# Honeyfarm: AI-based Honeypots for Industrial OPC UA Communication via an On-Demand Deployment Architecture

5th SecIndustry Workshop - Int. Conference on Availability, Reliability, and Security (ARES)

Olaf Sassnick[1,2,3], Florian Entleitner[1,2], Dalibor Sain[1,2], Thomas Rosenstatter[1,2]
Andreas Unterweger[2,3], Simon Hoher[1,2], Stefan Huber[1,2]

[1] Josef Ressel Center for Intelligent and Secure Industrial Automation (JRC ISIA)
[2] Salzburg University of Applied Sciences (SUAS)
[3] Paris Lodron University of Salzburg (PLUS)

27th August 2026

# Motivation

- Increase in OT incidents
- Require further defence mechanisms

→ Explore Honeypots as automated incident response mechanism

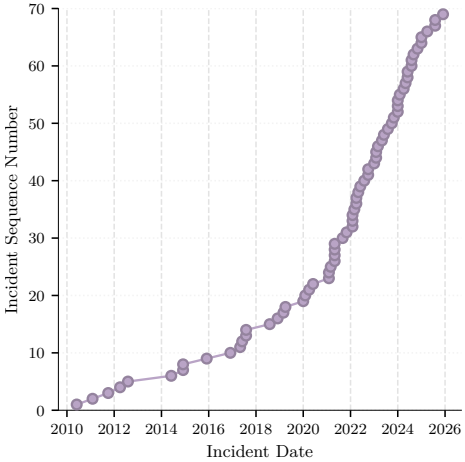
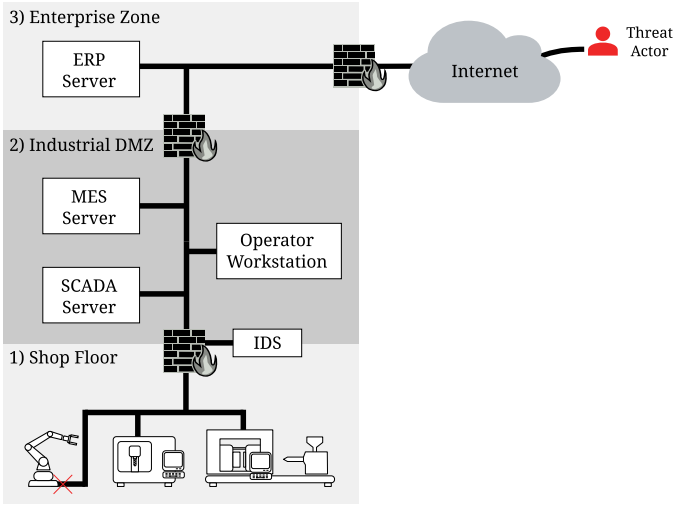
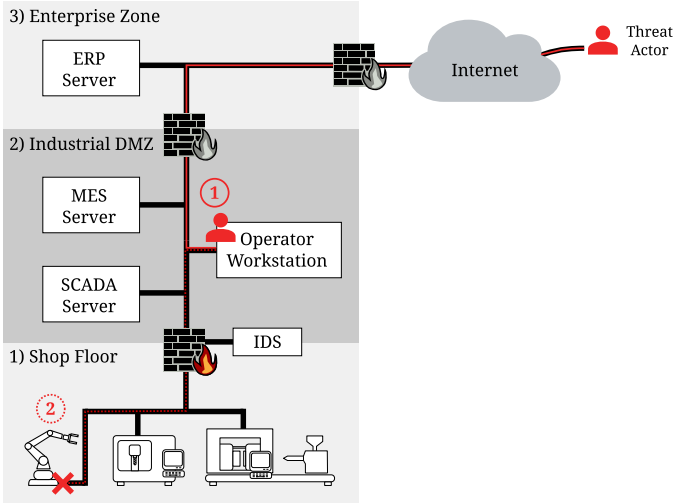



Figure: Documented OT incidents in the recent years (adapted from [Kap+26])

