Operational technology Malware Alarms with Sandboxing and Honeypotting.

Supervisors:

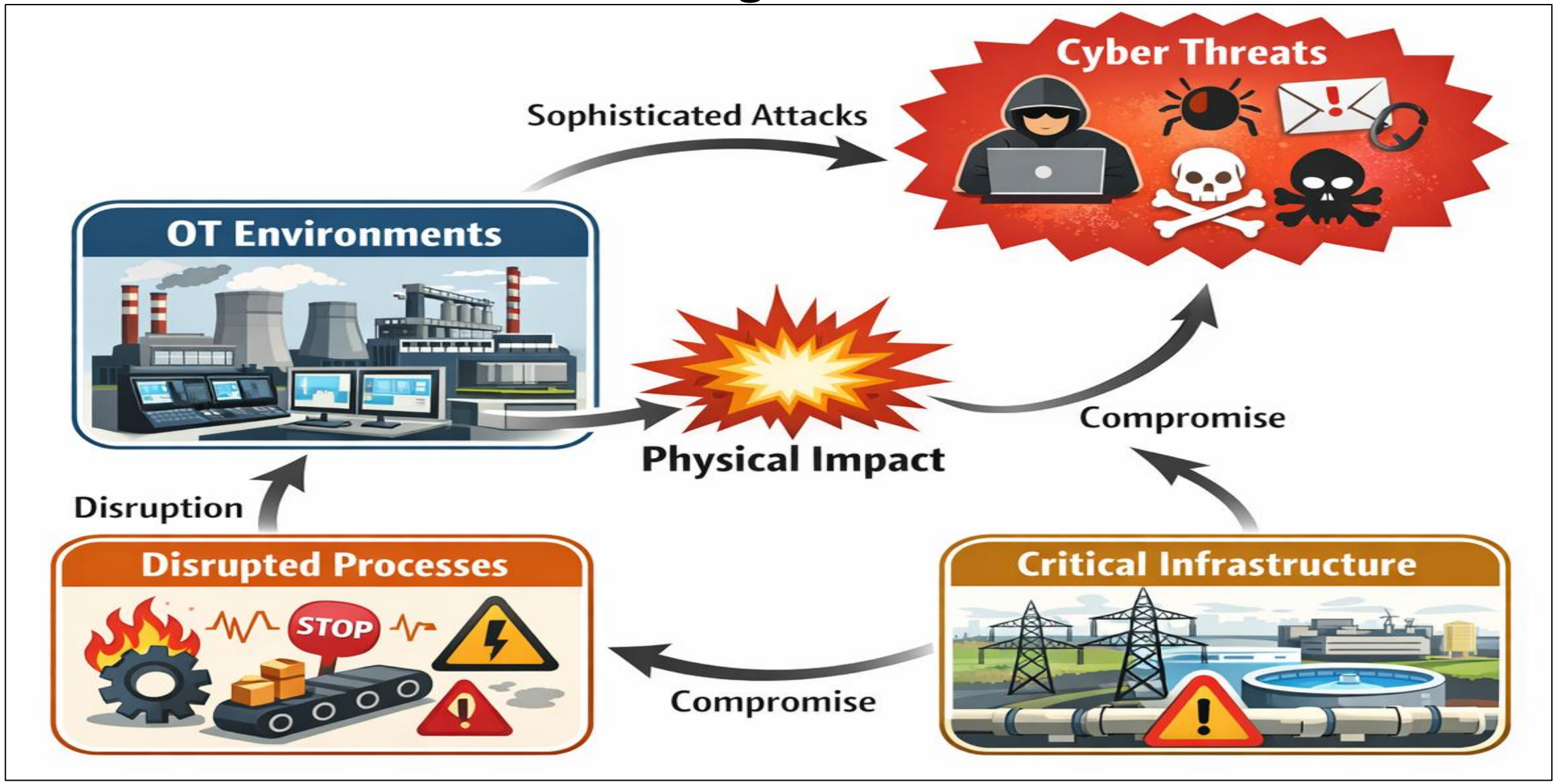
Prof. Stefano Bistarelli
Prof. Francesco Santini

PhD student:

