AsIf: Asset Interface Analysis of Industrial Automation Devices

@8th Cyber Security in Networking Conference (CSNet 2024)

Thomas Rosenstatter, Christian Schäfer, Olaf Saßnick, Stefan Huber

Josef Ressel Center for Intelligent and Secure Industrial Automation
Department for Information Technologies and Digitalisation
Salzburg University of Applied Sciences

2nd December 2024

Salzburg University
of Applied Sciences

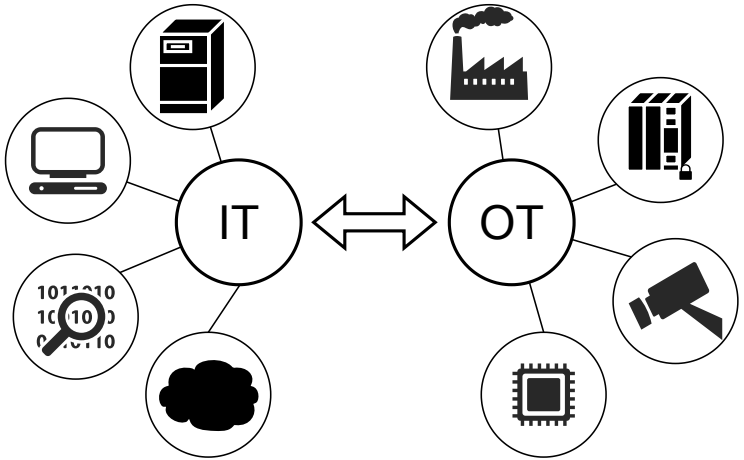
OT is not IT

Information Technology

- is for the cyber space
- examples are personal computer, office

Operational Technology

- is for the physical space
- examples are chemical, transportation, manufacturing, defense, ...