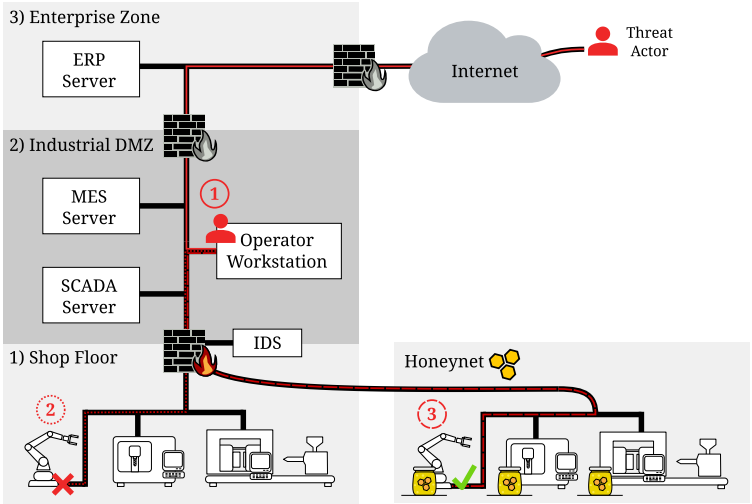
# Introduction Scenario



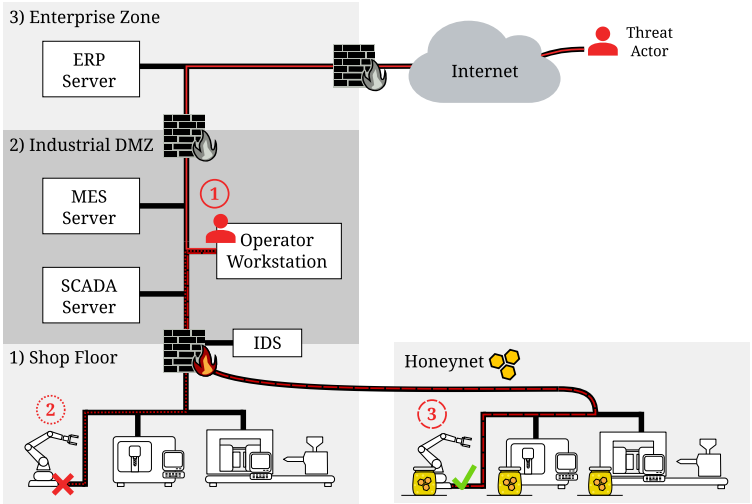
# Introduction Scenario



# Introduction Scenario



# Introduction Scenario

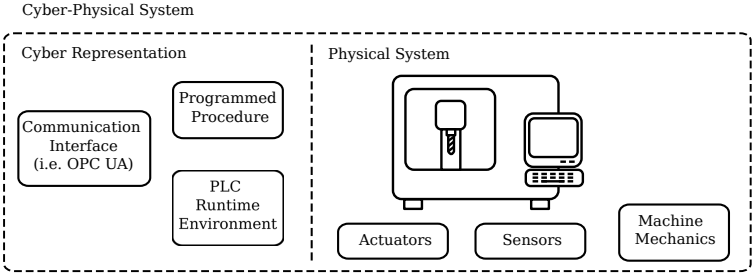



**Advantages**

- Attacker is ...
  - still unaware
  - isolated from CPS
- Gain time for counter measures
- Monitor attacker behaviour
  - Insights on attack goals
  - Learn about vulnerabilities / attack strategies

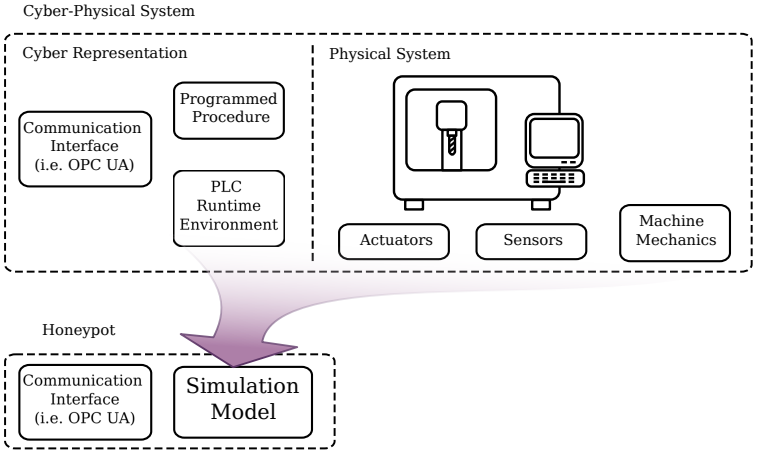
# Challenge 1 - Provide Plausible Interaction

- Realistic behaviour
  - → longer interaction with attacker
- Difference to IT:
  - Instead of Servers, PCs, VMs
  - Cyber-Physical Systems (CPSs)



# Challenge 1 - Provide Plausible Interaction

- Realistic behaviour
  → longer interaction with attacker
- Difference to IT:
  - Instead of Servers, PCs, VMs
  - Cyber-Physical Systems (CPSs)
- Typical solution:
  Simulation-based honeypots for CPSs [Fra+21]

