Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

Alejandra Ruiz[1], Barbara Gallina[2], Jose Luis de la Vara[3], Silvia Mazzini[4] and Huáscar Espinoza[1]

[1]ICT Division, TECNALIA, Spain
[2]MDH University, Sweden
[3]Universidad Carlos III de Madrid, Spain
[4]INTECS, Italy
alejandra.ruiz@tecnalia.com; barbara.gallina@mdh.se;
jvara@inf.uc3m.es;silvia.mazzini@intecs.it;
huascar.espinoza@tecnalia.com

Abstract: Unlike practices in electrical and mechanical equipment engineering, Cyber-Physical Systems (CPS) do not have a set of standardized and harmonized practices for assurance and certification that ensures safe, secure and reliable operation with typical software and hardware architectures. This paper presents a recent initiative called AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems) to promote harmonization, reuse and automation of labour-intensive certification-oriented activities via using model-based approaches and incremental techniques. AMASS will develop an integrated and holistic approach, a supporting tool ecosystem and a self-sustainable community for assurance and certification of CPS. The approach will be driven by architectural decisions (fully compatible with standards, e.g. AUTOSAR and IMA), including multiple assurance concerns such as safety, security and reliability. AMASS will support seamless interoperability between assurance/certification and engineering activities along with third-party activities (external assessments, supplier assurance). The ultimate aim is to lower certification costs in face of rapidly changing product features and market needs.

Keywords: Assurance, Safety, Security, Certification, System Architecture, Reuse, seamless Interoperability

1 Introduction

Embedded systems have significantly increased in number, technical complexity, and sophistication toward open, interconnected, networked systems (such as "the connected car"). This has brought a “cyber-physical” dimension with it, exacerbating the problem of assuring safety, security and reliability in the presence of human, environmental and technological risks. Furthermore, the products into which these Cyber-

Physical Systems (CPS) are integrated (e.g. aircrafts) need to respect applicable standards for assurance and in some areas they even need certification.

Unlike practices in electrical and mechanical equipment engineering, CPS do not have a set of standardized and harmonized practices for assurance and certification that ensures safe, secure and reliable operation with typical software and hardware architectures. As a result, the CPS community often finds it difficult to apply existing certification guidance. Ultimately, the pace of assurance and certification will be determined by the ability of industry and the certification and assessment authorities to overcome technical, regulatory, and operational challenges. Another key difficulty appears when trying to reuse CPS products between projects and even from one application domain to another. Product evolutions become costly and time consuming because they entail regenerating the entire body of evidence or their certification can be constrained by different standards. This may imply that the full assurance and certification process is applied as for a new product, thus reducing the return on investment of such reuse decision.

This paper presents a recent initiative called AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems) [1] to promote harmonization, reuse and automation of labour-intensive certification-oriented activities via using model-based approaches and incremental techniques. Section 2 describes the main challenges faced by AMASS in the light of current state of the art and Section 3 summarizes the proposed directions to solve those challenges.

2 Current state and challenges

AMASS builds upon two large-scale past projects, OPENCOSS [2] and SafeCer [3], which dealt with the problem of certification of safety-critical systems in multiple domains using model-based approaches and incremental techniques. Among the main targeted tangible results, AMASS will produce a Reference Tool Architecture (ARTA). The ARTA (Fig. 1) represents a virtual entity that embodies a common set of tool interfaces/adaptors, working methods, tool usage methodologies and protocols that will allow any stakeholder of the assurance and certification/qualification activities to seamless integrate their activities (e.g., product engineering, external/independent assessment, component/parts supply) into tool chains adapted to the specific needs of the targeted CPS markets, such as industrial automation, automotive, space, railway, avionics or air traffic management.

Fig. 1 also shows the AMASS Platform Basic Building Blocks, which are the result of merging existing technologies from OPENCOSS and SafeCer. These building blocks include tools for specification of system components, specification of assurance cases as structured argumentation trees, evidence management, and compliance management. In addition to these, the basic building blocks include user access management and data management tools, as well as the Common Assurance and Certification Metamodel (CACM). CACM is an evolution of the OPENCOSS and SafeCer metamodels. Using a common metamodel for different application domains and assurance activities will also enable management of assurance/certification assets in a

common format, sharing patterns of technology and architecture, and cost-effective reuse between different domains and standard frameworks.

Supported on the basic building blocks, AMASS will work on four pillars, which corresponds to specific challenges and Scientific and Technical Objectives (STO):

- **Architecture-Driven Assurance**. The standard architectures (such as AUTOSAR in the automotive industry and IMA in avionics) needed to handle these new large, networked systems are only now being equipped with mechanisms to handle dependability-related aspects. OPENCOSS and SafeCer approaches are agnostic regarding system architectural and engineering choices. This is an intentional feature to meet key requirements about cross-domain harmonization and flexibility. The architecture-agnostic approach is in the right direction since it permits to benchmark industrial case studies and demonstrate the feasibility of using a common framework for multiple application domains. However, the need for more cohesively integrated approaches (assurance/certification versus engineering activities) requires further research and industrial validation with standard and modern engineering practices (e.g., AUTOSAR-driven model-based development).
- **Multi-Concern Assurance.** OPENCOSS and SafeCer were oriented to safety aspects. The synergies between safety and security (among other dependability properties) seem to offer clear opportunities for the reuse of assurance assets, although prior research in this area has suggested that the domain-specific standards do not always support such reuse. Also, the contract-based approaches to compositional assurance developed in OPENCOSS and SafeCer depend, in some respects, on precise mechanisms associated with safety characteristics. There is a need to refine this approach to support the management of trade-offs between various system characteristics (including safety, security, reliability and the like).
- **Seamless Interoperability**. Providing a seamless interoperability between assurance/certification activities and engineering activities (e.g., design, implementation, validation and verification- V&V), along with third-party activities (e.g., external assessments and supplier assurance) is of prime importance to lower the threshold of product assurance and certification in face of rapidly changing product features and market needs. The challenge is to be able to gather evidence from different types of tools by means of standardized and well-defined adapters or exchange tools.
- **Cross and Intra-Domain Reuse**. The OPENCOSS and SafeCer approaches aim to reduce the assurance effort when reusing products, by promoting flexible and systematic reuse approaches that are fully cognizant of the similarities and differences between approaches to safety assurance across the main safety-critical system domains. While these approaches are a first proof of concept of cross- as well as intra-domain reuse and many safety-critical industries are convinced of the benefits to share some development with other industries, one obstacle to the cost-effective reuse of cross-domain assets is the fact that the terminology and semantics used to describe and manage assurance across different application domains are not consistent.

