Volume 1, Issue 4

20.4.2016

MERgE Consortium

MERgE News

MERGE SAFETY & SECURITY

MERgE: Multi-Concerns Interactions System Engineering

From the Project Coordinator's Pen

This is the fourth and last newsletter about the project MERgE. Inside we discuss some of the open challenges as well as how we have advanced some of the technologies for treating safety and security concerns. Some interesting collaborations to integrate technologies are also described. As is now traditional we present one of our demonstrators in each newsletter, in this particular issue we focus on the industrial control demonstrator. The market relevance of safety-security co-engineering is rapidly increasing across all use case domains, driven especially by communication and device connectedness. As an example, a Frost & Sullivan report[1] predicts that 85% of cars manufactured in 2020 will have access to the internet.

Thanks for your interest,

Charles Robinson

Thales Research & Technology

Plenary in Paris

The 9th plenary meeting took place at Paris (UPMC) 25th-27th November 2016. The focus was on workshops to tackle the latest challenges within tasks and planning for the remainder of the project. Global work package aspects were addressed on the final day.

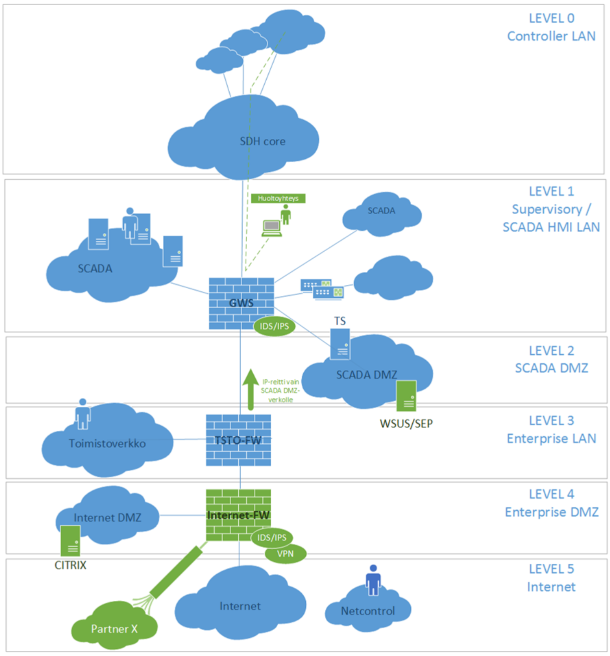
The invited guest speaker was Dr. Ziadi who presented his work on model variants for Software Production Lines. A particular focus was on their tool (Bottom-up Technologies for Reuse) that can be used for analysing software artefacts, such as to extract commonalities and variations, identify features, or discover structural or semantic constraints. Reverse engineering is one application, for instance aiding a company recover missing functional knowledge of legacy code.

Some challenges discussed at the Plenary are common with research technology. Tied with the de-risking TRL levels, sometimes called the valley of doom, tools traverse these levels to achieve sufficient maturity for confident industrial and commercial use. Bugs at this point should be few and far between for general functions. However, even a technology that works well needs efficient training mechanisms in place and support for user queries. Some constraints that SMEs face for technology uptake can only be relieved by large organisations or standards bodies. This is particularly a case with engineering technology used in large–scale projects with many partners. For instance, partitioned procurement approaches can be a hurdle to overcome - a commonality across our use case domains, but particularly for Industrial Control and Space. Also how do we get companies across industry to describe their resources with sufficient formalisation of processes to fully harness the capability of some tools (projects for the industrial internet of things should help here). Another challenge included determining the right levels of abstraction when introducing MDE for safety/security.

[1] Automotive and Transportation Technology--Cybersecurity Technology, March 2016

Industrial Control System Demonstrator

The Industrial Control Systems (ICS) use case is driven by the lack of suitable test environments in the EU that enable information security teams to assess the security of ICS used in industrial sectors—particularly in critical infrastructure such as energy, transportation and the manufacturing segments. To address this gap, ICS specific services have been chosen as the demonstrator to align ISA99/ISA62433 based example architecture and partners' security expertise with the ICS companies' business and security needs. To avoid significant production disruptions in industrial environments, high availability is one of the critical factors for every ICS. Therefore it becomes apparent that any security assessment to be performed by security experts should not cause a risk for any disruptions in ICS environments (safety viewpoint). In addition to the testing laboratory environment, services developed in collaboration by the use case partners include lab based ICS security testing and training services as the demonstrator. It should be noted that the USA are also looking to strengthen themselves with ICS testing environments shown for example by a call for proposals to develop a reconfigurable ICS cyber-security testbed[2].



