KASPERSKY lab

Industrial Cybersecurity 2018:
Opportunities and challenges in Digital Transformation

DAVID MEIER

Fraunhofer Institute of Optronics, System Technologies, and Image Exploitation IOSB
Germany

- Works on the framework ISuTest in Fraunhofer IOSB
- Part of the VDI expert committee on safety and security

linkedin.com/in/david-meier-de

IMPROVING THE EFFECTIVENESS OF SECURITY TRAININGS FOR INDUSTRIAL AND AUTOMATION PROFESSIONALS

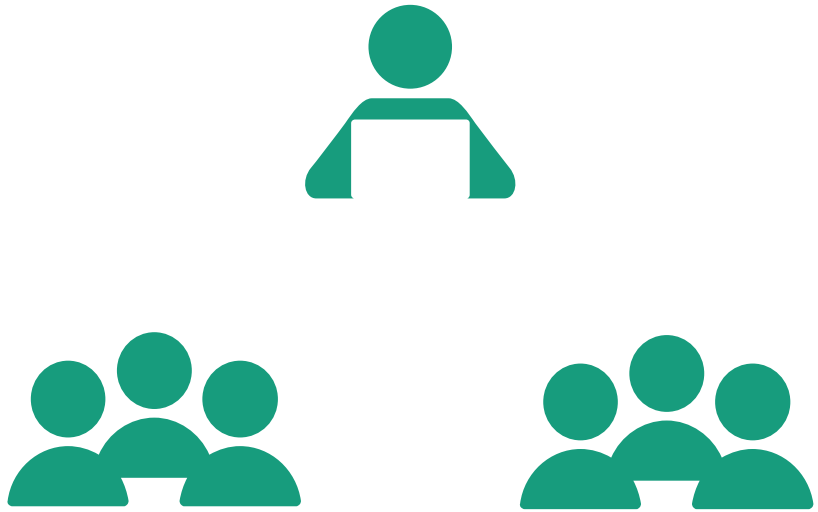
David Meier

Fraunhofer Institute of Optronics, System Technologies, and Image Exploitation IOSB, Germany

Fraunhofer IOSB

AGENDA

- Cyber Threats for ICS
  - Threat landscape
  - The human factor
- Staff training
  - Audiences, goals
  - Practical focus
- Our approach
  - Increase effectiveness
  - Training structure



CYBER THREATS FOR ICS
THREAT LANDSCAPE

- Cyber Threats are real for industrial facilities
  - As shown by the many known incidents
- Many companies still struggle to adapt
  - Especially hard for SMEs
- Increasing introduction of new technologies (“Industrie 4.0”, IIoT) enhances this development
- Why does this seem such a hard problem?

CYBER THREATS FOR ICS
BSI TOP 10 THREATS FOR ICS

- German Federal Office for Information Security (BSI)

BSI TOP 10 Cyber Threats for ICS	
Position	Threat
1	Social Engineering & Phising
2	Malware via Removable Media / External Hardware
3	Malware Infection via Inter- and Intranet
4	Intrusion via Remote (Maintenance) Access
5	Human Error & Sabotage
6	Controller Components Connected to the Internet
7	Technical Malfunctions & Force Majeure
8	Compromised Extranet and Cloud Components
9	(D)DoS Attacks
10	Compromising of Smartphones in Production Areas

Source: BSI-CS 005E - Top 10 Threats and Countermeasures 2016

CYBER THREATS FOR ICS
BSI TOP 10 THREATS FOR ICS

- German Federal Office for Information Security (BSI)

BSI TOP 10 Cyber Threats for ICS	
Position	Threat
1	Social Engineering & Phising
2	Malware via Removable Media / External Hardware
3	Malware Infection via Inter- and Intranet
4	Intrusion via Remote (Maintenance) Access
5	Human Error & Sabotage
6	Controller Components Connected to the Internet
7	Technical Malfunctions & Force Majeure
8	Compromised Extranet and Cloud Components
9	(D)DoS Attacks
10	Compromising of Smartphones in Production Areas

Human factor:

2 out of 10 Threats

Source: BSI-CS 005E - Top 10 Threats and Countermeasures 2016

CYBER THREATS FOR ICS
BSI TOP 10 THREATS FOR ICS

- German Federal Office for Information Security (BSI)

BSI TOP 10 Cyber Threats for ICS	
Position	Threat
1	Social Engineering & Phising
2	Malware via Removable Media / External Hardware
3	Malware Infection via Inter- and Intranet
4	Intrusion via Remote (Maintenance) Access
5	Human Error & Sabotage
6	Controller Components Connected to the Internet
7	Technical Malfunctions & Force Majeure
8	Compromised Extranet and Cloud Components
9	(D)DoS Attacks
10	Compromising of Smartphones in Production Areas

Human factor:

2 out of 10 Threats

Really?

