SEMINAR: OPERATIONAL TECHNOLOGY SECURITY WS23/24 PRE-COURSE MEETING 06.07.2023

Sebastian Peters, Veronique Ehmes

Fraunhofer

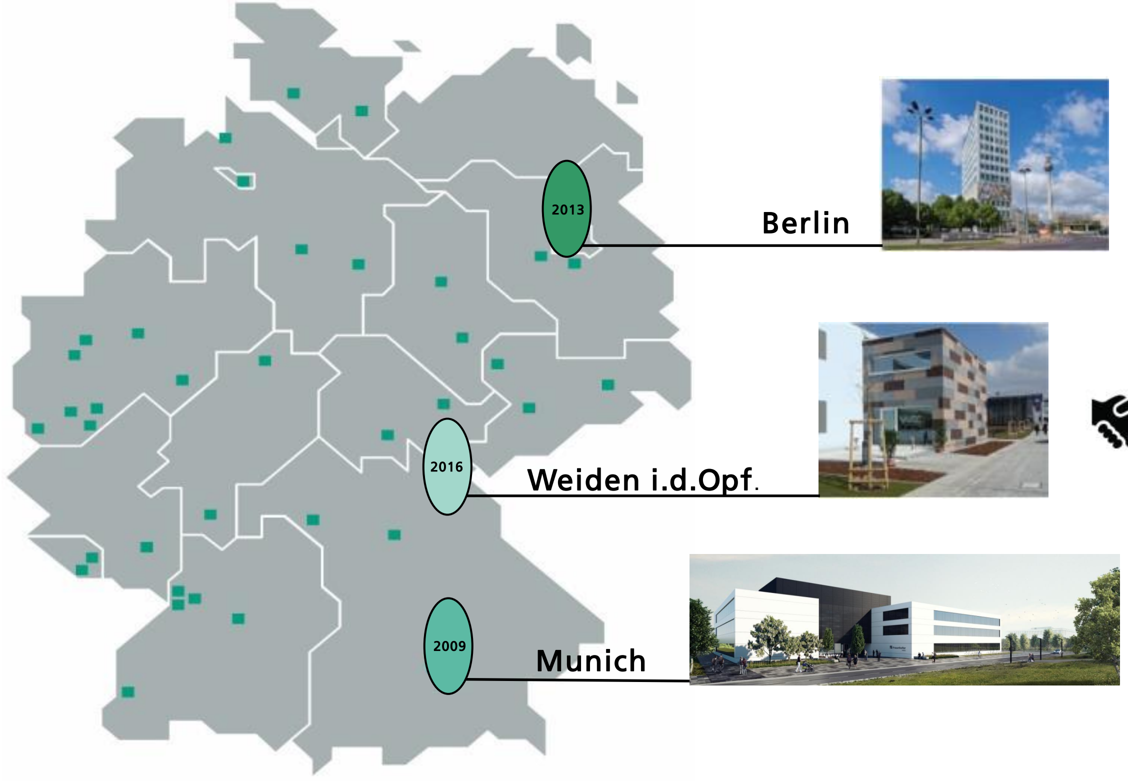
AISEC

SEMINAR: OPERATIONAL TECHNOLOGY SECURITY PRE-COURSE MEETING

- About Fraunhofer AISEC
- Course Objectives
- Orga
- Process
- Deliverables & Grading
- Paper & Presentation
- Topics
- FAQ

FRAUNHOFER AISEC
KEY FACTS & FIGURES

- Cognitive Security Technologies
- Hardware Security
- Product Protection & Industrial Security
- Service & Application Security
- Secure Operating Systems
- Secure Systems Engineering
- Secure Infrastructure



