Brandenburgische Technische Universität Cottbus

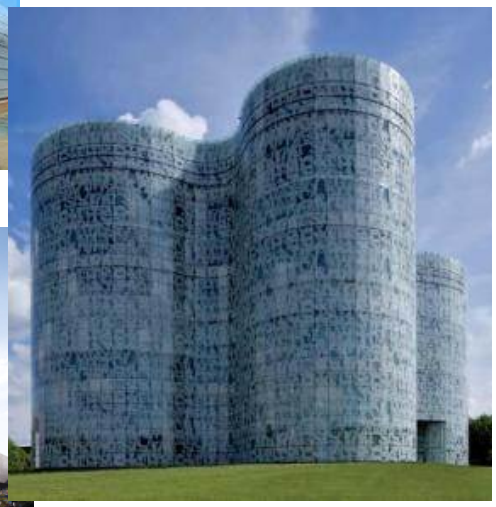
Verwundbarkeitsanalyse des Industrial-Ethernet Protokolls PROFINET

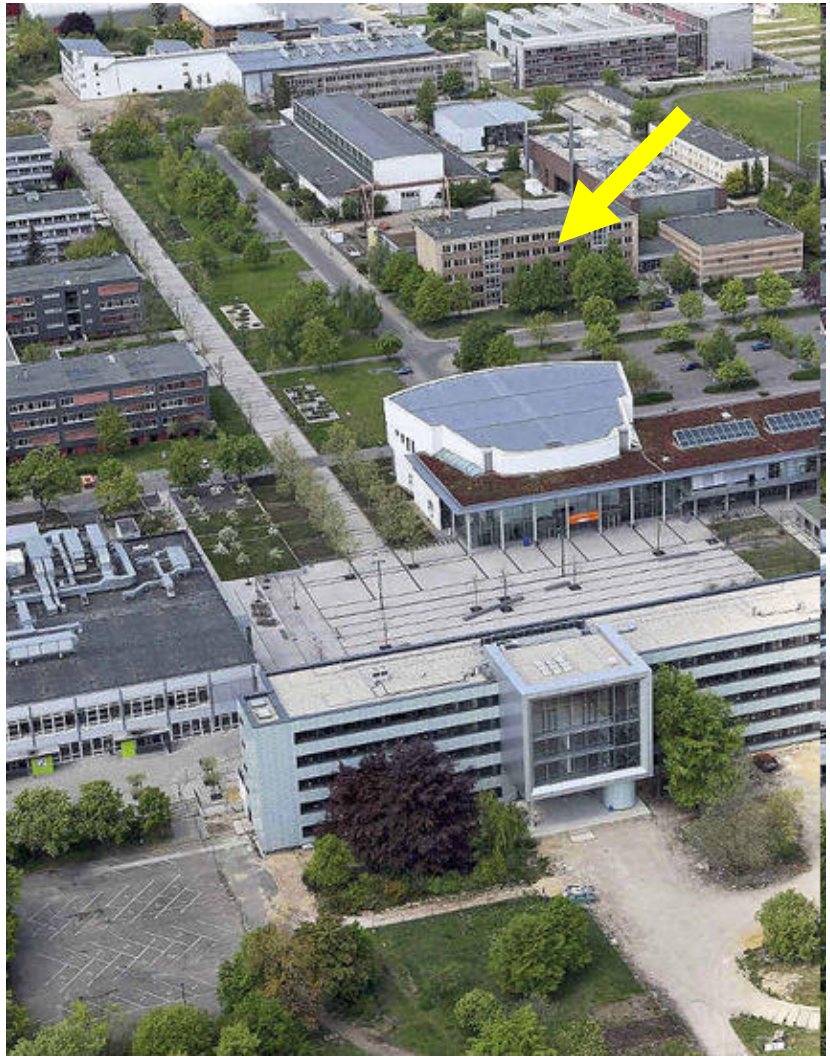
Andreas Paul

Brandenburgische Technische Universität Cottbus
Lehrstuhl Rechnernetze und Kommunikationssysteme

SPRING 7
GI SIDAR Graduierten-Workshop über Reaktive Sicherheit
Berlin 05-06.07 2012