Source: BSI-CS 005E - Top 10 Threats and Countermeasures 2016

CYBER THREATS FOR ICS
BSI TOP 10 THREATS FOR ICS

- German Federal Office for Information Security (BSI)

BSI TOP 10 Cyber Threats for ICS	
Position	Threat
1	Social Engineering & Phising
2	Malware via Removable Media / External Hardware
3	Malware Infection via Inter- and Intranet
4	Intrusion via Remote (Maintenance) Access
5	Human Error & Sabotage
6	Controller Components Connected to the Internet
7	Technical Malfunctions & Force Majeure
8	Compromised Extranet and Cloud Components
9	(D)DoS Attacks
10	Compromising of Smartphones in Production Areas

Human factor:

3 out of 10 Threats

- Who inserts Flash-Drives into Control Systems?
- Who needs to follow Security Processes?

© Hak5 Rubber Ducky

Source: BSI-CS 005E - Top 10 Threats and Countermeasures 2016

Fraunhofer IOSB

CYBER THREATS FOR ICS
BSI TOP 10 THREATS FOR ICS

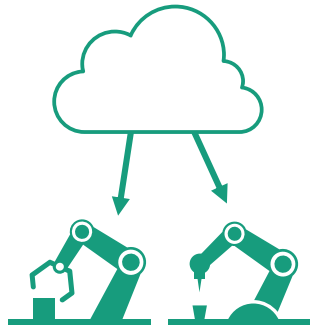
- German Federal Office for Information Security (BSI)

BSI TOP 10 Cyber Threats for ICS	
Position	Threat
1	Social Engineering & Phising
2	Malware via Removable Media / External Hardware
3	Malware Infection via Inter- and Intranet
4	Intrusion via Remote (Maintenance) Access
5	Human Error & Sabotage
6	Controller Components Connected to the Internet
7	Technical Malfunctions & Force Majeure
8	Compromised Extranet and Cloud Components
9	(D)DoS Attacks
10	Compromising of Smartphones in Production Areas

Human factor:

4 out of 10 Threats

- Who supervises Remote Access?
- Who uses Remote Access?



Source: BSI-CS 005E - Top 10 Threats and Countermeasures 2016

Fraunhofer IOSB

CYBER THREATS FOR ICS
BSI TOP 10 THREATS FOR ICS

- German Federal Office for Information Security (BSI)

BSI TOP 10 Cyber Threats for ICS	
Position	Threat
1	Social Engineering & Phising
2	Malware via Removable Media / External Hardware
3	Malware Infection via Inter- and Intranet
4	Intrusion via Remote (Maintenance) Access
5	Human Error & Sabotage
6	Controller Components Connected to the Internet
7	Technical Malfunctions & Force Majeure
8	Compromised Extranet and Cloud Components
9	(D)DoS Attacks
10	Compromising of Smartphones in Production Areas

Human factor:

5 out of 10 Threats

- Who helps malware overcome network boundaries?
- Influence of security aware behavior?

Source: BSI-CS 005E - Top 10 Threats and Countermeasures 2016

CYBER THREATS FOR ICS
BSI TOP 10 THREATS FOR ICS

- German Federal Office for Information Security (BSI)

BSI TOP 10 Cyber Threats for ICS	
Position	Threat
1	Social Engineering & Phising
2	Malware via Removable Media / External Hardware
3	Malware Infection via Inter- and Intranet
4	Intrusion via Remote (Maintenance) Access
5	Human Error & Sabotage
6	Controller Components Connected to the Internet
7	Technical Malfunctions & Force Majeure
8	Compromised Extranet and Cloud Components
9	(D)DoS Attacks
10	Compromising of Smartphones in Production Areas

Human factor:

6 out of 10 Threats

- Dangers of BYOD?
- What is allowed on a Smartphone used in OT?

