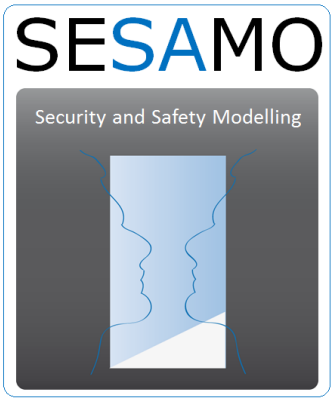

Security and Safety Modelling

Artemis JU Grant Agreement no.: 295354

D5.3 - Use Case Evaluation (Preliminary)
Version 1.0

20 May 2014

Final

Dissemination level: PU

Contributing partners
AKH, FTW, UC, PSA, SYSGO, IKV, ESY, IFAG, EADS IW Ge, EDF, SYSGO-CZ, SAG, GM

Project Partners:
Intecs, Institute of Informatics and Telematics - CNR, AKHELA, Università degli Studi di Roma La Sapienza, Technical University of Denmark, FTW Forschungszentrum Telekommunikation Wien, Adelard, UniControls, Czech Technical University in Prague, PSA Peugeot Citroën, SYSGO, ikv++ Technologies, eesy-id, Infineon Technologies AG Deutschland, EADS DEUTSCHLAND, Électricité de France, SYSGO s.r.o., Siemens AG Österreich, City University London - Centre for Software Reliability, General Motors Research & Development

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES


SESAMO
Security and Safety Modelling

1 INTRODUCTION

1.1 TECHNICAL CONTEXT AND OBJECTIVES

This document *D5.3 - Use Case Evaluation (Preliminary)* is the second delivery of SESAMO's WP5, which summarizes all activities related to use case modeling, implementation and evaluation.

WP5 addresses the following two overall objectives:

1. Modelling and implementation of defined use cases with the SESAMO tool chain;
2. Evaluation of improvements and advantages/disadvantages.

This specific report relates to the second objective.

This preliminary version of the document, which is an output of Task 5.3, is based on an evaluation of the preliminary results of task *T5.1 - Use Case Demonstrator Development*, which are presented in Deliverable *D5.1 - Use Case Demonstrator Development (Preliminary).* It is to be read as the result of the first round of an on-going evaluation and will be used as input for the final implementation phase of the tool chain in Task 4.2. The final results of the evaluation will be presented at the end of the project (M36) within Deliverable *D5.4 - Use Case Evaluation (Final).*

Within SESAMO a set of eight very different domain specific use cases are used as a test environment for the integrated safety and security approach. According to the nature of the project each use case is contributed by one of the industrial partners as an example, which is then elaborated together with one or more solution providers. Table 1-1 shows all the use cases and the involved partners.

Use Case	Industrial Owner	Solution Providers
Avionics	EADS	SYSGO, ADEL, CITY, DTU
Car Infotainment	PSA	EDF
Industrial Drive	SAG	IKV, INTECS, CITY
Automotive E-Motor	IFAG	IKV, CITY, CTU, EDF, INTECS
Oil & Gas	AKH	CITY, IKV
Medical	IFAG	ESY, IIT-CNR, CITY
Railway Communication	UC	DTU, FTW, INTECS, DICEA, SYSGO
Smart Grid	EDF	FTW

Table 1-1: List of use cases

The great variety in the use cases is a big strength of the project, although this complicates any overall and general evaluation, particularly since their respective technical focuses and states of completeness, after only five months of work in WP5, are very different.

The crucial issue for a meaningful evaluation is the definition of suitable success metrics that are taken into consideration. Naturally any uniform metric will fit the individual use cases to a greater or lesser extent.

The development of quantitative metrics for the evaluation of project success is generally difficult and often sensitive to the technical domain, potentially revealing competitive information. Long-term metrics are often measured for

- Project productivity;
- Adoption across projects;
- Individual system performance.

Such metrics, as discussed above, can lead into commercially sensitive areas, and in any case can involve analysis that goes beyond the resources of the project. Other metrics that require less implementation effort include:

- Degree of automation achieved with respect to current baseline;
- Cost of training against benefit of application.

In enable comparison amongst the use cases, the evaluation approach taken in SESAMO tries to combine quantitative measures and qualitative measures focusing on four areas:

- Fulfilment of the use case specific requirements;
- Effectiveness of safety-security conflict resolution within the use case;
- Reduction in accreditation efforts;
- Benefits of tool support.

