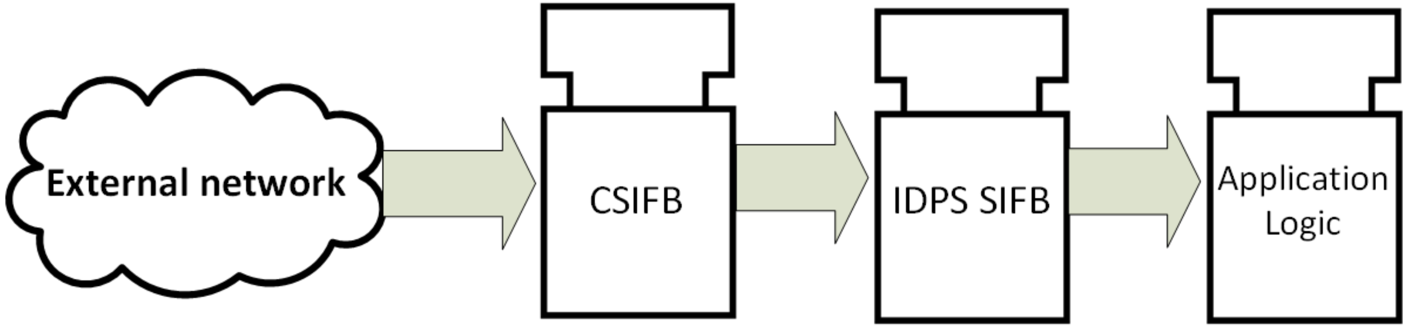
Designing Actively Secure, Highly Available Industrial Automation Applications

Awais Tanveer, Roopak Sinha, Stephen MacDonell, Paulo Leitão, Valeriy Vyatkin

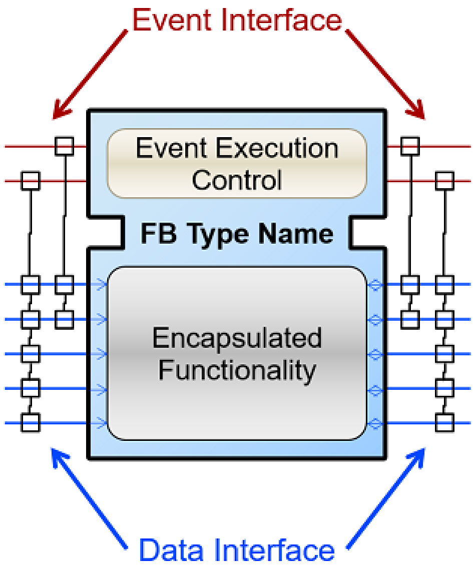
Overview

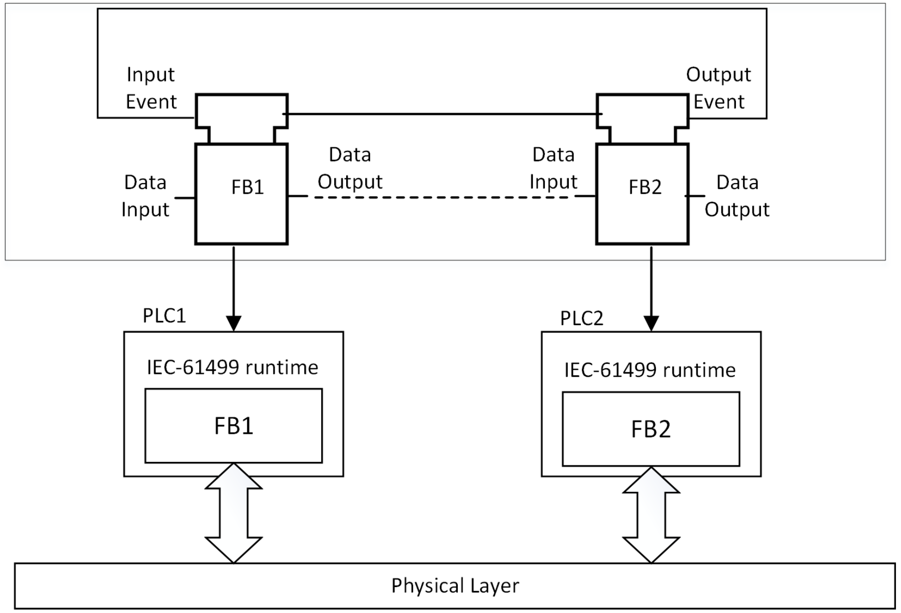
- **Problem**: detect and mitigate unknown availability attacks in IAS.
- **Approach**:
  - Survey literature to enumerate commonly-encountered availability attacks.
  - Create an application-level design pattern to prevent attacks.
- **Contribution**:
  - Service-interface function blocks for using IDPS at design time.



