Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P7522-cd

IP Protection using Simplification and Masking for Model-Based Safety Analysis (MBSA) Model Exchange

Tony GHUELDRE
IRT Saint Exupéry, France. E-mail: tony.ghueldre@irt-saintexupery.com

Wilkinson JOAS
IRT Saint Exupéry/Safran Aircraft Engines, France. E-mail: wilkinson.joas2@safrangroup.com

Julien VIDALIE
IRT Saint Exupéry/Airbus Protect, France E-mail: julien.vidalie@airbus.com

Xavier DE BOSSOREILLE
IRT Saint Exupéry/Airbus Protect, France E-mail: xavier.de-bossoreille@airbus.com

Model-Based Safety Analysis (MBSA) is a growing method for performing safety analysis. It aims to offer a closer integration with system modeling environments compared to traditional RAMS approaches. MBSA has proven particularly effective for assessing the safety of complex systems. However, in extended enterprise projects, one of the challenges to its use is the exposure of sensitive information embedded within the models, which may be subject to intellectual property (IP) protection. This includes detailed insights into the system being modeled, its internal management, and its reconfiguration processes. To address these concerns and enable continued use of MBSA in collaborative projects, models shared between companies may differ from those used internally.
We introduce two key activities —simplification and masking— to transform the original model while maintaining the necessary level of detail for collaboration. These activities regroup diverse pre-existing model transformation techniques, allowing models to range from ”white boxes”, where most details are accessible, to ”black boxes”, where only minimal information is shared.
Simplification is the process of reducing the complexity of an existing model. This process involves eliminating unnecessary details and focusing on essential behaviors, thereby optimizing calculations and improving the overall usability of the model.
Masking refers to the practice of concealing certain details or aspects of an existing model to protect intellectual property. This process ensures that proprietary information remains confidential while still allowing for collaborative work on a project.
In this paper, we propose and illustrate the use of simplification and masking for exchange of MBSA models. We discuss the possible tradeoffs between IP protection and assurance of correct results. In addition, we highlight that effective communication between suppliers and integrators is essential to ensure that the shared models comply with all safety-related project requirements, while respecting IP constraints.

Keywords: MBSA, Co-Simulation, Model Exchange, Collaborative design, Safety, RAMS, IP Protection, Simplification, Masking.

1. Introduction

The design of complex systems in extended enterprise projects often requires collaboration between multiple stakeholders, such as integrators and suppliers. This implies sharing data and models of the system, which can be sensitive for some of the stakeholders. Therefore two critical needs rose from extended enterprise collaborative design: data about the system has to be shared in a way that makes it usable, but it also has to be shared in a form that protects sensitive information.

Traditional approaches (e.g. fault trees), which are grounded in abstract mathematical equations, struggle to manage complexity efficiently. Model-based approaches provide a representation of the system closer to the architecture. This makes them

a more favorable paradigm for addressing complexity. Among model-based approaches, Model-Based Safety Analysis (MBSA) provides a structured framework for assessing the safety of complex systems by integrating Failure Propagation Models (ARP4761A (2023)). Currently, if someone wants to share an MBSA model in order to integrate it with another model, the MBSA tool saves and exports the model as a file that may contain too much information. The information collected by the final user might depend on the rights given at the export. However, in the context of extended enterprise, not all the information contained in the model can be shared. Combinatorial explosion also poses a problem as the models obtained through the combination of other models can be very time-consuming in terms of computations.

In this paper, we explore how simplification and masking processes can allow the sharing and collaboration of MBSA models while protecting proprietary information.

Section 2 describes relevant works related to MBSA models and collaboration. Section 3 provides a comprehensive description of masking and simplification concepts, along with ideas that could be used to operate them. Section 4 describes an electronic architecture, along with its MBSA modeling and the application of masking / simplification processes to create a model for exchange. Section 5 discusses the results of the model for exchange's modeling and creation. Finally, section 6 gives an overview of the work done and its results, along with perspectives for its use and further developments.

2. Related works

The use of models has been more and more common during the last years. The Model-Based System Engineering (MBSE) is an approach used in various industries in different domains of activities INCOSE (2024). This technique has inspired its adaptation to areas such as safety, where MBSA begins to gain popularity. The AltaRica language, created by LaBRI starting 1995 Signoret (1998), is one language for MBSA development. The second version of the language, named AltaRica Data-flow Boiteau (2006), helped with the development of MBSA tools. However, implementing new aspects can be complicated, so some projects were developed to demonstrate the real benefit of those methods.