Freie Universität Berlin

Ostbayerische Technische Hochschule Amberg-Weiden

TUM Technische Universität München

<210 employees

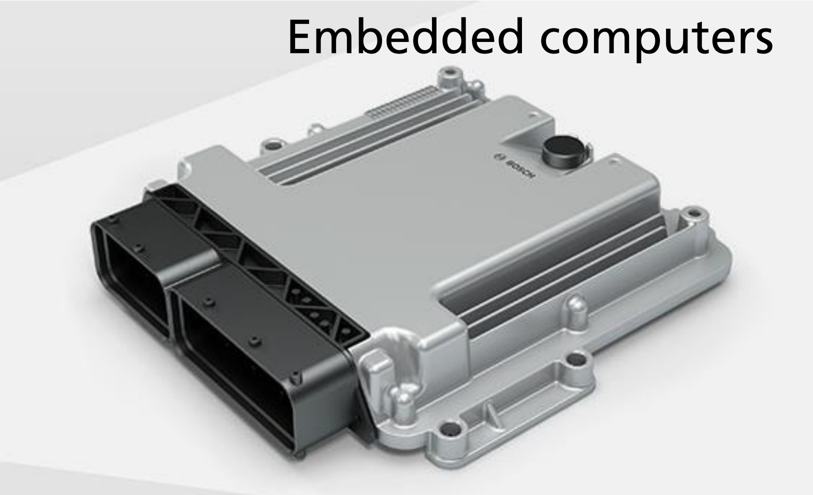
10 Hightech Security Labs

Funding €

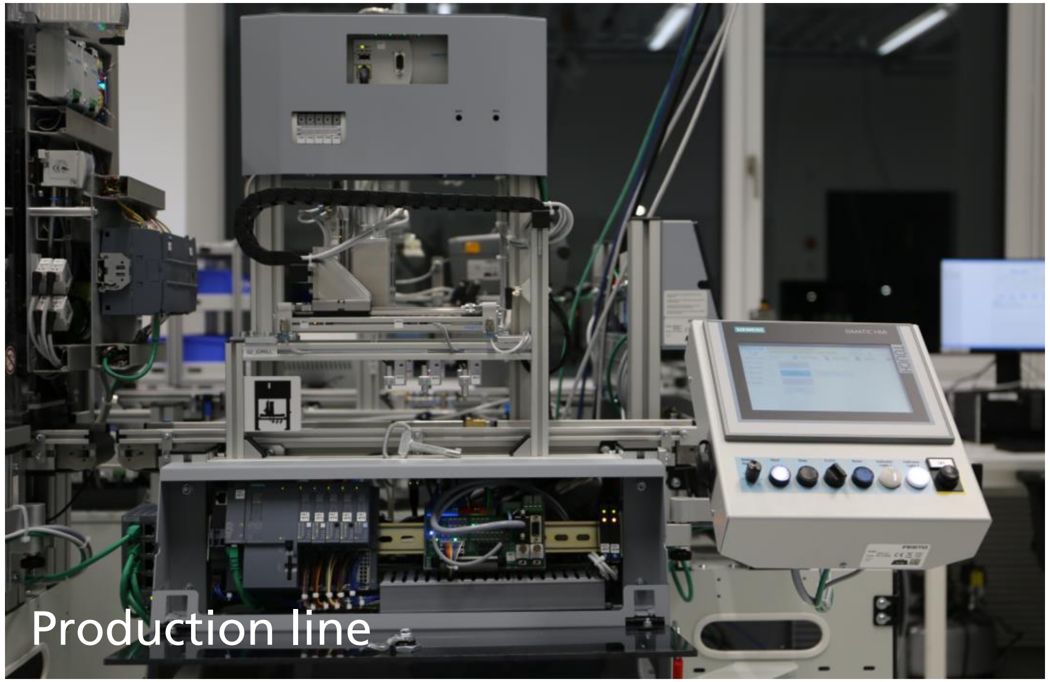
20% State directly

80% 3rd party research projects

What is OT?



Embedded computers



Production line

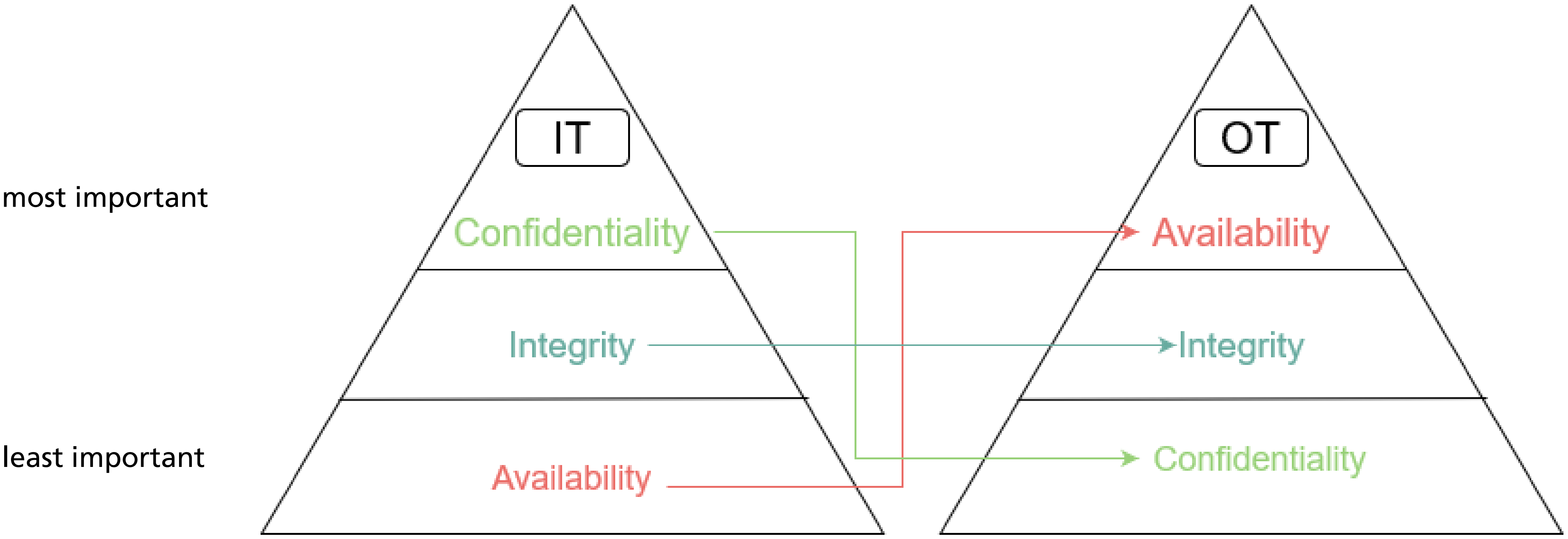
Robots

Automotive

PLCs

IT vs OT differences

Security triad (CIA) upside down (AIC)



