SUMMARY

Guide for conducting an MBSDA study (Model-Based Safety & Dependability Analysis)

P23-2 project for the Institute for Risk Management (Institut pour la Maîtrise des Risques (IMdR))

Ind A

Institut pour la **M**aîtrise **d**es **R**isques
Sûreté de Fonctionnement - Management - Cindyniques

November 24, 2025

Writers

Mustafa MOHAMED ABDALLA
Safety & Dependability Engineer (LGM)

Reviewers

Frédéric MILCENT
Safety & Dependability Expert (Naval Group)

Marc BOUISSOU
Safety & Dependability Expert (IMdR)

Approvers

Frédéric MILCENT
Safety & Dependability Expert (Naval Group)

Marc BOUISSOU
Safety & Dependability Expert (IMdR)

Revision history

Version	Date	Evolutions
A	November 24, 2025	Document creation

Table of Contents

1 Document purpose

This document aims to summarize the guide for conducting an MBSDA (Model-Based Safety & Dependability Analysis) study, produced as part of the P23-2 project for the Institute for Risk Management (*Institut pour la Maîtrise des Risques* (IMdR)). The guide was developed over an 18-month period in collaboration with several organizations: AIRBUS Protect, Arianegroup, DGA, EDF, INSA, ISAE-SUPMECA, LGM, MBDA, Naval Group, RATP, and Thales. This initiative enabled experts from these organizations, using different tools and modelling languages, to compare their practices, propose standardized definitions, and establish common foundations for modelling methods.

Based on the feedback from the P23-2 project members and the current state of the art, this guide provides a shared, clear, and trustworthy framework for conducting MBSDA studies. It highlights a common set of rules and best practices to ensure the representativeness of an MBSDA model, as well as its relevance and acceptance by stakeholders involved in Safety & Dependability.

Drafted in a normative document format (IEC – International Electrotechnical Commission), the guide will serve as a reference for the community in performing MBSDA analyses and could form the basis of a future standardization initiative.

2 Model-Based Safety & Dependability Analysis (MBSDA)

MBSDA has been defined as a method for conducting static or dynamic safety and dependability assessments/simulations (by fault propagation) based on a model written in a formal language and on a modular structure.

An MBSDA analysis presents the following properties/capabilities:

- Modelling of the functional and dysfunctional behaviour of the system to conduct a Safety & Dependability assessment;
- Performing several Safety & Dependability analyses from the same model by analysing different descriptors[1] ;
- Modelling of functions or organic components of a system structurally close to the design models;
- Modular aspect allowing to model a system from libraries of reusable modelling units;
- Global system behaviour obtained from the behaviour of modelling units and their interactions.

[1] Depending on the tools/languages, equivalent terms to the following: ‘observer’, ‘indicator’ or ‘observable’

3 Overview of the MBSDA study process

3.1 MBSDA REFERENCE FRAMEWORK

The guide for conducting an MBSDA study recommends that any organization intending to conduct MBSDA studies establishes an internal process aligned with the MBSDA reference framework presented in Figure 1. This framework is part of a broader Safety & Dependability management process (for example, in accordance with IEC 60300). The guide addresses only aspects specific to MBSDA studies.

A shared set of rules and best practices is highlighted through the detailed reference framework, ensuring that an MBSDA model accurately reflects its reference configuration (i.e., the key system elements to be considered at a given time for modelling, known as the 'Baseline').

The MBSDA reference framework, shown in Figure 1, consists of three main processes:

- Prepare the MBSDA study;
- Perform the MBSDA study;
- Support the MBSDA study.

