SECURENOK®

CYBERSECURITY FOR INDUSTRIAL CONTROL SYSTEMS

Securing Oil&Gas Installations from Cyberattacks in the Digital Age

Rune Halvorsen

June, 2019

SECURENOK

Cyber Security Threats to Society

2018: NSM NorCERT receives 20.000 cybersecurity incident alarms

Some are Major

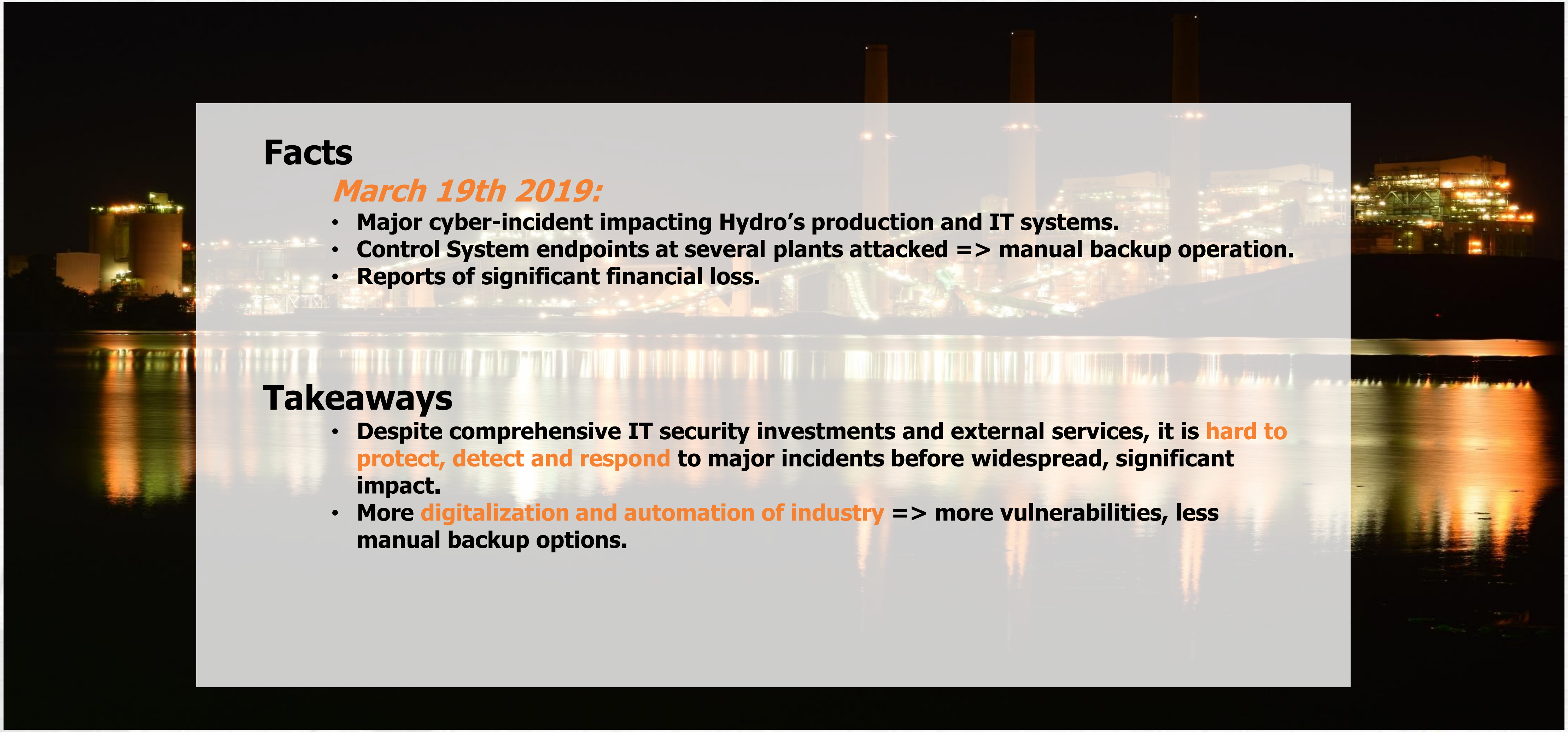
> ***Digital intrusions or other unwanted activity towards organizations operating critical infrastructure or other functions important to society.***

Cyber Threats to Industrial Systems

The **most serious** incidents are **increasing** in scale and complexity.

Trend reported by NSM.