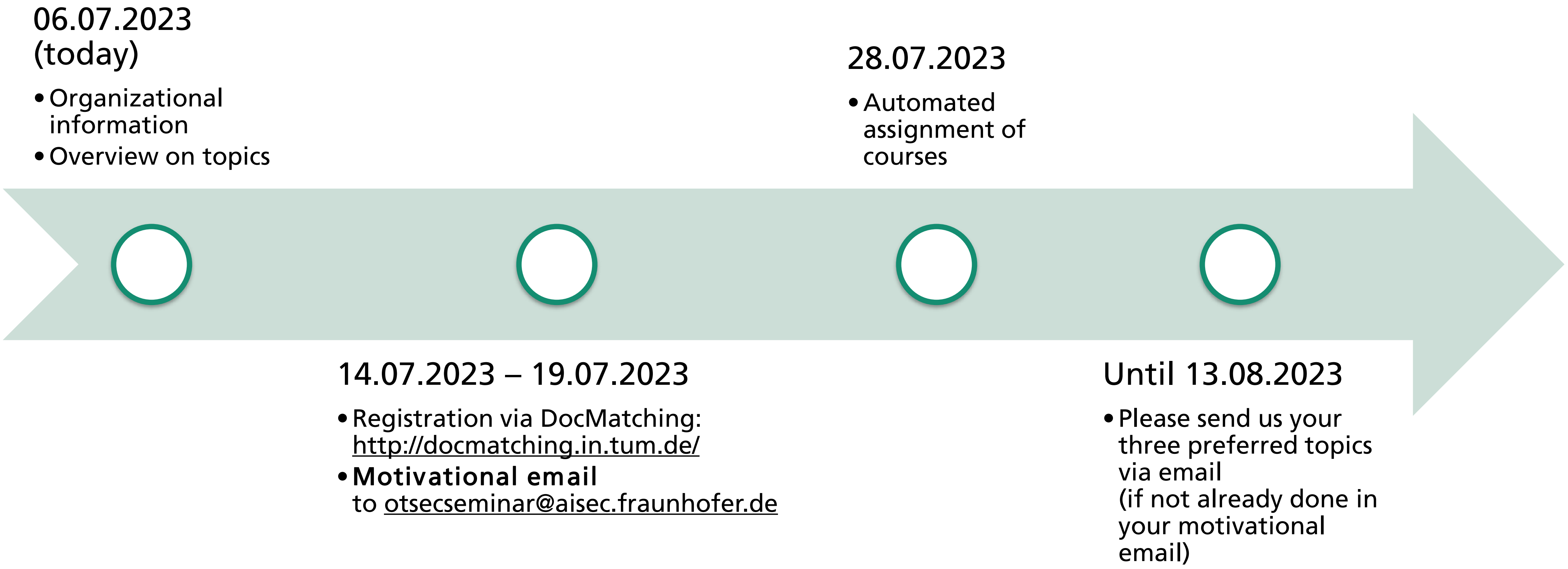
Course Objectives

- **Assessing** the state of the art regarding a specific topic in the context of OT security
  - **Write a paper** about your findings
  - **Give feedback** to (two of) your fellow students‘ papers (peer review)
  - **Give a talk** in order to **discuss** your topic with your fellow students at the end of the semester

Orga

- Communication
  - TUM Moodle
  - Video Calls via MS Teams
  - Email – **always use "reply-all"** when writing or answering to us!
  - Language of instruction and deliverables will be **English**
- Individual work (no groups)
- **Registration** in matching system (http://docmatching.in.tum.de/)
- **Motivational email** to otsecseminar@aisec.fraunhofer.de (e.g., which topic you like most, and why)

Process (1/4)



06.07.2023
(today)

- Organizational information
- Overview on topics

14.07.2023 – 19.07.2023

- Registration via DocMatching: http://docmatching.in.tum.de/
- **Motivational email** to otsecseminar@aisec.fraunhofer.de