Background

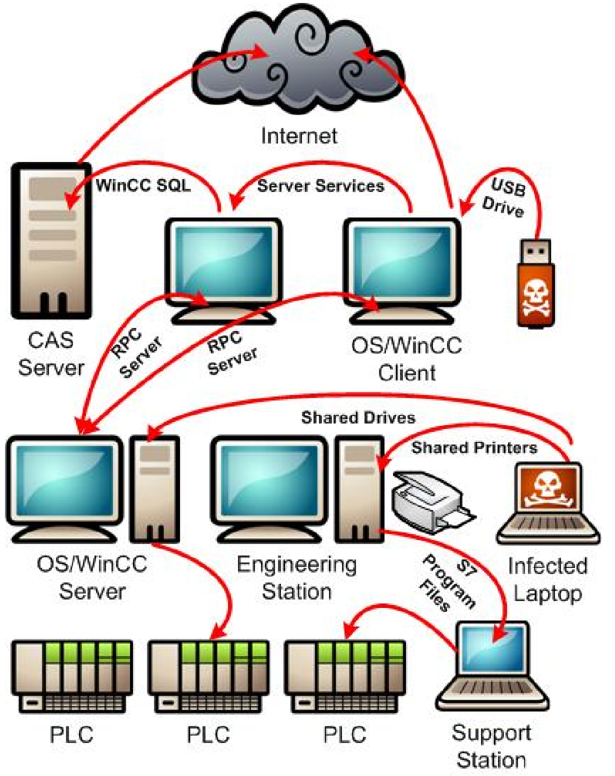
- IEC 61499: An established standard for programming IAS software.
  - Applications are highly distributed over multiple PLCs using networks.
  - Application-level security in IEC 61499 is a very new topic.
- Intrusion Detection and Prevention System (IDPS):
  - Network or host based.
  - Detects attacks and responds accordingly
  - Can be updated more easily

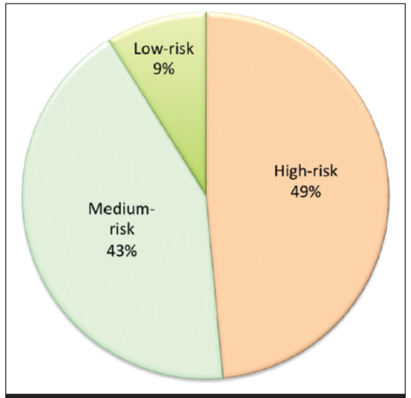




Background: IACS Security

- The Stuxnet worm [1]
  - Targeted PLCs.
- Exploitable vulnerabilities in IACS are growing (Kaspersky, 2016)
  - 49% vulnerabilities are high risk.
  - Zero-day vulnerabilities are the most risky.
- Availability attacks:
  - Replay, man-in-the-middle and stealth command modification attacks carried out on PLC devices [2].
  - Denial of Service (DoS) attacks carried out on real PLC devices rendered them unresponsive [3].





Types of vulnerabilities in industrial control systems in 2015. Source: Kaspersky.

Our Approach

1

Replicate surveyed availability attacks on IEC 61499 applications.

2

Explore the use of IDPS at the application-level during the design phase.

3

Test the chosen solution on a case study.

4

Experimentally quantify the security-performance trade-off.

