Recent Advances towards the Industrial Application of Model-Driven Engineering for Assurance of Safety-Critical Systems

Jose Luis de la Vara[1], Alejandra Ruiz[2] and Huáscar Espinoza[2]
[1]*Departamento de Informática, Universidad Carlos III de Madrid, Leganés, Spain*
[2]*ICT Division, TECNALIA, Derio, Spain*

Keywords: Safety-Critical Systems, Assurance, Certification, Model-Driven Engineering, Model-based Engineering.

Abstract: Safety-critical systems are typically subject to assurance processes as way to ensure that they do not pose undue risks to people, property, or the environment, usually in compliance with assurance standards. The planning, execution, and management of assurance processes can be a complex activity in practice because of issues in the application of the standards, the large amount of information to handle, and the need for providing convincing justifications of assurance adequacy, among other difficulties. As a solution, many authors have argued that the use of Model-Driven Engineering principles and techniques can facilitate and improve assurance of safety-critical systems. This paper presents some of the latest advances that have been and are being made towards the use of these principles and techniques in industry. Although models have been used for assurance of safety-critical systems for many years, e.g. to specify safety cases, it has only been recently when the full potential of Model-Driven Engineering has started to be more widely exploited. This includes aspects such as the specification of metamodels and domain specific languages for assurance, the extension and application of UML, and the use of model transformations.

1 INTRODUCTION

Safety-critical systems are those whose failure can harm people, property, or the environment, e.g. cars, trains, aircrafts, and medical devices. These systems are subject to rigorous assurance processes. Assurance can be defined as "the planned and systematic actions necessary to provide adequate confidence and evidence that a product or process satisfies given requirements" (RTCA, 2011); dependability requirements in general, safety ones in particular, and typically in compliance with assurance standards for certification.

Examples of assurance standards include IEC 61508 (IEC, 2011) for electrical, electronic, and programmable electronic systems in a wide range of industries, and more specific standards such as DO-178C for avionics (RTCA, 2011), the CENELEC standards for railway (e.g. EN 50128 (CENELEC, 2011)), and ISO 26262 for the automotive sector (ISO, 2011). Systems (and components) developers must follow the standards and enact assurance processes for safety-critical systems, and system evaluators (e.g. assessors, certification authorities, or regulators) must confirm the adequacy of the assurance activities executed by the developers.

Assurance of safety-critical systems is a complex activity in practice. Standards are usually large textual documents that contain hundreds of pages and define thousands of compliance criteria. Ambiguity and inconsistency are common. System developers can easily face challenges because of difficulties in following and applying the standards, having to manage large amounts of assurance evidence, and having to provide valid justifications of system assurance and of the adequacy of the assurance activities, among other difficulties (de la Vara, 2016a; Nair, 2015a). These difficulties can lead to assurance risks (Alexander, et al., 2010), which are conditions that can make a safety-critical system developer incapable of (1) developing a system that complies with assurance standards and can be deemed safe, (2) adequately collecting and managing assurance evidence and thus guaranteeing system safety, or (3) making a third-party (e.g. an assessor) gain sufficient confidence in system safety.

As a solution to the above issues, several authors have argued during the last decade that the use of Model-Driven Engineering (MDE) principles and

Vara, J., Ruiz, A. and Espinoza, H.
Recent Advances towards the Industrial Application of Model-Driven Engineering for Assurance of Safety-Critical Systems.
DOI: 10.5220/0006733906320641
In *Proceedings of the 6th International Conference on Model-Driven Engineering and Software Development (MODELSWARD 2018)*, pages 632-641
ISBN: 978-989-758-283-7

techniques can help practitioners to perform assurance activities, e.g. (Biggs, et al., 2016; de la Vara, et al., 2016c; Espinoza, et al., 2011; Falessi, et al., 2012; Panesar-Walawege, et al., 2013; Ruiz, et al., 2016; Wu, et al., 2015). Models, in conformance to metamodels (Bézivin, 2005), can used be e.g. to create representations of assurance standards and of how to follow them, to specify a reference of the assurance evidence to manage and of how to structure it, and to represent the justification of system assurance and of assurance adequacy, including the semi-automatic derivation of this justification with model transformations.

Many of the possible usages of MDE for assurance of safety-critical systems have only been proposed in the literature, but some results are already starting to be transferred to practice through collaborative industry-academia projects, software tools, and international standards. In addition to providing support to assurance processes, MDE has also been used as the overall technology to develop tools to support the processes.

This paper presents recent advances towards the industrial application of MDE for assurance of safety-critical systems. This information can be valuable (1) for practitioners (both system developers and evaluators) to gain awareness of how to exploit MDE for improvement of their assurance processes, (2) for tool vendors to find possible new features and new ways to develop software support to assurance processes, and (3) for academia to obtain an overall picture of recent research results on MDE-based assurance of safety-critical systems and to identify research opportunities.

The rest of the paper is organized as follows. Section 2 presents the main background of the paper, and Sections 3 to 7 describe specific efforts towards the industrial application of MDE for safety assurance. More specifically, Section 3 describes the OPENCOSS project, Section 4 the OpenCert platform, Section 5 initiatives and the OMG (Object Management Group), and Section 6 the AMASS project. Section 7 reports our main conclusions.

2 BACKGROUND

The background of the paper is divided into two broad areas: how models have been used for assurance of safety-critical systems in practice, and related work, i.e. other publications that have provided similar or related overviews about assurance process and practices.

2.1 Use of Models for Assurance of Safety-Critical Systems in Practice

The use of models, understood as graphical representations with a specific and constrained structure, in assurance activities for safety-critical systems is not an idea proposed during the last decade, but models have been used since long before. Practitioners have indeed reported the use of models to e.g. manage assurance evidence (de la Vara, 2016a; Nair, 2015a). In this section we focus on the arguably two main specific usages of models for safety-critical systems: the specification of safety cases and the representation of safety analyses.

A safety case can be defined as "a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context" (Kelly, 1999). Safety cases are a specialization of assurance cases, which can be defined as "A collection of auditable claims, arguments, and evidence created to support the contention that a defined system/service will satisfy its assurance requirements" (OMG, 2017d). The notion of and the need for creating and maintaining safety cases is common in practically all the safety-critical domains, in spite of being referred to with a different term, e.g. Software Accomplishment Summary for avionics software.

Safety cases are usually provided as textual reports, but they can contain graphical representations. There exist two main graphical notations: CAE (Claims, Arguments and Evidence) (Adelard, 2017) and GSN (Goal Structuring Notation) (Goal Structuring Notation, 2017). Both support the modelling of the claims that assure system safety, the arguments that justify the claims, and the supporting evidence. GSN provides further concepts to represent e.g. the context of a claim, argument modules, and argument patterns. Figure 1 shows an example of a GSN diagram.

Regarding safety analyses, the application of classical techniques (Ericsson, 2015) is usually based on tables, but some are based on models. The most typical one arguably is FTA (Fault Tree Analysis). It is used to determine the root causes and probability of occurrence of a specified undesired event, and allows systems analysts to model the unique combinations of fault events that can cause an undesired event to occur (Ericsson, 2015). A fault tree is a model that logically represents the various combinations of possible events, both faulty and normal one, occurring in a system that lead to an undesired event or state (Ericsson, 2015).

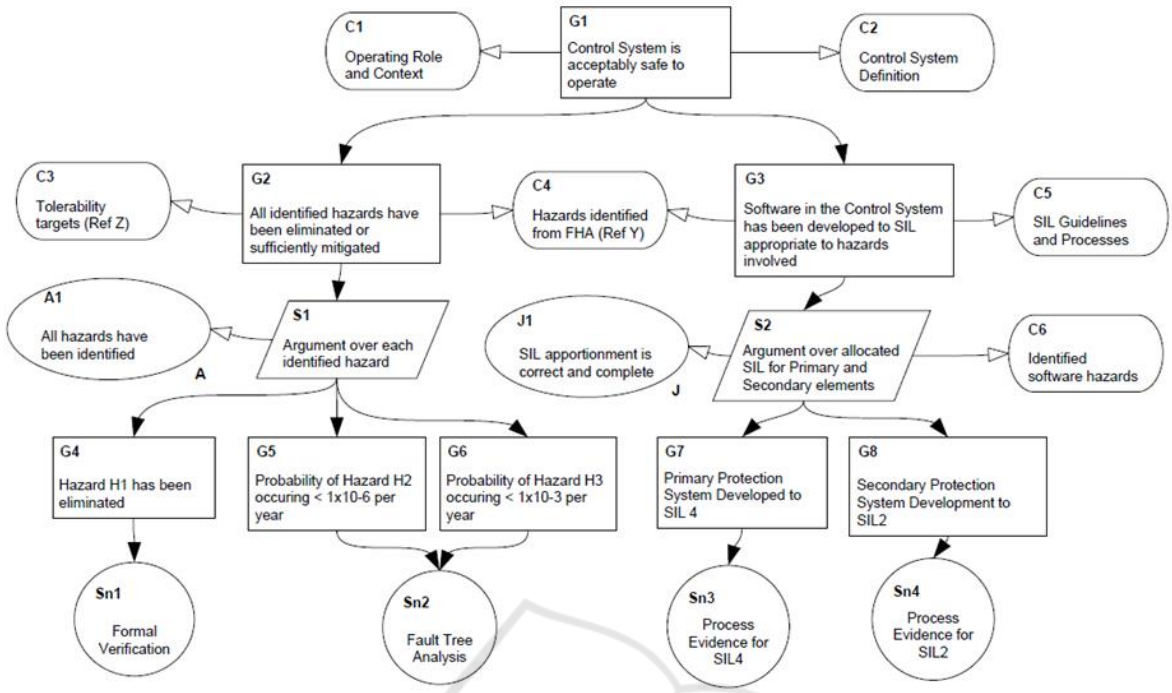

Figure 1: Example of GSN diagram (Goal Structuring Notation, 2017).

Recent techniques for safety analysis are based on models too, e.g. STAMP (Systems-Theoretic Accident Model and Processes) (Leveson, 2011). This technique has three basic underlying constructs: safety constraints, hierarchical safety control structures, and process models.

2.2 Related Work

Several publications have provided an overview of the safety assurance area and have provided insights into or referred to the application of MDE.

The periodic seminal vision papers about the future of software engineering research published at the International Conference on Software Engineering are part of these publications. In a paper on challenges and directions for safety-critical systems, (Knight, 2002) states that "It is essential that comprehensive approaches to total system modelling are developed so that properties of entire systems can be analyzed. Such approaches must […] provide high fidelity models of critical software characteristics". Five years later, (Heimdahl, 2007) reports that the "reliance on models and automated tools […] promises to increase productivity and reduce the very high costs associated with software development for critical systems". Nonetheless, he also acknowledges that "The reliance on tools rather than people, however, introduces new and poorly understood sources of problems, such as the level of trust we can place in the results of our automation". Heimdahl also reviews model-based development as an element of his vision for safety and software-intensive systems. In the latest related publication of this paper series, on certifiably safe software-dependent systems, (Hatcliff, et al., 2014) argue that: "The potential of domain modelling […] (now) is much more realizable by leveraging advancements in ontologies, modeling semantic networks, and knowledge representation combined with the use of stylized natural language", and that "Open source projects should be pursued that provide […] modeling environments for building qualifiable tools". Hatcliff et al. also review the potential of model-based system analysis and development.