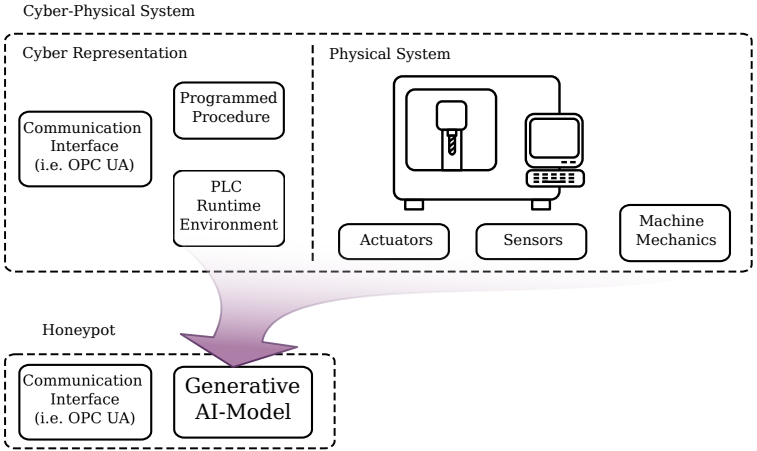


# Challenge 1 - Provide Plausible Interaction

**Approach**
Data-driven Generative AI

**Goals**

- Realistic CPS behaviour
- Reducing deployment effort and cost

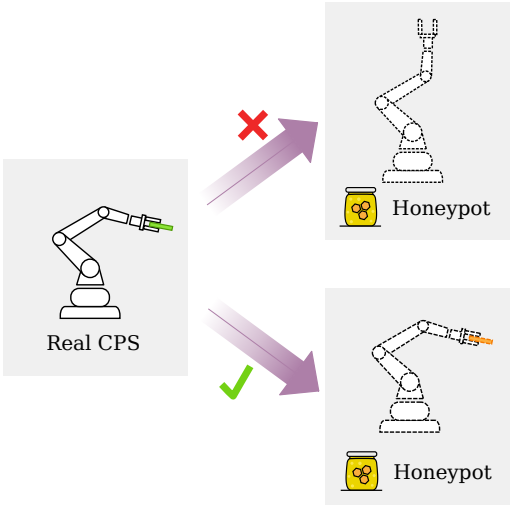


# Challenge 2 - On-Demand Deployment

**Ideally**: instant seamless switchover

**Requirements**

- Transfer the CPS state
- Redirect to attacker to honeypot



# Challenge 2 - On-Demand Deployment

**Ideally**: instant seamless switchover

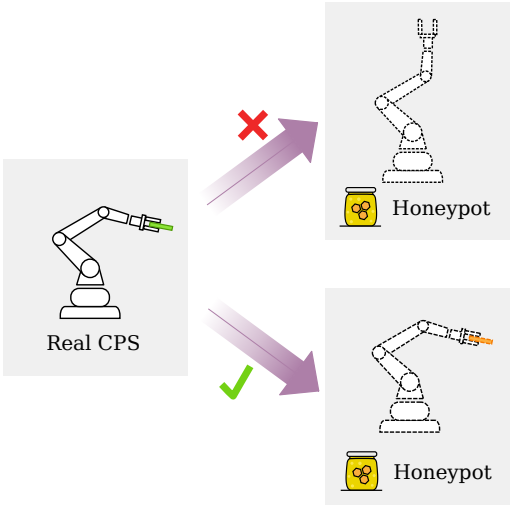
**Requirements**

- Transfer the CPS state
- Redirect to attacker to honeypot

**Approach**

"Honeyfarm"

- Managing honeypot instances
- Coupled to IDS



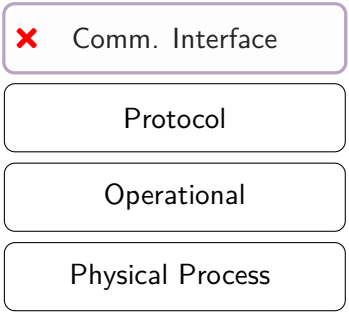
# Research Questions

**RQ1** How can an **AI-based honeypot** be designed for an industrial CPS communicating via **OPC UA** considering attacks on **industrial-process-level**?

**RQ2** How can the **on-demand deployment** of an **AI-based honeypot** be realised in an industrial network?

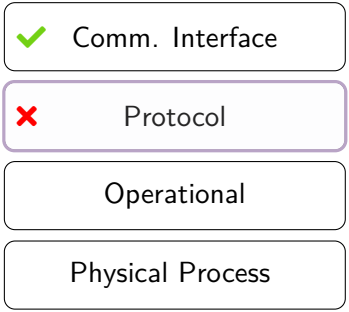
# Active Attack Levels

1. **Communication Interface**
   *Examples:* Malformed messages, packets, or frames, invalid payloads



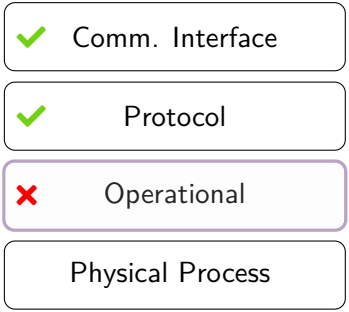
# Active Attack Levels

1. **Communication Interface**
   *Examples:* Malformed messages, packets, or frames, invalid payloads
2. **Protocol**
   *Examples:* Invalid requests, forged commands, wrong message sequences



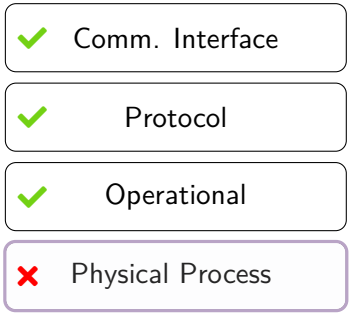
# Active Attack Levels

1. **Communication Interface**
   *Examples:* Malformed messages, packets, or frames, invalid payloads
2. **Protocol**
   *Examples:* Invalid requests, forged commands, wrong message sequences
3. **Operational**
   *Examples:* Invalid parameter values, unexpected configuration states



# Active Attack Levels

1. **Communication Interface**
   *Examples:* Malformed messages, packets, or frames, invalid payloads
2. **Protocol**
   *Examples:* Invalid requests, forged commands, wrong message sequences
3. **Operational**
   *Examples:* Invalid parameter values, unexpected configuration states
4. **Physical Process**
   *Examples:* Unsafe process trajectories, increased physical system degradation, reduced product quality



# Model Design Space

**Model design space**: defines what the generative model observes and generates (adapted from [Mor+23])

| **Model Design Space Level** | **Input (Observations)** | **Output** | **Attacker Interact.** |
|---|---|---|---|
| Comm. Interface | Raw communication | Raw communication responses | Level 1 - 4 |
| Protocol | Deserialised message | Protocol-specific responses | Level 2 - 4 |
| Operational | Cyber-physical state | Cyber-physical state trajectories | Level 3 - 4 |
| Physical Process | Physical state | Physical state trajectories | Level 4 |

