VIENNA 2018 TRA
TRANSPORT RESEARCH ARENA
A digital era for transport
solutions for society, economy and environment

Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, 2018, Vienna, Austria

Increasing and Validating the Safety and Reliability of Cyber-Physical Systems

Johannes Pribyl a, Willibald Krenn a*

[a]*AIT Austrian Institute of Technology, Giefinggasse 4, 1210 Vienna, Austria*

Abstract

Cyber-physical systems (CPS) like production facilities, medical devices, and modern cars play an increasingly significant role in the economic context but also in every-day life; catchphrases like “Industry 4.0” and “Mobility of the Future” are on everybody’s mind. Manufacturers and operators of such systems are highly interested in investigating and ensuring the safety and reliability of their systems.

The security researchers of AIT Austrian Institute of Technology’s research field “Dependable Systems Engineering” (DSE) deal with the challenge of increasing the safety and reliability of cyber-physical systems since many years. The team actively engages interesting problems in both, the scientific - and production domains together with key industry partners. In this way, they not only drive scientific progress in their field of study but also keep their eyes on the practical applicability of their solutions.

With this goal in mind, the DSE’s researchers and engineers develop tools and methodologies to address questions regarding Safe and Secure Co-Engineering. Examples include safe and secure reference architectures; methods for model-based analysis of safety-critical systems; automated test case generation; and real-time monitoring of complex systems. The group’s experts also contribute to the development of industry standards, e.g., ISO26262.

Keywords: cyber-physical systems; safety and security; verification and validation; dependable systems engineering; model-based; automated test case generation; real-time monitoring

* Corresponding author. Tel.: +43-664-8251222; fax: +43-50550-4150.
E-mail address: willibald.krenn@ait.ac.at

Nomenclature

V&V	Verification and Validation
CPS	Cyber-Physical Systems
FMVEA	Failure Mode, Vulnerabilities and Effects Analysis
STPA	Systems Theoretic Process Analysis
WEFACT	Workflow Engine for Analysis, Certification and Test
DuT	Device under Test

1. Introduction and Motivation

In today's interconnected world, there are several trends which render it imperative to work on methods for the verification and validation of highly reliable systems:

- With growing complexity, modern systems incorporate a multitude of dependencies between different modules within the system and between different systems. This leads to unforeseeable possible interactions which are impossible to check using manual V&V alone.

- Additionally, CPS are assigned tasks in critical environments involving more and more responsibility; the examples of autonomous industrial collaborative applications and autonomous vehicles come to mind.

- With emerging trends such as Industry 4.0 or the Internet of Things, CPS are mostly integrated into some form of data network. In the case of a security incident in such a network, the safety of the complete system cannot be guaranteed. Therefore, technical solutions have reached a level of complexity where safety cannot be addressed without considering the system's security as well (Schmittner et al. 2017).

Researchers at the AIT Austrian Institute of Technology are developing techniques and methodologies to deal with these challenges. This paper provides an overview of these activities and links to further information.

2. Design of Cyber-Physical Systems

2.1. Safety and Security Co-Engineering

Using state-of-the-art analysis knowledge, AIT's researchers created methods like FMVEA (Schmittner et al. 2015) and extended others, like STPA for analysing systems during the concept phase. Based on these achievements, analysts and consultants at AIT developed devices and tools for ensuring safe and secure systems, e.g., their Safe and Secure Gateway for allowing non-secure production machines to be included in a modern Industry 4.0 context. The Secure Gateway offers a customisable, restricted set of services, which minimizes the potential attack surface. Based on a framework of services like remote monitoring or remote update, the system is configurable to the specific needs. Furthermore, it can be adapted to the system to which it is applied to and to the intended use case. The Secure Gateway aims at embedded devices without continuous connection to infrastructure or even power supply. The system is running on a low-power, secured ARM platform which is placed between the system and the outside network. The framework of services consists not only of a set of software for the gateway, but also secured applications for the human user, enabling a secured end-to-end connectivity and gateway control.