OT is about distributed, realtime, embedded, cyber-physical systems

Industrial Automation Systems


Internet, Cloud

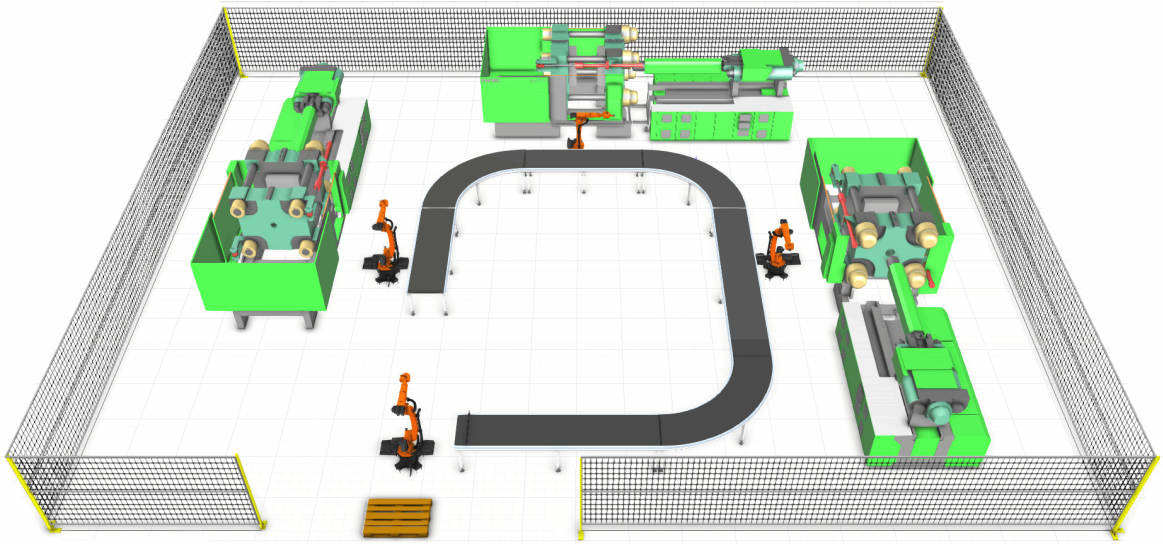

Business Planning


Plant DMZ


Monitoring & Control

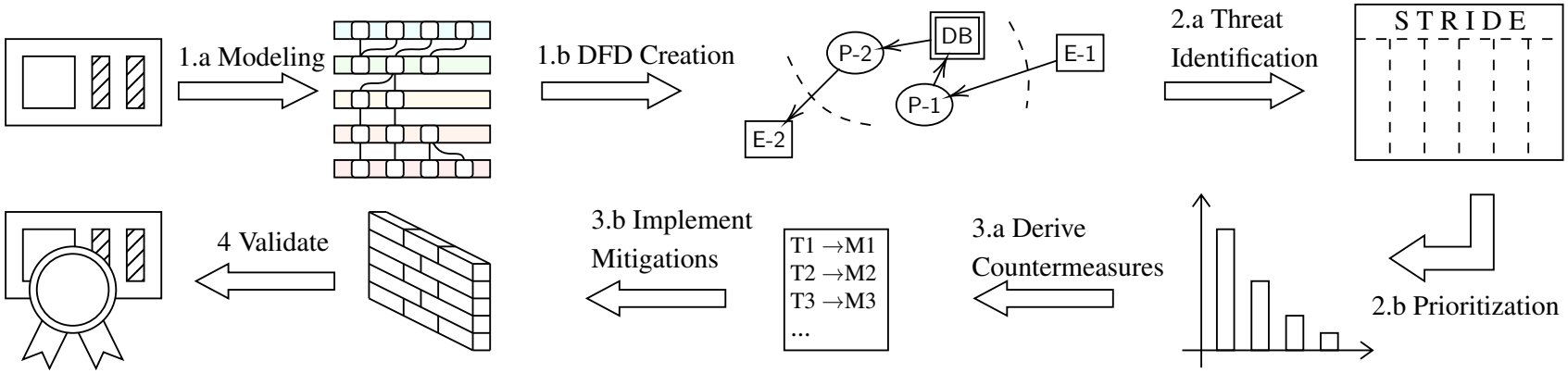

Programmable Logic Controllers


Sensors, Actuators



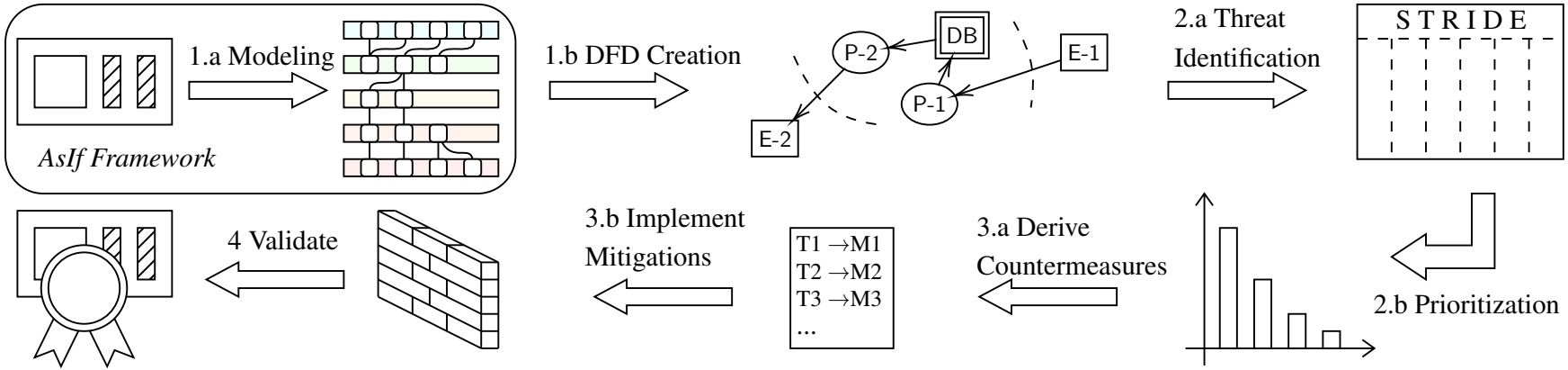
With Industry 4.0, CPS are more connected and have become viable targets for cyber attacks.

Threat modeling supports threat identification (detection)

