Towards the Protection of Industrial Control Systems – Conclusions of a Vulnerability Analysis of Profinet IO

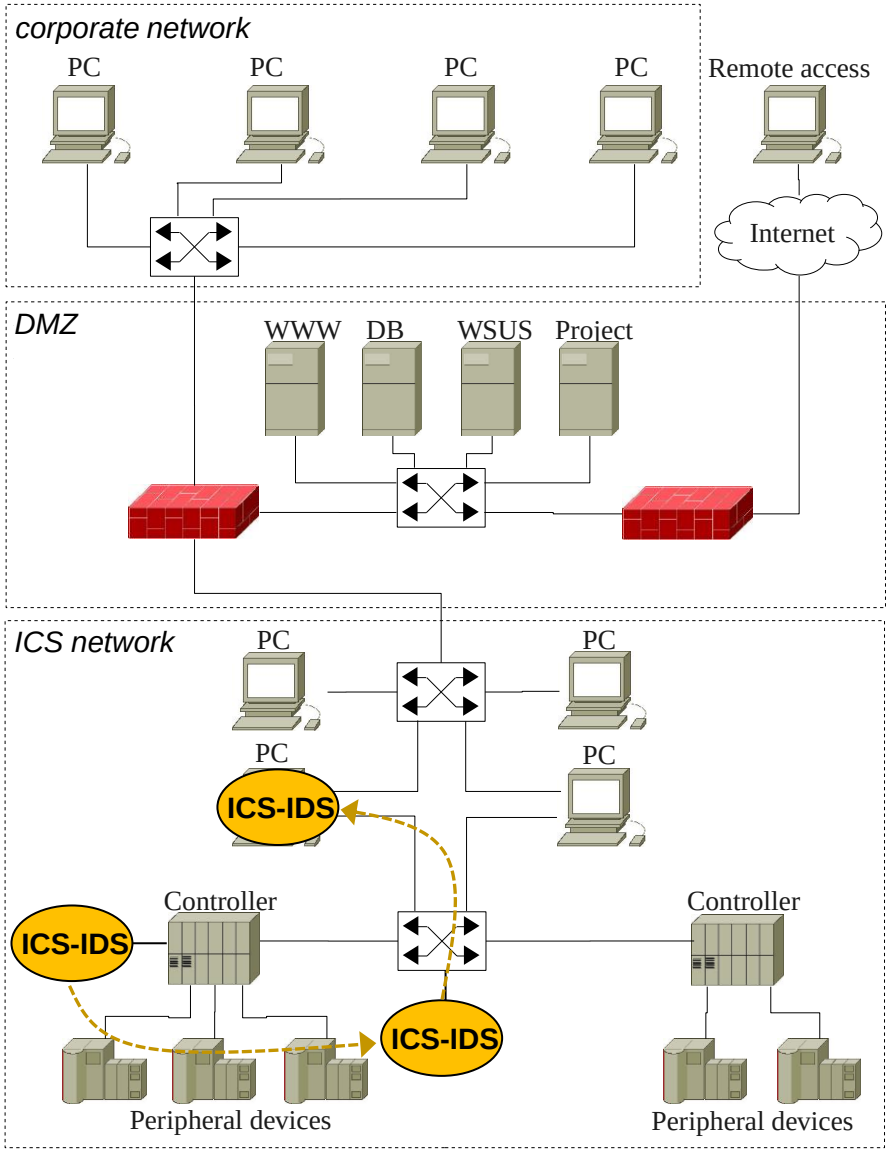
Andreas Paul, Franka Schuster, Hartmut König

19.07.2013

Brandenburg University of Technology Cottbus,
Cottbus, Germany

10th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2013)

Introduction: Industrial Control Systems (ICS)