2.2. Standards-based Workflow

One of the core competences of AIT's Dependable System Engineering group is working with standardization bodies in complex automation systems, robotics and automotive. Based on this expertise, DSE provides certification support of dependable and reliable systems. Several tools are available for guidance, validation and verification, e.g., a V&V-workflow tool (Schmittner, Althammer, Gruber 2015). The tool is adaptable to different standards and guides the user through a systematic development process that conforms to the chosen standard. In the end, the tool also produces the necessary documentation, e.g., safety cases. It has the potential to significantly simplify following a standard-conformant system development process, especially when a company does not have access to lots of highly trained safety/security experts and needs to follow the standards nevertheless. The tool

interacts with different, industry standard requirements management tools, e.g., DOORS, and can automatically trigger V&V activities through automation, e.g., using OSLC.
For IEC62443 compliant development, the group offers an extension for modelling network designs and automatically assigning security requirements to the network components, based on the requirements of the standard.

2.3. Threat Modelling

One method of assessing possible safety and security vulnerabilities of a given system is to perform a threat analysis. Threat modelling is a current methodology for analyzing threats with several tools readily available. Using these tools, AIT researchers have successfully applied threat modelling to domains like the automotive domain. AIT has produced its own Automotive Threat Library that enables systematic automotive cyber security engineering and is applying the tool in customer projects.

3. Verification and Validation of Cyber-Physical Systems

3.1. Automated, Fault-based Test Case Generation

Software has become an integral part of most technical systems and often is the major contributor of value. The big challenge manufacturers of all industries are facing is to make software code as safe and fault free as possible as software is more prevalent, but also more complex and more critical than ever before. Accepting this challenge turns out to be more difficult than commonly assumed because average code will contain 15 to 50 faults per 1000 lines delivered as today. A premium-class vehicle for example will contain upwards of 100 million lines of software code.
To mitigate the threat posed by low software quality to business, software testing is generally applied and will improve the error rate considerably. Keeping the increasing product complexity in mind, automated and model-based software testing is of inevitable value. Not only will automation help counter balancing the ever-increasing size of software systems but it will also generate a "proper set" of test cases that guarantees a certain (selectable) test coverage over the given specification that would be difficult and very expensive to attain with manual testing. Addressing this challenge, DSE has developed the automated test case generator MoMuT[†] (Fellner et al. 2017). At heart it is an efficient, fault-based test case generation tool. It will take a behaviour model of a DuT and support development in unit, integration, system and acceptance testing of functional as well as non-functional aspects. In difference to many other tools, MoMuT generates fault-based test cases. This means the tool automatically computes test cases that are guaranteed to check for the absence of (certain) faults. This approach is more powerful than checking for some control-flow or data-flow coverage. In its standard configuration, the tool comes with a set of common faults pre-defined, however, this set remains customizable. Apart from automated test design MoMuT can also provide feedback about the quality of pre-existing test suites, and extend a given test suite to achieve full fault coverage (Krenn et al. 2015).

3.2. Runtime Verification

Since testing never can find all bugs, runtime verification (Havelund et al. 2002) can be used to increase a system's safety and security during execution. It is a lightweight yet powerful formal technique used to check whether the current execution of a system satisfies or violates a property of interest. This technique differs from the more expensive model checking (Clarke et al. 1977) that aims instead to verify exhaustively property correctness for all the possible program behaviours. Monitoring is generally used when the system model is too big to handle with model checking due to the state explosion problem, or when the system model is not available (black-box with observable input/output interface). Furthermore, runtime verification can also be used to trigger some system recovery actions when a safety property is violated. AIT's experts have produced monitoring solutions (Selyunin et al. 2017) that check for property-violation/non-violation as well as robustness in real time or off line. The technology is especially useful in an analogue mixed signal setting, and helps the verification engineer not to miss bugs in the system design. It can check for complex interdependencies between signals over time. AIT's runtime verification technology has already been applied to industrial use cases.

