A Joint Venture of TÜV Austria and TU Wien

Safety and Security in Industry Research Lab „SafeSecLab“

TÜV AUSTRIA

TU WIEN

#SafeSecLab

Project 6 Model-Based Security and Safety Evaluation of OT Components

Evaluation of Operational Technology (OT) components in Industrial Control Systems (ICSs) is valuable in auditing, resource management, and essential in maintaining OT safety and security. This PhD project aims to develop a state-of-the-art model-based testing prototype for the functional safety and security of OT components based on engineering artifacts and network tools. Test results attempt to provide the possible threats, vulnerabilities, and safety concerns in ICSs and will suggest possible mitigation strategies.

Mukund Bhole

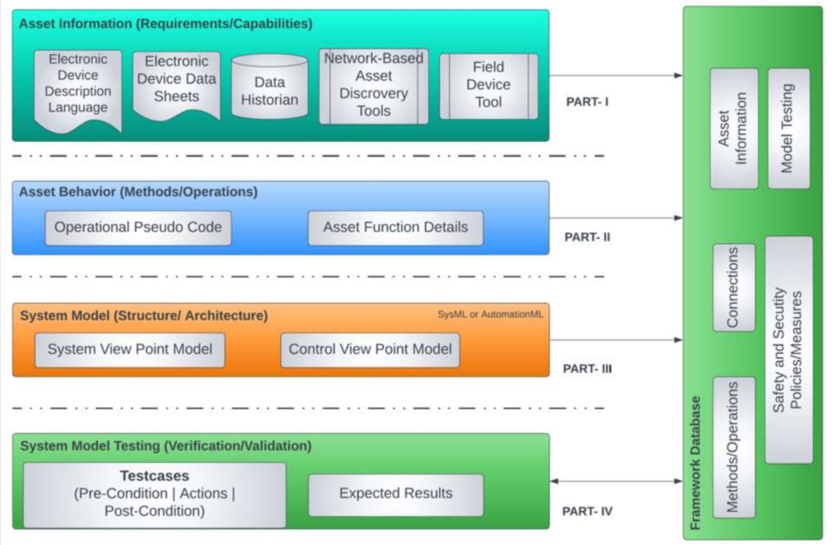
Education:
- Bachelor‘s in Information Technology
- Master‘s in Information Security

Experience:
Research Intern, Emerson Innovation Center

Interests:
Information Security | Penetration Testing | Industrial Automation-Control Systems | Intrusion-Vulnerability Detection.

State-of-the-Art

Model-Based Testing (MBT) is considered a leading cutting-edge technology in the industry. The development of automated test case generation, test data, and procedures to test the system in are most important. MBT has proven to increase the quality and efficiency of the system by behavioral analysis of a System Under Test (SUT) [*]. The results from the tests are used for debugging safety and security flaws in the system to protect and increase productivity in the system.


Asset Information (Requirements/Capabilities)
Electronic Device Description Language
Electronic Device Data Sheets
Data Historian
Network-Based Asset Discrovery Tools
Field Device Tool
PART- I
Asset Behavior (Methods/Operations)
Operational Pseudo Code
Asset Function Details
PART- II
System Model (Structure/ Architecture)
SysML or AutomationML
System View Point Model
Control View Point Model
PART- III
System Model Testing (Verification/Validation)
Testcases (Pre-Condition | Actions | Post-Condition)
Expected Results
PART- IV
Framework Database
Asset Information
Model Testing
Connections
Safety and Secutity Policies/Measures
Methods/Operations

Research Questions

- Which engineering artifacts are suitable for automated verification? What information/properties/parameters from the engineering artifacts should be used?
- Which procedure allow to check the entire components from the existing system?
- How far can safety and security of OT components be tested, and mitigation strategies of vulnerabilities be automatically identified?
- Which IT security tools applicable for OT?
- How can the system be kept up to date?

Protection Catalog

(Process-Specific)

Safety

- **IEC 61511** (Functional safety - Safety instrumented systems for the process industry sector)
- **IEC 61311-6** (Programmable controllers - Part 6: Functional safety)
- **IEC 61784-3** (Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions)
- **IEC 61508** (Methods on how to apply, design, deploy and maintain automatic protection systems called safety-related systems)
- **IEC 62061** (Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems)
- **IEC 13849-1** (Safety-related parts of a control system)

Security

- **IEC 62443** (Cybersecurity for operational technology in automation and control systems)
- **IEC TR 63074** (Safety of machinery - Security aspects related to functional safety of safety-related control systems)
- **IEC TR 63069** (Industrial-process measurement, control and automation Framework for functional safety and security)
- **ISO/TR 22100-4** (Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects)
- **ISO/IEC 27002** (Information technology — Security techniques — Code of practice for information security controls)
- Vulnerability Databases (NVD, OSVDB/VulnDB, US-CERT, CVE)

Supervisor: Wolfgang Kastner (TU Wien)
Co-Supervisor: Thilo Sauter (TU Wien)
Contact Person: Thomas Doms (TÜV)

[*] Peleska, J. *Industrial-strength model-based testing - state of the art and current challenges*. from https://arxiv.org/abs/1303.1006