Replicating Availability Attacks in IEC 61499

a) Attack with malicious or malformed data

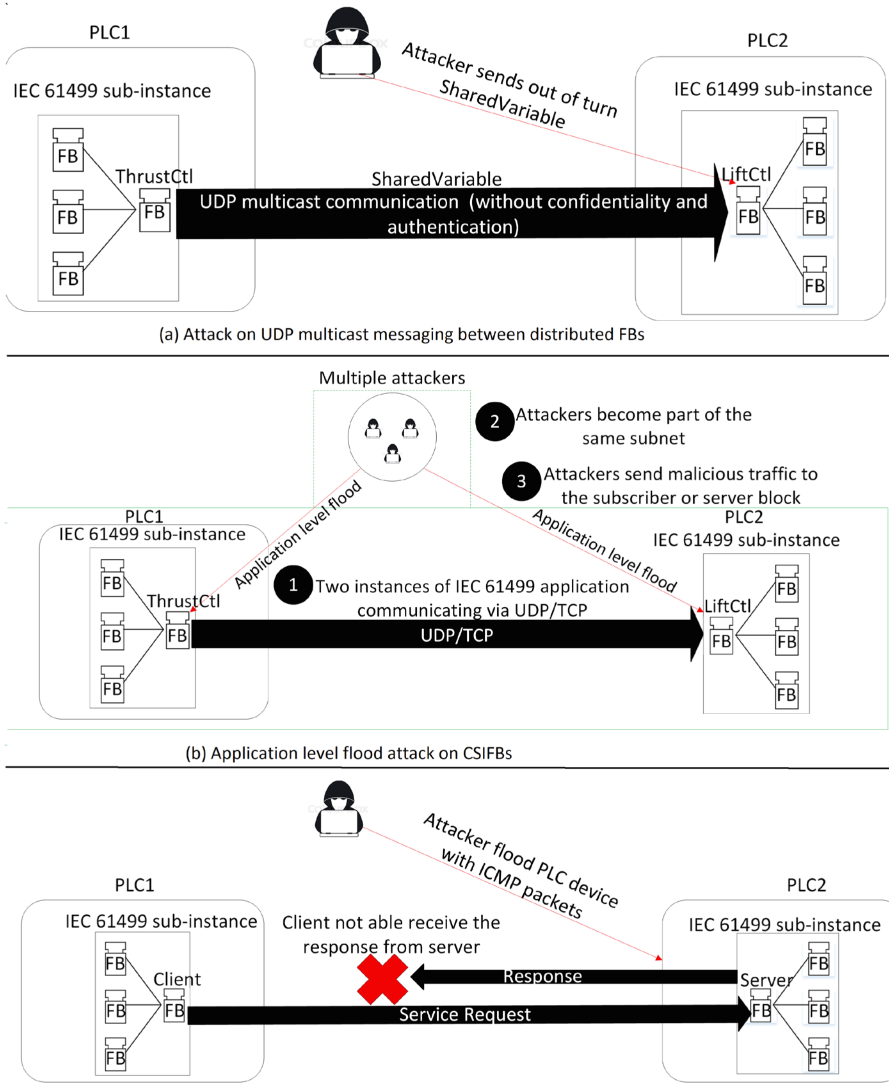
- ***Hypothesis 1:*** *An adversary can send malicious data to the subscriber or server block by masquerading itself as publisher/client Communication Service Interface Block (CSIFB), causing it to misbehave and subsequent disruption of the intended service.*

b) Application-level flood attack

- ***Hypothesis 2:*** *One or multiple adversaries can become a part of the multicast group and flood the publisher/subscriber interface to make it unavailable or slow to respond to legitimate traffic.*

c) Device-level flood attack

- ***Hypothesis 3:*** *One or multiple adversaries can flood the PLC running an instance of IEC 61499 distributed application to make it unavailable for other dependent instances.*

