Co-engineering of security and safety life-cycles for engineering security-informed safety-critical automotive systems in compliance with SAE J3061 and ISO 26262

Barbara Gallina and Muhammad Atif Javed, Mälardalen University, Västerås, Sweden
Helmut Martin and Robert Bramberger, Virtual Vehicle Research Center, Graz, Austria

Automotive systems are becoming more and more connected. As a consequence, (cyber)security is paramount for safety and co-engineering of (cyber)security and safety life-cycles becomes fundamental to be ready for the engineering of security-informed safety-critical systems. Currently, no standard provides a co-engineering process. ISO 26262 [1] provides a standardized safety life-cycle, which needs to be complemented by requirements stemming from security standards (e.g., the upcoming security standard ISO-SAE 21434 [14]) and/or guidelines (e.g., SAE J3061 [2]). SAE J3061 is the only published guidebook that provides suggestions for considering both concerns.

The co-engineering of safety and security life-cycles and more broadly the co-engineering of multi mono-concern life-cycles, separately proposed in standards targeting mono-concerns, can be facilitated by the explicit systematization and management of commonalities and variabilities, implicitly stated in the requirements of the different standards.

Security-informed Safety-oriented Process Line Engineering (SiSoPLE) [3] represents and extension of SoPLE, Safety-oriented Process Line Engineering [3]. Similar to SoPLE, SiSoPLE consists of a two-phase method for engineering families of safety life-cycles/processes. The first phase is aimed at engineering the domain from a process perspective i.e., identifying and systematizing process-related commonalities and variabilities, focusing on SiS (Security-informed Safety)-related commonalities and variabilities, in order to concurrently engineer a set of processes. The second phase is aimed at deriving single processes via selection and composition of commonalities and variabilities. From a tooling perspective, SiSoPLE as well as SoPLE can be supported by the integration between Eclipse Process Framework (EPF) Composer [8], recently re-brought to life [11], and Base Variability Resolution (BVR) Tool [15]. This integration was qualitatively evaluated as promising in [6]. To make the abstract self-contained, we recall that EPF Composer permits users to engineer processes in compliance with a SPEM (Software & Systems Process Engineering Metamodel) 2.0-like language [7], while BVR Tool permits users to orthogonally manage variability in compliance with the BVR [13] language. The integration between EPF Composer and BVR Tool for enabling the variability management at process level is hosted by OpenCert [16].

In this presentation, we point out our process for co-engineering security and safety life-cycles aligned with the SAE J3061 guidelines. This process exploits cross-concern commonalities and variabilities, which are systematized and managed via BVR Tool, integrated with EPF Composer.

Figure 1 shows a high-level view of the overall workflow of the proposed co-engineering process.

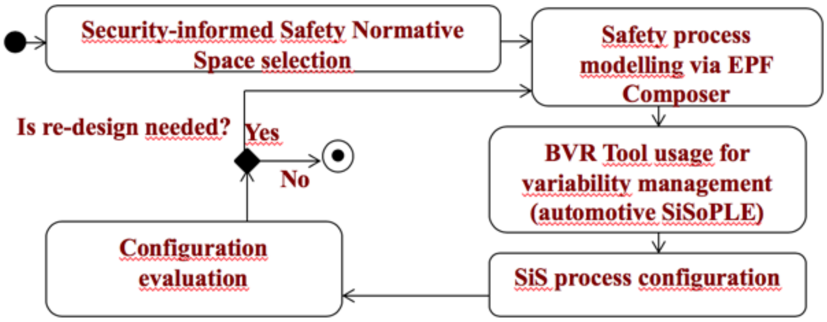
Security-informed Safety Normative Space selection
Safety process modelling via EPF Composer
BVR Tool usage for variability management (automotive SiSoPLE)
SiS process configuration
Configuration evaluation
Is re-design needed?
Yes
No

Figure 1 Co-engineering of Security and Safety Life-cycles via Exploitation of Cross-concern Commonalities and Variabilities

Further, the presentation shows the usage of the proposed co-engineering process in the context of the automotive regulations comprising ISO 26262 and SAE J3061, focusing on the risk analysis phase, as initially done in [17], where the automotive Security-informed Safety terminological framework for retrieving the implicit commonalities was proposed. Both ISO 26262 and SAE J3061 recommend the usage of specific methods for conducting the risk analysis phase. More specifically, ISO 26262 recommends HARA (Hazards Analyses and Risk Assessment) for safety; while SAE J3061 recommends TARA (Threat Analysis and Risk Assessment) for security-related analysis.

