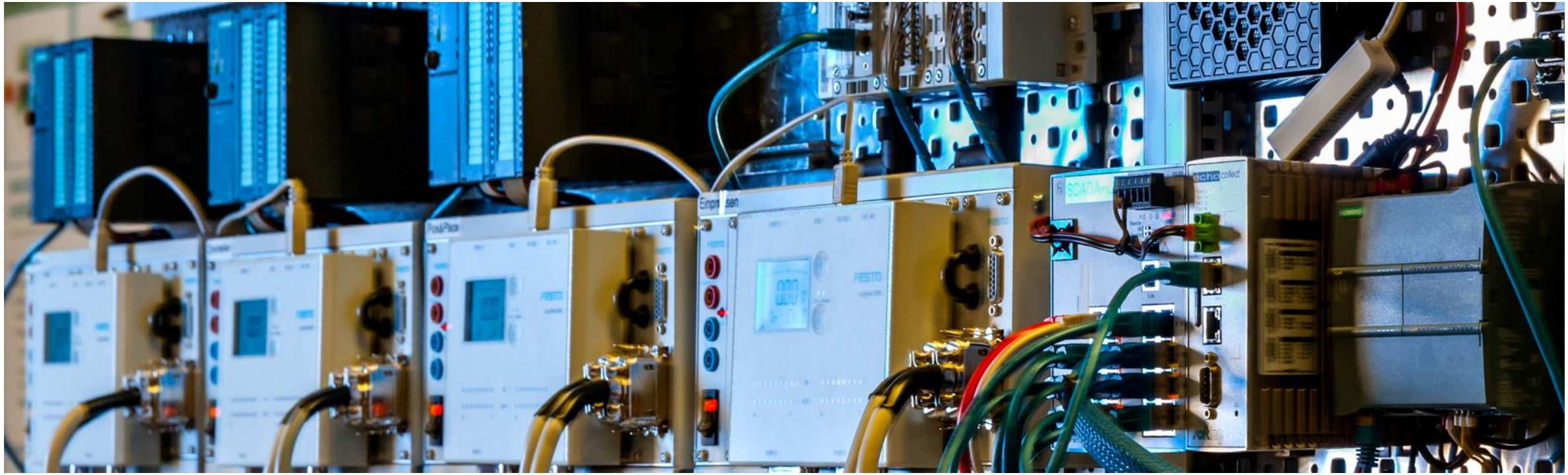
SECURITY IN INDUSTRIAL ENVIRONMENTS

Anne Borcherding, MSc

11.03.2021

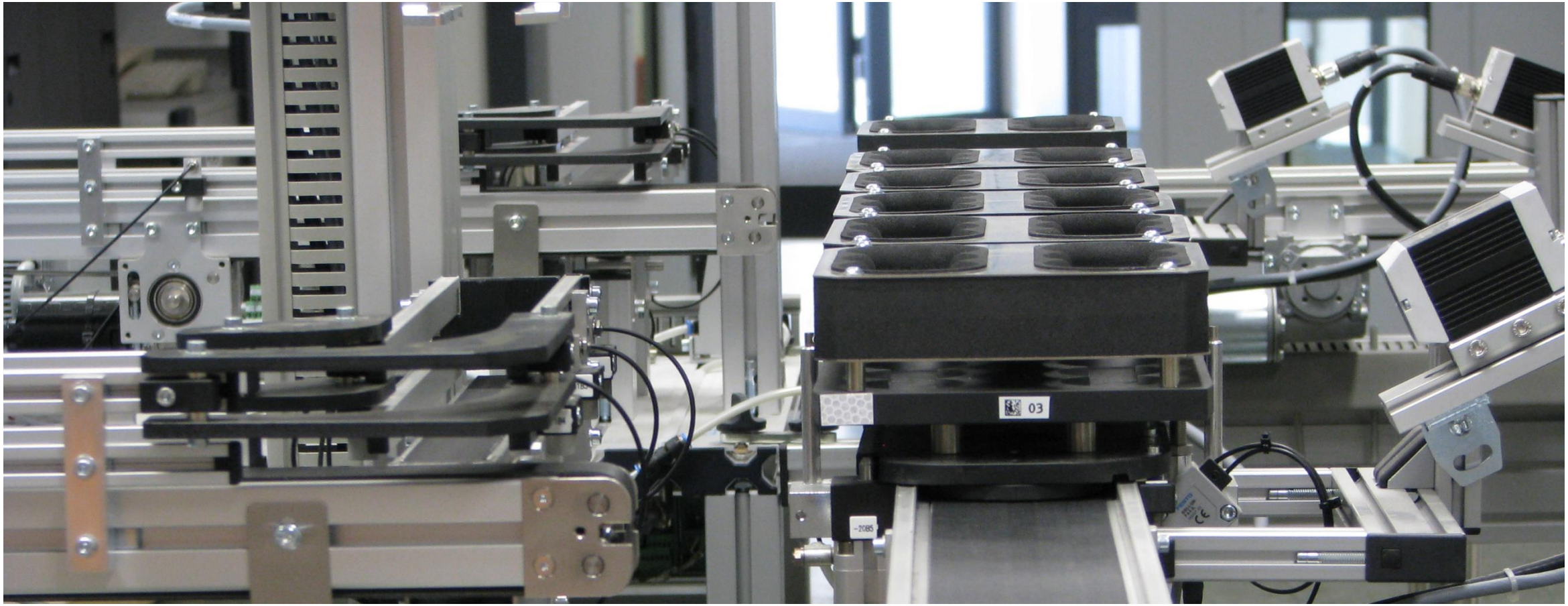


Fraunhofer IOSB

OBJECTIVE

- Awareness for security in industrial environments
- Teaser for different techniques to improve the security

INDUSTRIAL SECURITY



Industry 4.0

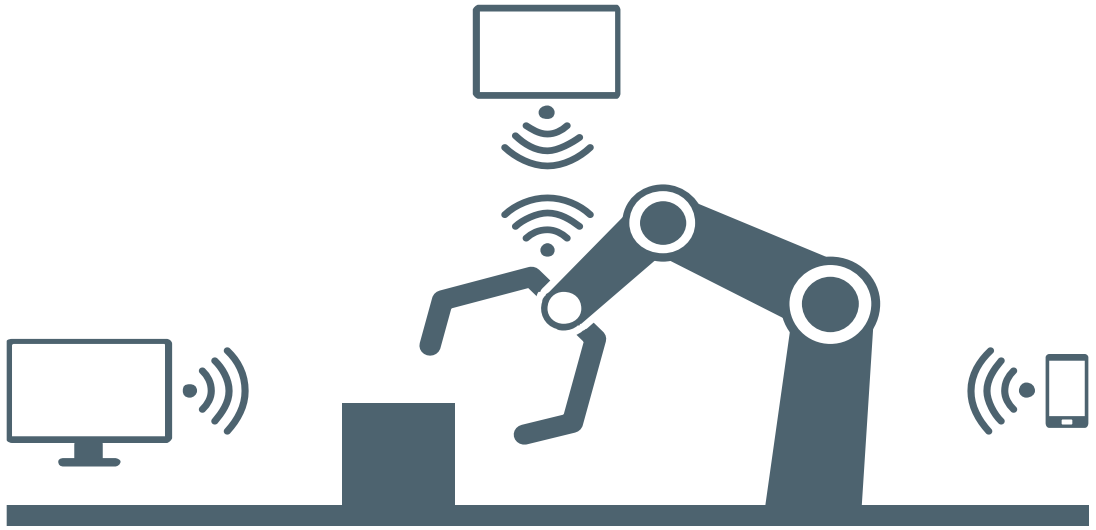
- Greater efficiency through intelligent crosslinking of product development, production, logistics and customers
- Individual, flexible production
- New business models through service orientation