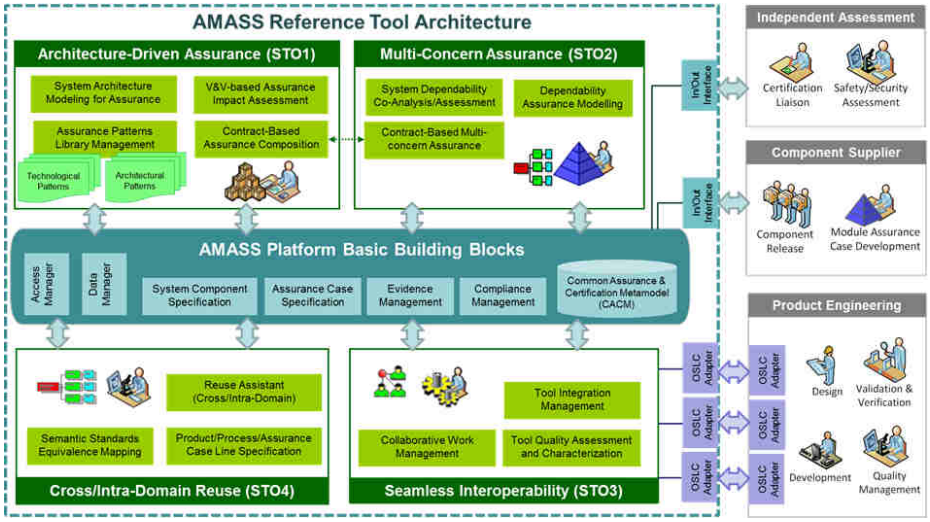

Fig. 1. AMASS High-level Tool Architecture

3 Approaches

3.1 Architecture-Driven Assurance

The architecture represents a major aspect for ensuring dependability of a CPS and for meeting assurance and certification needs and requirements. It describes the realization of the system and consists of the components and all the mechanisms necessary to fulfill, among others, safety, security, reliability, and availability requirements.

The architecture components shall have specific dependability characteristics. These characteristics impose constraints on component reuse, that can refer to both technical aspects (e.g., a component can only be deemed safe for a given operational context) and economical (e.g., component reuse will have an impact on CPS cost). In addition a CPS' architecture must conform to the applicable standards so that a system can be effectively certified according to them.

The AMASS architecture-driven reuse will build on the results of the OPENCOSS and SafeCer projects, and address the additional architecture-related features that can greatly increase the opportunities of cost reduction and of reuse for CPSs, as well as facilitate the analysis for assurance and certification.

System Architecture Modelling for Assurance. Architecture-driven reuse will build on the component model and contract-based verification facilities developed in the SafeCer project. The OPENCOSS CCL metamodel for assurance will be extended with a more detailed formalism for the definition of the system architecture and for analysis of the system dependability with the inclusion of the SafeCer component and contract models, enriched with "white box" information (e.g., fault, error, and failure), "black-box" annotations, and all the other concepts that would allow to improve the analysis of all the aspects that affect assurance activities.

We plan to study the relation of the OPENCOSS and SafeCer assurance models with different system modelling languages (e.g. UML, SysML, AADL, EAST-ADL, etc.), safety modelling profiles, and specific platform models and architectures like AUTOSAR for automotive and IMA for avionics. A finer-grained analysis of a CPS and its assurance and certification information will allow industry to make more informed decisions regarding what can be reused between systems (including different versions of systems) and reuse consequences.

Assurance Patterns Library Management. OPENCOSS and SafeCer have straightforward mechanisms to specify assurance patterns for argumentation and for compliance with standards. However, further research and case studies are necessary to cohesively integrate these patterns in specific assurance and certification activities. This includes safety/security architectural patterns definition and application (e.g. 3-level-monitoring, E2E protection, and partitioning, among others), and auto-generation of platform models and configurations based on these patterns (e.g. for AUTOSAR and IMA). The use of patterns speeds architecture specification and facilitates the (re)use of components, especially if developed to be used in such patterns. Moreover, it enables the reuse of models and associated analysis results, e.g. guarantees of tolerance on failure communication associated with E2E protection [4] or security-related non-interference associated with partitioning [5].

Assurance of specific technologies. AMASS will consider technology trends such as the use of new multi-core hardware platforms, the introduction of middleware solutions (such as AUTOSAR in the automotive domain), deterministic communication technologies, and new networked functionalities such as remote diagnosis, software upgrading, towards vehicle and aircraft autonomy. Since OPENCOSS and SafeCer results are technology-agnostic, they do not directly support the assurance and certification of many characteristics of the new technologies for CPS. However, these characteristics have a great impact on how CPS assurance and certification has to be managed for highly-critical CPSs. Therefore, the characteristics thus must be carefully taken into account as part of the technology patterns, and benchmarked in case studies to determine the circumstances under which they can be reused, assured, and certified.

Contract-Based Assurance Composition. The concepts of contracts in OPENCOSS and SafeCer will be integrated in AMASS. In particular, the AMASS approach for the argumentation that a system architecture is compliant with the system properties will follow the contract refinement defined in the system model. Therefore, the guarantees of the system will be ensured by the composition of the components contracts, while the assumptions of a component will be ensured by the context provided by the system architecture. In case contracts are specified and analyzed with formal methods, evidence for the contracts refinement argument will be provided by verification tools such OCRA [6], developed in the SafeCer project. Safety analyses based on the contract specification will enrich the assurance case with fault trees showing the dependency of system failures on the component failures.

V&V-based Assurance Impact Assessment. Automatic V&V-oriented techniques will enrich the OPENCOSS and SafeCer assurance approaches. These techniques include automated search of compliant arguments in a set of components to define a new safe application that conforms to a set of safety/security requirements, search of

adequate component candidates for a project (e.g. in railway: segregated safety controller, reduce footprint of hardware, safe communication protocol) starting with several functional and safety requirements (or safety patterns), formal techniques to validate that the requirements specification is complete, correct, and unambiguous, and automated support of assurance decisions by provision of what-if scenarios when changing any engineering feature.

3.2 Multi-Concern Assurance

The OPENCOSS project has developed an approach for mapping safety assurance artefacts, techniques and requirements across domains, using the OPENCOSS CCL, to resolve the inconsistencies in terminology across the target domains and to support informed reuse of assurance assets. Also, the compositional certification approaches developed in OPENCOSS and in SafeCer further support reuse by encapsulating assurance concerns for individual components into reusable assurance argument modules and by providing a mechanism to configure these modules to form an overall system assurance case. In order to fully leverage the benefits of development methodologies based on the informed reuse of components, however, it is important to consider other aspects of the system's design as part of the assurance framework: characteristics such as reliability, availability, maintainability, durability, performance and security also have an impact on safety, and need to be considered in the assurance of critical CPS.

In the AMASS project, we aim to exploit the existing OPENCOSS and SafeCer approaches and extend them to provide a tool-supported methodology for the development of assurance cases which address multiple system characteristics. There are three aspects to this work.

Dependability Assurance Modeling. The OPENCOSS CCL metamodel is relatively generic, and its extension to support the reuse of assurance data relating to other dependability-related requires considerable further domain modelling, but no fundamental re-engineering of the approach. Similarly, the CCL vocabulary will require the addition of further concepts, but the vocabulary-based and model-based techniques for using mappings between concepts are readily transferable. From a methodological point of view, the SafeCer Safety-oriented Process Line Engineering remains valid. However, its modeling means may require to be extended (through the AMASS CACM metamodel) to explicitly address additional dependability-related attributes .

Contract-Based Multi-concern Assurance. The contract-based approaches to compositional certification developed in OPENCOSS and SafeCer depend, in some respects, on precise mechanisms associated with safety characteristics. AMASS proposes to refine this approach to support the management of trade-offs between system characteristics.

System Dependability Co-Analysis/Assessment. The synergies between safety and security (among other dependability properties) seem to offer clear opportunities for the reuse of assurance assets, although prior research in this area has suggested that the domain-specific standards do not always support such reuse [7]. The AMASS project will focus initially on extending the OPENCOSS and SafeCer approaches to

address those aspects of security which impact on safety issues for critical CPS, where the potential to save costs through reuse is high. The project will then integrate and extend existing architecture-driven approaches to the assurance of system and security, such as the D-MILS approach [8], where the system architecture is the key element for hinging the assurance of both safety and security aspects such as partitioning and redundancies, or the SESAMO [9] component-oriented design methodology, based on model-driven technology and jointly addressing safety and security aspects and their interrelation for networked embedded systems in multiple domains. The interplay between security and safety will also be considered in terms of process requirements. The recently introduced notion of Security-informed Safety-oriented Process Line [10] will be further investigated in AMASS in order to enable the alignment of safety and security standards.

3.3 Seamless Interoperability

This area aims at guaranteeing the interoperability of the AMASS tool framework with other tools used in the lifecycle of CPS, such as design and V&V tools, whereby assurance evidence can be generated either manually or automatically by the tools themselves (code generators, testing tools, safety analysis tools, etc.). The challenge is to be able to gather evidence from different types of tools by means of standardized and well-defined adapters or exchange tools. There are some axes in this direction that can considerably improve the opportunities of AMASS adoption.

Tool Integration Management. AMASS will deal with the problem that (1) assurance information is present at each lifecycle phase (e.g. concept, design, implementation, and V&V) and (2) multiple different tools can be involved at each phase, so the AMASS tool framework needs to interwork with each of these tools. One promising approach is to use OSLC [11], by extending it to assurance aspects (safety, security, etc.). As part of this work, the AMASS consortium plans to reuse existing results from the Crystal (http://www.crystal-artemis.eu/) and MBAT projects (http://www.mbat-artemis.eu/) for OSLC-based tool interoperability, since many of their partners are also in AMASS. The data models for tool integration will be also part of the AMASS CACM metamodel. In addition, further assurance and certification needs for the integrated information must be considered, e.g. traceability requirements and analysis of information completeness and consistency according to the applicable standards.

Collaborative Work Management. We mean supply chain and collaborative issues when developing, assuring and certifying CPS. AMASS needs to address aspects and needs such as DIA definition (ISO 26262 OEM-Supplier interaction definition), the development of a platform to exchange safety related information (potentially as cloud-based collaboration services, and private), issues related to information composition, versioning and update, security and scalability problems, and provision of server side services, e.g. intelligent search, cross project consistency checks.

Tool Quality Assessment and Characterization. The engineering of CPS increasingly relies on the use of tools that automate, replace, or supplement complex development and V&V tasks. CPS safety can be compromised if the tools fail. To mitigate

this risk, safety standards (e.g. DO-178C/DO330, IEC 61508, EN 501258, and ISO 26262) define tool qualification processes, including tool characterization. Compliance with these processes can be required for (re-)certification purposes, thus a system supplier can need to collect information about tool qualification and to provide this information as assurance evidence for the overall system certification process. Within SafeCer, a tool qualification process line was investigated in order to reduce time and cost via reuse. Within AMASS, this exploratory work will be deepened and broadened to consider also AMASS-related tool-chains.

3.4 Cross/Intra-Domain Reuse: the ubiquitous need for reuse

The higher complexity and size of CPS products combined with the growing market demand requires the industry to redefine its core and non-core activities, and to implement a coherent and systematic reuse strategy instead of relying exclusively on in-house-developed applications. For example, if the engine control computer from the automotive industry is to be reused in aerospace industry, the full certification process is applied as for a new product, thus reducing the return on investment of such decision. In such circumstances, systematic cross-domain reuse would be crucial to reduce the cost of re-certification. In circumstances where a new version of a product comes from a previously certified version of that same product, systematic intra-domain reuse would be crucial. Systematic intra-domain reuse would also be crucial in case of incremental certification (e.g., from a generic product to a specific one, obtained via addition of functionalities).

The OPENCOSS and SafeCer approaches aimed to reduce much of this repeated assurance effort, by promoting a flexible and systematic reuse approach that is fully cognizant of the similarities and differences between approaches to safety assurance across the main safety-critical system domains. In particular, on the one hand the CCL allows OPENCOSS tool users to model “equivalence maps” between different standards and regulations (including intra- and cross-domain) in order to facilitate reuse decisions between assurance projects from different application domains. On the other hand, safety-oriented process lines allow users to model process commonality and variability enabling systematic reuse.