# Model Design Space - Implications

Depending on the model design space, further software components are required

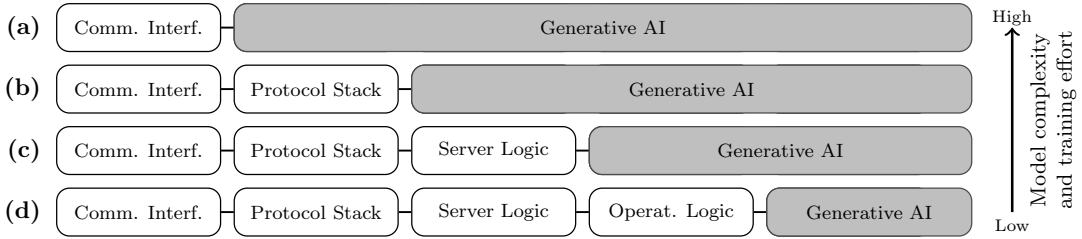
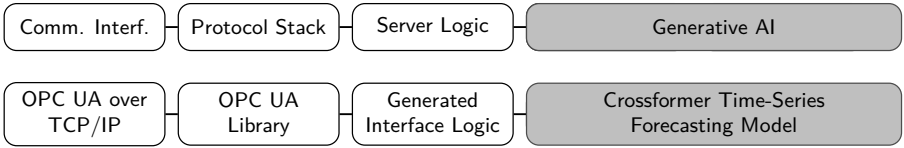



Figure: (a) is at Communication Interface level, (b) operates at Protocol level, (c) at Operational level and (d) at Physical Process level.

# Selected Approach

- Focus on operational level
- OPC UA variables as time-series data
- Utilize a multivariate time-series forecasting (MTSF) model (Crossformer [ZY23] )
- More extensive evaluation of different MTSF-models in [Saß+25]



# Required Steps

**Explore**

- Traverse OPC UA interface
  → Generate honeypot interface

**Collect Data**

- Normal operation
- Override interaction (malicious)

**Training**

- Apply Standard Scaler
- Optimisation with Ray [Mor+18]

# Required Steps

**Explore**

- Traverse OPC UA interface
  ➞ Generate honeypot interface

**Collect Data**

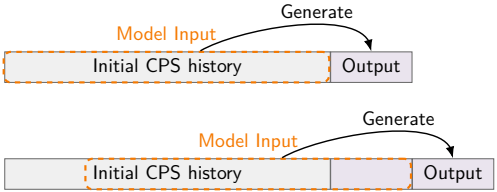
- Normal operation
- Override interaction (malicious)

**Training**

- Apply Standard Scaler
- Optimisation with Ray [Mor+18]

**Inference**

- Recursive forecasting strategy
- Interaction with attacker
  ➞ Modify lookback window



# Required Steps

**Explore**

- Traverse OPC UA interface
  → Generate honeypot interface

**Collect Data**

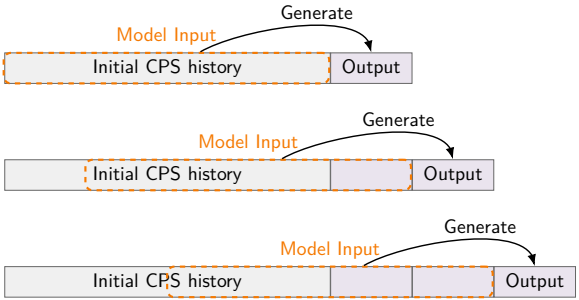
- Normal operation
- Override interaction (malicious)

**Training**

- Apply Standard Scaler
- Optimisation with Ray [Mor+18]

**Inference**

- Recursive forecasting strategy
- Interaction with attacker
  → Modify lookback window



# Required Steps

**Explore**

- Traverse OPC UA interface
  → Generate honeypot interface

**Collect Data**

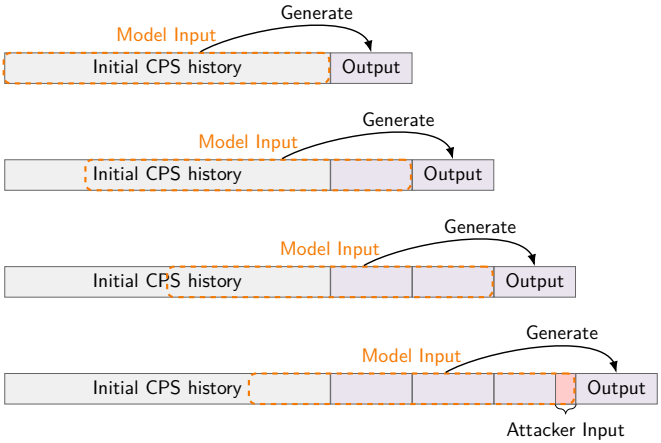
- Normal operation
- Override interaction (malicious)

**Training**

- Apply Standard Scaler
- Optimisation with Ray [Mor+18]