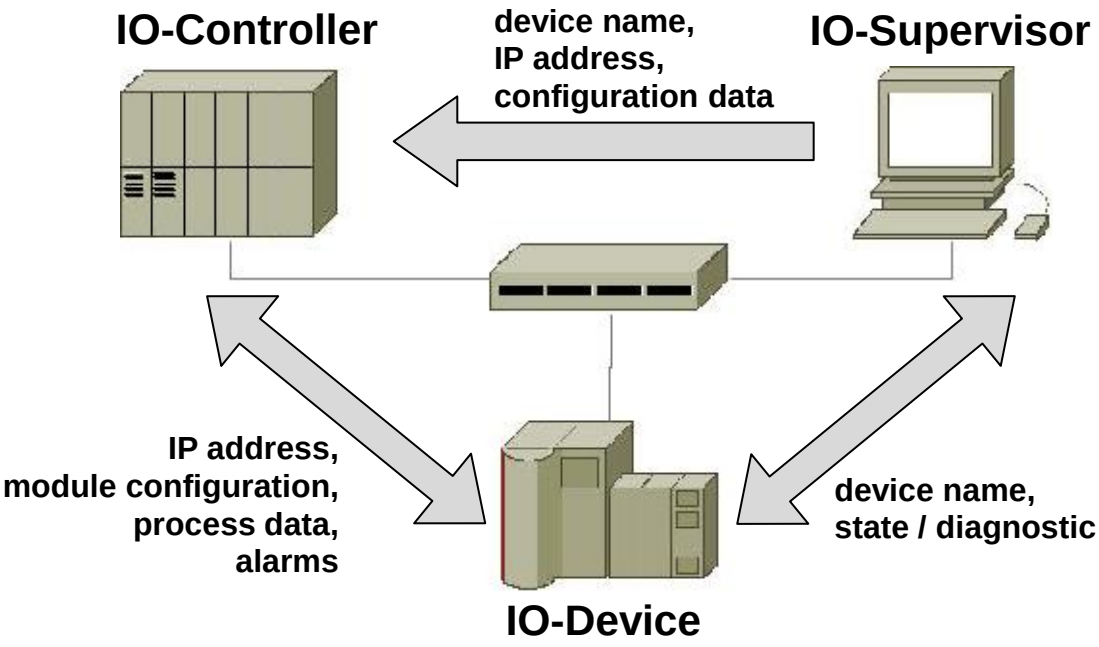


- **ICS network**
  - heterogeneous devices
  - special requirements on information technologies
    - reliability and availability
    - real-time capability
  - problem: missing security measures
- **Intrusion Detection for ICS networks**
  - passive analysis of Ethernet-based network traffic
  - analysis technique: anomaly detection
  - supporting industrial communication protocols

PROFINET IO: Basics

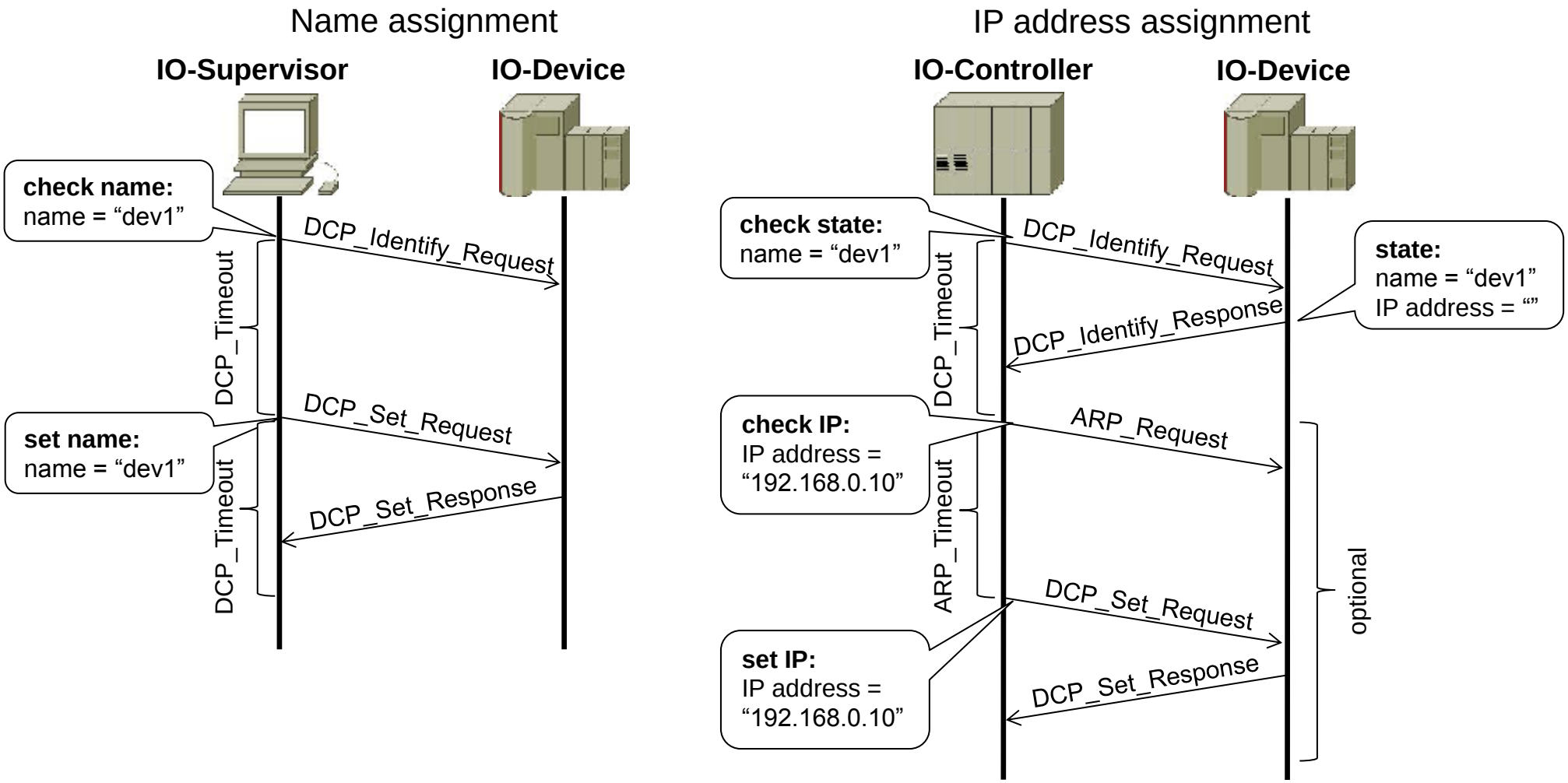
- **Device roles:**
  - IO-Supervisor: engineering station
  - IO-Controller: PLC
  - IO-Device: peripheral devices

