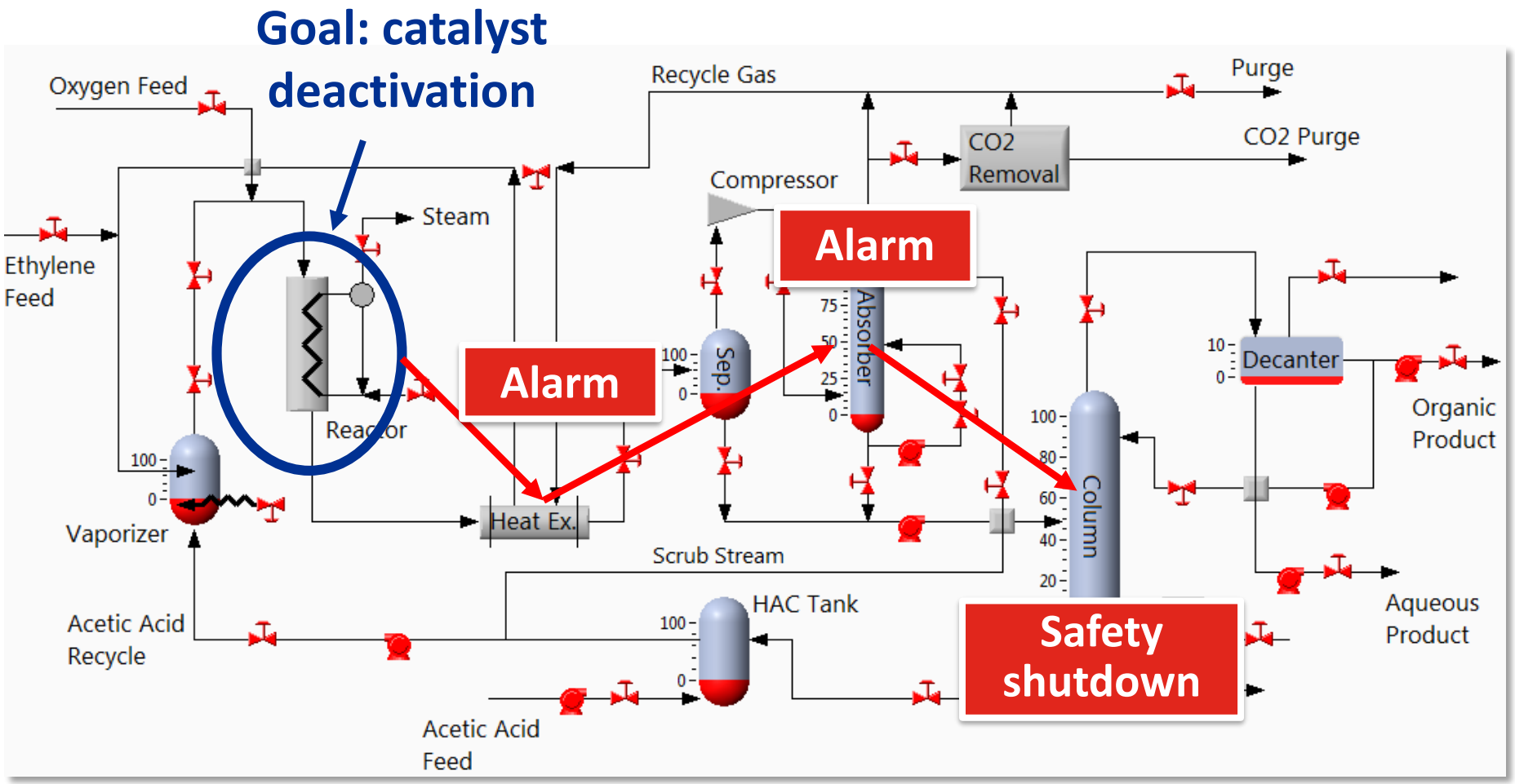
How to measure FAILURE of implosion attack?