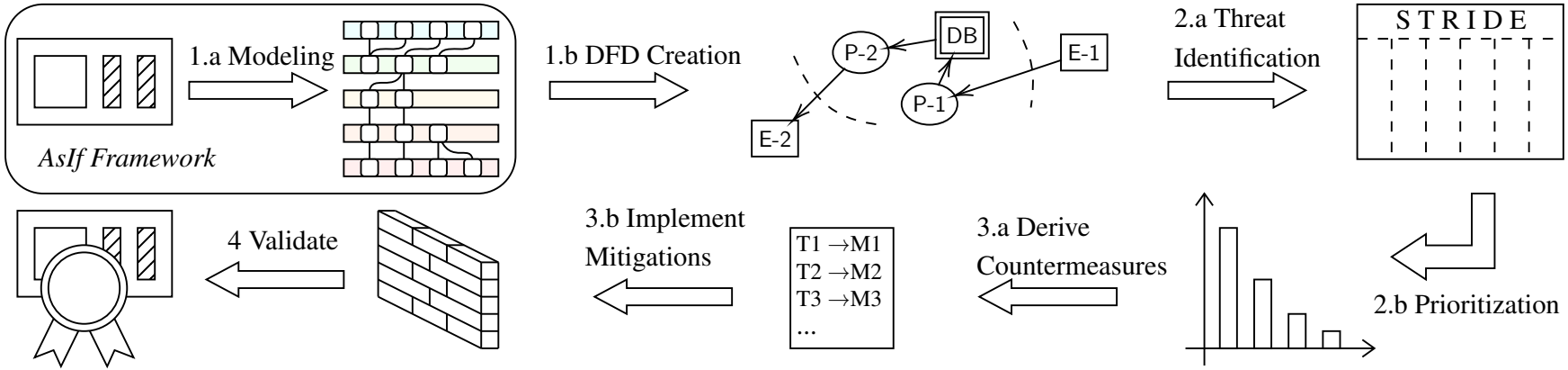


- Modeling and asset identification is often done through semi-structured meetings and brainstorming [Ysk+20]; [Sho14]
- Studies using STRIDE used different ways to model the system [Saß+24]

Threat modeling supports threat identification (detection)



Threat modeling supports threat identification (detection)



- **RQ.1** How can we effectively address the challenges of exhaustively modeling OT systems?
- **RQ.2** What are the current industrial perspectives on threat modeling practices and their impact on security posture?

- ISO/OSI model as guidance for modeling
- Identify assets in a bottom-up approach
- Visualise dependencies between interfaces – (*Interface Tree*)
- Infer data flow diagrams (DFDs) from the interface trees

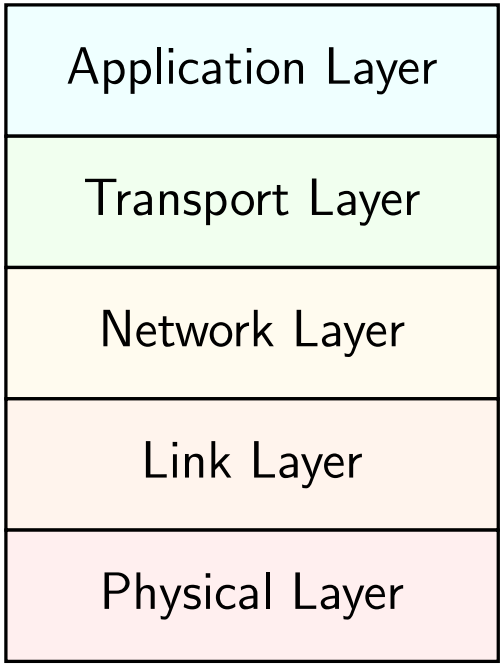


Figure: Hybrid TCP/IP model by Tanenbaum [TW10].

- step-by-step methodology
- offers systematic and exhaustive analysis
- provides a better understanding of the system
- physical interfaces will not be overlooked

This is important, as

- interconnection of machines is a central aspect of modern, industrial automation[1].
- interfaces are typically entry points for attacks

[1] Interconnection is also a central aspect of *Industry 4.0* [HPO16]

Aslf Interface Analysis

Interfaces are identified layer-by-layer:

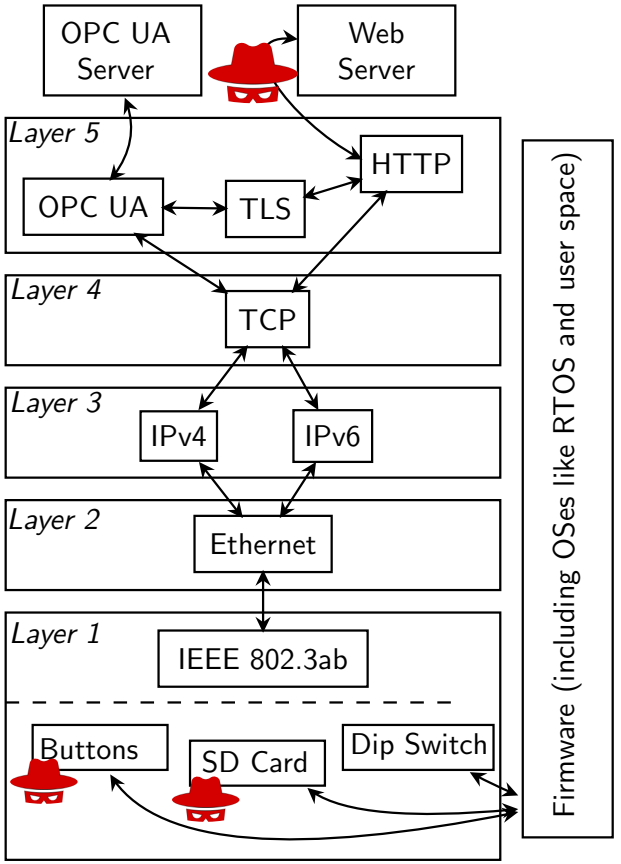
Layer	**Exemplary Methods***
Application Layer	Individually, based on the transport layer results from `Nmap` scan and `tcpdump` for open TCP & UDP ports
Transport Layer	`Nmap` scan for supported IP protocols
Network Layer	`Wireshark` and `tcpdump` traffic analysis
Link Layer	Derived from Physical Layer
Physical Layer	Physical inspection

*Note, based on the environment, further methods may be useful.