Dawit Berhan

Rimini, 06 February 2026

Background

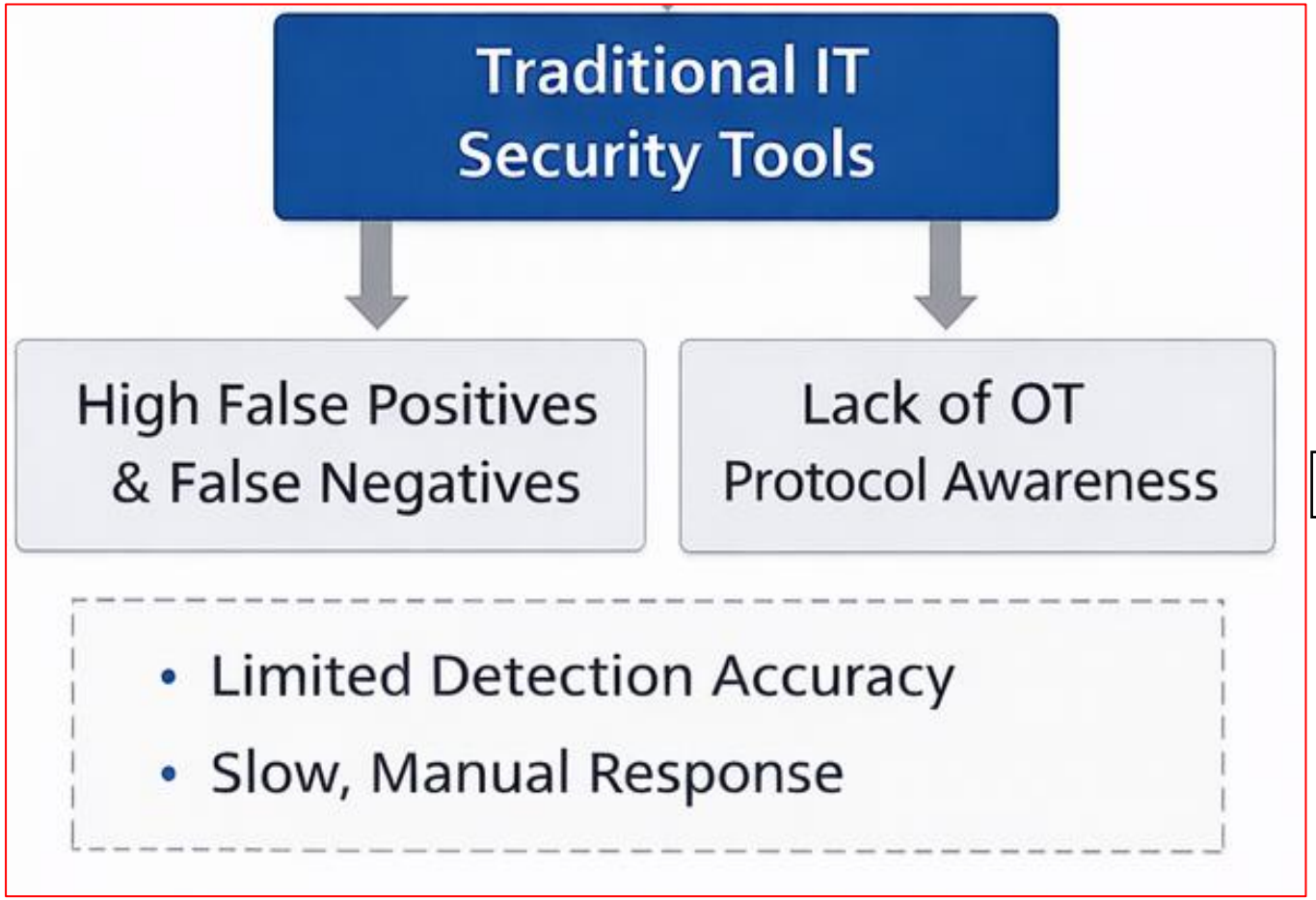

Cyber Threats
Sophisticated Attacks
OT Environments
Physical Impact
Compromise
Disruption
Disrupted Processes
STOP
Critical Infrastructure
Compromise

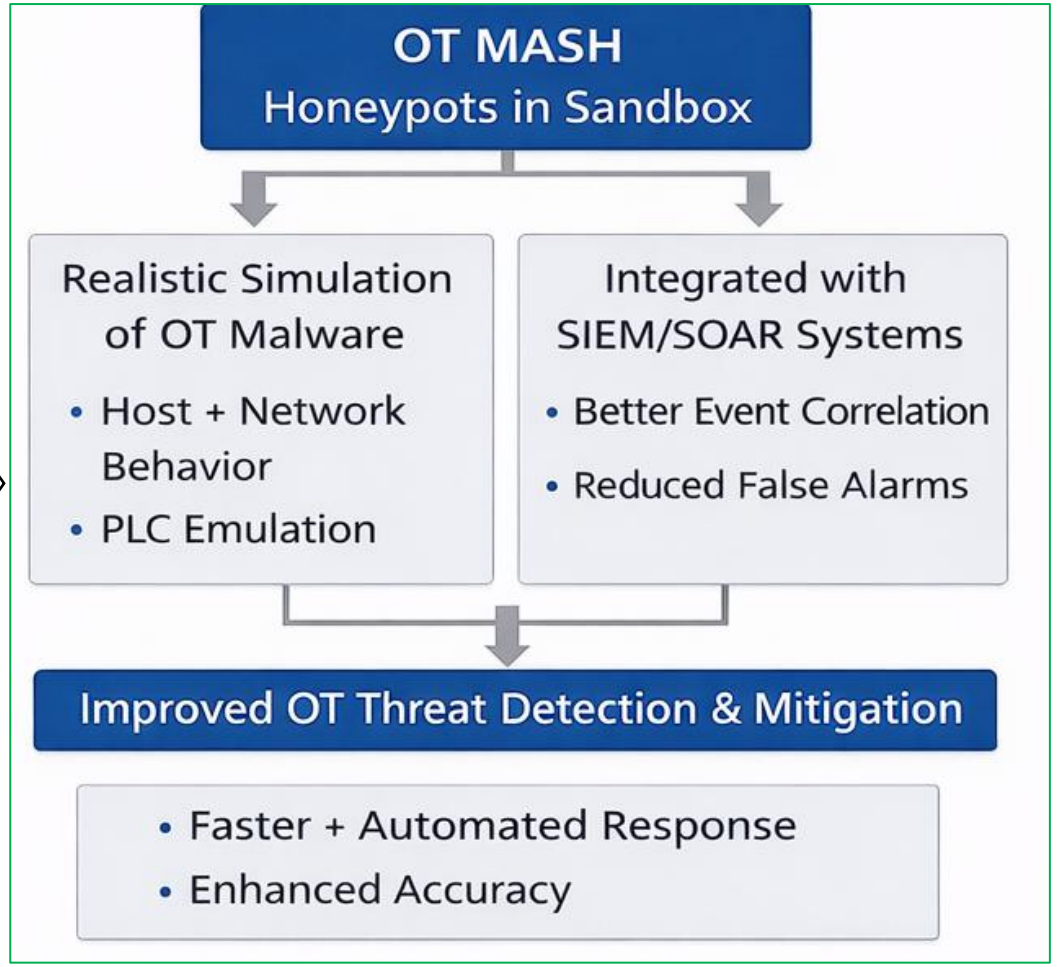
Real-World Examples of Sophisticated Cyber Attacks on OT/ICS

Russia-Aligned ELECTRUM Tied to December 2025 Cyber Attack on Polish Power Grid

Chinese cyber attacks on Taiwan's NSB critical infrastructure are up 113% daily since 2023

