CYBERSECURITY IN THE DIGITAL TRANSFORMATION

By: Erlend A. Engum

NORTEX DATA SCIENCE CLUSTER - OTC 2017 Digitalization Workshop

Secure-NOK® - Key Facts

- Secure-NOK®: a cybersecurity specialist company, focusing on Oil & Gas
- Established in 2010
  - By Siv Hilde Houmb, PhD in Cybersecurity, and Liv Elin Houmb
- Offices in Norway and Houston, Texas
- International team (Norway, US, Russia and India)
- Deep insights in automation and control systems security, and Oil & Gas

SECURENOK


DO WE HAVE A BACKUP?
Stuxnet VIRUS

Outline

- Real-time data and its effect on cybersecurity
- Increased frequency and sophistication of cyber-attacks
- Information Technology (IT) vs. Operational Technology (OT) systems
- Challenges involved in protecting OT systems
- Strategies for protecting OT systems

Introduction

- The future of a digital oilfield makes rig OT system increasingly dependent on real-time data processing over IT networks.

- Increasing deployments of digital industrial control system (ICS) technology in the drilling oil and gas industry leaves the industry vulnerable to cyber-attacks.

- Once considered rare, **cyber-attacks on ICS are increasing in frequency and sophistication.**

Cybersecurity attacks: An Increase in Frequency and Sophistication

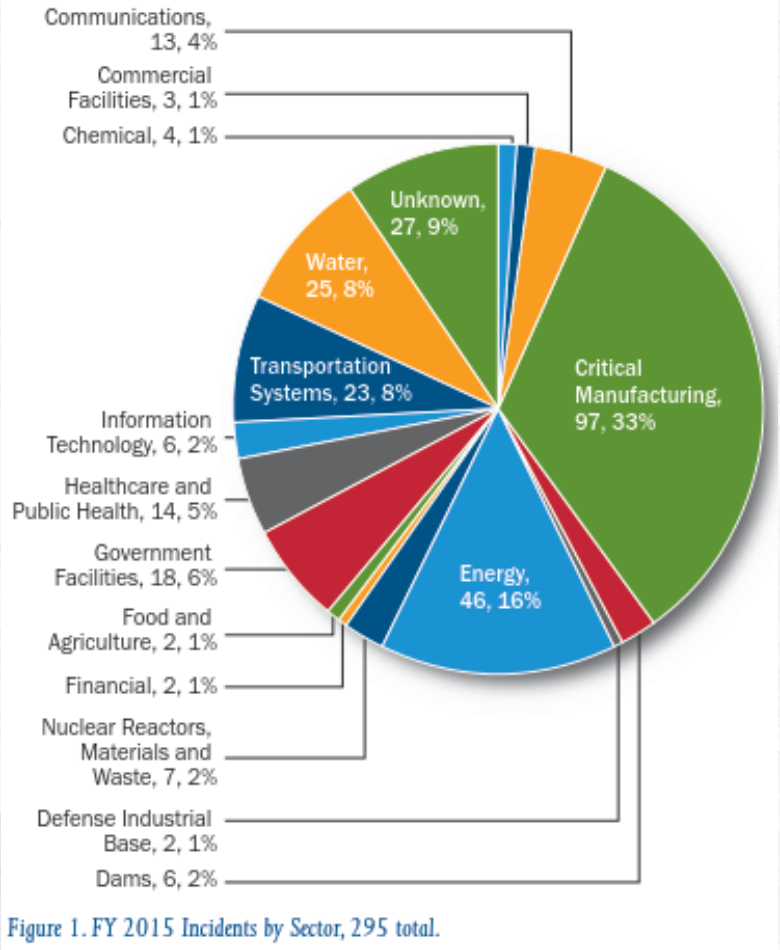
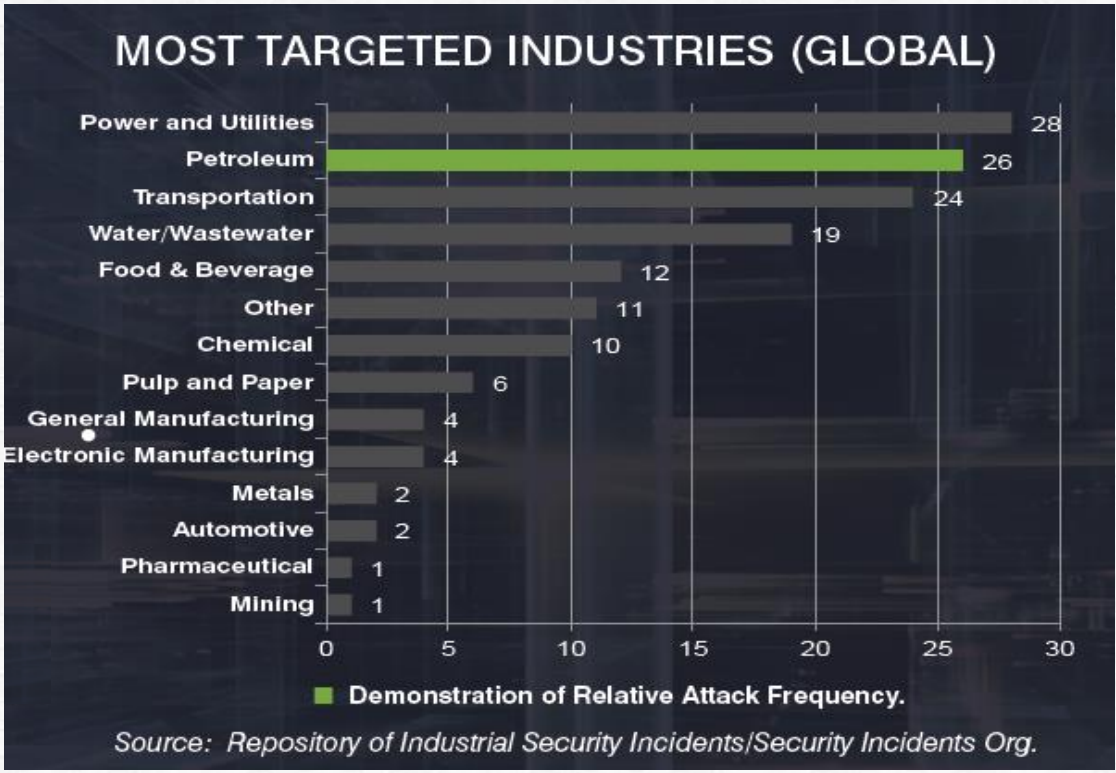


