Volume 1, Issue 2

6.3.2015

MERgE consortium

MERgE News

MERgE: Multi-Concerns Interactions System Engineering

From the Project Coordinator's Pen

Dear Reader, this second issue of our newsletter brings you more updates on the interesting activities taking place within the project MERgE. On this occasion out of the four demonstrators being developed we have a highlight on the Automotive scenario. You will also find articles on some of our recent advancements on system architecting and system protection. Model Driven Engineering has a strong presence within our project and particular domains. Outside these it is often viewed as purely for modelling of software and hardware. To prove this is not the case and showcase the adaptability of some of our tooling, one of our articles presents an agricultural scenario. MERgE has also just successfully passed its second ITEA review with flying colours. During the review encouraging feedback was provided on the collaboration and demonstrator advancement.

Thanks for your interest.

Charles Robinson
MERgE Project Coordinator

2nd ITEA Review and Consortium Meeting

Thales hosted the second ITEA review on December 2014. It was a great pleasure for the consortium to present the advances in each work package. The four industrial demonstrators had reached significant results, which were presented through videos and presentations. Note that we are presenting also at the ITEA-ARTEMIS co-summit. The consortium has also successfully disseminated the results according to the strategy. We will be reinforcing the links between dissemination and exploitation in 2015. The management requirements have been well addressed during the project.

In conjunction with the review UPMC hosted a two day consortium meeting. These focused on collaborative discussion sessions for the tasks and dealing with challenges. For instance: resolving differences in terminology; that reliability is not directly correlated with eliminating coding errors; different approaches for safety level (ASIL) management; improved revision methods for the MERgE platform. We also took into account the review feedback.

The MERgE consortium would like to thank the ITEA reviewers for their encouraging comments and the French hosts for their hospitality.

INSIDE THIS ISSUE:

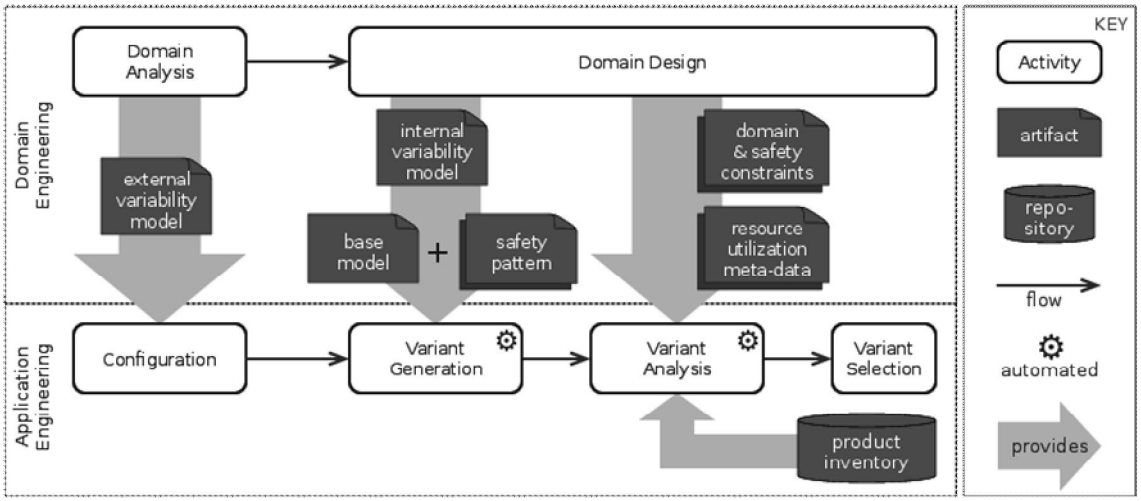
Automotive Demonstrator

The automotive demonstrator combines software product line engineering with model-driven generative design in the development of the Triaxis® Hall Effect Sensor. The Triaxis sensor handles angle calculation in a family of safety-critical automotive applications, ranging from a windshield wiper to a brake pedal.