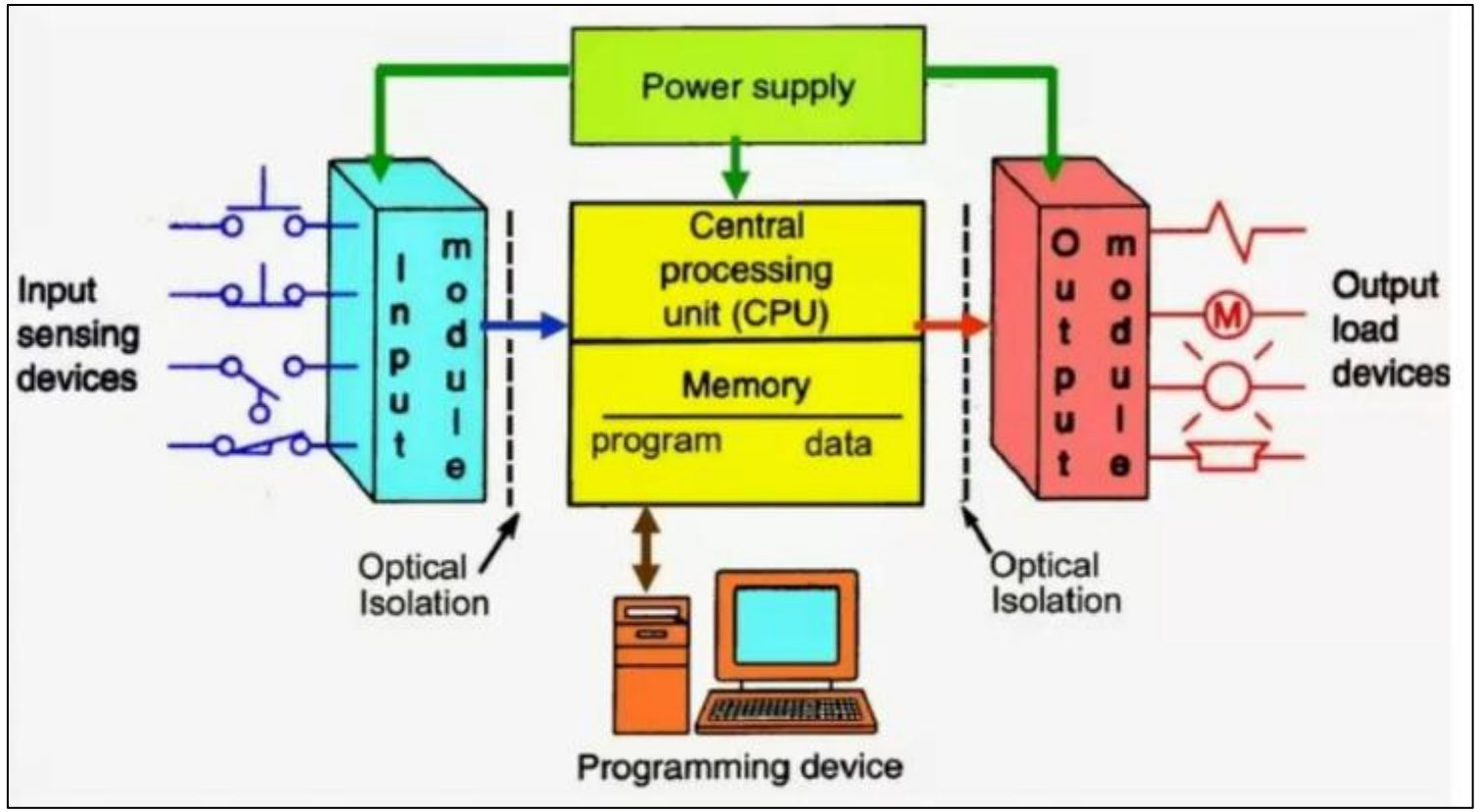
Motivation

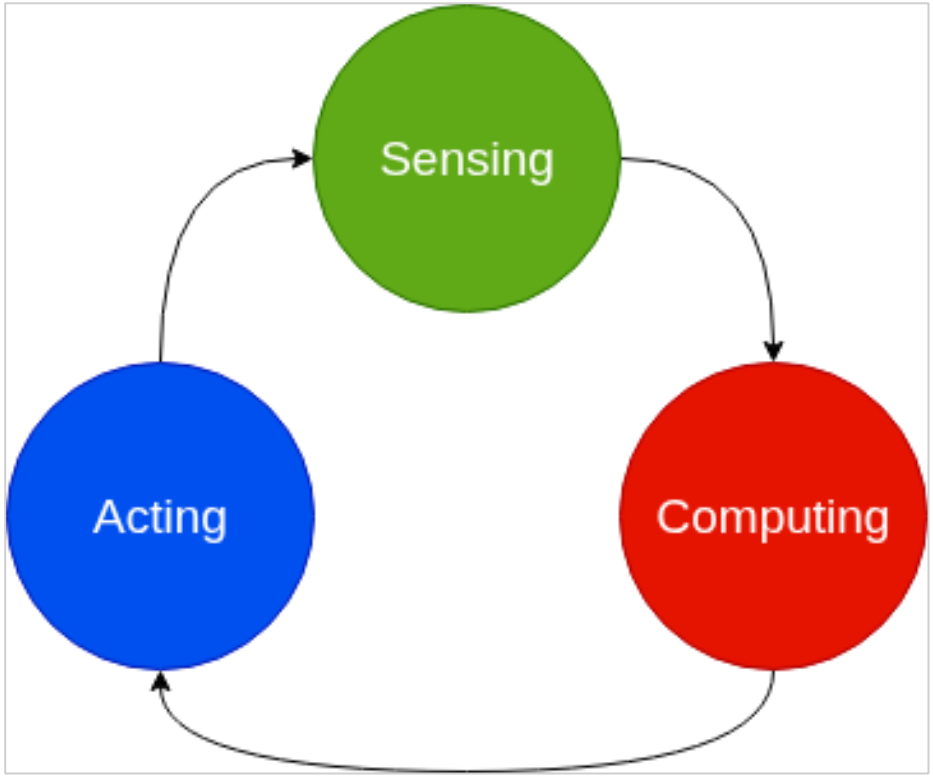




SIEM → Security Information and Event Management
SOAR → Security Orchestration, Automation, and Response

PLC Scan Cycle





PLC Scan Cycle

Communication protocol:Modbus

Modbus Protocol

TCP/IP

- Uses port 502/TCP when spoken over TCP/IP.