MBSA models use formal languages dedicated to safety. They explicitely represent the architecture through components and the flows between them. They represent the dysfunctional behavior at the component level and compute the global behavior of the system through interactions between the components.

At the beginning of the century, European projects ESACS [a], ISAAC [b] and then MISSA [c] worked in particular on providing robust tools and methodologies to apply MBSA in aeronautics, dealing with complex systems and several stakeholders

This led to the MOISE project [d] from IRT Saint Exupéry has defined a method for consistency between MBSE and MBSA models Prosvirnova et al. (2017a). The objective of the method is to assist safety model review by system architect. This method belongs fully to the category of "multi-model". The study case of this project is AIDA Prosvirnova et al. (2017b), a drone for preflight inspection.

Then the S2C project [e] from IRT Saint Exupéry and IRT System X also used the AIDA study case, in order to verify the project's 3 objectives: a generic process of System Engineering / Safety Analysis consistency; an MBSA modeling guide Project (2023); tools and methods to ensure consistency between MBSE and MBSA models Demachy and Guilmeau (2022).

In parallel, the aeronautic standard ARP4761A (2023) was under update starting 2014, in order to integrate the MBSA as part of acceptable safety method. The official release of the revision A was in December 2023.

Finally, the CoSMoS project [f] from IRT Saint

[a] https://cordis.europa.eu/project/id/G4RD-CT-2000-00361
[b] https://cordis.europa.eu/project/id/501848
[c] https://cordis.europa.eu/project/id/212088
[d] https://sahara.irt-saintexupery.com/MOISE
[e] https://www.irt-saintexupery.com/s2c/
[f] https://www.irt-saintexupery.com/le-projet-cosmos-

Exupéry (still on-going) which aims to provide means to share RAMS objectives and results of different system levels operated through heterogeneous MBSA models while complying with IP constraints; to analyse the sensitivity and ensure the representativeness of MBSA analyses results depending in their inputs; to adapt the granularity of the MBSA model to the need.

3. Methodology

To tackle the problem of model sharing, we propose two concepts: Masking and Simplification. These concepts are not modeling ideas such as saying that "a model is a simplification of reality", but rather operations of transformation of models. In order to produce an exchange model, a model is taken and masking and simplification of this model are operated. In this section we give an overview of what we call Masking and Simplification.

3.1. *Masking*

3.1.1. *Definition*

We call masking the practice of concealing certain details or aspects of a model to protect intellectual property, while keeping the model unchanged for the tool. This process ensures that proprietary information remains confidential while still allowing collaborative work on a project. Masking is not limited to a single level of project architecture; instead, it requires thorough discussions and trade-offs between involved parties to reach a mutual agreement on what information can be masked and what must remain visible.

The concept of masking is closely related to the idea of a black box, where the internal workings of a component are hidden, and only the inputs and outputs are exposed. This approach is commonly linked to the Functional Mock-up Unit (FMU) and Functional Mock-up Interface (FMI) methods, which facilitate the exchange and integration of models across different tools and platforms while protecting sensitive internal details. The FMI is the preferred method to obtain a model resistant to retro-engineering. However, its implementation in MBSA tools is not available at the moment, so the level of IP protection applied on current MBSA models have to go through tradeoffs between the duration of the masking process and its purpose.

3.1.2. *Application*

This section will describe the application of the masking process on a model, based on the black / grey / white box concept as shown in Amara et al. (2015).

- Transforming the model into a black box means hiding everything inside this model and only exposing inputs, outputs, and the model's overall behavior. By doing so, others can use the model for exchange without gaining access to the proprietary or sensitive information it contains. This approach is used to protect intellectual property, and can be performed by tools such as FMI[g] to have a maximum protection.
- On the opposite, a white box is a model with everything accessible. No protection has been applied and everyone has visibility on what is inside it.
- A grey box is a model with a mixture of masking and complete visibility. As implied by the scale of grey, there are infinite possibilities, but a common grey box model can be obtained by masking one block inside a white box model.

In summary, the masking process can be very useful for increasing the IP protection level of a model that will be shared with different stakeholders.