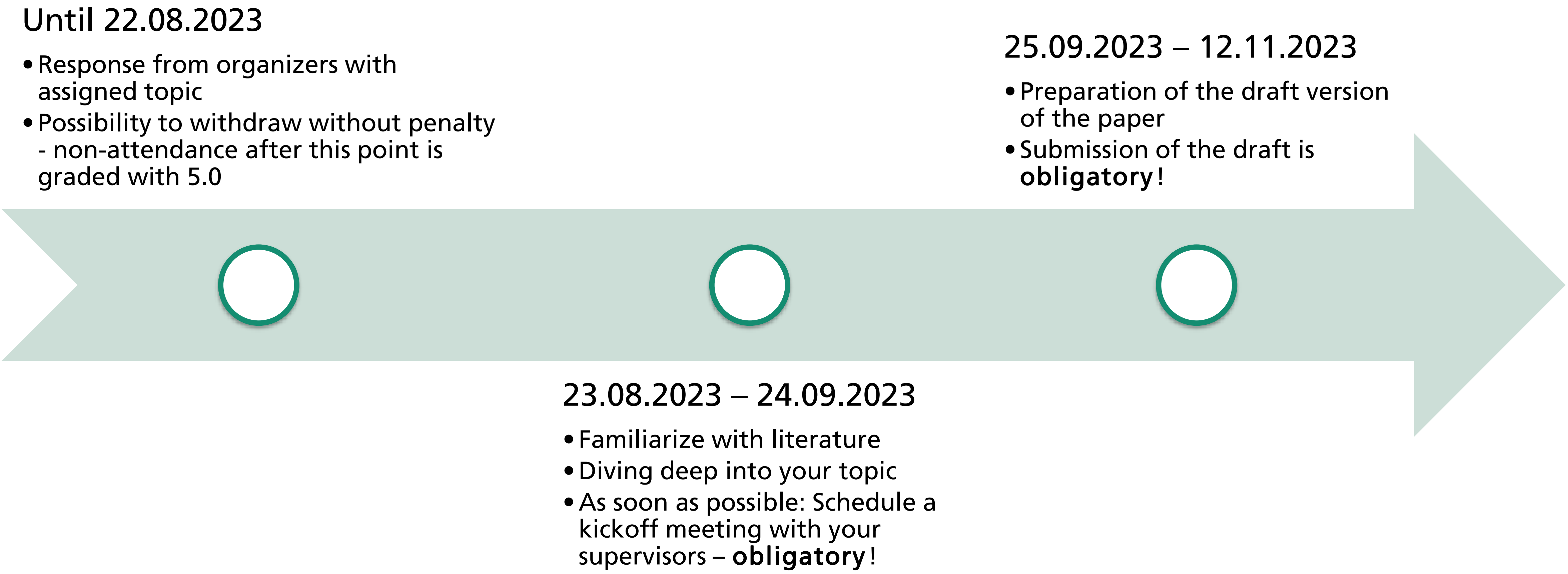
28.07.2023

- Automated assignment of courses

Until 13.08.2023

- Please send us your three preferred topics via email
(if not already done in your motivational email)

Process (2/4)



Until 22.08.2023

- Response from organizers with assigned topic
- Possibility to withdraw without penalty - non-attendance after this point is graded with 5.0

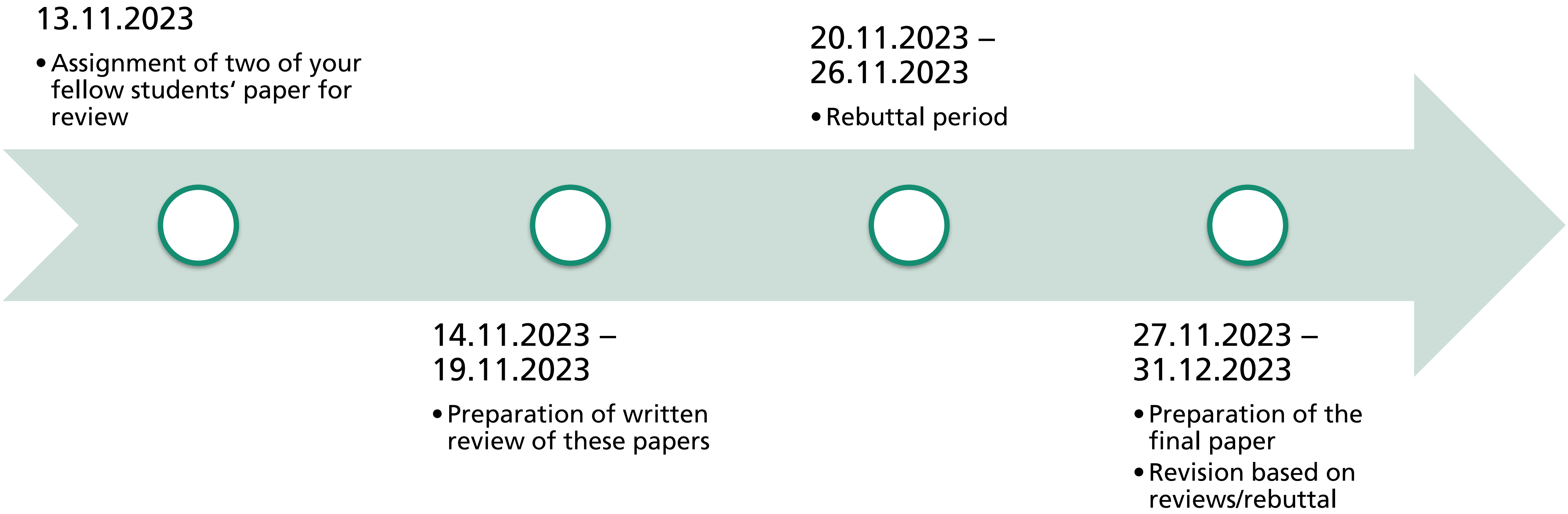
23.08.2023 – 24.09.2023

- Familiarize with literature
- Diving deep into your topic
- As soon as possible: Schedule a kickoff meeting with your supervisors – **obligatory**!

25.09.2023 – 12.11.2023

- Preparation of the draft version of the paper
- Submission of the draft is **obligatory**!