Regarding other publications, (Panesar-Walawege, et al., 2011) present their experience, position, and vision on how to use MDE for safety evidence characterisation and management, mainly based on work in the maritime and energy sector. They worked with companies on the application of MDE to create common interpretations of standards, specialise standards to industrial contexts, align standards to organisational practices, plan certification, and manage evidence electronically.

In our prior work (de la Vara, et al., 2016c), we reviewed approaches for model-based management of safety compliance and divided them into three

categories: (1) approaches for safety regulation modelling, to model the content (i.e. text) of standards in order to perform some analysis for identification of issues such as conflicts and inconsistencies, e.g. (Sannier, Baudry, 2014); (2) approaches for safety standard-specific modelling, which correspond to those model-based approaches that focus on some safety standard, e.g. DO-178B (Zoughbi, et al., 2011) or IEC 61508 (Panesar-Walawege, et al., 2013), and; (3) approaches for safety standard-independent modelling, which explicitly aim to support the specification of safety compliance needs in a generic way, so that they can be instantiated for any safety standard or domain, e.g. for process assurance (Gallina, et al., 2014) and for evidence traceability (Nair, et al., 2014a).

Finally, insights into the usage of models for assurance of safety-critical systems can be found in reviews of the literature (Nair, et al., 2014b) and in industrial surveys with practitioners (de la Vara, et al., 2016a; Nair, et al., 2015a), e.g. about the use of graphical argumentation notations.

3 THE OPENCOSS PROJECT

OPENCOSS (Open Platform for EvolutioNary Certification of Safety-critical Systems) (Espinoza, et al., 2011; OPENCOSS project, 2017) was a European research project on safety assurance and certification of embedded systems. The OPENCOSS consortium comprised four academic partners and 13 companies, including safety-critical system manufacturers, component suppliers, certification authorities, safety assessors, and tool vendors. The project was supported by a large advisory board with representatives from more than 20 organisations.

The project tackled the lack of precision and large variety of certification requirements, the lack of composable and system views for certification, the high and non-measured costs for (re)certification, and the lack of openness to innovation and new approaches. As solutions. OPENCOSS (a) devised a common certification framework that spans different vertical markets for railway, avionics, and automotive, and (b) developed an open-source safety certification infrastructure.

The ultimate goal of the project was to bring about substantial reductions in recurring safety certification costs and, at the same time, reduce assurance risks through the introduction of more systematic safety assurance practices. The project dealt with (1) creation of a common certification conceptual framework, (2) compositional certification, (3) evolutionary chain of evidence, (4) transparent certification process, and (5) compliance-aware development process.

Figure 2 shows the MDE approach for safety assurance and certification defined in OPENCOSS. It is based on several related metamodels targeted at different safety assurance and certification needs. The set of metamodels corresponds to the common certification conceptual framework.

- The Reference Assurance Framework Metamodel supports the specification of the safety compliance needs that have or might have to be considered in an assurance project. Safety compliance needs can be from specific standards, recommended practices, or company-specific practices, and typically have to be tailored to project-specific characteristics. The latter is done by means of baselines.
- Another source of information for safety compliance is the data about the product for which compliance is sought. The metamodels include the concepts and relationships necessary for modelling and managing project- and product-specific information.
  - The process executed to create a product (Process Metamodel).
  - The evidence of safety and of compliance (Evidence Metamodel).
  - The arguments that will be used to justify key safety-related decisions taken during the project (Argumentation Metamodel).

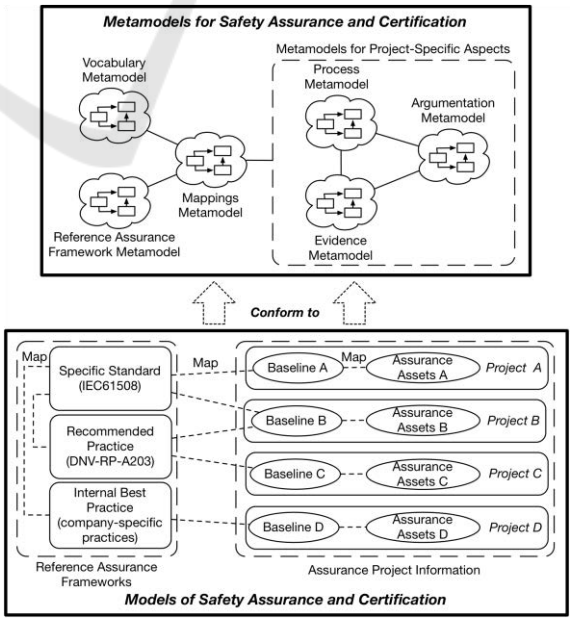

Figure 2: Overall OPENCOSS MDE approach for safety assurance and certification.

- The Vocabulary Metamodel is a means to define and record the terms and concepts used to characterize reusable assurance assets such as evidence, argumentation, and process data, as well as terms from standards.
- With the Mappings Metamodel, maps can be created to specify the degree of equivalence between vocabulary terms (e.g. from different domains), the assurance information of a project (e.g. artefacts) and its baseline for indicating compliance, and safety standards (i.e. reference assurance frameworks).

