DYNAMIC POSITIONING CONFERENCE
October 11-12, 2016

CYBERSECURITY

Building Cybersecurity into DP Systems

Siv Hilde Houmb

Secure-NOK

SECURENOK

Building Cybersecurity into DP Systems

MTS DP Conference 2016

By: Siv Hilde Houmb

Cyber attacks - U.S.

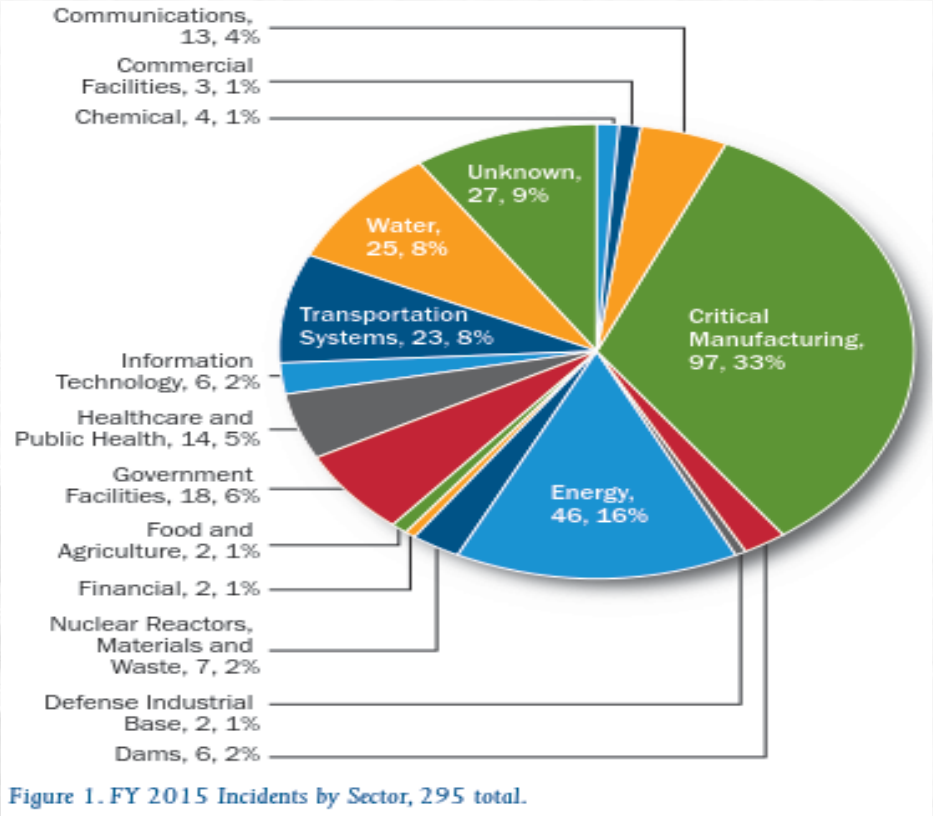
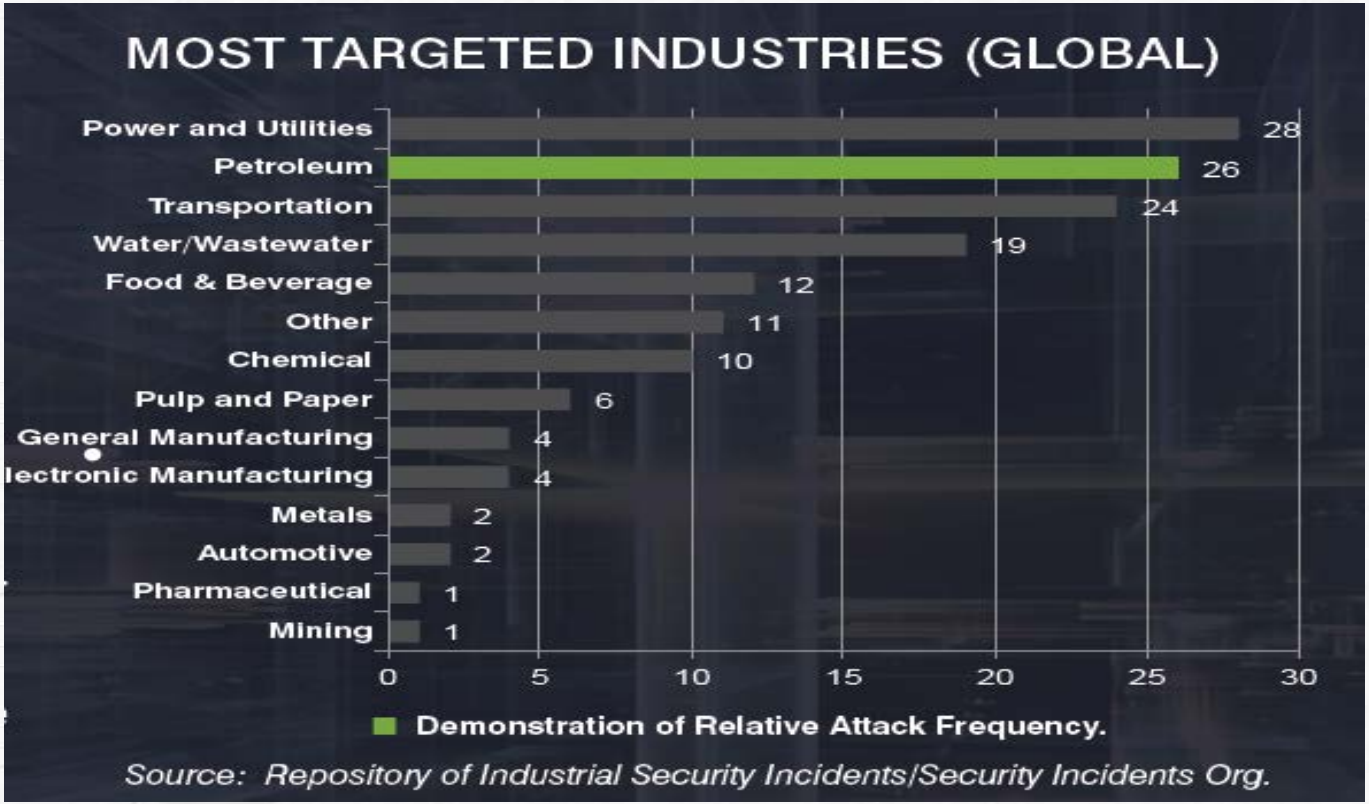


