New York University Abu Dhabi
Modern Microprocessor Architectures Lab
nyuad.nyu.edu/momalab

Enabling Multi-Layer Cyber-Security Assessment of Industrial Control Systems through Hardware-in-the-Loop Testbeds

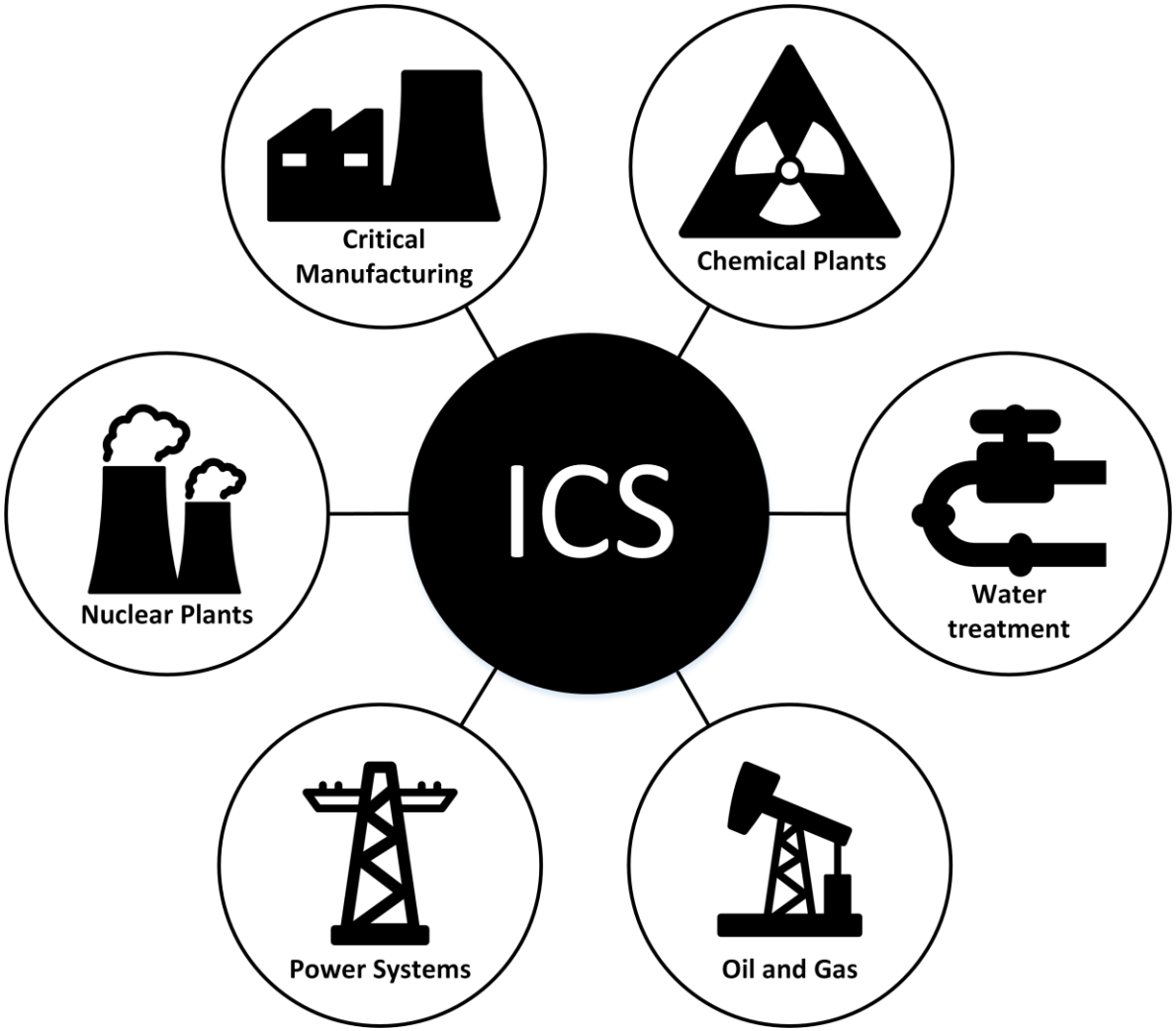
A. Keliris, C. Konstantinou, N. Tsoutsos
NYU School of Engineering