- **From configuration to data transmission:**
  1. configuration
  2. transmission of configuration data
  3. name assignment
  4. IP address assignment
  5. set up of application relation
  6. data transmission



PROFINET IO: Protocol sequences (1/2)

System Start-Up

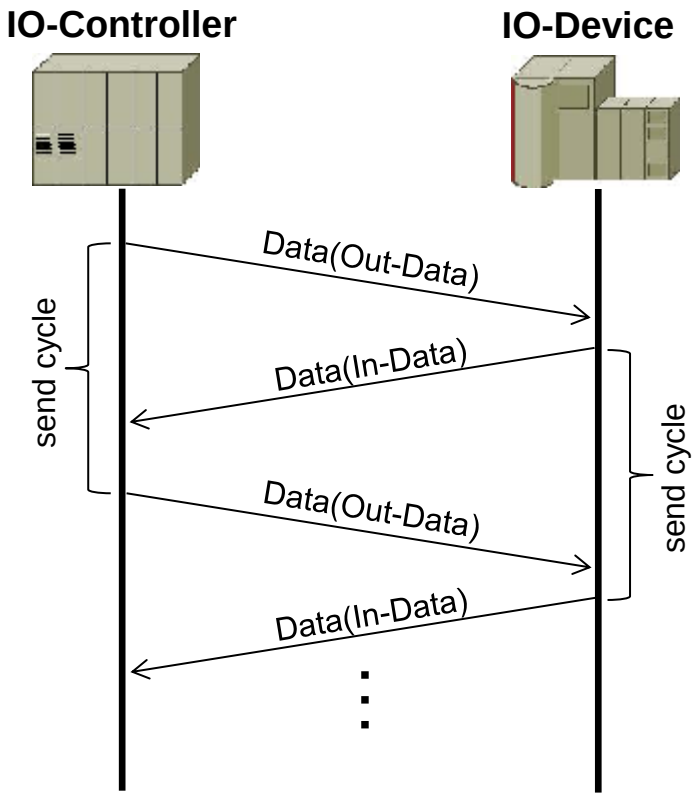


PROFINET IO: Protocol sequences (2/2)

Operating stage

- **acyclic data transfer**
  - request / response
  - alarms, diagnostics, reconfiguration
- **cyclic data transfer**
  - provider / consumer
  - *Out-Data:* process control, process regulation
  - *In-Data:* process data

Cyclic data transfer



PROFINET IO: Protocol-specific attacks (1/4)