Developing and maintaining a wide range of dedicated sensor product variants is costly in practice: rigorous safety assessment and verification of individual sensor product variant increases time-to-market, while the current hardware-software co-design approach complicates the necessary reuse efforts.

The solution proposed and illustrated in the demonstrator is a tailored software product line (SPL) approach that uses model-driven techniques and tools for deriving suitable sensor variants. The SPL approach consists of two phases. In the domain engineering phase, designers construct feature models, a reference architecture, a library of (safety) patterns, and many more reusable artefacts. In the application engineering phase, developers configure a variant by selecting the required features and the desired safety level using dedicated configuration tools. A set of candidate architectures is generated automatically - each involving slightly different engineering trade-offs - based on the reusable artefacts of phase one. A human expert uses architectural trade-off analysis to narrow the candidate set.

The demonstrator is the result of a joint effort between KU Leuven and E2S (Belgium), INRIA/IRISA and Thales (France), and practitioners of Melexis NV, a market leader in the development and production of Automotive Hall Effect Sensors.



Cyber Defenses for Critical Infrastructure with Robust Industrial Control Systems Planning and Evaluation (RIPE) Program

Digital technology, IT, and the Internet have revolutionized process and factory automation, and industrial production at large. Whether the anticipated benefits of this development will outweigh its inherent risk will depend on how well cyber security and fragility issues are addressed.

Convenience and comfort of modern cyber technologies come with a security risk, and this risk increases proportionally with networking and the degree you depend on it. Everything that can be monitored and re-configured comfortably via the network can be compromised as easily. The impact is then not restricted to isolated automation cells because more digital integration also means more dependencies, more potential sources of trouble, and more widespread consequence in the event of failure or compromise.

RIPE addresses the inherent shortcomings of digital technologies by providing a cyber security management system which includes cyber security capability measurements needed for system resilience and reliability.

The core of RIPE is not perfection but progress as defined in ISO/IEC 9000 series (PDCA – plan, do, check, act). Thus RIPE embodies the concept of continuous improvement as it is known from the field of quality management. The RIPE framework focuses on Industrial Control Systems and it is compliant with ISO/IEC 27001 based information security management system.

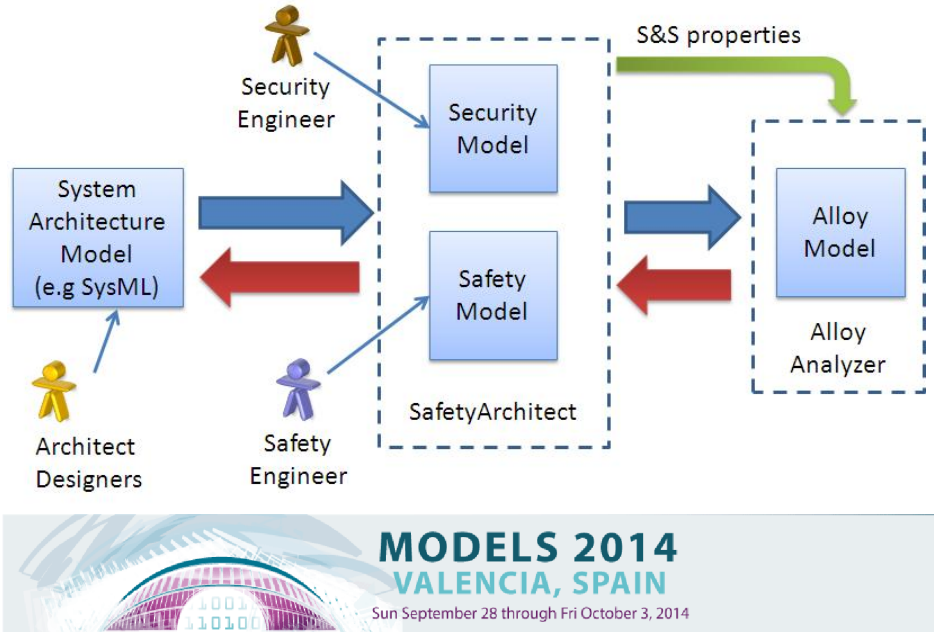
Contact the Langner Group (www.langner.com) for more information.

