The future of ICS
Network Security Monitoring

Martin Scheu
martin@ics-cyber.ch

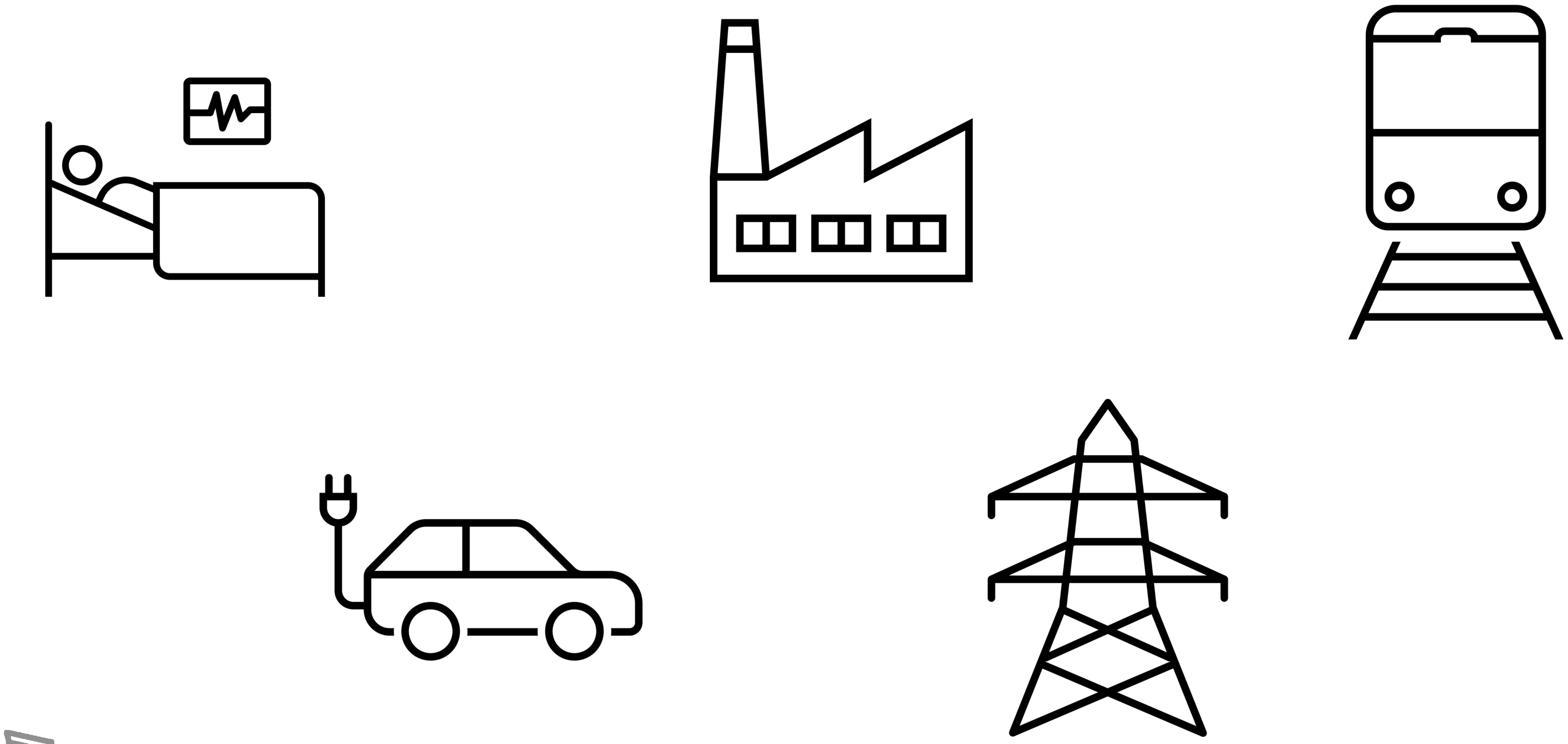
Agenda

- Introduction
- Threats
- Encryption
- Endpoint protection
- What’s next

Introduction

OT - Operational Technology

“ Programmable systems or devices that interact with the physical environment “



New Sub-Sectors

- Solar DC to AC power convertors
- EV charging terminals
- Smart Metering

-> all highly interconnected

New Legal requirements

Germany

Bundesamt
für Sicherheit in der
Informationstechnik

- Attack detection system
  - Logging
  - Detection security relevant events

Switzerland

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

- obligation to report an Attack, hence need to detect it

Threats

OT - Threats

- Remote Access
- Configuration Errors
  - KNX Protocol
- Not maintained hardware or patching not possible
- Missing asset inventory
- IT Threat “swapping” over to OT