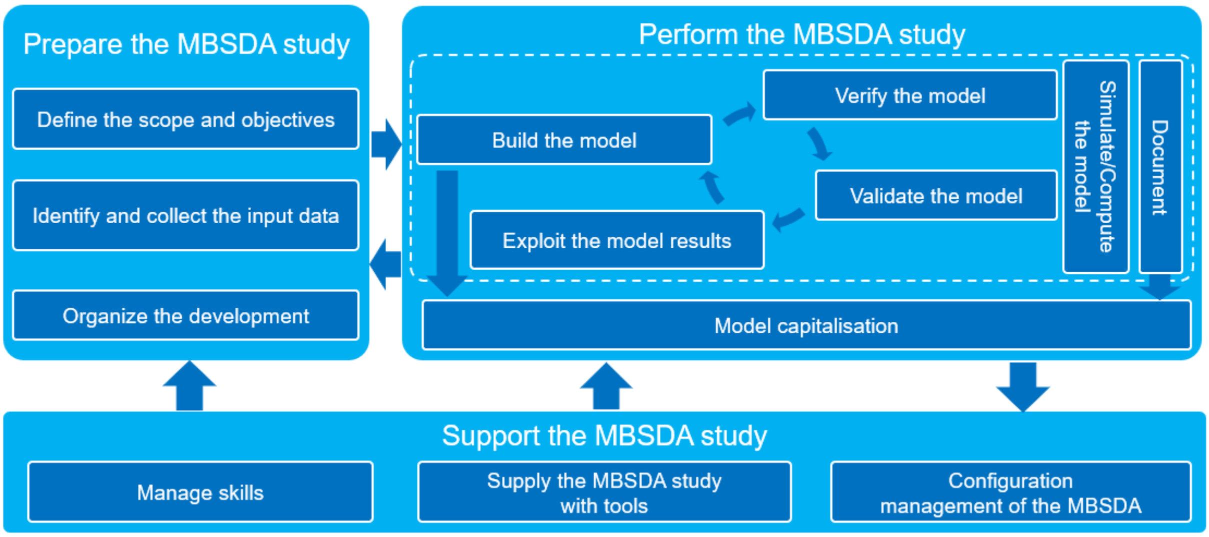
Prepare the MBSDA study
Define the scope and objectives
Identify and collect the input data
Organize the development
Perform the MBSDA study
Build the model
Verify the model
Validate the model
Exploit the model results
Simulate/Compute the model
Document
Model capitalisation
Support the MBSDA study
Manage skills
Supply the MBSDA study with tools
Configuration management of the MBSDA

Figure 1 – MBSDA reference framework

Each process and subprocess is detailed in the MBSDA guide. Two use cases, highlighting dynamic simulations and illustrating the overall methodology, are also provided in the guide's appendices:

- An emergency power supply system for a nuclear power plant;
- A heated tank.

The first use case demonstrates dynamic behaviours (such as reconfigurations and limited battery capacity). The second use case is a hybrid model incorporating continuous variables (for example, a dynamic failure rate that varies with temperature).

3.2 PREPARE THE MBSDA STUDY

The preparation of the MBSDA study involves setting the prerequisites for implementing MBSDA, contributing to the effectiveness of the approach. This approach is particularly suitable for Safety & Dependability analyses of systems with dynamic features, involving dependencies between system elements: reconfiguration, standby redundancy, limited resources, influence of the order of occurrence of events, consideration of continuous physical phenomena, etc.

This step allows for establishing and clarifying the need, gathering available data, and planning the MBSDA study both at the organizational and technical levels. The preparation of the MBSDA study includes the following three subprocesses:

- **Define the scope and objectives:** Defining the scope and objectives serves to justify conducting an MBSDA study. This phase involves characterizing the system under study, establishing the study's boundaries, defining the expected types of results, and identifying domain-specific constraints (industrial and/or normative context).

  The activities within this subprocess allow for formalizing the MBSDA requirements in the MBSDA requirement specification and initiating the formalization of modelling requirements in the modelling specification.

- **Identify and collect the input data:** This subprocess aims to ensure that all input data required for the MBSDA model are complete and traceable. Input data may vary depending on the type of system and its development stage, and may include elements from the definition file, descriptions of the system's life phases and missions, justification elements for the system definition, previous Safety & Dependability analyses (both qualitative and quantitative), the maintenance concept or logistics support details, data defining the system's environment, as well as system engineering–related data.