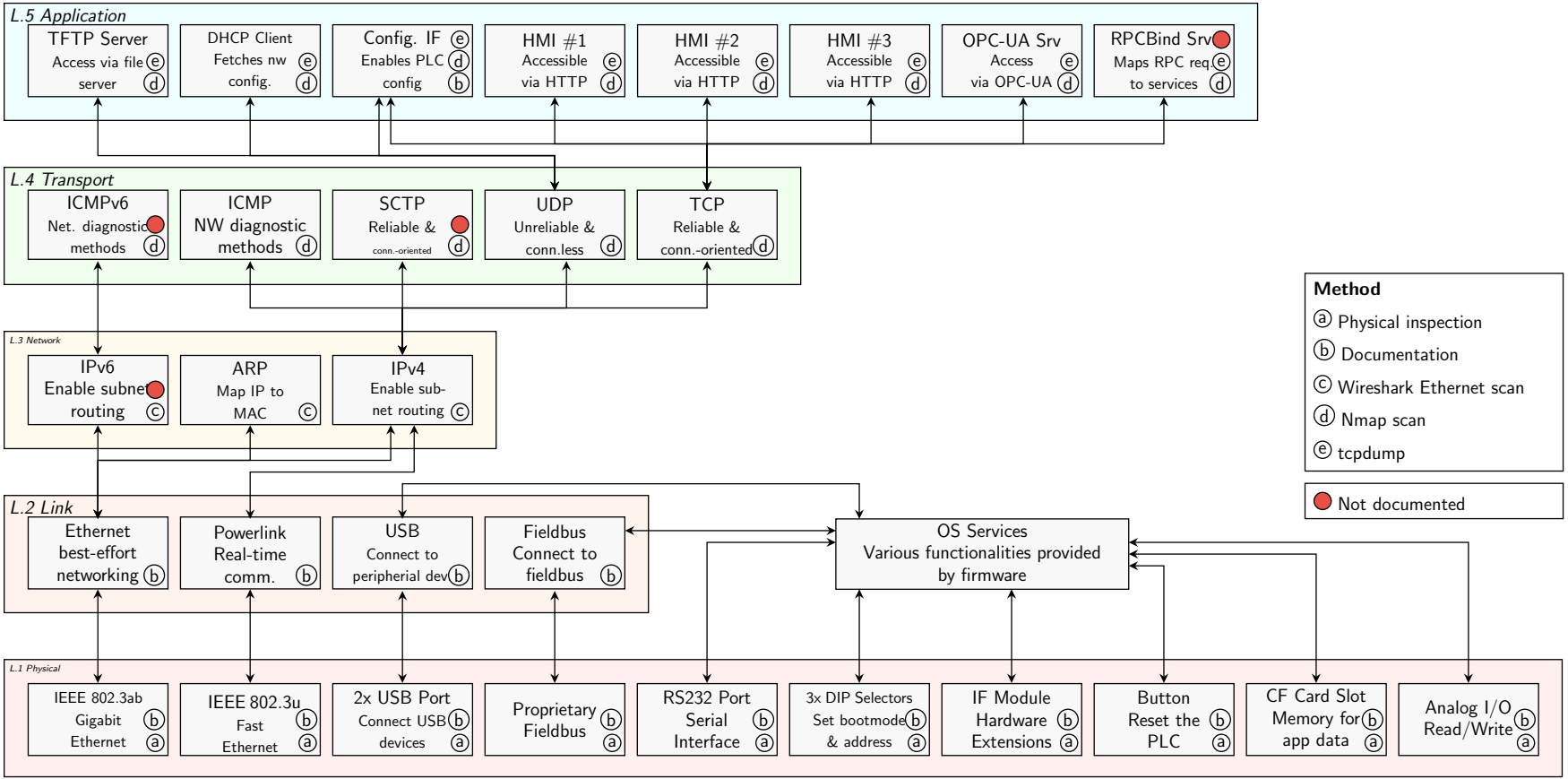
- Results are visualised as **Interface Tree**.