Process (3/4)



13.11.2023

- Assignment of two of your fellow students‘ paper for review

14.11.2023 – 19.11.2023

- Preparation of written review of these papers

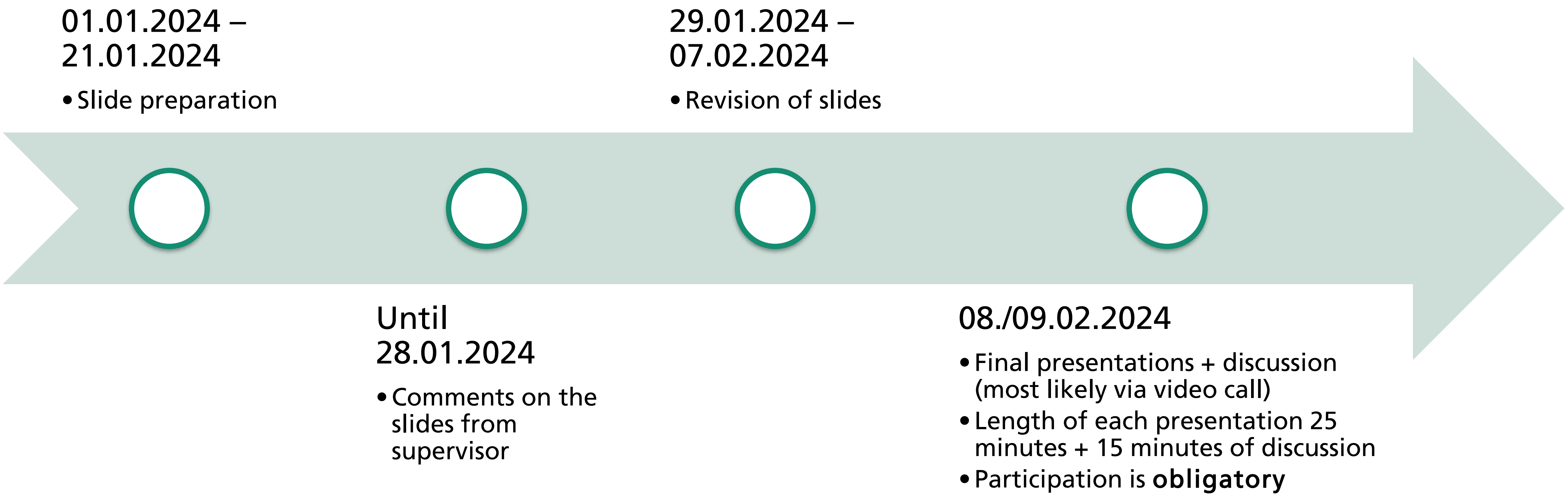
20.11.2023 – 26.11.2023

- Rebuttal period

27.11.2023 – 31.12.2023

- Preparation of the final paper
- Revision based on reviews/rebuttal

Process (4/4)



01.01.2024 –
21.01.2024

- Slide preparation

Until
28.01.2024

- Comments on the slides from supervisor

29.01.2024 –
07.02.2024

- Revision of slides

08./09.02.2024

- Final presentations + discussion (most likely via video call)
- Length of each presentation 25 minutes + 15 minutes of discussion
- Participation is **obligatory**

Obligatory Deliverables

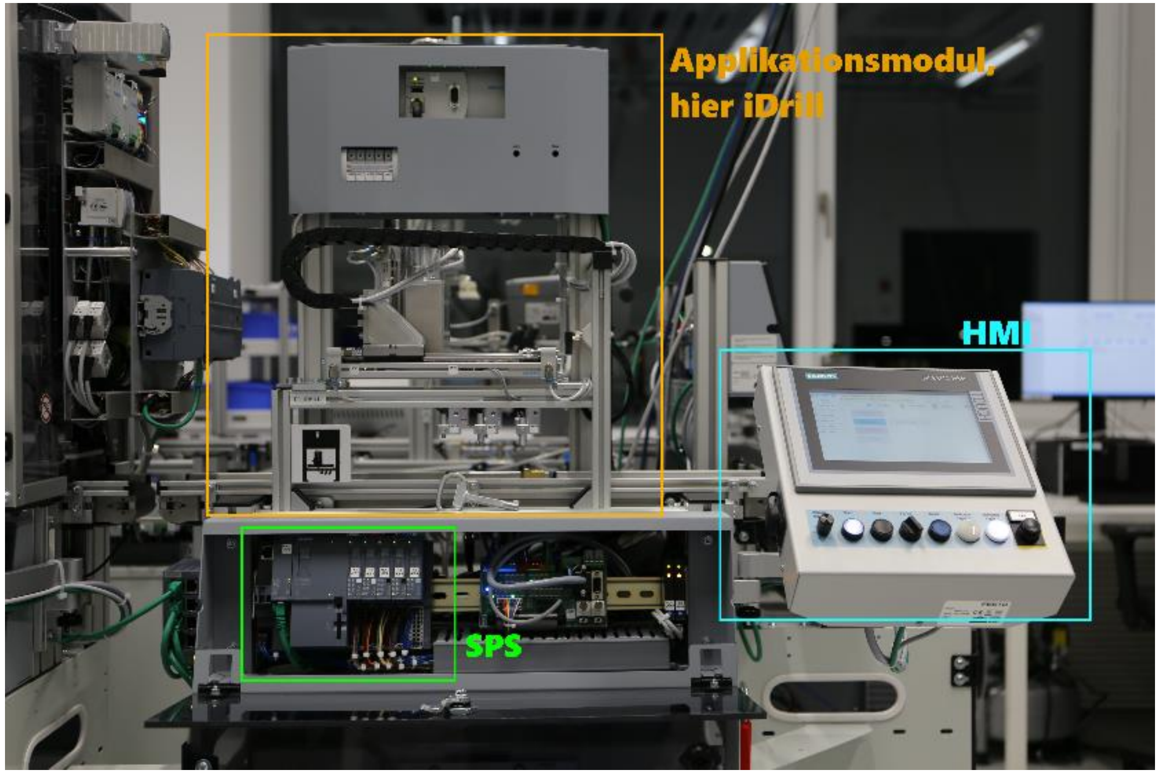
	Due to	Grading
1-to-1 Kick-Off Meeting with supervisors	24.09.2023	-
Submission of Draft Paper	12.11.2023	5%
Reviews & Rebuttal	19.11.2023 26.11.2023	5%
Submission of Final Paper	31.12.2023	50%
Presentation	08./09.02.2024	30%
Presentation Discussion	08./09.02.2024	10%
		Σ 100 %