R. Baiad, M. Maniatakos
NYU Abu Dhabi

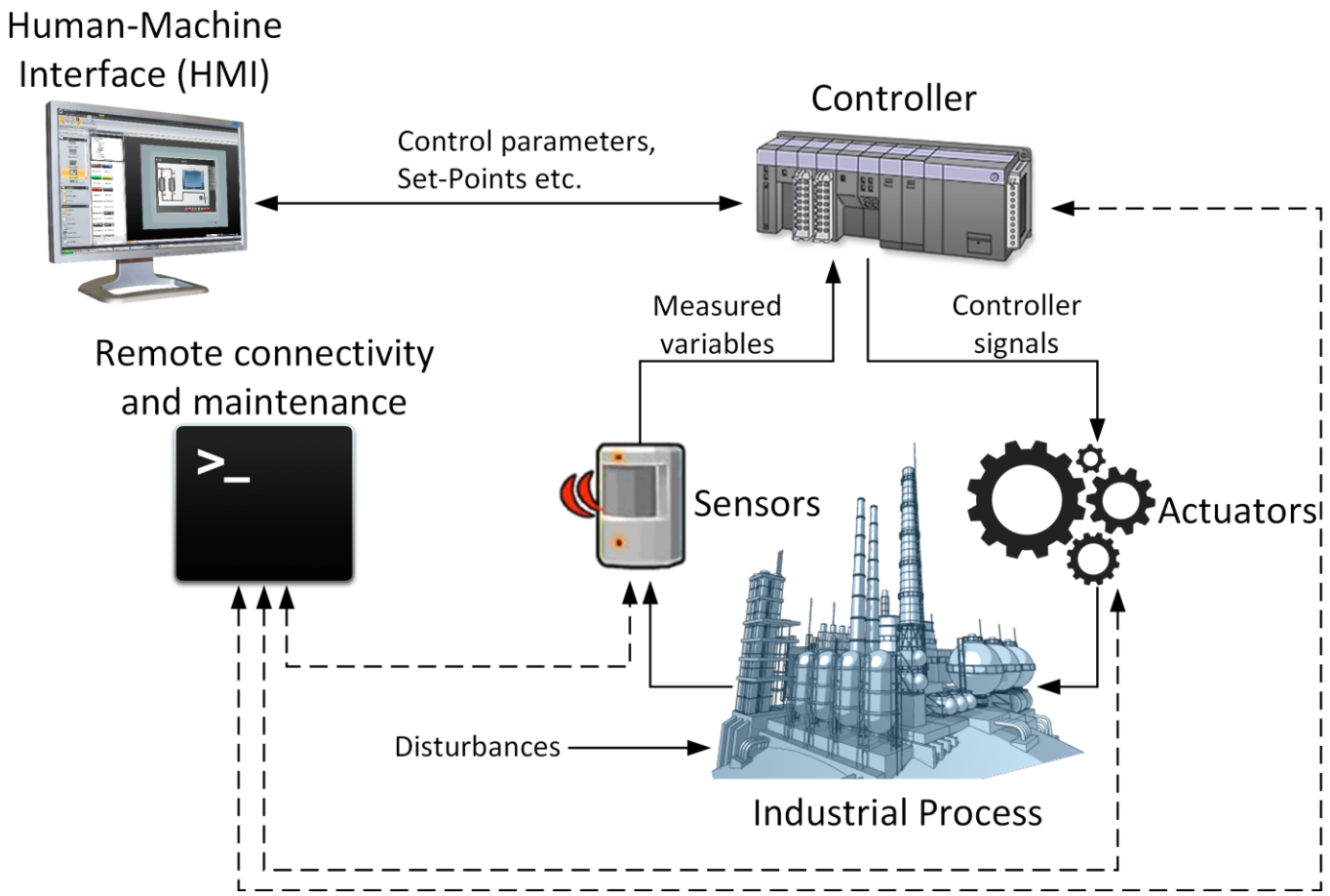
Outline

- Introduction to ICS cyber-security
- Assessment environment considerations
- ICS cyber-security testbed design
- Hardware-In-The-Loop Demo
- Conclusion

What are Industrial Control Systems?



