dtec.bw
JAHRESTAGUNG 2024

Security Considerations for IEEE 802.1 Time-Sensitive Networking in Converged Industrial Networks

Florian Fischer, Dominik Merli
Institut für innovative Sicherheit, Technische Hochschule Augsburg

TSN Basics

General:

- TSN: Time Sensitive Networking
- Origin: Audio-Video-Bridging (AVB)
- Issue using Ethernet for real time communication: Worst case latency not deterministic
- TSN is likely to replace traditional vendor specific fieldbuses e.g. EtherCAT, Profinet or Modbus-RTU.
- TSN is not a single communication stack, but a set of multiple IEEE 802.1 standards, partially not finalized

Goals of TSN:

- Deterministic communication via Ethernet
- Best Effort traffic on the same shared Medium
- Time synchronization within ns accuracy
- Jitter of cyclic real time traffic within us bounds

Converged Network and Security

- **Communication** is more and more converged to a single communication medium in Industrial Control System (ICS)
- Security Measure of using an air-gap is thus not feasible any more

- **Arguments for converged networking:**
  - **Flexible production** and increased productivity
  - **Cloud computing**, logging, predictive maintenance
  - **Cost reduction**

Motivation for this work: What about security?

- Technology TSN brings in new attack surface to OT networks
- Security plays no important role in TSN standards yet
- TSN might not be the first target for attackers
- Disturbance of TSN may have severe impact in OT domain: **Security considerations must be analyzed.**

General Threats

- Physical Tampering
- Man-in-the-Middle
- Stream Reservation Protocol Abuse
- Denial of Service
- Best-Effort Misuse
- Attacks based on PTP

Wireless Time Sensitive Networking threats:

- Jamming
- Sniffing
- Wardriving

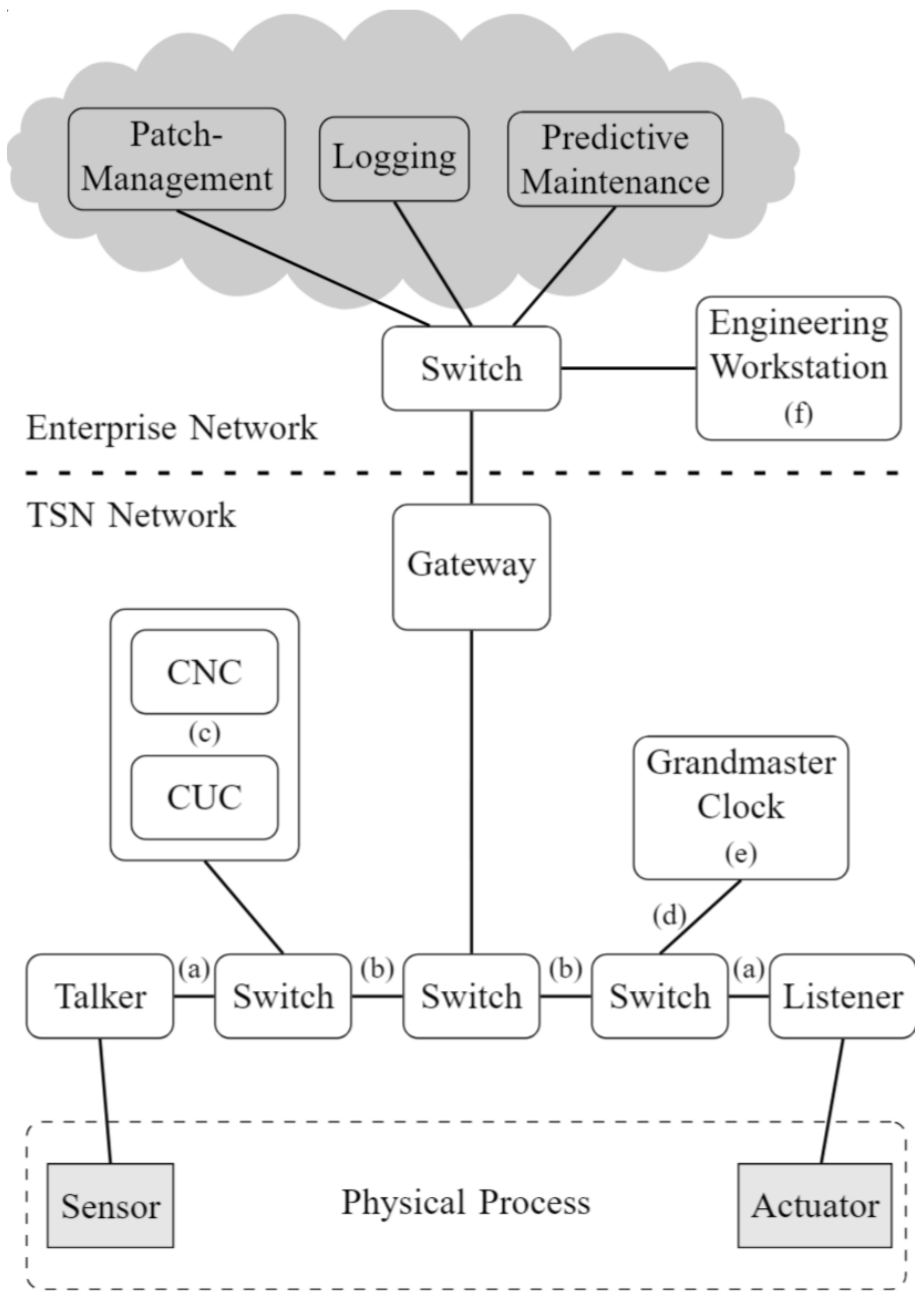

Fig. 1. General Industrial Control System Converged Network Setup using TSN

Considered Protection and Mitigation

Network Architecture according to

- Zones and conduits approach IEC 62443
- Segmentation of essential real-time data streams

Physical Security Measures

Physical tamper protection for core assets e.g. CNC/CUC
Measures should address the procurement process, initial commissioning, regular operation and maintenance windows of ICS

Cryptographic Measures

Protection of non-real-time management communication with TLS
MACSec for peer-to-peer protection Application Layer protection e.g. UADP in OPCUA-over-TSN

Network Filtering and Firewalls

Firewall implementation towards enterprise networks
IEEE 802.Qci Layer 2 filtering within TSN domain

Further Security Measures

Proper configuration as part of a defense-in-depth approach
Intrusion Detection and Prevention Systems
PTP specific security measures

References

This publication has the following DOI:
https://doi.org/10.1109/ICECCME55909.2022.9988000

Technische Hochschule Augsburg | THA_innos Institut für innovative Sicherheit

unibw.de
hsu-hh.de
dtecbw.de

DS2CCP
Digital Sensor-2-Cloud Campus-Platform

gefördert durch
dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU