Security and Safety Modelling in Embedded Systems

Silvia Mazzini, John Favaro, Alessandra Martelli, Laura Baracchi

Security and Safety Modelling in Embedded Systems

Silvia Mazzini,

John Favaro,

Alessandra Martelli,

Laura Baracchi

INTECS S.p.A.
Via Umberto Forti Trav. A, n.5
Polo di Attività Montacchiello, Loc. Ospedaletto
I-56121 Pisa, Italy
Silvia.Mazzini@intecs.it

Keywords: security, safety, embedded, certification, model

Congress Topics: Dependability: Safety, Security, Certification. Process, methods and tools: model-based system engineering.

Domain: embedded systems.

Abstract

The SESAMO project directly addresses the root causes of problems arising from the convergence of safety and security in embedded systems at architectural level, where subtle and poorly understood interactions between functional safety and security mechanisms impede system definition, development, certification, and accreditation procedures and standards. Intense market innovation is being held back by this root cause: the absence of a rigorous theoretical and practical understanding of safety and security feature interaction.

Introduction

SESAMO (Security and Safety Modelling in embedded systems) is an ARTEMIS JU Project begun in May 2012 and lasting three years, coordinated by Intecs S.p.A. SESAMO is developing a component-oriented design methodology based upon model-driven technology, which jointly addresses safety and security aspects and their interrelation for networked embedded systems in multiple domains (e.g., avionics, transportation, industrial control).

Safety and security have long been identified as two very important attributes of overall system dependability [AVIZ 2001]. The convergence of safety and security is happening everywhere in mission-critical embedded systems domains and today's methodologies are inadequately prepared for it. There are many subtle interactions and interdependencies among safety, Quality of Service (QoS) and security. Indeed absolute security is often less important than the quantifiable trade-offs between performance and security – as resource constraints may make it infeasible to guarantee absolute security in all circumstances. In addition, the introduction of security related considerations into embedded systems tends to invert the priorities of certain non-functional attributes. In traditional network Cybersecurity, confidentiality and integrity trump (that is, they are more important than) availability. But in embedded systems, it is invariably just the opposite: availability and integrity trump confidentiality. Furthermore, additional non-functional attributes of security come into play in the embedded area, including autonomy, timeliness, and isolation. Finally, in general, safety trumps security in the embedded area.

Making a system more secure can make it safer, e.g. by improving code quality to achieve a higher level of assurance. But making a system more secure can also make it less safe: for example, the authentication and authorisation might meet critical real time requirements in "most" cases, but not always, making it impossible to certify and use the system in a safety critical environment. Conversely, QoS constraints placed on systems by safety functions could preclude implementation of adequate security mechanisms, making the system unqualifiable for security critical use. In each case, not only are systems rendered inadequate in one or the other environment, but both the suppliers and users of the systems lose opportunities in a growing area of the mission-critical systems market.

Safety analysis techniques, both qualitative and quantitative, have been developed over the years and are now deployed. On the other hand, the development of quantitative security analysis techniques has been only recently investigated with

significant effort. We need to progress on both quantitative aspects of security analysis and the integrated quantitative and qualitative analysis and design of safety and security. These involve at least specification methods able to cope with both aspects from requirements elicitation to system design and analysis. We need thus an enriched language able to deal both with security aspects, such as cryptography modelling, and probabilistic/stochastic ones, including those for describing performance. Similarly we need an integrated validation framework that permits the use of multiple evaluation techniques in an organized manner. One can then consider both orthogonal analysis approaches, where one aspect is considered after the other, as well as fully composite ones, where all the aspects are considered (optimized when necessary) at once.

On a system level, the safety and security properties and concepts differ and means potentially collide when designing dependable systems for safety and security. For a start, assumptions between classical safety and security environments have traditionally been different as exemplarily depicted in the following table.