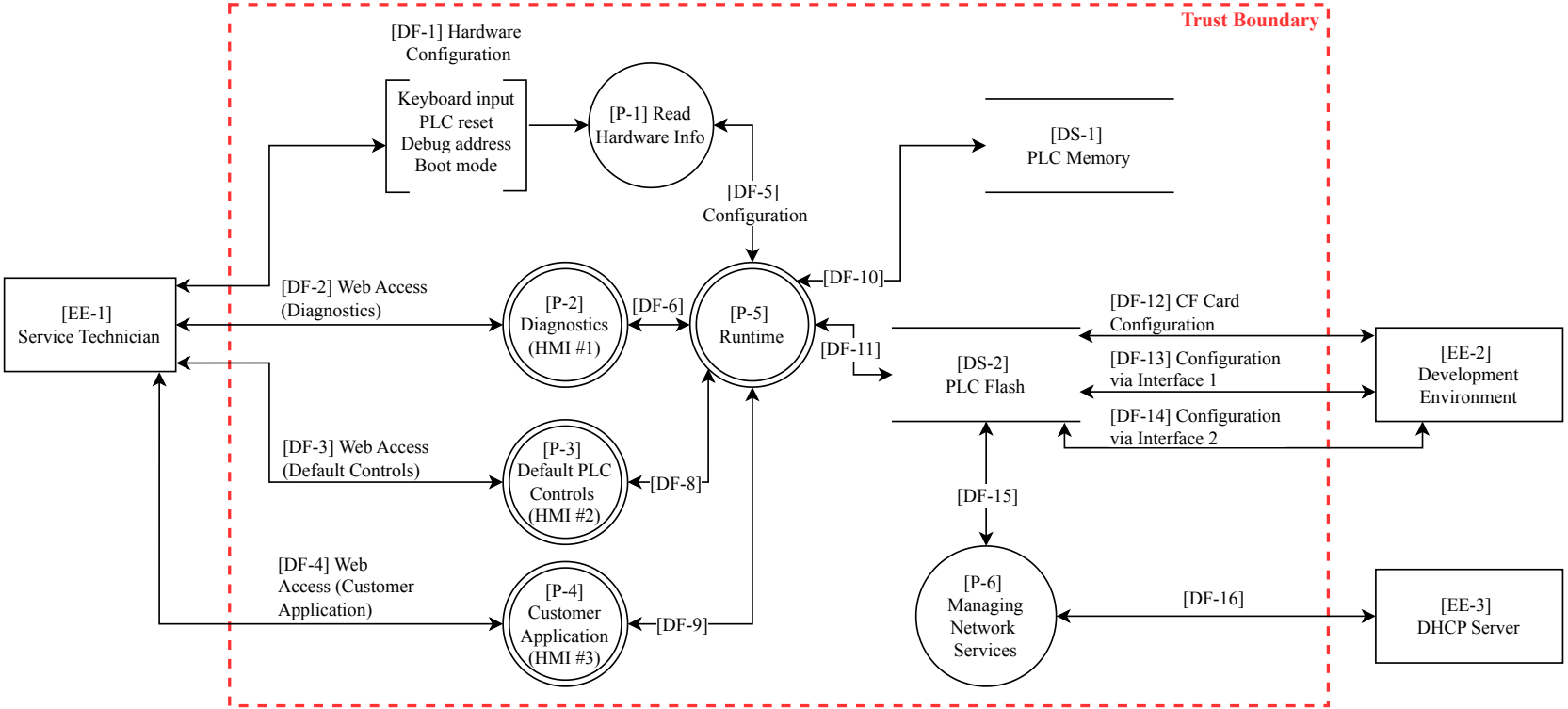
Aslf Interface Tree

- Start with the lowest level
- Identify accessible hardware interfaces, e.g., buttons, storage media, debug interfaces
- connect the interfaces, e.g., Ethernet enables IPv4 and IPv6 in the upper layer
- on top, an OPC UA server and web servers are running



Aslf Interface Tree




Trust Boundary
[DF-1] Hardware Configuration
Keyboard input
PLC reset
Debug address
Boot mode
[P-1] Read Hardware Info
[DS-1] PLC Memory
[DF-5] Configuration
[EE-1] Service Technician
[DF-2] Web Access (Diagnostics)
[P-2] Diagnostics (HMI #1)
[DF-6]
[P-5] Runtime
[DF-10]
[DF-11]
[DF-12] CF Card Configuration
[DF-13] Configuration via Interface 1
[DF-14] Configuration via Interface 2
[DS-2] PLC Flash
[EE-2] Development Environment
[DF-3] Web Access (Default Controls)
[P-3] Default PLC Controls (HMI #2)
[DF-8]
[DF-15]
[DF-4] Web Access (Customer Application)
[P-4] Customer Application (HMI #3)
[DF-9]
[P-6] Managing Network Services
[DF-16]
[EE-3] DHCP Server

How is Industry Perceiving Threat Modeling?