Condition Monitoring

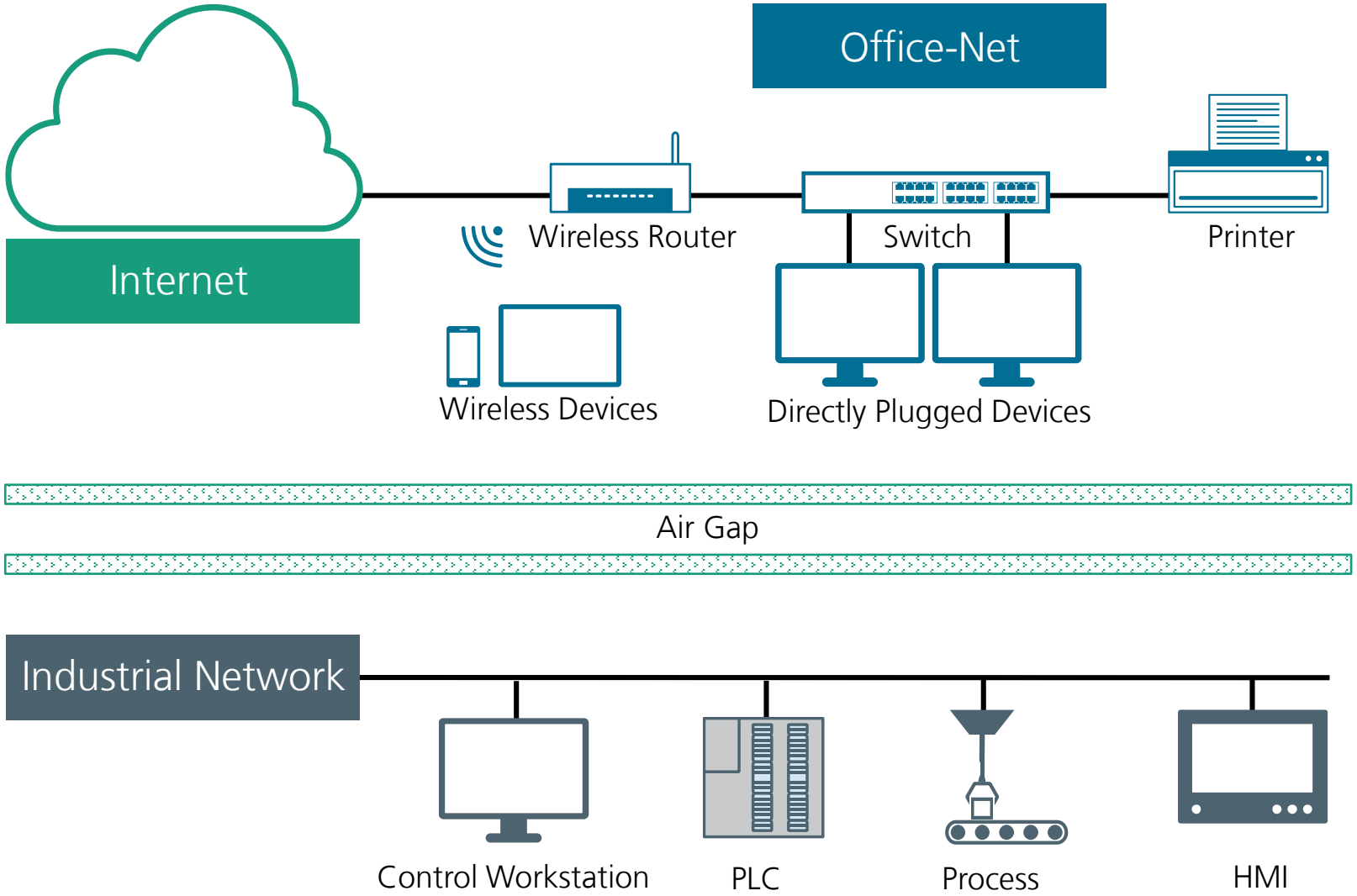
Predictive Maintenance

Machine Learning

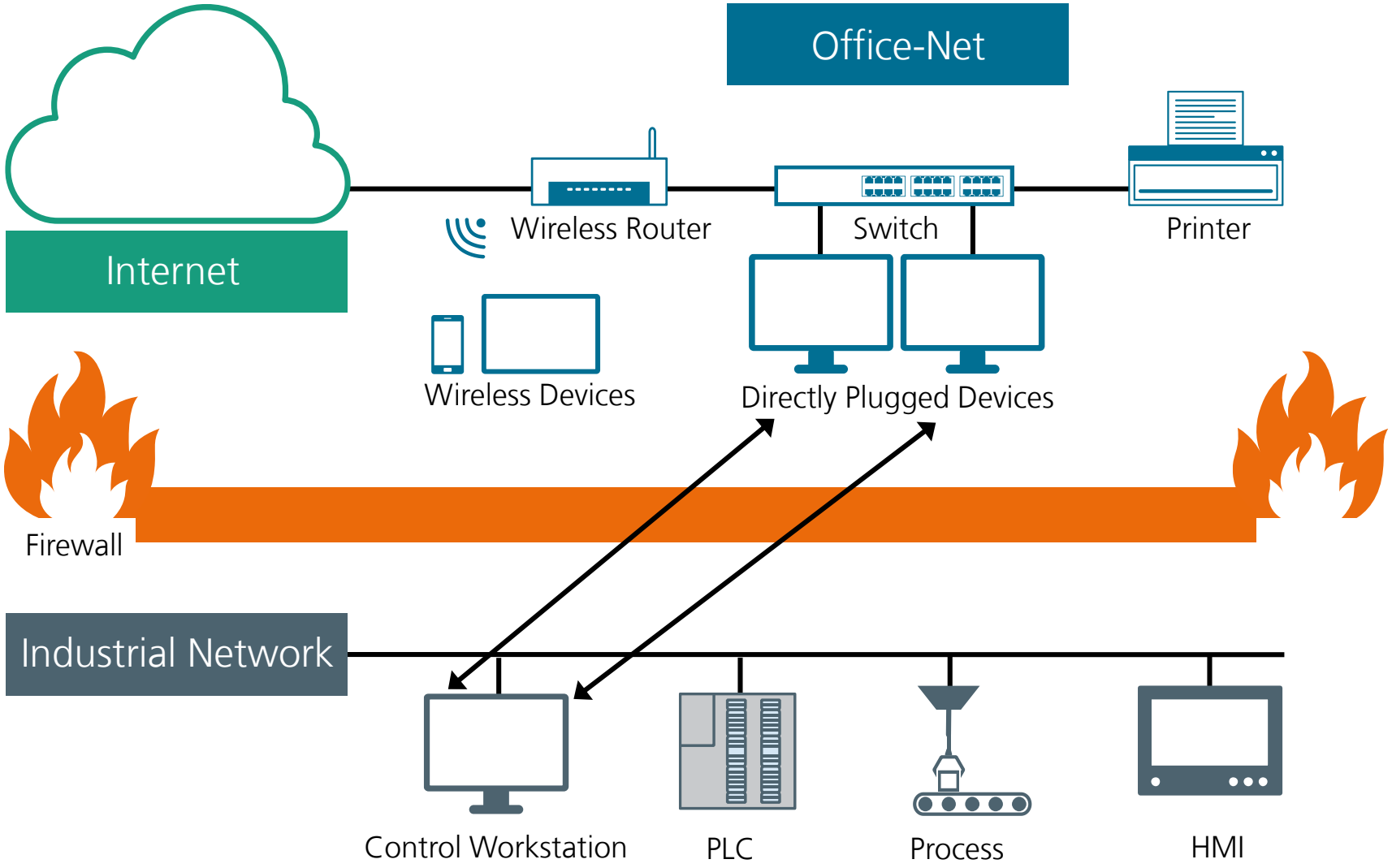
Industrial Internet of Things



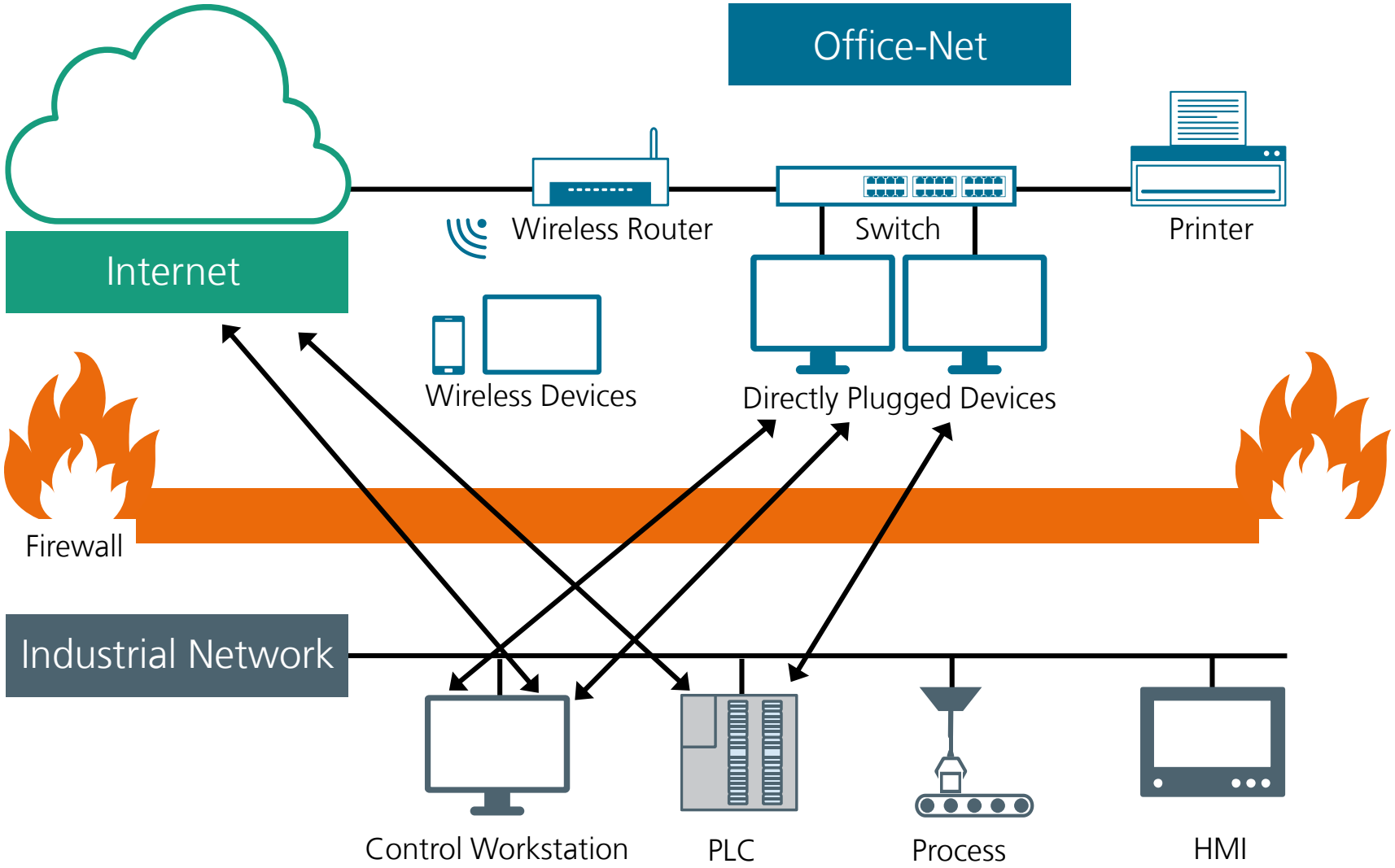
Industrial Networks of the Past



Industrial Networks nowadays



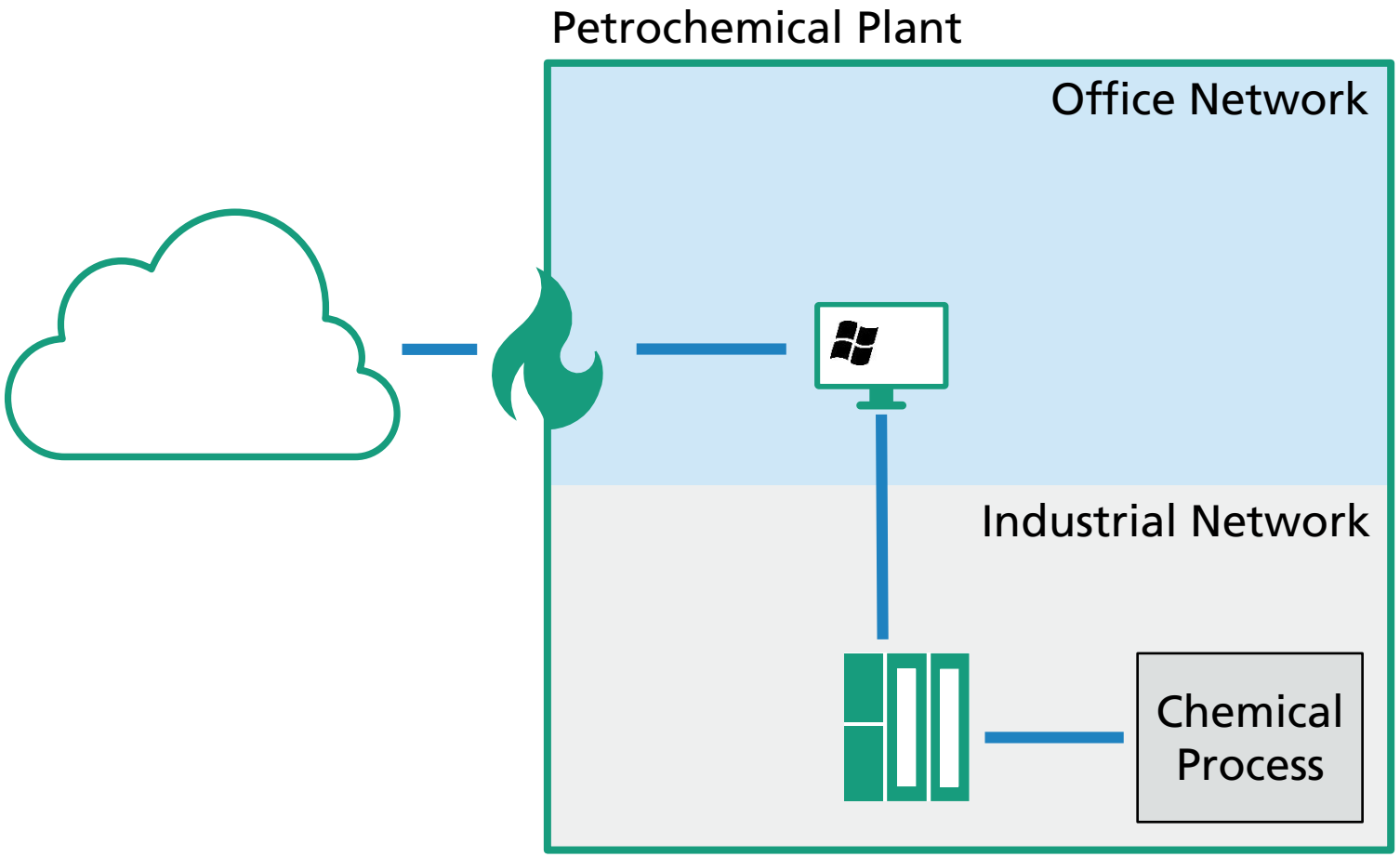