"Classical Safety-Oriented Dependability" versus "Classical Security"	
Safety	**Security**
Assumes trustworthy operators	Assumes fault free system
Assumes closed system	Assumes open connected system
Assumes time response from dedicated resources	Assumes shared generic platform

Furthermore, the technical means to achieve dependable operation in safety and security have been different, although some concepts have deceptively similar names. Consider the example of ensuring avoidance of altering or disclosure of information. In the safety world, the goal is to use error detection codes that maximize the so-called "Hamming distance" (the minimum distance between encoded words) to avoid unrecognized corruption of data. In the security world, encryption uses the same mathematical basis, but the goal is to *minimize* the Hamming distance and equally distribute code words over the available code space (in order to not disclose and protect change of any information). So a very good error detection code cannot be very secure at the same time. The following table lists some similarities with slightly different approaches to address either safety or security.

Concepts: "Classical" Safety-Oriented Dependability versus "Classical Security"		
Safety	**addresses**	**Security**
Partitioning (independent redundant channel)	Avoidance	Partitioning (firewalls / router filters; VPNs)
Design audits (code reviews / testing)		Design audits (open source code)
Redundancy (multiple nodes and channels)		
Selection of redundant channels (voters / selectors)		Selection of actors (authentication)
Error detection codes		Encryption
Parameter monitoring / limit checks	Sensing	Traffic monitoring
		Signature checks
		Anomaly checks
System diagnostics / mutual test	Correlation	Intrusion state estimation
Fail-silent shutdown of redundant node or channel	Isolation	Rerouting (router filtering, IP shunning); host shutdown
Fault masking	Recovery	Rerouting (routing filtering, IP shunning); host shutdown
Reboot	Repair	Backup site
Hardware repair		Scrub and re-install

As we have seen in the past, in the development of real world systems it is not possible to simply test systems in order to find such subtle issues of safety and security feature interaction. It is necessary to develop systems from the beginning to meet such joint requirements. Model based approaches offer a promising avenue to handling the emergent aspects of safety and security in a technologically and methodologically sound fashion. Through the appropriate application of constraints on the way in which systems are constructed and executed (the so-called *computational model* of a system), it becomes possible to construct systems with the properties of *composability* (that is, they can be

constructed from reusable parts that retain their individual properties when combined into larger systems) and *compositionality* (that is, the overall emergent properties of the system constructed under these appropriate constraints can be deduced from the individual properties of its parts). Such approaches offer the promise of a major advance not only in the way that systems are constructed but also in the way that they are accredited and certified (at the part level rather than only at the system level). Thus, a main objective of SESAMO is to provide a model-driven process for the compositional development of safety and security critical systems, by allowing modelling and reasoning about systems at different abstraction levels.

Building blocks

One important activity in SESAMO is the identification of a sufficiently large and useful set of mechanisms for safety and security that can form *building blocks* to be used in the construction of systems in the domain of interest to resolve (or balance) conflicts inherent in safe and secure system development. This is the constructive aspect of SESAMO. The term "building block" has been used within the project in a broad sense, in order not to prejudice the identification of mechanisms of all types. Bringing their background and experience to bear upon the activity, consortium members have identified and contributed building blocks of different levels of granularity. Some are large, architectural level building blocks such as:

- Time and space partitioning;
- Virtualisation;
- Redundancy / Diversity of architectural components.

Others are smaller, more specific building blocks, including:

- Signature generation and verification;
- Protocols and monitoring;
- Encryption / decryption;
- Plausibility checks.

Still others are process building blocks, such as joint safety and security FMEA. They are being classified within the project with respect to their safety aspects, security aspects, and most importantly, their characteristics that lead to either synergies or conflicts between safety and security.

Analysis methods

A further important activity is the identification and description of analysis and assessment techniques suitable for supporting the analysis of systems constructed using the building blocks and integrated methodological approach and tool chain of SESAMO, as well as their assessment according to current requirements or those to be recommended by the consortium as a result of the project work. It is viewed as a continuation of the constructive aspect of SESAMO, whereby building blocks are accompanied by contextual analysis of both qualitative and quantitative types. Without analysis, the enabling mechanisms – the building blocks – of SESAMO are useless for certification or accreditation.

