A Testbed for Cyber Attack Emulation and AI-Driven Anomaly Detection in Industrial IoT and OT-Networks

Prof. Dr. K.-O. Detken (DECOIT®), Prof. Dr. Axel Sikora (University of Applied Science Offenburg), M. Eng. Jaafer Rahmani (University of Applied Science Offenburg)

Prof. Dr. Kai-Oliver Detken
DECOIT® GmbH & Co. KG
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
detken@decoit.de

Contents

Chapter 1: Introduction

- Problem Statement & Motivation:
  - Legacy industrial protocols (Modbus, PROFINET) lack encryption/authentication
  - IIoT connectivity exposes critical infrastructure to malware, ransomware, and botnets (e.g., Mirai)
  - Advanced Persistent Threats (APTs) exploit multi-stage tactics beyond simple DoS
  - Existing testbeds are domain-specific and cannot emulate cross-industry attacks or collect unified data

Chapter 2: Research Context (1)

- Research gaps in current testbeds:

Research Gap	Specific Problem	Impact
Vertical Limitations	Single-industry focus restricts generalization	Models fail to work across diverse industrial environments
Attack Complexity	Few platforms model multi-stage APTs or VLAN hopping	Poor detection of sophisticated attack chains and lateral movement
Monitoring Deficiencies	Network, host, and protocol data seldom correlated in real time	Incomplete telemetry hinders multi-layer threat detection

Chapter 2: Research Context (2)

- Key contributions & innovations:
  - Generic OT/IIoT testbed for deep field buses
  - Simultaneous Modbus, MQTT, PROFINET support
  - Hybrid physical (Raspberry Pi) + virtual IT architecture
  - Unified NetFlow + auditd + Zeek in Elastic SIEM
  - MITRE ATT&CK-aligned attack playbook (published in IEEE ICEST 2025, N. Macedonia)
  - ML-ready datasets (CSV/JSON/ES indices)

Chapter 2: Research Context (3)

Phase	Technique(s)	Entry Point	Impact	Counter-measure
Initial Access	T1190, T1133	RDP on Exchange Web Service (EWS)	Network foothold	Multi-Factor-Auth. (MFA), RDP firewall/ VPN
Discovery (ICS)	T0842, T0840	Packet sniffing	Extract device info	Encrypt traffic, continuous monitoring
Impair Process Control	T0855	Modbus PLC	Process disruption	Command authentication, anomaly detection