BTU Cottbus und Lehrstuhl RNKS

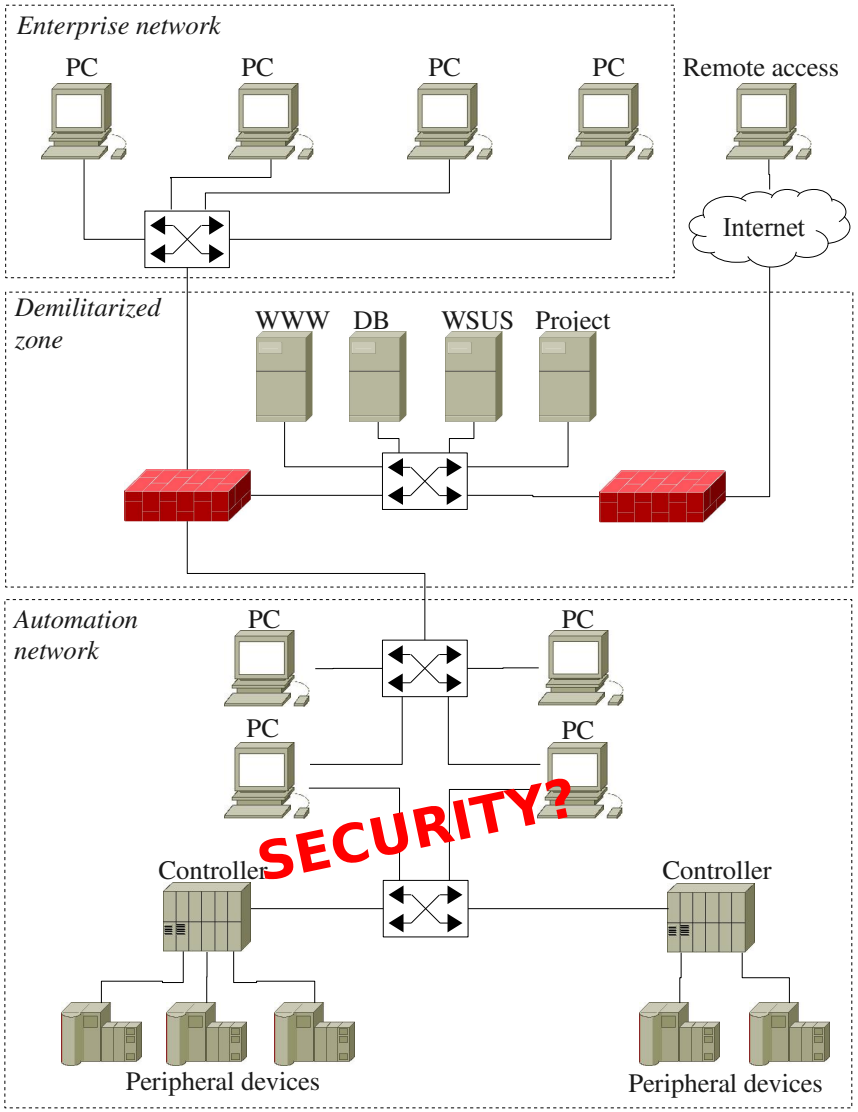




Inhaltliche Gliederung

- **Einleitung**
  - SCADA-Architektur
  - Einordnung in aktuelle Arbeiten
- **PROFINET**
  - Prinzip
  - Protokollabläufe
  - Angriffsszenarien
- **Zusammenfassung**

SCADA-Architektur (Beispiel)



- **Automation network**
  - **Prozessleitebene**
    - Planung, Visualisierung + Beobachtung von Prozessen
    - Archivierung von Messwerten
  - **Steuerungs- und Feldebene**
    - Steuerung + Regelung von Prozessen
    - Schnittstelle zum Prozess über I/O Signale
  - **Anforderungen eingesetzter Kommunikationstechnologien**
    - hohe Ausfallsicherheit → Verfügbarkeit!
    - Echtzeitfähigkeit