The Loviisa nuclear power plant (Finland) uses RIPE as part of their information security management system. The key element for Loviisa is the systematic approach for Industrial Control Systems cyber security provided by the RIPE framework.

Formal Safety & Security Assessment of System Architectures Using Viewpoints

This work results from a joint effort between ONERA, Thales Research & Technology and ALL4TEC. An article was presented at the workshop MoDeVVa 2014, co-located with the conference MODELS 2014, in Valencia, Spain (September 28 - October 3 2014). This research addresses safety and security assessment during system engineering. An integrated process is proposed, where system engineers, safety engineers and security engineers work on different views of the system architecture. Then, security and safety assessment are performed using the Alloy formal method.

In the proposed approach, system engineers design a model of the system architecture using the tool Capella from Thales. Safety and security engineers then specify the propagation of failures and attacks inside each component of the architecture using the tool Safety Architect from ALL4TEC. The underlying analyses are subsequently performed using Alloy. This work is illustrated on a system that implements a landing approach of an aircraft.



Variability and Patterns in Safety/Security System Engineering: An Overview

Variability and Patterns in Safety/Security System In systems and software engineering, the analysis of architectural variants is most of the times subjective and manual. The justification of a variant is seldom based on the assets and the flaws and strengths of the different options. Ideally, assessing or comparing several candidate architectures (variants) should be based on some decision criteria - corresponding to a Multi-Criteria Decision Aiding (MCDA) problem. A first step to address the problem is to support the automatic generation of variants.

Inria and several division of THALES are collaborating on this within MERgE. In December they presented a paper at 'Journées Lignes de Produits' regarding the industrial experience to bridge the gap between variability modelling and system engineering practices. They detailed an approach based on CVL and the EMF Diff/Merge patterns technology to generate model variants. This approach is evaluated through several possible industrial scenarios in the communications and security domain. Their long term goal is to allow stakeholders to explore the design space of variants for multi-criteria optimization.

Inter Project Co-operation — 2nd ISSE Workshop

The MERGE consortium in collaboration with the SESAMO ARTEMIS project are proud to announce to you that they will organize the 2nd Edition of the ISSE (Integration of Safety and Security Engineering) workshop co-located with the SAFECOMP 2015 conference the 22 September 2015 at DELFT in The Netherlands. To remind you of the objective for this workshop we wish to share ideas, experiences and solutions to concretely combine or integrate safety and security engineering activities. Industrials are also invited to provide feedback on applying both safety and security verification techniques in their context. This workshop will also encourage discussions about issues and opportunities to apply safety and security co-engineering.

http://safecomp2015.tudelft.nl/

SAFECOMP 2015
international conference on computer safety, reliability & security 22-25 September | Delft | the Netherlands

MERgE consortium

Follow
@MERgE_Project

Subscribe
http://www.merge-project.eu/mailing-list

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

Modelling Everywhere: Farming

In the context of the MERgE Platform, we speak a lot about the versatility of the framework. We are applying it to System Modelling, and Specialty Engineering Modelling, such as Safety and Security. But modelling is a formal abstraction of a reality, so the approach is not limited to the software domain, or even Information Technology.

In collaboration with INRIA, Obeo uses Domain Specific Languages with tooling based on Sirius and Xtext to describe an agricultural exploitation from a structural and behavioural point of view. The structural point of view is the description of the exploitation and its constraints, such as resources, surfaces or workshops (crop, ovine and bovine). The behavioural point of view is more on process and tasks asked by this kind of exploitations, depending on short term renewal (feeding, milking of bovine) or long term, for birth season or harvesting.

The farming model is then used for simulation and constraint satisfaction checking, mainly as a means for the realization of each farming activity, which can be updated if we simulate evolution of the farm surface and resources.

This framework instance was presented by Obeo and INRIA to IDM2014, a conference about model driven engineering, as an example of the generalization of modelling concepts. http://devlog.cnrs.fr/_media/idm2014_mdeandsle_combemale-web.pdf