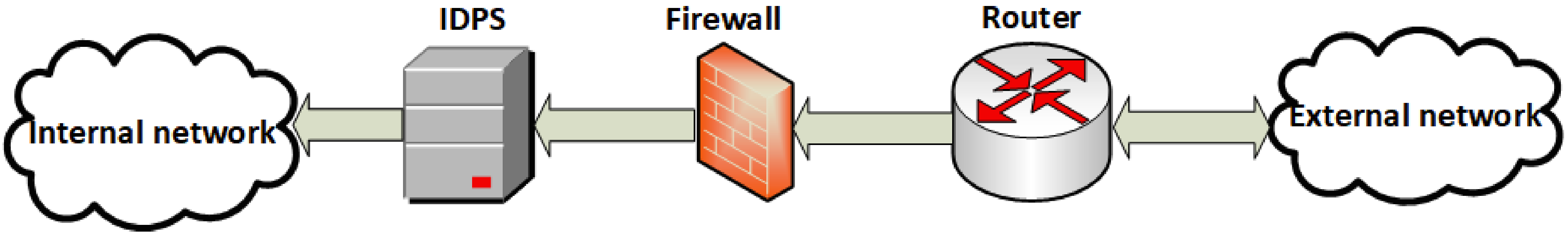

PLC1
IEC 61499 sub-instance
FB
FB
FB
ThrustCtl
FB
Attacker sends out of turn SharedVariable
SharedVariable
UDP multicast communication (without confidentiality and authentication)
PLC2
IEC 61499 sub-instance
LiftCtl
FB
FB
FB
FB
Multiple attackers
2 Attackers become part of the same subnet
3 Attackers send malicious traffic to the subscriber or server block
Application level flood
Application level flood
1 Two instances of IEC 61499 application communicating via UDP/TCP
UDP/TCP
Attacker flood PLC device with ICMP packets
Client not able receive the response from server
Client
Server
Response
Service Request

(a) Attack on UDP multicast messaging between distributed FBs

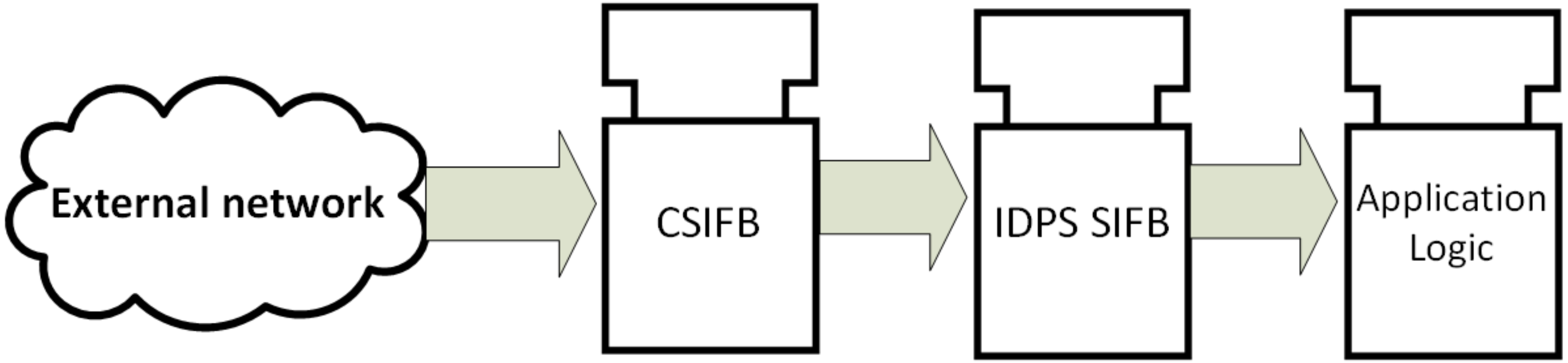
(b) Application level flood attack on CSIFBs

(c) Device level flood attack on PLC

Solution: An SIFB Based Intrusion Detection and Prevention System (IDPS)