Hydro
- Ransomware attack on IT and OT systems



Facts

March 19th 2019:

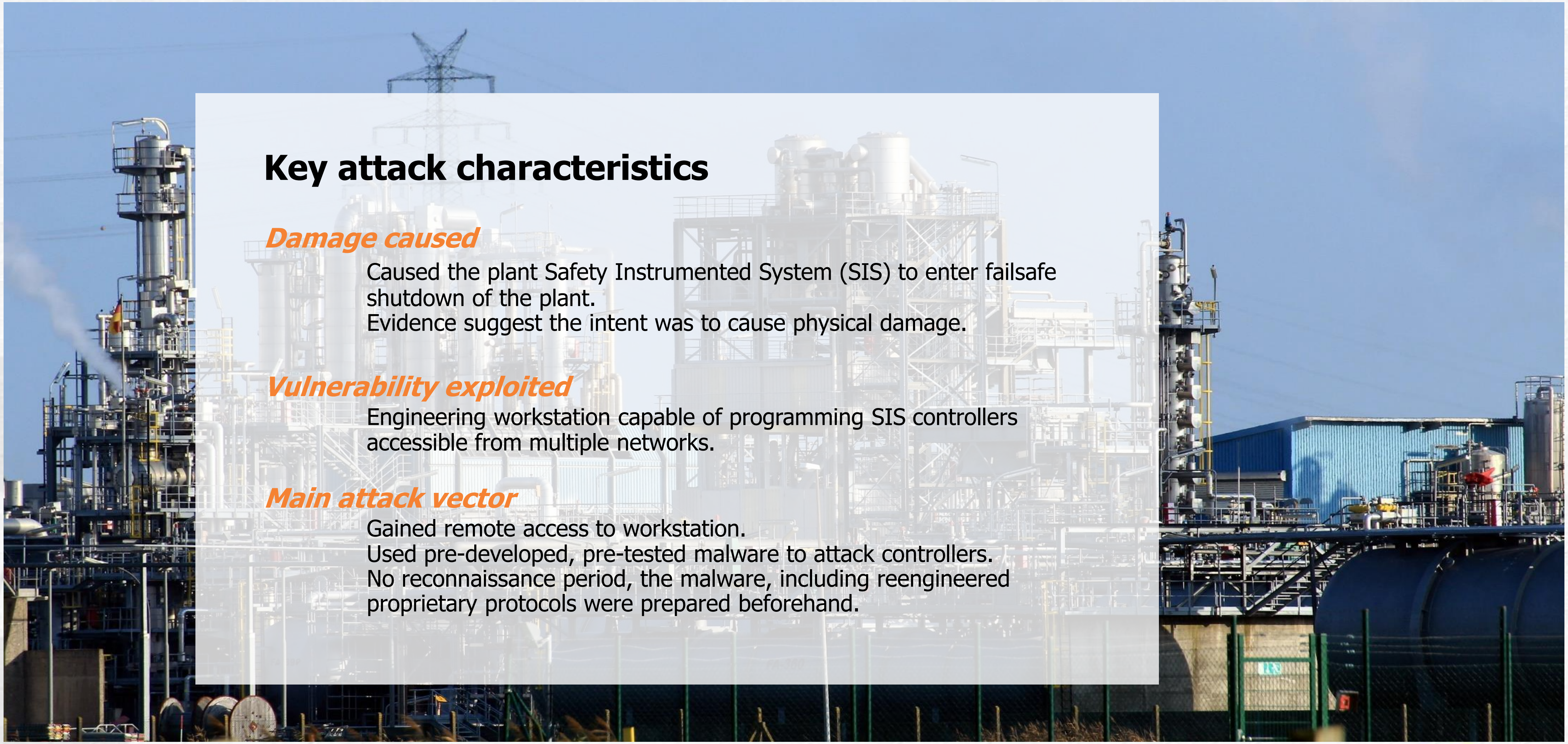
- **Major cyber-incident impacting Hydro’s production and IT systems.**
- **Control System endpoints at several plants attacked => manual backup operation.**
- **Reports of significant financial loss.**

Takeaways

- **Despite comprehensive IT security investments and external services, it is hard to protect, detect and respond to major incidents before widespread, significant impact.**
- **More digitalization and automation of industry => more vulnerabilities, less manual backup options.**

Triton

- attack on industrial plant Schneider Electric controllers



Key attack characteristics

Damage caused

Caused the plant Safety Instrumented System (SIS) to enter failsafe shutdown of the plant.
Evidence suggest the intent was to cause physical damage.

