DEFENSIFY

BUSINESS SECURITY SOLUTIONS

OT vs IT Cybersecurity

Ludwig Seitz, OT Security Specialist

June 2023

Agenda

1. OT Legacy
2. Convergence – Industry 4.0
3. OT Lifecycle
4. Operational conditions and priorities
5. Cybersecurity in OT

    Example: Remote Access

    Example: Network Monitoring

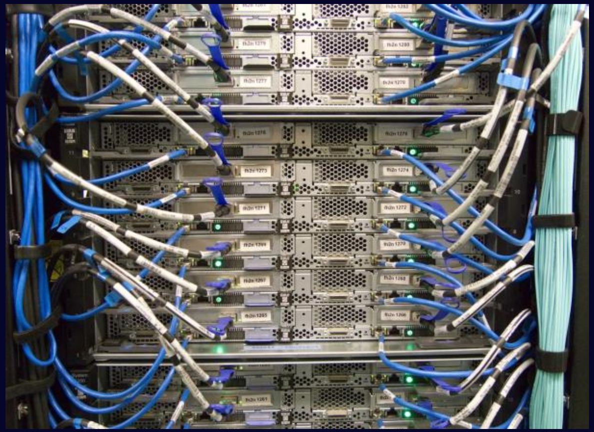
    Example: Patching

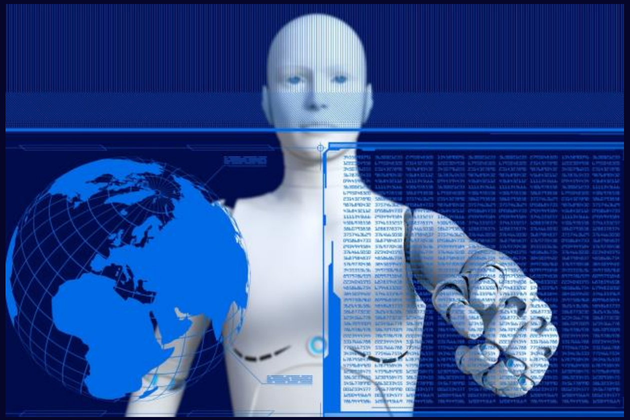
OT Legacy

- OT used to be air-gapped
  - Very open configurations
  - Unprepared for IT threats
  - Equipment sensitive to disturbance
- Siloed world
  - OT protocols ≠ IT protocols
  - Vendor lock-in common

IT – OT Convergence

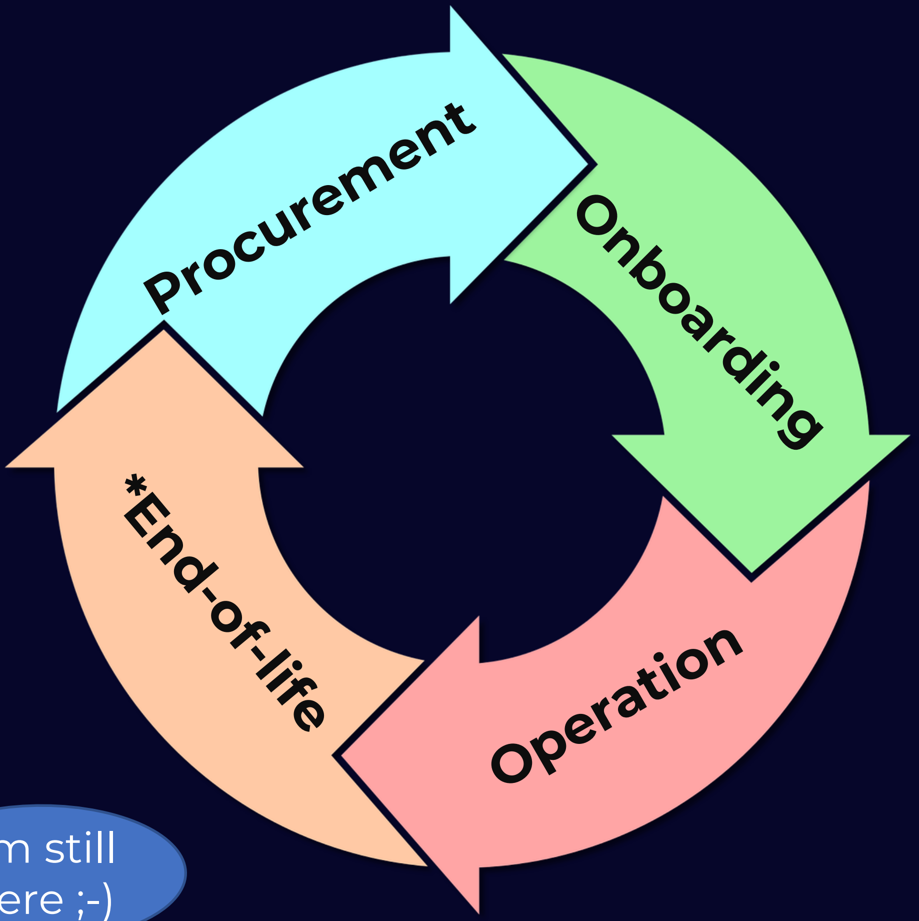
- OT increasingly connected
    - Remote working
    - Remote support
- Generic IT solutions & protocols used
    - TCP/IP, MQTT, HTTP(S)
- Big data & AI – Industry 4.0
    - Predictive maintenance
    - Production optimization





OT Lifecycle

- Equipment has **<u>very</u>** long lifetime
  - Up to 20 years
- Changes are rare
  - “Never touch a running system”
- Why?
  - Machines are expensive (~$500K for a CNC)
  - Machine EOL* == Software EOL >> OS EOL
  - Changes can cause downtime
  - Changes can require re-certifying



*EOL: End-of-life

Operational conditions and priorities

- IT: Confidentiality > Integrity > Availability
- OT: Availability > Integrity > Confidentiality
  - Or: Safety > Reliability > Productivty
- Real-time requirements
  - OS and protocols
- Harsh environments
  - Dust, heat, vibrations

Cybersecurity in OT vs IT

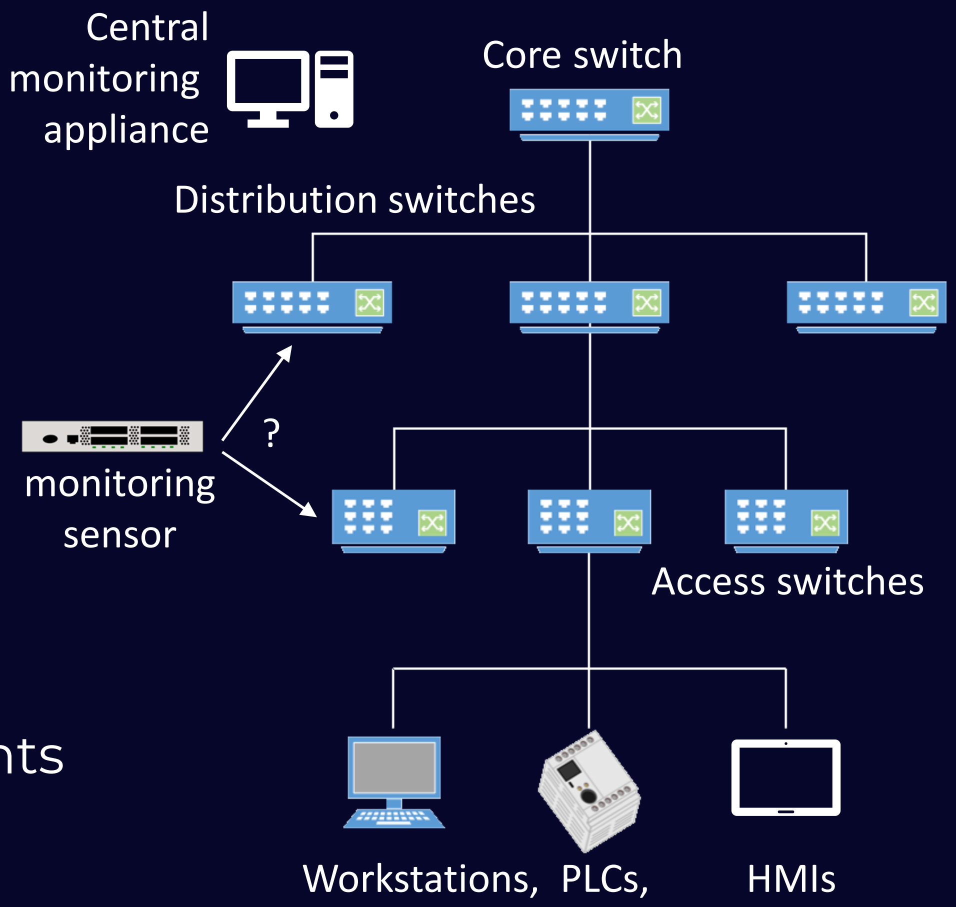
Security Control	IT	OT
Endpoint protection	Signature or behaviour-based, automated response, always online	Application whitelisting, detect-only, offline
Segmentation	Internet DMZ, Firewalls, Tier model	Industrial DMZ, Segment OT from IT, Segment production zones
Vulnerability Management	Regular, streamlined process. Patching automated with good tool support (e.g., SCCM, WSUS)	Bad visibility, Infrequent patching, legacy may not be patchable, need scheduled downtime to patch, manual process
Incident Response	Detect, Isolate, Eradicate, Recover, Analyze	Maintain safety, isolation possible?, restore operations, full eradication on next maintenance window

Example: Remote Access

- Problem
  - Specialist support at remote locations
- Security goals
  - Isolate factory from remote client
  - Access control & monitoring
- Challenges
  - Manage remote access credentials
  - Tools and licenses on client machine

Example: Network Monitoring

- Goals
  - Visibility
  - Detect malware
  - Raise alerts on anomalies
- Challenges
  - OT protocols
  - Active scanning vs Real-time requirements & legacy
  - Side-channels (e.g., wireless modems)



Example: Patching

- Goal: Close vulnerabilities
- IT
  - Automated patching is the norm
  - Vulnerability management tools used
- OT
  - 24/7 operations → Need downtime → $$$
  - Breaks legacy system? → Need to roll-back
  - Environment certified? → re-certify → **$$$**

DEFENSIFY

BUSINESS SECURITY SOLUTIONS

THANK YOU!

Ludwig Seitz

E: ludwig.seitz@defensify.se

W: www.defensify.se

June 2023