» Attack scenario

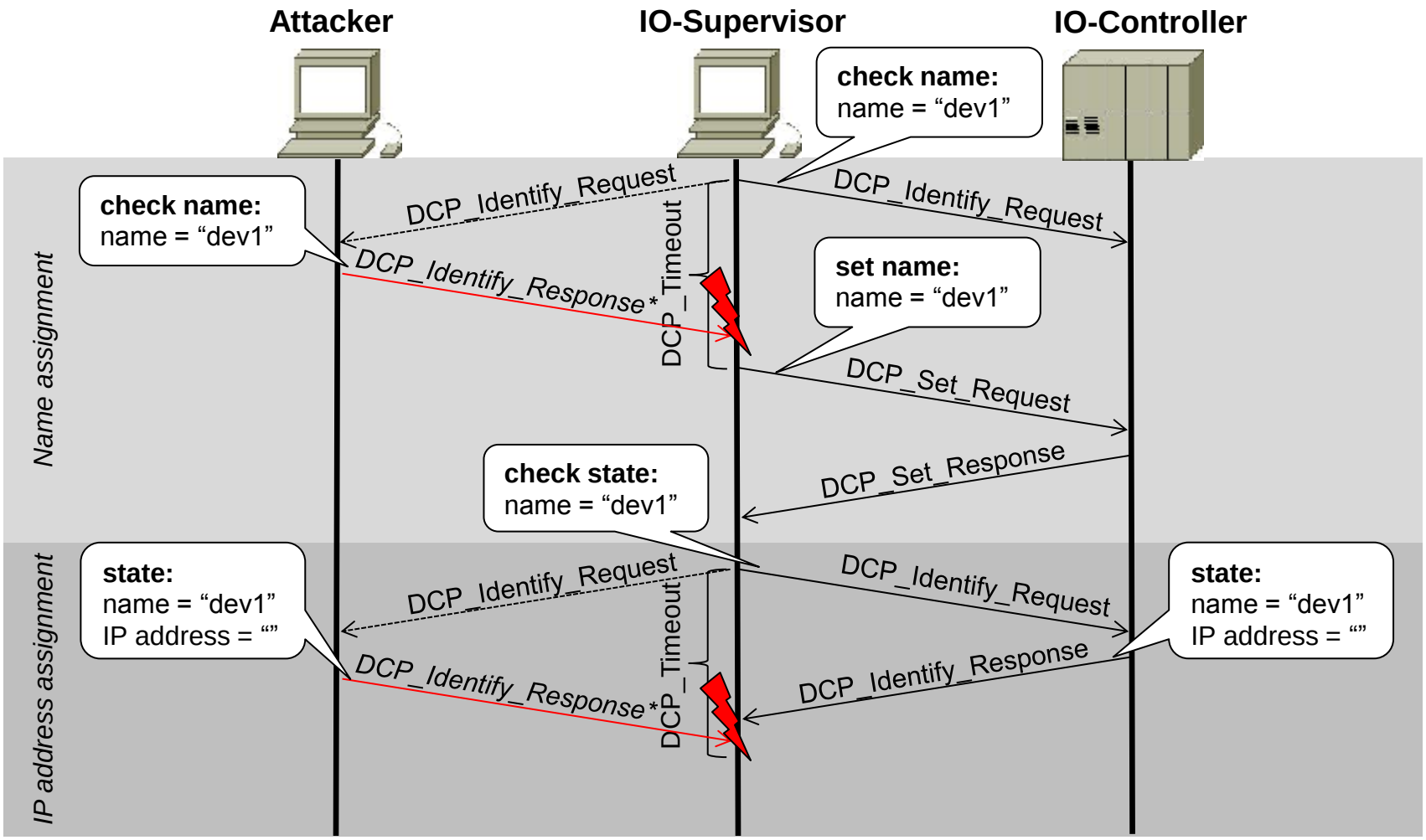
- attacker: compromised PROFINET IO device or additional network device
- performs attacks by interfering regular protocol sequences
- requirement: knowledge about network topology
  - *DCP:* device polling via *DCP_Identify_All_Request*
  - *LLDP/SNMP:* collecting device and topology information via *SNMP*

» Attack classification

	Denial-of-Service	Man-in-the-Middle
Device name assignment	x	
IP address assignment	x	x
Cyclic data transfer		x

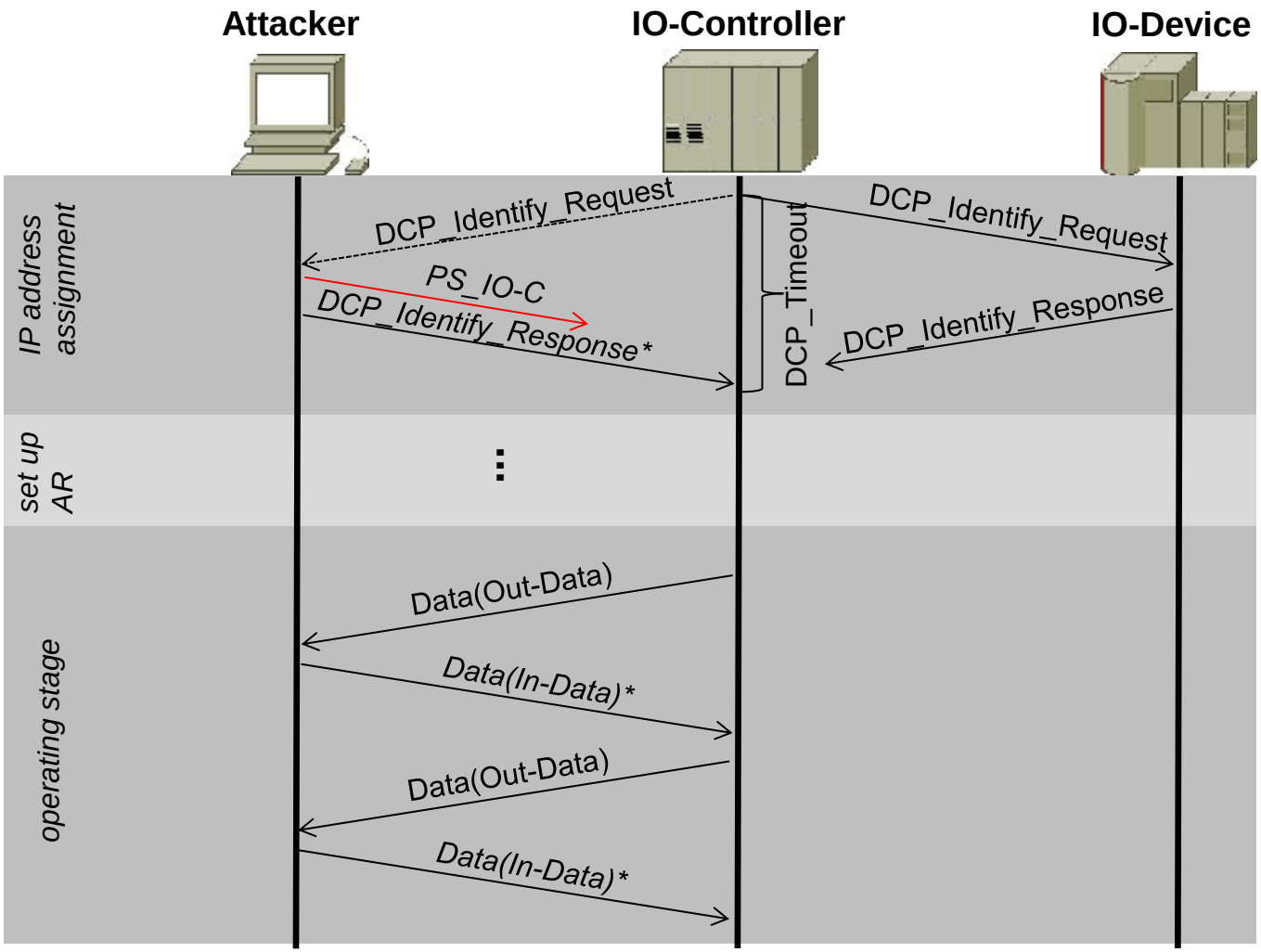
PROFINET IO: Protocol-specific attacks (2/4)