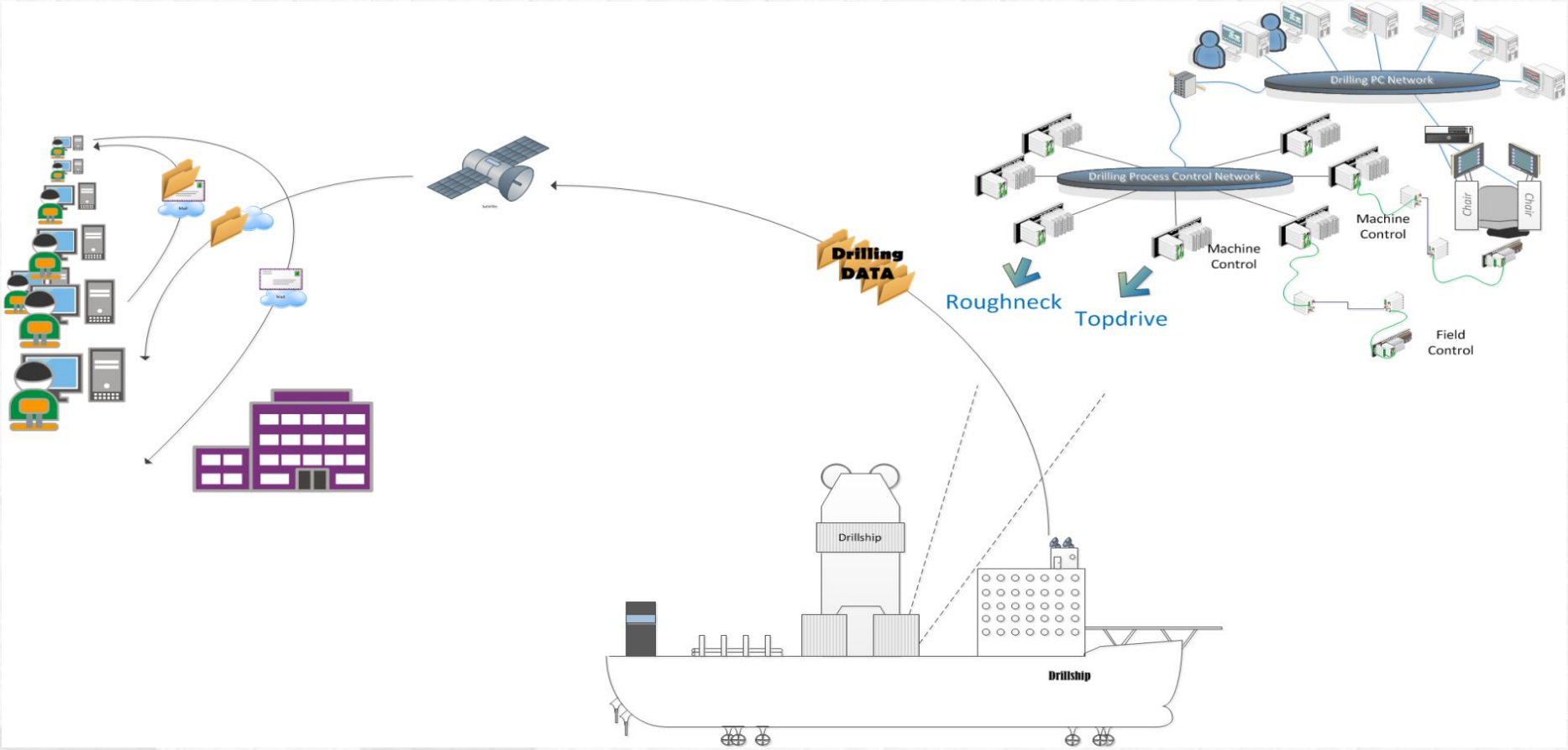
Figure 1. FY 2015 Incidents by Sector, 295 total.