Within the context of this use case there was also exploration of 'technical debt' such as when different aspects are developed for a time before reconciliation; and exploration of improved capability for large-scale requirements engineering. Involved partners for these aspects included both academic and governmental organizations (University of Oulu, University of Jyväskylä, STUK), in addition to security and technology practitioners (Codenomicon, Pohto, nSense). nSense has developed further services utilizing the capabilities developed by the involved partners. Earlier this year they organised a private invitation-only security conference in Estonia for the third time. The audience consisted of decision makers and subject matter experts within cyber security. While a networking event by nature, the discussion is fostered by topical presentations – this time featuring also results from MERgE project where a senior nSense consultant presented a bypass technique developed against physical access control systems.

While physical ICS simulation and ICS security tools and business processes have been enhanced within MERgE, and are much in demand, the use case expertise was also used as an opportunity for exploring Model Driven Engineering (MDE). This style of system architecting and modelling of processes is only beginning to enter this domain. Obeo and UPMC in particular brought their competence in MDE to look at the value that may be brought here. It is believed significantly improved connectivity of safety/security could be achieved if MDE was used in this domain both for system design, but also for system operation and training. However ICS vendors have a lot of autonomy and lobbying is needed for large organisations and standards bodies to appreciate fully the benefits of MDE and call for wider usage.

Joint Co-engineering Workshop Between MERgE & SeSaMo

The 2nd International workshop on the Integration of Safety and Security Engineering (ISSE) was coordinated jointly between the projects MERgE (ITEA) and SeSaMo (Artemis). It follows on from the prior year and examined and discussed the latest developments. Thales and City University London introduced the work done in their respective projects. Topics were then spread across :

- Methods - A Combined Safety-Hazards and Security-Threat Analysis Method for Automotive Systems
- Approaches - Combining MILS with Contract-Based Design for Safety and Security Requirements
- Tools - Safety and Security Assessment of Behavioral Properties Using Alloy), and
- Techniques - Sequential and Parallel Attack Tree Modelling
- Perspectives - Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective

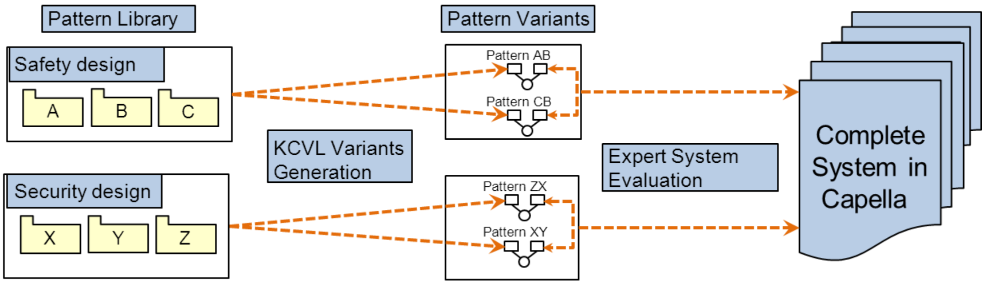
The co-engineering theme was also apparent in other workshops at the conference (related to systems of systems / system assurance) providing further indication of its importance at the current time.

[2]: http://www.securityweek.com/nist-testbed-measure-industrial-control-systems-under-cyberattack

Optimising System Architecture Generation

At the 19th International Conference on Software Product Line, Inria (France) presented a research paper describing collaboration with Thales Divisions in the context of the ITEA2 MERgE project. "The design of complex systems challenges engineers to deal with massive pieces of software (a typical contemporary car has about 100 million lines of code). A divide and conquer approach is usually employed, involving a multiplicity of stakeholders and expertise: each concern of the system is engineered separately through the use of several domain-specific languages and specialized tooling support". Thales employ the open source workbench Capella when architecting large-scale electronic systems. From the requirements to implementation many design decisions are taken based on expert experience. While strong solutions can be developed in this way, time resources limit the amount of possible configurations that may produce more optimal systems that satisfy the client, whilst respecting standards and reducing costs.

The purpose of the collaboration here has been to integrate three technology components that will aid the exploration of the solution space. Based on the Diff/Merge Pattern technology (Thales Global Services), parts of models can be linked with particular constraints (such as requirements) - these *patterns* can be extracted to a library. The technology KCVL (Inria) is an extension of the common variability language and provides the capability of selecting appropriate pattern combinations that may realize a particular solution. Finally, an architecture evaluation *expert system* (Thales R&T) assesses the choices and proposes the best candidate(s) to be integrated in the system structure.



Sirius - A Graphic Model is Worth a Thousand Words

As was noted in the last newsletter, the uptake of state-of-the-art technology by industry and especially SMEs is often a challenge. One of the roadblocks here, given the context, is the evident lack of expertise available on the market when recruiting. Mechanisms are needed to facilitate and maximize the efficiency of training programs. This can be extended more generally to one's ability to recruit new personnel and get them up to speed on company specific business processes or system design. Furthermore such mechanisms also help explaining to clients the significance of a company's offerings.