Paper writing and presentation

- Paper
  - Systematization of Knowledge (SoK)
  - ~10 pages excl. list of references and appendices
  - IEEE conference proceedings template
  - Utilization of LaTeX (highly recommended)
  - Note the *Scientific writing guide* in the Moodle course
- Presentation
  - MS Powerpoint or similar
  - 25 minutes presentation
  - 15 minutes discussion - moderated by you

Topics (Overview)

1. Secure date and time in OT/automotive
2. Secure remote attestation for safety-critical OT
3. Secure PLC Programming
4. History of authentication in OT
5. Security of UWB in OT/Automotive
6. IDS in OT
7. Anomaly Detection in OT
8. Applications of homomorphic encryption in OT
9. Secure bootstrapping in OT and (I)IoT
10. Secure Manufacturing Process Chains
11. OT attack datasets
12. Common vulnerability and exposure (CVEs) ecosystems



Topic 1: Secure date and time in OT/automotive

Possible questions to be answered: Which protocols/standards exists to sync date/time securely? Which concepts/approaches of date/time exist? Which known attacks target date/time functionality in OT or automotive?

Literature to start from:

- A Secure Time Synchronization Protocol Against Fake Timestamps for Large-Scale Internet of Things (2017) - https://ieeexplore.ieee.org/abstract/document/7947091
- Secure time in a portable device (2001) - https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=10636c36498b4cd8e0ad9ddd262e096edb7cf663
- A Survey of Secure Time Synchronization (2023) - https://www.mdpi.com/2076-3417/13/6/3923
- Robust and Secure Time-Synchronization Against Sybil Attacks for Sensor Networks - https://ieeexplore.ieee.org/abstract/document/7307178
- Next Steps in Security for Time Synchronization: Experiences from implementing IEEE 1588 v2.1 (2019) - https://ieeexplore.ieee.org/abstract/document/8886641
- On the Security of IEEE 802.1 Time-Sensitive Networking - https://ieeexplore.ieee.org/abstract/document/9473542

Topic 2: Secure remote attestation for safety-critical OT

Possible questions to be answered:

Which problems does remote attestation solve? Categorize solutions/standards/approaches. What are difficulties of remote attestation? How does the environment influence the attestation requirements?

Literature to start from:

- Remote Attestation: A Literature Review - https://arxiv.org/abs/2105.02466
- Secure remote access to autonomous safety systems: A good practice approach - https://www.researchgate.net/publication/242259414_Secure_remote_access_to_autonomous_safety_systems_A_good_practice_approach
- HSE and Cyber Security in Remote Work - https://ieeexplore.ieee.org/abstract/document/9478249
- Safety of Unmanned Ships - https://aaltodoc.aalto.fi/handle/123456789/28061
- Development of Dam Safety Remote Monitoring & Evaluation - https://www.jstage.jst.go.jp/article/jdr/16/4/16_607/_article/-char/ja/
- Federated Remote Labs - https://link.springer.com/chapter/10.1007/978-3-030-52575-0_2
- Real-Time Video Latency Measurement between a Robot and Its Remote Control Station: Causes and Mitigation - https://www.researchgate.net/publication/329369713_Real-Time_Video_Latency_Measurement_between_a_Robot_and_Its_Remote_Control_Station_Causes_and_Mitigation

Topic 3: Secure PLC Programming

Possible questions to be answered:

How to securely develop programs for OT devices? What are similarities and differences to IT development? How do development techniques differ?

Literature to start from:

- Software security: Application-level vulnerabilities in SCADA systems - https://ieeexplore.ieee.org/abstract/document/6009603
- Programmable logic controllers based systems (PLC-BS): vulnerabilities and threats https://link.springer.com/article/10.1007/s42452-019-0860-2
- Awareness of Secure Coding Guidelines in the Industry - A First Data Analysis https://ieeexplore.ieee.org/abstract/document/9343011
- Employing secure coding practices into industrial applications: a case study https://link.springer.com/article/10.1007/s10664-014-9341-9
- Empirical Study of PLC Authentication Protocols in ICS - https://ieeexplore.ieee.org/abstract/document/9474296
- Walking under the ladder logic: PLC-VBS: a PLC control logic vulnerability scanning tool https://www.sciencedirect.com/science/article/pii/S0167404823000263
- [non-scientific] Top 20 Secure PLC Coding Practices - https://plc-security.com/content/Top_20_Secure_PLC_Coding_Practices_V1.0.pdf

Topic 4: History of Authentication in OT

Possible questions to be answered:

How has authentication in OT developed over the years? Which methods have been added? Which ones are not pursued any further? How have recommendations changed over the years (length of passwords, regular changing of passwords, use of MFA, use of EC, …)? Which standard works have been published by relevant organisations (BSI, IEC, NIST, etc.) or researchers and had an impact?