3.2. *Simplification*

3.2.1. *Definition*

A model, by its nature, is a simplification of reality. It is however possible to simplify an existing model. We call simplification the process of reducing the complexity of a model to enhance its clarity. As information might be lost during this process, simplification shall ensure that the

accroitre-la-maturite-de-lutilisation-des-analyses-mbsa/

[g]https://fmi-standard.org/

results are consistent with the original model. This process involves eliminating details unnecessary from the integrator's point of view and focusing on essential components, consequently optimizing calculation's efficiency and performances, and improving the overall usability of the model.

The simplification aspect can be summarized in 3 main categories:

(1) Simplification for clarification: a simplified model is easier to understand and communicate. Such models have a full traceability with the original ones.
(2) Simplification borderline with optimization: the model is simplified so that the final user can obtain results more efficiently. Such process can lead to traceability difficulties for justifying the results.
(3) Simplification borderline with masking. An extreme simplification can lead to a model very different from its original one, almost similar to a masking process, with few to no traceability.

These categories are not independent, they can overlap with another.

3.2.2. *Application*

The application of the simplification process can be different in function of the category previously mentioned, hence the following detail per category:

(1) Simplification for clarification: in Figure 1, there are several ways to simplify the model, each one exposed by a square of a defined color. The simplification depends on what the user wants to show: do they want to have a single block for the system (blue square), do they want to have one block per engine (red square), or do they want to assemble the power supply with the computer (green squares)?
(2) Simplification borderline with optimization: in Figure 2, the model architecture is simplified by performing a simplification of the state machine, using a Cartesian product. The states corresponding to one beam failed are gathered into a single state. The same goes for the states corresponding to two beams failed. It reduces the failure possibilities, without degrading the results (in this very use case), but enhancing the calculation performances.
(3) Simplification borderline with masking: an initial model can be remodeled using its simulation results to build its new version. In MBSA, there can be lots of sequences of different orders for a single model. The simplification process applied here consists in gathering all the sequences of the same order into one event, then to build a model with all the identified events. Doing so, the simplified model has no information about the original one, but the sequences details can be delivered in an appropriate documentation.

In summary, the simplification can sometimes be used for the IP protection, but only in case of extreme simplification where the hidden information cannot be traced back. In the vast majority of the cases, other simplification processes can be deemed sufficient to hide information under a block, sharing in the end a grey box model.

4. Application on the Wheel Braking System (WBS)

4.1. *WBS presentation*

The WBS is the example used in the appendices of the document ARP4761A (2023), to show the reader how to apply the different safety methods explained in the core of the document. It is a fictional system, whose main function is described as "Decelerate on ground". In the MBSA appendix of the document (Appendix Q9), the system is specified and its associated model is produced in order to check the system compliance to safety requirements. The final results are built on a MBSA model accessible to all [h].

4.2. *Use case based on WBS*

The masking and simplification processes defined above will now be applied on the WBS model from ARP4761A (2023) appendix Q9.

