Automated Security Risk Identification Based on Engineering Data

Matthias Eckhart, Andreas Ekelhart, Edgar Weippl

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

SBA Research

Background & Motivation

Security by Design for Industry 4.0

Security risk management efforts are vital for adopting a security-enhanced engineering process for cyber-physical systems [4], as security risks need to be addressed in a cost-effective manner.

This requires:

- Integration of security aspects in digitized engineering workflows
- Utilization of existing engineering know-how
- Adoption of the IEC 62443-3-2 [6] for security risk assessments
- Methods to efficiently identify risk sources and attack consequences

Problems

- Existing engineering data formats, such as AutomationML [2], lack semantic modeling concepts for expressing security know-how
- Carrying out security risk assessments according to IEC 62443-3-2 [6] is complex and effortful since tool support is missing
- Identifying and understanding relationships among the detected security risks is difficult [3]

Need: Method that automatically identifies security weaknesses based on engineering data and visualizes their cyber-physical relevance.

Automated Risk Identification Method

Contribution [5]: Provide a method for the automated identification of security risks based on AutomationML engineering artifacts and visualization of threats by means of cyber-physical attack graphs (CPAGs).

Overview

- Risk identification method follows the IEC 62443-3-2 [6]
- Introduction of a security modeling concept named *AMLsec* for the adequate representation of the cyber-physical systems' security properties in AutomationML [2] artifacts
- Knowledge-based approach
- Novel variant of attack graphs that systems integrators can apply to gain insights into possible multistage cyber-physical attacks
- Open-source prototype: `https://github.com/sbaresearch/amlsec`

Ontological Security Modeling

- Engineering knowledge present in AutomationML artifact is transformed to OWL
- Conceptual mapping via AutomationML libraries
- Data validation checks via reasoners and SHACL constraints
- ICS security ontology and SHACL shapes comprise security know-how
- Knowledge is interlinked with data from public sources (e.g., CVEs)

Automated Risk Identification

- Based on a combination of SPARQL queries and SHACL constraints
- SPARQL queries check whether zone and conduit requirements as per the IEC 62443-3-2 [6] are met
- Validation rules expose insecure components and configurations
- Interlinked knowledge graph (e.g., CVEs) reveals known vulnerabilities
- Attack consequences are identified by interpreting the semantics of plant components and associating them to assets that are at risk