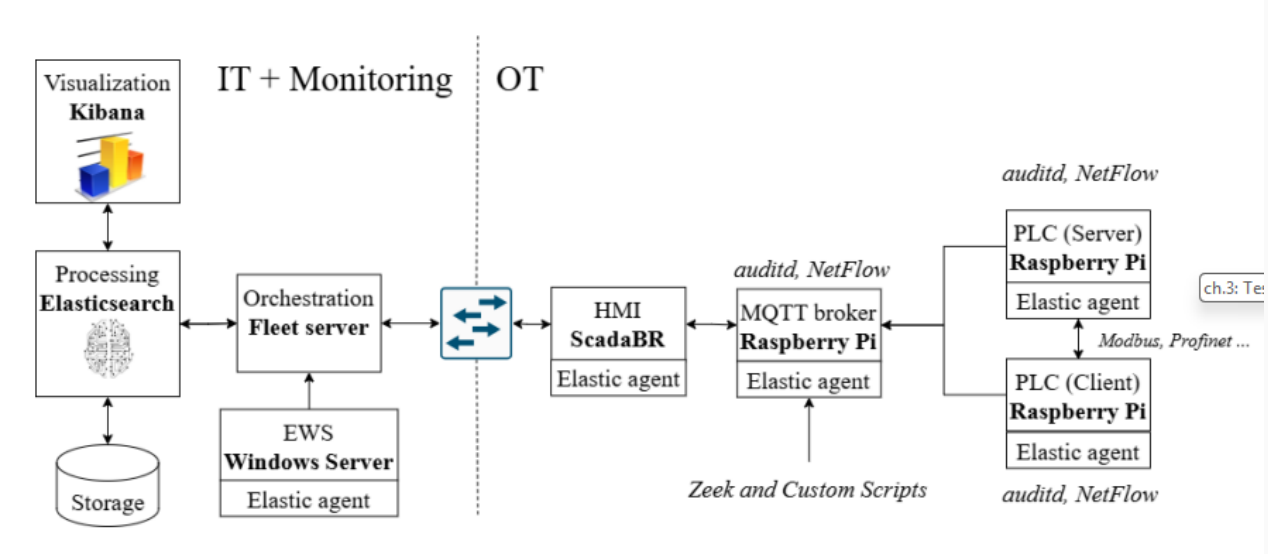
TABLE I
MODBUS ATTACK MAPPED TO THE ENTERPRISE AND ICS MITRE ATT&CK FRAMEWORKS

Tactic (MITRE ATT&CK) [2]	Technique (MITRE ATT&CK) [2]	Entry Point (ICS)	Impact (ICS)	Security Consideration (ICS)	Description
Initial Access - Enterprise	T1190: Exploit Public-Facing Application T1133: External Remote Services	EWS via RDP	Establish a foothold in the network	Harden the EWS by enforcing strong passwords, MFA, and restricting RDP via firewalls or VPNs	Attacker exploits weak RDP credentials using `xfreerdp /u:pwned /p:Password123! /v:10.10.0.30 +cert-ignore` to gain initial access.
Privilege Escalation - Enterprise	T1078: Valid Accounts T1548: Abuse Elevation Control Mechanism	EWS	Gain administrative access on the EWS	Enforce least privilege policies and monitor PowerShell/CMD usage for anomalies	Attacker launches an elevated PowerShell session via CMD with custom shellcode on the EWS to escalate privileges.
Persistence - Enterprise	T1053.005: Scheduled Task/Job	EWS	Maintain long-term remote access on the EWS	Monitor and audit scheduled tasks; enforce strict administrative controls on the EWS	Immediately after privilege escalation, a hidden scheduled task is created on the EWS (IP `10.10.0.5`) using `schtasks` to automatically reinitiate RDP sessions.
Discovery - Enterprise	T1049: System Network Connections Discovery	EWS	Map internal network topology	Deploy intrusion detection systems and segment the ICS network to restrict scanning activity	Attacker uses `nmap -p 502 10.10.0.6 -sV` and Wireshark to discover network devices and capture traffic.
Discovery - ICS	T0842: Network Sniffing T0840: Network Connection Enumeration	EWS	Extract detailed ICS device information	Encrypt ICS traffic and implement continuous monitoring to detect unauthorized packet capture	Attacker captures and analyzes Modbus/TCP packets between the HMI and PLC to extract device configurations and communication patterns.
Lateral Movement - Enterprise	T1570: Lateral Tool Transfer	EWS → HMI	Enable remote script execution on the HMI	Secure file transfer channels on the EWS; enforce application allowlisting and use encrypted transfers on the HMI	Attack scripts are transferred from the EWS to the HMI via an HTTP server and downloaded using `Invoke-WebRequest`.
Execution - Enterprise	T1059: Command and Scripting Interpreter	HMI	Execute malicious scripts and commands	Monitor script execution on the HMI and restrict unauthorized code via endpoint detection and response solutions	The attacker executes the Python Modbus client script on the HMI to establish connection with the Modbus Server and send malicious commands to it.
Execution - ICS	T0807: Command-Line Interface T0823: Graphical User Interface	HMI	Send unauthorized commands to PLC	Enforce strict authentication on HMI interfaces and validate all incoming commands	Crafted Modbus commands are sent from the HMI to manipulate PLC operations, bypassing built-in safety protocols.
Impair Process Control - ICS	T0855: Unauthorized Command Message	PLC	Disrupt industrial process control	Implement robust command authentication, detailed logging, and real-time anomaly detection on PLCs	Attacker injects malicious Modbus commands via the advanced injection script (`modbusinjection.py`) and launches a DoS attack using (`modbusdos.py`) to overload the PLC.

Chapter 3: Testbed Architecture (1)

Component	Purpose & Rationale
Kibana	Interactive dashboard for multi-layer event visualization and incident response
Elasticsearch	Central log processing, storage, and cross-layer event correlation
Fleet Server	Central agent orchestration and configuration management
EWS (Windows Server)	Engineering workstation for administrative control and attack origin point
HMI (ScadaBR)	Supervisory control interface for operator environment simulation
MQTT Broker (Raspberry Pi)	IIoT communication handling and telemetry collection
PLC Server/Client (Raspberry Pi)	Physical ICS device emulation with real-time telemetry collection
Smart Switch	Network segmentation enabling VLAN isolation and lateral movement studies

Chapter 3: Testbed Architecture (2)



- Key Design Principles:
  - Hybrid Architecture: Physical PLCs + virtual IT components for realistic network behavior
  - Multi-Protocol Support: Simultaneous Modbus, MQTT, PROFINET capability
  - Unified Monitoring: First real-time NetFlow + auditd + Zeek integration in ICS environments
  - Attack Surface Diversity: Supports multi-stage APT emulation across IT-OT boundaries

Chapter 4: Technical Implementation (1)