  The activities associated with this subprocess allow for the initialization of the configuration management subprocess, the creation of the first version of the model Baseline, and the completion of the formalization of modelling requirements in the modelling specification.

- **Organize the development:** This subprocess aims to organize the development of the MBSDA study. In this phase, the working environment must be selected, the relevance of reusing modelling units analysed, adaptation tasks identified, modelling rules defined, and MBSDA activities planned.

  The activities within this subprocess contribute to the finalization of the modelling specification by incorporating development and organizational requirements and/or by establishing a dedicated specification (such as a MBSDA plan or a MBSDA test plan).

3.3 PERFORM THE MBSDA STUDY

This process encompasses the essential steps for developing the MBSDA model, ensuring that the model remains representative of its Baseline. The process is partly iterative, involving successive phases:

- **Build the model:** The objective of this sub-process is to build all or part of the model used for the MBSDA study. This involves creating, adapting, or instantiating variable domains and modelling units; connecting modelling units or subsets of units to build the system model; modelling the system's common-cause (or common-mode) failures; modelling system reconfigurations (including their prioritization); and modelling the descriptor(s).
- **Verify the model:** The objective of this sub-process is to ensure the structural and behavioural compliance of the model with respect to the reference configuration of the system of interest. This involves verifying that the model's construction is consistent with its specification. The verification activities must be adapted to the complexity of the element concerned and to the modelling formalism used. The following sub-tasks may be carried out:
  - Compliance with modelling rules;
  - Syntactic and semantic review;
  - Compliance of variable typing/domain for each modelling unit;
  - Consistency of model events with input data and probability law parameters;
  - Proper use of all model inputs, outputs, and states;
  - Compliance of finite state machines (transitions);
  - Compliance of equations (differential or logical) based on the expected behaviour of the modelling unit;
  - Graphical visualisation displaying the correct colours and icons based on the states of the modelled components (in the case of a modelling using a graphical view);
  - Consistency of the links between the elements of the model (structural, functional, and/or organic coherence);

  - Compliance of the local behaviours of the model with any preliminary studies conducted on the system of interest;
  - Compliance of the equations related to the model descriptors;
  - Alignment with the expected behaviour of the options chosen for prioritising instantaneous or quasi-instantaneous transitions.

  Recommendations regarding the model for any non-compliance with a modelling requirement (criteria not met) shall be issued.
- **Validate the model:** The objective of this sub-process is to ensure that the results generated from the model, in relation to the model's reference configuration, are consistent and representative of the real system (state of knowledge) within the limits of the chosen level of abstraction. The tasks to be performed are as follows:
  - Validate the representativeness of the model in accordance with the requirements of the various stakeholders in the engineering project: This involves validating the compliance of the overall model's behaviour with the different scenarios identified in the modelling specification and in the MBSDA requirement specification, in collaboration with the various stakeholders;
  - Validate the consistency of the results generated by the model (consistency of the observed cut sets or sequences, and relevance of the quantitative results).

  Recommendations regarding the model for any non-compliance with a modelling / MBSDA requirement (criteria not met) shall be issued.
- **Exploit the model results:** This sub-process aims to analyse all the results generated by the model with regard to the requirements specified in the MBSDA requirement specification.

Supporting the iterative part throughout the development of the model, the '**Simulate/Compute the model**' sub-process enables the production of qualitative results (cut sets and sequences) and/or quantitative results (probability, numbers, etc.). This activity is carried out at different stages of construction, whenever simulation or computation is possible, in order to provide the expected results in response to the specifications or to verify/validate modelling units, assemblies of modelling units, or the complete model. It is essential to identify the required computation engines and the descriptor(s) on which the generated results must be analysed, as well as to correctly configure and parameterize the computation engines.