More details about the metamodels and the MDE approach can be found in (OPENCOSS project, 2015c). The approach provides support to all the areas dealt with in OPENCOSS. For example, the MDE approach has enabled the systematic reuse of assurance information across systems and projects (Ruiz, et al., 2017), the semi-automatic generation of arguments (Ruiz, et al., 2015), the modelling of context-aware process families (Ayora, et al., 2016), and argument-based assessment of confidence in evidence (Nair, et al., 2015b).

The approach was applied in three industrial case studies (OPENCOSS project, 2015a): an ePARK system for an electric vehicle in the automotive domain, the reuse of a railway execution platform in the avionics domain, and the certification of a signalling system in the railway domain. The application resulted in the determination of several improvements over the current practices for safety assurance and certification (OPENCOSS project, 2015b), including a reduction of recurring costs for safety certification across systems, a reduction of recurring costs for safety certification across vertical markets, and a gain for product innovation and upgrading. Experiments in which people have used some parts of the OPENCOSS MDE approach have also been conducted to validate it (de la Vara, et al., 2016b; de la Vara, et al., 2017c).

4 OPENCERT

The safety certification infrastructure for MDE-based safety assurance and certification implemented in OPENCOSS (Ruiz, et al., 2015) has been further developed and maintained and has resulted in the OpenCert platform (OpenCert platform, 2017; Figure 3). OpenCert is an open-source integrated and holistic solution for assurance and certification management of Cyber-Physical Systems (CPS) spanning the largest safety and security-critical industrial markets, such as aerospace, space, railway, manufacturing, energy, and health. The ultimate aim of the platform is to lower certification costs in face of rapidly changing product features and market needs.

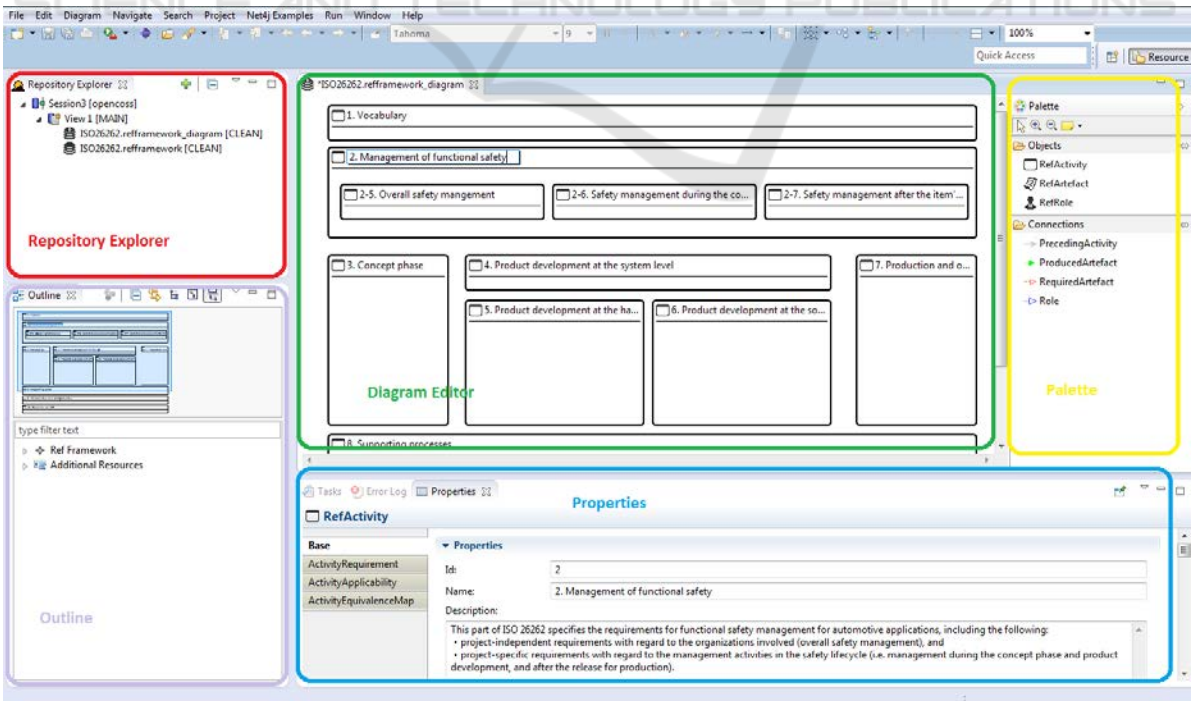

Figure 3: OpenCert screenshot.

OpenCert is hosted and managed by the Eclipse Foundation through the PolarSys Working Group (PolarSys, 2017). This group corresponds to a collaboration of large end-user companies and open-source tools providers dedicated to supplying industrial-grade open-source tools for the development of embedded systems. All the PolarSys solutions are based on technology and tools that have been deployed by large systems engineering and embedded systems development teams.

The current features of OpenCert include the management of information from standards and regulations, the management of assurance projects, architecture-driven assurance, assurance case management, and compliance management. For architecture-driven assurance, OpenCert is linked with the Papyrus (Papyrus, 2017) and CHESS (PolarSys CHESS, 2017) Eclipse projects, and with the EPF project (Eclipse Process Framework Project, 2017) for compliance management.

In addition to supporting model-based CPS assurance and certification, the development of OpenCert itself exploits Eclipse-based MDE technologies such as EEF (Eclipse EEF, 2017), EuGENia (EuGENia, 2017) and GMF (Graphical Modeling Framework, 2017) for editor development, Epsilon (Epsilon, 2017) for model transformation, and CDO (CDO Model Repository, 2017) for data storage.