Literature to start from:

- A Review on Authentication Methods - https://hal.science/hal-00912435v1/preview/A_Review_on_Authentication_Methods.pdf#page=2
- A survey on continuous authentication methods in Internet of Things environment - https://www.sciencedirect.com/science/article/abs/pii/S0140366420319204
- Modern Authentication Methods: A Comprehensive Survey – https://www.intechopen.com/journals/1/articles/100
- Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications – https://ieeexplore.ieee.org/abstract/document/8675176
- Empirical Study of PLC Authentication Protocols in Industrial Control Systems – https://ieeexplore.ieee.org/abstract/document/9474296
- [idea for analogous methodology] Two decades of SCADA exploitation: A brief history – https://ieeexplore.ieee.org/document/8270432

Relevant standards:

BSI ICS-Security-Kompendium (2013) and later/related recommendations

NIST Guide to Industrial Control Systems (ICS) Security (Rev1 2013, Rev2 2015)

ISA/IEC 62443 Industrial communication networks – Network and system security (revs from 2009-2020)

Topic 5: Security of UWB in OT/Automotive

Possible questions to be answered: What is UWB and how does it work? How can it improve security of user to vehicle authentication? How does it compare to previous solutions? Which problems does it solve in (I)IoT?

Literature to start from:

- An Evaluation of UWB for Location-Based Hands-Free Authentication Charging of Electric Vehicles - https://ieeexplore.ieee.org/abstract/document/9831628
- Ultra-wideband (UWB) for the IoT–a fine ranging revolution (Whitepaper) - https://www.allaboutcircuits.com/uploads/articles/UWBWP.pdf
- Security analysis of IEEE 802.15.4z/HRP UWB time-of-flight distance measurement - https://dl.acm.org/doi/abs/10.1145/3448300.3467831
- Ultra-Wideband Technology in Telematics Security - A short Survey - https://ieeexplore.ieee.org/abstract/document/9515057

Topic 6: Intrusion Detection Systems in OT

Possible questions to be answered:

What is an Intrusion Detection System (IDS)? What are ways to enhance IDS to sufficiently protect the OT environment? What are future recommendations and guidance related to cybersecurity issues for IDS in the IoT environment? What is the difference between anomaly detection and IDS?

Literature to start from:

- A Comprehensive Analyses of Intrusion Detection System for IoT Environment - https://doi.org/10.3745/JIPS.03.0144
- A three-tiered intrusion detection system for industrial control systems – https://doi.org/10.1093/cybsec/tyab006
- Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks – https://dl.acm.org/doi/10.1145/3264888.3264896
- Cyber-Physical Architecture for Automated Responses (CyPhAAR) Using SDN in Adversarial OT Environments – https://ieeexplore.ieee.org/document/9241285

Topic 7: Anomaly Detection in OT

Possible questions to be answered:

What is Anomaly Detection and how is it used to secure the OT environment? What are open research topics, like privacy preserving anomaly detection? What are the most common used techniques for Anomaly detection and what makes it a good/bad approach e.g., Machine Learning with Autoencoders?

Literature to start from:

- WADAC: Privacy-Preserving Anomaly Detection and Attack Classification on Wireless Traffic - https://doi.org/10.1145/3212480.3212495
- Anomaly Detection: A Survey - http://doi.acm.org/10.1145/1541880.1541882
- Distributed Anomaly Detection of Single Mote Attacks in RPL Networks - http://doi.org/10.5220/0007836003780385
- High-Performance Unsupervised Anomaly Detection for Cyber-Physical System Networks - https://doi.org/10.1145/3264888.3264890

Topic 8: Applications of homomorphic encryption in OT

Possible questions to be answered:

What is homomorphic encryption? Which problems can such algorithms solve? How can homomorphic encryption be used in OT?

Literature to start from:

- Protecting privacy in practice, The Royal Society – https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/Protecting-privacy-in-practice.pdf?la=en-GB&hash=48A28CDF4FB012663652BE671CFFED08
- Homomorphic Encryption in Manufacturing Compliance Checks – https://link.springer.com/chapter/10.1007/978-3-031-17926-6_6
- A privacy-preserving resource trading scheme for Cloud Manufacturing with edge-PLCs in IIoT – https://www.sciencedirect.com/science/article/abs/pii/S1383762121000825
- Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption - https://www.sciencedirect.com/science/article/pii/S0022000017300284#fg0010

Topic 9: Secure bootstrapping in OT and (I)IoT

Possible questions to be answered: Which algorithms exist for secure bootstraping? How do they compare in detail? Which features do they have in common, which ones does a protocol have exclusively, which ones should they have? What are their different target groups/applications?