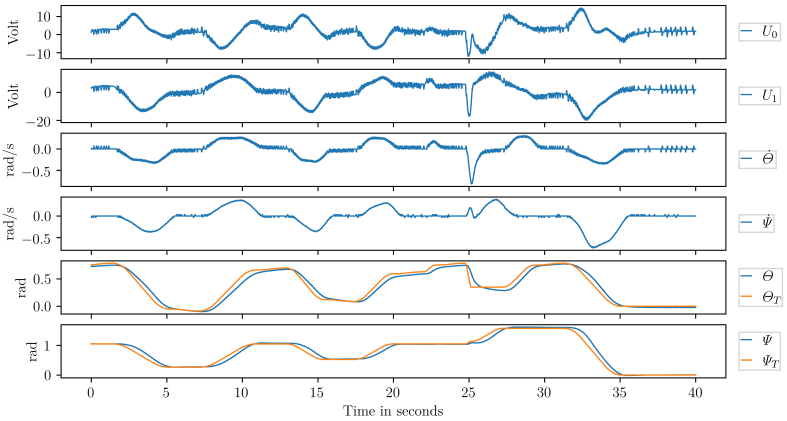
**Inference**

- Recursive forecasting strategy
- Interaction with attacker
  → Modify lookback window



# Selected CPS

Resembling a repeated pick-n-place process with 2 revolute joints




**8 Variables:**

- Actuator Voltages $U_0$ and $U_1$
- Angular Velocities $\dot{\Theta}$, $\dot{\Psi}$
- Target positions Yaw $\Phi_T$ and Pitch $\Theta_T$
- Actual positions Yaw $\Phi$ and Pitch $\Theta$

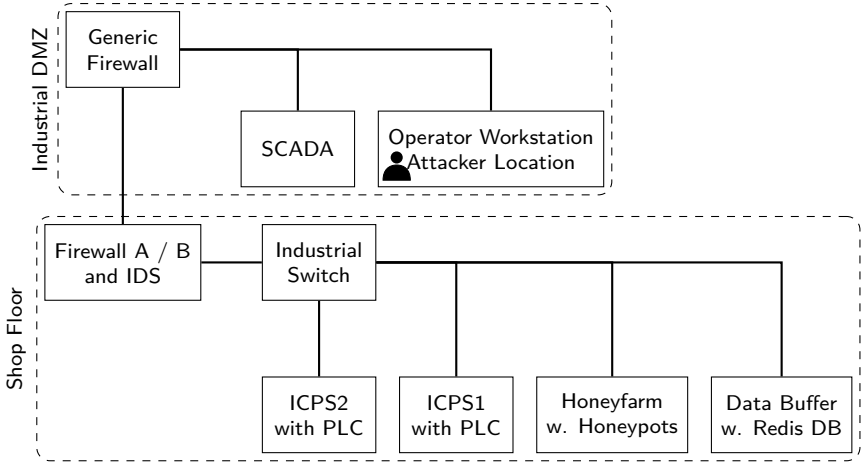
**Methods:**

- to override Yaw $\Phi_T$ and Pitch $\Theta_T$

# Deployment Scenario

**Components**

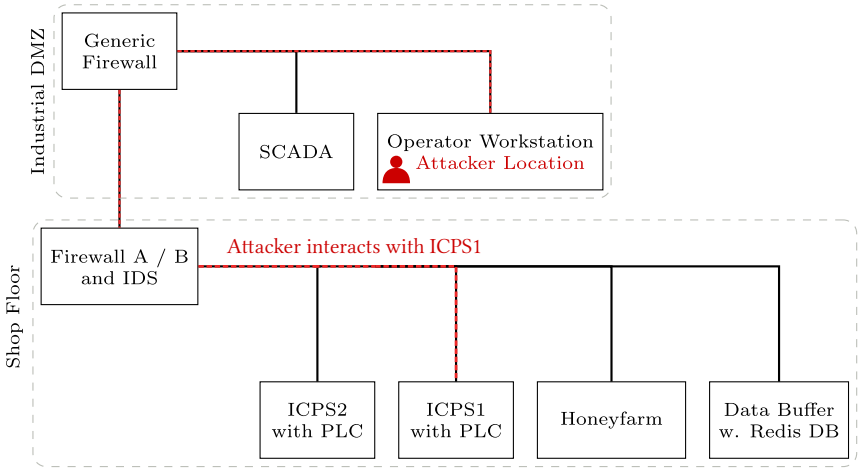
- Firewall
  - **Variant A:** Separate IDS
  - **Variant B:** IDS Integrated
- Data Buffer
- Honeyfarm
- Honeypot



# Deployment Scenario - Part 2

**Sequence**

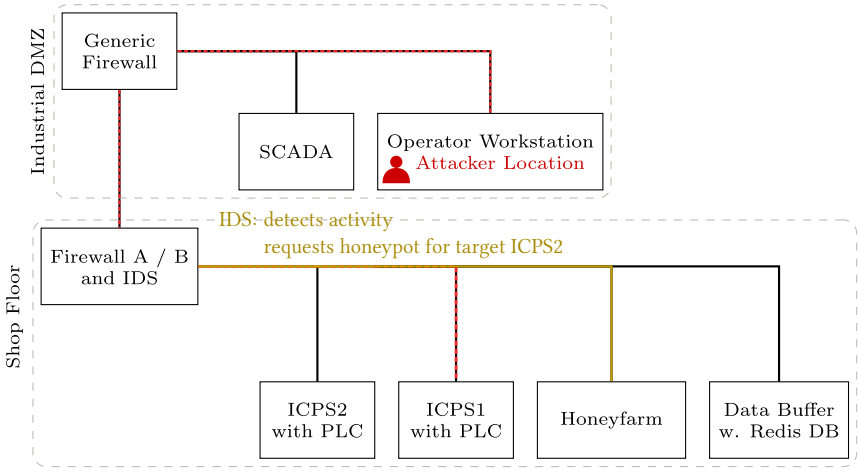
1. Attacker → ICPS1
2. IDS detects attack