Facts about the questionnaire:

- Video[2] introducing Aslf
- 22 Questions[3]
- three parts: (i) background of participants, (ii) security in industrial systems, (iii) Aslf evaluation
- target group works in R&D at a company within the industrial systems domain

[2] https://www.youtube.com/watch?v=2GpFI3XDmgA

[3] https://doi.org/10.5281/zenodo.11201810

How is Industry Perceiving Threat Modeling?

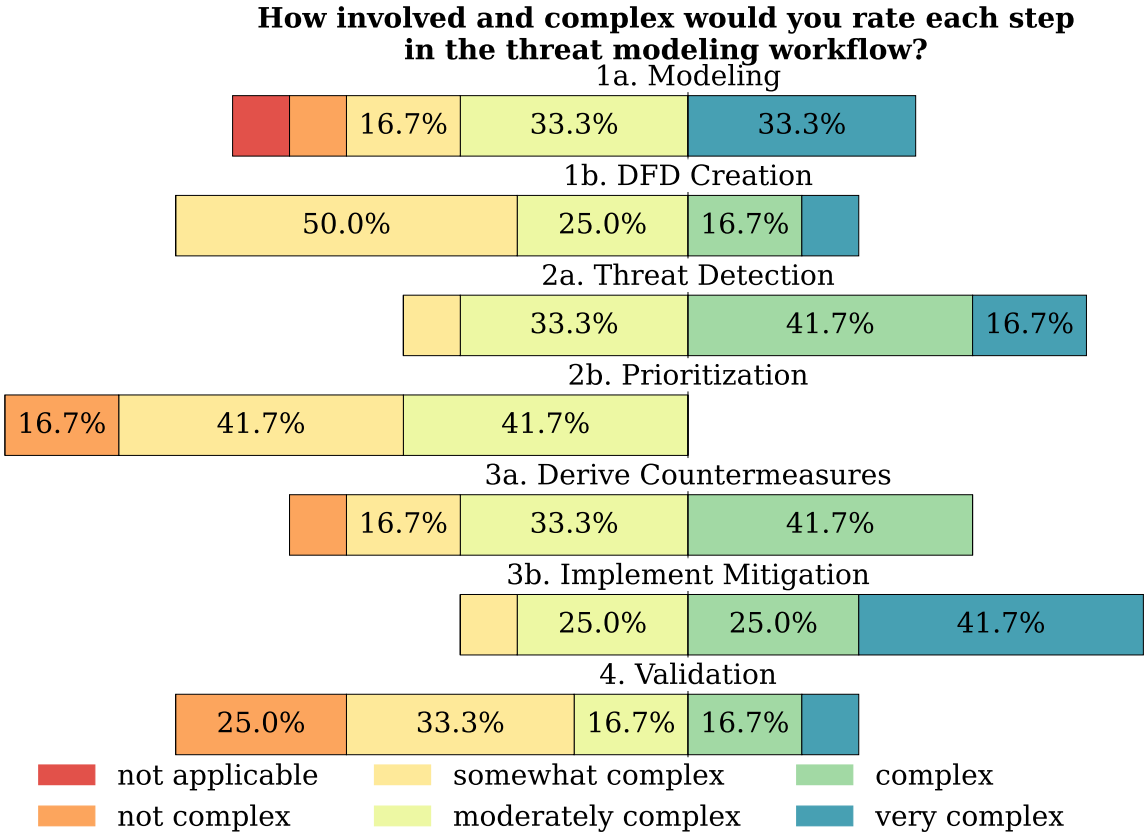
Facts about the questionnaire:

- Video[2] introducing AsIf
- 22 Questions[3]
- three parts: (i) background of participants, (ii) security in industrial systems, (iii) AsIf evaluation
- target group works in R&D at a company within the industrial systems domain

- 12 respondents ranging from automation, research, security consulting, and production
- Overwhelmingly positive feedback