An example of a technical analysis technique under study is a *quality calculus*, from the Technical University of Denmark [NIEL 2012], for which a type system has been developed for checking the extent to which safety and security goals have been met in the system under analysis. To deal with conflicting safety and security goals, the calculus has been extended with a primitive for "endorsing" data to a higher trust level (accepting violations of the explicit flow) to explore the effects of relaxing security in controlled situations, thereby lowering costs. The calculus has been applied to a realistic automotive engineering scenario in which the CD-player is used not only for playing music (a non-critical context) but also for updating the functionality of the car (a critical context).

An example of an analysis technique under study under the lead of SESAMO partner Adelard with an eye toward assessment and certification is *security-informed safety cases* (see [ASCE 2013] and [PAUL 2012]). The use of safety cases in the context of safety-related assessment is a well proven approach in several domains now, from nuclear to railway to automotive. In the context of safety and security related systems, we believe that an effective approach is to enhance the existing safety case methodology and use it to demonstrate and communicate security requirements in addition to safety. In this way we can benefit from a mature, effective and time-tested safety case approach and have both safety and security properties considered in an integrated manner within a security-informed safety case. This approach should also give us a better understanding of the interactions between system safety and security aspects and help us to address the potential issues associated with their interrelation.

Decision support

It is a premise of SESAMO that safety and security cannot always be reconciled in a perfect "win-win" manner. The elaboration of decision support strategies is a natural consequence of this premise. To date there has not been a significant amount of structured work in analyzing the trade-offs between safety and security, and some of the work in the project is aimed at establishing a firm basis for decision support development.

Reaching over to results in the economic domain, one activity in this area currently being pursued in the project is the exploration of *Pareto frontiers*, where the balance between security and safety can be seen as a multiple criteria optimization problem that can be approached by Pareto optimality (that is, the design space is characterized as involving multiple criteria while achieving overall optimal use of resources such that no further improvements can be made without penalizing one of the parameters). A quantitative approach is being investigated that introduces probabilities and metrics, as well as quantitative verification using stochastic model checking. [NIEL 2013]

In our opinion, equally important as the quantitative aspect of decision support is the qualitative aspect represented by the different safety and security cultures, which have potentially clashing value systems. For example, it is commonly stated in the safety community – well represented in the SESAMO consortium – that during a crisis, safety takes precedence over security. Within the consortium, there is also a strong security community, which notes that authenticity must also be given its due within a combined safety/security context; it would be imprudent, they argue, not to check that orders to change course do in fact originate from authorised sources rather than intruders. The existence of qualified and robust safety and security cultures within the SESAMO consortium is providing an important opportunity to explore this interaction among cultural value systems that is also a strong factor within any framework for decision support. It is also a strong factor in any examination of a joint methodological approach to safety and security related development.

A Combined Methodology?

The safety community in particular has established standards in a number of domains governing safety-related embedded systems development, including avionics (e.g. [DO-178C]), railway (e.g. [EN 2010]), and the automotive industry (e.g. [ISO 2011]). A number of security related standards have also been developed, such as ISO 27002 [ISO 2013] establishing guidelines for information security management in an organization, IEC 62443 for industrial communication networks [IEC 2013], and the ISO/IEC 15408 Common Criteria [IEC 2009] for security assurance.

Given the importance of both safety and security in mission-critical systems, it is natural to consider the inclusion of both within a single standard. But to date there has been little cross-fertilization between the safety and security communities developing these standards [PIET 2012]. Even the vocabulary used in the two communities is often confusing and contradictory [PIET 2010]. Thus, incorporating security requirements into safety related standards (and vice versa) has been extremely challenging to date.

Nevertheless, an increasing amount of activity is becoming evident, both in the technical community (e.g. [HANS 2009], [REIC 2012]) and in the standardization committees, reflecting the increasing need within the embedded systems industry. An example in standardization is the latest version of IEC 61508 [IEC 2010], the domain-independent safety standard for electrical and electronic systems. In its latest edition, it introduces for the first time requirements related to security. Clause 1.2 k) of Part 1 of the standard " … requires malevolent and unauthorised actions to be considered during hazard and risk analysis …"

This opens the door to the integration of security requirements also into the domain specific safety standards for which it serves as the "mother" standard. This has process already begun: for example, Draft EN 50126-5:2012 states that "… the Safety Case shall demonstrate that […] misuse-based failures on external interfaces do not adversely impact on the safety integrity of the system."