Denial-of-Service



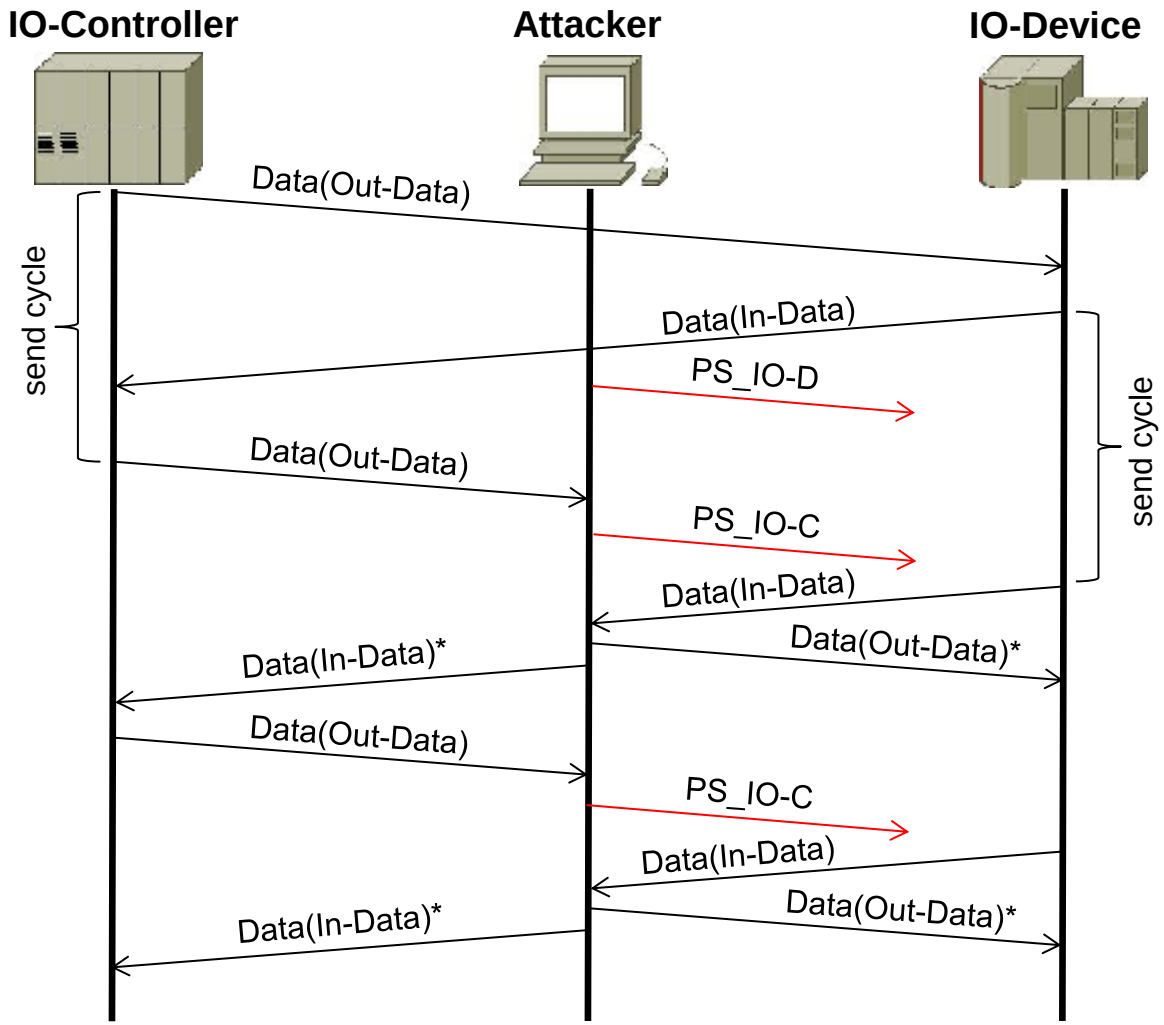
PROFINET IO: Protocol-specific attacks (3/4)