5 OMG INITIATIVES

We have presented above approaches, projects, and tools for MDE-based assurance of safety-critical systems that have resulted from arguably reduced-scope initiatives, such as a consortium of organizations. However, the recent advances towards the industrial application of MDE for safety assurance go beyond these results. There are international, world-wide organizations and collaborations working on the topic. OMG (OMG, 2017a) is among the main ones.

OMG is a non-profit organization that develops open technical specifications and international standards for application of MDE in different domains, e.g. UML (OMG, 2017g) and SysML (OMG, 2017f) for software modelling and systems modelling, respectively. OMG members correspond to a consortium with international organizations of vendors, developers, end users, and researchers. The set of OMG specifications has also started to address system assurance aspects, and we review them in this section. Most of these specifications have been or are being developed in the scope of System Assurance Task Force (OMG, 2017e).

SACM (Structured Assurance Case Metamodel) (OMG, 2017e) supports the representation of assurance cases in a structured and standard way. Its main sources have been CAE and GSN, and the main developers of these notations have contributed to the standard. SACM consists of a sub-metamodel for argumentation, one for evidence artefacts, and another for terminology. The metamodels aim to allow the interchange of structured arguments between diverse tools by different vendors. In a structured argument, the relationships between the asserted claims, and from the evidence to the claims are explicitly represented. The latest SACM version represents a considerable re-work and improvement to address certain limitations of previous versions (see e.g. (de la Vara, et al., 2017a)).

DAF (Dependability Assurance Framework For Safety-Sensitive Consumer Devices) (OMG, 2017b) provides a system assurance methodology for the dependability argumentation for consumer devices. This is achieved by integrating conventional system assurance approaches, e.g. risk analysis and assessments, with a new way of approaching unique characteristics of consumer devices. The specification supports the objectives of device integration and includes the dependability case for argumentation, as well as new dependability development processes. The focus is to include the dependability argumentation particularly for consumer devices. To this end, a link with SACM is established.

The most recent initiative is a request for proposals for a standard UML profile for safety and reliability (OMG, 2017c). The scope and content of this profile will be similar to some published in the latest years, e.g. (Biggs, et al., 2016; Wu, et al., 2015), which are profiles that include concepts from safety standards so that they are explicitly and directly included in a system representation, e.g. created with SysML. This way, the system and the assurance information can be processed and analysed together. In addition, the request explicitly states that "proposals must consider how the safety information […] can be integrated into a SACM model as supporting evidence for an assurance case argument", and that "Proposals shall discuss how the profile/model library can be used in conjunction with SACM, and how the proposed profile/model library's argument notation compares with SACM and GSN". This way, different OMG's MDE means for assurance of safety-critical systems will be linked together.

There is also some work ongoing for UML-based operational threat and risk modelling (OMG, 2017h). This initiative aims to provide a conceptual model that unifies the semantics of and can provide a bridge across multiple threat and risk schemas and interfaces. The conceptual model will be informed by high-level concepts as defined by the cyber domain and other domains, but it will not be specific to any particular domain.

Finally, the above specifications are recent and more work on their development and usage is expected in the future. This has been argued as necessary, e.g. for SACM (de la Vara, 2014).

6 THE AMASS PROJECT

The previous three sections have presented projects and initiatives from which stable, mature results exist. This section introduces an ongoing effort that is already providing new MDE-based support for assurance of safety-critical systems: the AMASS project (AMASS project, 2017a; Ruiz, et al., 2016).

AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems) is a very large-scale European research project. The consortium consists of 29 partners; 21 from industry. The main issues addressed are the increase in CPS product complexity, the very high costs and effort for CPS assurance and certification, the lack of standardised and harmonised practices, the new assurance and certification risks, the need for dealing with architecture-specific aspects and with multiple dependability concerns, the wider variety of tools and stakeholders, and the insufficient reuse support.

The project is developing an integrated and holistic approach and supporting tools for assurance and certification of CPS by creating and consolidating the first European-wide certification platform, ecosystem and community spanning the largest CPS vertical markets. The approach will be driven by architectural decisions, including multiple assurance concerns such as safety, security, availability, robustness and reliability. The main goal is to reduce time, cost and risks for assurance and (re)certification by adopting an evolutionary compositional certification and reuse approach.

The AMASS approaches focus on the development and consolidation of an open and holistic framework that constitutes the evolution of the approaches from the OPENCOSS project and the SafeCer project (SafeCer project, 2017) towards an architecture-driven, multi-concern assurance, reuse-oriented, and seamlessly interoperable tool platform. In more specific terms, AMASS has four main scientific and technical objectives, each addressing several sub-areas and all using MDE principles and techniques for the development of solutions for CPS assurance (Figure 4):