However, this "opening" is in at least one respect less a door than a Pandora's Box. Once the step is taken of including both types of requirements in a standard, a much more difficult problem comes into the foreground: the process. Mature development processes for safety related embedded systems have existed for years, and lifecycle activities for security related development (e.g. [HOW 2006]) have also been defined. But the integration of safety and security related development processes has been a controversial topic.

A case in point is the automotive safety standard ISO26262 [ISO 2011], another of the domain-specific "children" of the generic IEC61508 standard. In 2013, the ISO26262 standardization committee (ISO TC22/SC3/WG16) began to debate the inclusion of security related considerations in the standard. During the debate, a strong position was presented that security and safety are very different areas, requiring different skills, and that the respective processes must remain separate (see also [CZER 2012]). This position argued that, rather than including specific security

requirements in the standard, *interaction points* between the two (separate) processes be identified, and requirements defined to establish appropriate communication channels. Another position presented preliminary ideas for what could happen at the interaction points, such as combining FMEA with security analysis (e.g. by adding failure modes to the FMEA representing security attacks).

This concept of establishing points of contact between parallel safety and security lifecycle activities is also more or less in line with the approach being taken within the EUROCAE/RTCA community, where ongoing work is examining the addition of security related activities to the heavily safety-oriented ARP4754 system development process [ARP 2010].

The SESAMO approach is proceeding along these lines. Figure 1 illustrates how SESAMO positions itself within this scheme.

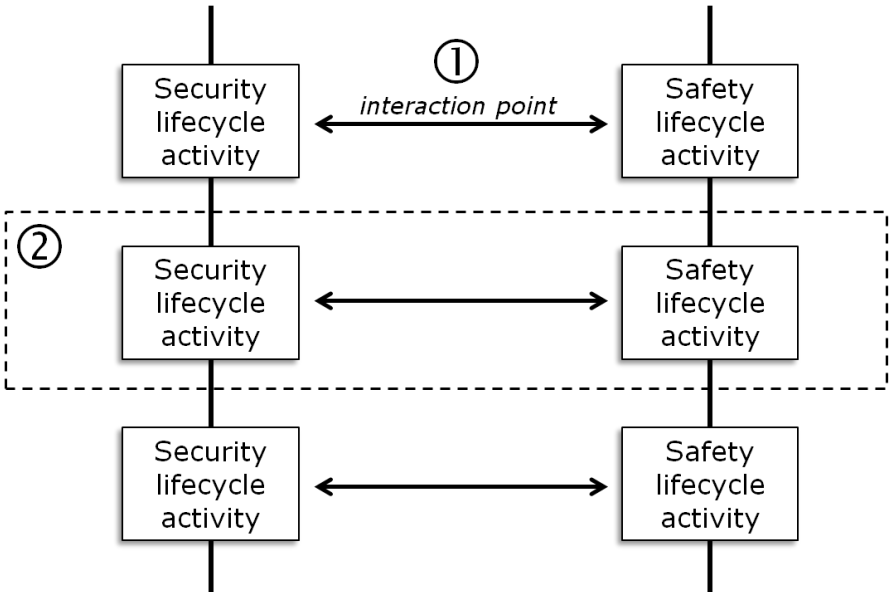

Figure 1: Safety and security lifecycle activities

Two types of SESAMO intervention can be identified:

1. *Trade-off analyses at the interaction points*. These are particularly relevant for those lifecycle activities and mechanisms that tend to be purely safety or security related. For example, cryptography and authentication is squarely in the security domain. The analysis methods developed in SESAMO can make it possible during communication at the interaction points to judge the effects of the activities in each parallel process on the other, and to provide appropriate decision support based on the results. Note that this tends to concern the building blocks that are architectural in nature.
2. *Joint lifecycle activities*. This is a deeper intervention, where the lifecycle activities are actually combined, such as joint hazard and threat analysis, or joint FMEA and attack analysis. Note that this tends to concern the process building blocks rather than the architectural building blocks – but it is not always the case. For example, a "redundancy" building block (and its accompanying analysis methods) could be instrumental in a joint safe and secure architectural design activity.