Figure 1. FY 2015 Incidents by Sector, 295 total.

Source: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf

Cyber attacks - Global



What Do We Know?

- Increasing number of cyber attacks
- Cyber attacks are becoming more sophisticated (APT)

- The attackers are more organized:
  - Well funded
  - Highly skilled
  - Aggressive

Advanced Persistent Threat

- **Advanced** – high level of coordinated human involvement to monitor and control the attack
- **Persistent** – priority to gain (several) foothold(s), remain «invisible» to the target for as long as possible with priority to complete a mission (low and slow) and get back out UNDETECTED
- **Targeted** – has a specific target in mind


DO WE HAVE A BACKUP?
Stuxnet VIRUS

STUXNET – Targeted Cyber Sabotage

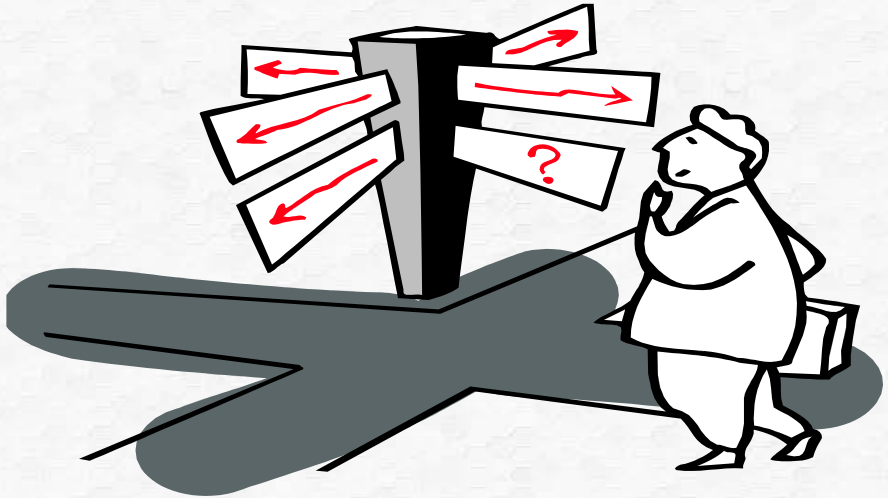
- Designed to sabotage the Natanz nuclear facility
- Destroyed 1000 centrifuges
- Continues to affect the Natanz plant
- Undetected for more than 3 years
- Attacked more than 20 control systems
- An APT attack design to be destructive and targeted

Cyber Attacks:
Information Technology vs Operational Technology

Cyber attacks in IT	Cyber attacks in OT
• Information Systems • Corporate networks • Consumers • Homes • ...	• SCADA Systems • PLCs • ...

Can´t We Just Adopt Solutions from IT Systems?

- Anti-virus software?
- Firewalls?
- Whitelisting?
- Hardening?
- Access control?
- Network monitoring?
- Encryption?



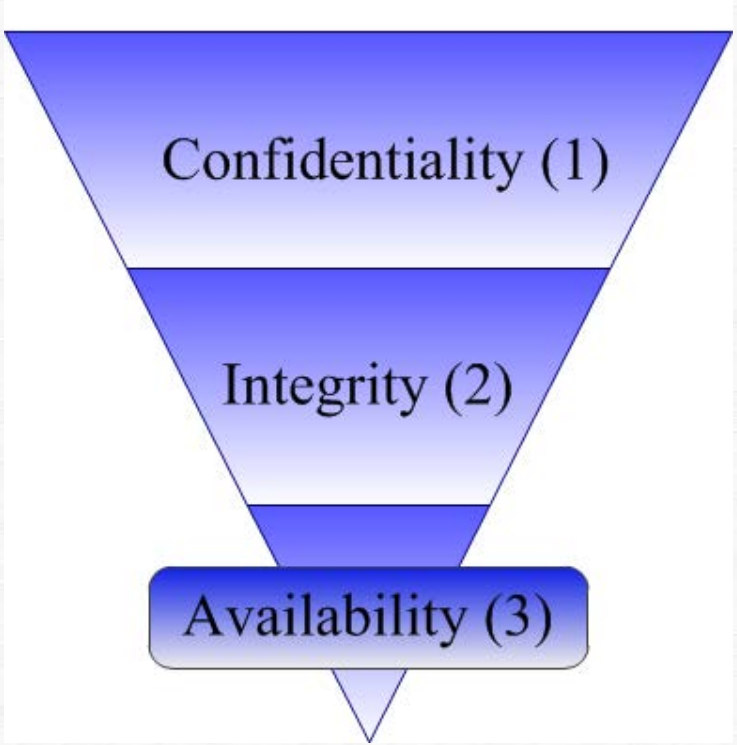
IT System Security Model

IT security focus (CIA)

- Confidentiality
- Integrity
- Availability

IT security safeguards

- Firewalls
- Access control
- Malware protection
- Antivirus solutions
- Patch management
- Network monitoring