# Deployment Scenario - Part 2

**Sequence**

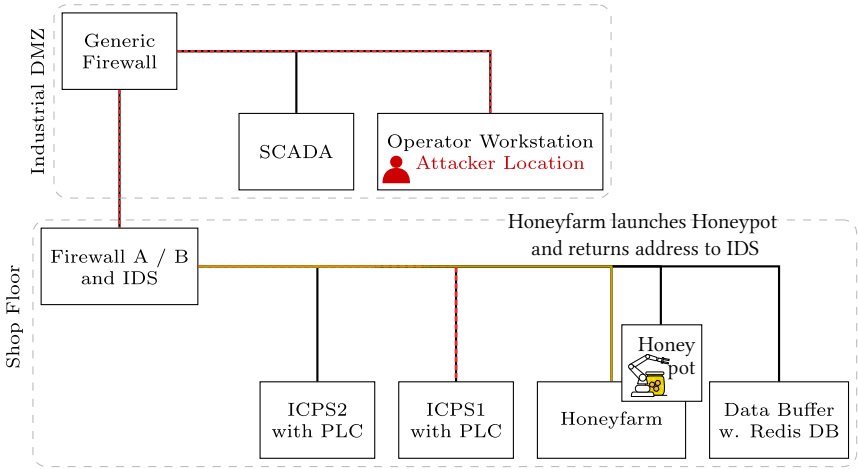
1. Attacker → ICPS1
2. IDS detects attack
3. Request Honeypot



# Deployment Scenario - Part 2

**Sequence**

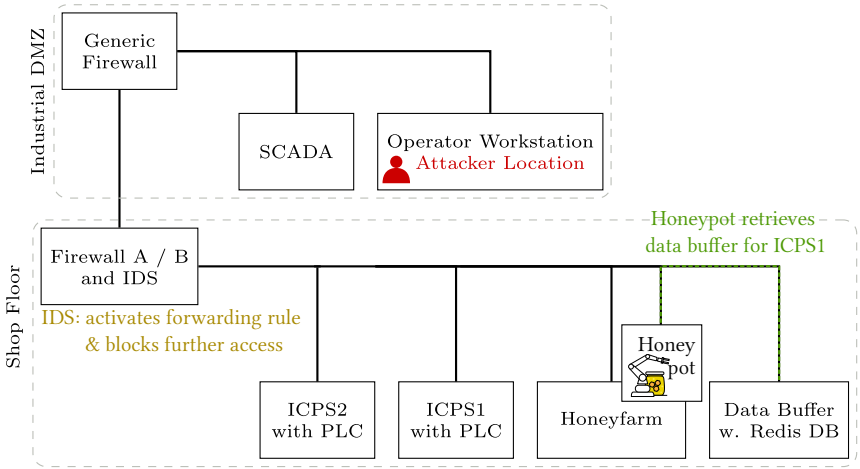
1. Attacker → ICPS1
2. IDS detects attack
3. Request Honeypot
4. Launch Honeypot



# Deployment Scenario - Part 2

**Sequence**

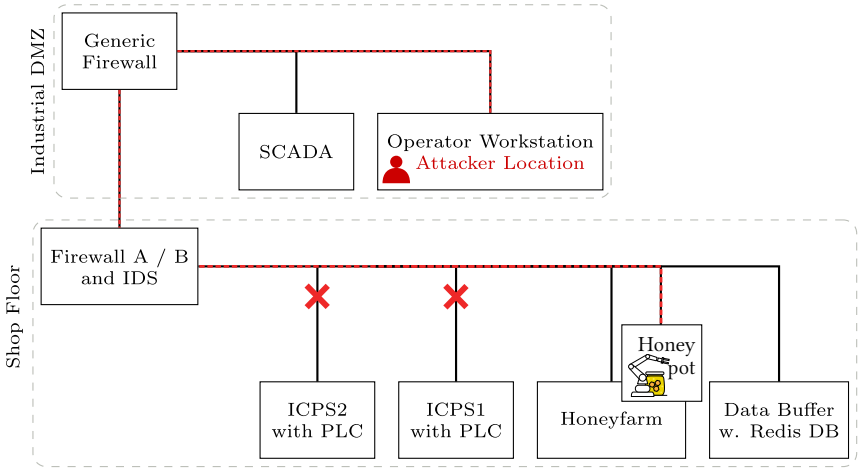
1. Attacker → ICPS1
2. IDS detects attack
3. Request Honeypot
4. Launch Honeypot
5. Read State from Data Buffer
6. Redirect attacker



# Deployment Scenario - Part 2

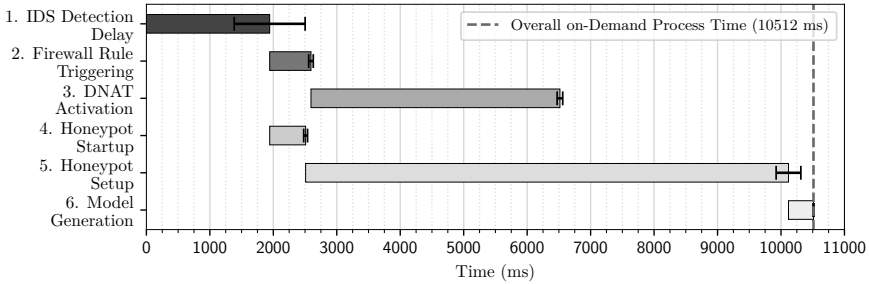
**Sequence**

1. Attacker → ICPS1
2. IDS detects attack
3. Request Honeypot
4. Launch Honeypot
5. Read State from Data Buffer
6. Redirect attacker