Vulnerability exploited

Engineering workstation capable of programming SIS controllers accessible from multiple networks.

Main attack vector

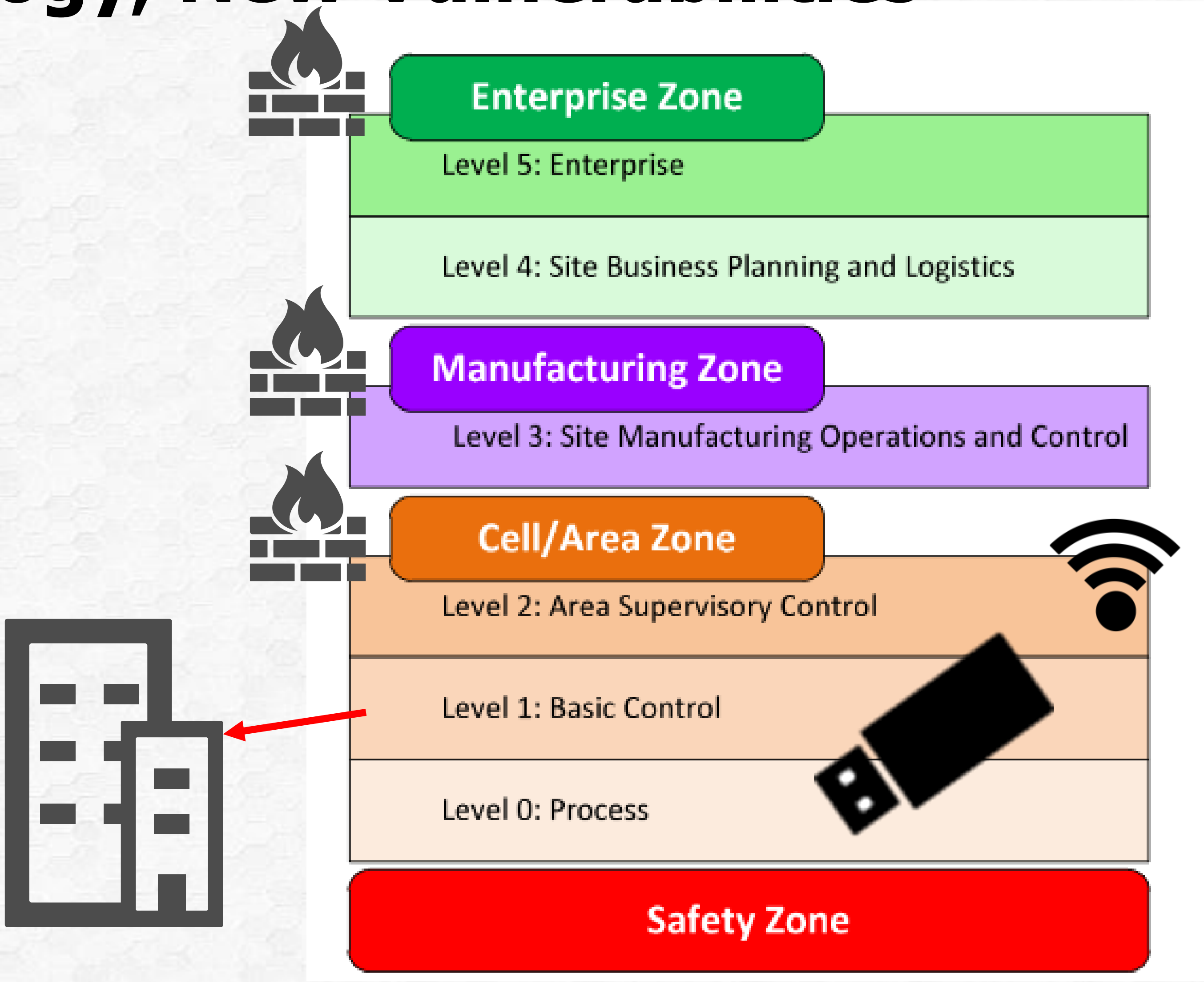
Gained remote access to workstation.
Used pre-developed, pre-tested malware to attack controllers.
No reconnaissance period, the malware, including reengineered proprietary protocols were prepared beforehand.

Who are the Threat Actors?