While these approaches are a first proof of concept of cross- as well as intra-domain reuse and many safety-critical industries are convinced of the benefits to share some development with other industries, it first and foremost requires a common and strongly validated assurance and certification platform. This way, the certification results for a system or component originally developed for a different domain or for a different criticality level can be carried over to other domains. Also, a number of open technical aspects need further research:

Semantic Standards Equivalence Mapping. One obstacle to the cost-effective reuse of cross-domain assets is the fact that the terminology and semantics used to describe and manage assurance across different application domains are not consistent. For example, there is some degree of overlap between concepts such as ‘fault’, ‘hazard’ and ‘mishap’ and what constitutes a ‘component’ or a ‘subsystem’, but there are also gaps between the definitions of these concepts across the standards. OPENCOSS

started to solve this issue by using the CCL Vocabulary approach. The CCL Vocabulary is a structured and harmonised way to store and communicate knowledge about assurance artefacts and concerns. However, no complex, real cases were explored with this approach. Within SafeCer, an ontology-based method for process elements reuse was explored [12]. AMASS shall extend the CCL Vocabulary (though the AMASS CACM metamodel) approach by automating its creation and usage via deepened usage of the SafeCer ontology-based method. An automated CCL Vocabulary approach will also allow us to perform informed gap analysis on the standards and mitigate against the danger of inappropriate reuse where a given assurance asset does not appropriately match the requirements of the reuse context.

Cross-concern Reuse. In addition to mappings between standards related to the same concern, we need to identify mappings between standards that focus on different concerns in order to enable cross-concern reuse. It is well known for instance that the safety and security communities could be merged within a unified terminological framework under the dependability umbrella. This potential merge could foster the identification of commonalities and thus reusable artefacts.

Reuse Assistant (Cross/Intra-Domain). In addition to semantic mappings, we need to understand how the concepts work in terms of their relationship with one another to define the objectives of the standards – i.e. the intent which informs requirements and process activities, and the artefacts they result in -, in order to come to a clearer understanding of the role played by each activity and artefact in the overall assurance effort. AMASS will support users to understand whether reuse of the assurance assets is reasonable or determine what further analysis is required to justify claims of compliance. For example, AMASS will provide tool assistance to highlight the reasons why fault analysis is performed and the point in the development of the system at which it is applied (and hence the degree of detail involved). The compositional argument approach developed by SafeCer and OPENCOSS will evolve to get the ability to characterise pre-existing argument modules in terms of the intent of the applicable standards. This characterisation will rely on a clear understanding and statement of the assurance objectives of each standard, and of the assurance assets used to evince the claims made to demonstrate their satisfaction.

Product/Process/Assurance Case Line Specification. Variability management creates a pain in the industry. Various methods have been developed to manage variability and thus relieve industry from such a pain. For software, subversion and git are already an improvement to manage variability due to product evolution. Subversion, however, does not satisfy the management of all sources of variability. A systematic approach is needed to deal with software/hardware variability management, but also process and assurance case-related variability. The AMASS project will focus on extending and integrating the current methods in order to manage for instance ripple-effects that changes on product requirements might have on processes as well as assurance cases. The objective is to promote a fully integrated approach addressing the fundamental dimensions for certification purposes.

4 Conclusion

Despite the wide adoption of the concept of cyber-physical systems (CPS), its entrance in critical domains such as automotive, medical or aerospace is not advancing at the pace that the designers and producers would want in order to exploit the many benefits brought to these domains. While CPS can more efficiently react to changing requirements and adapt to different environments, these properties are challenging for the adoption in critical domains. Connectivity and complexity introduce new risks and extend potential risk causes towards security threats.

The validation and certification of the new-implemented solutions is the main barrier preventing this adoption. Critical domains present a long tradition of certification procedures and standards since the very early stages of software and systems engineering history. Unfortunately, this long history translates into complex validation procedures that require extensive testing and long certification campaigns, increasing the associated costs and preventing fast adoption of new concepts. In addition due to the isolation of critical systems validation, the certification focus was mainly restricted to safety and not threats from malicious causes. Furthermore, the increase in the complexity of the systems has been handled by extending exponentially the validation test campaigns.

The AMASS project brings a new vision into these assurance and certification procedures where extensive testing and validation and black box models are replaced by an intelligent approach based on the underlying architecture of the CPS system. The procedures will profit not only from previous certification results of pre-existing modules, but also from equivalent or similar architectures already validated.