ICS components



Modernization of ICS

- Adoption of IT technologies for increased efficiency, controllability and reliability
- Use of COTS Hardware and Software
  - ARM, Linux
- Advanced features
  - GUI web-servers for management, monitoring and configuration
  - FTP access
  - "Smart" sensors and actuators

ICS targeting cyber-attacks

- Cyber-Security of ICS is critical
- Large number of cyber-attacks on ICS
  - Baku-Tbilisi-Ceyhan pipeline (2008)
  - Stuxnet (2010)
  - Ukraine power-outage (Dec. 21, 2015)
- Urging need for thorough cyber-security assessment
  - At ICS design time and during ICS lifetime cycle

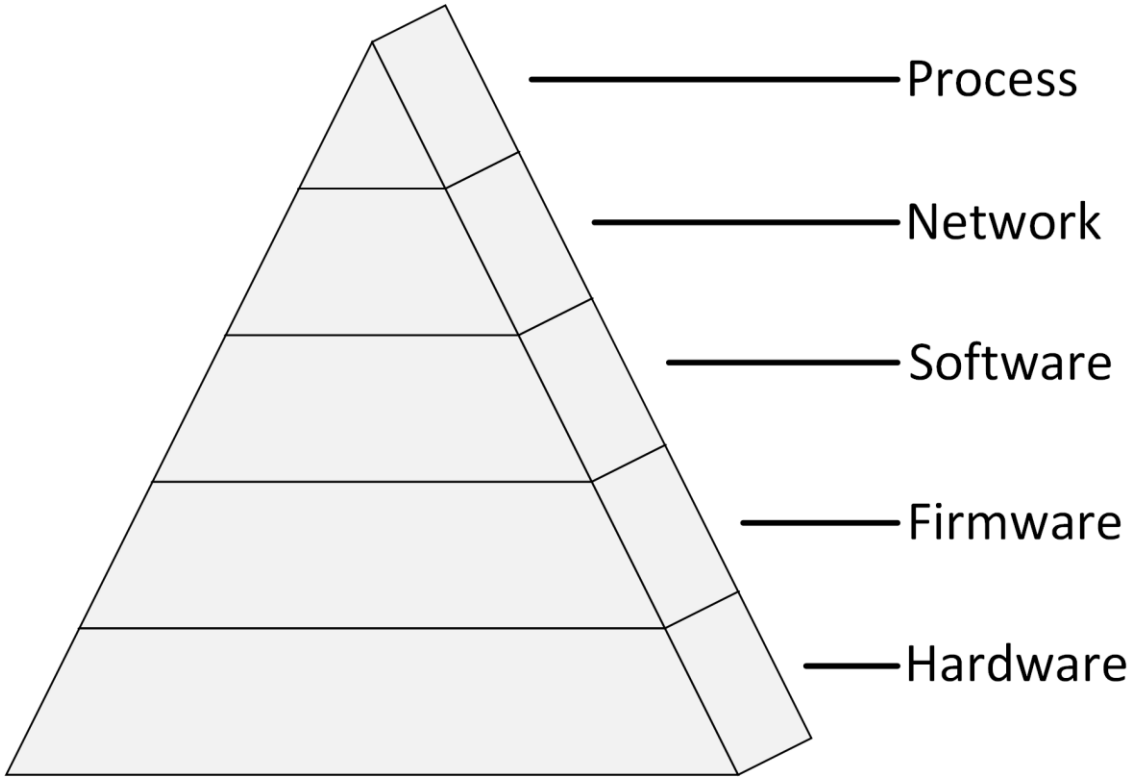
Outline

- Introduction to ICS cyber-security
- Assessment environment considerations
- ICS cyber-security testbed design
- Hardware-In-The-Loop Demo
- Conclusion

IT vs. OT security

- Major differences between IT and OT
  - Physical interaction
  - Security objectives
  - Component lifespan
  - Response time criticality
  - Software changes/updates
  - Protocols

ICS layers



Example attacks on ICS layers

Layer	Vulnerabilities & Threats
Hardware	• Hardware Trojans • Fault Injection Attacks • Side-Channel Attacks
Firmware	• Firmware reverse engineering • Firmware vulnerabilities • Firmware modifications
Software	• Memory corruption & control flow attacks • Web attacks on multipurpose workstations • Zero-day vulnerability markets
Network	• Firewall misconfiguration • Protocol vulnerabilities • Internet-facing ICS
Process	• Process-aware manipulation of control logic & process variables • False data injection attacks • Automatic payload generation