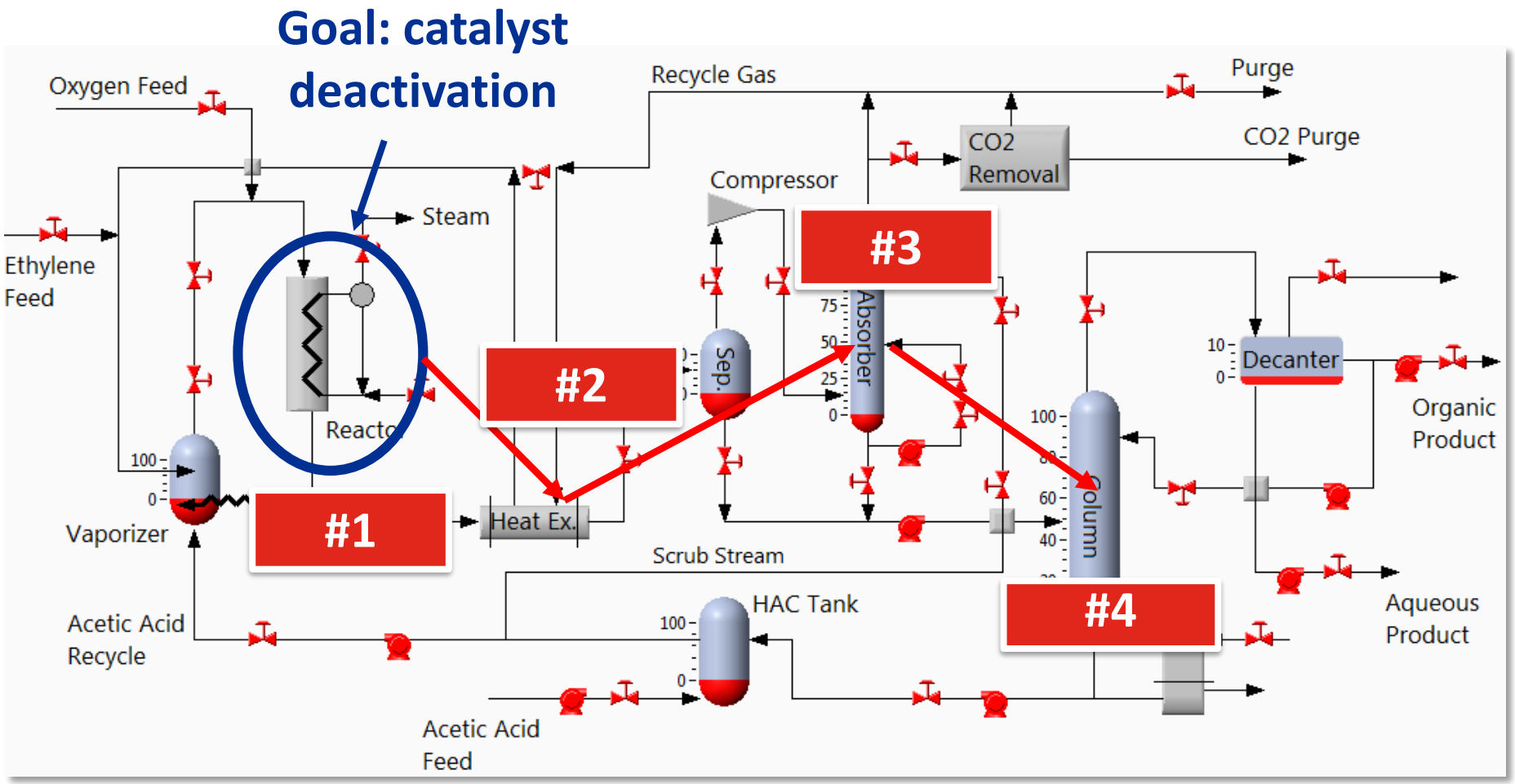
Stuff typically not on the diagrams

J. Larsen. Hacking Critical Infrastructure like You are not a n00b. RSA, 2016.

Alarm and physics propagation



Number of needed implants



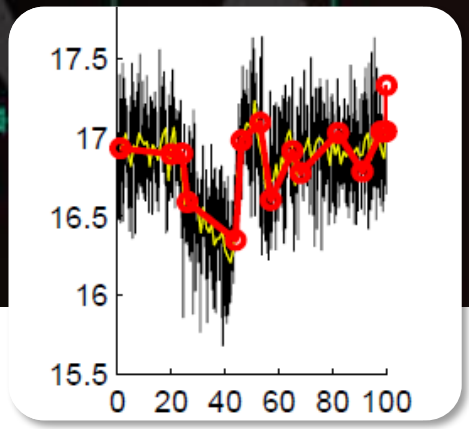
Growing complexities and uncertainties

- An exploit can be always built, but
  - What will be the cost of final effort?
  - What is total cumulative uncertainty?