An important point to observe is that the SESAMO approach assumes that, although the processes are parallel, they are working on a single set of workproducts: the two types of intervention described above are intended to support the development of this single set of workproducts with the appropriate set of safety and security attributes.

The approach of parallel processes with "weak" trade-off interactions and "strong" interactions for joint activities has the advantage of providing a smooth migration path, starting from the separate processes of today and gradually identifying and implementing architectural and process building blocks that promote an ever-closer integration of the processes, while continuously approaching the Holy Grail of a fully integrated process.

Tool Support

A model-based approach to tool support for the integrated SESAMO safety and security methodology is being taken. The elaboration of a cross-domain tool chain has been organized as a bottom-up process, involving first an examination of the tools made available by the consortium partners for their relevant characteristics. These relevant characteristics might be either domain-specific (e.g. automotive) or technique-specific (e.g. assurance management). Secondly, the possibilities for integration of the individual tools are being explored, often in a pair-wise manner, in order to arrive at an understanding of the overall possibilities for integration. As a specific example of the model-based approach being pursued in the project, the pair-wise integration of two toolsets is presented in the following.

The *medini analyze* toolset [IKV 2013] has been developed for the automotive domain, and supports a high level of process integration for the ISO26262 safety standard. Possibilities have been identified for the integration of security-related activities including threat analysis, attack trees, security FMEA, and security informed safety cases.