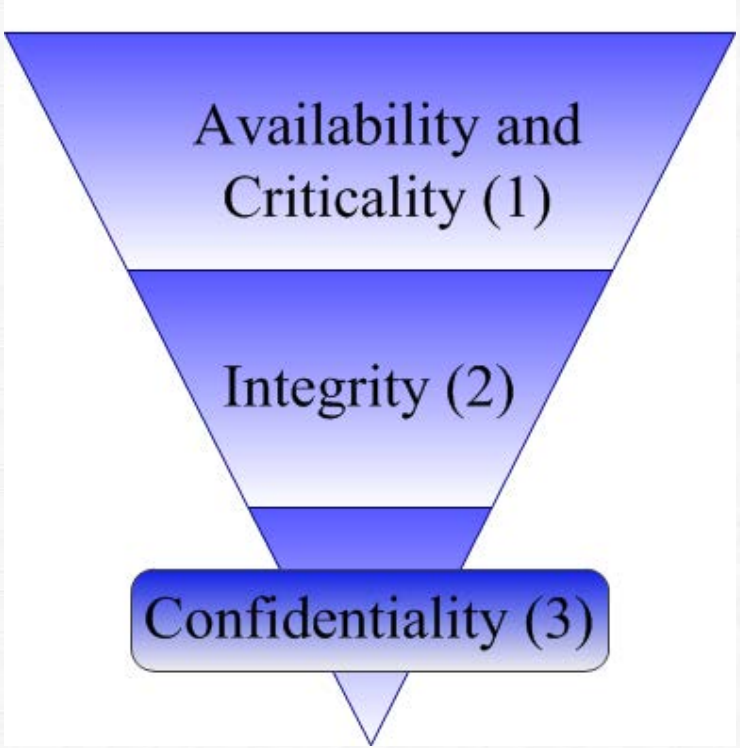
Traditional OT System Security Model

OT security focus (AIC)

- Availability/Criticality
- Integrity
- Confidentiality

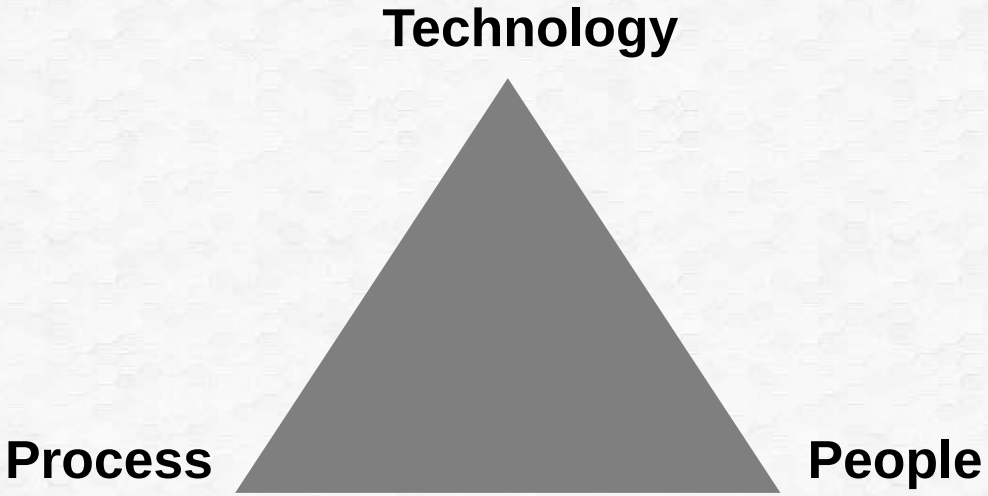
OT security safeguards

- Air-gapped/Island network



Strategy for Protecting OT Systems (1)

- Defence-in-depth strategy tailored for OT systems
- Built on NIST Cybersecurity Framework (CSF)
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover



Strategy for Protecting OT Systems (2)