1.2 DOCUMENT STRUCTURE

Following this concept, a set of six evaluation criteria was defined in order to evaluate all use cases. They are presented in *Section 2, Definition of the Success Metrics*.

For all use cases an initial evaluation was conducted and the results are presented within SESAMO deliverable *D5.5 - Use Case Evaluation (Preliminary, Confidential).*

The individual results were combined and totals are presented and discussed in section 3.
Due to the nature of the criteria, only the first three (relatively quantitative) criteria could be evaluated for all use cases, resulting in an overall count. For the remaining, relatively qualitative criteria, only individual statements are given.

A final conclusion after the first evaluation cycle is drawn in section 4.

2 DEFINITION OF THE SUCCESS METRICS

The following set of success indicators has been derived directly from an examination of the industrial benefits expected from SESAMO. They are realistic and applicable with an acceptable relationship of implementation effort versus information benefit. The achievement of the success metrics defined below will be assessed and evaluated throughout the development of the SESAMO use cases.

The metrics cover the entire set of seven objectives of SESAMO, and is realistic both in terms of the achievable targets and in terms of their measurability.

2.1 CRITERION 1:

Percentage of safety / security related requirements that can be captured at model level (with SESAMO tool chain) against the total set of such requirements known to be applicable to the specific SESAMO use cases specified in deliverable D1.1. The goal is 100%, whereby the success threshold for SESAMO is considered to be 60%. This is considered to be a realistic threshold within the scope of the project due to a number of challenging modeling issues to be addressed in the project (e.g. capture of safety-related performance requirements such as "… must be accomplished in x msec." and analogous obstacles to security requirements modeling).

2.2 CRITERION 2:

Percentage of unresolved safety and security related conflicts in relationship to overall safety and security related architecture in end product developed in the use cases (similar to metrics in existing standards that measure percentage of certain types of failures in overall product architectures). The goal is reduction to 1%, whereby the success threshold for SESAMO is considered to be 10%.
The safety and security related conflicts are determined by analyzing the safety and security related requirements of the specific SESAMO use case (specified in deliverable D1.1). A conflict is found, if a safety related requirement is in contrast to a security related requirement.
These conflicts will be classified into unresolved and resolved conflicts. A conflict is classified as "resolved", if a SESAMO safety and security balanced mechanism exists (specified in deliverable D2.2), which provides a tradeoff between safety and security requirement.
This criterion measures the percentage of unresolved conflicts in relationship to all safety and security conflicts.

2.3 CRITERION 3:

Percentage of unresolved safety and security related conflicts caused by problems or errors that should have been prevented or captured by the SESAMO tool chain and methodology (as opposed to conceptual errors made by the user that could not be prevented by any tool). The goal is 1%, whereby the SESAMO success threshold is defined as 5%.
The unresolved conflicts/errors (found in criterion 2) are categorized into two types of conflicts/errors. The first type comprises all conflicts/errors that could be found by a tool. The second type comprises all other conflicts/errors (e.g. conceptual errors).
This criterion measures the percentage of unresolved conflicts (first type of conflicts) that could have been found theoretically by a tool chain in relationship to all safety and security conflicts.

2.4 CRITERION 4:

Percentage improvement of safety and security related architectural definition automation through the methodology and tool chain. The goal is 60%, whereby the threshold for SESAMO is set to 40%. Ideally, the degree of automation of the architectural definition should be fully aligned with the first metric defined above ("if it can be modeled, it can be automated"). In practice, the degree of automation tends to lag behind the modeling because of the need to manage more implementation-related details.

2.5 CRITERION 5:

Percentage improvement of safety and security related accreditation automation through the methodology and tool chain. The goal is 25%, whereby the threshold for SESAMO is set to 10%. (This metric depends heavily on non-technical factors such as the degree of success in modifying standards to accept automatically produced accreditation documentation.).

2.6 CRITERION 6:

Percentage improvement in integration of the safety and security related tool chain, whereby the integration is measured through the reduction of manual intervention required between tools. The goal is 100%, whereby the SESAMO success threshold is set to 70%.