Model-driven engineering (MDE), although primarily for the architecting of systems and processes, also provides for the mechanisms mentioned above. For over the last decade MDE has been maturing in various domains. The workbench Sirius is a further evolution of the existing technology opening up the ability for particular tailoring of MDE for domain-specific or company-specific requirements. This is especially useful for the safety and security sectors given the diversity of problems and solutions for both system design and system operation.

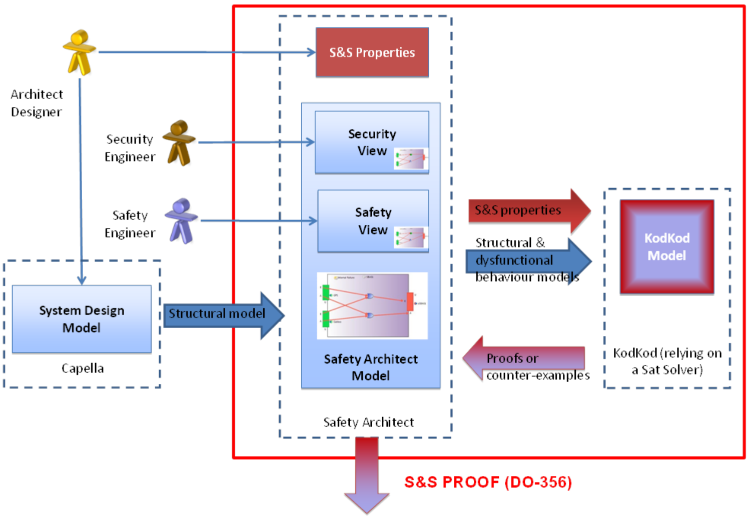
MERgE has contributed towards the development of Sirius with the technology being explored by the various use cases. Of particular interest are the advantages still to be unlocked in the industrial control domain which is new to the technology. Obeo (France) presented Sirius at EclipseCon in Germany in November 2015. Further details available at:

http://cedric.brun.io/eclipse/eclipsecon-europe-2015/

Further to this Sirius itself had a convention, Nebojša Taušan (Oulu) reports "As part of the MERgE research project, University of Oulu members participated in the SiriusCon conference that took place in Paris, France. Sirius is an open source and eclipse based technology that allows rapid development and customization of modelling workbench. SiriusCon gathered industry experts interested in this technology, Sirius committers and enthusiasts interested in this modelling technology. During the conference, participants had an opportunity to learn about industrial use-cases, to attend the tutorials and discuss with Sirius committers about future development initiatives. More details about the Sirius technology can be found following this link: https://eclipse.org/sirius/index.html

All4Tec Tool: Safety Architect - An MBSSA Approach Enhanced in MERgE

Model-based safety analysis is nowadays more and more considered in order to improve the safety analysis of complex systems. It relies on the idea that safety assessment activities can follow the design process in a parallel flow using the system functional and physical architectures as a common basis. Safety Architect is a tool achieving risk analysis of complex systems using functional or physical architectures. Safety Architect allows the user to automatically generate the Fault Tree through a local analysis of the architecture.



The Model-Based Safety/Security Analysis (MBSSA) approach enhanced in the MERgE project consists in adding a security view in Safety Architect and decoupling the system architecture model from safety & security models. This way, every engineer (be it an architect, a security or a safety engineer) can focus on her concerns solely, with dedicated tools and terminology. As of now, we chose to use two separate views: one for the safety concern and the second for the security concern. The main motivation for this separation is that safety and security domains are quite different in terms of practices, concepts used and wording. The tool chain developed for this purpose is the following: The system architecture model is built with Cappella (Thales) and then imported into Safety Architect (All4tec) to perform Safety and Security analyses. The results are translated into Alloy so that both safety and security properties can be verified with the Kodkod Analyser (SAT solver - Onera).

Thus the solution consists in 3 stages:

- A design layer where system architects design the system architecture and can verify its performances (thanks to "Capella");
- A safety/security layer where safety engineers/security engineers can model their safety/security behaviour and automatically generate failure trees/attack trees (thanks to "Safety Architect");
- A third layer which consists in a formal model (Alloy model) to assess safety and security properties of the system architecture.

MERgE Consortium

Follow
@MERgE_Project

Contact sanja.aaramaa@oulu.fi for more information about the articles above or potential joint dissemination activities.

Contact charles.robinson@ thalesgroup.com for other MERgE matters.

Check out
http://www.merge-project.eu/

Within the "Engineering support" theme of ITEA2 roadmap, the purpose of this project is to develop innovative concepts and design tools for multi-concern engineering when designing complex systems. The applicability and benefits of these innovations will be demonstrated in particular with "safety" and "security". Other concerns such as performance, reliability and traceability will also be considered. Four concrete use cases from different domains are provided as suitable test environments: radio communication, automotive, aerospace and industrial control.

MERGE
SAFETY & SECURITY

Multi-Concerns Interactions
Systems Engineering