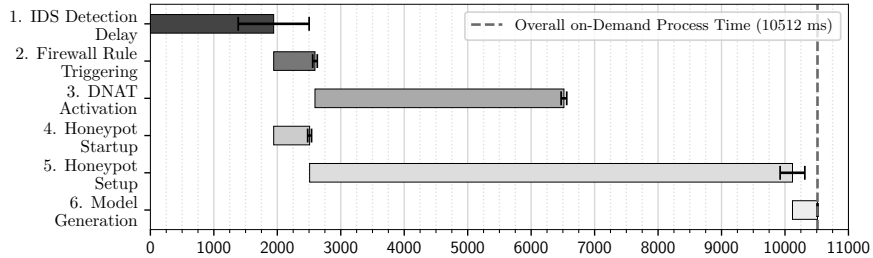
# Results - Switchover Timing

**Variant A**
Separate IDS

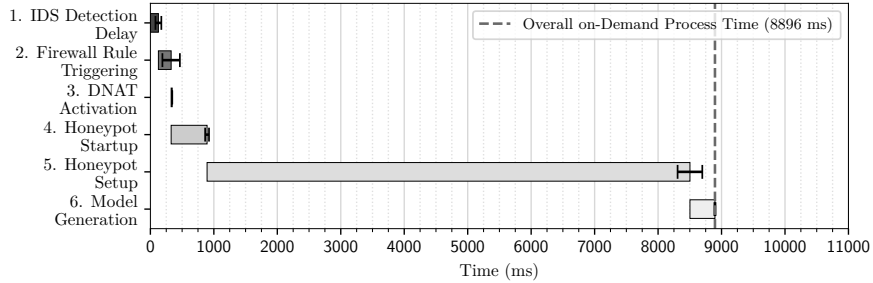


# Results - Switchover Timing

**Variant A**
Separate IDS




**Variant B**
Integrated IDS



# Results - Generative Model Performance

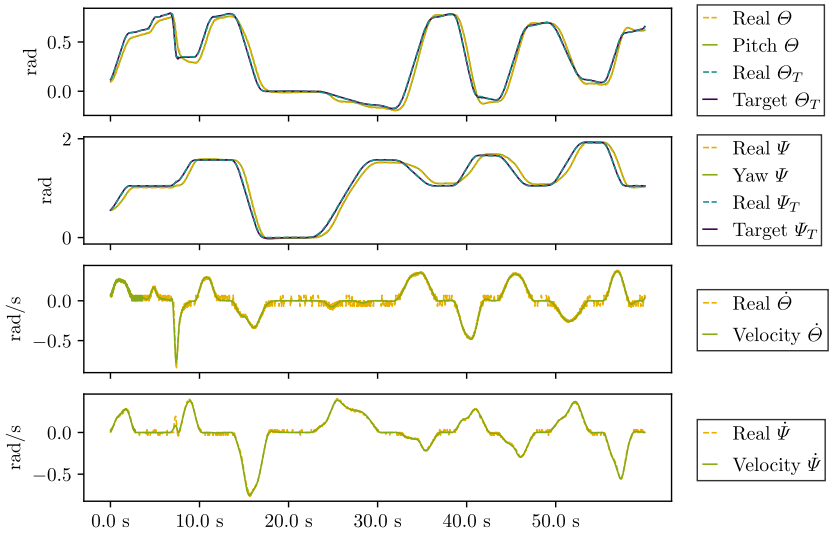
- Mean Absolut Error (MAE) and Mean Squared Error (MSE)
- Normalized variables, $n = 100$ runs

**Stability** Normal cyclic procedure, 60 s recording, taken after deployment time $t_{dp}$ with random start time.

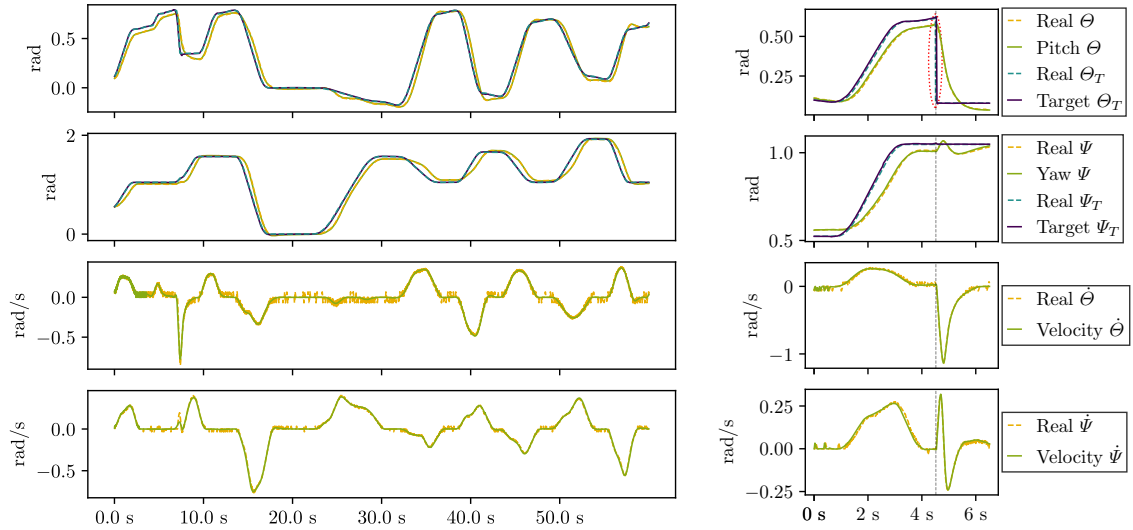
**Interaction** CPS response to attacker overriding actuator joint angle.