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

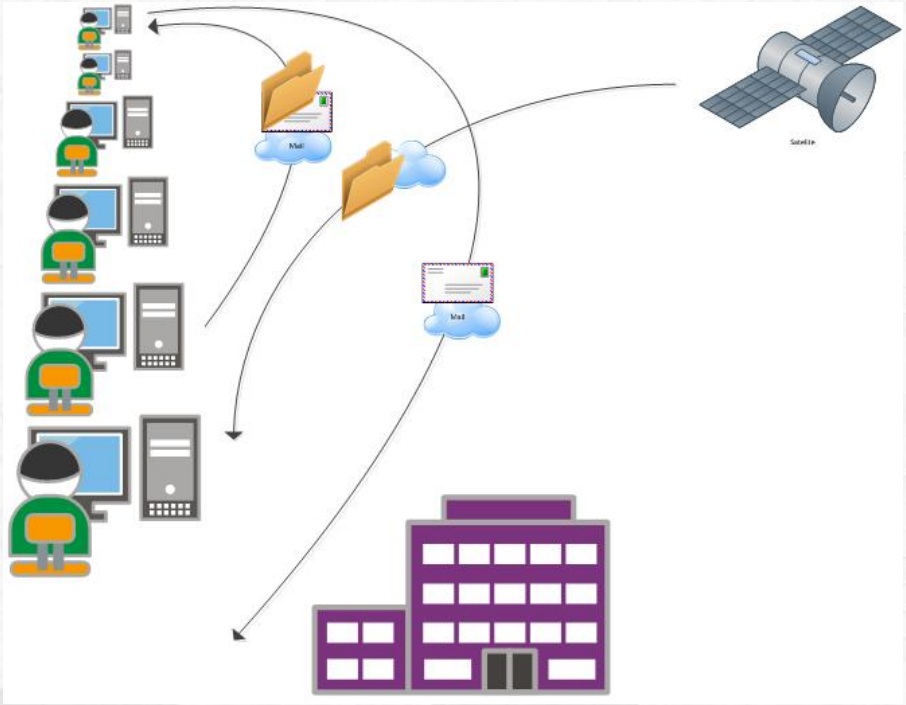
SECURENOK

Real-Time Data and its Path through the Systems

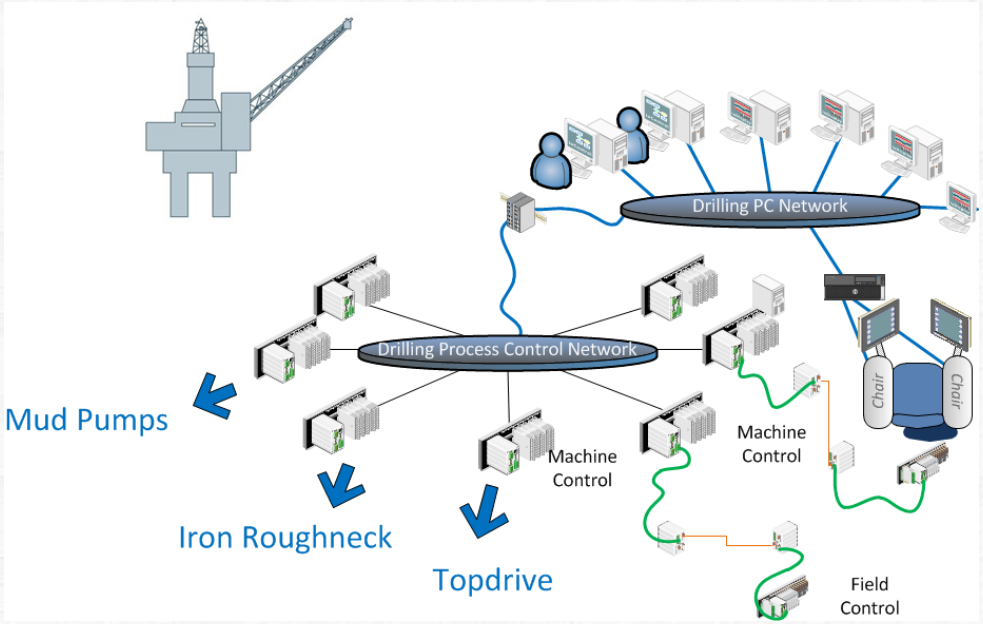


IT versus OT Systems – How they Differ

IT



OT



SECURENOK

OT ≠ IT

Primary purpose:

Robust
predictable
reliable

Flexible

Execute specific tasks in a **reliable and timely manner**
=> millisecond precision.

Provide user with the programs, applications and systems **needed at any given time**
=> agreed availability.

OT systems need non-intrusive solutions

SECURENOK

OT ≠ IT

Use of resources:

Robust
predictable
reliable

Flexible

Tasks do not change much over the system lifetime
=> **access to a minimum of required resources only** (memory, processing power, bandwidth, connections).

IT systems must install patches, new or improved programs and applications as they become available in the market
=> need **plenty of reserve resources** (memory, CPU power, bandwidth etc.)