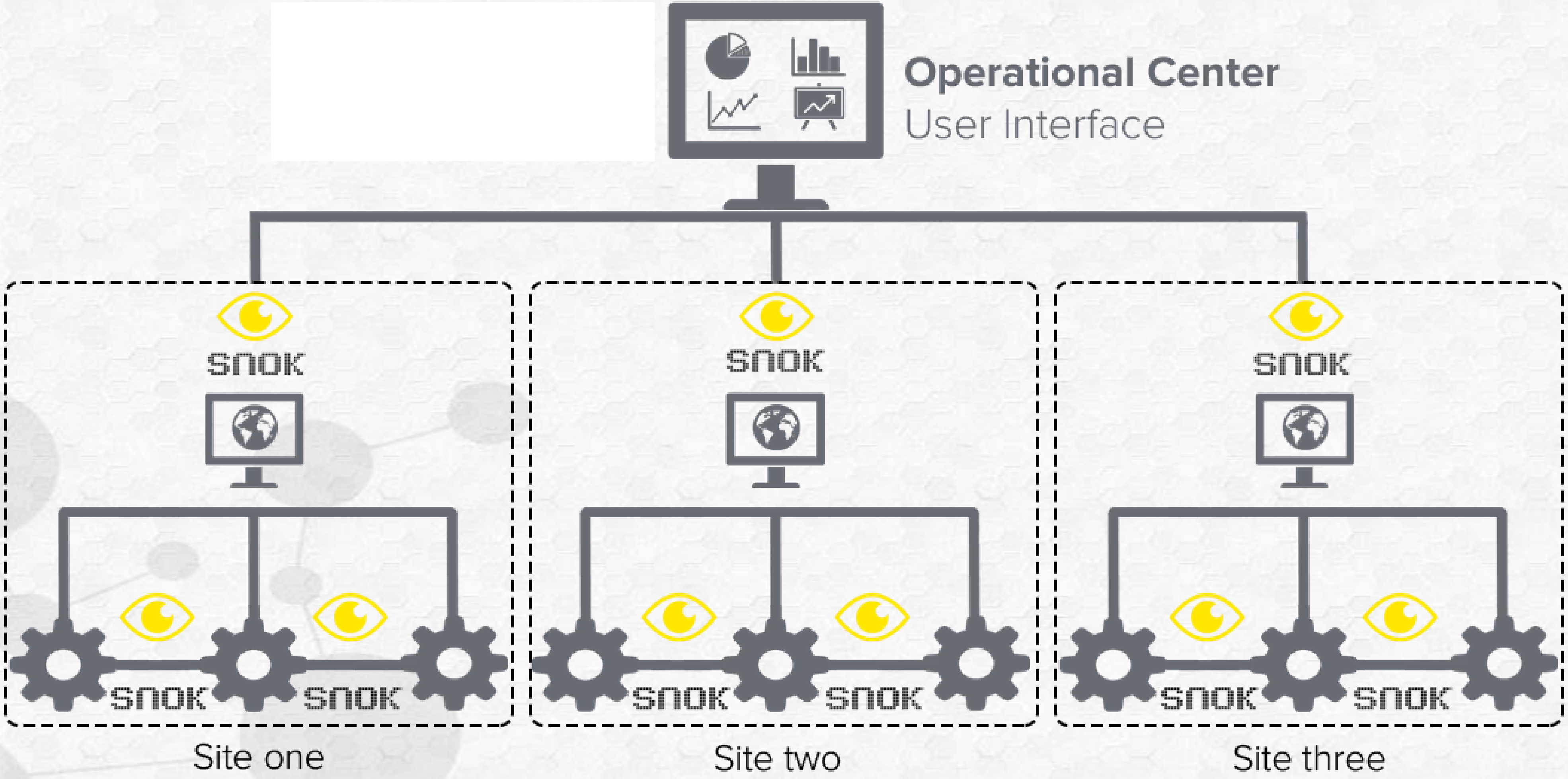
- Malicious or unintentional **insiders** contribute a significant portion of events.
- Trend towards more **professional hackers** employed by nation states or corporations.
- Besides causing harm motive can be preparing **contingency**.