	Start Conditions	Learning	Control	Spoof	Success Feedback	Failure Check	Control Out	Spoof Out
lvlAlcohol				95	95			
lvlCatch				85				
tmpCatch								
tmpIgnitor				81				
optPlateStrikePos				82				
pmpFountainOn			82					
pmpFountainSpeed			95	95		95		
ignitorOn						90		
setpntPssFountain			91	91		91		
						Total Uncertainty	1168	
						Number of Implants	2	
						Total	2336	

J. Larsen. Hacking Critical Infrastructure like You are not a n00b. RSA, 2016.

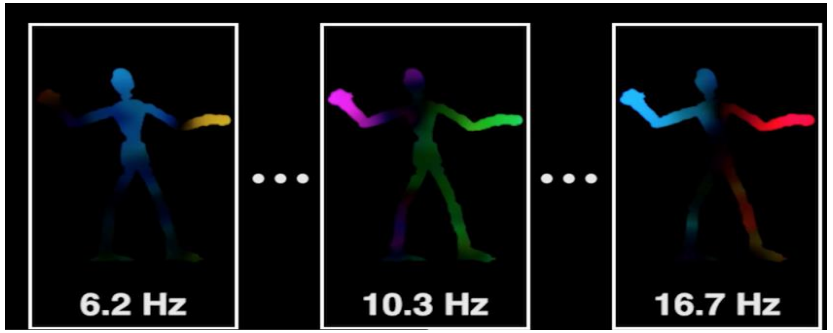
Reverse Engineering Physical Processes: MK



Black Hat'15: We should probably automate this process

- A. Winnicki, M. Krotofil, D. Gollmann. **Reverse Engineering Physical Processes in Industrial Control Systems.** In proceedings of 3rd ACM Cyber-Physical System Security Workshop, 2017.
- Standard approaches from control engineering worked, but did not serve well our needs
- 9 months of work (tons of testing)
- **Eventually we developed a customized approach based on few standard and home brewed algorithms**

Reverse Engineering Physical Processes: JL



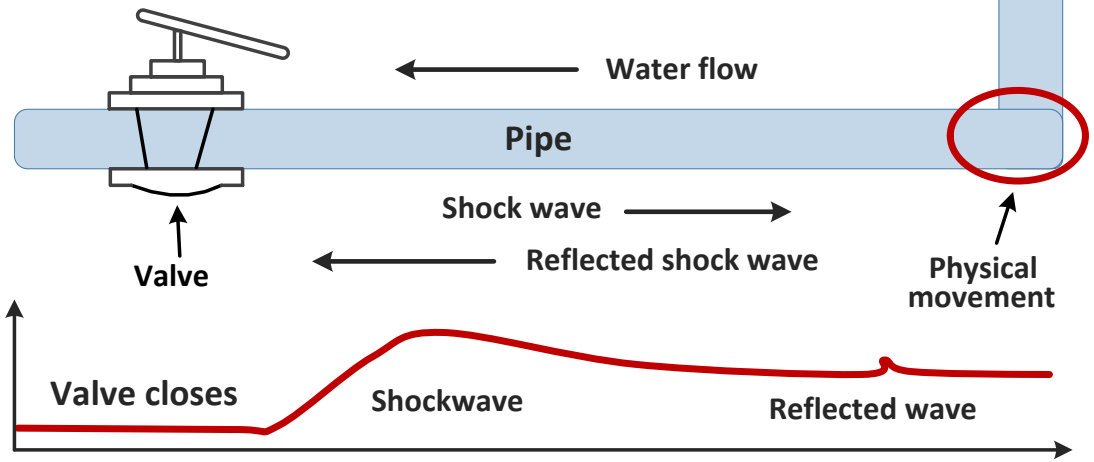
- Abe Davis -> automatic generation of physical models using modes (common frequencies)
- JL tested the approach to building process models
- **Challenge #1: Process data is not as rich as image data**
- **Challenge #2: Not suitable for processes with frequent changes of states (on/off)**
  - E.g. water treatment