Future Industrial Networks



Attacks on Industrial Networks

TRITON

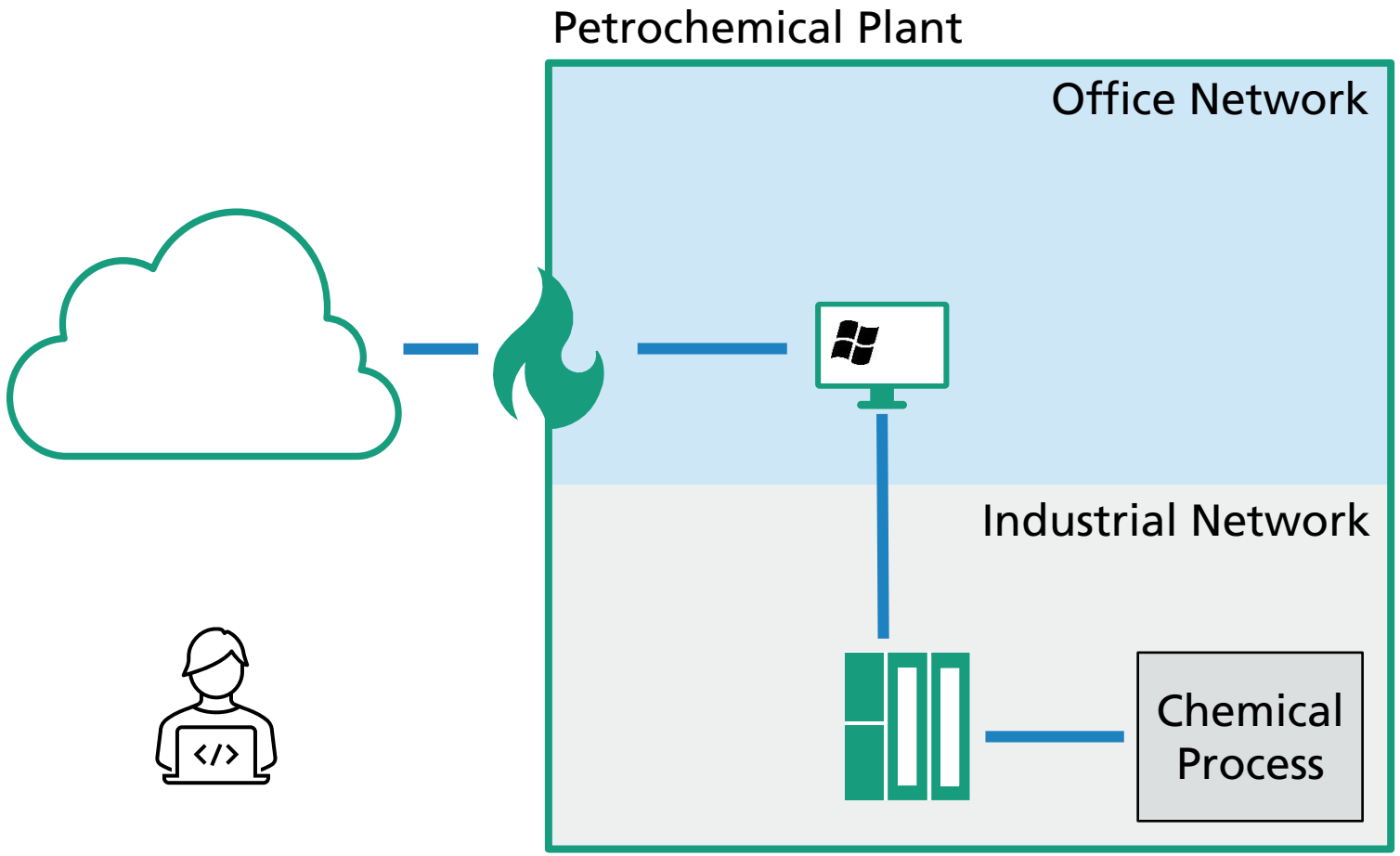
- Attack on a petrochemical plant
- Aim: Explosion



Attacks on Industrial Networks

TRITON

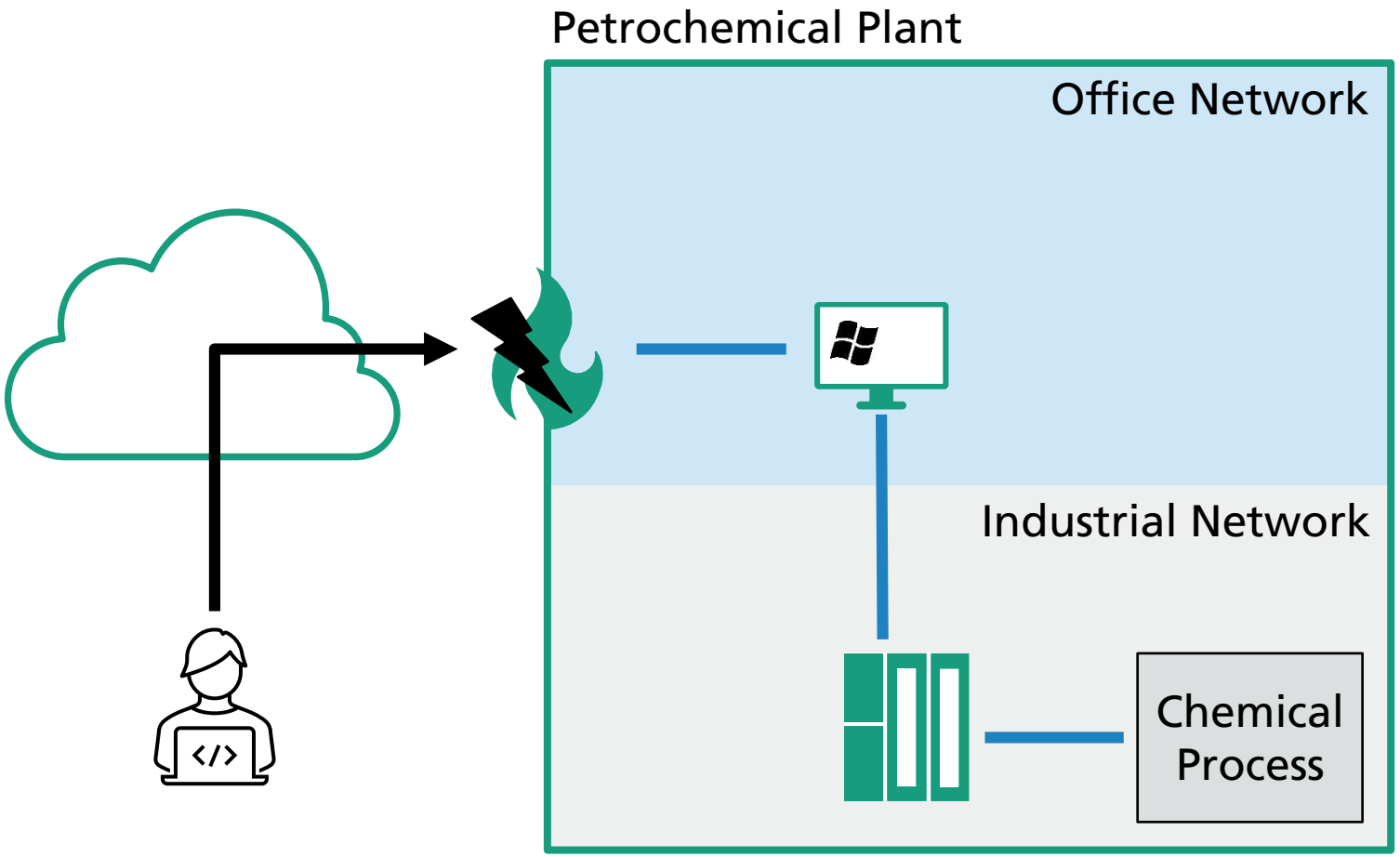
- Attack on a petrochemical plant
- Aim: Explosion