New Technology, New Vulnerabilities

1. Enterprise firewall
2. Manufacturing zone firewall (?)
3. Cell/Area segmentation (?)
4. 4G/Wifi for remote access
5. Data directly to the 'Cloud'
6. Cyber un-aware technicians accessing systems
7. Operators charging smartphones
8. Non-hardened OEM devices
9. Open Source
10. APT


Enterprise Zone
Level 5: Enterprise
Level 4: Site Business Planning and Logistics
Manufacturing Zone
Level 3: Site Manufacturing Operations and Control
Cell/Area Zone
Level 2: Area Supervisory Control
Level 1: Basic Control
Level 0: Process
Safety Zone

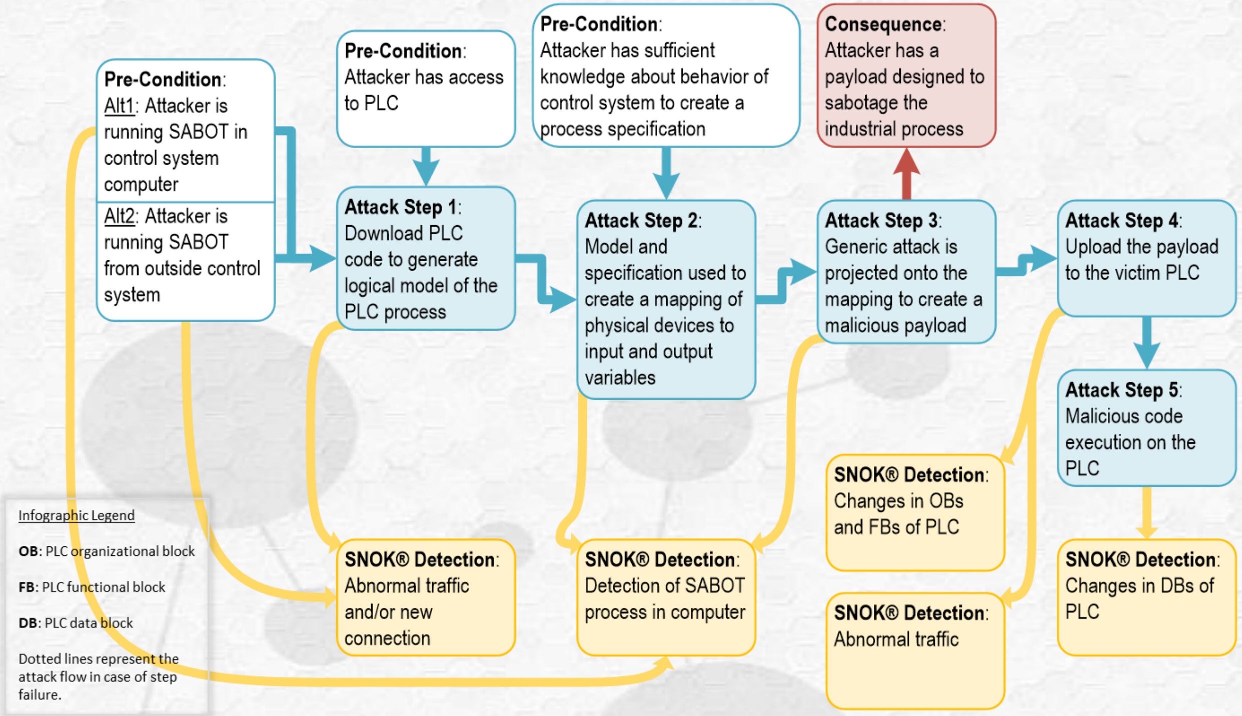
Where do they attack next?



Attacks & detection in OT environment

Attack Scenario – Sabotage Payload

Tool that maps the control instructions in a PLC to an adversary-provided specification of the system behaviour to create and upload a malicious payload to the PLC



Pre-Condition: Alt1: Attacker is running SABOT in control system computer

Alt2: Attacker is running SABOT from outside control system

Pre-Condition: Attacker has access to PLC

Pre-Condition: Attacker has sufficient knowledge about behavior of control system to create a process specification

Consequence: Attacker has a payload designed to sabotage the industrial process

Attack Step 1: Download PLC code to generate logical model of the PLC process

Attack Step 2: Model and specification used to create a mapping of physical devices to input and output variables

Attack Step 3: Generic attack is projected onto the mapping to create a malicious payload