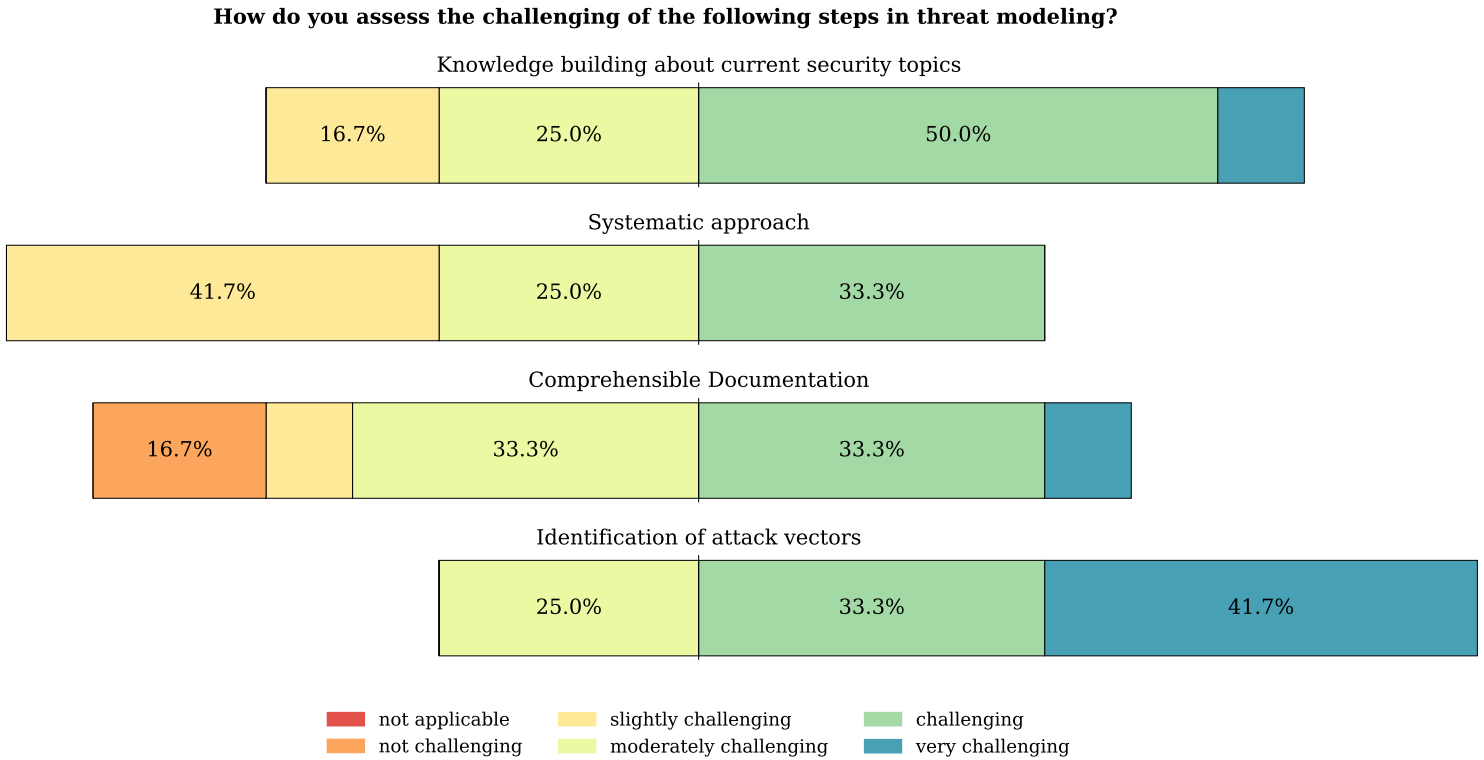
[2] https://www.youtube.com/watch?v=2GpFI3XDmgA