ICS testbed requirements

- Adhere to OT security objectives
- Enable studying attacks at all layers
  - Individual layer and cross-layer attacks
- Capture complex ICS behavior
  - For operational and non-operational conditions
- Support for modern and legacy components
- Cost-effective and scalable

Outline

- Introduction to ICS cyber-security
- Assessment environment considerations
- ICS cyber-security testbed design
- Hardware-In-The-Loop Demo
- Conclusion

Possible approaches

- Testbed cannot include production environment
  - Hazardous: Physical world interaction
- Complete duplication of ICS setup
  - Not cost effective
- Software-only approach
  - Software models and simulation

Software-only testbed

+ cost effective

+ scalable

+ fast simulation

– cannot capture complexity of ICS

– analysis is restricted

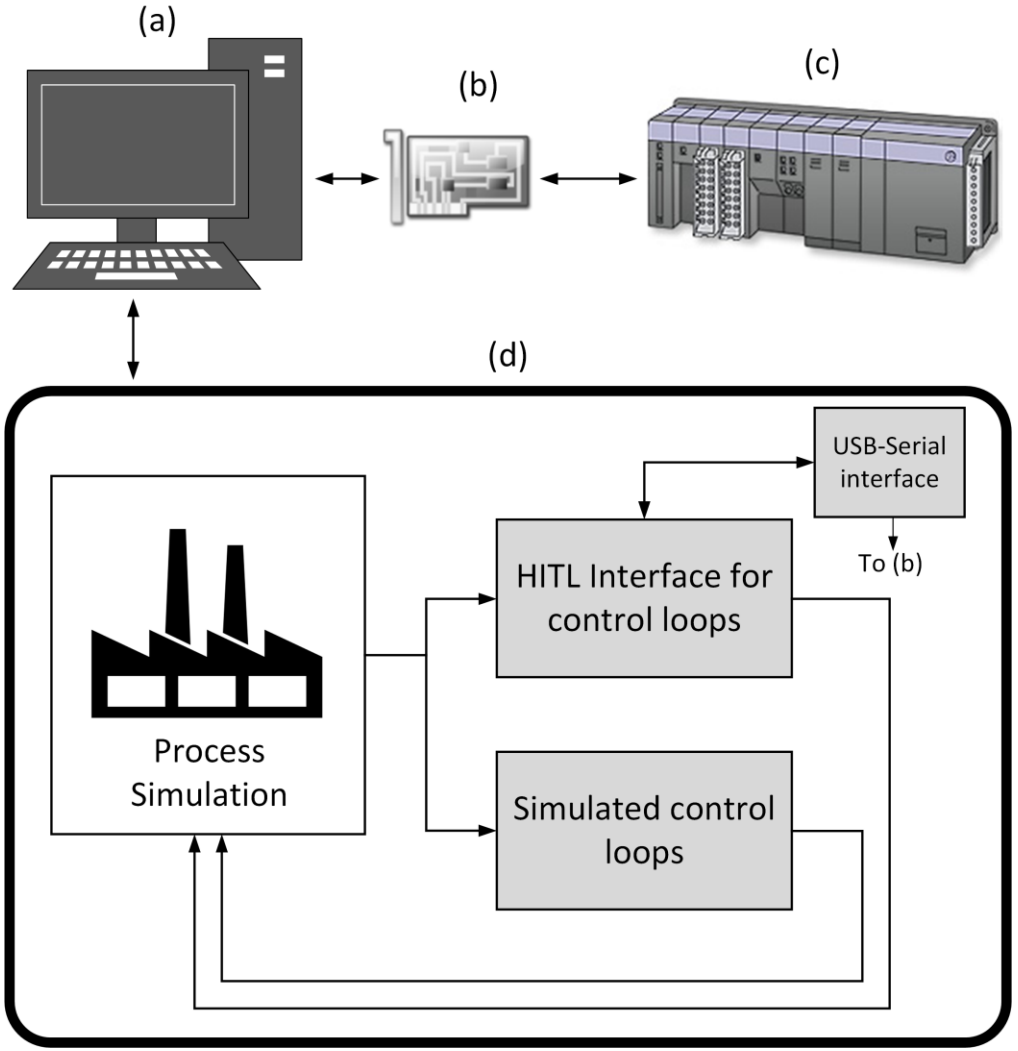
– software models introduce delays and simplifying assumptions