This process of learning from similar architectures is performed more or less unconsciously by all the designers during early architectural design phases. All the designers and companies rely on a series of architectures that are well known “to work properly”. AMASS project will provide a systematic methodology and tooling to pass from this qualitative and intuitive approach into a formal validation procedure where the underlying architecture of the CPS to be certified plays a key role in defining and executing the validation process. AMASS will extend this approach to architectures with inherent safety and security properties. AMASS will bridge between safety and security validation and certification, and ease both.

AMASS will shape this approach in a complete toolset that will integrate all the experience and developments of previous projects such as OPENCOSS and SafeCer and extend it towards cybersecurity. The AMASS approach should allow to handle the changing system security over the product lifetime. A safe system is designed once and is not changed over the product lifetime. A secure system can change massively due to e.g. software updates and therefore also the security has to be ensured in these changing lifetime process. This toolset approach is a key element in the impact strategy, as it will reduce dramatically the entry barriers of new actors in the CPS business by providing them with a consistent and easy-to-use validation toolset that shall reduce their learning curves and increase their chances to perform a “right-first-time” validation of new CPS architectures.

To obtain the maximum impact from this new approach it is necessary that the proposed methodologies and tooling are perfectly aligned with both the industrial validation procedures and standards, and with the emerging architectures derived from cutting edge cyber-physical systems. Here is where the full potential of AMASS will develop. The project includes the complete value chain of actors involved in CPS validation procedures, from tool providers to industrial end users, including top-notch technological providers. This allows AMASS to identify the most commonly used architectures and those new emerging ones identified by the industry as the most promising ones, adapting the tools and procedures to them and therefore guaranteeing the applicability of the results in the domains included in the project, as well as easing its fast extension into those domains not included in the project.

References

1. AMASS ECSEL Project (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems); http://www.amass-ecsel.eu/
2. OPENCOSS FP7 Project (Open Platform for EvolutioNary Certification of Safety-critical Systems); http://www.opencoss-project.eu/
3. SafeCer ARTEMIS Project (Safety Certification of Software-Intensive Systems with Reusable Components); http://www.safecer.eu/
4. Ewen Denney and Ganesh Pai, "A Formal Basis for Safety Case Patterns", In Proceedings of the 32nd International Conference on Computer Safety, Reliability and Security (SafeComp '13), Toulouse, France, September 2013.
5. J. Rushby: Noninterference, Transitivity, and Channel-Control Security Policies. Tech. Report SRI-CSL-92-02, December 1992
6. Alessandro Cimatti, Michele Dorigatti, Stefano Tonetta: OCRA: A tool for checking the refinement of temporal contracts. ASE 2013: 702-705
7. Bock, H-H., Braband J., Milius, B. and Schäbe, H., Towards an IT Security Protection Profile for Safety-Related Communication in Railway Automation in F. Ortmeier and P. Daniel (eds), Computer Safety, Reliability and Security: Proceedings of SAFECOMP 2012, Lecture Notes in Computer Science vol 7612, Springer 2012, 137-148
8. http://www.d-mils.org/
9. M. Born, J. Favaro, M. Winkler, L. Heidt, and A. Boulanger "Integrated Design and Evaluation of Safety and Security in Automotive System Development", Proceedings VDA SYS 2015, 15-16 July 2015, Berlin.
10. A. Baldovin, A. Zovi, G. Nelissen, S. Puri, "The CONCERTO methodology for model-based development of the avionics software" Proc. of the Ada Europe Conference 2015 , June 2015, Madrid
11. Open Services for Lifecycle Collaboration(OSLC); http://open-services.net/
12. B. Gallina, Z. Szatmari. Ontology-based Identification of Commonalities and Variabilities among Safety Processes. Proceedings of the 16th International Conference on Product-Focused Software Process Improvement (PROFES), Springer, LNCS, Bolzano, Italy, December 2-4, 2015