OT systems need minimal footprint solutions

OT ≠ IT

Maintenance required:

Robust
predictable
reliable

Flexible

Once an OT system is installed and put in production, it should **run for its intended lifetime**

⇒ Low tolerance for maintenance or other interruptions

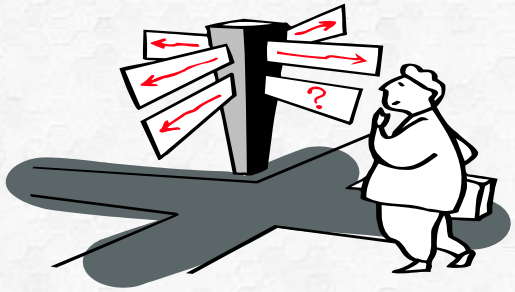
IT systems assume access to **periodic maintenance windows**.
Continuous updates to keep **a healthy patch status** fundamental to keep IT systems secure.

OT systems need minimal maintenance solutions

SECURENOK

Can´t We Just Adopt Solutions from IT Systems?

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



SECURENOK

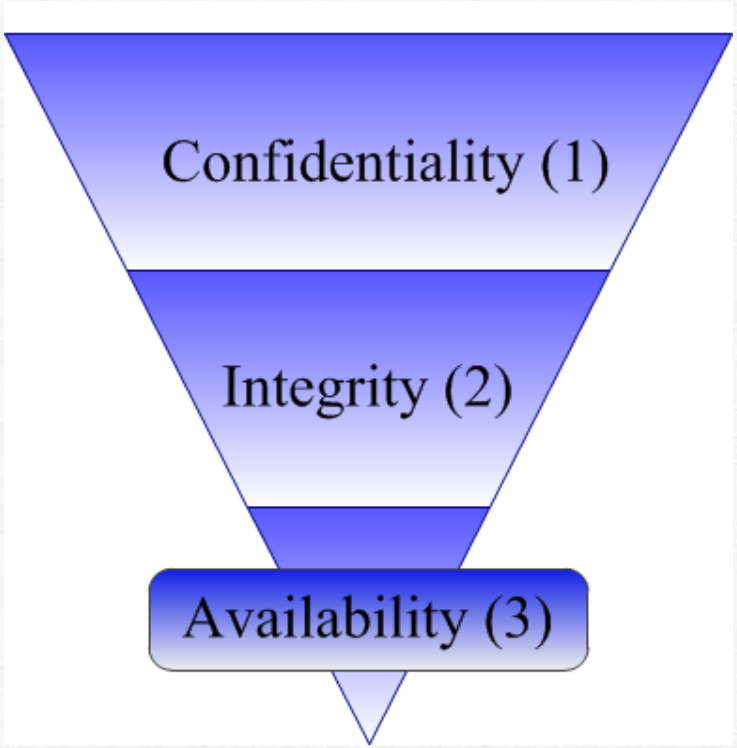
IT System Security Model

IT security focus (CIA)

- Confidentiality
- Integrity
- Availability

IT security safeguards

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



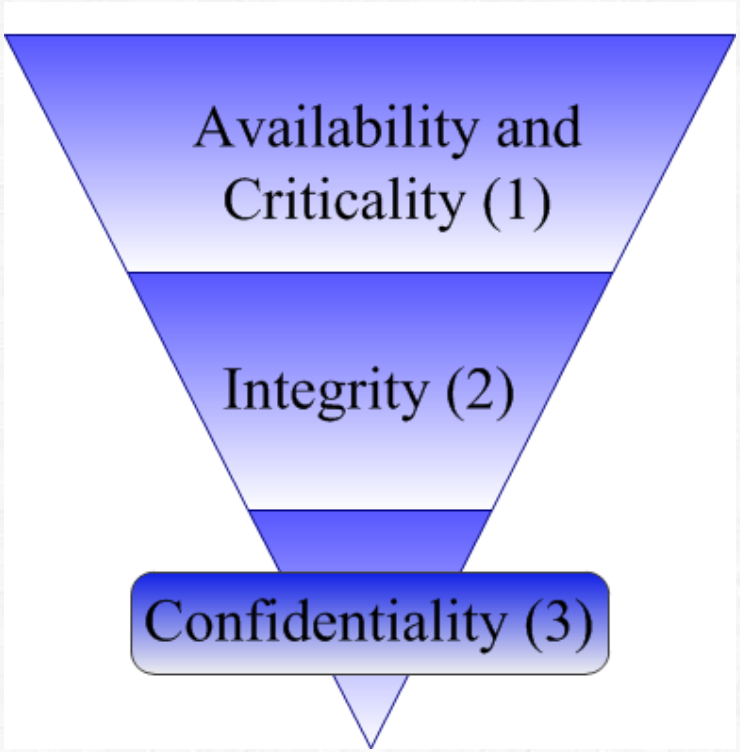
Traditional OT System Security Model

OT security focus (AIC)