TCP/IP port 502

Communication Model

- Modbus uses a client-server (master-slave) model for communication.

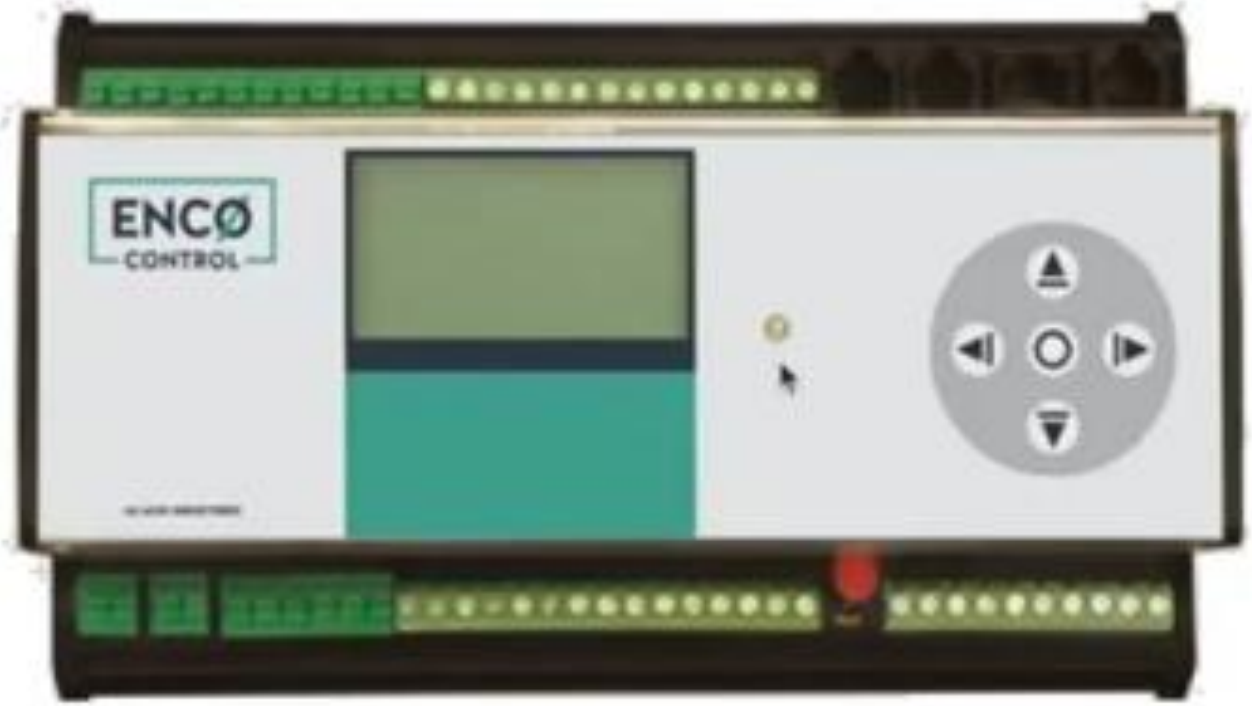
Client (Master)

Server (Slave)

Flexibility

- Modbus is independent of the underlying PLC architecture, making it a highly versatile protocol.

Modbus data types and example devices



Enco Control Device

Primary tables	Object type	Type of
Discretes Input	Single bit	Read-Only
Coils	Single bit	Read-Write
Input Registers	16-bit word	Read-Only
Holding Registers	16-bit word	Read-Write

Modbus Data Types

PLC Scan cycle

Sensing Phase

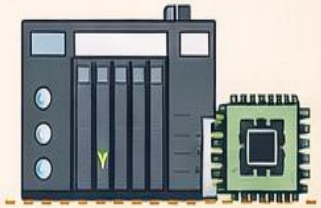
- **Input states from sensors** (e.g., temperature, pressure) are **read** and **latched** into the **Process Image Input (PII)** memory buffer. Acquisition of input values.

Process Image Input (PII)		
I 0.0	I 0.1	I 0.1
I 0.1	I 0.2	I 0.1
I 0.3	I 0.3	I 0.1

Computing Phase

- **The user-written control** program (in languages like Structured Text) **executes once**, using the frozen PII data to calculate output commands.

Execution of the user program.