Attacks on Industrial Networks

TRITON

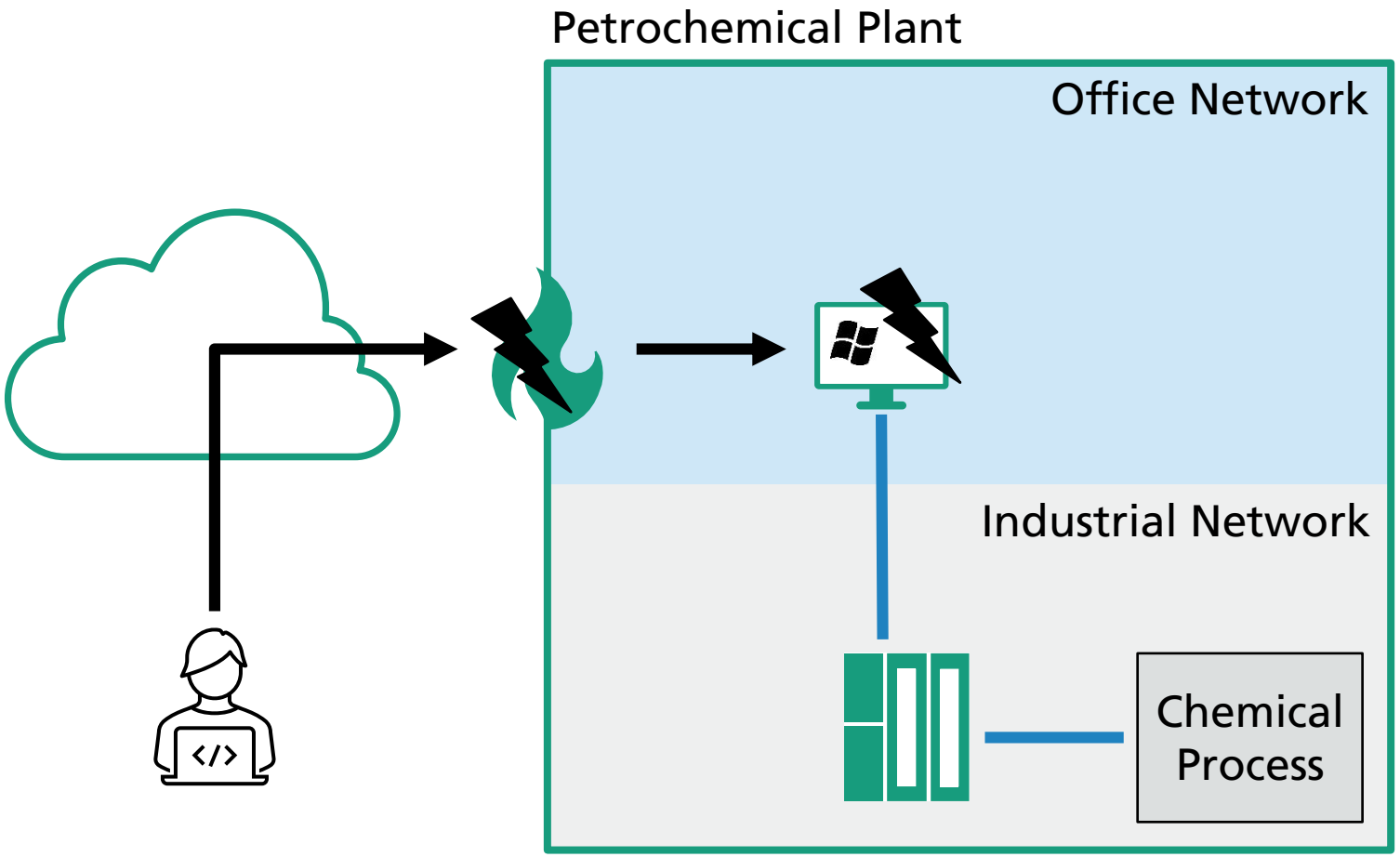
- Attack on a petrochemical plant
- Aim: Explosion



Attacks on Industrial Networks

TRITON

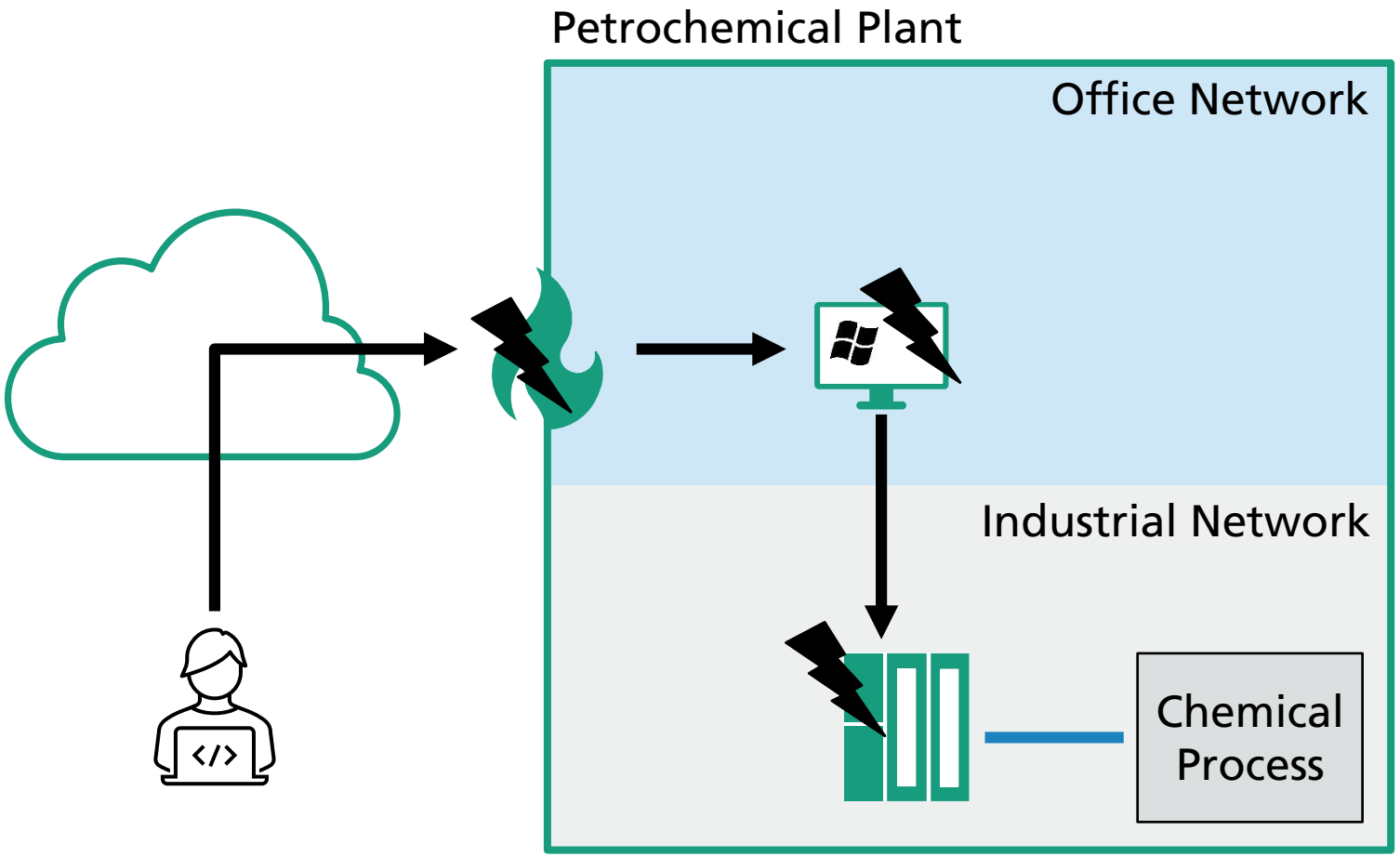
- Attack on a petrochemical plant
- Aim: Explosion