Source: BSI-CS 005E - Top 10 Threats and Countermeasures 2016

CYBER THREATS FOR ICS
BSI TOP 10 THREATS FOR ICS

- German Federal Office for Information Security (BSI)

BSI TOP 10 Cyber Threats for ICS	
Position	Threat
1	Social Engineering & Phising
2	Malware via Removable Media / External Hardware
3	Malware Infection via Inter- and Intranet
4	Intrusion via Remote (Maintenance) Access
5	Human Error & Sabotage
6	Controller Components Connected to the Internet
7	Technical Malfunctions & Force Majeure
8	Compromised Extranet and Cloud Components
9	(D)DoS Attacks
10	Compromising of Smartphones in Production Areas

Human factor:

7 out of 10 Threats

- Who would connect a PLC to the Internet?
- Intentional?

Source: BSI-CS 005E - Top 10 Threats and Countermeasures 2016

CYBER THREATS FOR ICS
BSI TOP 10 THREATS FOR ICS

- German Federal Office for Information Security (BSI)

BSI TOP 10 Cyber Threats for ICS	
Position	Threat
1	Social Engineering & Phising
2	Malware via Removable Media / External Hardware
3	Malware Infection via Inter- and Intranet
4	Intrusion via Remote (Maintenance) Access
5	Human Error & Sabotage
6	Controller Components Connected to the Internet
7	Technical Malfunctions & Force Majeure
8	Compromised Extranet and Cloud Components
9	(D)DoS Attacks
10	Compromising of Smartphones in Production Areas

Human factor:

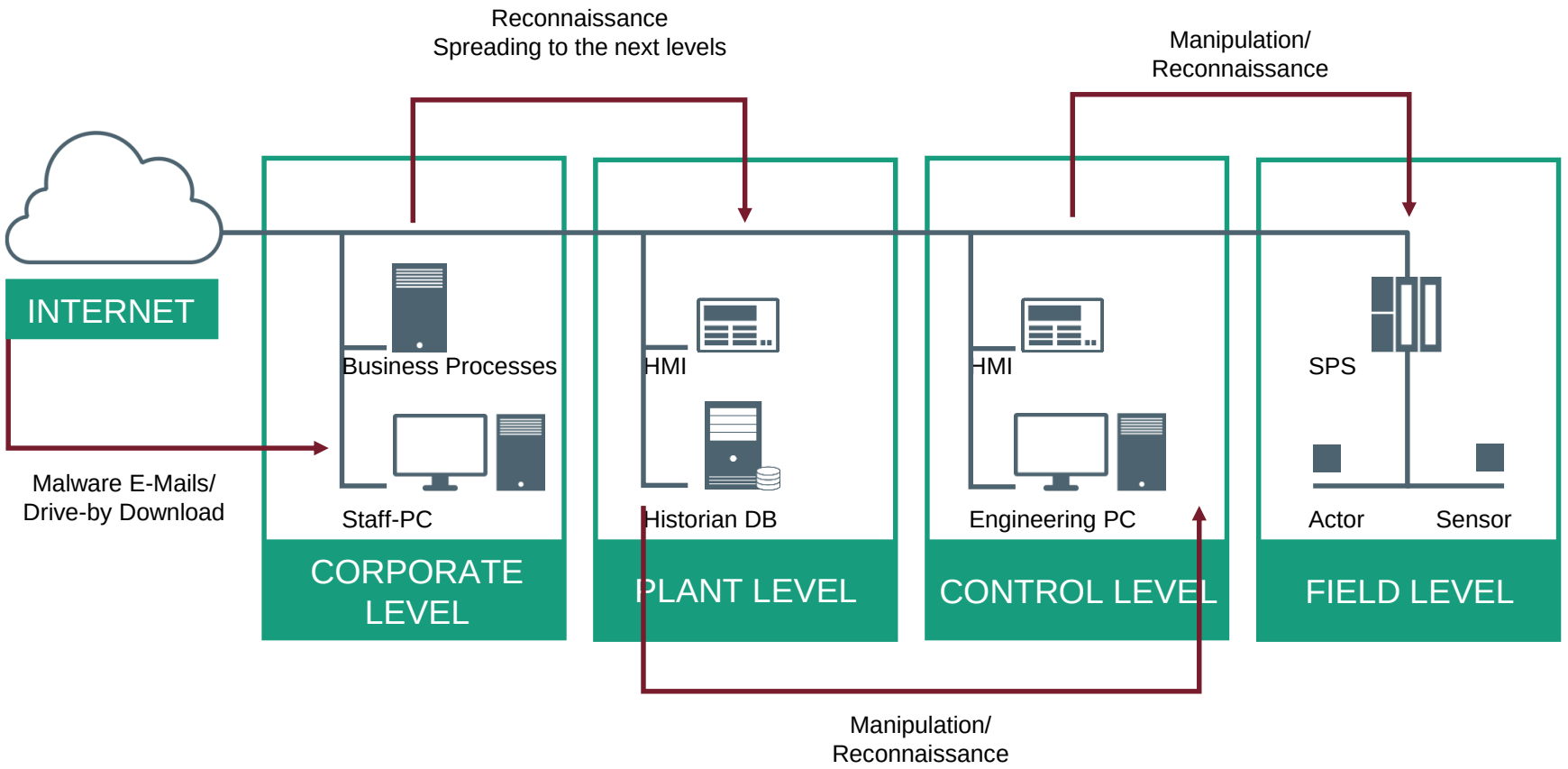
At least 7 out of 10 Threats?