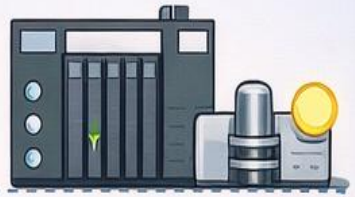


PLC Control Program
IF
IF -/0
THEN
END_IF

Acting Phase

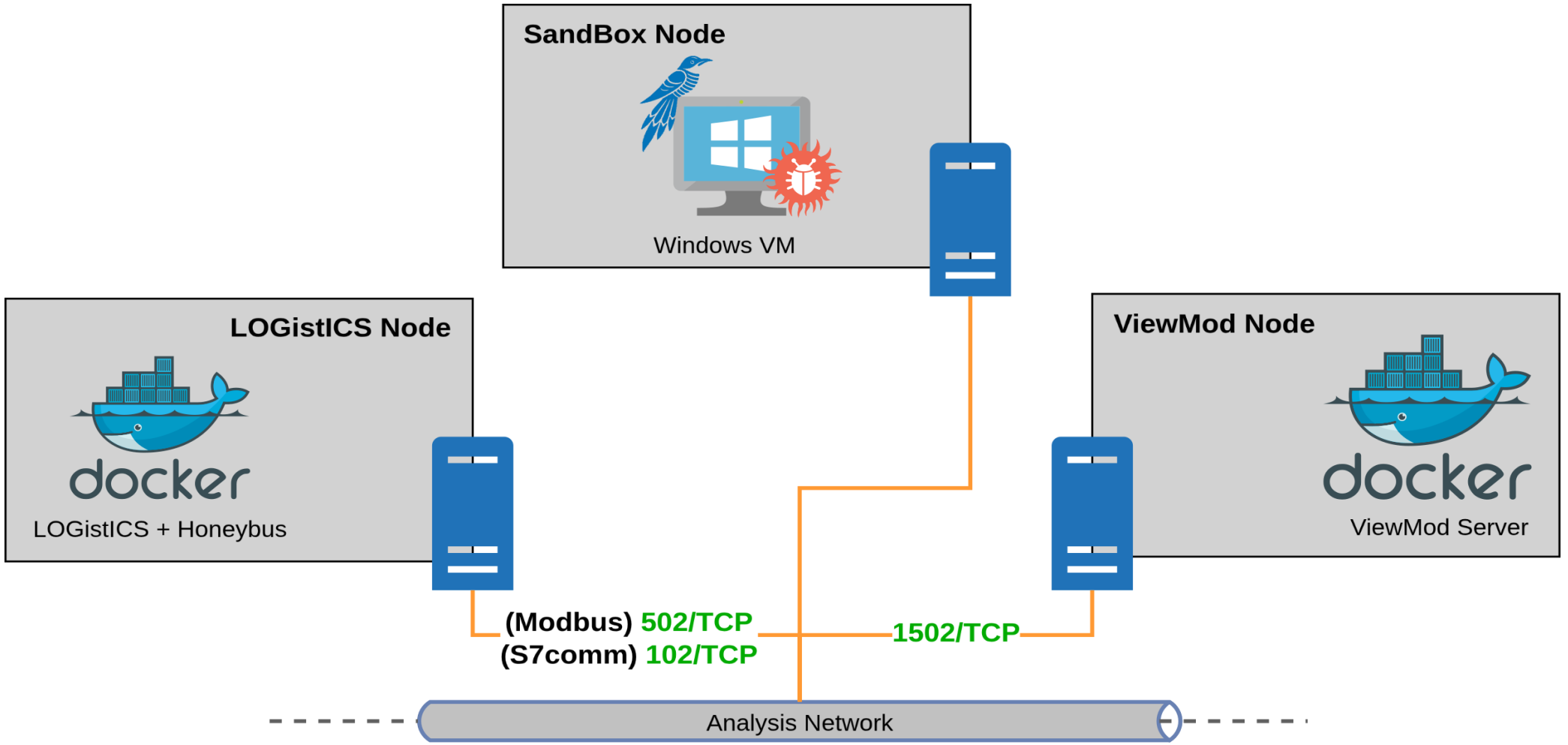
- The computed outputs are written to the Process **Image Output (PIO)** buffer, which is then used to update physical actuators.

Update of output states.



Process Image Output (PIO)		
Q0.0	Q0.1	I 0.1
Q0.2	Q0.2	I 0.1
Q0.3	Q0.3	I 0.1

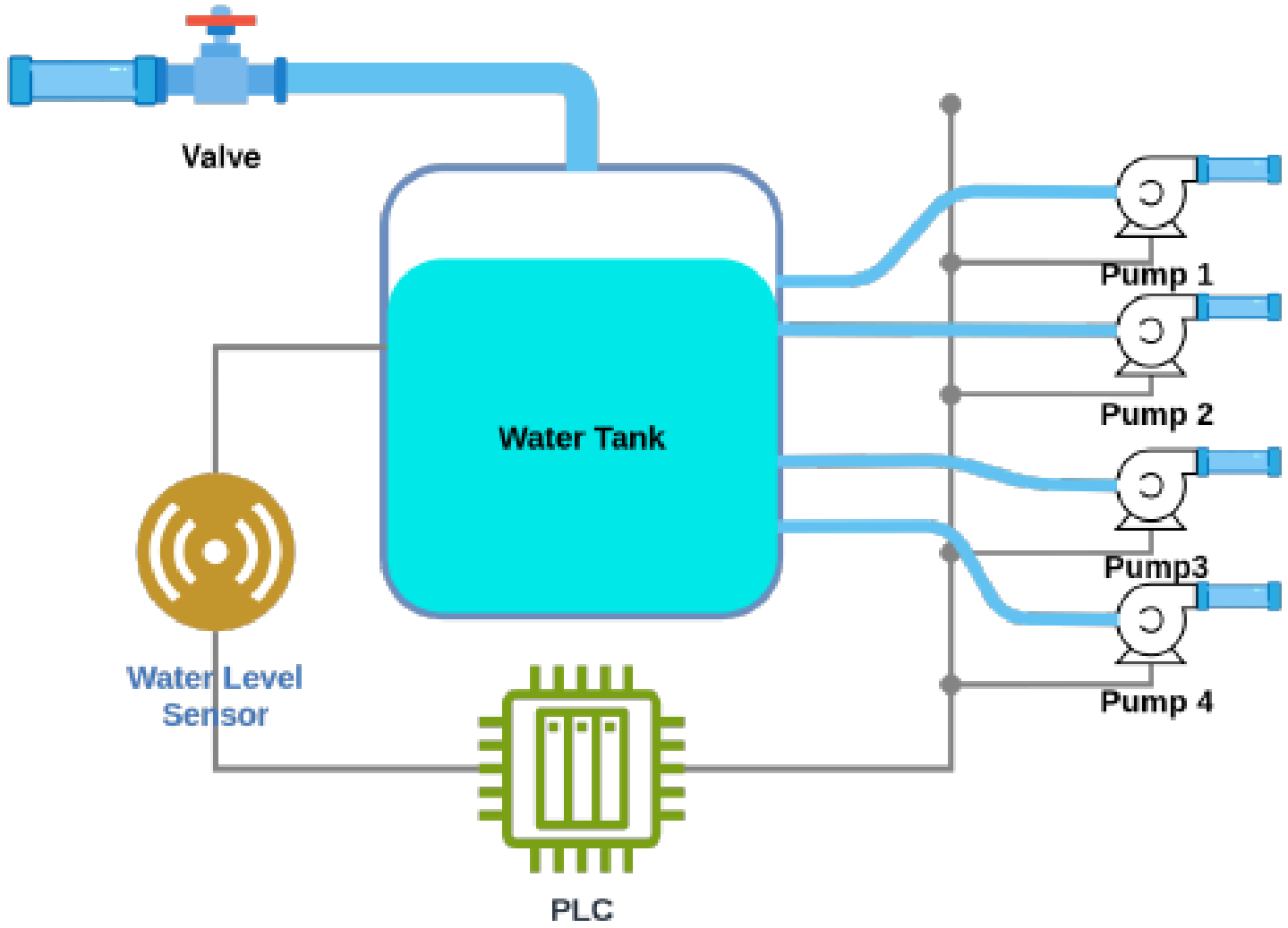
The connection of the three Modules: Network Architecture