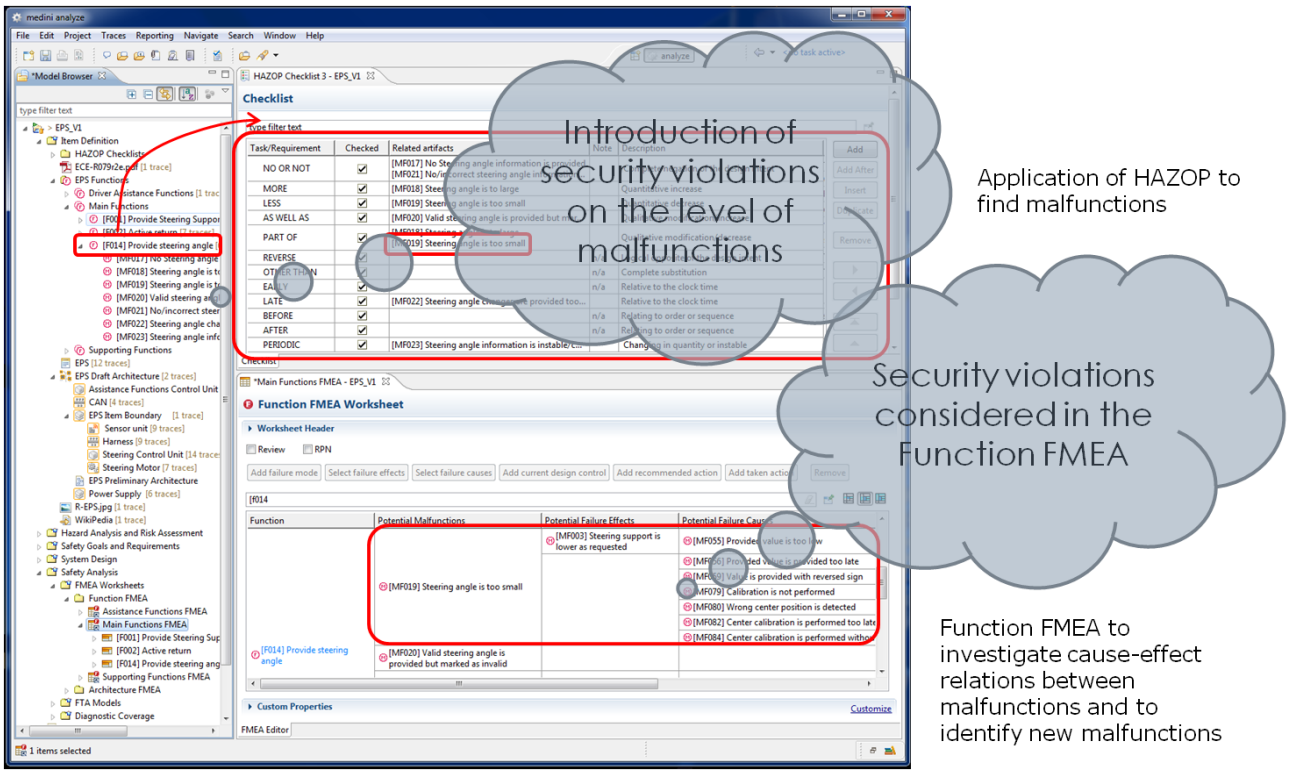

Figure 2: Integration of security related activities in *medini analyze* (*Source: ikv++*)

Figure 2 illustrates the integration of facilities for integrating the consideration of security violations as malfunctions, which allows them to be treated in a harmonious fashion alongside safety related malfunctions in further lifecycle activities. For example, also illustrated is the incorporation of the security violations into the FMEA, to create the type of joint lifecycle activity described in the previous section on the methodology.

Another toolset available for integration into the SESAMO toolchain is CHESS [CHES 2013], an Eclipse-based framework that supports a domain-independent process for general model-based, dependability-related development. Its UML metamodel based profile is extensible to relevant SESAMO concepts. CHESS has particularly well developed facilities for schedulability and dependability analysis, which can support the analysis and trade-off techniques being elaborated in SESAMO. Thus, a pair-wise integration with *medini analyze* has been undertaken to cover the development lifecycle using the most appropriate tool for each phase. *Medini analyze* is used for the system design, safety and security management, risk/hazard analysis, ASIL association, etc. CHESS is used for software design, schedulability/dependability analysis, trade-off analysis, and code generation. Figure 3 illustrates the process, as explained in the following.

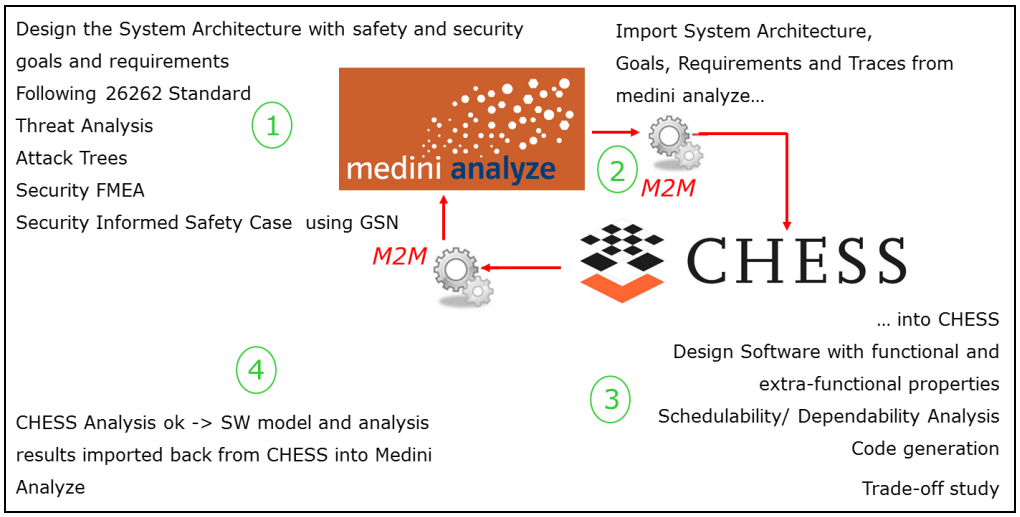

Figure 3: *medini analyze* / CHESS process

1. The safety related activities of the ISO26262 development process are followed, enhanced by security related activities as discussed in the previous section on methodology (whereby some joint activities such as security and safety FMEA are carried out). Note also the reference to joint safety and security activities for the elaboration of a security informed safety case using the Goal Structured Notation (GSN) facilities provided by the ASCE tool of consortium partner Adelard [ASCE 2013].

2. *Medini analyze* SysML based models representing the system architecture and requirements are imported into CHESS in the System View and Requirements View respectively, using Model-to-Model (M2M) transformations written in the Operational QVT language [QVT 2013]. An import facility was created in CHESS for this purpose (Figure 4) and the CHESS profile was extended with SysML stereotypes to represent Medini elements (such as controllers, actuators and sensors) and to include specific safety/security related properties (such as ASIL information).