J. Larsen. Automatic Generation of Attack Models.S4, 2016.

Let’s make some predictions

Near future unlikely mass-scale attacks

- **Complex cyber-physical attacks**
  - Of high engineering precision
  - Requiring high coordination
  - Requiring considerable time and effort

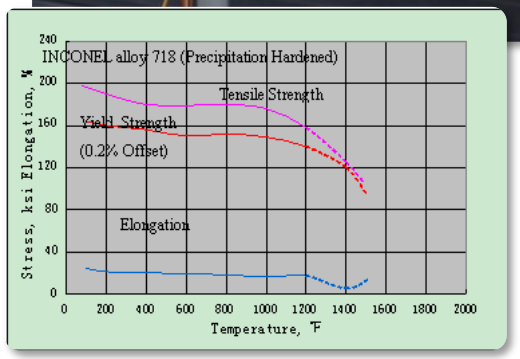


- **Attacks which take unknown/extended time to cause needed impact**
  - Killing catalyst vs. disconnecting circuit breakers
- **In general all attacks which require feedback loop**
- Attacks with unclear collateral damage (?)

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

Near future realistic threats (1)

- **Attacks with instantaneous/clear impact**
  - Design deviation attacks (“Out-of-Spec” attacks), e.g. in additive manufacturing
  - Equipment shut off, e.g. in power distribution industry



http://www.prototypetoday.com/3d-printed-news
http://keywordsuggest.org/gallery/145628.html

Near future realistic threats (2)

- **Attacks which do not require extensive/<u>custom</u> OT comprehension** (physical process, failure conditions, control strategies, alarms, etc.)
  - More of cyber-oriented attacks; attacks executed over HMI
  - “Easy Button” attacks

Code	Name	Logic address	Access	Type
TDC1	IDC injection time	16#28A2 = 10402	R/W	UINT (Unsigned16)
JOG	Jog assignment	16#2B66 = 11110	R/WS	WORD (Enumeration)
PS4	4 preset speeds	16#2C8A = 11402	R/WS	WORD (Enumeration)
PS8	8 preset speeds	16#2C8B = 11403	R/WS	WORD (Enumeration)
SP8	Preset speed 8	16#2C98 = 11416	R/W	UINT (Unsigned16)
JPF	Skip frequency	16#2C25 = 11301	R/W	UINT (Unsigned16)
PIF	PID : PI function feedback assignment	16#2E7D = 11901	R/WS	WORD (Enumeration)

Near future realistic threats (3)

- **OT attacks which parameters can be "calculated" or reliable estimated**, e.g. cavitation in pumps
  - Cavitation conditions can be calculated
  - One never exactly knows the intensity of cavitation (but can try to maximize it)

Pump impeller inspection at Palisades nuclear power plant

http://steamshovel2002.blogspot.com/2014/05/palisades-pcp-impeller-inspection.html

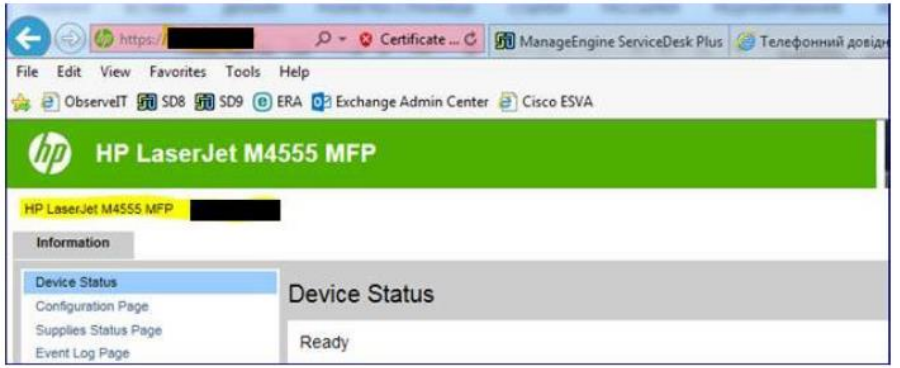
Will terrorist be able to do it?