ViewMod Default GUI

Modbus Memory & Logs Viewer -192.168.30.4:55296									
CO									
@0 **x (1/0)**	@1 x	@2	@3	@4	@5	@6	@7	@8	@9
@10	@11	@12	@13	@14					
DI									
@0 x	@1	@2	@3	@4	@5	@6	@7	@8	@9
@10	@11	@12	@13	@14	@15	@16	@17	@18	@19
@20	@21	@22	@23	@24	@25	@26	@27	@28	@29
@30									
HR									
@0 x	@1	@2	@3	@4	@5	@6	@7	@8	@9
@10	@11	@12	@13	@14	@15				
IR									
@0 x	@1	@2	@3	@4	@5	@6	@7	@8	@9
@10	@11	@12	@13	@14	@15	@16	@17	@18	@19
@20	@21	@22	@23	@24	@25	@26	@27	@28	@29
@30									

Case-study Example:Water problem PLC

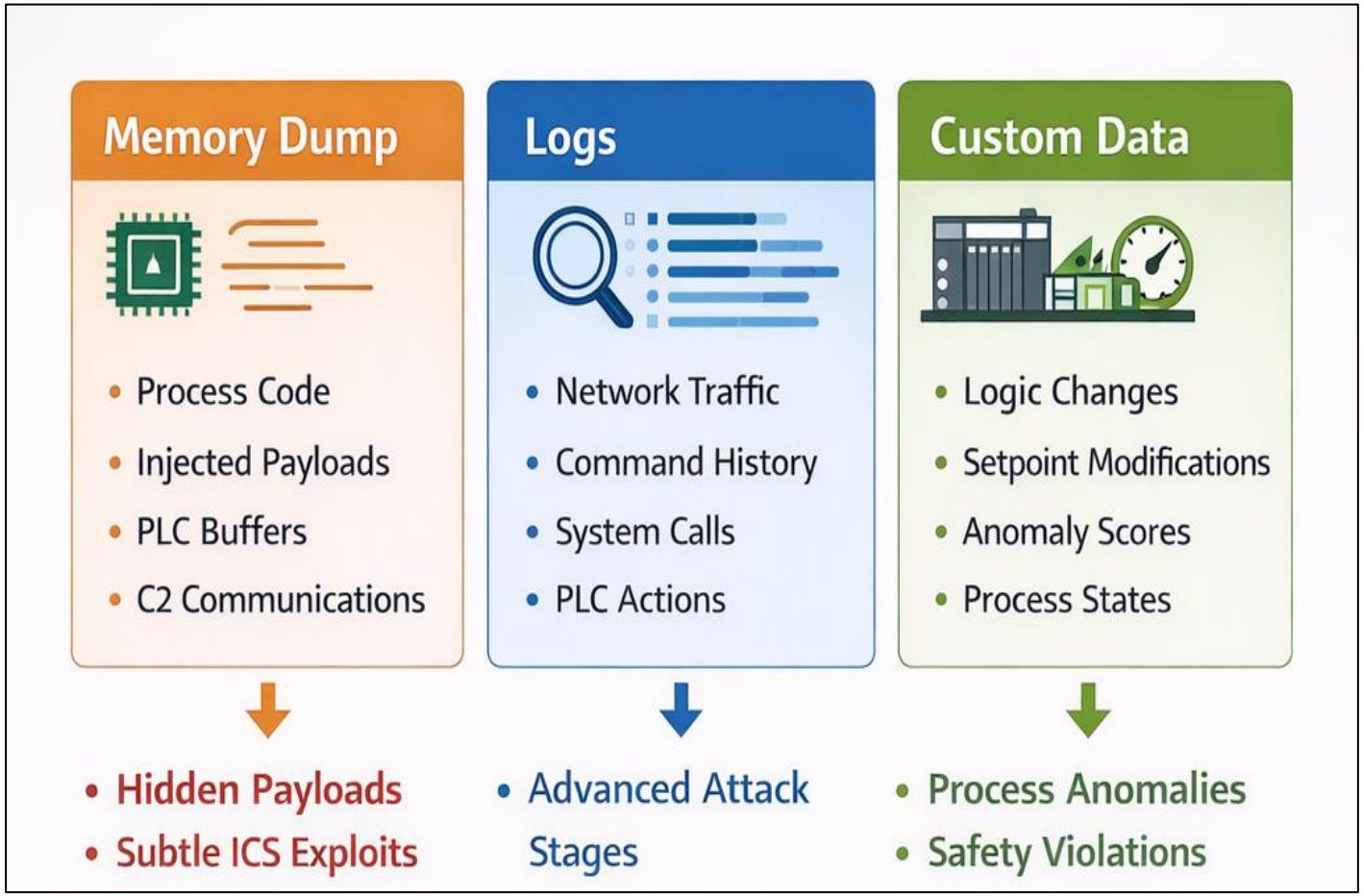


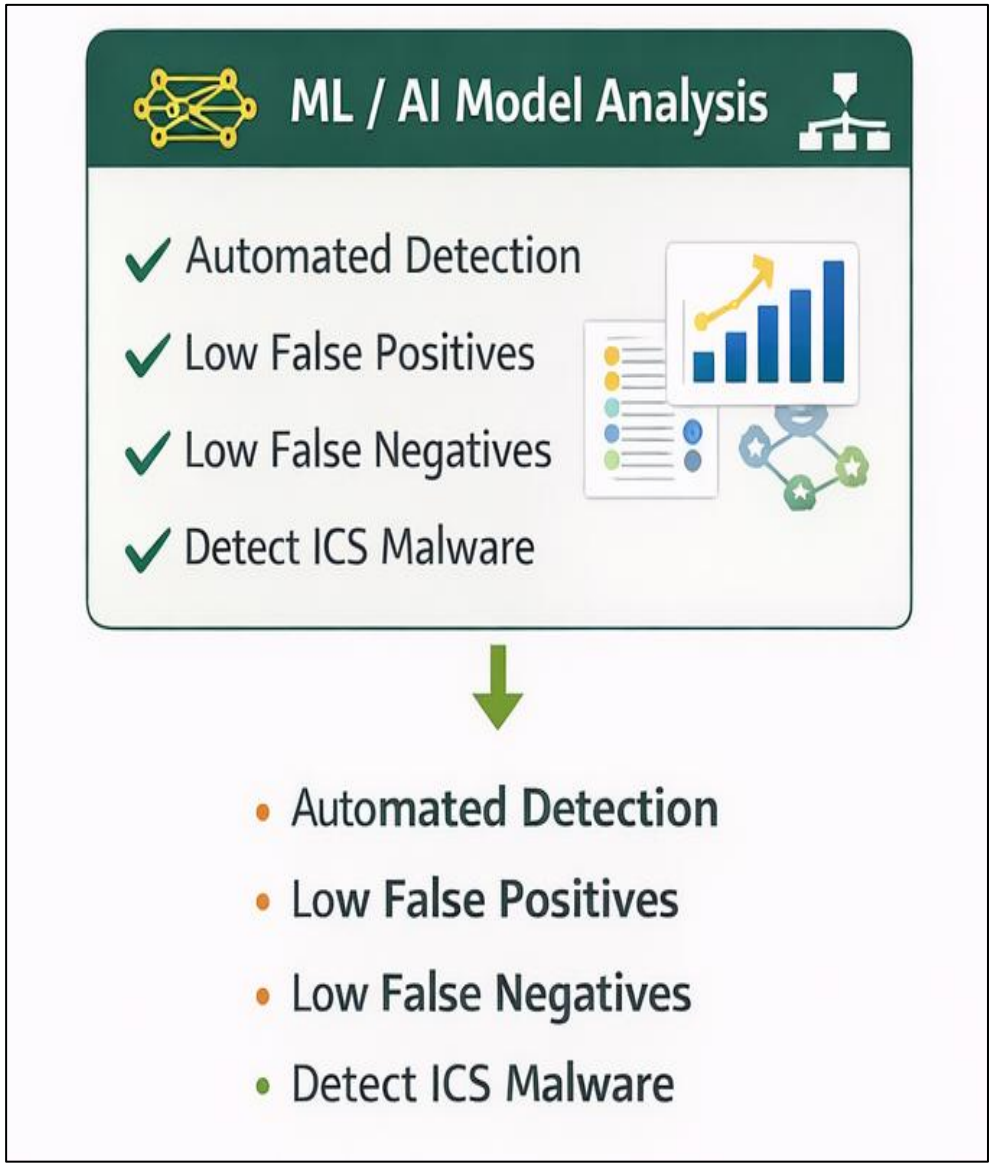