Man-in-the-Middle: IP address assignment



PROFINET IO: Protocol-specific attacks (4/4)

Man-in-the-Middle: cyclic data transfer



Intrusion Detection for Industrial Control Systems (1/4)

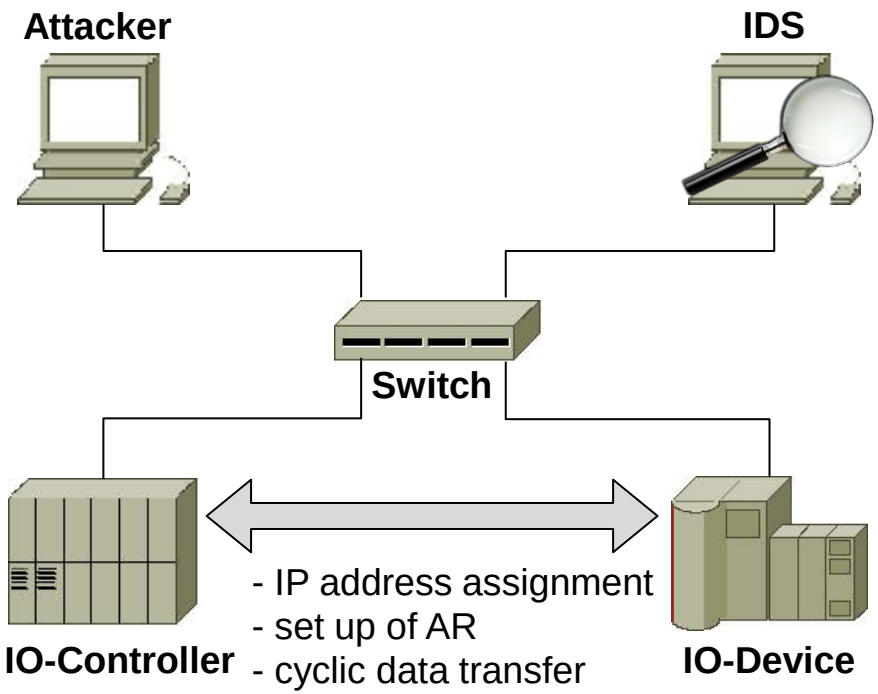
Classification

- **Information source**
  - *host-based:* analysis of data acquired from hosts (e. g. system calls)
    → requires additional resources of the hosts to be protected
  - *network-based:* analysis of network traffic (packet header, payload)
    → enables passive analysis

- **Analysis concept**
  - *misuse detection:* detection of **known attacks** described by patterns
    → requires detailed knowledge about attack and protocol functionality
  - *anomaly detection:* detection of **deviations** from model of normal behavior
    → promising: high degree of traffic homogeneity within ICS networks

Intrusion Detection for Industrial Control Systems (2/4)