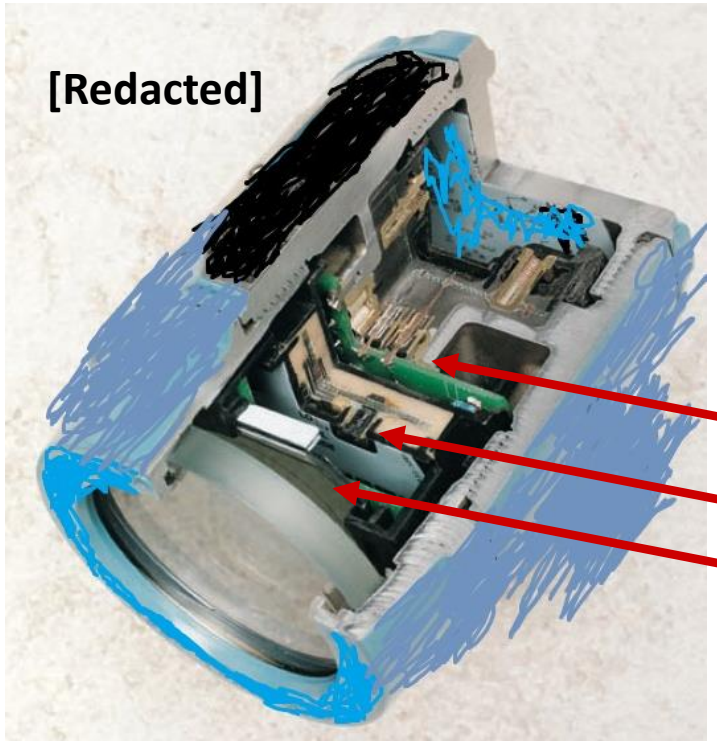
- It takes just a small leak and a drone to cause ignition

Near future realistic threats (4)

	End Time	Name	Attacker Address	Target Address
	Thursday, February 23, 2017 8:57...	[redacted]	[redacted]	69.172.201.153
	Thursday, February 23, 2017 8:56...	[redacted]	[redacted]	69.172.201.153

- **Supply-chain attacks**
  - Allows to bypass multiple levels of security
  - Better scaling of attack efforts





Layers of standardized electronics (for a given vendor)

Real threats and attacker capabilities (1)

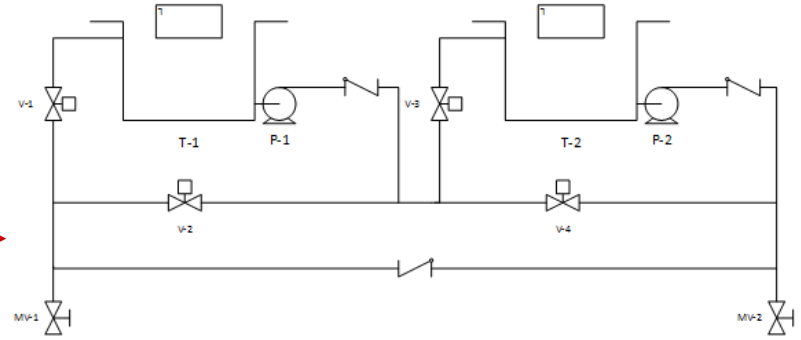
- Massive espionage (stale news)
  - Increasing number of targeted process-related information espionage
- Non-ICS specific attacks
  - Ransomware, KillDisk, etc.
- Cyber-oriented attacks
  - Attacks executed over HMI; tools for targeted protocol and control equipment manipulation
  - **Recently, tools were left behind by the adversary**