– heavy dependence on model quality

Hardware-In-The-Loop

- Assessment environment must include hardware components
- Hybrid approach: Duplication & Software
- Hardware-In-The-Loop (HITL)
  - Cost effective, fast simulation
  - Modular design, scalable
  - All ICS layers can be studied
  - Hardware components enable realistic and accurate security analysis of ICS

HITL setup



a) Host PC running simulation model

b) Serial Interface Board

c) PLC controller with offloaded control loops

d) Simulation model

Outline

- Introduction to ICS cyber-security
- Assessment environment considerations
- ICS cyber-security testbed design
- Hardware-In-The-Loop Demo
- Conclusion

NYU-AD testbed environment

- Hardware-In-the-Loop setup
- Simulation model of Tennessee Eastman chemical process in Simulink
- 2 cascade PI controllers responsible for *Reactor Pressure* offloaded to PLC
  - Wago 750-881 PLC
  - 2 analog inputs, 2 analog outputs
- Communication: Serial Interface Board
  - ADC, DAC, voltage amplification

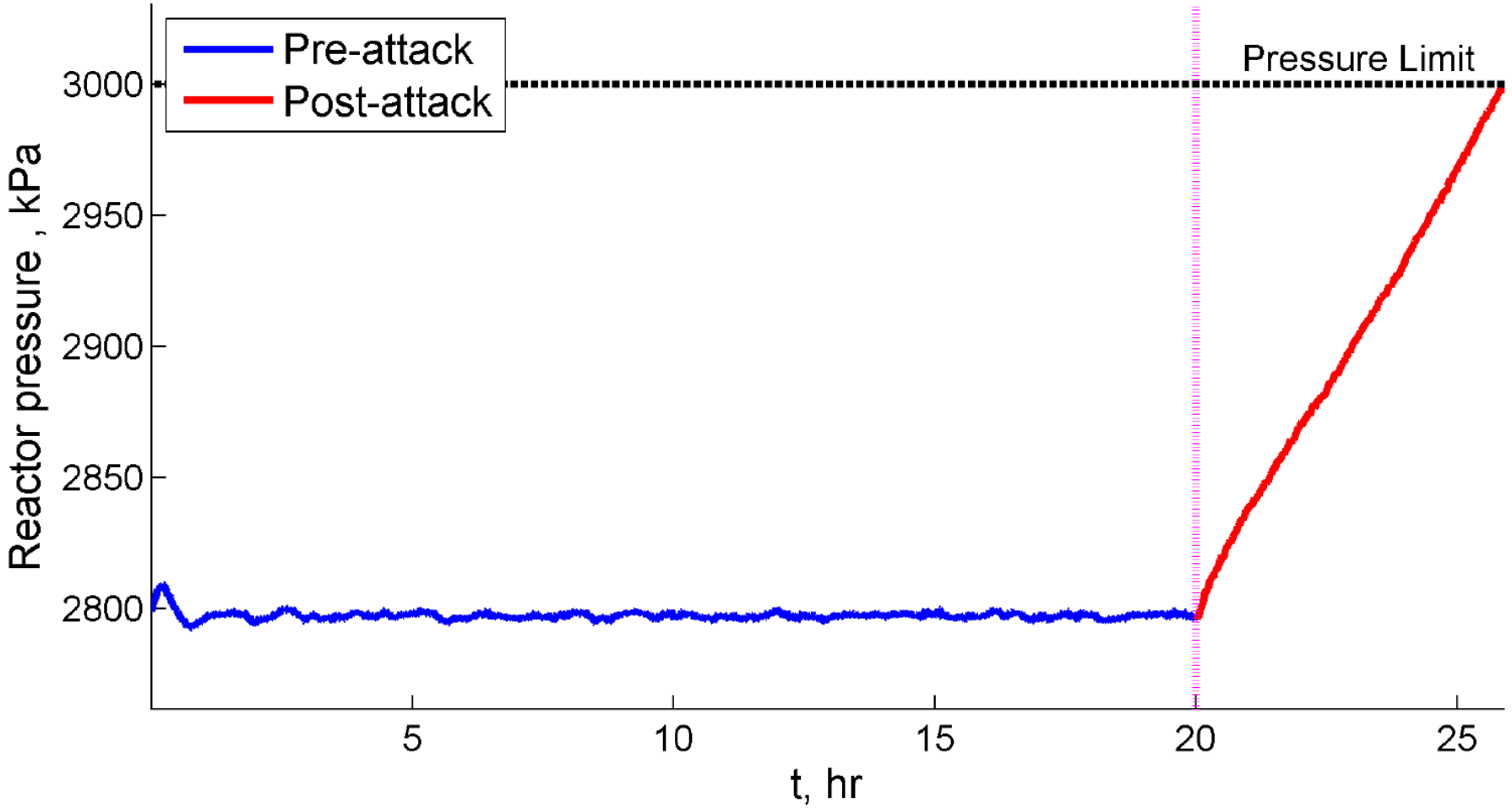