Comprehensive telemetry capture using Elasticsearch-supported integrations:

Layer	Tool	Key Capabilities	Security Value
Network	NetFlow	Flow volume, VLAN tags, protocol IDs, bidirectional analysis	Traffic pattern anomaly detection, lateral movement tracking
Host	auditd	Process execution, authentication events, file I/O, privilege changes	Insider threat detection, privilege escalation monitoring
Protocol	Zeek	Deep packet inspection (Modbus/MQTT), transaction analysis, error codes	Industrial protocol abuse detection, command injection identification

Key Innovation: First real-time integration of NetFlow + auditd + Zeek within unified SIEM framework for ICS environments → Real-time ingestion into Elastic SIEM enabling cross-layer event correlation and forensic analysis

Chapter 4: Technical Implementation (2)

- Systematic threat simulation aligned with MITRE ATT&CK for ICS:
  - Attack capabilities:
    - Modbus/TCP packet & register manipulation: direct industrial protocol exploitation
    - Multi-stage attack progression: EWS compromise → VLAN hopping → PLC tampering
    - Advanced Persistent Threat (APT) modeling: realistic dwell times and lateral movement
  - MITRE ATT&CK ICS integration:
    - Automated technique tagging (e.g. T0855: impair process control)
    - Systematic attack labeling for supervised learning
    - Cross-domain mapping spanning enterprise and ICS tactics
  - Benefits:
    - Behavioral fidelity: emulates realistic attacker patterns vs. synthetic data
    - Reproducible scenarios: standardized benchmarking across industrial environments
    - ML-ready datasets: comprehensive labeled data for AI model training

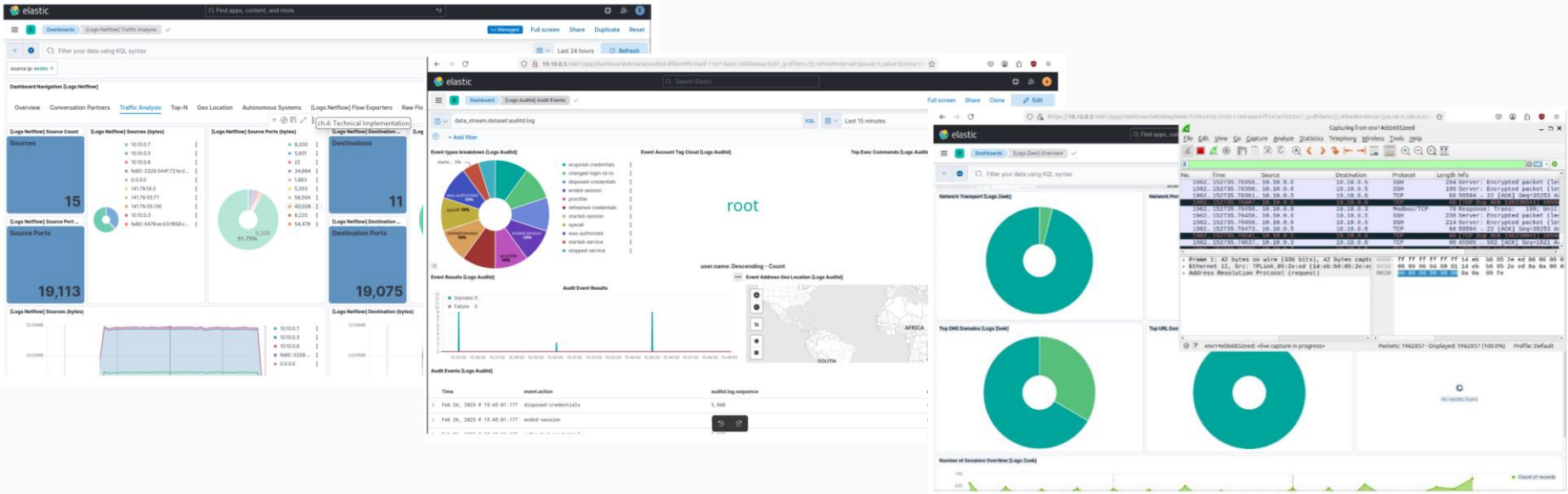
Chapter 5: Validation and Comparison (1)

- Comparative analysis with existing testbeds:

Capability	Our Testbed	CPGrid-OT [9]	ICSSIM [13]
Protocol Support	**Modbus/TCP, MQTT, PROFINET**	DNP3 primary; IEC 61850 demonstrated	User-defined modules (e.g., Modbus/TCP)
Integrated Monitoring	**Unified: network + host + protocol**	Separate IT/OT network monitoring	Process simulation + network logging
SIEM Integration	**Embedded ELK (real-time)**	None	File-based logs (no native SIEM)
Cross-Layer Correlation	**Automated correlation scripted engine**	Manual event matching	None
Attack Framework	**MITRE ATT&CK ICS playbooks**	Scenario scripts (DoS, spoofing)	Process-level attack scripts
Data Export	**CSV, JSON, ES indices**	Standard power formats (CSV/JSON)	Proprietary format (CSV via scripts)
Edge Integration	**Agents on physical/virtual edges**	Centralized hardware	Centralized host

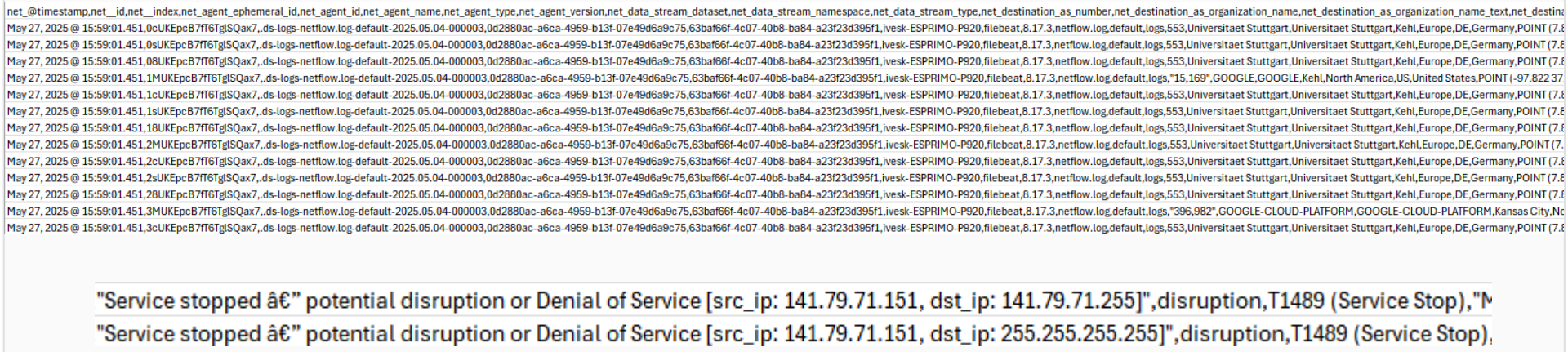
Chapter 5: Validation and Comparison (2)

- Multi-layer data validation results:
  - Network: VLAN-tagged flows & protocol detection (>95% coverage)
  - Host: Privilege escalation & auth events captured
  - Protocol: Modbus FC anomalies flagged
  - Cross-layer: Correlated flow + events → security alerts



Chapter 6: Dataset generation

- Dataset generation & AI readiness:
  - Normal + attack traffic, telemetry, host logs
  - MITRE ATT&CK fields embedded
  - Export: CSV, JSON, Elasticsearch snapshot
  - Supports latent-space ML and federated learning



Chapter 7: Limitations and Future Work

- Current limitations & challenges:
  - Raspberry Pi timing (no sub-ms PLC validation)
  - Modbus-centric attacks; other protocols pending
  - Lab scale (≤ 12 nodes) vs. industrial (> 100 nodes)
- Future work:
  - Add OPC-UA, extended PROFINET, MQTT-SN…
  - Deploy in industrial partner environments
  - Integrate federated learning for distributed IDS
  - Standardize ICS testbed evaluation criteria
  - Upscale the testbed by using additional physical/virtual devices

Chapter 8: Conclusions (1)

- Key achievements:
  - First cross-industry OT/IIoT testbed supporting Modbus, MQTT, and PROFINET
  - Unified real-time monitoring with NetFlow, auditd, and Zeek in single SIEM
  - Multi-stage attack emulation aligned with MITRE ATT&CK ICS framework
  - Hybrid physical-virtual architecture combining Raspberry Pi edge devices and virtual IT components
  - High-fidelity synchronized datasets for AI-driven anomaly detection
  - Addressed critical gaps in testbed scope, attack complexity, and telemetry integration

Chapter 8: Conclusions (2)

- Research impact:
  - Established foundation for advancing industrial cybersecurity research through comprehensive IT-OT threat emulation and data collection
- Future work:
  - Expanded protocol support, expanded testbed scale, federated learning integration, industrial partner deployments

- Acknowledgment:
  - German Federal Ministry (BMWK)
  - KISTE project: http://kiste-project.info
  - Participants: University of Applied Science Offenburg, DECOIT® GmbH & Co. KG

Thank you for your attention!

DECOIT GmbH & Co. KG
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
info@decoit.de