Verteiltes IDS zum Schutz von SCADA-Systemen

分布式

- **Analysekomponente: Vortrag Franka Schuster!**
- **Simulationsumgebung**

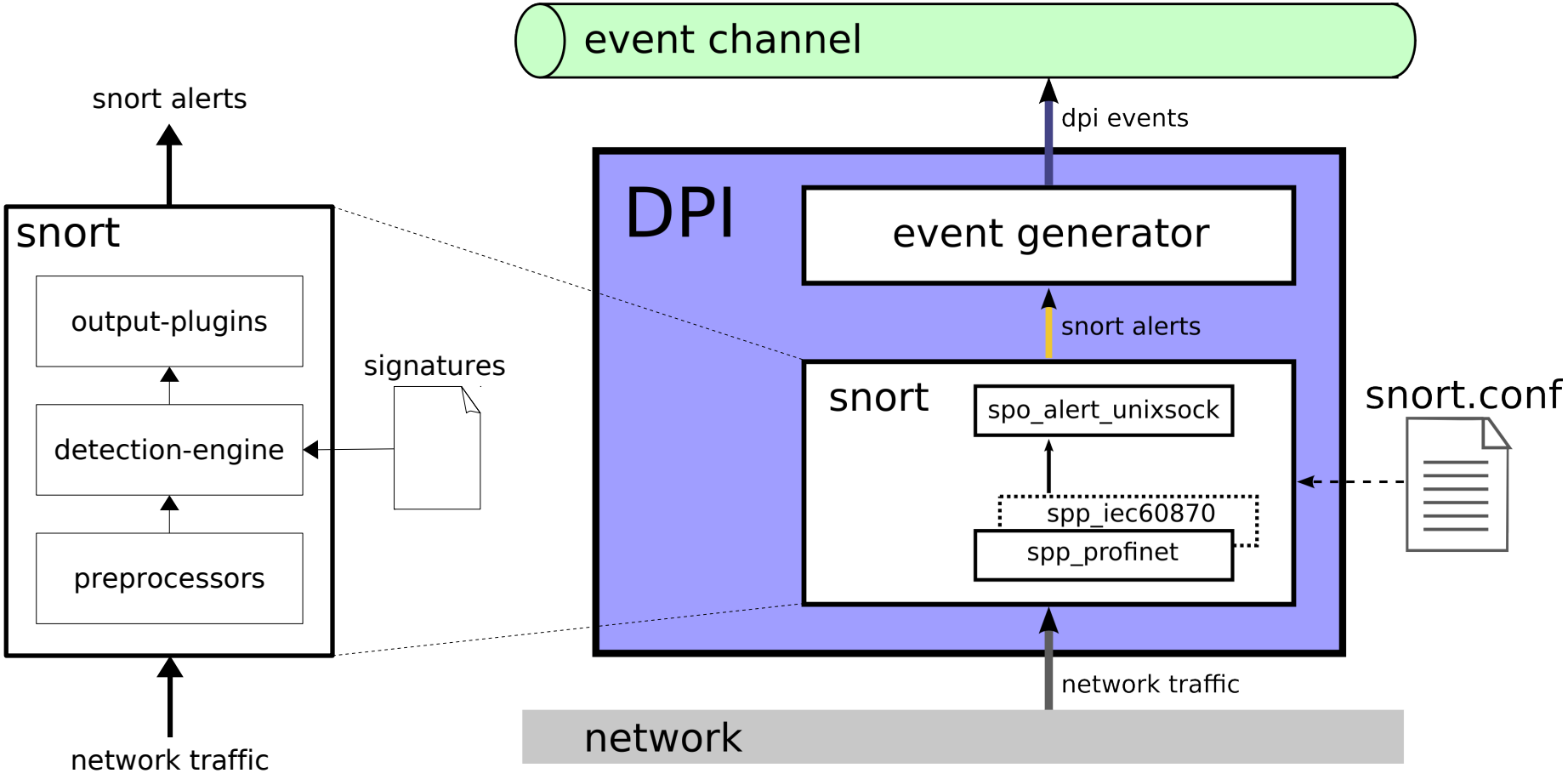
仿真环境

基础设施

  - Modellierung von SCADA-Infrastrukturen (Komponenten + Verhalten)
  - Generierung Protokoll-konformer Nachrichten
  - Simulation von Angriffsszenarien
- **Deep Packet Inspection**
  - Datenanalyse basiert auf dekodierte Informationen der Protokollfelder

  → “DPI-Komponente”

DPI-Komponente 1/2



DPI-Komponente 2/2

- **spp_profinet:** Snort-Präprozessor
  - Dekodierung von Profinet-Frames
  - Generierung von Snort-Alarmen
- **spo_alert_unixsock:** Snort-Ausgabe-Modul
  - schreibt Alarme in Unix Domain Socket
- **snort.conf:** Snort-Konfigurationsdatei
  - Aktivierung und Konfiguration von Präprozessoren:

    ```
    preprocessor profinet: alert { dcp rt_unicast alarm_high }
    ```
  - Aktivierung des Ausgabe-Moduls:

    ```
    output alert_unixsock
    ```
- **event generator**
  - Generierung von DPI-Events
  - Weiterleitung der Events an event channel (publish)