Encryption

Encryption

- Available and supported (TLS & certificates)

but

- Impact on Availability and Control

- Dead-Man's PLC cyber extortion for OT

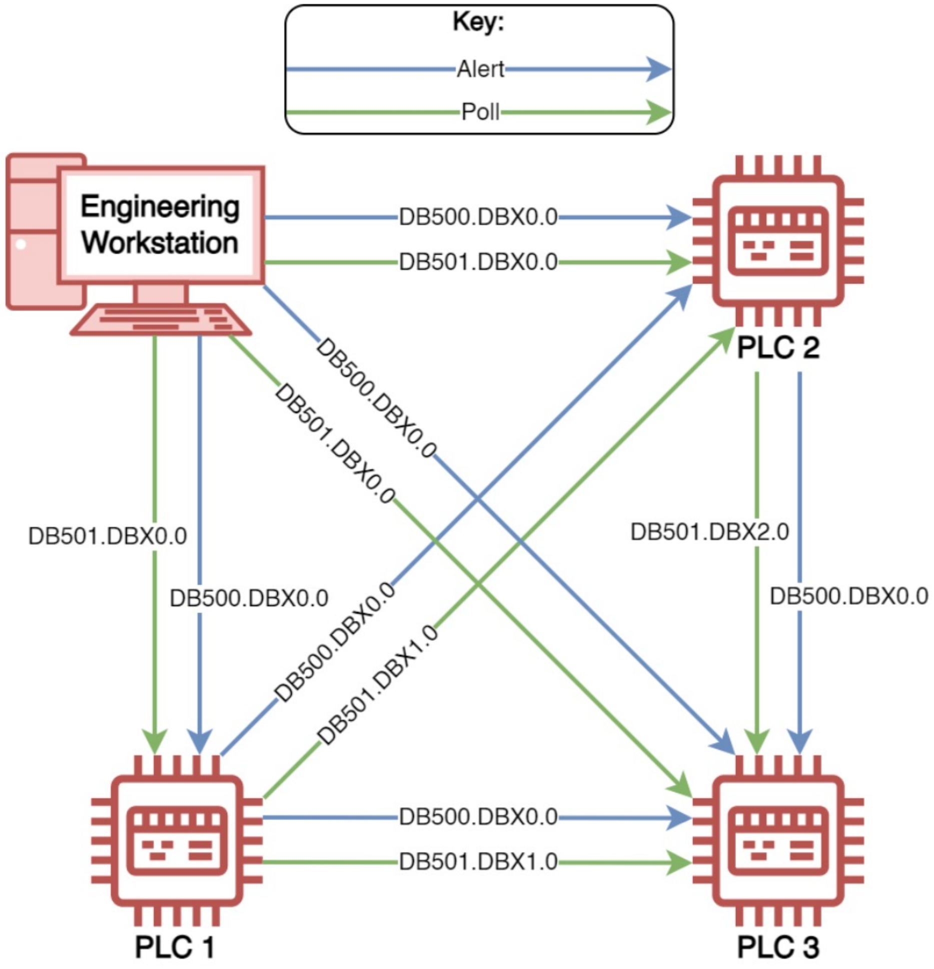


Fig. 7. DM-PLC's covert monitoring network example with 3 PLCs

Endpoint Protection

Endpoint Protection

- Most OT devices do not support agent installation
- Security logs might be available
- If agent can be used, it is safe to do so (maybe passive mode)

What’s next

Preventive Measures

- Train your engineers
- Network segmentation
- Access control
- Use jump hosts and self managed hosts
- Turn logging on

SOC Integration

- Asset Owner demand OT/ICS SOC
- SOC needs OT awareness & tooling
- Quick wins do not need OT protocol parsing

Outlook

Network security monitoring remains the only way to have visibility

- Full pcap for critical processes
- Netflow where full pcap is not possible

Simple and it works - “Old” OT Protocols revival

- Like ModbusTCP, IEC 60870-5-104

Thank you

Martin Scheu
martin@ics-cyber.ch