Staff / personnel, contract workers etc. have a big influence on Cyber Threats

Source: BSI-CS 005E - Top 10 Threats and Countermeasures 2016

CYBER THREATS FOR ICS
EXAMPLE ATTACK SCENARIO

- Attacks are often multi-staged
- Security boundaries and countermeasures
  - Firewalls
  - IDS
- Defense in Depth
- Staff can help attacks bypass boundaries



CYBER THREATS FOR ICS
ICS SECURITY MYTHS

- Our systems are not „on the internet“!
- Our systems are secure, we have a firewall!
- We are not a target!
- Hackers don‘t understand industrial automation systems!
- What could possibly go wrong, we have safety systems installed!

CYBER THREATS FOR ICS
ICS SECURITY MYTHS

- Our systems are not „on the internet“!
  - Shodan and co say otherwise
- Our systems are secure, we have a firewall!
- We are not a target!
- Hackers don‘t understand industrial automation systems!
- What could possibly go wrong, we have safety systems installed!

Shodan.io: Search engine for Internet-connected devices

CYBER THREATS FOR ICS
ICS SECURITY MYTHS

- Our systems are not „on the internet“!
  - Shodan and co say otherwise
- Our systems are secure, we have a firewall!
  - How good is the rule set?
- We are not a target!

- Hackers don‘t understand industrial automation systems!

- What could possibly go wrong, we have safety systems installed!

A Quantitative Study of Firewall Configuration Errors

The protection that firewalls provide is only as good as the policy they are configured to implement. Analysis of real configuration data shows that corporate firewalls are often enforcing rule sets that violate well-established security guidelines.

Avishai Wool
Tel Aviv University

Firewalls are the cornerstone of corporate intranet security. Once a company acquires a firewall, a systems administrator must configure and manage it according to a security policy that meets the company's needs. Configuration is a crucial task, probably the most

system on which the firewall runs, the firewall's software version, and a new measure of rule-set complexity.

DATA COLLECTION

Between 2000 and 2001, a total of 37 Check

A. Wool, "A quantitative study of firewall configuration errors," in Computer, vol. 37, no. 6, pp. 62-67, June 2004.

CYBER THREATS FOR ICS
ICS SECURITY MYTHS

- Our systems are not „on the internet“!
  - Shodan and co say otherwise
- Our systems are secure, we have a firewall!
  - How good is the rule set?
- We are not a target!
  - Do not need to be a target (Malware, Ransomware)
- Hackers don‘t understand industrial automation systems!

- What could possibly go wrong, we have safety systems installed!