- Availability/Criticality
- Integrity
- Confidentiality

OT security safeguards

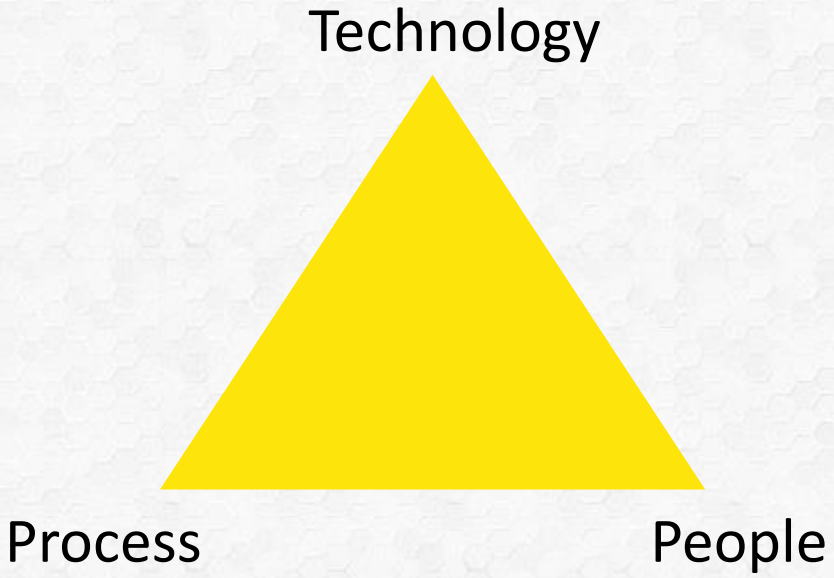
- Air-gapped/Island network



Defence-in-depth strategy tailored for OT systems

Built on NIST Cybersecurity Framework (CSF)

- Identify
- Protect
- Detect
- Respond
- Recover



SECURENOK

Technical safeguards for Protecting OT Systems

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

Non-technical safeguards for Protecting OT Systems

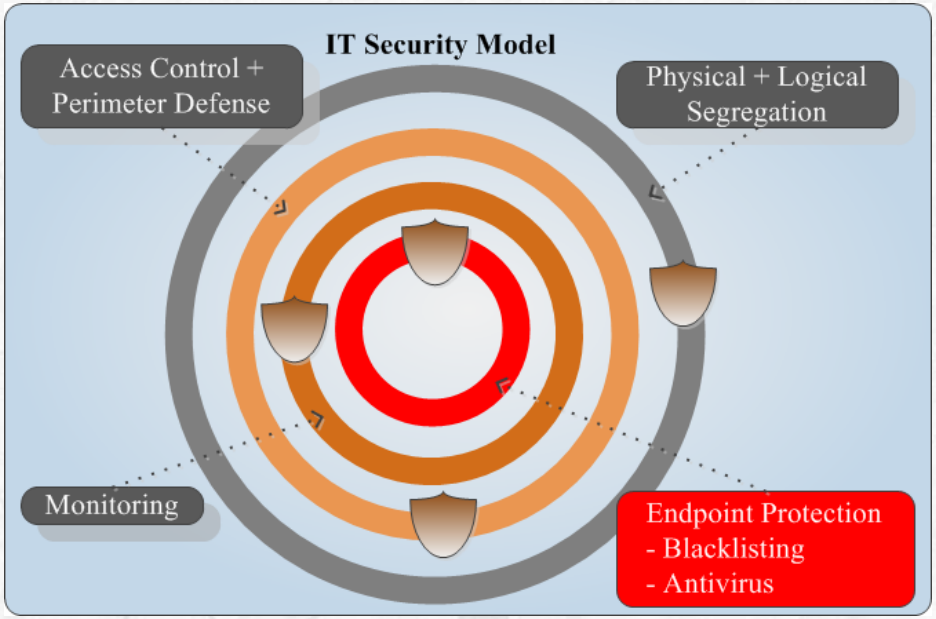
- Security policies and procedures
- Incident response plans and procedures
- Security awareness training