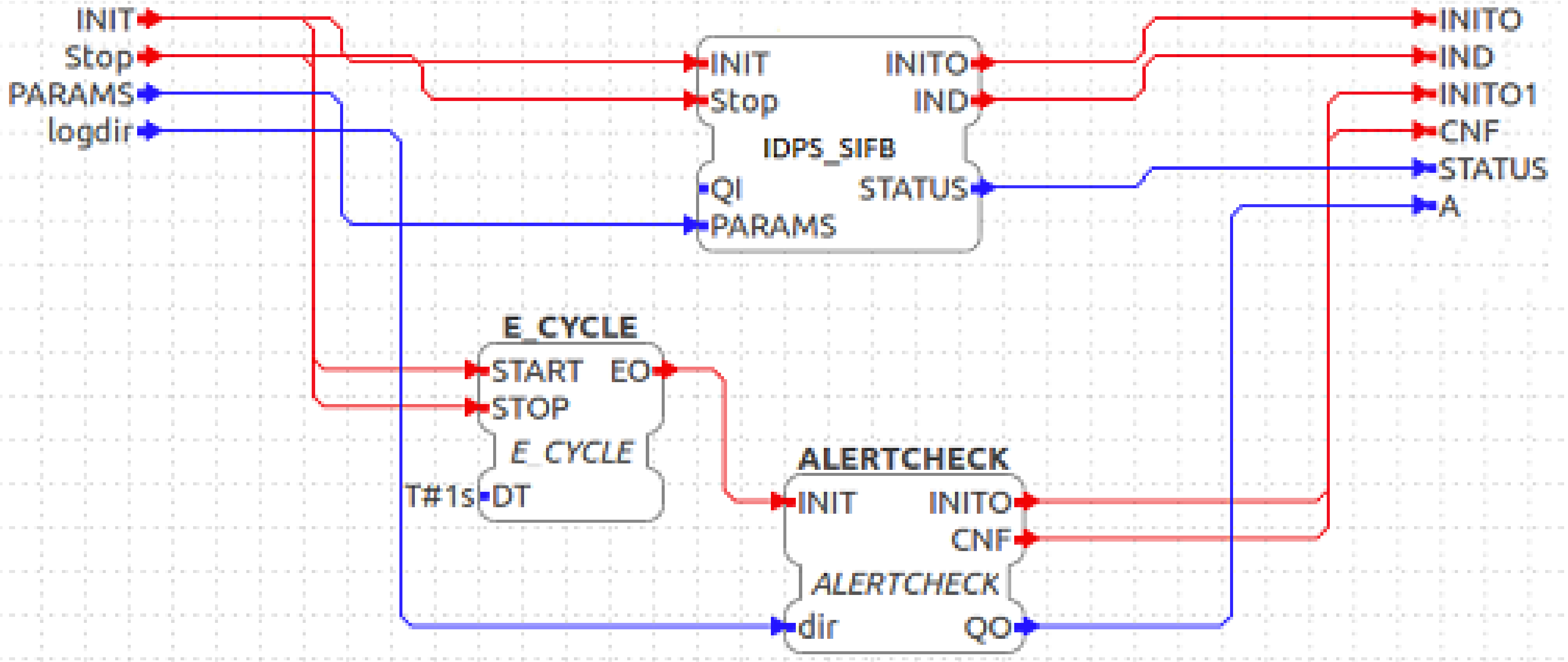


A simple network configuration containing IDPS



Proposed configuration of IDPS SIFB in IEC 