Technology

iPhone Chipmaker Blames WannaCry Variant for Plant Closures

By Debby Wu

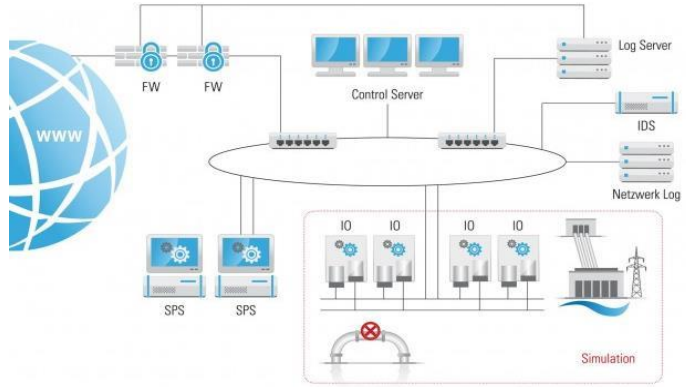
6. August 2018, 11:28 MESZ *Updated on 7. August 2018, 06:35 MESZ*

- Chipmaker was infected by virus akin to the 2017 ransomware
- Incident may weigh on relationship between Apple, TSMC

Source: bloomberg.com, August 2018

CYBER THREATS FOR ICS
ICS SECURITY MYTHS

- Our systems are not „on the internet“!
  - Shodan and co say otherwise
- Our systems are secure, we have a firewall!
  - How good is the rule set?
- We are not a target!
  - Do not need to be a target (Malware, Ransomware)
- Hackers don‘t understand industrial automation systems!
  - Honeypots show otherwise
- What could possibly go wrong, we have safety systems installed!



Source: TÜV Süd, Honeynet

CYBER THREATS FOR ICS
ICS SECURITY MYTHS

- Our systems are not „on the internet“!
  - Shodan and co say otherwise
- Our systems are secure, we have a firewall!
  - How good is the rule set?
- We are not a target!
  - Do not need to be a target (Malware, Ransomware)
- Hackers don‘t understand industrial automation systems!
  - Honeypots show otherwise
- What could possibly go wrong, we have safety systems installed!
  - Safety != Security

Related topics

Whitepaper: Top 20 cyber attacks on ICS

Featured news

(IN)SECURE Magazine issue 59 released

Break out of malware myopia by focusing on the fundamentals

How to gain visibility with global IT asset inventory

Data privacy automation: Unlock your most valuable asset

Preventing exfiltration of sensitive docs by flooding systems with hard-to-detect fakes

Tech support scammers leverage "evil cursor" technique to "lock" Chrome

Hackers wage a new Cold War

New infosec products of the week: September 14, 2018

Analysis of half-a-billion emails reveals malware-less email attacks are on the rise

Researchers exploring how IoT apps can to imitate human decisions

Magecart compromises Feedify to get to hundreds of e-commerce sites

DDoS attack frequency grows 40%, low volume attacks dominate

Zeljka Zorz, Managing Editor
December 15, 2017

Share this article

Attackers disrupt plant operations with ICS-tailored malware

Security researchers from FireEye and Dragos have analyzed and detailed a new piece of malware targeting industrial control systems (ICS).

Dubbed "TRITON" and "TRISIS" by the two groups of researchers, the malware was discovered after it was deployed against a victim in the Middle East, and inadvertently led to an automatically shutdown of the industrial process.

About the malware

The malware has been specifically designed to target Schneider Electric's Triconex Safety Instrumented System (SIS) – an autonomous control system

Source:
https://www.helpnetsecurity.com/2017/12/15/attackers-disrupt-plant-operations-ics-malware/

CYBER THREATS FOR ICS
THE HUMAN FACTOR - CHALLENGES

- Many TOP10 threats involve human factors
  - Directly and indirectly
  - Influence effectiveness of security architecture

- Misconceptions about ICS security persist
  - Missing awareness?
  - Missing points of contact within own field of work?

CYBER THREATS FOR ICS
THE HUMAN FACTOR - OPPORTUNITIES

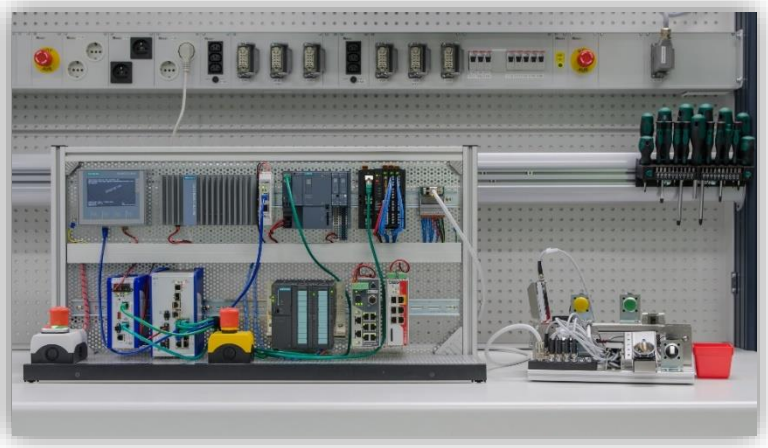
- Human factors are a main opportunity to increase cyber security
  - Increase cyber security effectiveness
  - Increase cyber attack resilience
  - Remedy vulnerabilities