3 OVERALL EVALUATION

3.1 CRITERION 1:

After combining all the individual results of the use cases the average requirement coverage is calculated as presented in Table 3-1 and Figure 3-1. To give every use case the same weight the average of the percentage value was considered instead of calculating it out of the sum of resolved and unresolved requirements. With an average percentage 80% the anticipated threshold of 60% for criterion 1 is already reached.

Criterion 1	Number of total requirements of use case	Number of requirements, which can be captured at	Percentage
Industrial Drive	41	34	83%
Automotive E-Motor	12	10	83%
Car Infotainment	4	4	100%
Medical	12	9	75%
Railway	13	12	92%
Oil & Gas	16	14	88%
Avionics	26	20	77%
Smart Grid	12	7	58%
Average	**136**	**110**	**82%**
Goal			**60%**

Table 3-1: Overall Evaluation Criterion 1 table

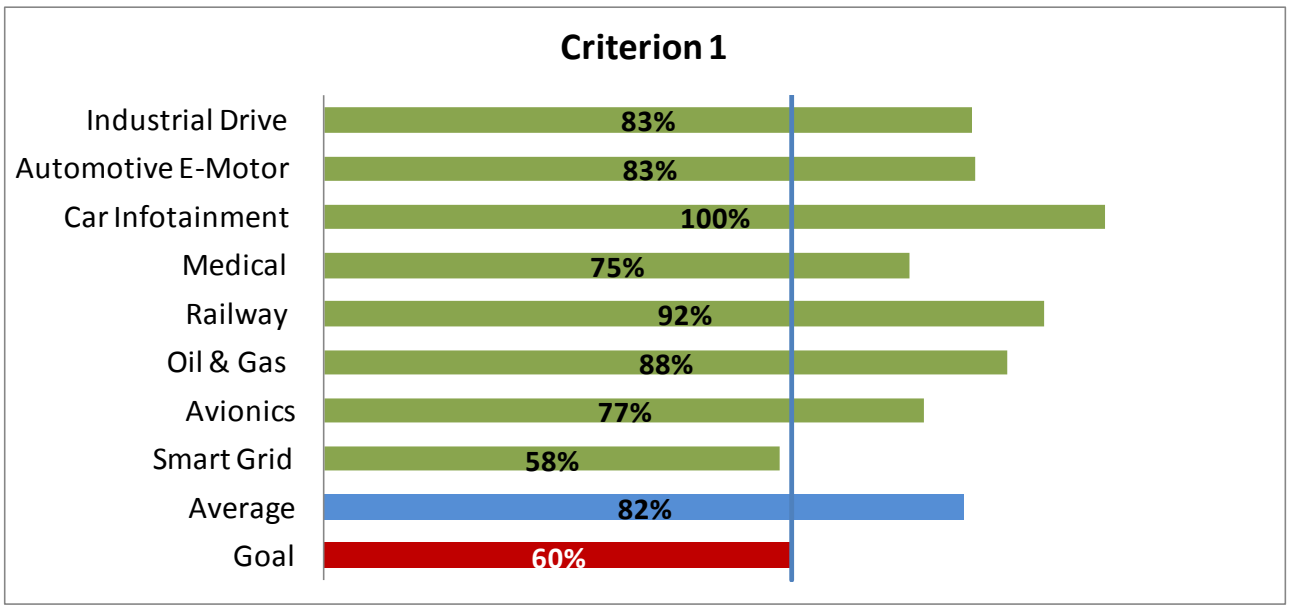

Figure 3-1: Overall Evaluation Criterion 1 Graph

3.2 CRITERION 2:

After combining all the individual results of the use cases the average requirement coverage is calculated as presented in Table 3-3 and Figure 3-3. The average percentage over all use cases is 38% while the SESAMO goal was defined by 10%. The table clearly shows one obvious weakness of the approach, which results from the differing number of requirements per use case. For industrial drives, 41 requirements are considered while for car infotainment there are only four requirements. Obviously, the number of high-level requirements considered limits the number of potential conflicts. For most use cases, only a small number of conflicts were already visible from the top-level perspective. It is worth noting that for some use cases where the requirements were defined at a lower level, a significant number of conflicts could be identified.