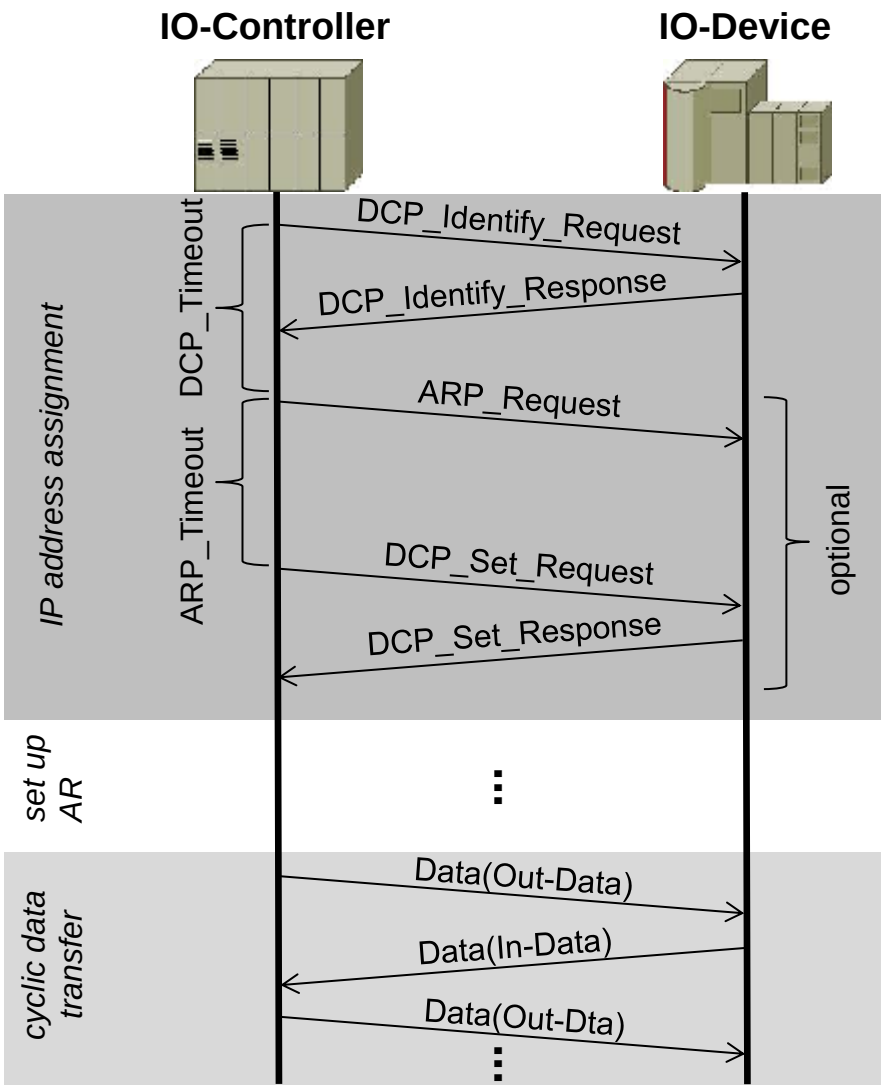
Attack scenario



- **IO-Controller / IO-Device**
  - performing regular system start-up and cyclic data transfer
- **Attacker**
  - interferes protocol sequences
  1. Denial-of-Service attack on IP address assignment
  2. Man-in-the-Middle attack on IP address assignment
- **IDS**
  - full access to the network traffic
  - learning vs. attack detection

Intrusion Detection for Industrial Control Systems (3/4)