Attack Step 4: Upload the payload to the victim PLC

Attack Step 5: Malicious code execution on the PLC

SNOK® Detection: Abnormal traffic and/or new connection

SNOK® Detection: Detection of SABOT process in computer

SNOK® Detection: Changes in OBs and FBs of PLC

SNOK® Detection: Abnormal traffic

SNOK® Detection: Changes in DBs of PLC

Infographic Legend

OB: PLC organizational block

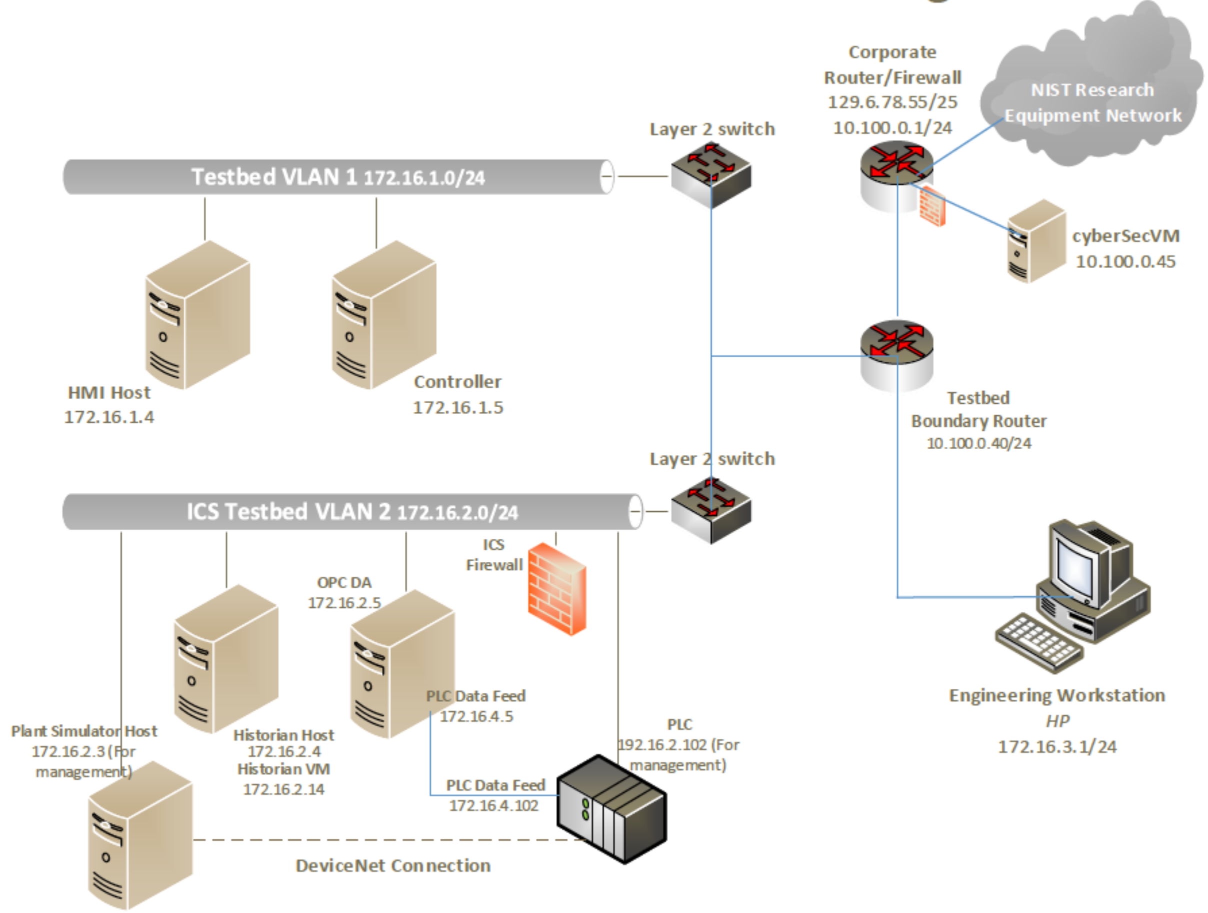
FB: PLC functional block

DB: PLC data block

Dotted lines represent the attack flow in case of step failure.

Source: McLaughlin, P., et al: ***SABOT: Specification-based Payload generation for Programmable Logic Controllers***. In Proc. of the 2012 ACM Conference on Computer and Communications Security, pp. 439-449.