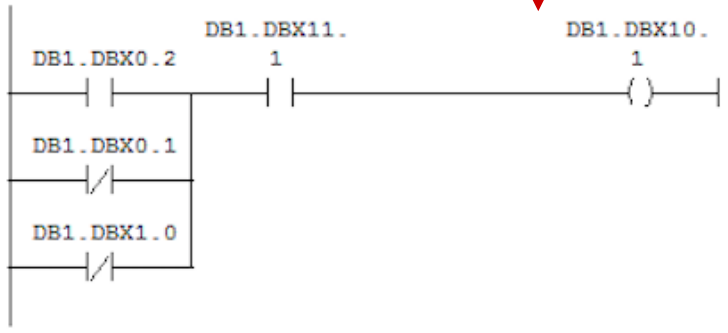
Real threats and attacker capabilities (2)

❑ Automation of control infrastructure reconnaissance

- Most known example being usage of OPC

```
▸ Internet Protocol Version 4, Src: 192.16
▸ Transmission Control Protocol, Src Port:
▸ TPKT, Version: 3, Length: 127
▸ ISO 8073/X.224 COTP Connection-Oriented
▾ S7 Communication
  ▸ Header: (Job)
  ▾ Parameter: (Read Var)
      Function: Read Var (0x04)
      Item count: 9
    ▸ Item [1]: (DB1.DBX 0.2 BIT 1)
    ▸ Item [2]: (DB1.DBX 10.1 BIT 1)
    ▸ Item [3]: (DB1.DBX 10.0 BIT 1)
    ▸ Item [4]: (DB1.DBX 10.3 BIT 1)
    ▸ Item [5]: (DB1.DBX 10.5 BIT 1)
    ▸ Item [6]: (DB1.DBX 10.2 BIT 1)
```





Most critical piece of info

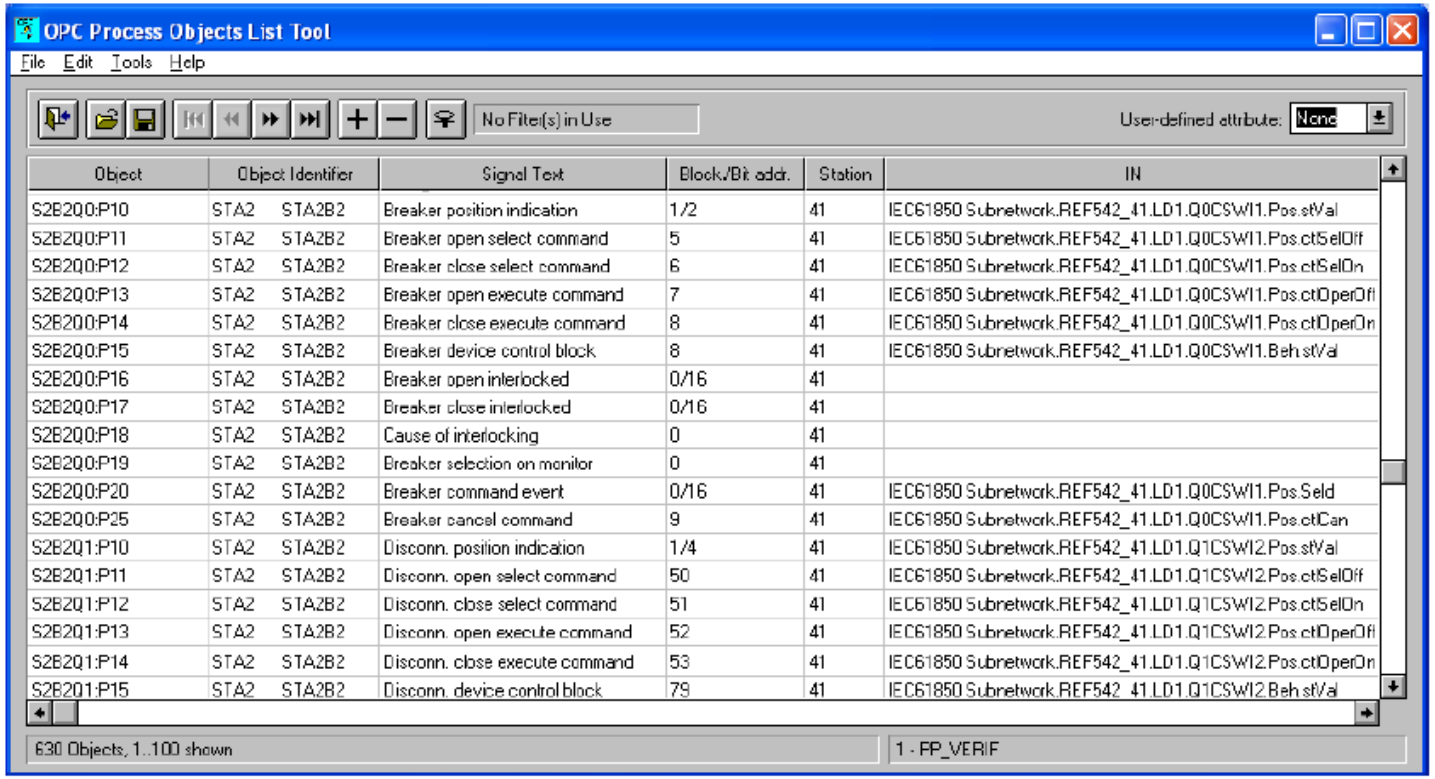
Name	Connection	Data type	Address
Auto Mode HMI On/Off	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 0.1
Manual Mode On/Off	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 0.2
Pump 1 Manual On/Off	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 13.2
Pump 1 State	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 10.2
Pump 2 Manual On/Off	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 13.5
Pump 2 State	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 10.5
Valve 1 Manual Open/Closed	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 13.0
Valve 1 State	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 10.0
Valve 2 Manual Open/Closed_0	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 13.1
Valve 2 State	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 10.1
Valve 3 Manual Open/Closed_1	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 13.3
Valve 3 State	Field Site 3 PLC (ET200S)	Bool	DB 1 DBX 10.3