Criterion 2	Number of overall safety and security related conflicts	Number of unresolved safety and security related conflicts	Percentage
Industrial Drive	28	11	39%
Automotive E-Motor	10	8	80%
Car Infotainment	1	0	0%
Medical	7	3	43%
Railway Communication	1	0	0%
Oil & Gas	4	3	75%
Avionics	3	2	67%
Smart Grid	1	0	0%
Overall	**55**	**27**	**38%**
Goal			**10%**

Table 3-2: Overall Evaluation Criterion 2 table

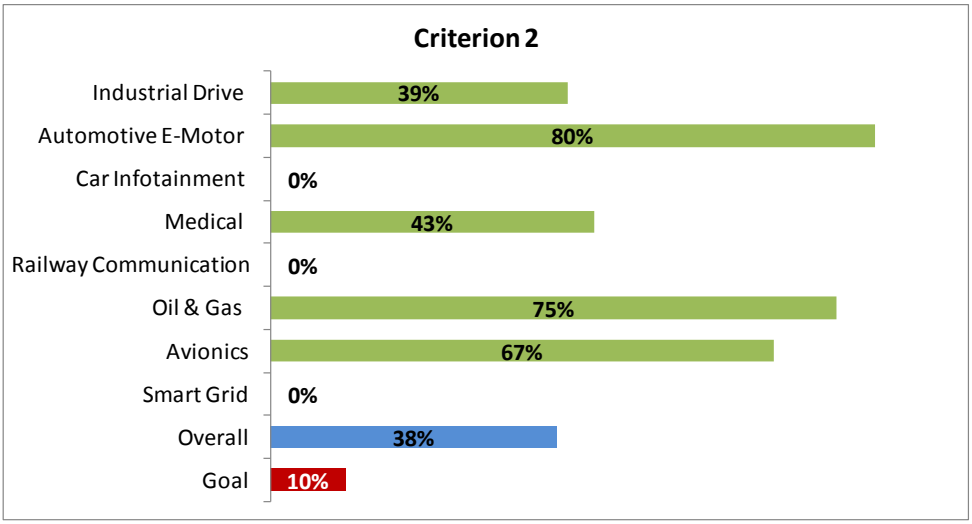

Figure 3-2: Overall Evaluation Criterion 2 Graph

3.3 CRITERION 3:

The next metric is very similar to the previous. The only difference is that conflicts that are systematic and therefore cannot be solved by any method are not taken into consideration. This approach reduces the unresolved conflicts and gives an average of 30% unresolved conflicts that could have been solved, where the goal was set to 5%.

Criterion 3	Number of overall safety and security related conflicts	Number of unresolved safety and security related conflicts	Percentage
Industrial Drive	28	2	7%
Automotive E-Motor	10	7	70%
Car Infotainment	1	0	0%
Medical	10	2	20%
Railway Communication	2	0	0%
Oil & Gas	4	3	75%
Avionics	3	2	67%
Smart Grid	1	0	0%
Overall	**59**	**16**	**30%**
Goal			**5%**