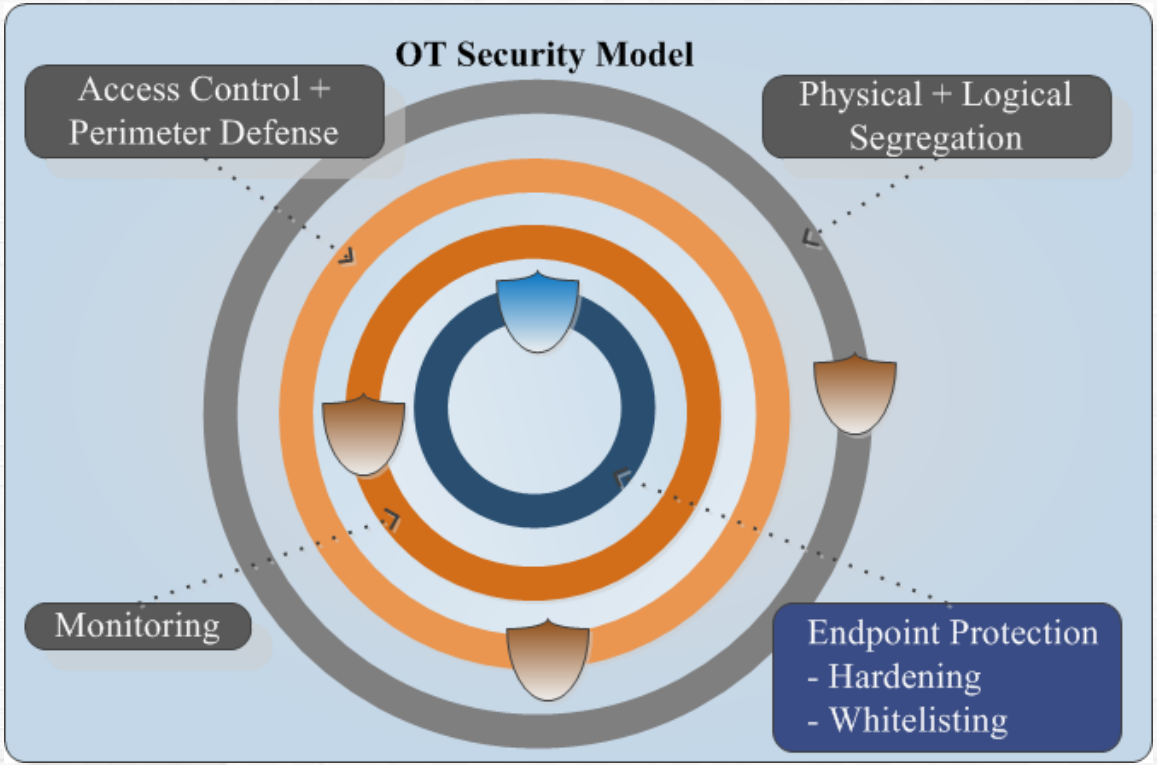
NIST CSF group security safeguards into following categories:

- Technical safeguards
  - Physical and logical segregation
  - Authentication and access control
  - Perimeter defence
  - Network monitoring
  - End-point protection

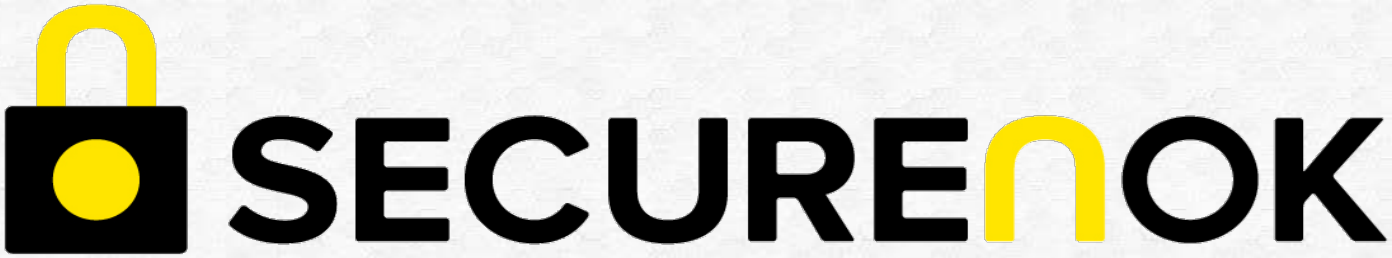
Strategy for Protecting OT Systems (3)

- Non-technical safeguards
  - Security policies and procedures
  - Incident response plans and procedures
  - Security awareness training

Defense-in-Depth Strategy for OT Systems




Credit: 401kcalculator.org



Thank you for your Attention

Questions?