Wago PLC vulnerabilities

- Hardcoded credentials
  - Reverse engineered firmware
- Unencrypted network communication
  - Reverse engineered communication protocol
- Unauthenticated FTP access
- Secondary Ethernet port allows concurrent connections

Attack methodology

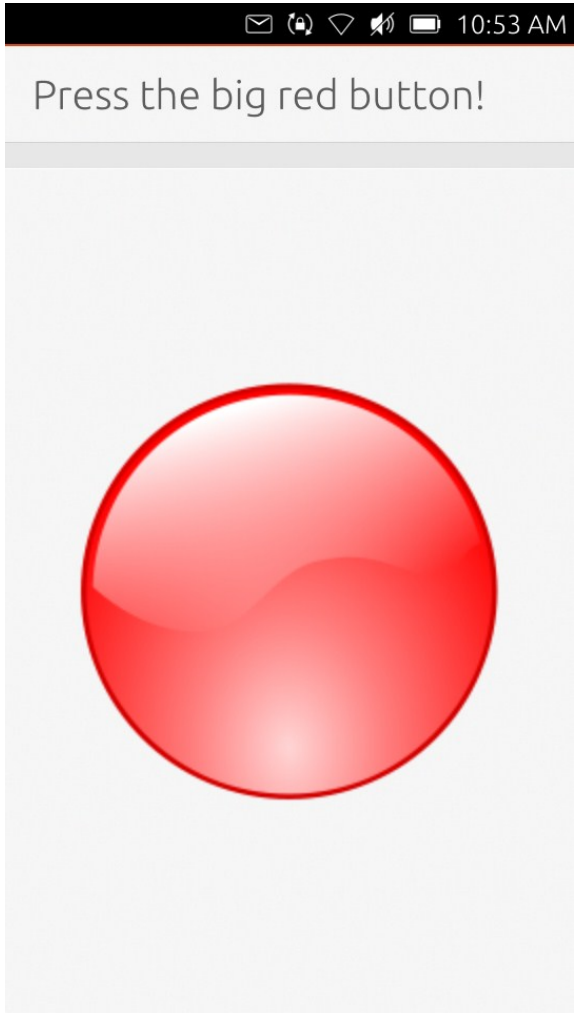
- [HW] Connect to secondary Ethernet port
- [NW] Establish communication link
- [FW] Authenticate with hardcoded credentials
- [NW] Download existing ladder logic over FTP
- [PR] Modify constant variables in ladder logic
- [SW] Calculate new checksum
- [NW] Send modified back to PLC
- [NW] Force-reload the modified ladder project

Attack: Modify integral gain



Attack deployment

- Ubuntu phone
  - Aquaris BQ E4.5
  - Ubuntu 13.04
- Phone application
  - Ubuntu SDK
  - QML app
- Attack script
  - Python 2.7
  - *socket* module




DEMO

Conclusion

- Critical infrastructure is vulnerable to cyber-attacks
- To study and protect against them we need cyber-security assessment environments (testbeds)
- Presence of hardware is required
- → Hardware-in-the-Loop testbeds