AUSTRIAN INSTITUTE OF TECHNOLOGY

Dependable Systems Engineering

CENTER FOR DIGITAL SAFETY & SECURITY

STANDARDIZATION

One of the core competences of the Dependable Systems Engineering (DSE) research group at the AIT Austrian Institute of Technology is working with standardization bodies in the area of 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. the WEFACT[1] V&V-workflow support tool. Furthermore, DSE is involved in the development of a Safe and Secure Reference Architecture for ensuring easier development of safe and secure systems.

SAFE AND SECURE CO-ENGINEERING

Safety and Security are of critical importance when it comes to complex, networked systems. Nowadays, technical solutions have reached a level of complexity where safety cannot be addressed without considering the system's security as well. Researchers at AIT developed several techniques to deal with this situation:

SAFETY AND SECURITY CO-ANALYSIS

Using state-of-the-art analysis knowledge, AIT's researchers created methods like FMVEA[2] and extended others, like STPA[3], for analyzing systems during the concept phase. Based on these achievements, analysts and consultants at AIT developed 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.

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.

VERIFICATION AND VALIDATION

Software has become an integral part of most technical systems and often is the major contributor of value. The big challenge manufacturers are facing is to make this code as safe and fault free as possible. The DSE group is accepting this challenge by developing new methods, tools or process approaches for the verification and validation of highly reliable and safety critical software and systems in the fields of embedded or cyber-physical systems.

AUTOMATIC TEST CASE GENERATION

To ensure high software quality, software testing is generally applied and – when done correctly – improves the error rate considerably. Keeping the increasing product complexity in mind, automated and model-based software testing is of inevitable value. MoMuT[4], a tool developed at DSE, uses automatic and mutation-based test case generation methods.

MONITORING

Despite the most sophisticated testing methods, a complete system test is sometimes not feasible. In these cases, real-time system monitoring is a valid alternative for ensuring correct system behavior. Together with industry partners, DSE is working on several tools for this purpose; additionally, research concerning predictive monitoring is done at DSE.

BINARY AND STATIC CODE ANALYSIS

In addition to the methods presented above, AIT's DSE is working on methods and tools to directly analyze compiled program code. This includes checking for adherence to system requirements, and automated generation of test data to achieve branch coverage on machine code level.

The binary code analysis allows for the semi-automated detection of systematic weaknesses in, e.g., cryptographic code.

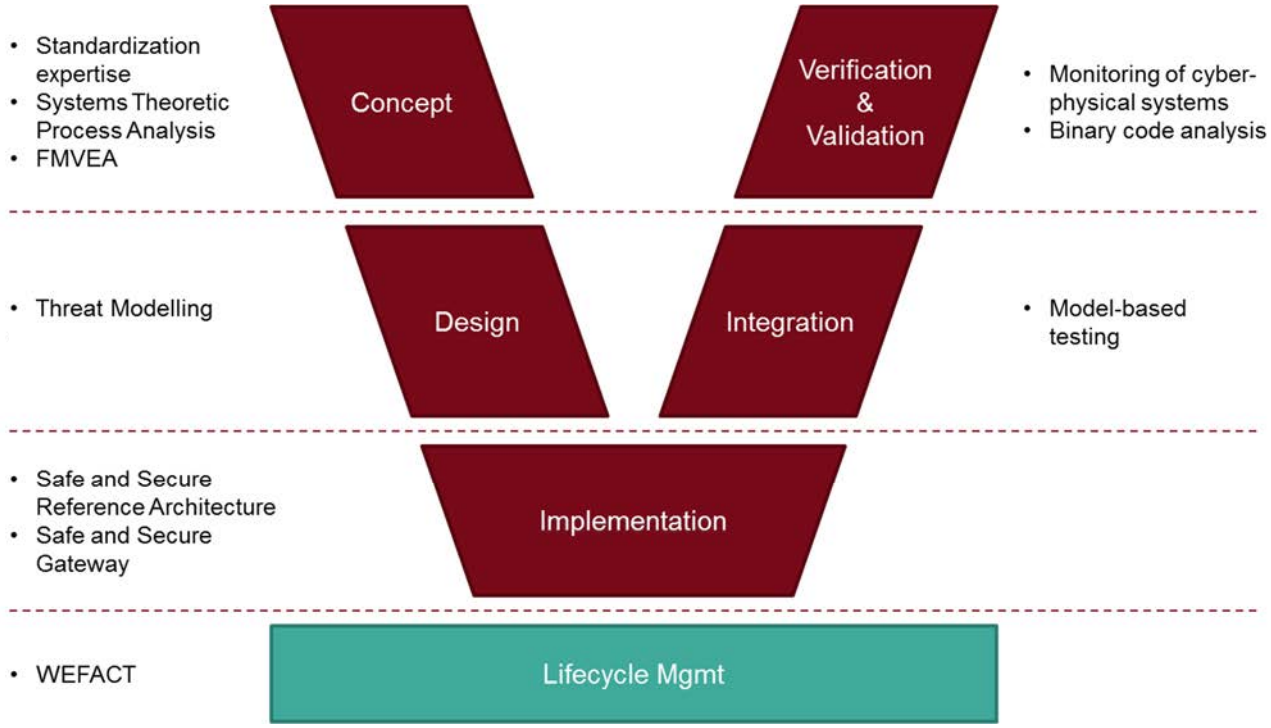
---

[1] Workflow Engine for Analysis, Certification and Test

[2] Failure Mode, Vulnerabilities and Effects Analysis

[3] Systems Theoretic Process Analysis

[4] Model-based Mutation Testing



The Dependable Systems Engineering research group at the AIT Austrian Institute of Technology has a systematic understanding of the development process of safety-critical and dependable systems. The group's expertise ranges from developing new standards, over providing workflow support, to verification & validation activities like testing and runtime verification.

CONTACT

AIT Austrian Institute of Technology
Center for Digital Safety & Security
Giefinggasse 4, 1210 Vienna

DR. WILLIBALD KRENN
Thematic Coordinator
Dependable Systems Engineering
Center for Digital Safety & Security

AIT Austrian Institute of Technology GmbH
Giefinggasse 4 | 1210 Wien, Austria
T +43 50550-4109 | M +43 664 8251222
willibald.krenn@ait.ac.at | www.ait.ac.at