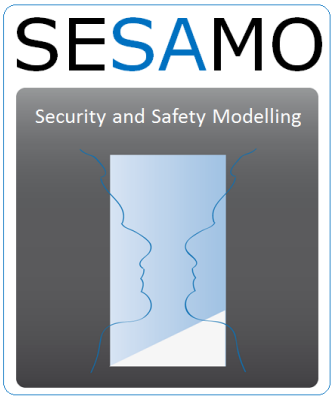

Security and Safety Modelling

Artemis JU Grant Agreement no.: 295354

D5.4 - Use Case Evaluation (Final, Public)

Version 1.0

May 2015

Final

Dissemination level: PU

Contributing partners

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

EXECUTIVE SUMMARY

The current document *D5.4 - Use Case Evaluation (Final, Public)* gives an overview of the final outcome of the use case evaluation task that was performed as a final action within WP5. Since this report is classified 'public' it does not contain all use case specific evaluation details. The complete evaluation results are presented within *D5.6 - Use Case Evaluation (Final, Confidential).*

Based on the reviewer's feedback of the 2nd review the evaluation approach presented in the preliminary version of the document was adopted. Now the final results of SESAMO are assessed in three ways. All tree perspectives have to be considered to see the full value of the results that were achieved within SESAMO.

1. Fulfilment of the six numeric criteria that were defined in the beginning of the project:

The early approach that was based on very formal calculation of percentage values was still finalized and all six criteria were evaluated for the seven use cases. As already expected after the first evaluation round, the target values turned out to be extremely ambiguous and could only be reached for two out of six criteria. Major reasons are different abstraction levels of the requirement definition for each use case and the different system scope. It also turned out that some of the criteria were not directly applicable for all use cases (e.g. accreditation effort for smart grid is not comparable to a single industrial product/device). Nevertheless the formal metrics showed that the SESAMO approach brought significant benefits towards all of the project objectives even where the absolute goal percentage values were not reached.

2. Feedback of the expert advisory board (project level and use case specific):

Following the reviewer's recommendation to involve the EAB, all its members were asked to evaluate a questionnaire addressing questions about one individual use cases presented in D5.2. The use cases were associated with respects to the expert's field of expertise. All these use case specific details of the EAB feedbacks are presented within *D5.6*, because of confidentiality. Anyway, these comments are only meaningful in combination with the non public deliverable *D5.2*.

I addition the experts were asked to judge the overall SESAMO objectives based on major previous deliverables and reports. These overall feedbacks were combined and show that the SESAMO objectives were successfully addressed.

3. Individual contribution to the strategic Artemis targets of each use case:

In addition to the analysis based on formal criteria the use cases were assessed in the light of the Artemis strategic targets. In specific two new 'soft' criteria were added:

- Innovation and Cost Benefits
- Impact to the ARTEMIS Strategic Targets

Naturally these analyses are very use case specific and in many cases include confidential information. For that reason only the confidential deliverable *D5.6 – Use Case Evaluation (final, confidential)* contains the discussion of the additional criteria.

INTRODUCTION

1.1 TECHNICAL CONTEXT AND OBJECTIVES

This final version of the document, which is an output of Task 5.3, is based on an evaluation of the final results of task *T5.1 - Use Case Demonstrator Development*, which are presented in Deliverable *D5.2 - Use Case Demonstrator Development (final).* It is to be read as the result of the final round of evaluation.

In SESAMO WP5 addresses the following two overall objectives:

1. Modelling and implementation of defined use cases with the SESAMO tool chain and SESAMO methodology;

2. Evaluation of improvements and advantages/disadvantages.

This specific report relates to the second objective.

Within SESAMO a set of seven 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 2-1 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
Medical	IFAG	ESY, IIT-CNR, CITY
Railway Communication	UC	DTU, FTW, INTECS, DICEA, SYSGO
Smart Grid	EDF	FTW

Table 2-1: 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.

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.

To 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 SESAMO methodology and SESAMO tool chain.

1.2 DOCUMENT STRUCTURE

Following above concept, a set of six evaluation criteria was defined in order to evaluate all use cases. They are presented in *chapter 2.1 Definition of the Success Metrics.*

For all use cases the final evaluation was conducted and the results are presented within SESAMO deliverable *D5.6 - Use Case Evaluation (Final, Confidential).*

The individual results were combined and totals are presented and discussed in *chapter 2.2 Results of the formal Evaluation*

Chapter 3Expert Advisory Board feedback provides a summary of overall feedback received from the members of the SESAMO expert advisory board.

A closing conclusion after the final evaluation cycle is drawn in chapter 4.

2 FORMAL EVALUATION

2.1 DEFINITION OF THE SUCCESS METRICS

As an attempt to make the results of SESAMO measurable the following set of success indicators has been derived directly from an examination of the industrial benefits expected from SESAMO. They seem to be applicable with an acceptable tradeoff of implementation effort versus information benefit.

For each of the success criteria an initial target value was defined already in the project definition phase. Since there was no comparable reference data available, these expectations turned out to be very ambiguous from the current perspective at the end of the project and could only be reached in few cases.

To achieve higher level confidence the criteria need to be applied to more cases to show whether the target value has to be adjusted.

In addition the evaluation in SESAMO can only rely on one single use case per domain and shall not be considered as fully representative for that whole domain.

2.1.1 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 value is a first attempt to come up with a target value that may be adjusted when more data is available.

2.1.2 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.

2.1.3 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.

2.1.4 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.

2.1.5 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.).

2.1.6 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%.

2.2 RESULTS OF THE FORMAL EVALUATION

2.2.1 Criterion 1:

After combining all the individual results of the use cases the average requirement coverage is calculated as presented in Table 2-1 and Figure 2-1. 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 84% the anticipated threshold of 60% for criterion 1 is already reached.

Some of the requirements (e.g. product has to fulfil standard EN61800) are too general to judge them as 'Yes' with respect to modellability. 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.

Criterion 1	Number of total requirements of use case	Number of requirements, which can be captured at model level	Percentage
Industrial Drive	41	34	83%
Automotive E-Motor	12	10	83%
Car Infotainment	5	5	100%
Medical	12	9	75%
Railway	13	12	92%
Avionics	26	20	77%
Smart Grid	12	9	75%
Average			**84%**
Initial Target			**>= 60%**

Table 2-1: Overall Evaluation Criterion 1 table

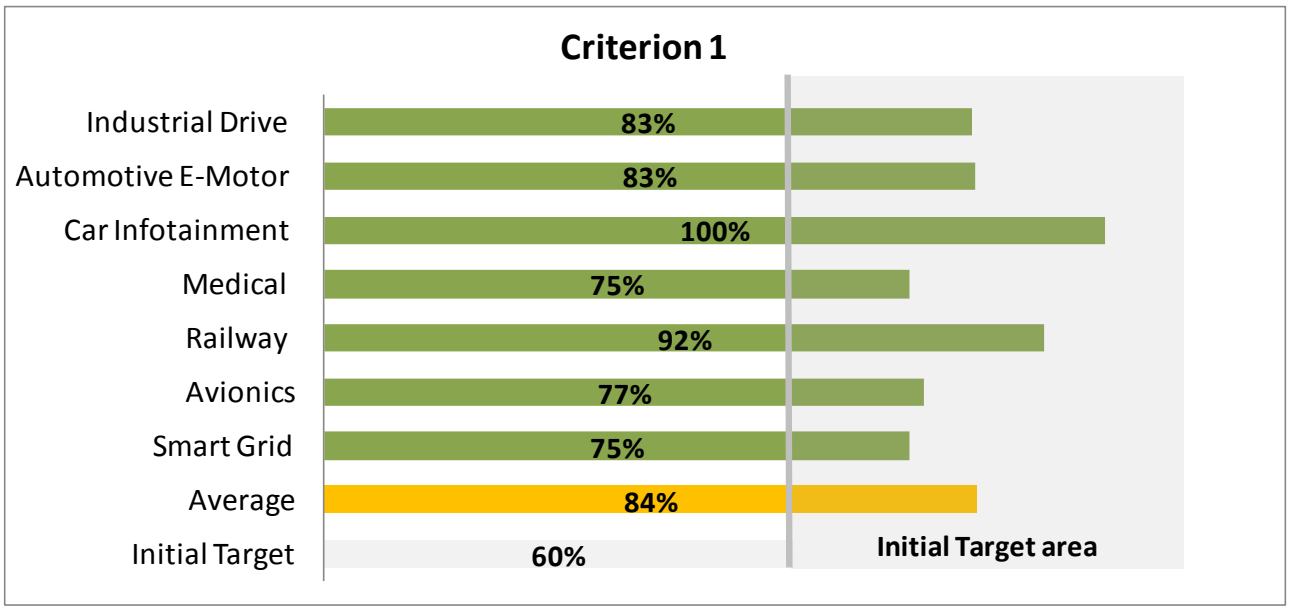

Figure 2-1: Overall Evaluation Criterion 1 Graph

2.2.2 Criterion 2:

After combining all the individual results of the use cases the average requirement coverage is calculated as presented in Table 2-2 and Figure 2-2. The average percentage over all use cases is 28% while the SESAMO goal was defined by less than 10%.

The table clearly shows one obvious weakness of the approach, which results from the small amount of conflicts and the representation of the individual results in percentages. Percentages

don't "scale", especially in the downward direction. The Avionic use case has two unresolved conflicts out of only three conflicts, which results in 67%. This value seems extremely high, but in reality it results only from two unresolved conflicts. Both conflicts base on a security requirement, that realisation reduce the system performance and violate the timing limits of the safety function. With further detailed WCET analysis it could be possible to optimize the system performance and resolve one unresolved conflict. This would mean a reduction of 33% of the individual Avionics result value. 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.

While both automotive E-Motor and Medical Use Case may seem unsuccessful at the first glance, the starting position needs to be kept in mind: For e.g. automotive available technologies have been fully exploited to meet safety goals, such as described in ISO 26262. Making the step from 'safety only' to 'combined safety and security' leads to situations where (new) security requirements violate (existing) safety features.

On the other hand, a detailed description of unresolved conflicts will provide guidance for future development, especially by addressing such conflicts in early development phases.

The target value of criterion 2 was not reached, but with further refinement of requirements and further analysis better result values can be reached.

Criterion 2	Number of overall safety and security related conflicts	Number of unresolved safety and security related conflicts	Percentage
Industrial Drive	27	2	7%
Automotive E-Motor	10	8	80%
Car Infotainment	2	0	0%
Medical	7	3	43%
Railway Communication	2	0	0%
Avionics	3	2	67%
Smart Grid	1	0	0%
Average			**28%**
Initial Target			**<= 10%**

Table 2-2: Overall Evaluation Criterion 2 table

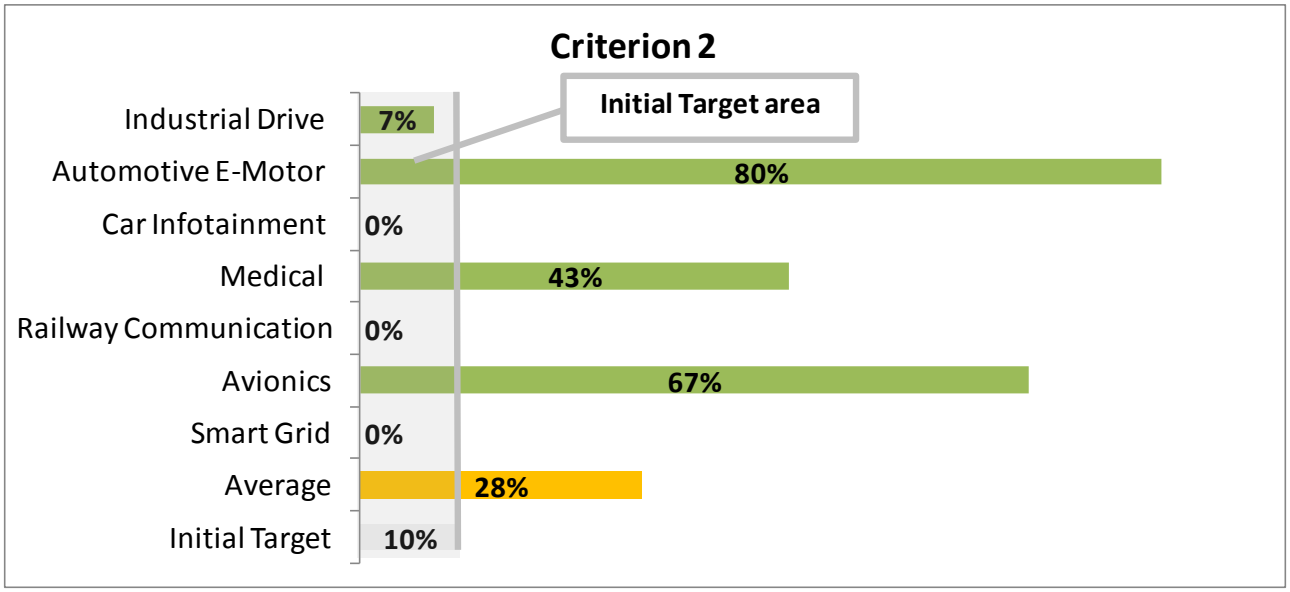

Figure 2-2: Overall Evaluation Criterion 2 Graph

2.2.3 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 17% unresolved conflicts that could have been solved, where the goal was set to less than 5%.

For the avionic use case one unresolved conflict is solvable with more powerful hardware that can reduce the jitter effects resulting from security operations, such as cryptographic algorithms (for example used for signatures and validation of communication data). The second unresolved conflict remains not resolvable, since the time window of security compromising actions cannot be guessed in advance. Hence, the actions countering attacks need to be scheduled on demand as soon as an attack is recognized. This can have significant impact to the hard real-time criteria of the entire system. An obvious solution to solve this issue is to reserve a processing unit of a system for security countermeasures. However, the use of multicore hardware for high critical avionic equipment is nowadays topic of much research activities and multicores are not deployed in operational fields.

As described in criterion 2 in the automotive E-Motor and Medical Use Case the combined safety and security consideration leads to a many violated safety features.

The threshold of criterion 3 was not reached, but we can see a trend into the right direction.

Criterion 3	Number of overall safety and security related conflicts	Number of unre-solved safety and security related conflicts	Percentage
Industrial Drive	27	1	4%
Automotive E-Motor	10	7	70%
Car Infotainment	2	0	0%
Medical	7	1	14%
Railway Communication	2	0	0%
Avionics	3	1	33%
Smart Grid	1	0	0%
Average			**17%**
Initial Target			**<= 5%**

Table 2-3: Overall Evaluation Criterion 3 table

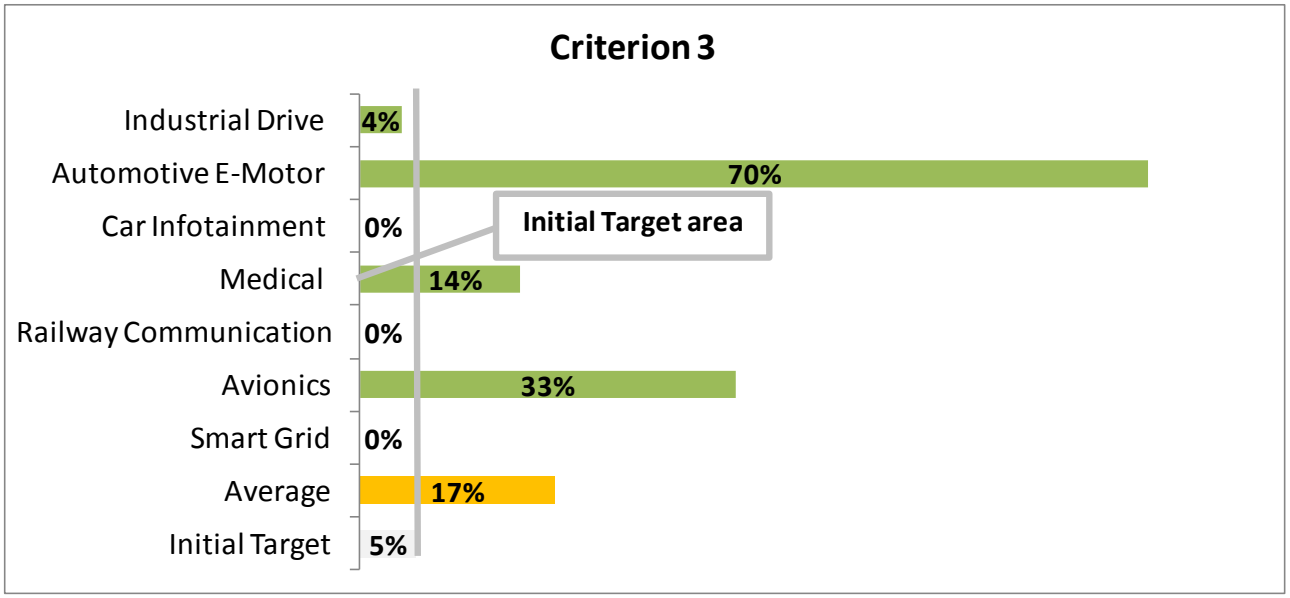

Figure 2-3: Overall Evaluation Criterion 3 Graph

2.2.4 Criterion 4:

After combining all the individual results of the use cases the average improvement of the architectural definition is calculated as presented in Table 2-4 and Figure 2-4. Depending on the use case improvement values are based on estimations of design experts for the individual demonstrator.

The Smart Grid use case is focused on safety and security problems of an entire smart grid system. It is very different from a system having well identified limits such as most other use cases in SESAMO. Therefore the evaluation of this criterion is not applicable for the Smart Grid use case.

Even if the average result (28%) over all use cases stays below expectation (threshold = 40%), an important result is to describe the needs towards automation. Within the SESAMO context it was impossible (in terms of effort) to achieve higher automation, however, this is important input for vendors of EDA (electronic design automation) tools.

Criterion 4	Improvement of safety and security related architectural definition automation
Industrial Drive	30%
Automotive E-Motor	30%
Car Infotainment	25%
Medical	25%
Railway Communication	30%
Avionics	30%
Smart Grid	not applicable
Average	**28%**
Initial Target	**>= 40%**

Table 2-4: Overall Evaluation Criterion 4 table

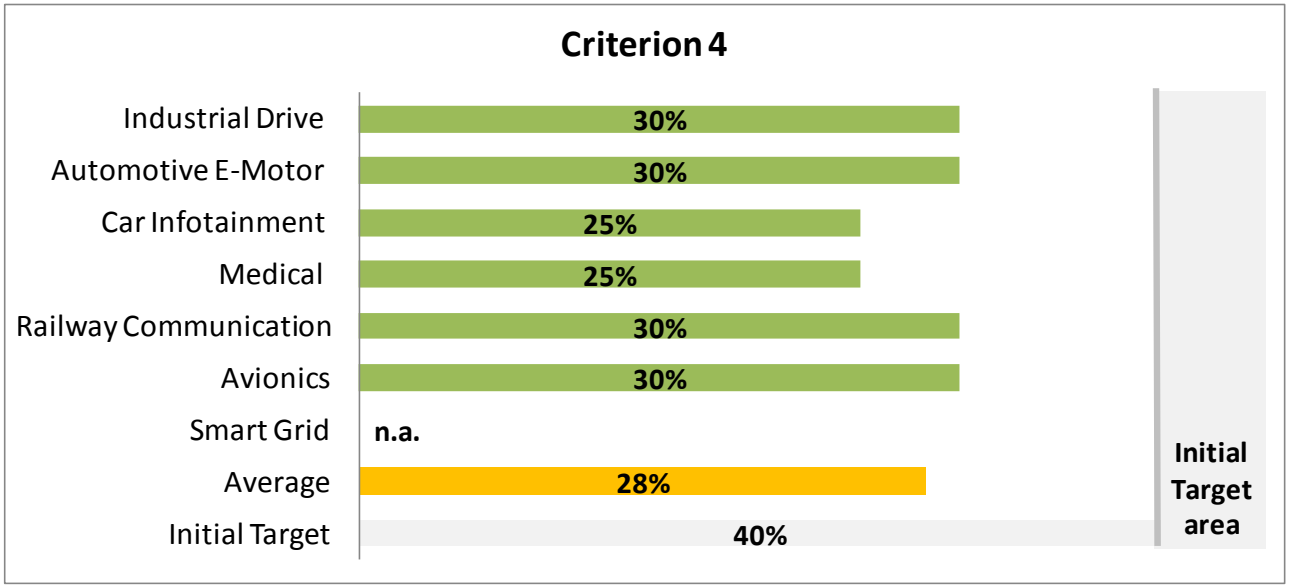

Figure 2-4: Overall Evaluation Criterion 4 Graph

2.2.5 Criterion 5:

Table 2-5 and Figure 2-5 present the evaluation results of criterion 5 of each use case and the average evaluation result is calculated. The average percentage over all use cases (except Smart Grid) is 19% while the SESAMO goal was defined by 10%. The threshold of criterion 5 is reached.

The Smart Grid use case is focused an entire smart grid system. It is a "system of systems" and only its parts can be accredited. Therefore this criterion is not applicable for this use case.

Criterion 5	Improvement of safety and security related accreditation automation
Industrial Drive	15%
Automotive E-Motor	15%
Car Infotainment	25%
Medical	10%
Railway Communication	25%
Avionics	25%
Smart Grid	not applicable
Average	**19%**
Initial Target	**>= 10%**

Table 2-5: Overall Evaluation Criterion 5 table

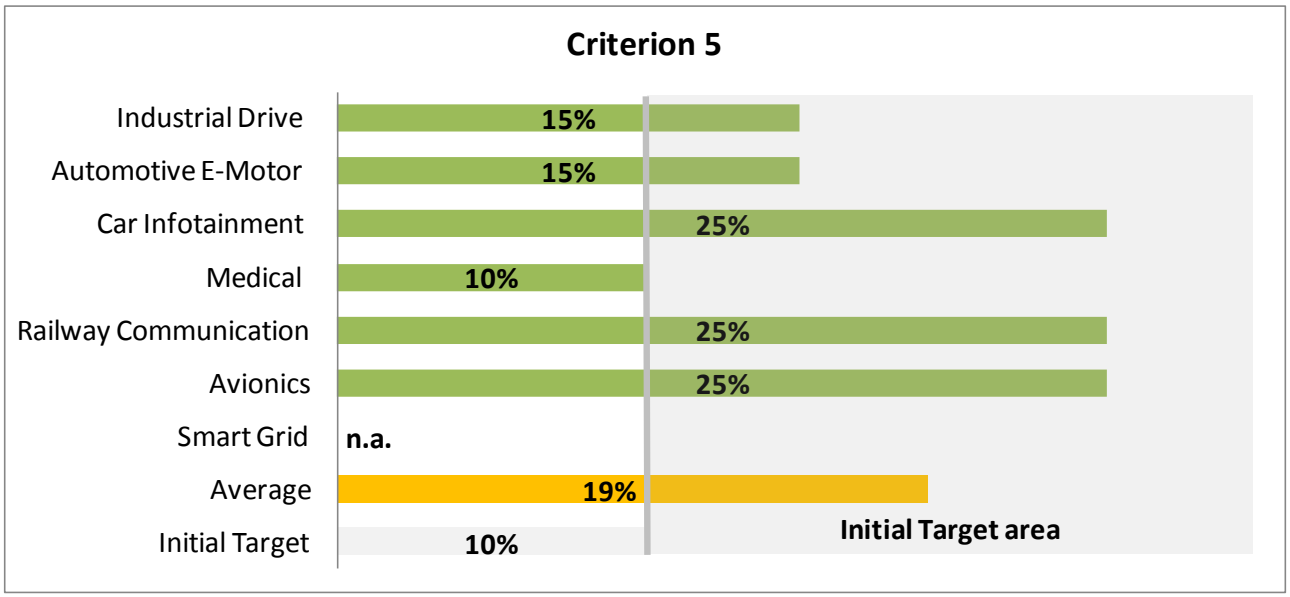

Figure 2-5: Overall Evaluation Criterion 5 Graph

2.2.6 Criterion 6:

After combining all the individual results of the use cases the average design improvement caused by the SESAMO integrated tool chain is calculated as presented in Table 2-6 and Figure 2-6. Depending on the use case improvement values are based on estimations of design experts for the individual demonstrator.

The Smart Grid use case is focused on an entire smart grid system. A new simulator prototype was developed for verification of security and safety related mechanisms in an entire smart grid. The

integration of this simulator prototype in to the SESAMO tool chain exceeds the time frame of the SESAMO research project. Therefore the evaluation of this criterion is not assessed for this use case.
The average percentage over all use cases (except Smart Grid) is 50% while the SESAMO goal was defined by 70%. The goal was not completely reached, because the threshold is ambitious in any case. Within the lifetime of the project it might have been too ambitious to think, that we could achieve complete tool integration. But we have achieved the integration of some important tools used in the SESAMO methodology.

Criterion 6	Improvement in integration of the safety and security related tool chain
Industrial Drive	50%
Automotive E-Motor	50%
Car Infotainment	40%
Medical	40%
Railway Communication	60%
Avionics	60%
Smart Grid	not assessed
Average	**50%**
Initial Target	**70%**

Table 2-6: Overall Evaluation Criterion 6 table

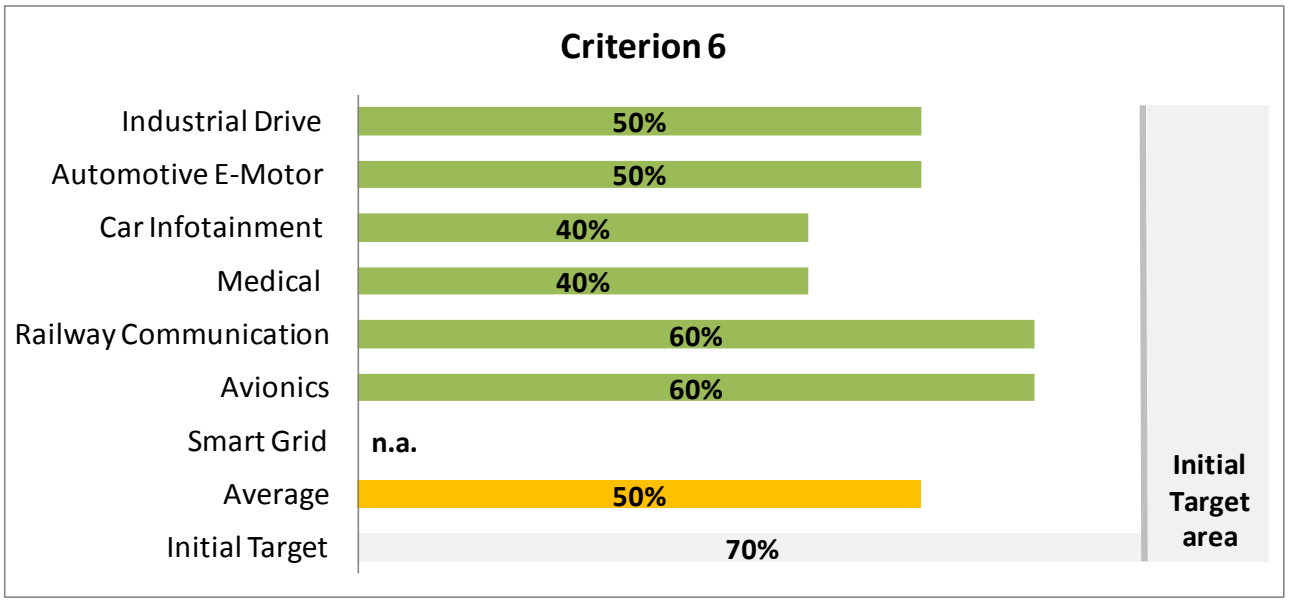

Figure 2-6: Overall Evaluation Criterion 6 Graph

3 EXPERT ADVISORY BOARD FEEDBACK

With respect to the comments received at the 2nd project review the members of the EAB were invited to evaluate individual use cases and the overall project objectives. This section contains the overview of feedbacks from the members of the SESAMO Expert Advisory Board with the focus on the entire project. Each of the experts completed the questionnaire based on his expert knowledge and the available final SESAMO deliverables and reports. The detailed feedback of the members of the SESAMO Expert Advisory Board is strongly related to the confidential document *D5.2* and is therefore presented in *D5.6* [3].

Overall the feedback of the SESAMO experts is very positive concerning the SESAMO methodology to identify and resolve security and safety related conflicts. A potential for improvement was detected for the security aspects in the tools and for the cross-domain harmonization.

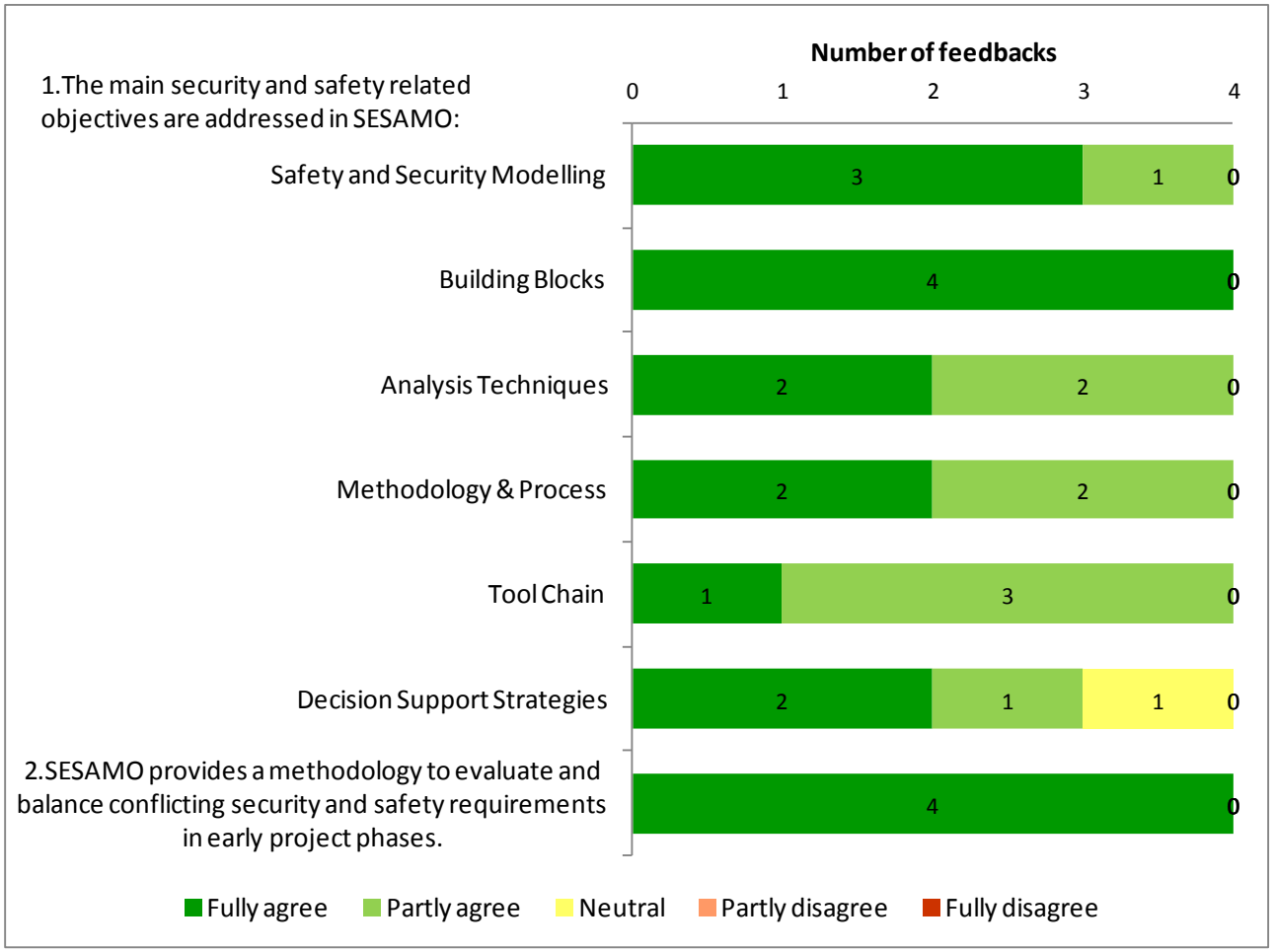

Figure 3-1: SESAMO expert feedback question 1 and 2

4 CONCLUSION

The current report has shown the results of the final evaluation cycle for SESAMO, which was performed at the end of the 3rd year, based on the final use case implementations.

We have seen that the initial thresholds set for the **formal evaluation** criteria could be reached in 2 out of 6 criteria, 1 was almost reached and 3 were missed. Nevertheless all 6 criteria show clear improvements compared to the traditional approach. More case studies should be analyzed in future to come to realistic thresholds.

Major reasons why some criteria were not reached completely:

- Some thresholds were too ambitious and could not be reached within the limited frame of the SESAMO project
- Different abstraction levels of requirements and different amount of safety and security related conflicts
- Different system scopes of use case (smart grid – communication interface)

The first three criteria were directly related to the defined requirements for the use cases. 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. In many use cases the SESAMO tool chain and methodology capture and resolve nearly all safety and security related conflicts. Some use cases found a small amount of conflicts and therefore could not reach the limits for the evaluation criteria.

The **EAB** was involved in the evaluation and judged the final use cases and the overall SESAMO objectives. The feedback was very positive and gave valuable inputs and ideas for further related improvements and activities.

Additional 'soft' evaluation criteria, assessing the contribution to the **ARTEMIS strategic targets,** were introduced and can be found within the related deliverable *D5.6.*

5 REFERENCES

[1] SESAMO D1.1 - Functional safety and security related process and methods requirements

[2] SESAMO D1.2 – Use Case Specification

[3] SESAMO D5.6 - Use Case Evaluation (Final, Confidential)