Process variability is managed based on parameters for safety, i.e. ASIL, and security, i.e. Security risk level (SecRL), which influence selection/inclusion of Safety and Security Activities. For example, an ASIL B process only requires deductive analysis e.g. FMEA (Failure Mode and Effect Analysis) for the verification of the safety concept, where ASIL D requires deductive and inductive analysis e.g. FTA (Fault Tree Analysis). With the help of the BVR tool the process can be tailored based on specified parameters. The tailoring activity deals with safety and security aspects and includes the specification of their dependencies.

The presentation will illustrate the co-engineering workflow (see Figure 1) by using the AMASS toolchain in a use case, which deals with verification of the system design of a car2x communication management unit. Safety and security concerns will be properly tailored via BVR Tool. The presentation aims at illustrating the importance of explicitly systematizing commonalities and variabilities for co-engineering the life-cycles needed for engineering multi-concern-critical systems.

This work is partially supported by the AMASS project [9], whose main objectives were presented in [10] and the SECREDAS project [18].

References

[1] ISO26262. Road vehicles – Functional safety. International Standard, November 2011.

[2] SAE J3061- Cybersecurity Guidebook for Cyber-Physical Automotive Systems. SAE - Society of Automotive Engineers.

[3] B. Gallina, L. Fabre. (2015, September). Benefits of security-informed safety-oriented process line engineering. In Digital Avionics Systems Conference (DASC), IEEE/AIAA 34th (pp. 8C1-1), IEEE, 2015.

[4] B. Gallina, I. Sljivo, O. Jaradat. Towards a Safety-oriented Process Line for Enabling Reuse in Safety Critical Systems Development and Certification. Post-proceedings of the 35th IEEE Software Engineering Workshop (SEW-35), 2012.

[5] B. Gallina, S. Kashiyarandi, H. Martin, R. Bramberger. (2014, July). Modeling a safety-and automotive-oriented process line to enable reuse and flexible process derivation. In Computer Software and Applications Conference Workshops (COMPSACW), IEEE 38th International (pp. 504-509), 2014.

[6] I. Ayala, B. Gallina. Towards Tool-based Security-informed Safety Oriented Process Line Engineering. 1st ACM International workshop on Interplay of Security, Safety and System/Software Architecture (ISSA), Copenhagen, Denmark, November 28th, 2016.

[7] OMG. Software & systems Process Engineering Meta-model (SPEM), v 2.0. Full Specification formal/08-04-01, Object Management Group, 2008.

[8] Eclipse Process Framework http://www.eclipse.org/epf/.

[9] AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems), http://www.amass- ecsel.eu.

[10] Ruiz A., Gallina B., de la Vara J. L., Mazzini S. and Espinoza H., "Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems", 5th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems (SASSUR), Trondheim, September 2016.

[11] Javed, M. A. and Gallina, B. (2018a). Get epf composer back to the future: A trip from Galileo to Photon after 11 years. In EclipseCon, Toulouse, France, JUNE 13-14, 2018.

[12] M. A. Javed and B. Gallina. Safety-oriented Process Line Engineering via Seamless Integration between EPF Composer and BVR Tool. In 22nd International Systems and Software Product Line Conference (SPLC), Sept 10-14, Gothenburg, Sweden, in press. ACM Digital Library, 2018.

[13] VARIES D4.2- BVR - The language. http://bvr.modelbased.net/docs/VARIES_D4.2_v01_PP_FINAL.pdf

[14] ISO-SAE 21434 Road vehicles –Cybersecurity Engineering- General Overview. https://www.iso.org/standard/70918.html

[15] BVR Tool. https://github.com/SINTEF-9012/bvr

[16] OpenCert- hosting the AMASS platform. https://www.polarsys.org/opencert/about/

[17] Castellanos Ardila, J., Gallina, B.: Towards Efficiently Checking Compliance Against Automotive Security and Safety Standards. In: The 7th IEEE International Workshop on Software Certification., Toulouse, France, 2017.

[18] SECREDAS (Product Security for Cross Domain Reliable Dependable Automated Systems), http://secredas.eu/