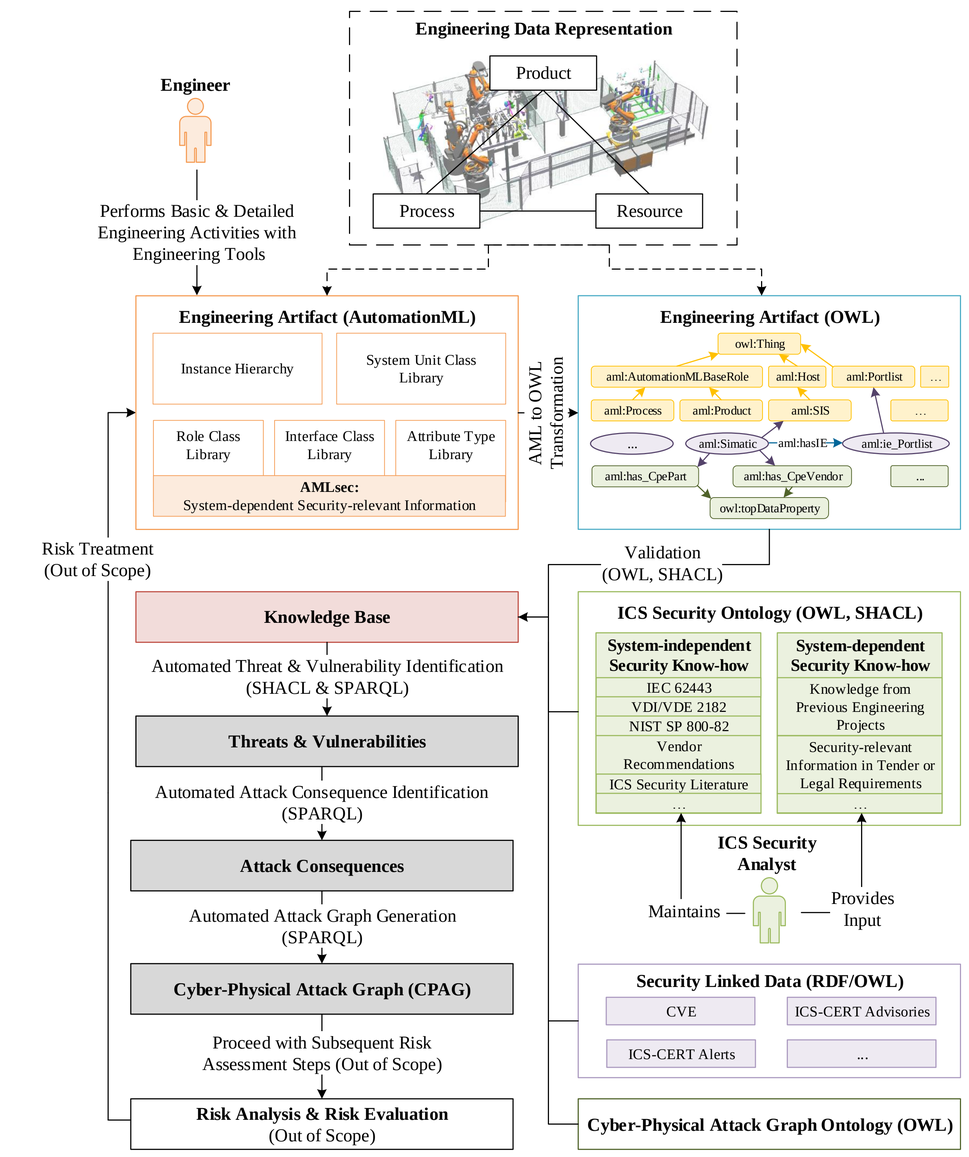

Figure 1: Overview of our AutomationML-based risk identification method (robot cell illustration taken from [1]).

Cyber-Physical Attack Graphs

A cyber-physical attack graph (CPAG) is a directed vertex- and edge-weighted graph $\boldsymbol{CPAG} = (\boldsymbol{V}, \boldsymbol{E}, \omega_{\boldsymbol{V}}, \omega_{\boldsymbol{E}})$, where $\boldsymbol{V}$ is the finite vertex set of assets, $\boldsymbol{E}$ is a multiset of directed edges from $\boldsymbol{V} \times \boldsymbol{V}$ representing vulnerabilities, $\omega_{\boldsymbol{V}}\colon\ \boldsymbol{V} \rightarrow \boldsymbol{S}$ is the vertex weight function that maps all vertices according to the assets' cyber-physical criticality onto the set $\boldsymbol{S}$, $\omega_{\boldsymbol{E}}\colon\ \boldsymbol{E} \multimap \boldsymbol{S}$ is the edge weight function that maps all edges according to the vulnerabilities' severity onto the set $\boldsymbol{S}$, and $\boldsymbol{S} = [0, 10]$.

CPAGs can be automatically generated by means of a SPARQL query. Subsequent pruning increases the utility and usability of CPAGs.

Conclusion & Outlook

- Method fosters a security-by-design engineering process
- Automated identification of risk sources and attack consequences
- Introduction of security concepts for AutomationML (AMLsec)
- Method seamlessly integrates into the engineering workflow
- CPAGs visualize potential multistage cyber-physical attacks that exploit the weaknesses identified in engineering data
- Open-source prototypical implementation of our method exists
- Incorporating COLLADA and PLCOpen XML is worthwhile
- Quantitative analysis capabilities will be added in the future

[1] AutomationML. AutomationML example: Robot cell. Technical report, March 2017.
[2] R. Drath, A. Luder, J. Peschke, and L. Hundt. AutomationML - the glue for seamless automation engineering. In *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, pages 616–623, Sept 2008.
[3] M. Eckhart, B. Brenner, A. Ekelhart, and E. Weippl. Quantitative security risk assessment for industrial control systems: Research opportunities and challenges. *Journal of Internet Services and Information Security (JISIS)*, 9(3):52–73, August 2019.
[4] M. Eckhart, A. Ekelhart, A. Lüder, S. Biffl, and E. Weippl. Security development lifecycle for cyber-physical production systems. In *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*, volume 1, pages 3004–3011, Oct 2019.
[5] M. Eckhart, A. Ekelhart, and E. Weippl. Automated security risk identification based on engineering data (in review). 2020.
[6] IEC. 62443-3-2: Security for industrial automation and control systems – part 3-2: Security risk assessment and system design. *International Standard, Draft, International Electrotechnical Commission, Geneva*, 1, 2018.

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
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.