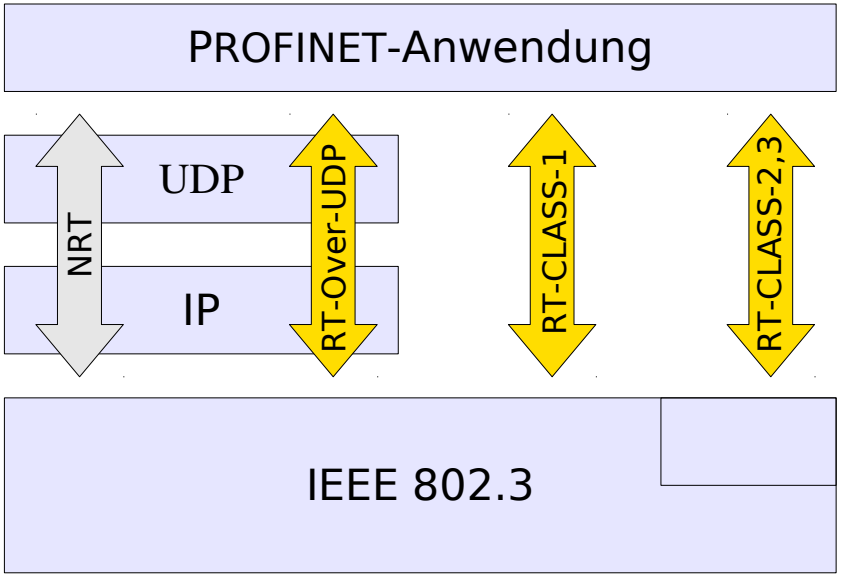
PROFINET: Einleitung

介绍

实时

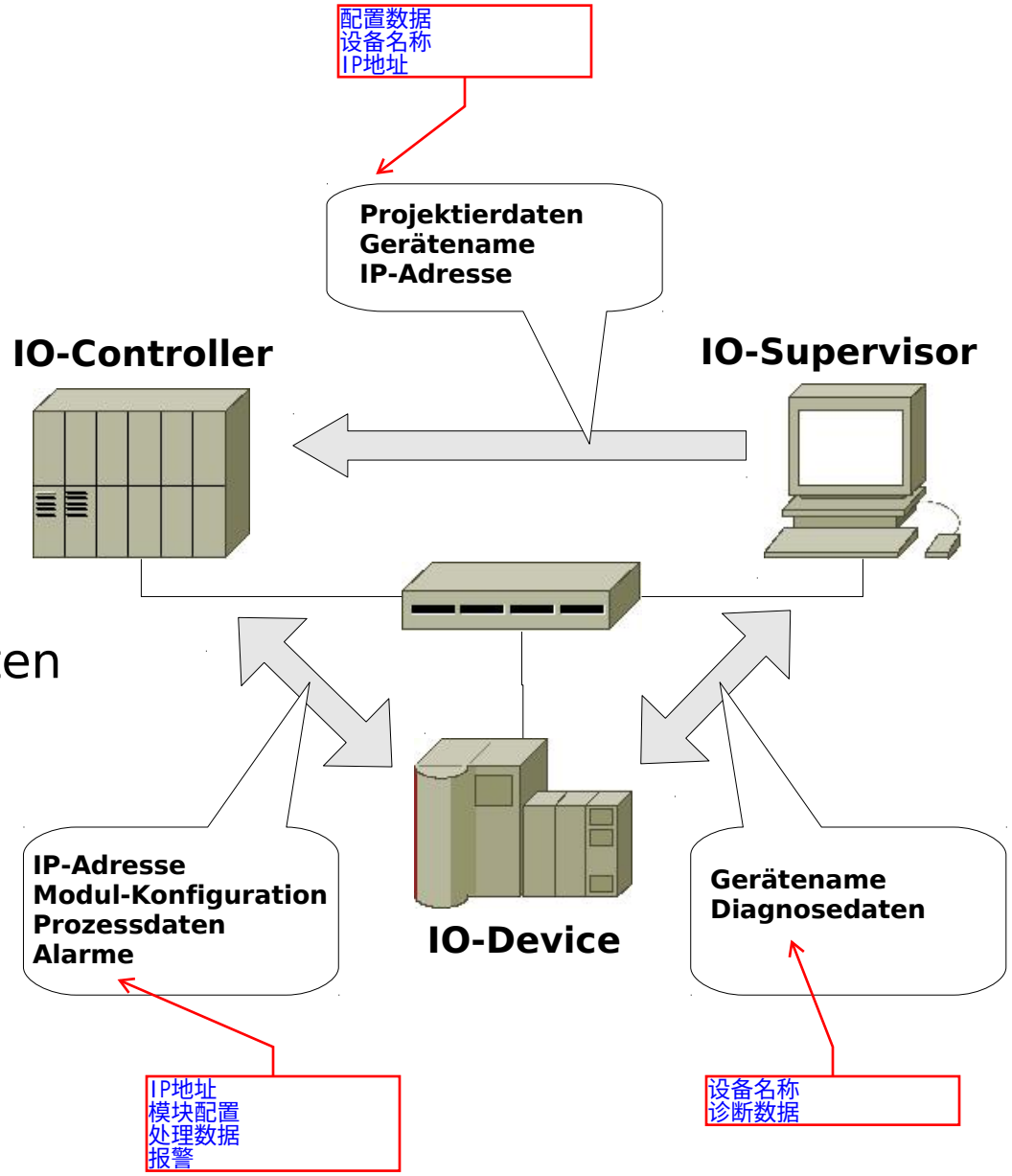
低循环周期 低抖动

- **Industrial Ethernet**
  - Echtzeitfähiges Ethernet: geringe Zykluszeiten + geringer Jitter
  - weitere Ansätze: SERCOS III, ETHERNET/IP, Modbus/TCP, ETHERCAT, ...
- **Realisierung der Echtzeitfähigkeit**
  - **RT-Over-UDP:**
    - geplante Kommunikation
    - VLAN-Priorisierung (IEEE 802.1Q)
  - **RT-Klasse 1:**
    - Kommunikation innerhalb eines Subnetzes
  - **RT-Klasse 2,3:**
    - Zeitsynchronisation
    - Eingriff in MAC-Layer



