ISIA-AF: Orchestrating Reproducible Attacks and Multi-Source Data Collection for OT Systems

Euromicro SEAA 2026

Stefan Manfred Haratzmüller, Thomas Rosenstatter, Olaf Saßnick, Dalibor Sain, and Stefan Huber

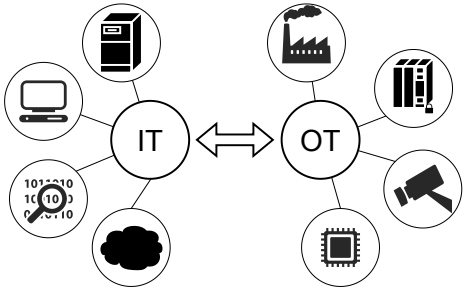
Josef Ressel Center for Intelligent and Secure Industrial Automation
Department for Information Technologies and Digitalisation
Salzburg University of Applied Sciences

3rd September 2026

Salzburg University
of Applied Sciences

Operational Technology

- Are cyber-physical systems
- Examples: chemical, transportation, manufacturing, defense, energy, ...



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

Industrial Automation Systems


Internet, Cloud

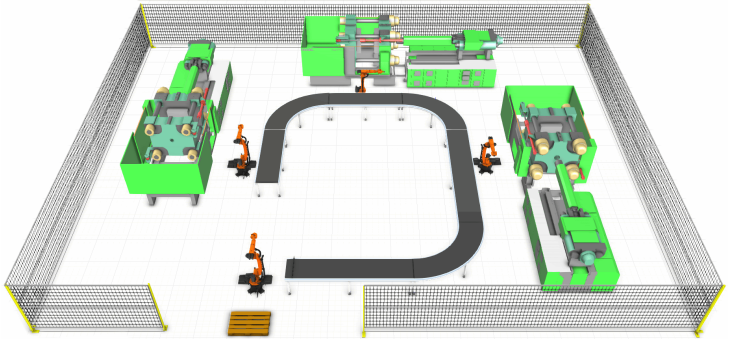

Business Planning


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.

Dataset Challenges in OT

Datasets are necessary for most anomaly detection systems

- Low number of public OT security datasets
- Attacks often limited (e.g., full attack path not included)
- Lack of state-of-the-art protocols (e.g., OPC UA)
- Some domains underrepresented (e.g., industrial discrete automation)

Comparison of Frameworks

Criterion	MITRE Caldera	ISIA-AF
OPC UA support	✗	✓
Customisability	substantial effort required	easily customisable
Planner behaviour	stochastic[1]	deterministic
Dataset generation	✗	✓
OS independent	✗[2]	✓

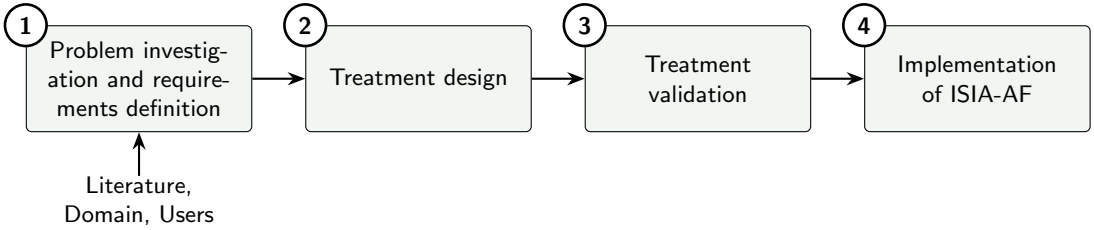
[1] built-in stochasticity in advanced planners

[2] Requires Linux for coordinator and agents

Contributions

- ISIA-AF: modular OT attack framework with native OPC UA support
- Distributed attack clients & orchestrator
- Deterministic, reproducible attack execution
- Built-in dataset generation, labelling and transfer
- Easily customisable and extensible

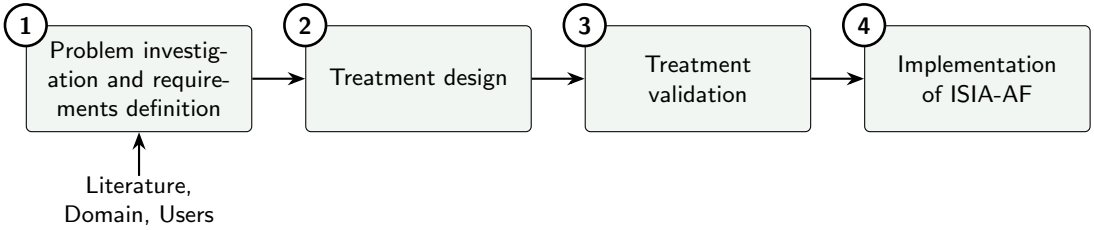
Designing ISIA-AF



- Development based on Wieringa's Design Science Research (DSR) methodology [Wie14]

[3] Lightweight Communications and Marshalling (LCM) is used in robotics and autonomous system environments.