Process Control Enclave Network Diagram



There are no shortcuts to security

NIST Cybersecurity Framework (CSF) - a simple and intuitive philosophy to help develop and implement critical cybersecurity functions:

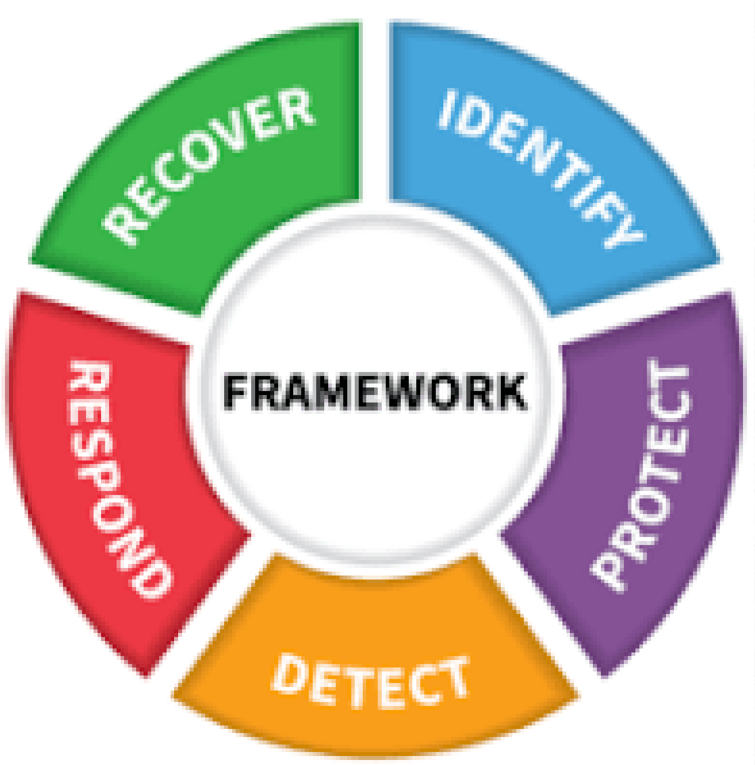
Identify: … manage cybersecurity risk to systems, people, assets, data, and capabilities.

Protect: … implement appropriate safeguards to ensure delivery of critical services.

Detect: … identify the occurrence of a cybersecurity event.

Respond: … take action regarding a detected cybersecurity incident.

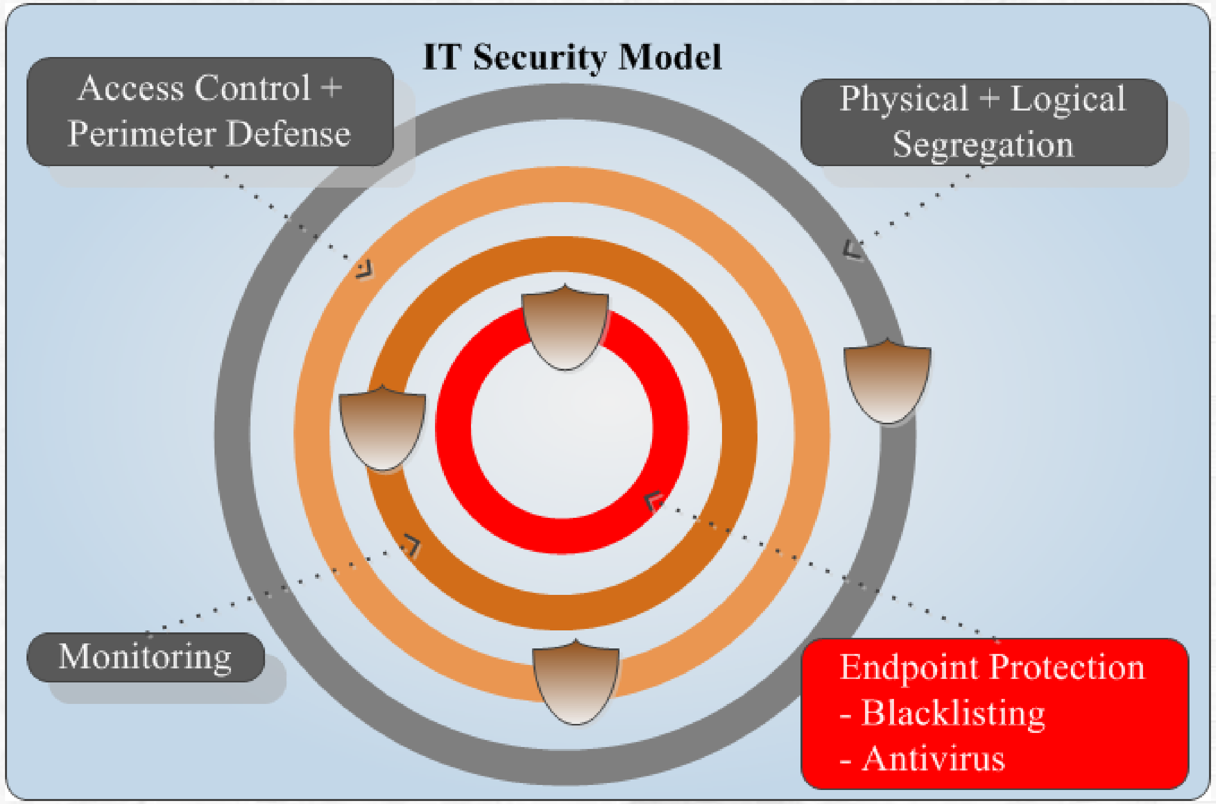
Recover: … maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