A simple representation of the hypothetical problem.

viewmod on attack

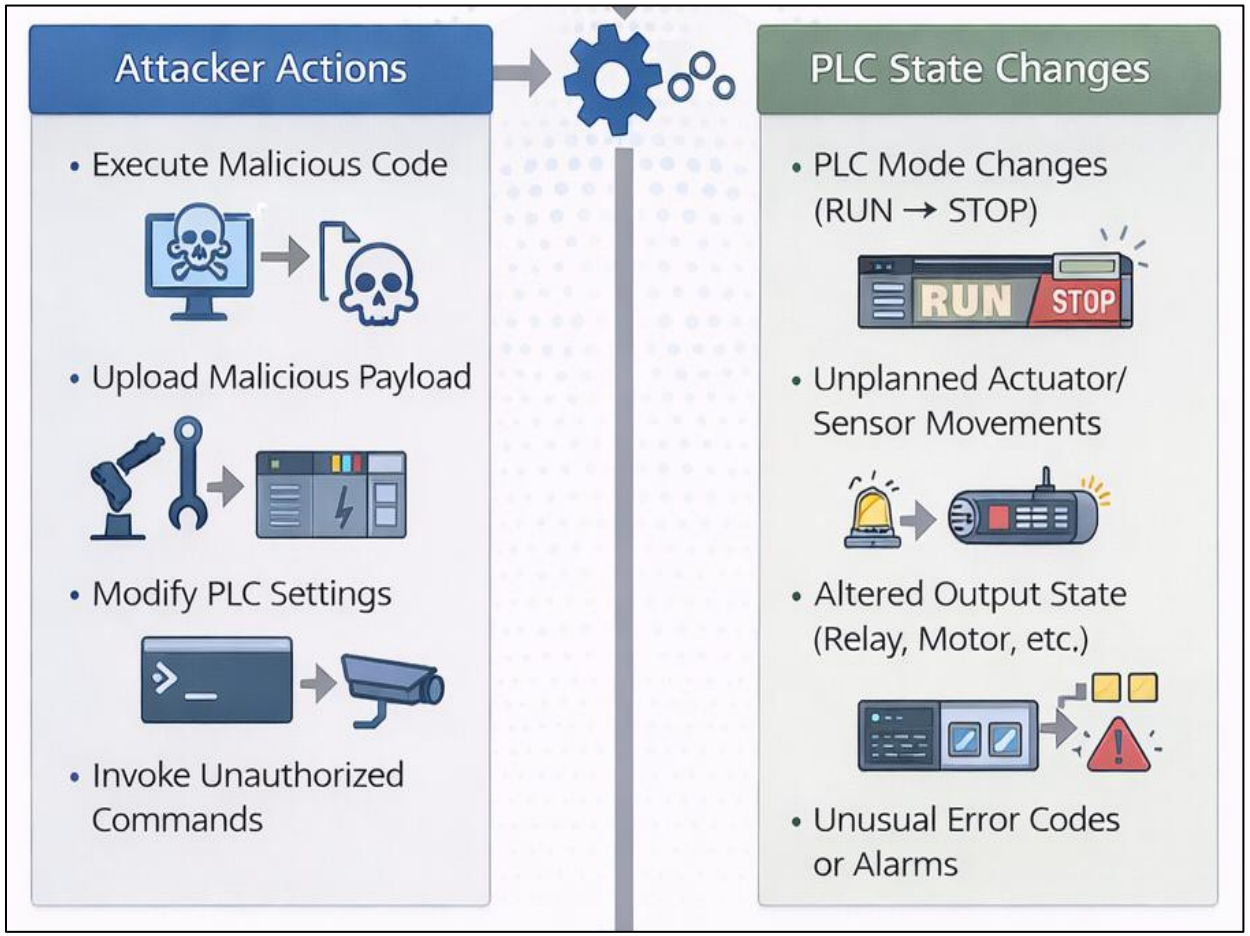
Modbus Memory & Logs Viewer -192.168.30.4:55296									
CO									
@0 **x (1/0)**	@1 x	@2	@3	@4	@5	@6	@7	@8	@9
@10	@11	@12	@13	@14					
DI									
@0 x	@1	@2	@3	@4	@5	@6	@7	@8	@9
@10	@11	@12	@13	@14	@15	@16	@17	@18	@19
@20	@21	@22	@23	@24	@25	@26	@27	@28	@29
@30									
HR									
@0 x	@1	@2	@3	@4	@5	@6	@7	@8	@9
@10	@11	@12	@13	@14	@15				
IR									
@0 x	@1	@2	@3	@4	@5	@6	@7	@8	@9
@10	@11	@12	@13	@14	@15	@16	@17	@18	@19
@20	@21	@22	@23	@24	@25	@26	@27	@28	@29
@30									