61499 distributed applications

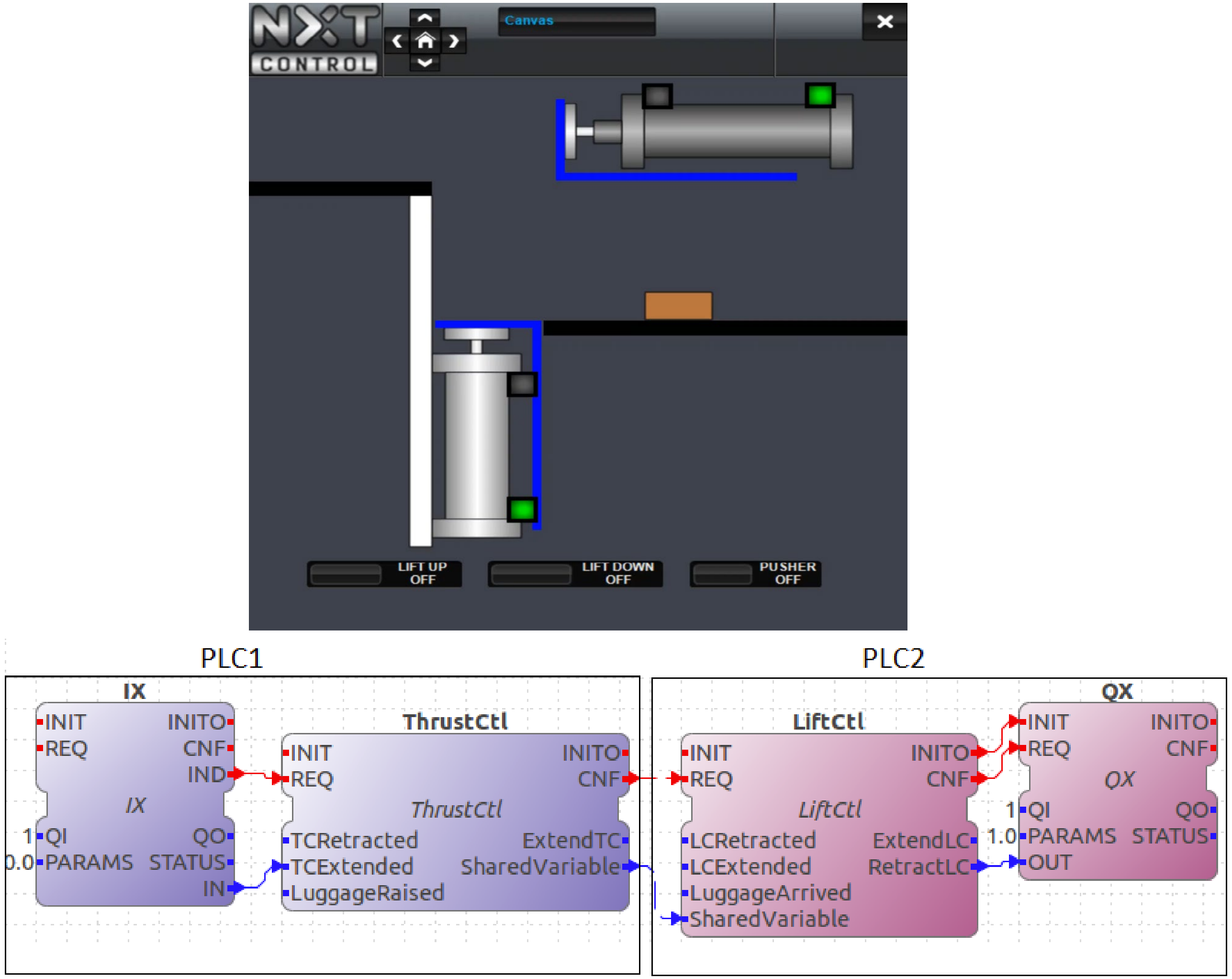
Solution: A Composite Function Block (CFB) using SIFB based IDPS