B. Green, M. Krotofil, A. Abbasi. **On the Significance of Process Comprehension for Conducting Targeted ICSS Attacks.** In proceedings of 3rd ACM Workshop on Cyber-Physical Systems Security & Privacy, 2017.

Real threats and attacker capabilities (2)

❑ Automation of control infrastructure reconnaissance

- Most well-known example being usage of OPC



- ❑ Havex (2012-2014)
- ❑ Ukr power grid attack (2016)

https://library.e.abb.com/public/2218181b3098dd37c1257ab800417a8d/SYS600_External%20OPC%20Data%20Access%20Client_756647_ENb.pdf

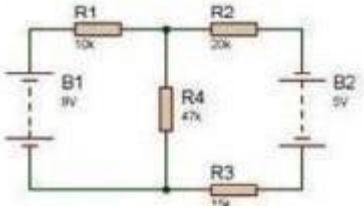
Real threats and attacker capabilities (3)

- **Easily accessible facilities serve as training platforms**
  - Provide access to equipment and protocols
  - Provide real-world level of complexity
  - Allows to study human behaviors and reactions

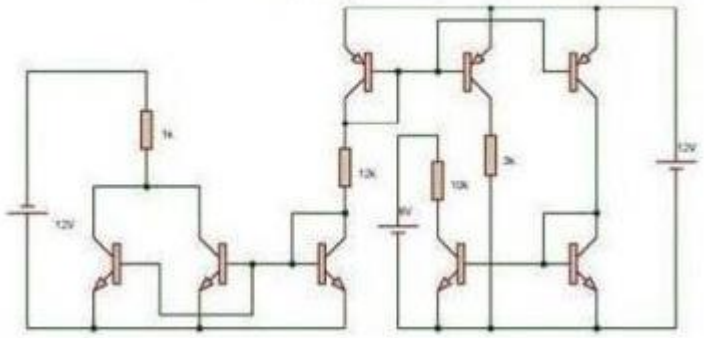
Engineering

Class:

Homework:



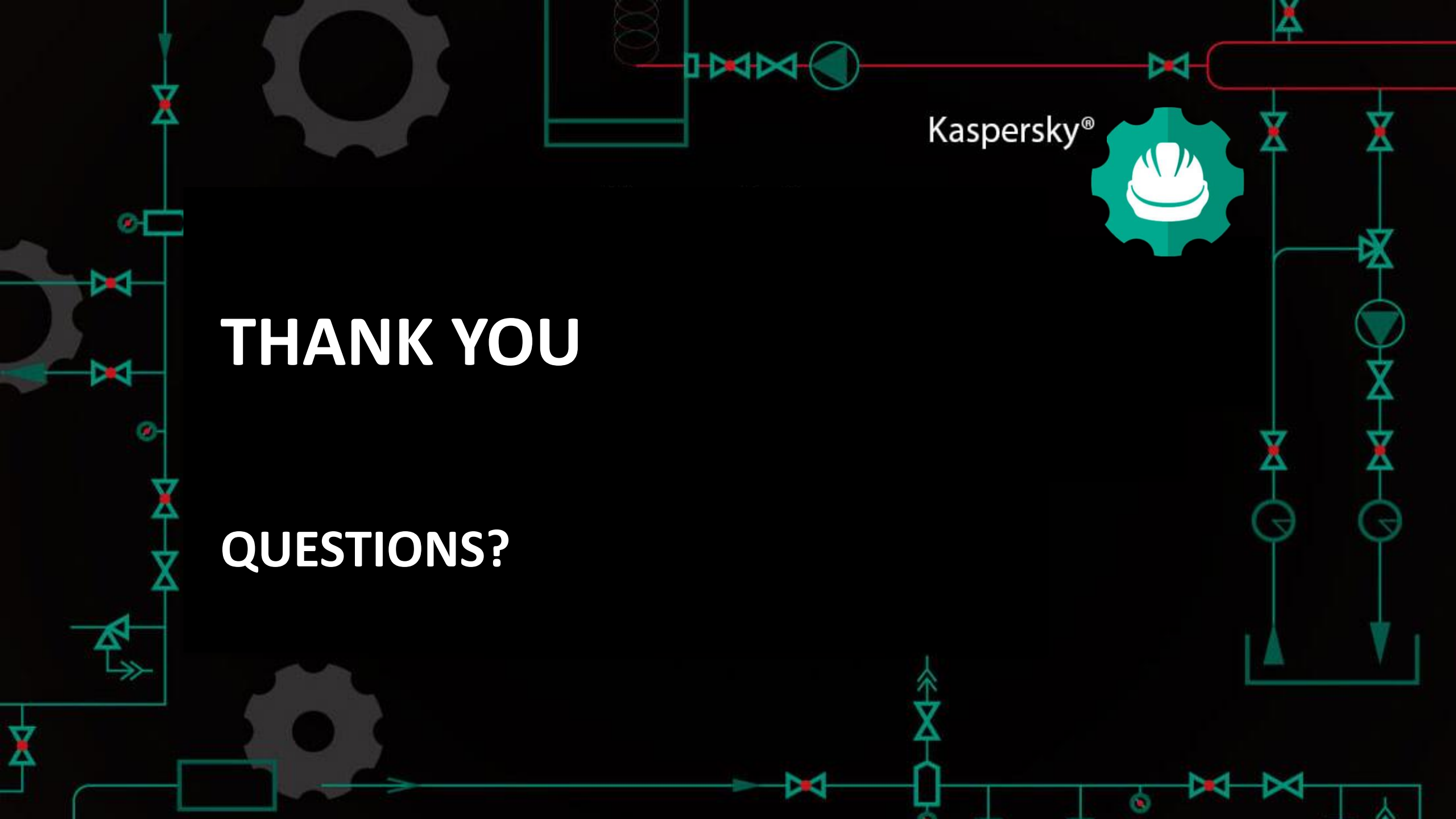
Exam:



Conclusions

- **Cyber-physical attacks becoming new normal**
  - None of recent power grid hacks was publicly disaproved by any government
  - At the same time owners of industrial infrastructures still struggling to believe in security threats

- **Attack tools getting more advanced and wide-spread**
  - Open-source tools
  - Tools found in wild
  - Tools for purchase
- **Distinction between governmental and criminal threat actors is fading**
  - “Trading” and “business” relationships



THANK YOU

QUESTIONS?