Attacks on Industrial Networks

TRITON

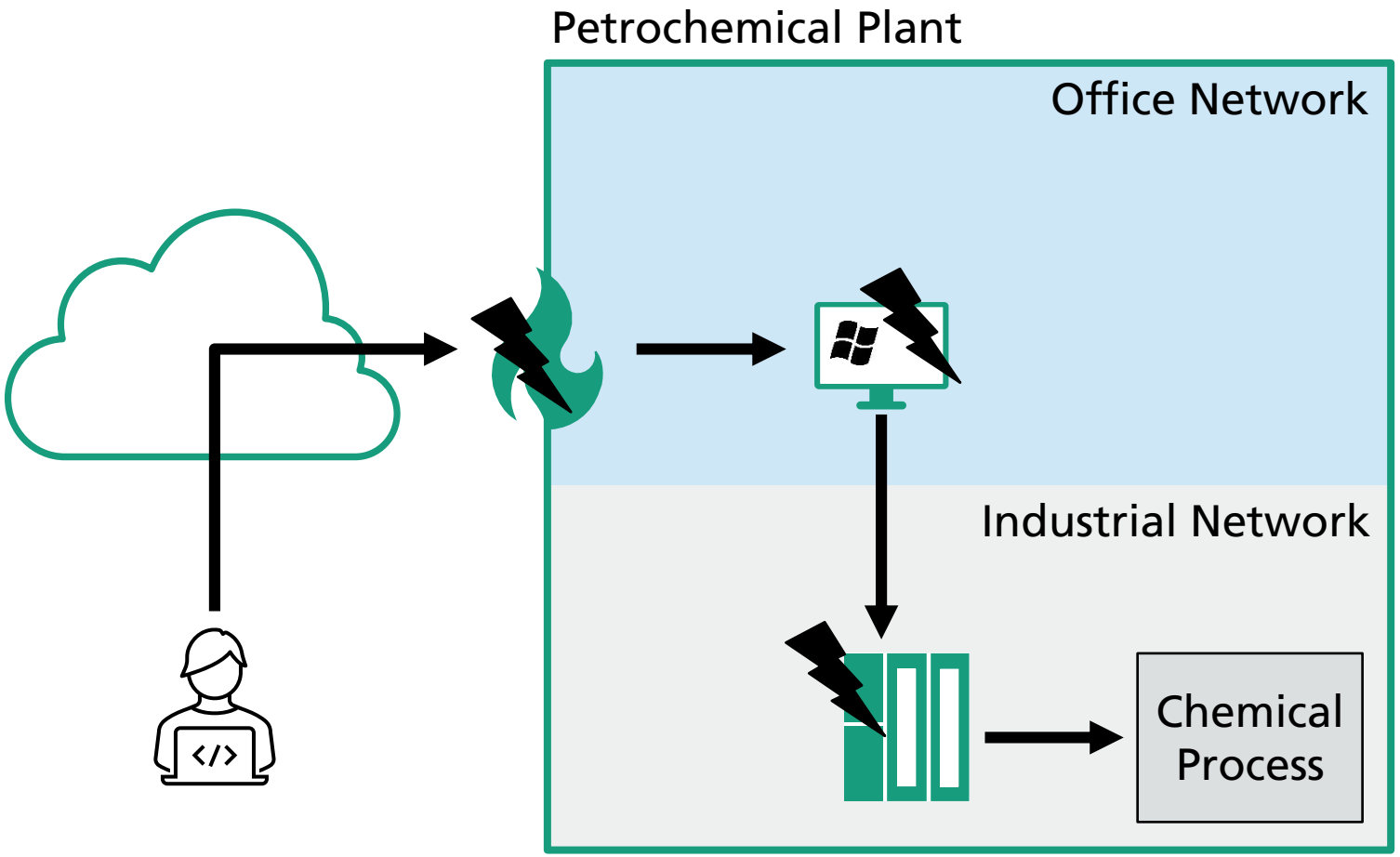
- Attack on a petrochemical plant
- Aim: Explosion



Attacks on Industrial Networks

TRITON

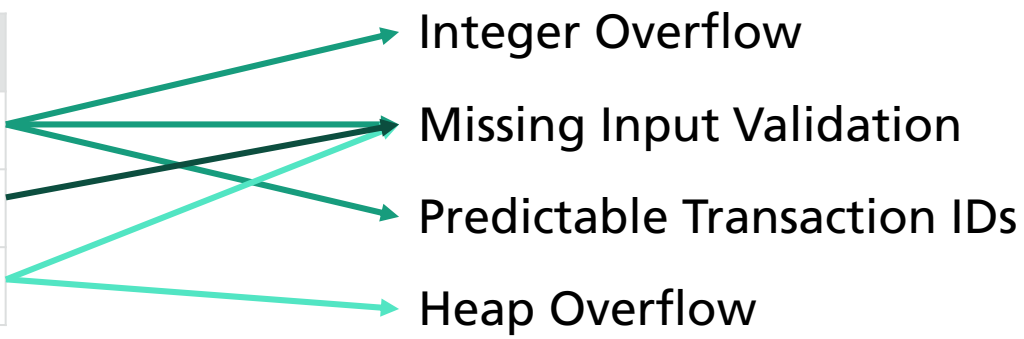
- Attack on a petrochemical plant
- Aim: Explosion



Vulnerabilities in Industrial Networks

Ripple20

CVE	Severity (CVSS)
CVE-2020-11901	9.0
CVE-2020-11898	9.1
CVE-2020-11896	10.0



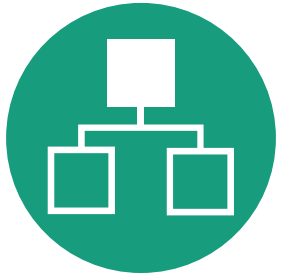
Top 10 Threats

Top 10 Threats	Trend
Infiltration of Malware via Removable Media and External Hardware	
Malware Infection via Internet and Intranet	
Human Error and Sabotage	
Compromosing of Extranet and Cloud Components	
Social Engineering and Fishing	
(D)Dos Attacks	
Control Components Connected to the Internet	
Intrusion via Remote Access	
Technical Malfunctions and Force Majeure	
Compromising of Smartphones in the Production Environment	

Source: Industrial Control System SecurityTop 10 Threats and Countermeasures 2019, Federal Office for Information Security