| | **Stability** | | | **Interaction** |
|---|---|---|---|---|
| **Metric** | $t_{dp} = 0\,s$ | $t_{dp} = 200\,s$ | $t_{dp} = 2000\,s$ | |
| MAE | $0.208 \pm 0.005$ | $0.209 \pm 0.009$ | $0.220 \pm 0.003$ | $0.245 \pm 0.094$ |
| MSE | $0.235 \pm 0.014$ | $0.242 \pm 0.021$ | $0.263 \pm 0.007$ | $0.254 \pm 0.127$ |

# Results - Generative Model Performance Sample



# Results - Generative Model Performance Sample



# Future Work

**Deployment**

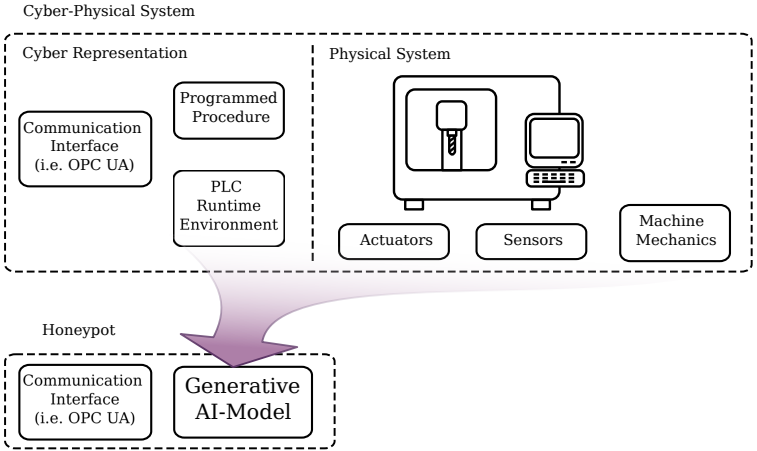
- TCP/IP session handling
- OPC UA authentication
- Forward-stream data buffer during startup
- Honeypot lifecycle management

**Generative Model**

- Restore higher frequency components
- Explore more complex CPS, for instance: injection moulding

# Conclusion

- Generative AI can enable data-driven CPS honeypots
- Process-level attacker interaction is possible
- On-demand deployment was demonstrated as a proof-of-principle



# ISIA Research Project

Intelligent and Secure Industrial Automation (ISIA)
at Salzburg University of Applied Sciences (SUAS)

**Focus**

- Architecture
- Artificial Intelligence
- Security

**Industrial Partners**

- B&R (ABB Group)
- Sigmatek
- COPA-DATA

# References I

## References


[Fra+21] Javier Franco, Ahmet Aris, Berk Canberk, and A. Selcuk Uluagac. "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems." In: *IEEE Communications Surveys & Tutorials* 23.4 (2021), pp. 2351–2383. ISSN: 1553-877X, 2373-745X. (Visited on 10/23/2023).

[Kap+26] Sarthak Kapoor, Sumit Kumar, Harsh Vardhan, Daniel Balasubramanian, and Sandeep Neema. *Cyber security of OT networks: A tutorial, survey of attacks and overview of current state of defense tools, protocols, & challenges*. 2026. URL: https://arxiv.org/abs/2502.14017.

[Mor+18] Philipp Moritz, Robert Nishihara, Stephanie Wang, Alexey Tumanov, Richard Liaw, Eric Liang, Melih Elibol, Zongheng Yang, William Paul, Michael I. Jordan, and Ion Stoica. "Ray: A Distributed Framework for Emerging AI Applications." In: *13th USENIX Symposium on Operating Systems Design and Implementation (OSDI 18)*. Carlsbad, CA: USENIX Association, 2018-10, pp. 561–577. ISBN: 978-1-939133-08-3. URL: https://www.usenix.org/conference/osdi18/presentation/moritz.

# References II


[Mor+23] Meredith Ringel Morris, Carrie J. Cai, Jess Holbrook, Chinmay Kulkarni, and Michael Terry. "The Design Space of Generative Models." In: (2023). DOI: 10.48550/arXiv.2304.10547. (Visited on 03/09/2026).

[Saß+25] Olaf Saßnick, Thomas Rosenstatter, Andreas Unterweger, and Stefan Huber. "Deep Learning-based Time Series Forecasting for Industrial Discrete Process Data." In: *8th IEEE Conf. on Ind. CPS (ICPS)*. IEEE, 2025. DOI: 10.1109/ICPS65515.2025.11087869.

[ZY23] Yunhao Zhang and Junchi Yan. "Crossformer: Transformer Utilizing Cross-Dimension Dependency for Multivariate Time Series Forecasting." In: *International Conference on Learning Representations*. 2023.