- How can we achieve this?
  - Raise Awareness
  - Increase security knowledge in OT
    - As mentioned by cyber security standards (e.g. IEC 62443, Part 2-1)

➢ **Security trainings for industrial and automation professionals**

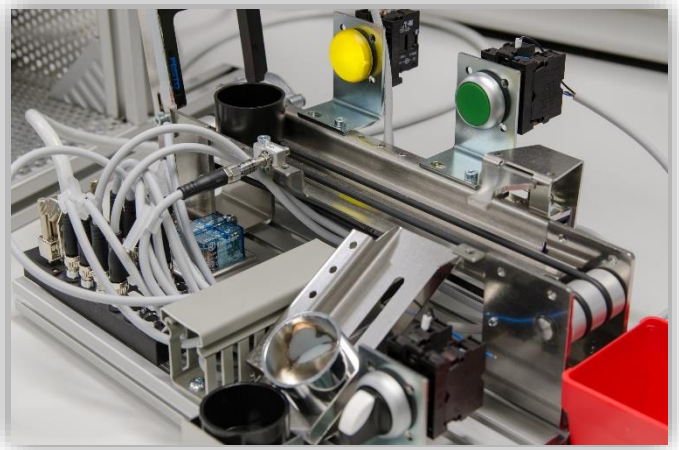
TRAINING FOR OT-PROFESSIONALS
FOCUS, TARGET AUDIENCE

- Effective training needs to
  - Address all relevant audiences
    - Management level
    - Engineer/ Developer level
    - Operator level
  - Be suited for respective audience
    - Focus on fields of interests / respective part of cyber security management system
    - Responsibilities
    - Organizational and technical knowledge



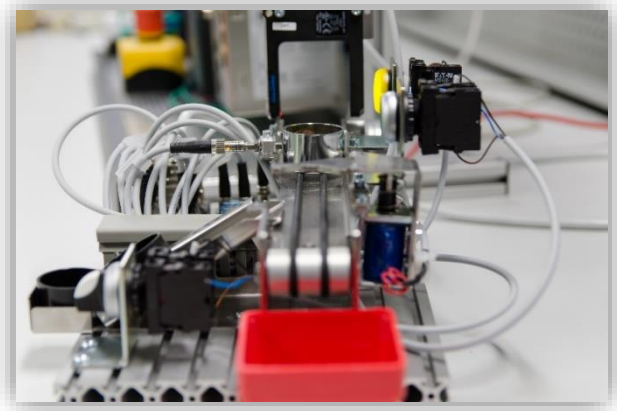
OUR TRAINING APPROACH
PROMOTING PROBLEM AWARENESS

- Awareness is the foundation of every security process
  - „Why do I need to do this?“
    - …allocate resources
    - …follow procedures
    - …show additional effort
- Raise awareness by
  - …showing what could happen
    - “How am I affected?“
  - …showing what is possible



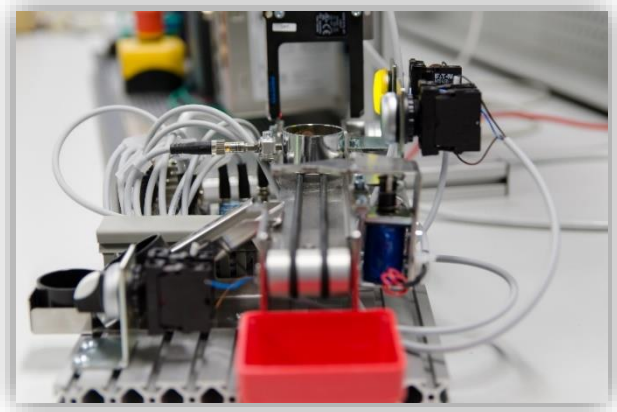
OUR TRAINING APPROACH
IMPLEMENT PRACTICAL RELEVANCE

- Trainings should be praxis-oriented
  - Participants should be able to recognize systems and behavior
    - Easier to understand underlying concepts
    - Improved applicability to own systems
  - Work on real systems and processes
    - Encourage usage of technologies
    - Experience effects of measures