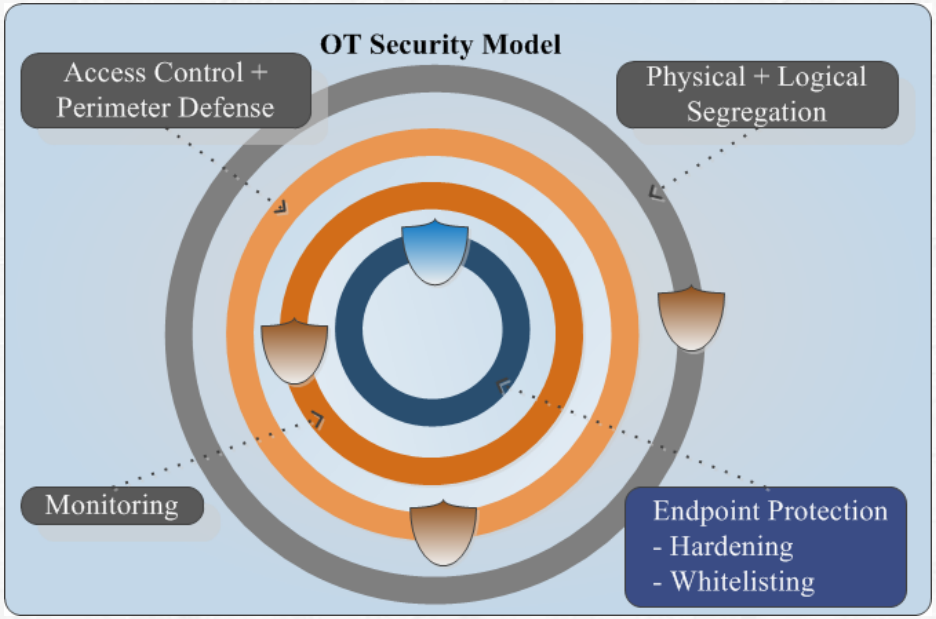
SECURENOK

Fundamental differences in models poses challenges to adopting and deploying solutions

- Shutdowns of the control system
- Onshore support teams to make changes online
- Changes made during operations
- Software or firmware changes to systems once they are working as functionally designed