3. The software modelling process proceeds in CHESS, where the software is designed and elements in the software model are linked to system level architectural elements and requirements, thus providing support for system and software co-engineering. In preparation for trade-off analysis (e.g. the effect of cryptographic mechanisms on system schedulability), real-time properties are specified and schedulability analysis is launched in CHESS. Schedulability analysis is executed by the MAST tool (Modelling and Analysis Suite for Real-Time Applications) developed by CHESS partner University of Cantabria [MAST 2013]. Based upon the results of the analysis, the best solution may be chosen for code generation. Alternatively, the user may return to the *medini analyze* environment for further development as described in the next step.

4. The software models and analysis results are imported back into *medini analyze*, through another Model-To-Model transformation. As noted above, the results of the analysis may lead to necessary changes in the architecture or in the mechanisms used in the architecture (e.g. weakening of the cryptographic mechanisms in order to permit the safety-related scheduling deadlines to be respected).

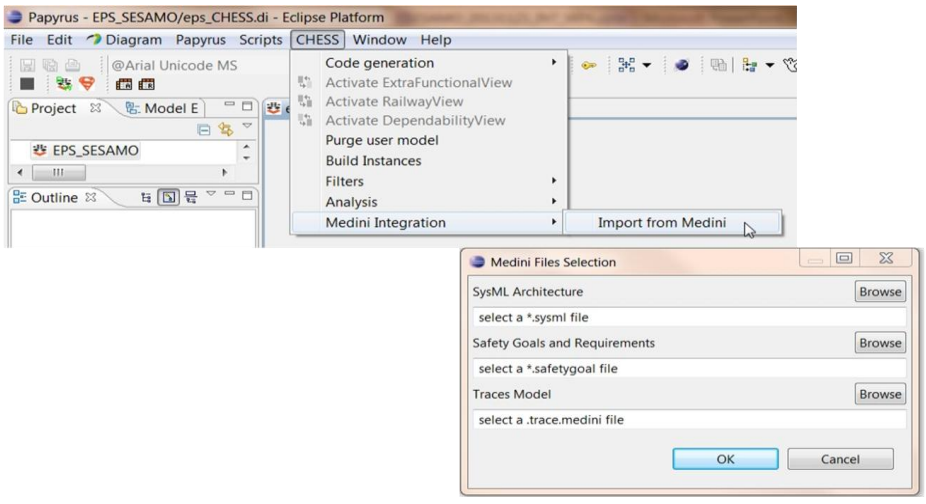

Figure 4: Import of *medini analyze* models into CHESS

Conclusions

Key elements of the SESAMO approach are:

- a methodology to reduce interdependencies between safety and security mechanisms and to jointly ensure their properties;
- constructive elements for the implementation of safe and secure systems;
- procedures for integrated analysis of safety and security;
- an overall design methodology and tool chain that utilize the constructive elements and integrated analysis procedures to ensure that safety and security are intrinsic characteristics of the system.

The relevance of the SESAMO results is guaranteed by the involvement of large partners with significant economic interests in safety and security critical systems in several domains, a sound group of technology providers (including SMEs) and prestigious research entities (academia and institutes) with deep and complementary multi-domain expertise.
The characterisation and assessment of the applicability of SESAMO results from a multiple domain industrial perspective is based on elaboration of the following use cases:

- integrated modular avionics,
- motor control in automotive and industrial environments,
- car infotainment system,
- safe & secure communication in railway and medical applications,
- smart-grid security,
- security of SCADA systems in oil and gas refineries.

SESAMO has also adopted an instrument of consultancy to ensure the maximum impact possible within the communities of potential end users: the SESAMO Expert Advisory Board (EAB), consisting of important industrial organisations external to the project with significant activity and needs in the key areas addressed by SESAMO.

Mid-term results have been presented to the EAB in a public event, the 1st SESAMO Industrial Day in Vienna on November 20th 2013, where the challenges of the project objectives and results have been recognised, positive feedback as well as useful hints and challenging guidelines for future work have been collected. Final results are expected by the end of 2014.