Improving Security

Processes



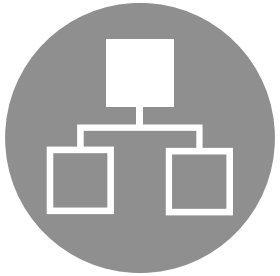
Systems

Components

based on IEC62443

Improving Security

Processes



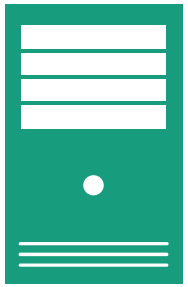
Systems

Components

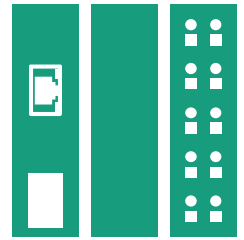
VULNERABILITY SCANNING

Automated Black Box Security Testing

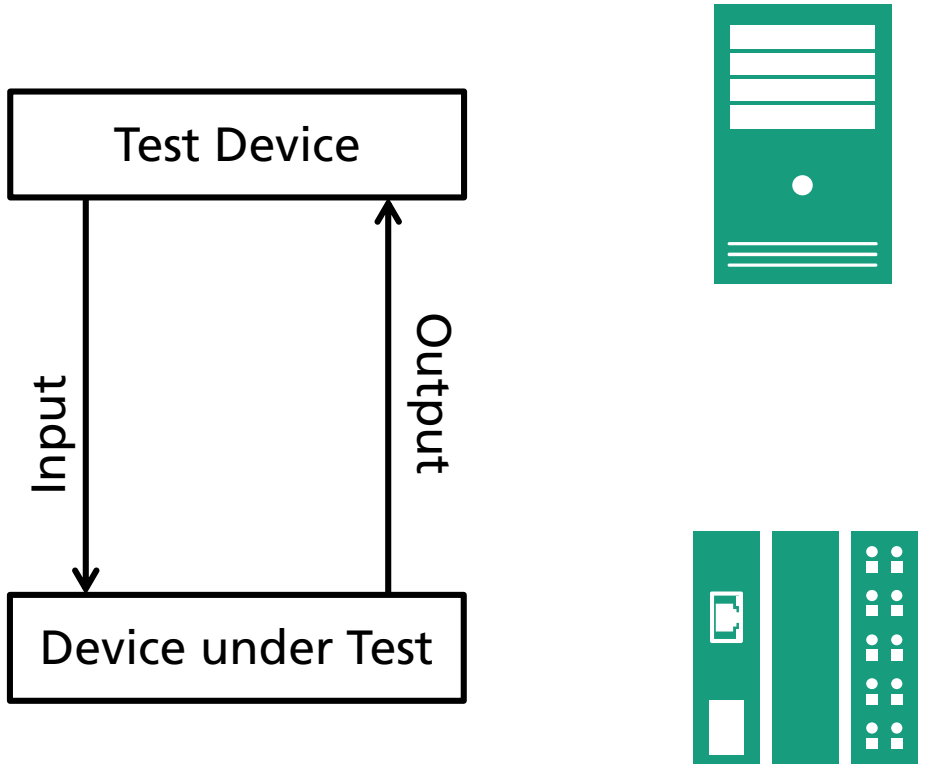
Test Device



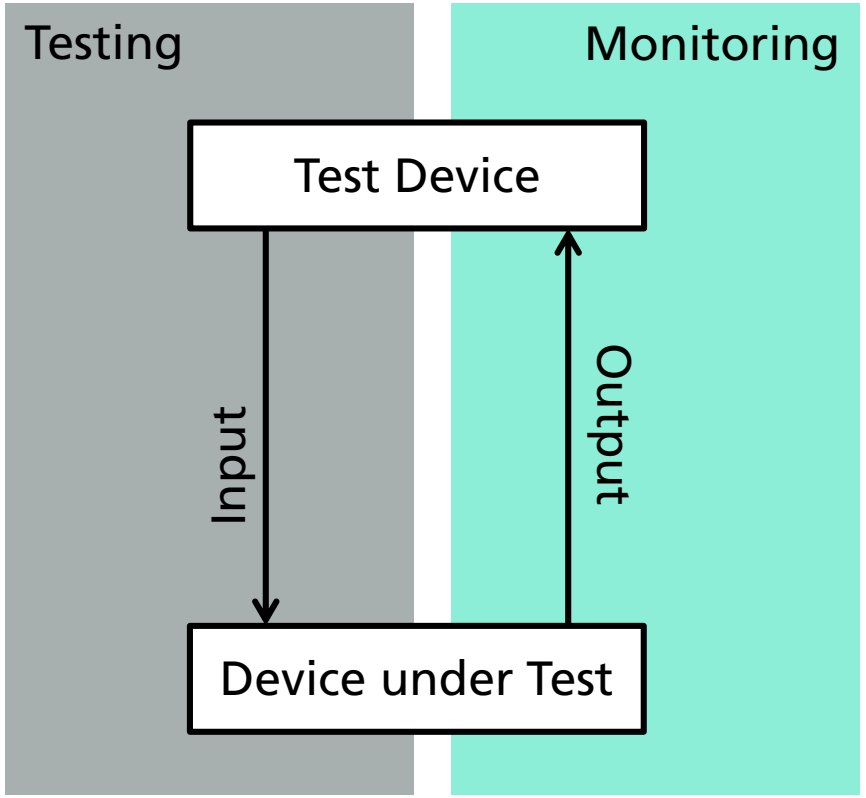
Device under Test



Automated Black Box Security Testing

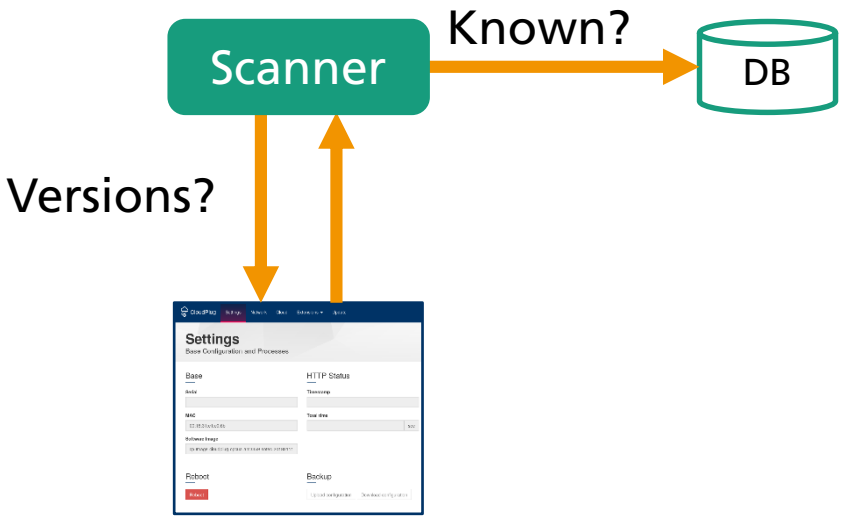


Automated Black Box Security Testing

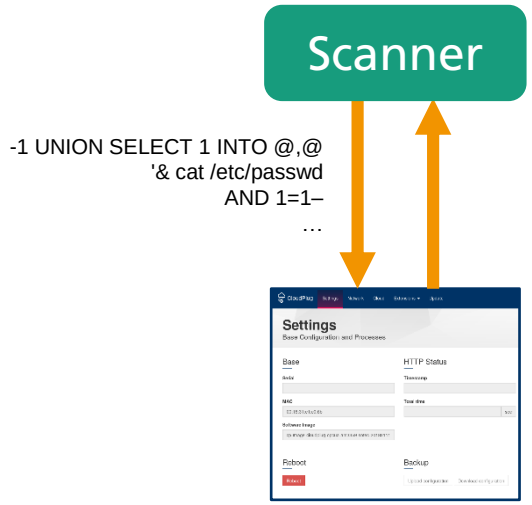


Web Security Scanners

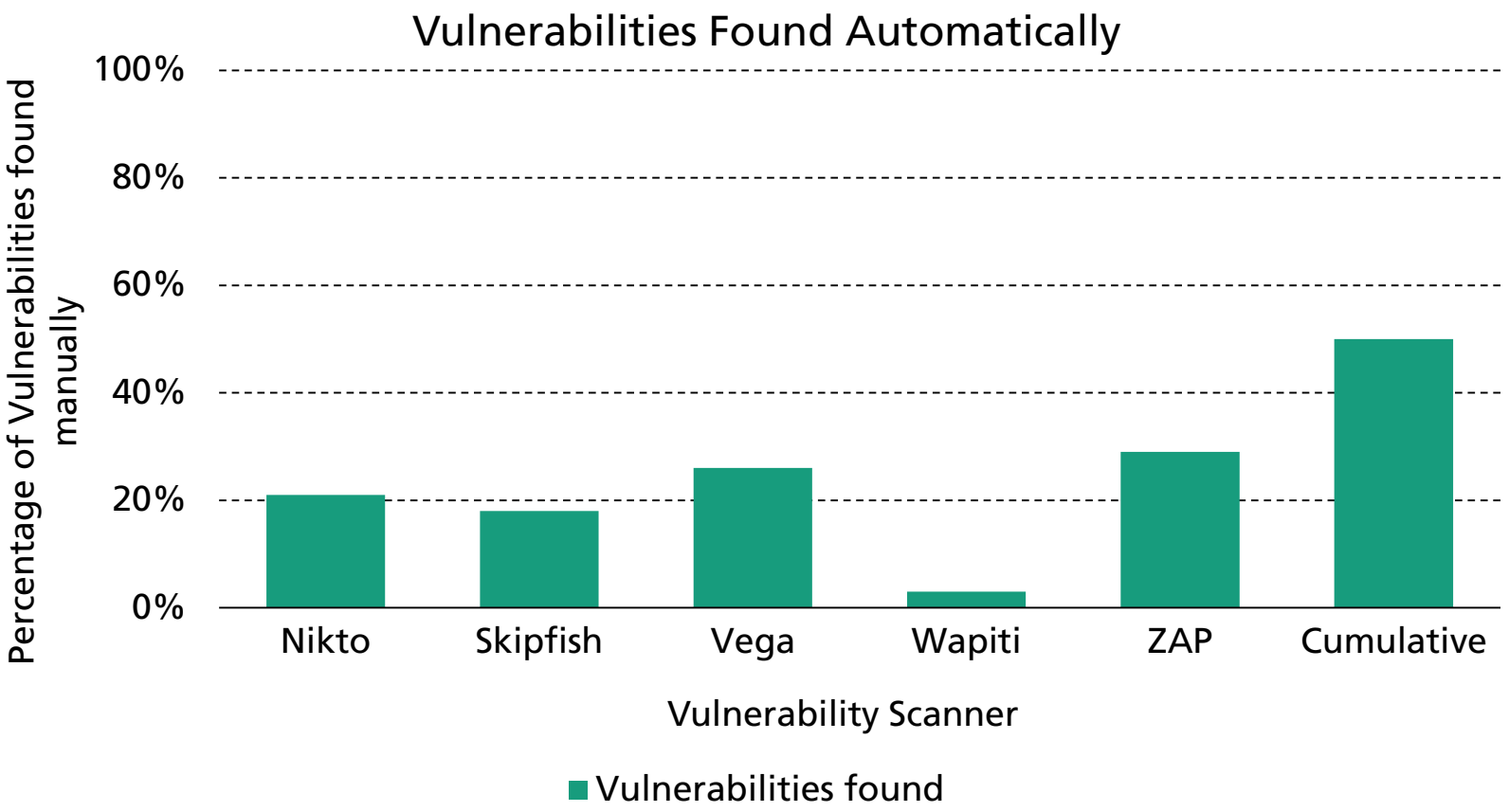
Web Vulnerability Scanners



Web Application Scanners



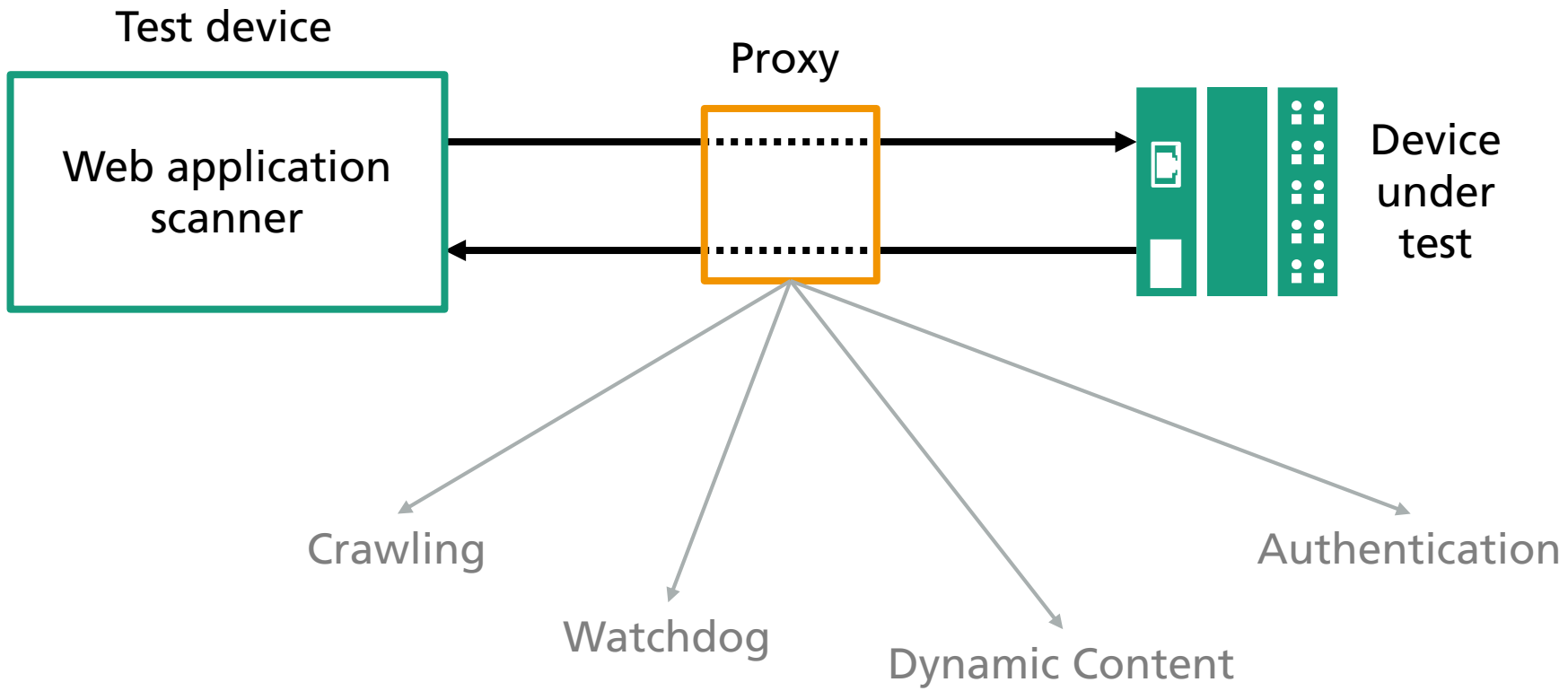
Web Application Scanners



- Web Application Scanners only find half of the vulnerabilities found manually
- But they are a lot faster