[3] https://doi.org/10.5281/zenodo.11201810

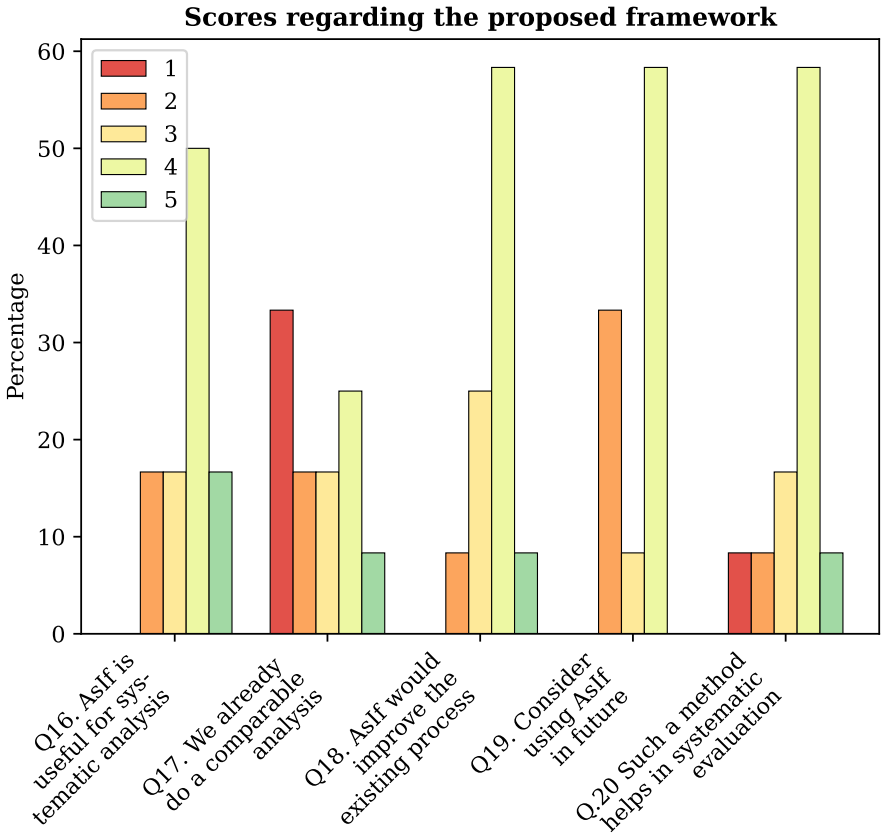

How involved and complex would you rate each step in the threat modeling workflow?
1a. Modeling
16.7%
33.3%
33.3%
1b. DFD Creation
50.0%
25.0%
16.7%
2a. Threat Detection
33.3%
41.7%
16.7%
2b. Prioritization
16.7%
41.7%
41.7%
3a. Derive Countermeasures
16.7%
33.3%
41.7%
3b. Implement Mitigation
25.0%
25.0%
41.7%
4. Validation
25.0%
33.3%
16.7%
16.7%
not applicable
not complex
somewhat complex
moderately complex
complex
very complex

How is Industry Perceiving Threat Modeling?

Where the challenges lie

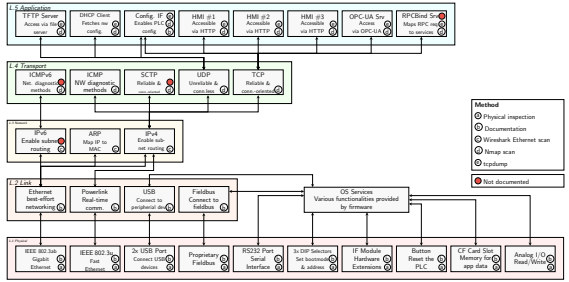


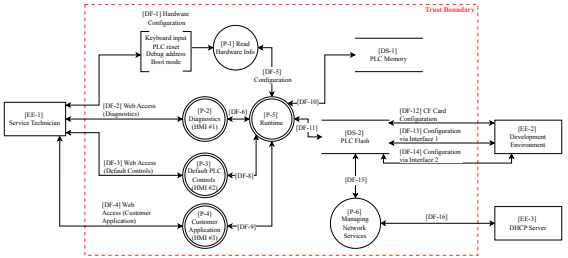
Response to the AsIf Framework



Asset Interface Identification (ASIF)

- method to find and model interfaces (physical & virtual)
- the hybrid TCP/IP model supports a structured approach
- layer-by-layer collection of the interfaces and their dependencies
- visualisation of dependencies between interfaces (*Interface Tree*)
- interface trees as a platform for discussions, and
- foundation for data flow diagrams (DFDs)





Bibliography I

[HPO16] Mario Hermann, Tobias Pentek and Boris Otto. 'Design Principles for Industrie 4.0 Scenarios'. In: *2016 49th Hawaii Int. Conf. on System Sciences (HICSS)*. 2016-01, pp. 3928–3937. DOI: 10.1109/HICSS.2016.488. (Visited on 07/12/2023).

[Saß+24] Olaf Saßnick, Thomas Rosenstatter, Christian Schäfer and Stefan Huber. 'STRIDE-based Methodologies for Threat Modeling of Industrial Control Systems: A Review'. In: *2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS)*. in print. St. Louis, USA: IEEE, 2024-05.

[Sho14] Adam Shostack. *Threat Modeling: Designing for Security*. Indianapolis, IN: Wiley, 2014. ISBN: 978-1-118-80999-0.

[TW10] Andrew S. Tanenbaum and David J. Wetherall. *Computer Networks*. 5th. USA: Prentice Hall Press, 2010-09. ISBN: 978-0-13-212695-3.

[Ysk+20] Koen Yskout, Thomas Heyman, Dimitri Van Landuyt, Laurens Sion, Kim Wuyts and Wouter Joosen. 'Threat modeling: from infancy to maturity'. In: *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering: New Ideas and Emerging Results*. ICSE-NIER '20. Seoul, South Korea: Association for Computing Machinery, 2020, pp. 9–12. ISBN: 9781450371261. DOI: 10.1145/3377816.3381741. URL: https://doi.org/10.1145/3377816.3381741.