PROFINET: Prinzip

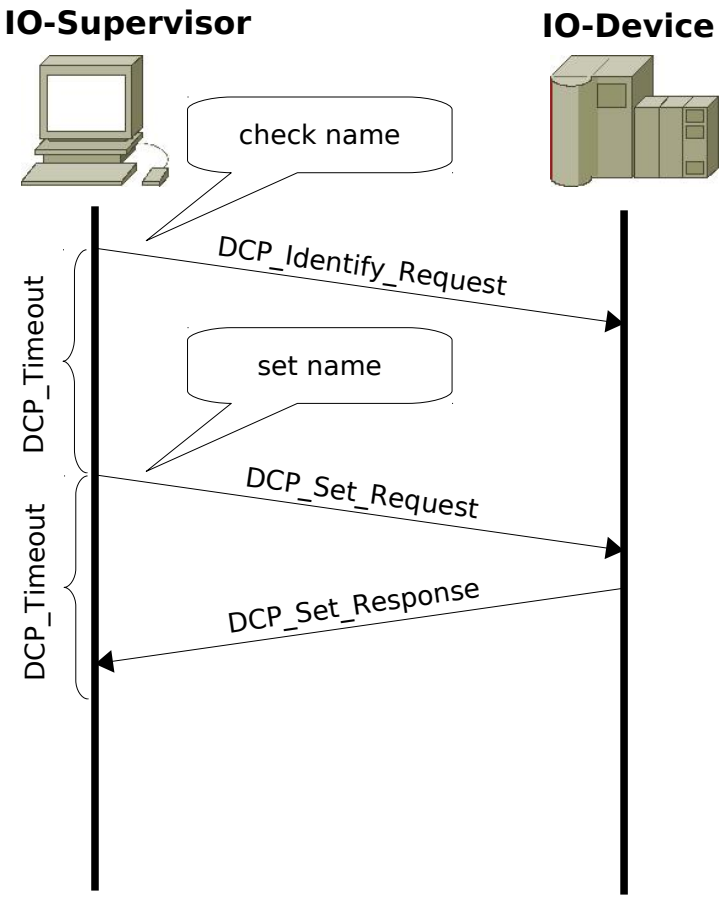
- **Geräterollen**
  - IO-Supervisor
  - IO-Controller
  - IO-Device
- **Schritte**
  1. Projektierung
  2. Übertragung der Projektierdaten
  3. Initialisierung
     - Vergabe des Gerätenamens
     - Vergabe der IP-Adresse
  4. Systemhochlauf
  5. Betriebsphase
     - zyklisch: Prozessdaten
     - azyklisch: Diagnose, Alarm



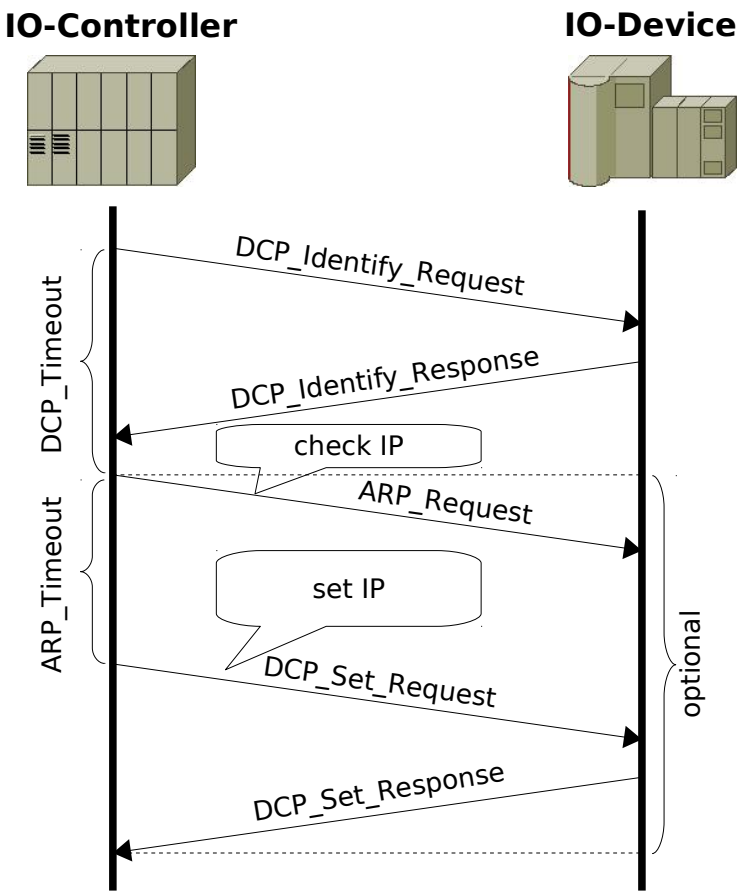
PROFINET: Protokollabläufe 1/2

Initialisierung:

Vergabe des Gerätenamens



Vergabe der IP-Adresse

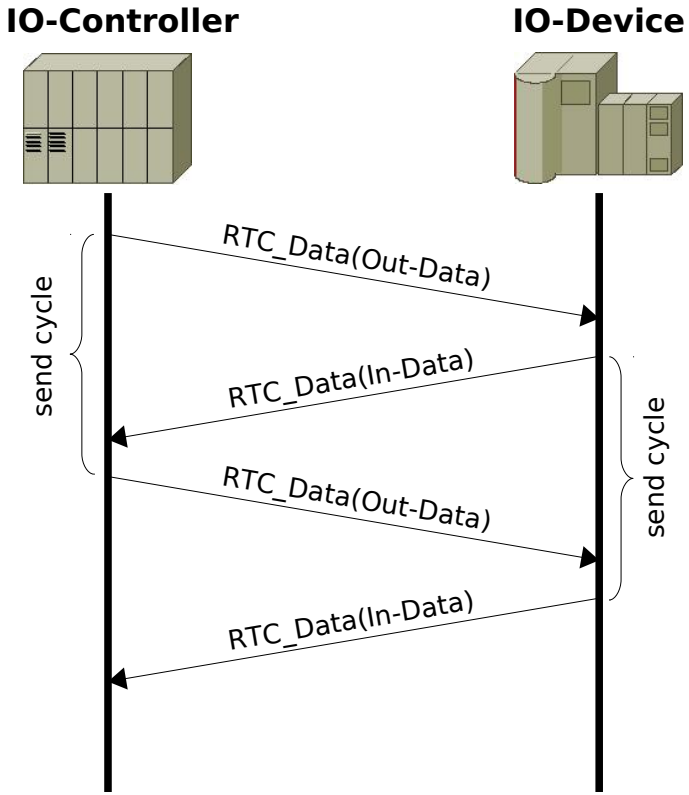


Profinet协议的脆弱性评估

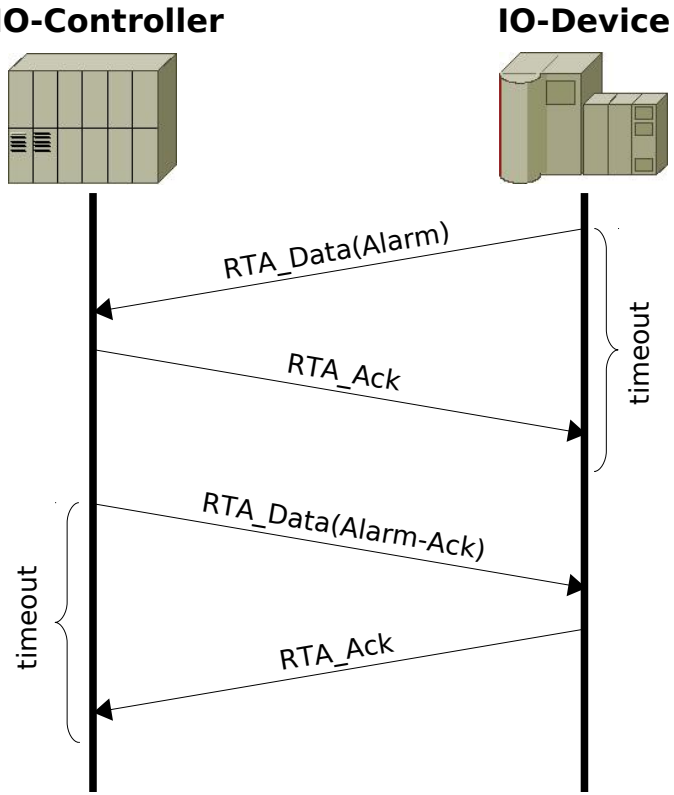
PROFINET: Protokollabläufe 2/2

Betriebsphase:

zyklische Datenübertragung



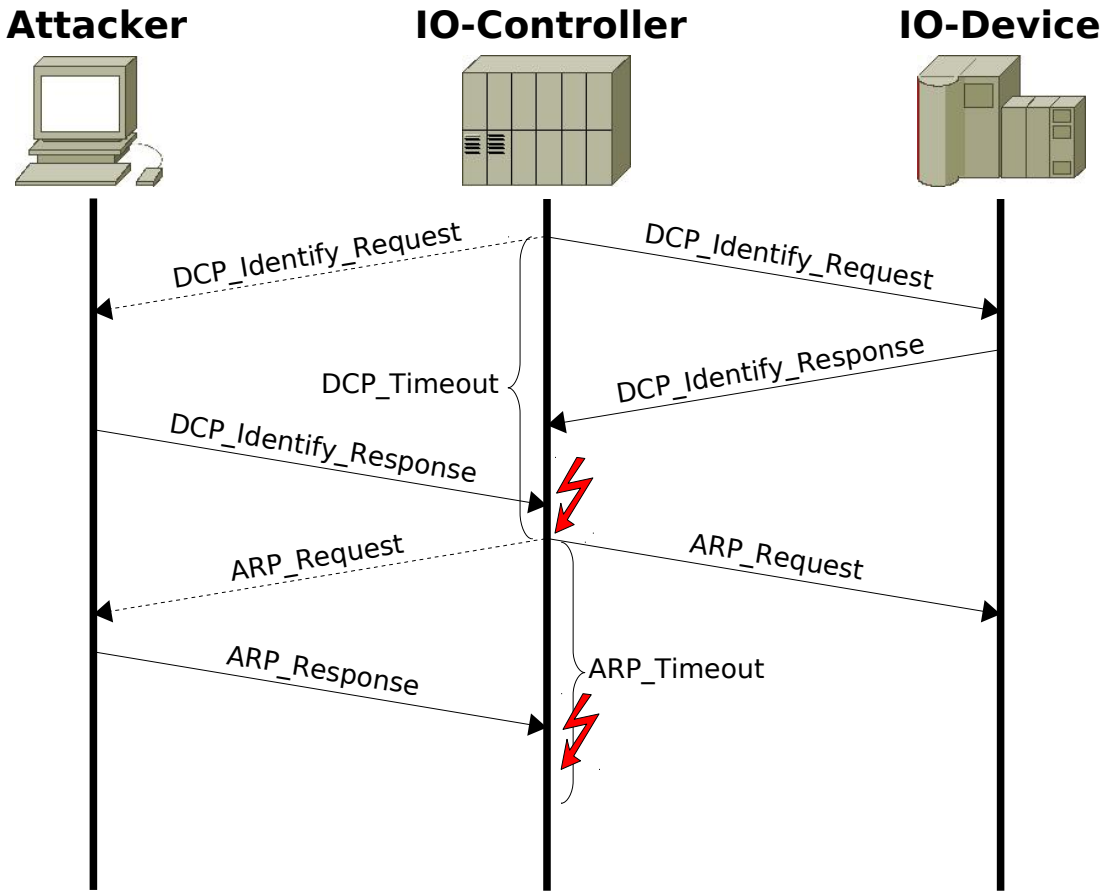
azyklische Datenübertragung



PROFINET: Angriffsszenarien 1/2

Denial-Of-Service:

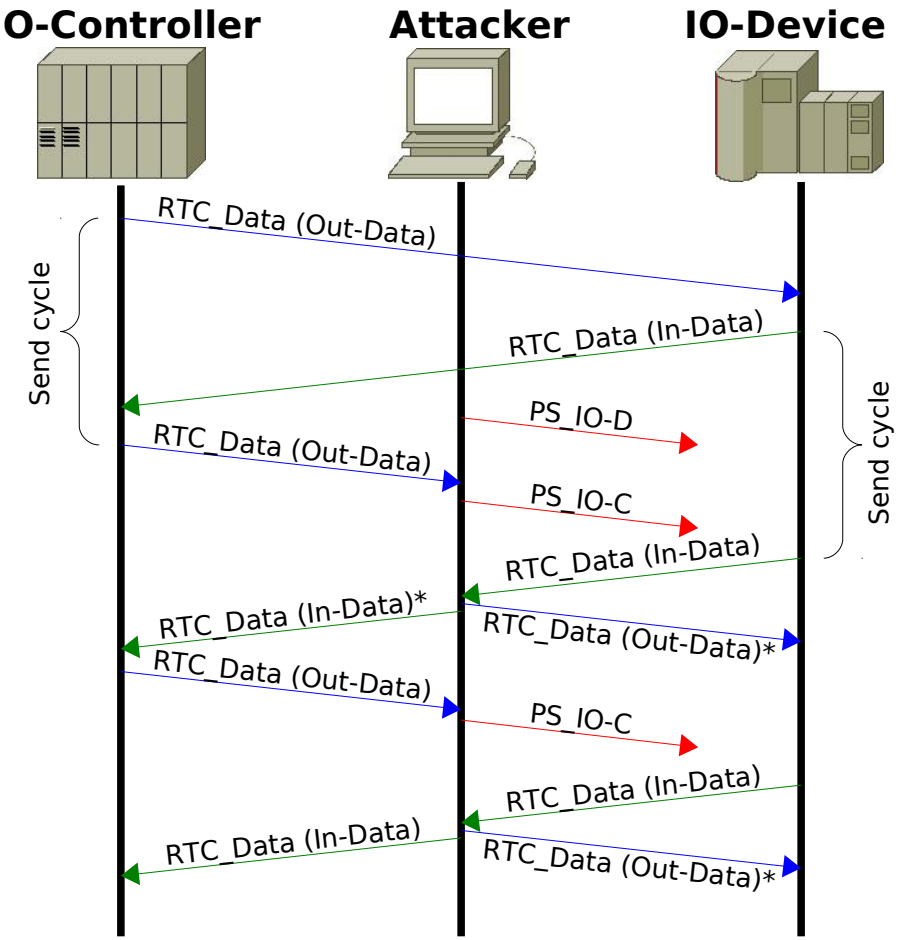
Initialisierung: Vergabe der IP-Adresse



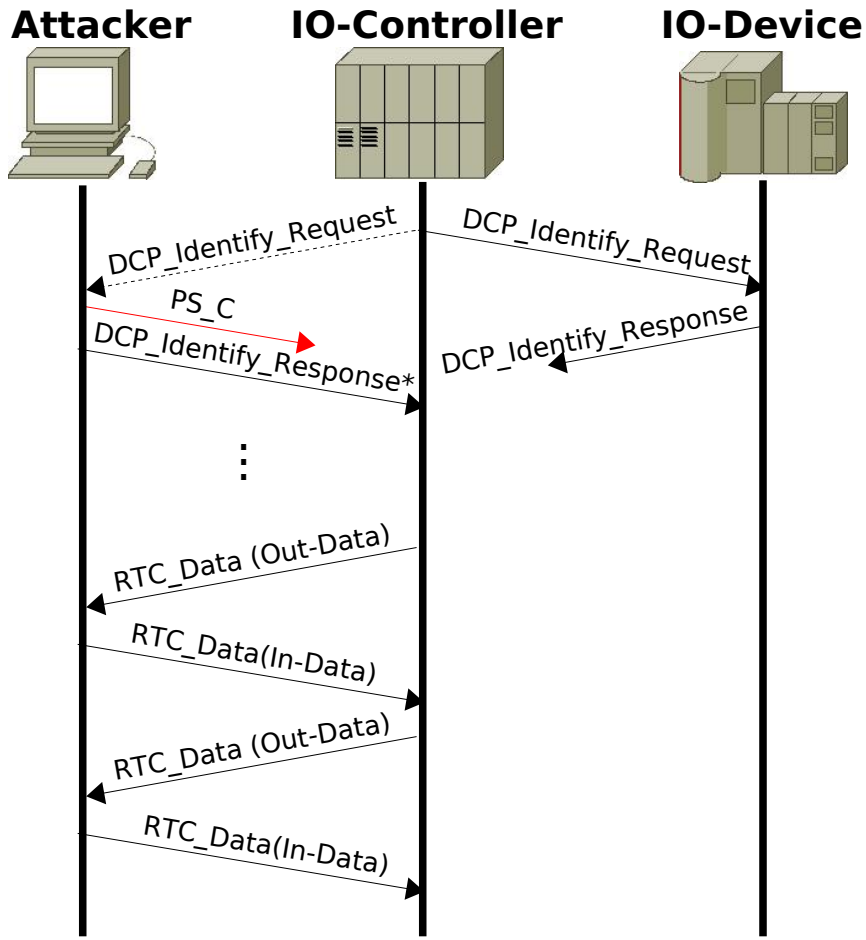
PROFINET: Angriffsszenarien 2/2

Man-In-The-Middle:

Betriebsphase: zyklische Datenübertragung



Initialisierung: Vergabe der IP-Adresse



Zusammenfassung

- **Automatisierungsnetz (spez. Feldbus-Systeme)**
  - Anforderungen stehen mit denen zur Gewährleistung klassischer IT-Schutzziele in Konkurrenz
  - fehlende Mechanismen zur Sicherung einer *authentifizierten Kommunikation* + Wahrung der *Datenintegrität*

  → abgeleitete Angriffe können auf andere Technologien übertragen werden!

- **Ausblick: Schutz des Automatisierungsnetzes**
  - Ziel: Erweiterung der Sicherheit von SCADA-Systemen unter Berücksichtigung gegebener Anforderungen

  → Franka Schuster: “Intrusion-Detection für Automatisierungstechnik”

Vielen Dank für Ihre Aufmerksamkeit!

Fragen? Anmerkungen?