Table 3-3: Overall Evaluation Criterion 3 table

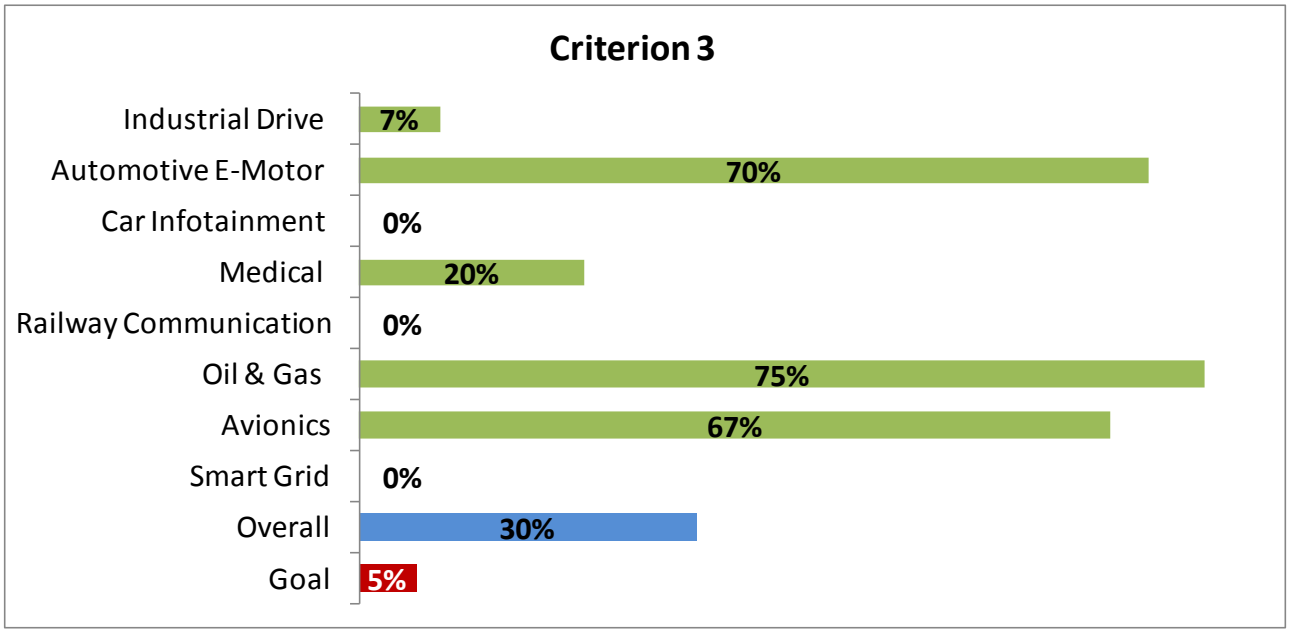

Figure 3-3: Overall Evaluation Criterion 3 Graph

3.4 CRITERION 4:

In the current state of progress of the use case, the overall evaluation for this criterion is not available and will be added in the final version.

3.5 CRITERION 5:

In the current state of progress of the use case, the overall evaluation for this criterion is not available and will be added in the final version.

3.6 CRITERION 6:

In the current state of progress of the use case, the overall evaluation for this criterion is not available and will be added in the final version.

4 CONCLUSION AND NEXT STEPS

The current report has shown the results of the first evaluation cycle for SESAMO, which was performed at the end of the 2nd year.

For this evaluation cycle of SESAMO, a set of six evaluation criteria was defined and each use case was evaluated individually. In this preliminary evaluation round, only three of the six criteria could provide meaningful results for each use case, mainly because of their different state of progress.

1. Percentage of safety / security related requirements that can be captured at model level (with SESAMO tool chain) against the total set of such requirements known to be applicable to the specific SESAMO use cases specified in deliverable D1.1.
   Goal : 60%
   Actual : 78%
   Status : fulfilled

2. Percentage of unresolved safety and security related conflicts in relationship to overall safety and security related architecture in end product developed in the use cases (similar to metrics in existing standards that measure percentage of certain types of failures in overall product architectures).
   Goal : 10%
   Actual : 38%
   Status : not fulfilled

3. Percentage of unresolved safety and security related conflicts caused by problems or errors that should have been prevented or captured by the SESAMO tool chain and methodology (as opposed to conceptual errors made by the user that could not be prevented by any tool).
   Goal : 5%
   Actual : 30%
   Status : not fulfilled

4. Percentage improvement of safety and security related architectural definition automation through the methodology and tool chain.
   Goal : 40%
   Actual :
   Status : not yet evaluated

5. Percentage improvement of safety and security related accreditation automation through the methodology and tool chain.
   Goal : 10%
   Actual :
   Status : not yet evaluated

6. Percentage improvement in integration of the safety and security related tool chain, whereby the integration is measured through the reduction of manual intervention required between tools.
   Goal : 70%
   Actual :
   Status : not yet evaluated

The first three criteria were directly related to the defined requirements for the use cases, and clearly unveiled a weakness of the early project phase, in that the selection of the requirements did not take into account that a percentage evaluation would be done.

Many of the requirements are too general to judge them as 'Yes' wrt. modellability. To address this, the requirements could be reconsidered and split into modellable and non-modellable parts, the non-modellable parts possibly being the more general requirements. This would increase the percentages and make the results for each use case more comparable. One example is that the use cases have many process requirements, which are judged as not modellable. Such requirements simply have to be followed, so there is not even a need for modelling. Naturally, tools might provide help on implementing the processes, e.g. by modelling the process itself.

For criterion 2 and 3, the conflict resolution was judged based on the requirements. At the current stage in the project, this has to be seen as a first step that needs to be carefully reconsidered. Obviously a better, more accurate and ideally automated method for identifying and solving conflicts is desirable for the second, final evaluation.

For the final evaluation, the remaining criteria will be elaborated for each use case. At the current stage of the project, initial estimations were available for only a few of the use cases, and no meaningful overall result was possible.