[†] https://www.momut.org

3.3. Machine Code Analysis

Running any third-party software requires trust in the software supplier. Malicious or negligent suppliers could have added hidden functionality (Papp et al. 2017) that could endanger the systems safety and security, or could have delivered a product full of systematic weaknesses that an attacker can exploit. Especially when dealing with software that uses cryptographic algorithms it is important to check whether there are no such hidden weaknesses. Techniques like penetration testing, fuzzing, etc. help to reduce the risks involved; however, to gain the highest level of confidence in the software, investment in manual analysis is necessary. This is an expensive and time-consuming process, often carried out on the machine code level, as the source code of the software usually is not available. Therefore, AIT's researchers developed the Machine-Code Analyzer, a tool to help with this analysis. It can point out program-locations in need of further inspection and program-locations without this need.
AIT's Machine Code Analyzer takes an application and a set of machine-readable requirements as inputs. It runs the application and watches the execution. It looks at the dataflow inside the application, at the use of memory locations, and generally monitors the control flow coverage and checks whether the application meets the requirements specified. This way it can point out potentially unsafe instructions, information leaks, and other critical issues. In addition to this, the tool will automatically create new program inputs so that the next run of the application will go down paths in the control flow graph that have never been taken before. This way, the tool is able to discover functionality hidden in the application, triggered with special inputs only.

4. Conclusion

The tools and methodologies developed by AIT's Dependable Systems Engineering experts support the user in both, the system design as well as the system verification phases with innovative solutions. The experts also consult companies introducing new or updated standards, e.g., ISO26262, IEC62443, or related standards and have amassed the experience of more than 20 years of safety-critical software maintenance. Their scientific work regularly is published in peer-reviewed conference proceedings or journals and often evaluated on industrial use cases. Together with their partners, they strive to improve and automate the design and validation of dependable cyber-physical systems. Current results have been pointed to in this article[‡].

5. References

K. Havelund and G. Rosu, "Preface (Runtime Verification)," Electron. Notes Theor. Comput. Sci., vol. 70, no. 4, pp. 201–202, Dec. 2002.

E. M. Clarke and E. A. Emerson, "Design and synthesis of synchronization skeletons using branching time temporal logic," in Logics of Programs, vol. 131, D. Kozen, Ed. Berlin/Heidelberg: Springer-Verlag, pp. 52–71.

A. Pnueli, "The temporal logic of programs," 1977, pp. 46–57.

Andreas Fellner, Willibald Krenn, Rupert Schlick, Thorsten Tarrach, Georg Weissenbacher: Model-based, mutation-driven test case generation via heuristic-guided branching search. MEMOCODE 2017: 56-66

Willibald Krenn, Rupert Schlick, Stefan Tiran, Bernhard K. Aichernig, Elisabeth Jöbstl, Harald Brandl: MoMut: : UML Model-Based Mutation Testing for UML. ICST 2015: 1-8

Konstantin Selyunin, Stefan Jaksic, Thang Nguyen, Christian Reidl, Udo Hafner, Ezio Bartocci, Dejan Nickovic, Radu Grosu: Runtime Monitoring with Recovery of the SENT Communication Protocol. CAV (1) 2017: 336-355

Christoph Schmittner, Zhendong Ma, Thomas Gruber, Erwin Schoitsch: Safety and Security Co-engineering of Connected, Intelligent, and Automated Vehicles. ERCIM News 2017(109) (2017)

Christoph Schmittner, Zhendong Ma, Erwin Schoitsch, Thomas Gruber: A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive Cyber-Physical Systems. CPSS@ASIACSS 2015: 69-80

Christoph Schmittner, Egbert Althammer, Thomas Gruber: Workflow Engine for Analysis, Certification and Test of Safety and Security-Critical Systems. ERCIM News 2015(102) (2015)

Dorottya Papp, Levente Buttyán, Zhendong Ma: Towards Semi-automated Detection of Trigger-based Behavior for Software Security Assurance. ARES 2017: 64:1-64:6

[‡] For more information, please visit https://www.ait.ac.at/en/research-fields/dependable-systems-engineering/