[h] https://satodev.com/en/mbsa-analyses/mbsa-models/

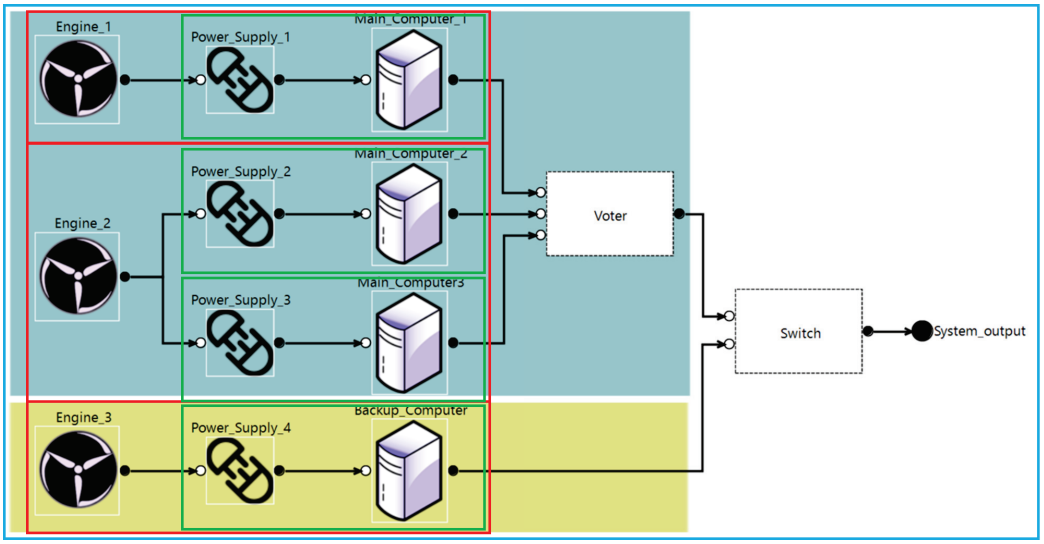

Fig. 1. Simplification for clarification

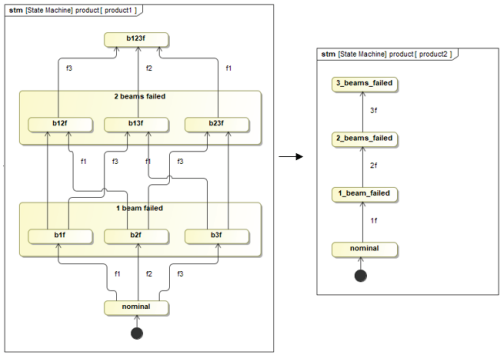

Fig. 2. Simplification for optimization

The focus will be on the Brake System Control Unit (BSCU) of this system, as it is the one matching all the requirements for this paper. Note that in this paper, the logic blocks were refined in order to separate the hardware part from the software part, as shown in Figure 3.

4.3. *Masking*

For the masking process, the BSCU can be adapted into a supplier-defined level of grey box, to match the supplier's IP protection level required. In the original model, the more detailed view allows to show how the failures propagate in the system using step-by-step simulation. In the final model, all the logic blocks could be modified in order to show only their inputs and outputs.

In case of a white box, the BSCU model will be exported as-is to the customer.

In case of a black box, the model sent to the customer is a single box whose behavior is based on the entire unit behavior. The customer will have only access to the box, which will cover IP protection in the vast majority of cases.

For all three cases, the inputs and outputs of the exported model shall match the customer needs.

4.4. *Simplification*

The model simplification can be different based on the categories detailed in section 3.

Categories (1) and (2) : Figure 4 is a simplification of the Figure 3, as the logic blocks are now without sub-level architecture.

The updated model reaches both categories (1) and (2) because:

(1) The model is now easier to understand, as its architecture modification allows to review it on a single level, without compromising its initial behavior.
(2) The model has been optimized, as the logic blocks' hardware and software failures are now integrated in the logic blocks themselves.

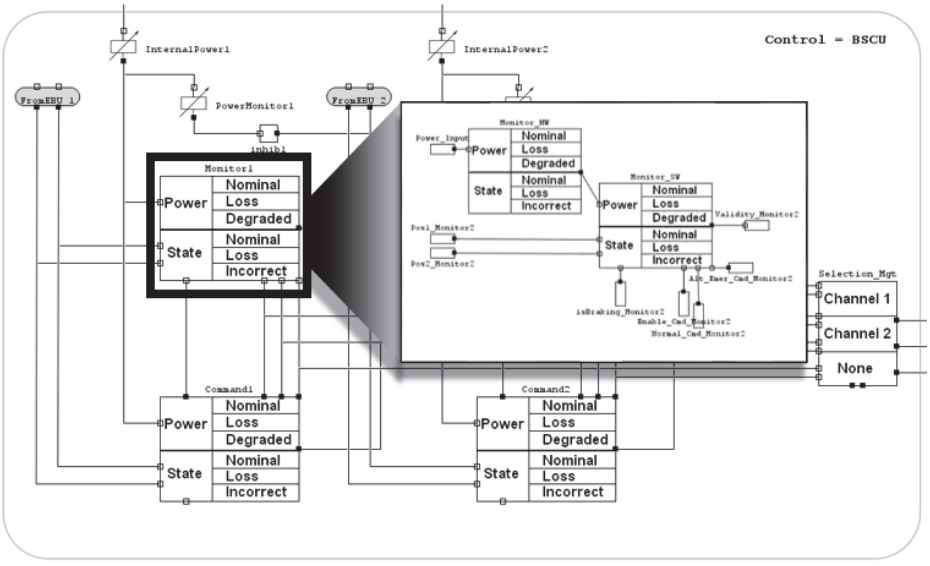

Fig. 3. Use case: BSCU MBSA model with hardware and software separation on logic blocks