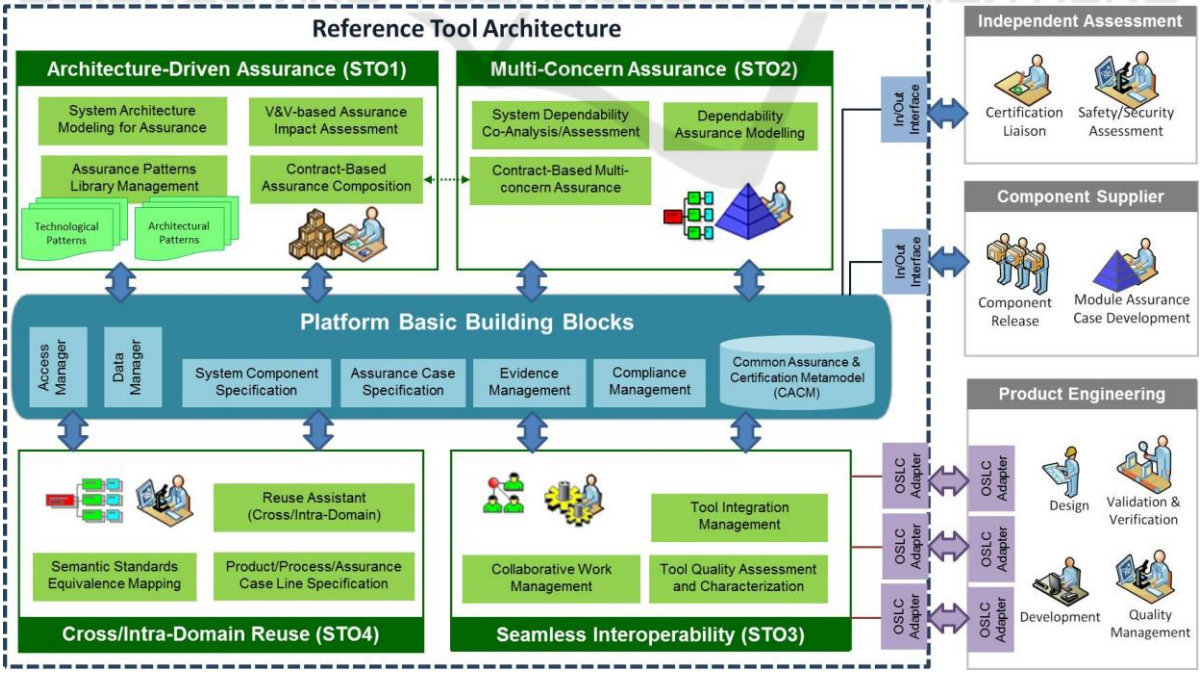

Figure 4: AMASS work areas.

- Architecture-driven assurance, to adequately link system architecture specifications and assurance models. This includes system architecture modelling for assurance, management of assurance pattern libraries, assurance impact assessment based on verification and validation, and component contract-based assurance composition.
- Multi-concern assurance, to deal not only with safety for CPS but also with assurance of further concerns, most notably security. Other relevant concerns are reliability and performance, among others. Multi-concern assurance requires system dependability co-analysis and co-assessment, dependability assurance modelling, and contract-based multi-concern assurance.
- Seamless interoperability, to ensure that assurance and engineering activities and the joint effort of the different assurance stakeholders are properly linked and supported. To this end, the sub-areas addressed are tool integration, collaborative work management, and tool quality characterisation and management.
- Cross- and intra-domain assurance reuse, to make the reuse of CPS products across systems, standards, and domains more cost-effective. This will be possible thanks to new reuse assistance, semantic equivalence mapping of standards, and product, process, and assurance case lines.

AMASS technology will be applied in 11 industrial case studies from the automotive, railway, aerospace, space, and energy domains (AMASS project, 2016). Initial results from the application of the first project outcomes are available (AMASS project, 2017b), e.g. about modelling and co-assessment of safety and security characteristics and about modelling of standards. Effort is also being spent to link the AMASS MDE approaches with other industrial practices for safety-critical systems engineering, e.g. the use of ontologies for system quality analysis (de la Vara, et al., 2017b).

Last but not least, it is planned that the open-source AMASS results are integrated, maintained, and further developed in OpenCert.

7 CONCLUSION

Assurance processes must be performed to provide confidence in the dependability of safety-critical systems. These processes can however be complex, and the application of Model-Driven Engineering (MDE) as supporting technology is advocated by many researchers and practitioners as a solution.

We have reviewed recent advances that have been and are being made so that MDE becomes an industrial practice for the assurance of safety-critical systems. By using MDE principles and technologies such as metamodels and model transformation, complex and challenging assurance activities can be facilitated and improved, e.g. the specification of how to comply with a standard, the management of assurance evidence, the development of assurance cases, the specification of assurance processes, and the reuse of assurance information between projects. These benefits are a result of initiatives such as the OPENCOSS project, the OpenCert platform, OMG standards, and the AMASS project.

We argue and envision that MDE will be a central technology in the future for system assurance in most organizations developing safety-critical systems. Many organizations are already using MDE principles and techniques although they might not be aware of it, e.g. when using models to represent assurance information or MDE-based tools such as OpenCert. This usage will be very likely extended in the future thanks to more mature MDE approaches for assurance that result in international standards.

Finally, and based on our knowledge and experience, the full adoption of MDE for assurance of safety-critical systems needs to overcome some barriers. Challenges arising from practical aspects such as scalability, efficient model storage, and tool qualification must be tackled, at least for many open-source solutions. From a research perspective, the development of MDE solutions that cover a wide range of domains and of dependability concerns remains an area where further work is necessary.

ACKNOWLEDGEMENT

The research leading to this paper has received funding from the AMASS project (H2020-ECSEL no 692474; Spain's MINECO ref. PCIN-2015-262). We also thank all the people that have contributed to the results presented in the paper and with whom we have collaborated to develop them.

REFERENCES

Adelard, 2017. *Claims, Arguments and Evidence (CAE)*. Online, https://www.adelard.com/asce/choosing-asce/cae.html (Accessed October 31st, 2017)

Alexander, R., Kelly, T., Gorry, B., 2010. Safety Lifecycle Activities for Autonomous Systems Development. In *5th SEAS DTC Technical Conference*.