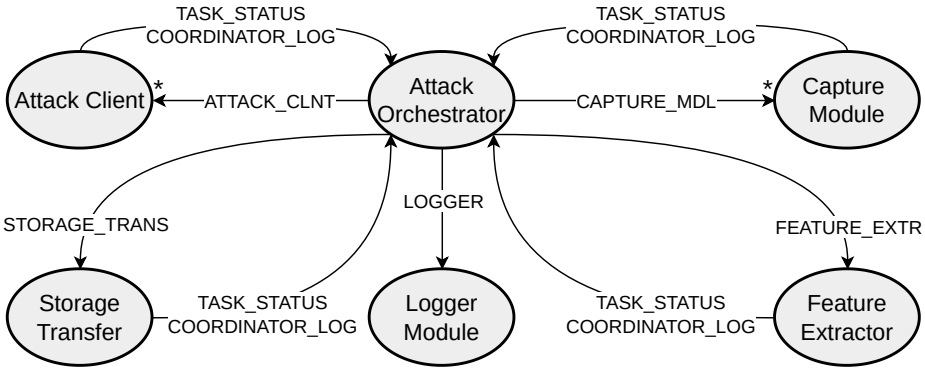
Designing ISIA-AF



- Development based on Wieringa's Design Science Research (DSR) methodology [Wie14]
- LCM[3] (UDP broadcasts) for communication
- Abilities, e.g., coordination, attack execution, capture of network traffic in various segments, feature extraction, final dataset generation incl. labelling
- Reproducibility of experiments
- Extensible, e.g., new attacks

[3] Lightweight Communications and Marshalling (LCM) is used in robotics and autonomous system environments.

ISIA-AF Communication Architecture



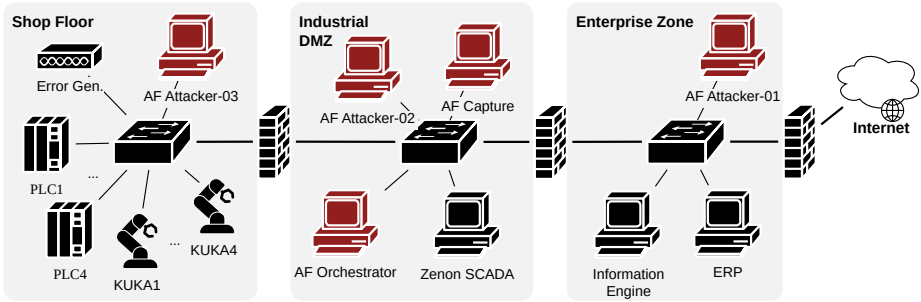
JRC ISIA Testbed

Implementation as mobile testbed

① Enterprise Zone ③ Shop Floor Zone

② Industrial DMZ ④ Legacy Zone

Integration into the Testbed



Evaluation

Testing the framework in action

- Timed order of events
- Copy necessary scripts and binaries
- Capture traffic (start/record/stop)
- Trigger industrial equipment (i.e., PLC)
- Execute attacks
- Download, extraction, labelling of logs
- Store dataset on server

```
tasks ::= [ Action* ]
Action ::= {
  id: String,
  type: { execute_local, start_capture,
     stop_capture, set_alias,
     start_attack_script, start_attack,
     stop_attack, extract_features,
     store_dataset },
    targets: [ String* ],
    time: (RelativeTime | AbsoluteTime) |
          null,
  blocking: Boolean,
  params: { (String : Value)* }
}
```

Conclusion

- ISIA-AF is a framework for
  - testing the security of industrial automation systems
  - generating security datasets
- Coordination of agents via LCM
- Tested and deployed at JRC ISIA textbed

github.com/JRC-ISIA/isia-attack-framework

Future Work

- Detailed labeling of attacks
- Integration of additional attack vectors

Bibliography I

[Wie14] Roel Wieringa. *Design science methodology for information systems and software engineering*. Springer, 2014. ISBN: 978-3-662-43838-1. DOI: 10.1007/978-3-662-43839-8.