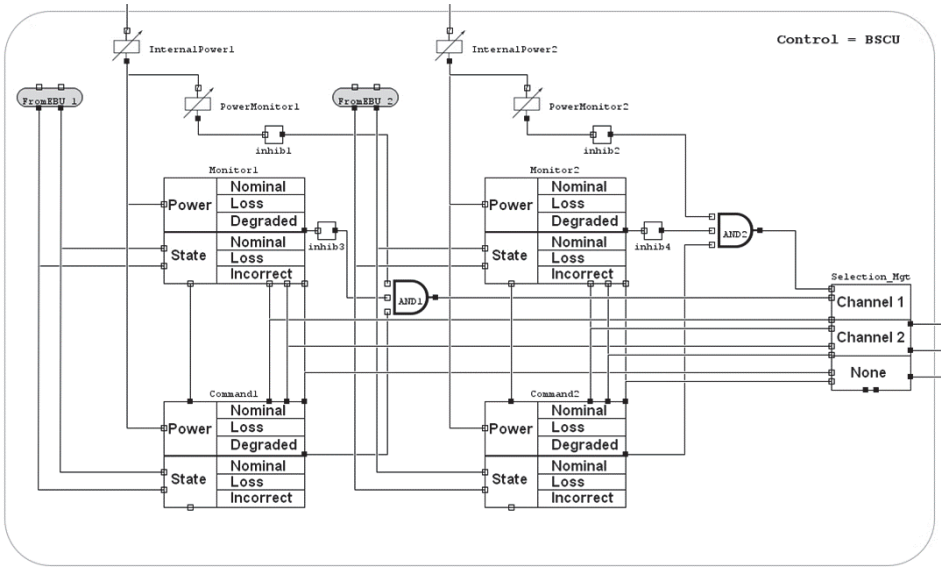

Fig. 4. Simplified BSCU MBSA model, categories 1 and 2

The calculation will be quicker and the results easier to understand.

For the simplification category (3), a model has been built based on the cutsets associated to each failure mode of the BSCU's outputs. In order to clarify the process, Figure 5 shows how to model the behavior of one output from the computation results, based on its possible transition paths from the initial state "OK" to the final state "Failed".

To create this model, the computation results were assumed to be a set of cutsets from order 1 to order 3. Then, all cutsets of order N are

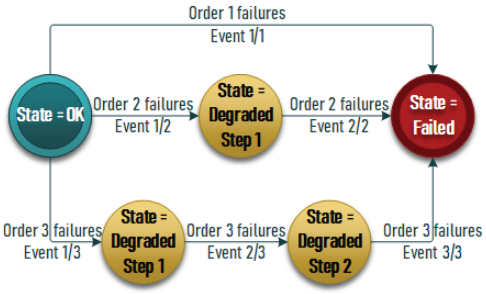

Fig. 5. Simplified BSCU, category 3

gathered into a set of (N-1) intermediate states and N events. The cutsets' probabilities are summed into a single order N probability, which will be evenly distributed between all transitions. When all those events are triggered, the output goes into its final state.

Example: for the order 2 cutsets, we have one intermediate state between the output's initial and final state. The probabilities associated to the transitions ["State = OK" to "State = Degraded step 1"] and ["State = Degraded step 1" to "State = Failed"] are equal to the square root of the sum of the order 2 cutsets' probabilities.

As a result, the final model will likely be a grey box: its content will be shared with the stakeholders, but without a proper documentation, the model will hide all the information necessary to understand its behavior.

5. Modeling results

Based on what has been described in the previous section, Table 1 summarizes the results of the simplification and masking processes and their impact on the IP protection of the model for exchange.

In the end, the best way to have an high level IP protection is to hide some characteristics of the initial model. If this is agreed with the stakeholders, this can be done through a black box with an associated documentation only describing what is necessary in the final model.

In case of grey box, the process is more or less equivalent, as it depends on the level of masking applied on the part(s) chosen to be hidden.

For the majority of application cases, the simplification process does not intend to provide IP protection to a model, but more a clarification and / or a calculation optimization. The category (3) can be assimilated to a grey box, which can lead to a masking if no appropriated documentation has been delivered to the stakeholders along with the model.