Solution: Active Security Protection using IDPS_SIFB

- Generic SIFB that may embedded different kinds of IDPS.
- Reactive security: Current signature or rule-based IDPSs cannot detect an new attack.
- Active security: use anomaly-based IDPS using Machine Learning (ML) techniques to identify new attacks.
  - An ML based Intrusion Prevention System (IPS) has been used to prevent attacks against PLCs [4].
  - No current work targets application-level active security protection.

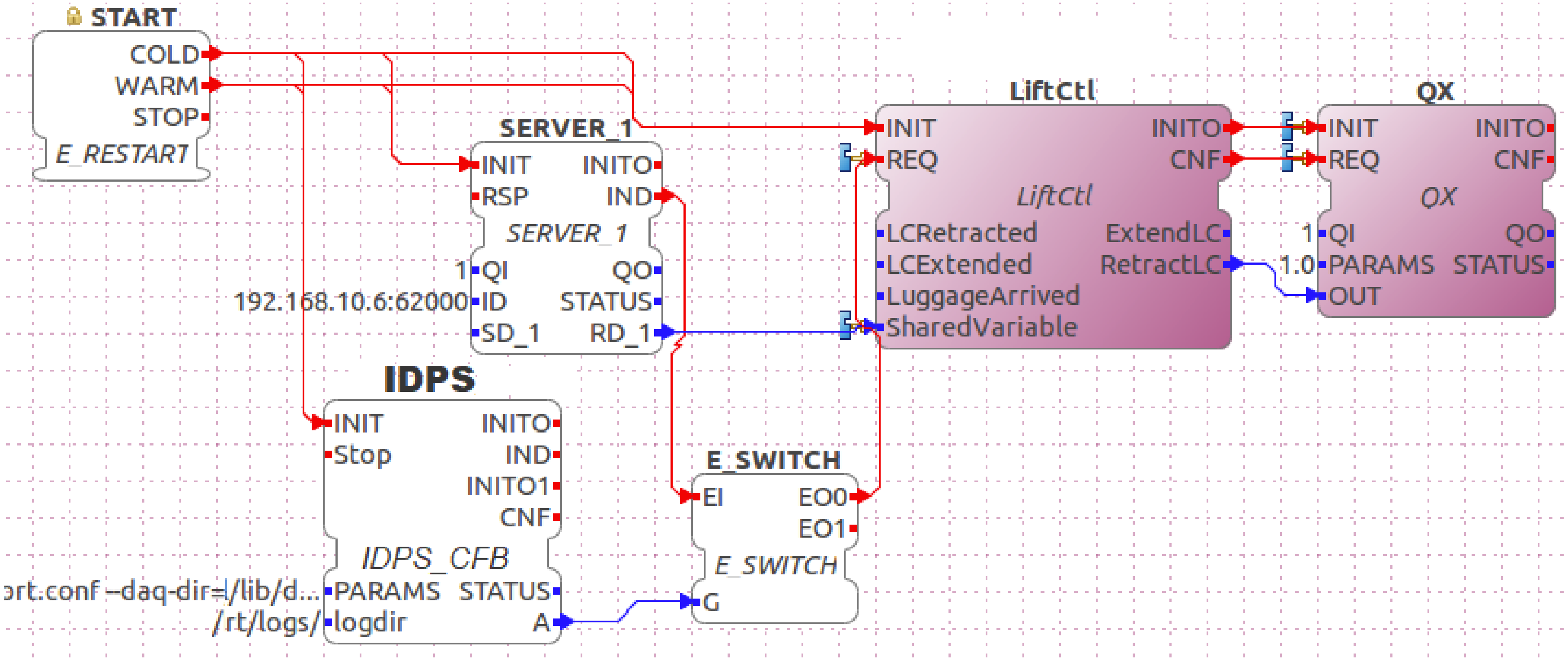
Case Study: Cylinders and Luggage



IEC 61499 implementation of case study

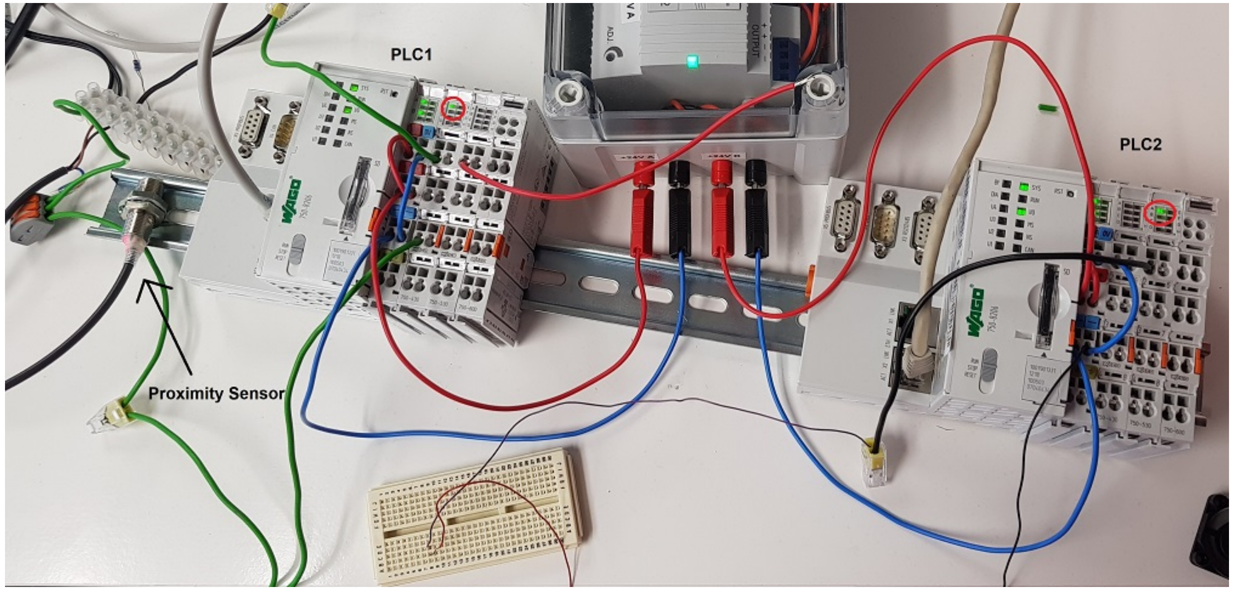
Case Study: Implementation in IEC 61499

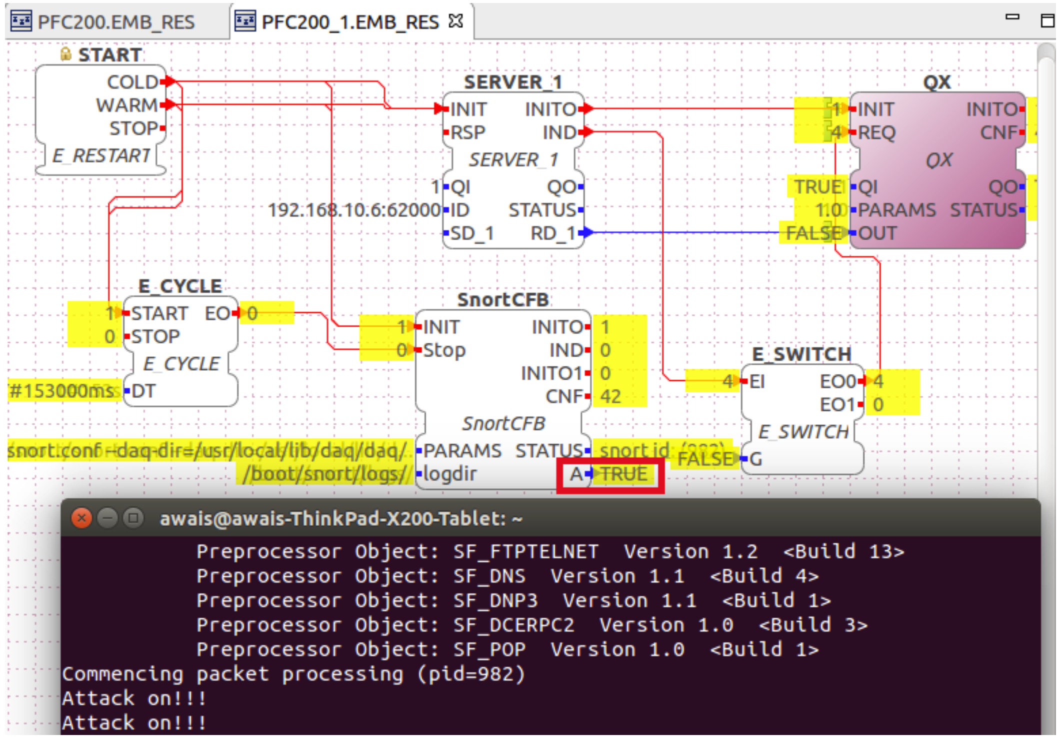
- Usage of *IDPS_CFB* in the case study scenario



Experimental setup

- Two Wago PFC200 PLCs. 4DIAC IDE and FORTE runtime.
- Proximity sensor on PLC1 acting as an input signal to PLC2.
- When PLC2 receives the signals, it intends to lift cylinder 2.
- PLC2 is executing *IDPS_CFB* that is running snort as an IDPS in the background.
- `hping3`: launch DoS attacks
  - Scenarios 1 and 3
- `PackETH`: send malicious data
  - Scenario 2





```
awais@awais-ThinkPad-X200-Tablet: ~
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
Commencing packet processing (pid=982)
Attack on!!!
Attack on!!!
```

Observations: Throughput vs Security

- We observed the number of packets dropped by Snort as the packet frequency increased.