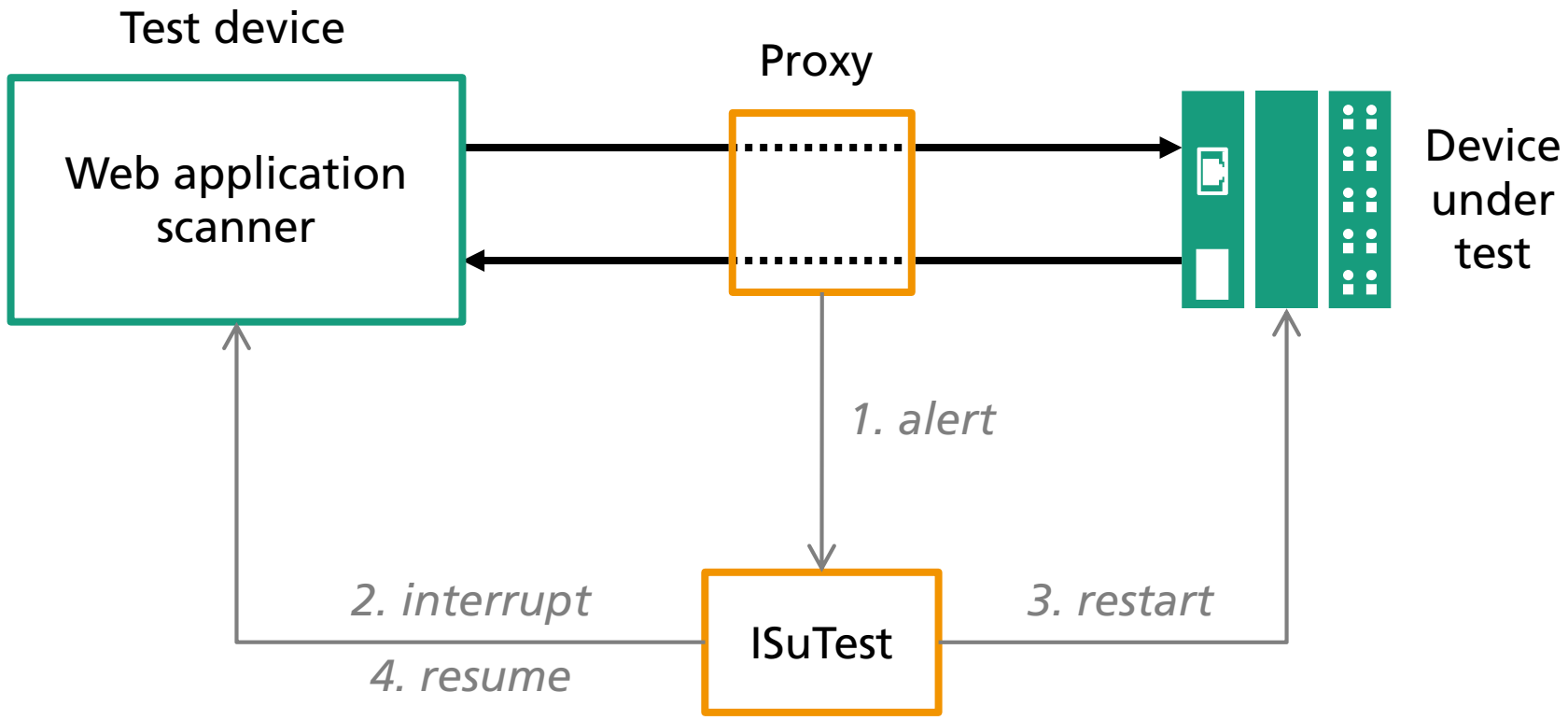
Source: Pfrang, S., Borcherding, A., Meier, D., et al. 2019. *Automated security testing for web applications on industrial automation and control systems*. at - Automatisierungstechnik. 67(5): 383-401

Helper-in-the-Middle



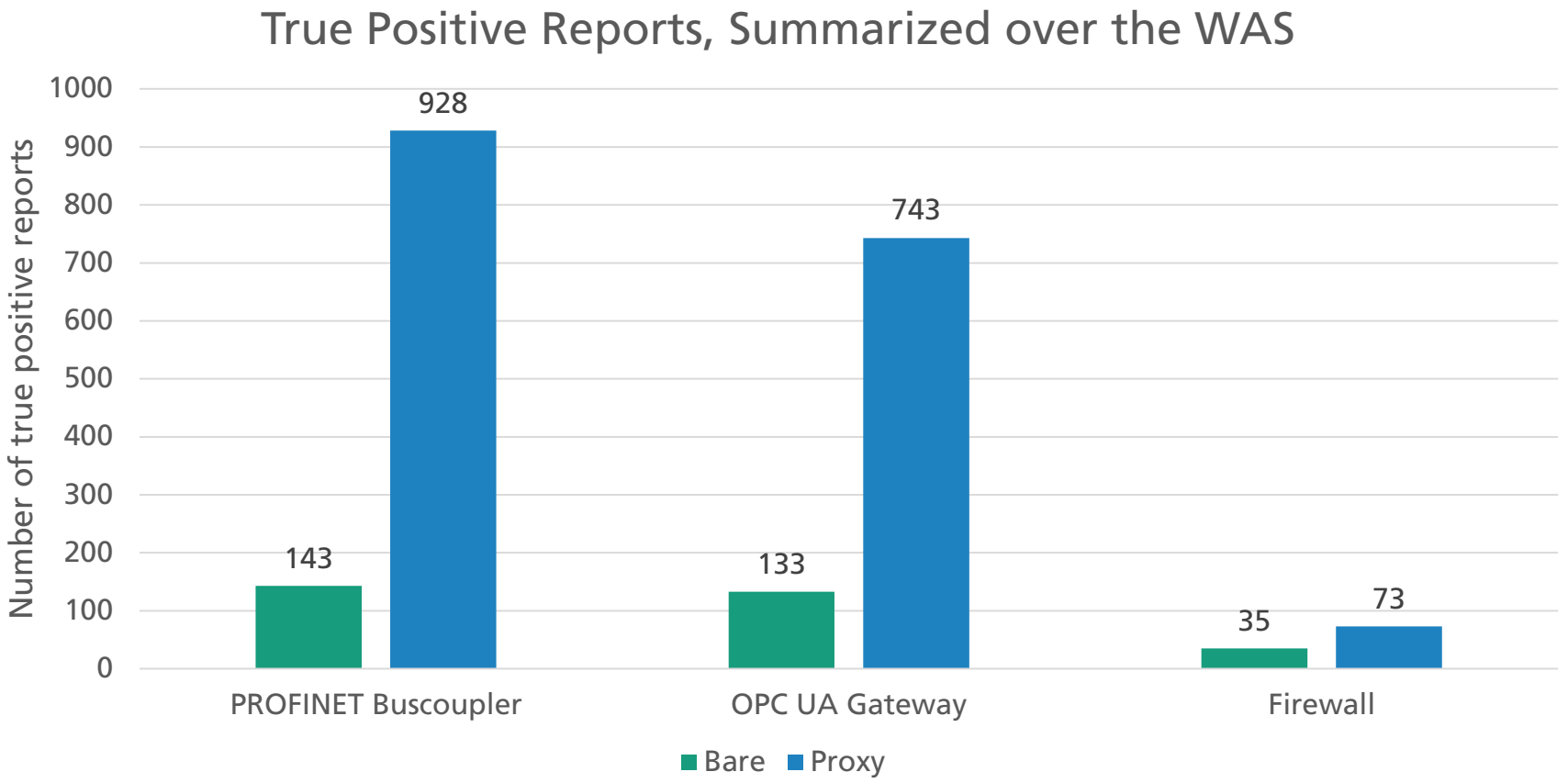
Borcherding, A., Pfrang, S., Haas, C., Weiche, A., & Beyerer, J. (2020). *Helper-in-the-Middle: Supporting web application scanners targeting industial control systems*, SECRYPT 17th International Conference on Security and Cryptography

Helper-in-the-Middle



Borcherding, A., Pfrang, S., Haas, C., Weiche, A., & Beyerer, J. (2020). *Helper-in-the-Middle: Supporting web application scanners targeting industial control systems*, SECRYPT 17th International Conference on Security and Cryptography

Helper-in-the-Middle



Proxy helps to improve performance

Borcherding, A., Pfrang, S., Haas, C., Weiche, A., & Beyerer, J. (2020). *Helper-in-the-Middle: Supporting web application scanners targeting industial control systems*, SECRYPT 17th International Conference on Security and Cryptography