Table 1. IP protection in function of the process applied to the model for exchange

Process		IP Protection level
Masking	White box	No IP protection
	Black box	Maximum IP protection
	Grey box	Depends on the level of grey applied on the model produced
Simplification	Simplification for clarification	No IP protection
	Simplification borderline with optimization	No to slight IP protection, because some simplification actions can result in hiding parts of the model produced
	Simplification borderline with masking	Depends on the level of masking applied on the model produced

Another aspect mentioned is the assurance of correct results associated to those models for exchange. For the ones without IP protection, the results' correctness is easy to prove, as there was no intention of hiding information. For the rest, the proof of results' correctness mainly depends on the traceability set in place by the model provider: the more information provided to understand the results, the more correctness the results will have. This last aspect can also reveal the importance of mutual trust between stakeholders, which sets the basis for the level of information shared. Effective communication can enhance this trust and foster optimal collaboration.

6. Conclusions and Perspectives

As MBSA's popularity increases, it might be used by various stakeholders of an extended enterprise's project. The idea of exchanging MBSA models is slightly gaining interest, but for this exchange to be as efficient as with previous analyses, some consensus has to be found between the stakeholders.

As presented in this paper, there are processes of simplification and masking that can be applied to an existing MBSA model. Those processes have to be agreed between the stakeholders before applied on the model for exchange, in particular if the traceability between the results obtained by the model and the remaining project's documentation is difficult to perform.

Model simplification is meant to improve the usability of the model, whereas model masking is used to strenghten IP protection. While proper documentation aids in validation, it may not contain the necessary information when IP protection is high. Building mutual trust among stakeholders can reduce IP restrictions, enabling greater information sharing and facilitating the verification of results.

A study, performed with the CoSMoS (cf. section 2) projects' members but also with people outside the project, shows that nowadays the customers are more used to receive models that cannot be modified or accessed by them (note: here the term 'models' does not refer to MBSA but to other types of models, such as Fault Tree Analysis). Only a few models, among the ones received by the customers, are modifiable (meaning only the model parameters can be updated to obtain new results) or executable (meaning the model can only be executed). This shows that the final customer is used to have models that are not entirely accessible, and not entirely hidden: grey boxes. In the end, this study showed that the models for exchange are more likely to be simplified in categories (1) and (2), or masked as grey box with only one level of black box within the model for exchange. The final customer should not modify their expectation on the model's level of details. Doing so, the models for exchange provided as black boxes are not supposed to exist, and might remain theoretical as they would introduce too many questions, mainly about their results' correctness.

As for traditional analyses, a good communication between stakeholders to understand the needs and the associated means to answer them will be the basis for an efficient MBSA-based collaborative project.

Acknowledgement

This work was conducted within the CoSMoS (Collaborative Safety (&RAMT) Modeling Studies) from IRT Saint Exupéry and would not have been possible without its funding. Therefore the authors would like to thank the project and its partners.

References

Amara, F., K. Agbossou, A. Cardenas, Y. Dubé, and S. Kelouwani (2015, 01). Comparison and simulation of building thermal models for effective energy management. *Smart Grid and Renewable Energy 06*, 95–112.

ARP4761A (2023). Arp4761a: Guidelines for conducting the safety assessment process on civil aircraft, systems, and equipment. Technical report, SAE International.

Boiteau, M. (2006). The altarica data-flow language in use: Modeling of production availability of a multistates system. *Reliability Engineering and System Safety*.

Demachy, R. and S. Guilmeau (2022, June). Structural consistency of MBSE and MBSA models using Consistency Links. In *11th European Congress Embedded Real Time System (ERTS 2022)*, Toulouse, France.

INCOSE (2024). The guide to the systems engineering body of knowledge (sebok). Technical report, SEBoK Editorial Board.

Project, S. (2023). S2c mbsa modeling guide and validation report. Technical report, IRT Saint exupery/IRT SystemX.

Prosvirnova, T., E. Saez, C. Seguin, and P. Virelizier (2017a, September). Handling consistency between safety and system models. In *Model-Based Safety and Assessment*, Trento, Italy, pp. pp. 19–34.

Prosvirnova, T., E. Saez, C. Seguin, and P. Virelizier (2017b, 08). Handling consistency between safety and system models. *Conference: International Symposium on Model-Based Safety and Assessment*, 19–34.

Signoret, J.-P. (1998). The altarica language. *ESREL, Proceedings of European Safety and Reliability Association Conference*.