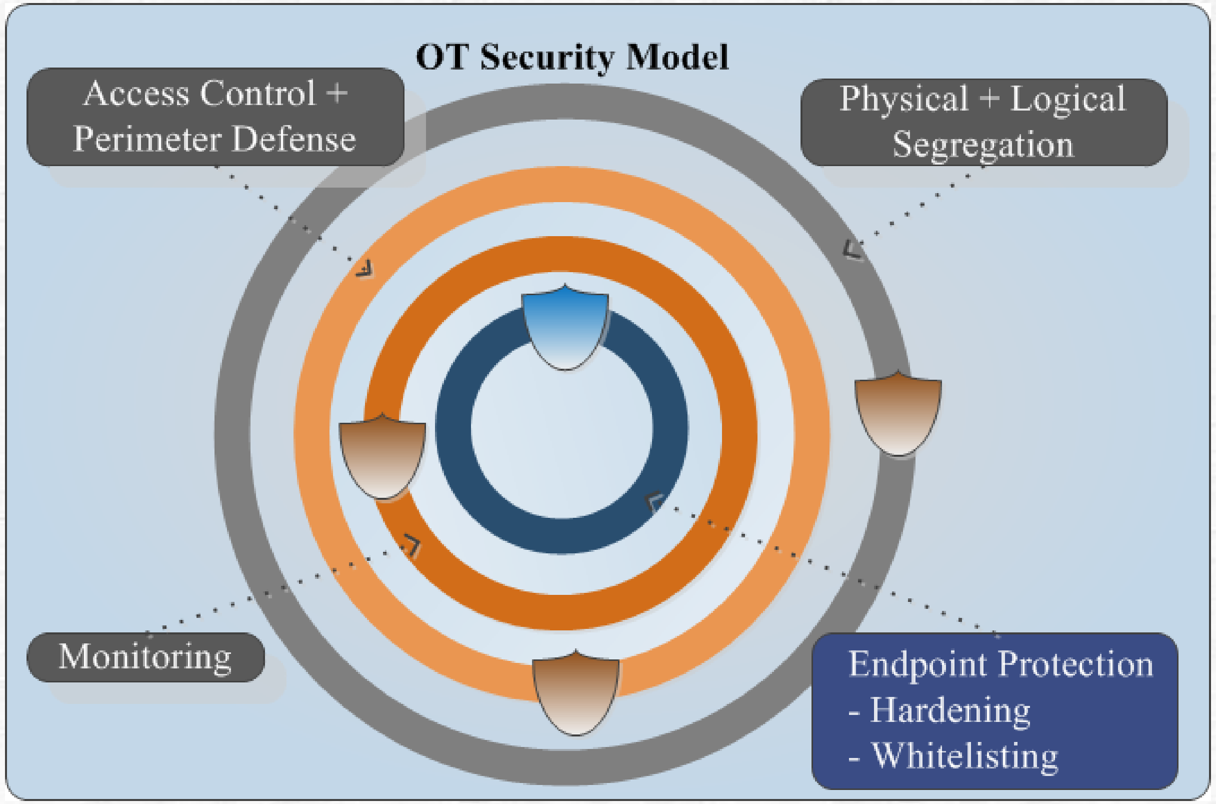


Implementation should not be a linear list of tasks. All functions must be in place at any given time.

Defense in depth for IT and OT

Know your assets. Segregate. Harden. Monitor.





Cybersecurity Risk

=

Threat Landscape

x

Vulnerability

x

Consequences

Questions, thoughts, ideas or comments?

Thank you for your attention!

Rune.Halvorsen@securenok.com
www.securenok.com