Literature to start from:

- On the Security of IIoT Deployments: An Investigation of Secure Provisioning Solutions for OPC UA - https://ieeexplore.ieee.org/document/9478911
- Zero-touch bootstrap of a network connected device - https://www.tdcommons.org/cgi/viewcontent.cgi?article=2980&context=dpubs_series
- Accountable Bootstrapping Based on Attack Resilient Public Key Infrastructure and Secure Zero Touch Provisioning – https://ieeexplore.ieee.org/abstract/document/9996145
- Protocol specifications:
  - BRSKI/EST - https://datatracker.ietf.org/doc/rfc8995/ and https://datatracker.ietf.org/doc/html/rfc7030
  - SZTP - https://datatracker.ietf.org/doc/rfc8572/
  - FIDO automatic onboarding - https://fidoalliance.org/intro-to-fido-device-onboard/
  - OMA LwM2M - https://technical.openmobilealliance.org/index.html
  - Wi-Fi Alliance Device Provisioning Protocol (DPP) - https://www.wi-fi.org/downloads-public/Device_Provisioning_Protocol_Specification_v1.1_1.pdf/35330

Topic 10: Secure Manufacturing Process Chains

Possible questions to be answered:

What are methods to secure multi-party manufacturing or to enable secure manufacturing-as-a-service (MaaS)?

Literature to start from:

- Hardware Rooted Trust for Additive Manufacturing - https://doi.org/10.1109/ACCESS.2019.2923573
- Blockchain-based ubiquitous manufacturing: a secure and reliable cyber-physical system - https://doi.org/10.1080/00207543.2019.1680899A
- Privacy-preserving resource trading scheme for Cloud Manufacturing with edge-PLCs in IIoT - https://doi.org/10.1016/j.sysarc.2021.102104
- A Blockchain-Based G-Code Protection Approach for Cyber-Physical Security in Additive Manufacturing - https://doi.org/10.1115/1.4048966
- Blockchain in Distributed CAD Environments - https://doi.org/10.1007/978-3-030-18072-0_3
- Intellectual Property Protection of 3D Print Supply Chain with Blockchain Technology - https://doi.org/10.1109/ICE.2018.8436315

Topic 11: OT Attack Datasets

Possible questions to be answered:

What attacks are the most common in OT networks and what traces do they leave in the logs?
What are useful aspects of them, especially regarding machine learning?
What requirements can be derived for an optimal OT adversary dataset?

Literature to start from:

- Building a dataset through attack pattern modeling and analysis system - https://doi.org/10.1016/j.compeleceng.2021.107614
- eXplainable and Reliable Against Adversarial Machine Learning in Data Analytics - https://ieeexplore.ieee.org/document/9852204
- Datasets are not Enough: Challenges in Labeling Network Traffic - https://www.sciencedirect.com/science/article/pii/S0167404822002048
- Dataset of anomalies and malicious acts in a cyber-physical subsystem - https://www.sciencedirect.com/science/article/pii/S2352340917303402
- A Survey on Industrial Control System Testbeds and Datasets for Security Research - https://ieeexplore.ieee.org/abstract/document/9471765
- SWaT Dataset - https://itrust.sutd.edu.sg/testbeds/secure-water-treatment-swat/

Topic 12: Common vulnerability and exposure (CVEs) ecosystems

Possible questions to be answered:

What are CVEs and Security Advisories? What kind of vulnerability databases do exist and how can they be mapped to each other logically? How can vulnerabilities be mapped to OT incidents? How do individual CVEs change throughout their lifetime?

Vulnerability Databases to be considered:

- NIST NVD (National Vulnerability Database) https://nvd.nist.gov/vuln/search
- GitHub Security Advisory https://github.com/advisories/
- Common Weakness Enumeration https://cwe.mitre.org/index.html
- Google ecosystem: A distributed vulnerability database for Open Source https://osv.dev/
- CVExploits Search: Your comprehensive database for CCVE exploits from across the internet https://cvexploits.io/

Scientific Sources to start from:

- Analysis of Vulnerability Trends and Attacks in OT Systems https://link.springer.com/chapter/10.1007/978-981-19-1610-6_12
- Mapping of CVE-ID to Tactic for Comprehensive Vulnerability Management of ICS https://link.springer.com/chapter/10.1007/978-981-19-4960-9_44
- Topic Modeling And Classification Of Common Vulnerabilities And Exposures Database: https://ieeexplore.ieee.org/abstract/document/9183814

FAQ

- Do I need to answer all the „*possible questions*“?
  - *No. They are just an orientation/a starting point.*
- Do I need to include all the listed publications in my SoK paper?
  - *No. Not even a single one, if you find better/more interesting/more fitting ones on your topic.*
- Many listed publications = lots of work?
  - No. Just lots of hints ;-)
- Are the listed publications to be considered conclusively?
  - *No. You are expected to find and read a lot more!*
- Do I need to read each publication completely?
  - *No. Learn quick-reading to quickly sort out less interesting* publications.
- How can I access publication xyz or specification abc?
  - *Check the university library tools. University VPN. Main authors webpage.*
- How to find scientific literature?
  - *Attend a course on scientific writing! References of the listed papers. Google Scholar & Co.*

Thanks for your attention. Open questions?

Veronique Ehmes, Sebastian Peters
Department Product Protection & Industrial Security
Fraunhofer Institute for Applied and Integrated Security AISEC

otsecseminar@aisec.fraunhofer.de

Address: Fraunhofer AISEC
Lichtenbergstr. 11
85748 Garching
Germany
Internet: www.aisec.fraunhofer.de

Fraunhofer
AISEC