AMASS project, 2016. *Deliverable D1.1 - Case studies description and business impact*. Online, https://www.amass-ecsel.eu/sites/amass.drupal.pulsartecnalia.com/files/documents/D1.1_Case-studies-description-and-business-impact_AMASS_Final.pdf (Accessed October 31st, 2017)

AMASS project, 2017a. Online, https://www.amass-ecsel.eu/ (Accessed October 31st, 2017)

AMASS project, 2017b. *Deliverable D1.4 – AMASS Demonstrators (a)*. Online, https://www.amass-ecsel.eu/sites/amass.drupal.pulsartecnalia.com/files/documents/D1.4_AMASS-demonstrators-%28a%29_AMASS_Final.pdf (Accessed October 31st, 2017)

Ayora, C., Torres, V., de la Vara, J.L., Pelechano, V., 2016. *Variability Management in Process Families through Change Patterns*. Information and Software Technology 74: 86-104.

Bézivin, J., 2005. *On the unification power of models*. Software and System Modeling 4(2): 171-188.

Biggs, G., Sakamoto, T., Kotoku, T., 2016. *A profile and tool for modelling safety information with design information in SysML*. Software and System Modeling 15(1): 147-178.

CDO Model Repository, 2017. Online, https://www.eclipse.org/cdo/ (Accessed October 31st, 2017)

CENELEC, 2011. *EN 50128 - Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems*.

de la Vara, J.L., 2014. Current and Necessary Insights into SACM: An Analysis Based on Past Publications. In *RELAW 2014, 7th International Workshop on Requirements Engineering and Law*. IEEE.

de la Vara, J.L., Borg, M., Wnuk, K., Moonen, L., 2016a. *An Industrial Survey on Safety Evidence Change Impact Analysis Practice*. IEEE Transactions on Software Engineering 42(12): 1095-1117.

de la Vara, J.L., Marín, B., Giachetti, G., Ayora, C., 2016b. Do Models Improve the Understanding of Safety Compliance Needs? Insights from a Pilot Experiment. In *ESEM 2016, 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*. ACM.

de la Vara, J.L., Ruiz, A., Attwood, K., Espinoza, H., Panesar-Walawege, R.K., Lopez, A., del Rio, I., Kelly, T., 2016c. *Model-Based Specification of Safety Compliance Needs: A Holistic Generic Metamodel*. Information and Software Technology 72: 16-30.

de la Vara, J.L., Génova, G., Álvarez-Rodríguez, J.M., Llorens, J., 2017a. *An Analysis of Safety Evidence Management with the Structured Assurance Case Metamodel*. Computer Standards & Interfaces 50: 179-198.

de la Vara, J.L., Gómez, A., Gallego, E., Génova, G., Fraga, A., 2017b. Representation of Safety Standards with Semantic Technologies Used in Industrial Environments. In *SASSUR 2017, 6th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems*. Springer.

de la Vara, J.L., Marín, B., Ayora, C., Giachetti, G., 2017c. An Experimental Evaluation of the Understanding of Safety Compliance Needs with Models. In *ER 2017, 36th International Conference on Conceptual Modeling*. Springer.

Eclipse EEF, 2017. Online, https://eclipse.org/eef/#/ (Accessed October 31st, 2017)

Eclipse Process Framework Project, 2017. Online, https://eclipse.org/epf/ (Accessed October 31st, 2017)

Epsilon, 2017. Online, https://www.eclipse.org/epsilon/ (Accessed October 31st, 2017)

Ericson, C. A., 2015. *Hazard analysis techniques for system safety*. John Wiley & Sons. 2nd edition.

Espinoza, H., Ruiz, A., Sabetzadeh, M., Panaroni, P., 2011. Challenges for an Open and Evolutionary Approach to Safety Assurance and Certification of Safety-Critical Systems. In *WoSoCER 2011, First International Workshop on Software Certification*. IEEE.

EuGENia, 2017. Online, https://www.eclipse.org/epsilon/doc/eugenia/ (Accessed October 31st, 2017)

Falessi, D., Sabetzadeh, M., Briand, L., Turella, E., Coq, T., Panesar-Walawege, R.K., 2012. *Planning for Safety Standards Compliance: A Model-Based Tool-Supported Approach*. IEEE Software 29(3): 64-70.

Gallina, B., Pitchai, J.P., Lundqvist, K., 2014: S-TunExSPEM: Towards an Extension of SPEM 2.0 to Model and Exchange Tunable Safety-Oriented Processes. In *Software Engineering Research, Management and Applications*. Springer.

Goal Structuring Notation, 2017. Online, http://www.goalstructuringnotation.info/ (Accessed October 31st, 2017)

Graphical Modeling Framework, 2017. Online, https://www.eclipse.org/modeling/gmp/ (Accessed October 31st, 2017)

Hatcliff, J., Wassyng, A., Kelly, T., Comar, C., Jones, P.L., 2014. Certifiably safe software-dependent systems: challenges and directions. In *FOSE 2014, Future of Software Engineering*. ACM.

Heimdahl, M.P.E., 2007. Safety and Software Intensive Systems: Challenges Old and New. In *FOSE 20017, Workshop on the Future of Software Engineering*. IEEE.

IEC, 2010. *IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*. 2nd edition.

ISO, 2011. *ISO 26262 - Road vehicles - Functional safety*.

Kelly, T., 1999. *Arguing Safety - A Systematic Approach to Managing Safety Cases*. University of York. PhD thesis.

Knight, J.C., 2002. Safety critical systems: challenges and directions. In *ICSE 2002, 24th International Conference on Software Engineering*. ACM.

Leveson, N., 2011. *Engineering a safer world: Systems thinking applied to safety*. MIT press.

Nair, S., de la Vara, J.L., Sabetzadeh, M., Falessi, D., 2015a. *Evidence Management for Compliance of Critical Systems with Safety Standards: A Survey on the State of Practice*. Information and Software Technology 60: 1-15.