Acknowledgements

The work presented is based on the results of the ARTEMIS SESAMO Project, Grant Agreement 295354. The authors would like to thank all the members of the consortium for their contributions to the results described therein.

References

[ASCE 2013] Adelard LLC. ASCE. http://www.adelard.com/asce/. Accessed 9 December 2013.

[ARP 2010] S-18 Aircraft and System Development and Safety Assessment Committee. Guidelines for Development of Civil Aircraft and Systems. Revision A. 21 December 2010.

[AVIZ 2001] Avizienis, A., Laprie, J.-C., and Randell, B., Fundamental Concepts of Dependability, Technical Report 739, pp. 1-21, Department of Computing Science, University of Newcastle upon Tyne, 2001.

[CHES 2013] ARTEMIS – JU CHESS Project. http://www.chess-project.org. Accessed 9 December 2013.

[CZER 2012] Czerny, B., Towards a System Security Engineering Process for Automotive Embedded Control Systems, 30th International System Safety Conference, Atlanta, 6-12 August 2012.

[EN 2010] CSN EN 50159 Railway applications – Communication, signalling and processing systems– Safety-related communication in transmission systems. 2010.

[HANS 2009] Hansen, K. Security attack analysis of safety systems, the IEEE Conference on Emerging Technologies & Factory Automation, 22-25 Sept., 2009, pp. 1-4.

[HOW 2006] Howard, M. and Lipner, S. The Security Development Lifecycle, Microsoft Press, Redmond, Washington, 2006.

[IEC 2009] ISO/IEC 15408:2009. Information technology – Security techniques – Evaluation criteria for IT security.

[IEC 2010] IEC 61508, Ed. 2.0 (2010), Part 1 – 7, "Functional Safety of E/E/PE safety-related Systems", 2010.

[IEC 2013] IEC 62443. Security for industrial automation and control systems–Network and system security, standardization work in progress.

[IKV 2013] ikv++ Technologies, *medini analyze*. http://www.ikv.de/index.php/en/products/functional-safety. Accessed 9 December 2013.

[ISO 2013] ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security management.

[ISO 2011] ISO 26262:2011, Part 1- 9, “Road vehicles – functional safety”.

[MAST 2013] University of Cantabria. Modelling and Analysis Suite for Real-Time Applications. http://mast.unican.es/. Accessed 9 December 2013.

[NIEL 2012] Nielson, H-R., Nielson, F., Vigo, R. A Calculus for Quality. Formal Aspects of Component Software. Lecture Notes in Computer Science, Volume 7684, 2013, pp 188-204.

[NIEL 2013] Nielson, H-R., Nielson, F. Safety versus Security in the Quality Calculus. Theories of Programming and Formal Methods. Lecture Notes in Computer Science Volume 8051, 2013, pp 285-303.

[PAUL 2012] Paulitsch, M., Reiger, R., Strigini, L., Bloomfield, R. Evidence-Based Security in Aerospace: From Safety to Security and Back Again. 2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW 2012). Dallas. 27-30 November 2012.

[PIET 2010] Pietre-Cambacedes, L. and C. Chaudet, C. The SEMA referential framework: Avoiding ambiguities in the terms “security” and “safety”, International Journal of Critical Infrastructure Protection, Vol. 3 Issue 2, pp. 55-66, July 2010.

[PIET 2012] Pietre-Cambacedes, L., Bouissou, M., Cross-fertilizations between safety and security engineering, Reliability Engineering & System Safety, 2012.

[QVT 2013] QVT Operational Language. http://projects.eclipse.org/projects/modeling.mmt.qvt-oml. Accessed 9 December 2013.

[REIC 2012] Reichenbach, F., Endresen, J., Chowdhury, M., Rossebø, J. A pragmatic Approach on Combined Safety and Security Risk Analysis, IEEE 23rd International Symposium on Software Reliability Engineering Workshops, 2012.

[RTCA 2011] Radio Technical Commission for Aeronautics. DO-178C: Software Considerations in Airborne Systems and Equipment Certification, 2011.