OUR TRAINING APPROACH
IMPLEMENT PRACTICAL RELEVANCE

- Trainings should be praxis-oriented
  - React to situations
    - Learn how to handle threat situations
    - Foster problem-solving strategies
- Exercises should be repeatable
  - Increases the learning success



OUR TRAINING APPROACH
EXAMPLE TRAINING COURSE

- Training course in collaboration with Kaspersky Lab

- Target audience
  - Management level
  - Operator / Engineer level

- Real hardware demonstrators
  - Analyze network
  - Demonstrate attacks
  - Implement countermeasures

OUR TRAINING APPROACH
EXAMPLE TRAINING COURSE

- Structure
  - Risk awareness
  - Network and security basics
  - Risk addressing

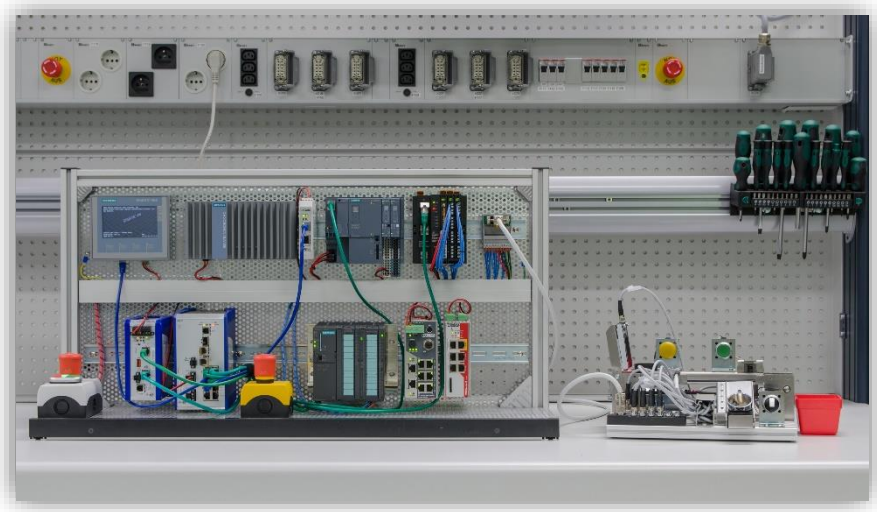
Knowledge on basic concepts and processes

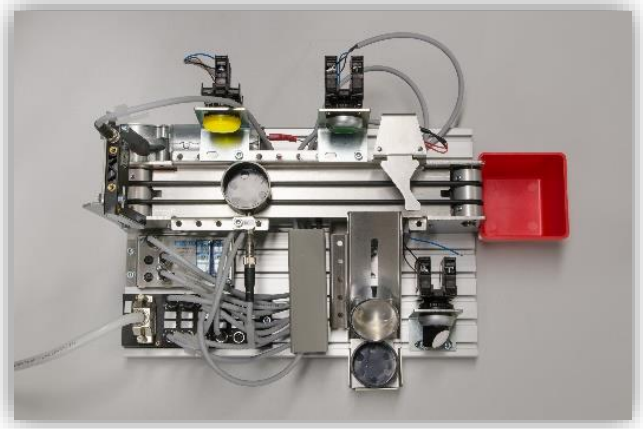
  - Countermeasures
  - Incident detection and handling
  - Vulnerability handling

Practical training and procedures

OUR TRAINING APPROACH IMPROVED EFFECTIVENESS

- Concentrate on the Human Factor
  - Focus on target audience
  - Enhance real-world applicability





- Hands-on experiences
  - For organizational knowledge
  - For practical knowledge
- Exercises to enhance knowledge

CONCLUSION
LESSONS LEARNED

- ICS are clearly at risk
  - Human factor is important
- Countermeasures and controls need to take human factor into account
  - Staff needs to be prepared accordingly
- Security awareness and training is the key
  - Needs to target key OT staff
  - Practical training similar to work processes