Nair, S., Walkinshaw, N., Kelly, T., de la Vara, J.L., 2015b. An Evidential Reasoning Approach for Assessing Confidence in Safety Evidence. In *ISSRE 2015, 26th IEEE International Symposium on Software Reliability Engineering*. IEEE.

Nair, S., de la Vara, J.L., Melzi, A., Tagliaferri, G., de-la-Beaujardiere, L., Belmonte, F., 2014a. Safety Evidence Traceability: Problem Analysis and Model. In *REFSQ 2014, 20th International Working Conference on Requirements Engineering: Foundation for Software Quality*. Springer.

Nair, S., de la Vara, J.L., Sabetzadeh, M., Briand, L., 2014b. *An Extended Systematic Literature Review on Provision of Evidence for Safety Certification*. Information and Software Technology 56(7): 689-717.

OMG, 2017a. Online, http://www.omg.org/ (Accessed October 31st, 2017)

OMG, 2017b. *Dependability Assurance Framework For Safety-Sensitive Consumer Devices (DAF)*. Online, http://www.omg.org/spec/DAF/ (Accessed October 31st, 2017)

OMG, 2017c. *Safety and Reliability for UML RFP*. Online, http://www.omg.org/cgi-bin/doc.cgi?ad/2017-3-5 (Accessed October 31st, 2017)

OMG, 2017d. *Structured Assurance Case Metamodel (SACM)*. Online, http://www.omg.org/spec/SACM/ (Accessed October 31st, 2017)

OMG, 2017e. *System Assurance (SysA) Task Force*. Online, http://sysa.omg.org/ (Accessed October 31st, 2017)

OMG, 2017f. *System Modeling Language (SysML)*. Online, http://www.omgsysml.org/ (Accessed October 31st, 2017)

OMG, 2017g. *Unified Modeling Language (UML)*. Online, http://www.uml.org/ (Accessed October 31st, 2017)

OMG, 2017h. *UML Operational Threat & Risk Model*. Online, http://www.omg.org/cgi-bin/doc.cgi?sysa/2014-6-17 (Accessed October 31st, 2017)

OpenCert Platform, 2017. Online, https://www.polarsys.org/opencert/ (Accessed October 31st, 2017)

OPENCOSS project, 2015a. *Deliverable D1.4 - Implementation of use cases on top of OPENCOSS platform*. Online, http://www.opencoss-project.eu/sites/default/files/D1.4_Implementation_of_use_cases_on_top_of_OPENCOSS_platform_final.pdf (Accessed October 31st, 2017)

OPENCOSS project, 2015b. *Deliverable D1.5 – OPENCOSS Benchmarking*. Online, http://www.opencoss-project.eu/sites/default/files/D1.5_OPENCOSS_Benchmarking__Final.pdf (Accessed October 31st, 2017)

OPENCOSS project, 2015c. *Deliverable D4.4 - Common Certification Language: Conceptual Model*. Online, http://www.opencoss-project.eu/sites/default/files/D4.4_v1.5_FINAL.pdf (Accessed October 31st, 2017)

OPENCOSS project, 2017. Online, http://www.opencoss-project.eu/ (Accessed October 31st, 2017)

Panesar-Walawege, R.K., Sabetzadeh, M., Briand, L., 2011. Using Model-Driven Engineering for Managing Safety Evidence: Challenges, Vision and Experience. In *WoSoCER 2011, First International Workshop on Software Certification*. IEEE.

Panesar-Walawege, R.K., Sabetzadeh, M., Briand, L., 2013. *Supporting the verification of compliance to safety standards via model-driven engineering: Approach, tool-support and empirical validation*. Information & Software Technology 55(5): 836-864.

Papyrus, 2017. Online, https://eclipse.org/papyrus/ (Accessed October 31st, 2017)

PolarSys, 2017. Online, https://www.polarsys.org/ (Accessed October 31st, 2017)

PolarSys CHESS, 2017. Online, https://www.polarsys.org/projects/polarsys.chess (Accessed October 31st, 2017)

RTCA, 2011. *DO-178C - Software Considerations in Airborne Systems and Equipment Certification*.

Ruiz, A., Larrucea, X., Espinoza, H., 2015. A Tool Suite for Assurance Cases and Evidences: Avionics Experiences. In *EuroSPI 2015, 22nd European Conference on Systems, Software and Services Process Improvement*. Springer.

Ruiz, A., Gallina, B., de la Vara, J.L., Mazzini, S., Espinoza, H, 2016. Architecture-driven, Multi-concern, Seamless, Reuse-Oriented Assurance and Certification of Cyber-Physical Systems. In *SASSUR 2016, 5th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems*. Springer.

Ruiz, A., Juez, G., Espinoza, H., de la Vara, J.L., Larrucea, X., 2017. *Reuse of safety certification artefacts across standards and domains: A systematic approach*. Reliability Engineering and System Safety 158: 153-171.

SafeCer project, 2017. Online, http://www.safecer.eu/ (Accessed October 31st, 2017)

Sannier, N., Baudry, B., 2014. INCREMENT: A Mixed MDE-IR Approach for Regulatory Requirements Modeling and Analysis. In *REFSQ 2014, 20th International Working Conference on Requirements Engineering: Foundation for Software Quality*. Springer.

Wu, J., Yue, T., Ali, S., Zhang, H., 2015. *A modeling methodology to facilitate safety-oriented architecture design of industrial avionics software*. Software - Practice and Experience 45(7): 893-924.

Zoughbi, G., Briand, L., Labiche, Y., 2011. *Modeling safety and airworthiness (RTCA DO-178B) information: conceptual model and UML profile*. Software and System Modeling 10(3): 337-367.