Learning normal system behavior

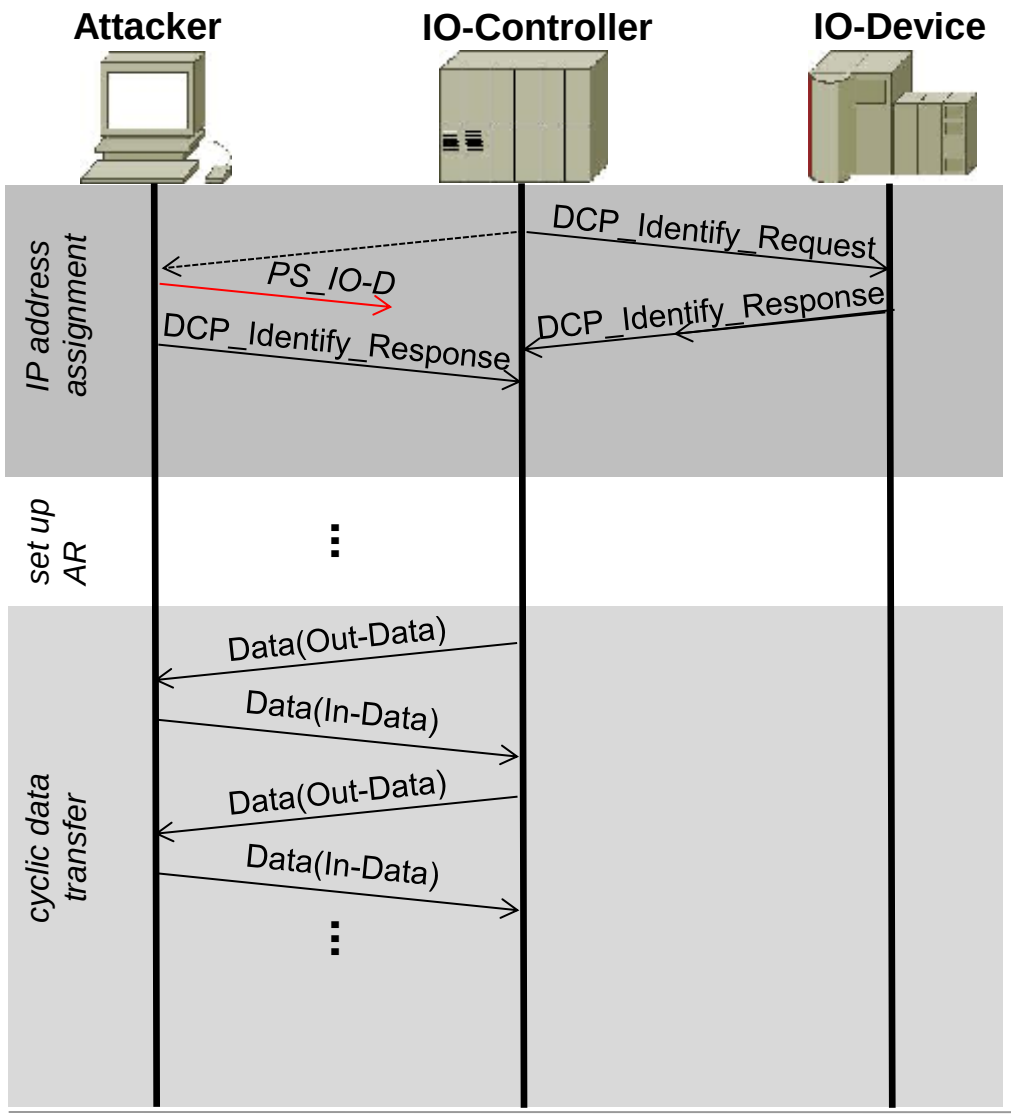


Message type	Event Source	Destination
1	IO-C	IO-D
2	IO-D	IO-C
3	IO-C	IO-D
4	IO-D	IO-D
6	IO-D	IO-C
5	IO-C	IO-D
6	IO-D	IO-C
5	IO-C	IO-D

Model of normality Set of 2-grams
(1,2) (2,3) (3,4) (4,…) (…,5) (5,6) (6,5) (2,…)

Intrusion Detection for Industrial Control Systems (4/4)

Attack detection

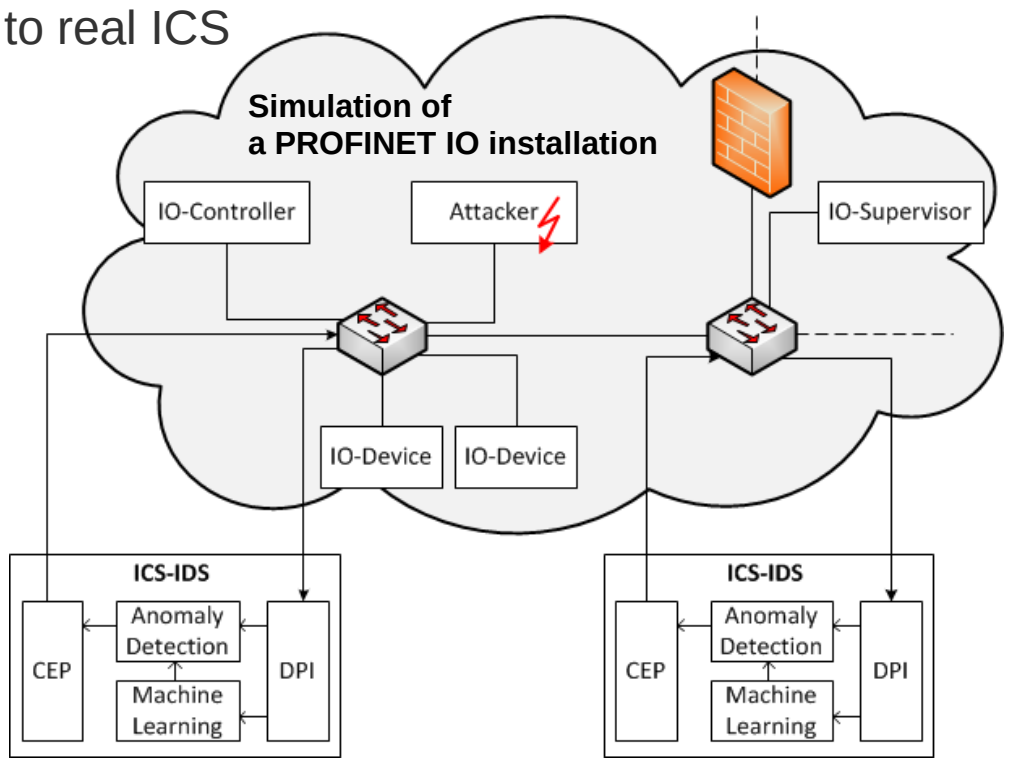


Message type	Event Source	Destination
1	IO-C	IO-D
2	IO-D	IO-C
2	IO-D	IO-C
...		
5	IO-C	IO-D
6	IO-D	IO-C
5	IO-C	IO-D
6	IO-D	IO-C

Model of normality Set of 2-grams
(1,2) (2,3) (3,4) (4,…) (…,5) (5,6) (6,5) (2,…)

Final Remarks

- **Security issues within ICS networks**
  - lack of measures to provide authorized communication + ensuring data integrity
  - Intrusion Detection is a promising measure to enhance ICS security
- **Simulation-based PROFINET IO network**
  - problem: missing/restricted access to real ICS
  - traffic generation
    - *regular protocol sequences:* learning normal behavior
    - *attack simulation:* IDS evaluation
  - IDS integration



Thank you for your attention!

Questions? Remarks?