FUZZING

Network Fuzzing

Network Fuzzing

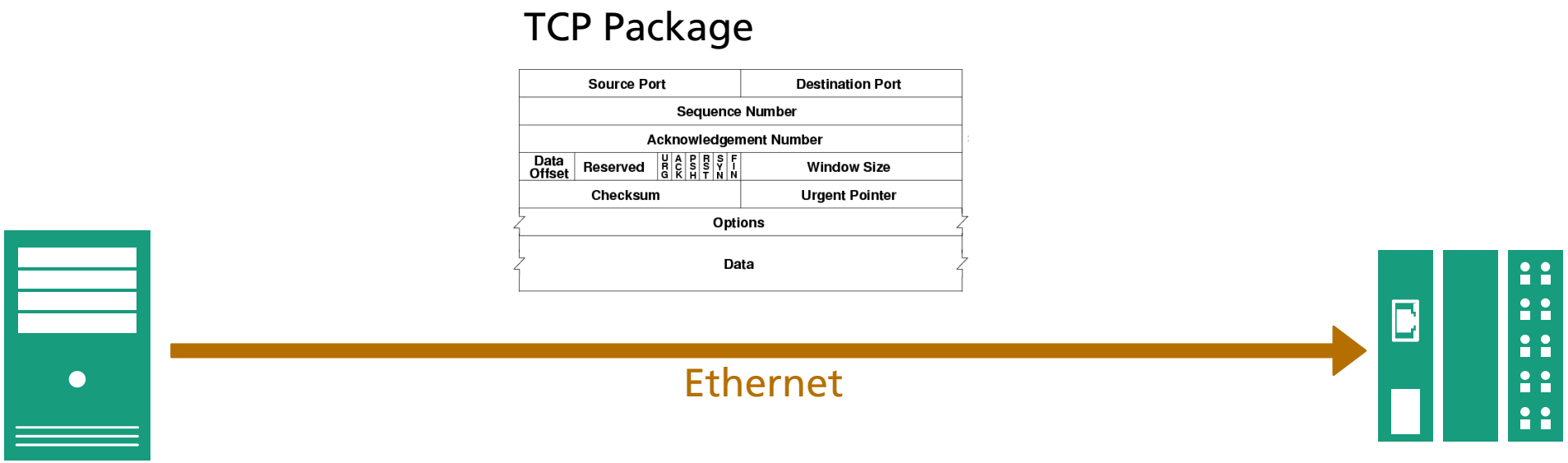


Image Source: https://commons.wikimedia.org/wiki/File:TCP_header.png

Network Fuzzing

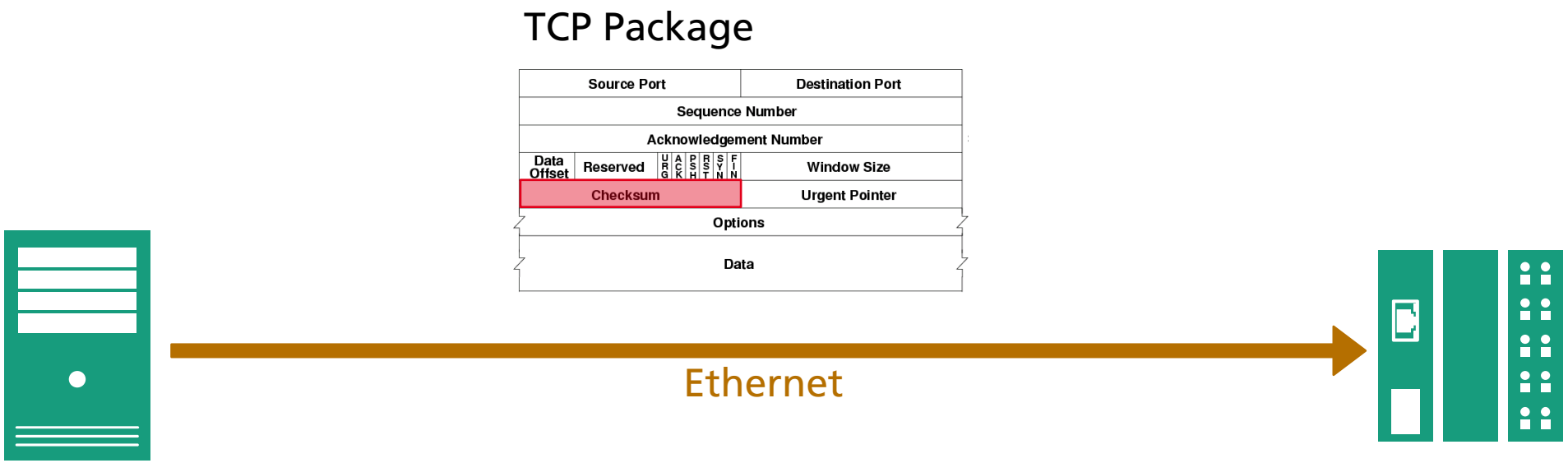


Image Source: https://commons.wikimedia.org/wiki/File:TCP_header.png

Network Fuzzing

- Full test of 2 Bytes: 2^{16} possibilities
  - Assuming 1 test per second, this will last for 18,2 hours

Network Fuzzing

- Full test of 2 Bytes: 2^{16} possibilities
  - Assuming 1 test per second, this will last for 18,2 hours

Heuristics

Network Fuzzing

- Full test of 2 Bytes: 2^{16} possibilities
  - Assuming 1 test per second, this will last for 18,2 hours

Heuristics

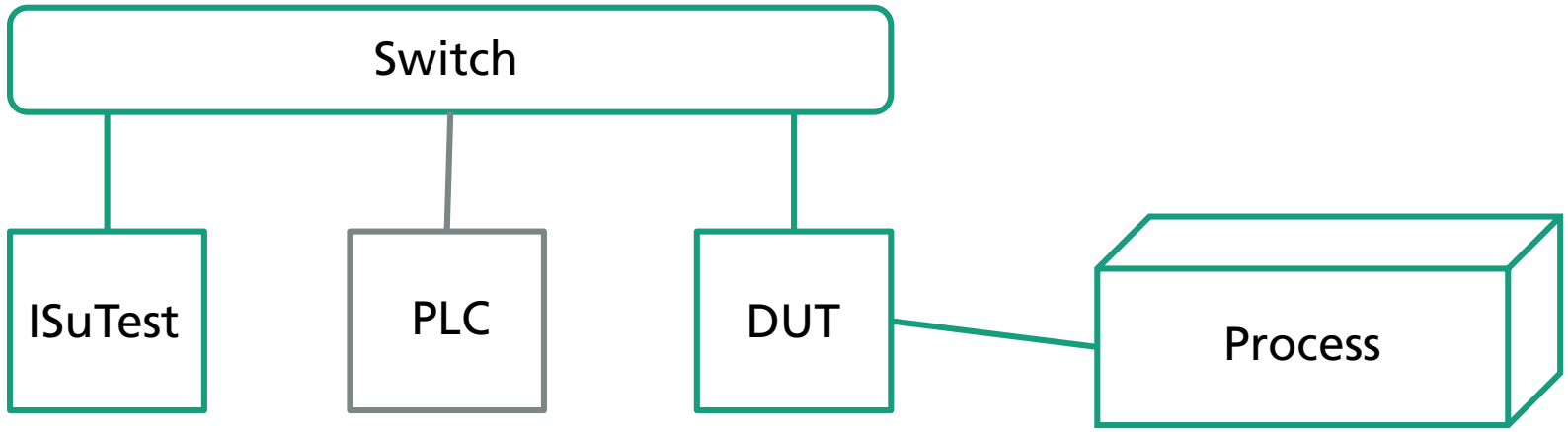
- Using experience from ealier projects and detected vulnerabilities
- Examples
  - Integer: minimum, maximum, 2^n, 2^{n-1}
  - String: "A" $*$ $self.size()$, "2019-02-31"

Bus Coupler Study

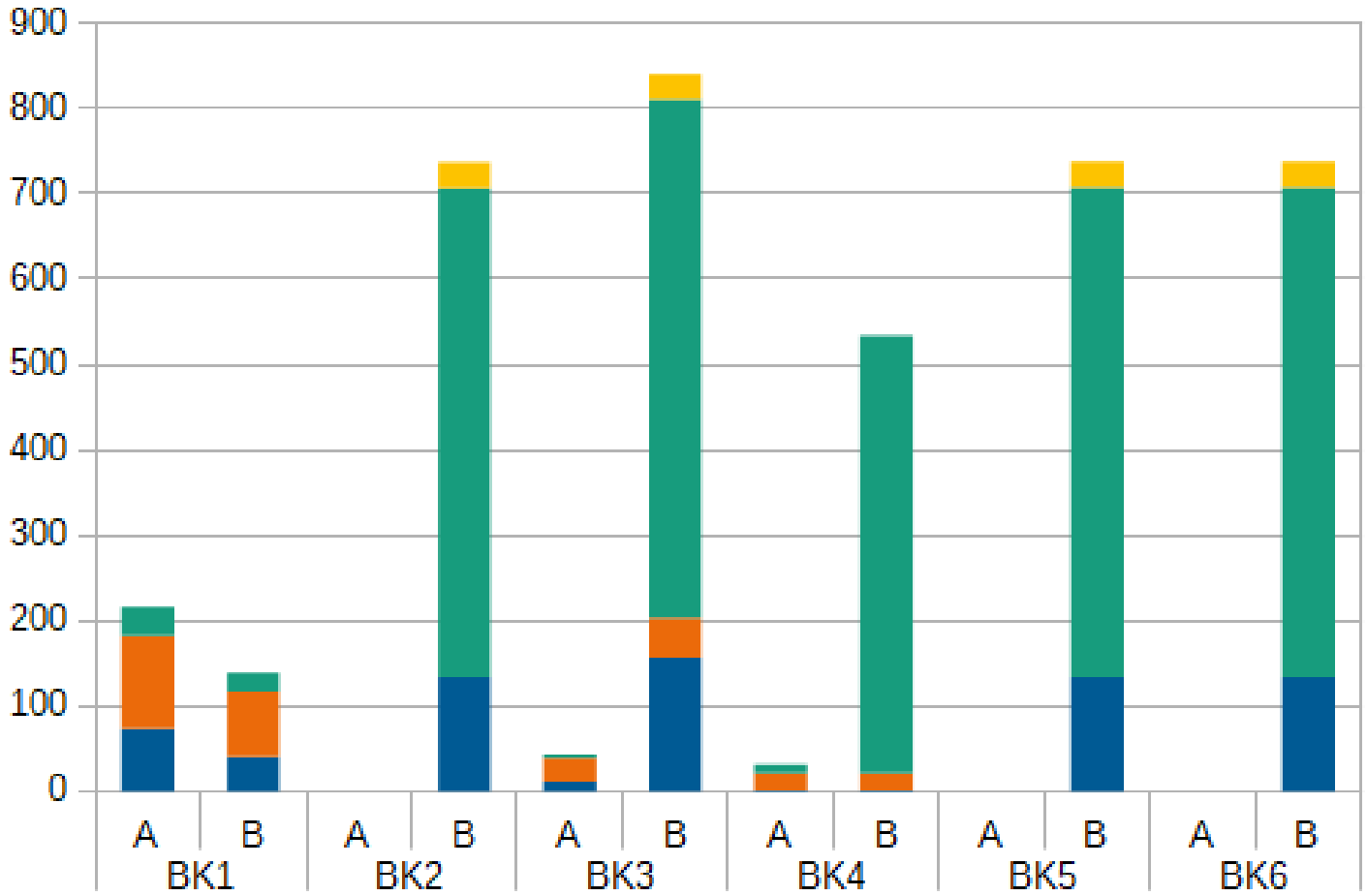
- 6 Profinet bus coupler from different German manufacturers
  - Security tests of the Profinet implementation (DCE/RPC and PNIO-CM)
  - ~ 70 000 test cases per bus coupler

Bus Coupler Study

- 6 Profinet bus coupler from different German manufacturers
  - Security tests of the Profinet implementation (DCE/RPC and PNIO-CM)
  - ~ 70 000 test cases per bus coupler
  - Szenario A: without PLC
  - Szenario B: with PLC



Bus Coupler Study



- All bus couplers are vulnerable
- Similarity of stacks is visible

Source: Steffen Pfrang, Anne Borcherding: *Security-Testing für industrielle Automatisierungskomponenten: Ein Framework, sein Einsatz und Ergebnisse am Beispiel von Profinet-Buskopplern*,16. Deutscher IT-Sicherheitskongress des BSI, 2019

Summary

- Transformation of industrial networks
- Recent attacks, vulnerabilities, and threats
- Web Application Scanners
- Fuzzing