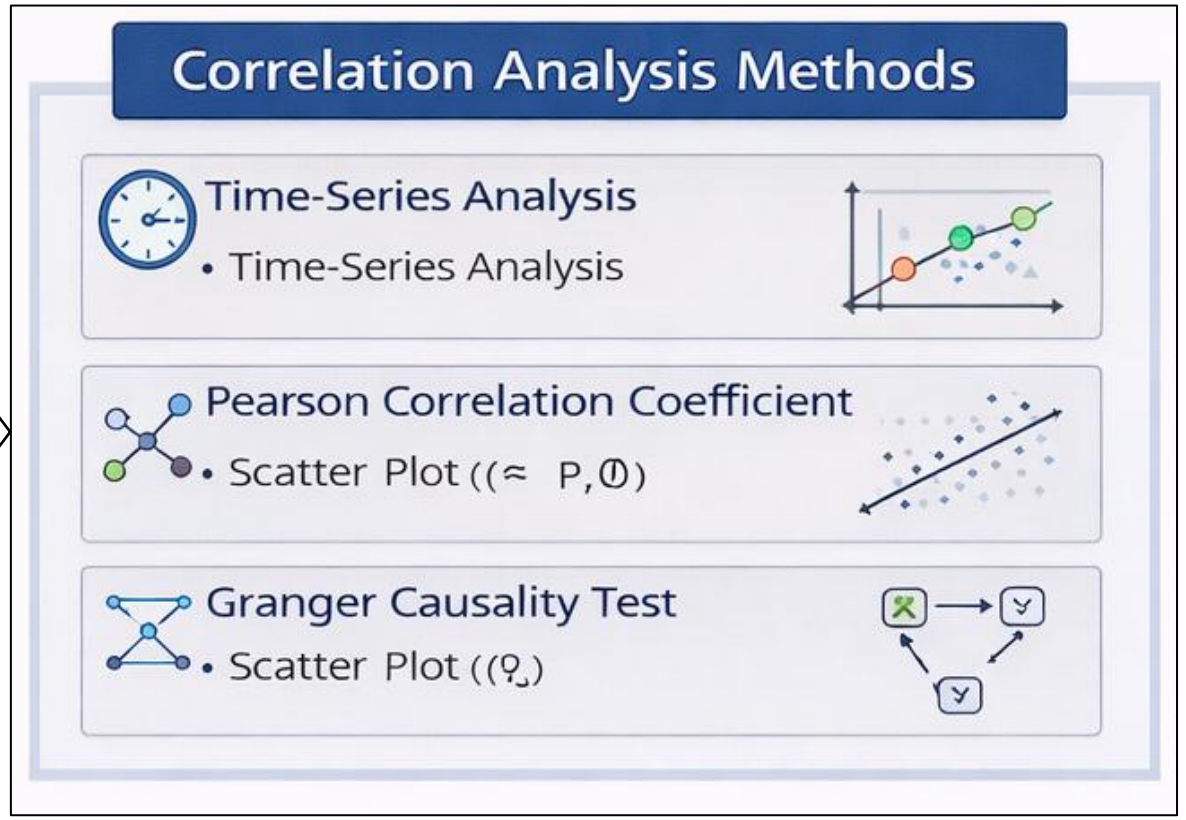
Data Extraction from Honeypot-sandbox interactions to ViewMod





Correlate Attacker Actions with changes in PLC state





False Positive

Benign Activity Labeled as Malicious

Example:

A maintenance script that updates PLC firmware gets detected as malware.

False Negative

Malicious Activity Labeled as Benign

Example:

A hacker installs malware that manipulates PLC registers but it goes undetected.

False Alarm Causing Disruptions

Consequence:

- Unnecessary Downtime
- Reduced Trust in Security System

Undetected Threat Leading to Damage

Consequence:

- Loss of Control & Safety Risks
- Potential Financial & Physical Damage

✓ Benign

Malicious

Project expected outcome

Thank you very much!