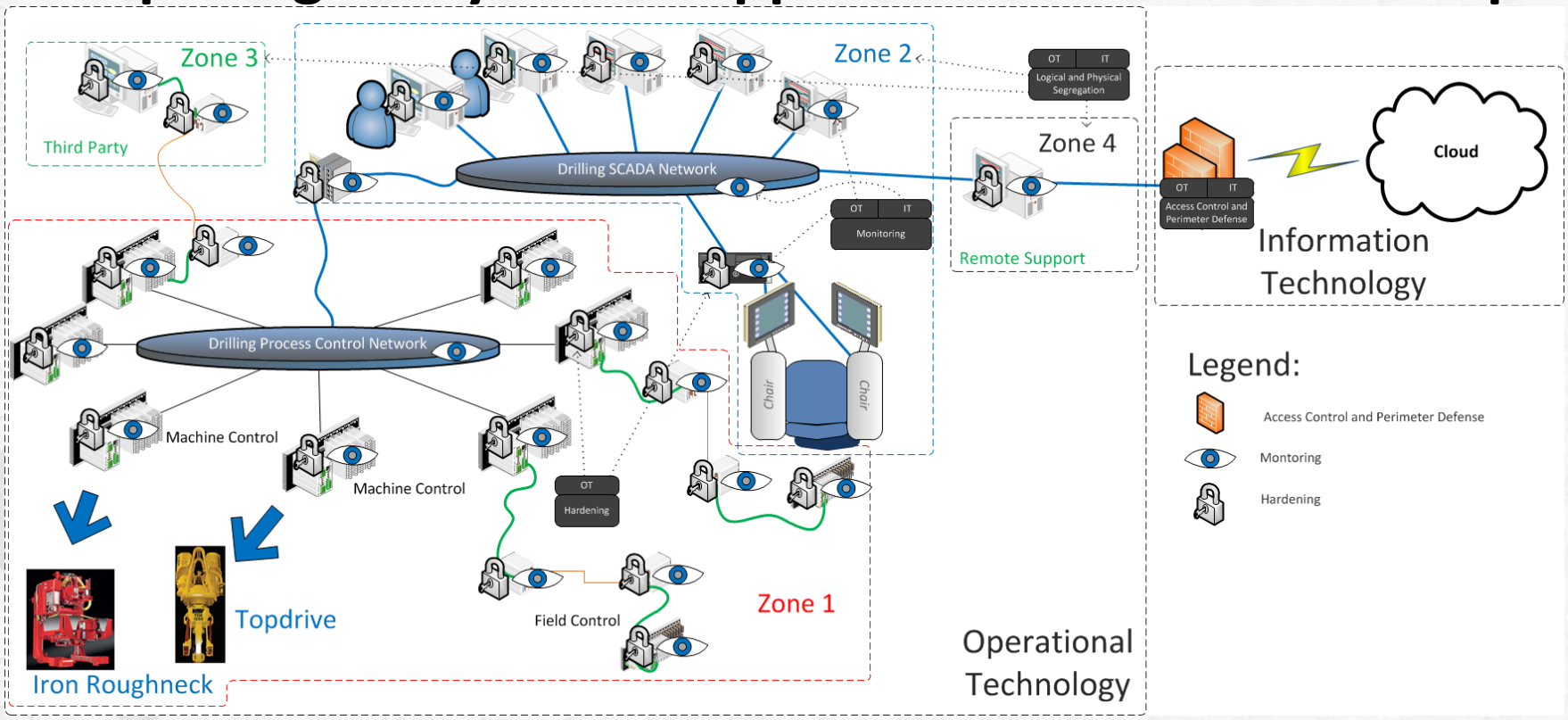
Defense-in-Depth Strategy for IT and OT Systems





SECURENOK

Example Rig OT System – Application of Defense-in-Depth



Conclusion

- Deploy a defense-in-depth strategy
- Use barriers and mitigation solutions designed to operate in an OT environment
- Consider a flexible and thoughtful approach when building cybersecurity resilience into OT systems
- An efficient OT cybersecurity strategy requires a close collaboration between OT and IT

More Information

- http://www.upstreampumping.com/article/instrumentation/2016/new-early-warning-cybersecurity-system-adds-extra-hardening-safeguards
- http://www.drillingcontractor.org/tailored-layered-defense-depth-strategy-can-help-build-cyber-resilience-rig-ot-systems-40086
- http://www.upstreampumping.com/article/drilling-special-sections/2015/protecting-drilling-rigs-and-production-platforms
- http://www.controleng.com/single-article/protecting-industrial-control-systems/c07ce49f515a643842a41060a1d2e177.html
- http://www.drillingcontractor.org/drilling-cybersecurity-36727
- http://www.drillingcontractor.org/secure-nok-cyber-attack-detection-paramount-to-protecting-asset-integrity-37150

SECURENOK


Your Partner in Oil & Gas
cyber security. Secure-NOK AS
is the leading provider for securing
critical infrastructure in the industry.
SECURENOK
Secure-NOK AS
Professor Olav Hanssensvei 7A
N-4068 Stavanger, Norway
Secure-NOK USA
177 West Gray St.
Houston, TX 77019, USA
www.securenok.com