  - When `hping3` was configured with the `–faster` option to send packets each microsecond, the PLC becomes completely unresponsive
  - A sufficiently powerful attacker can succeed even in the presence of an IDPS
  - Such attacks are better handled at device or network level.
- However, application-level IDPS can be very useful in logging and/or filtering out illegitimate traffic that escapes other mitigation strategies
  - Especially during low to medium intensity attacks.

Conclusions and Future Work

- The use of secure SIFBs results in a repeatable, application-level solution for secure design
- At application-level, the attacks that can be handled are limited
  - This solution forms part of an overall strategy to secure an IAS
- Future Work:
  - Formalising the solution as a replicable design pattern in IEC 61499
  - Testing novel ML-based active security protection algorithms

References

1. Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security and Privacy*, *9*(3), 49–51.
2. A. Ghaleb, S. Zhioua, and A. Almulhem, “On PLC network security,” International Journal of Critical Infrastructure Protection, 2018.
3. E. N. Ylmaz, B. Ciylan, S. G¨onen, E. Sindiren, and G. Karacayılmaz, “Cyber security in industrial control systems: Analysis of dos attacks against plcs and the insider effect,” in 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG). IEEE, 2018.
4. T. Alves and T. Morris, “Openplc: An iec 61,131–3 compliant open source industrial controller for cyber security research,” Computers & Security, vol. 78, pp. 364–379, 2018.

Thank you