Securing the Testing Process for Industrial Automation Software

Matthias Eckhart and Andreas Ekelhart

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
SBA Research

Problem & Motivation

The software testing process represents an **attractive attack target**:

- Risk of software piracy & theft of IP
- Covert attacks based on know-how gained via stolen artifacts (cf. Stuxnet)
- Means to conceal injected malicious code
- Potential damages to physical systems during test execution

Conducting security analyses (e.g., as per the VDI/VDE 2182 [7] guideline) of the testing process is **challenging**:

- Requires expert security know-how
- Is complex and effortful to perform
- Insufficient tool support available

Need: Framework to (semi-)automate security risk assessments with flexible assessment scope

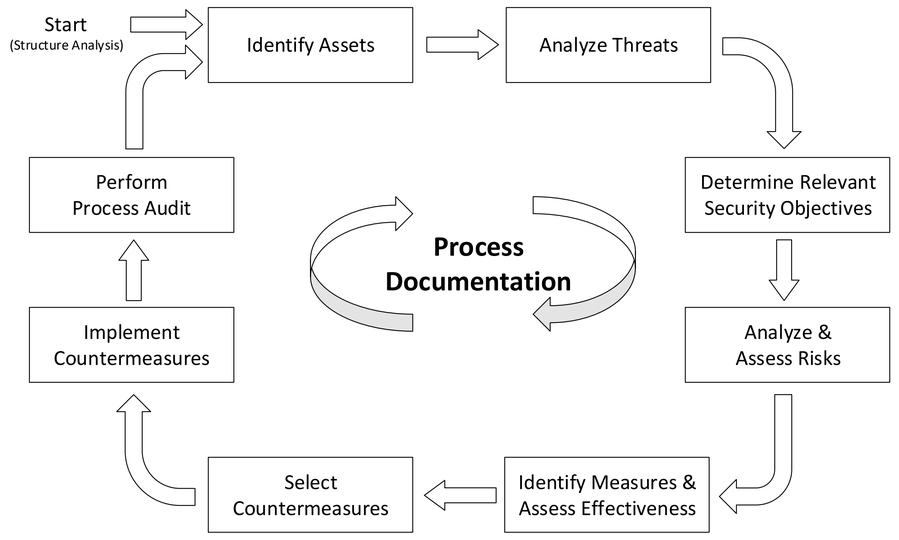

Figure 1: The procedural method according to the VDI/VDE 2182 [7] guideline.

Semi-Automated Security Analysis Framework

Contribution [1]: Provides the capabilities to conduct security analyses of an organization's software testing process for industrial automation software in a semi-automated manner.

Generic Software Testing Process as the Target of Inspection

- Investigated state of practice
- Performed unstructured interviews with employees of an Austrian-based systems integrator to design a generic testing process
- Reviewed the process together with a software quality consultancy
- Aligned the process to the ISO/IEC/IEEE 29119 [2] series of standards

Overview

- Framework supports the VDI/VDE 2182 [7] guideline
- Ontological modeling approach
- Flexible assessment (scope)
- Combination of STRIDE [6] and attack–defense trees (ADTrees) [4]
- Automated generation of ADTrees
- Open-source prototype: `https://github.com/sbaresearch/adtgenerator`

Security Modeling Approach

- STRIDE: 6 categories of security threats used to build threat trees [6] that are included in the knowledge base
- ADTrees [4]: Attack trees extended by defense measures
- Description and formalization of various threat scenarios
- Automated generation of ADTrees, which can be imported into ADTool [3]
- Development of SPARQL queries to extract valuable security information from knowledge base (e.g., STRIDE threats to assets)

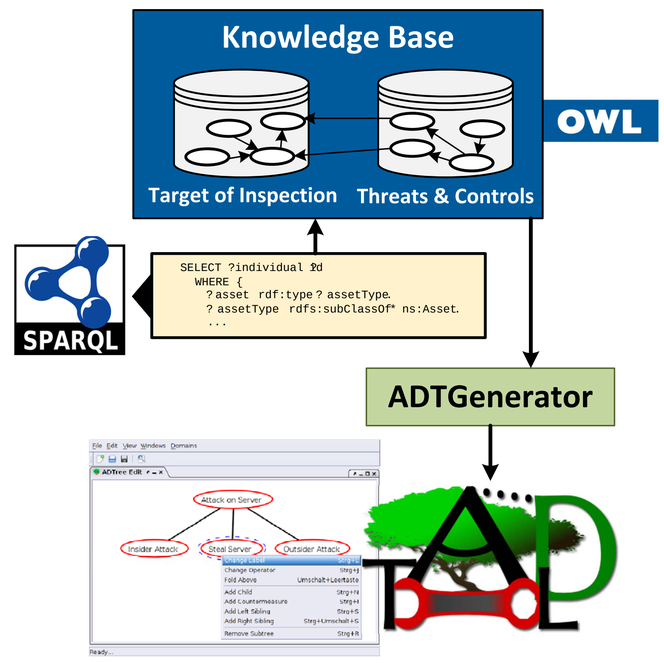

Figure 2: High-level overview of analyzing security risks in a semi-automated manner (ADTool illustrations taken from [3]).

Evaluation

- Two-step process: Tool selection step according to [5] and tool evaluation
- Considered 10 tools, two of which were extensively evaluated
- **Results:** Provides valuable support for security analyses, but needs to be improved to facilitate the structure analysis

Conclusion

- Designed a **generic software testing process for industrial automation applications** to define the target of inspection
- Proposed a framework that enables a **flexible, semi-automated security analyses**
- Adaptation to other engineering activities possible
- Developed a **prototype: ADTGenerator** (generation of ADTrees)
- SPARQL queries and ADTool [3] further support the analysis

Outlook

- **Automating risk identification** based on engineering data
- **Security modeling** extension for AutomationML (AMLsec)
- Detection of **vulnerabilities in plant structure** (e.g., attack graph generation), **consequences** of potential attacks, **business impact** analysis
- **Dynamic security risk analysis** methods for CPSs
- **Digital-twin-based attack simulation** for risk analysis

[1] M. Eckhart, K. Meixner, D. Winkler, and A. Ekelhart. Securing the testing process for industrial automation software. *Computers & Security*, 85:156 – 180, 2019.
[2] ISO/IEC/IEEE 29119-1. Software and systems engineering – software testing – part 1: Concepts and definitions, 2013.
[3] B. Kordy, P. Kordy, S. Mauw, and P. Schweitzer. ADTool: Security analysis with attack–defense trees. In K. Joshi, M. Siegle, M. Stoelinga, and P. R. D'Argenio, editors, *Quantitative Evaluation of Systems*, pages 173–176, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.
[4] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer. Foundations of attack–defense trees. In P. Degano, S. Etalle, and J. Guttman, editors, *Formal Aspects of Security and Trust*, pages 80–95, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.
[5] R. M. Poston and M. P. Sexton. Evaluating and selecting testing tools. *IEEE Software*, 9(3):33–42, May 1992.
[6] A. Shostack. *Threat Modeling: Designing for Security*. Wiley Publishing, 1st edition, 2014.
[7] VDI/VDE 2182-1. Sheet 1: IT-security for industrial automation - general model, 2011.

This research was further funded by the FFG under the industrial PhD program (grant no. 874644). Moreover, the financial support by the Christian Doppler Research Association, the Austrian Federal Ministry for Digital and Economic Affairs and the National Foundation for Research, Technology and Development is gratefully acknowledged.

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.