In parallel with the iterative part, it is necessary to '**Document'** the model throughout its development. The objectives of this sub-process are as follows:

- Document the information necessary for a good understanding of the model of the system of interest through the preparation of a modelling file;
- Justify the different modelling choices made through the preparation of a modelling choices file;
- Collect compliance proofs of the model of the system of interest with respect to the modelling specification and the MBSDA requirement specification through the preparation of a model definition justification file.

Once the model is validated, the '**Capitalize the model**' sub-process enables the preservation of the knowledge and experience gained during the development of the system-of-interest model, makes this knowledge and experience accessible and useful to other modelers, reduces the cost and time required to create future MBSDA models depending on the level of similarity between the architectures or components of the studied systems, and increases the efficiency of developing MBSDA models by leveraging knowledge and experience acquired from previous studies.

The following elements must be retained for each specific project milestone before being handed over to configuration management: the developed model, the modelling unit libraries associated with the model, and the documentation related to the model. For capitalization purposes, it is primarily recommended to identify, among these elements, the relevant information and the means of accessing all this information.

The expected outcome of this step is the creation of a useful and structured knowledge base for the analysis of new systems that share similarities with the one studied.

3.4 SUPPORT THE MBSDA STUDY

The support of the MBSDA study consists of identifying the resources that can be made available to modelers, enabling them to plan and implement the models. This process includes the following three subprocesses:

- **Manage skills:** This subprocess aims to acquire, develop, and maintain the skills of the Safety & Dependability engineers necessary for conducting an MBSDA study, and to raise awareness among Safety & Dependability engineers as well as other stakeholders about the approach and methodological rules for carrying out an MBSDA study.

  This will ensure the availability of modelers with a satisfactory level of competence for conducting MBSDA studies.

- **Supply the MBSDA study with tools:** The objective of this subprocess is to identify the appropriate tools to meet the needs of the MBSDA study.

  The expected outcome is the provision of tools fully meeting the study's requirements, the adoption of a tool partially meeting the requirements, or the decision to forgo the need if no suitable tool is available.

- **Configuration management of the MBSDA:** The objectives of this subprocess are to monitor and control changes made to the model and its associated documentation according to the model baseline throughout the model's lifecycle, to know at any given time which reference version is being used and its evolution, to enable reverting to previous versions of the model to understand the origin and consequences of a belatedly discovered error, to help ensure that the model remains consistent with its reference (system of interest/modelling need), to have continuous knowledge of the simulated model, and to identify any discrepancies resulting from ongoing modifications.

  The outcomes of this subprocess are a database for storing the different versions of model elements (including frozen reference configurations), and configuration states defined for the model baselines, serving as reference points for the results of the MBSDA study.

4 Deliverables table for an MBSDA study

Table 1 of deliverables presented below lists all the deliverables to be considered in the context of an MBSDA study.

Table 1 – Deliverables of an MBSDA study

Deliverable	Deliverable Description	Related Process	Related Sub-process
MBSDA requirement specification	MBSDA requirements	Prepare the MBSDA study	Define the scope and objectives
Modelling specification (first version)	First version of modelling requirements	Prepare the MBSDA study	Define the scope and objectives
Modelling specification (second version)	Second version of modelling requirements	Prepare the MBSDA study	Identify and collect the input data
Modelling specification (third version)	Third version of modelling requirements	Prepare the MBSDA study	Organize the development
MBSDA plan	MBSDA study general development organisation	Prepare the MBSDA study	Organize the development
MBSDA test plan	Strategy for implementing model verification and validation	Prepare the MBSDA study	Organize the development
Modelling file	Information required for a proper understanding of the model of the system of interest	Perform the MBSDA study	Document
Modelling choices file	Justification of the different modelling choices	Perform the MBSDA study	Document
Model definition justification file	Evidence proving compliance of the model of the system of interest with the modelling specification and the MBSDA requirement specification	Perform the MBSDA study	Document

5 Presentation of use cases

5.1 FIRST USE CASE

The first use case concerns a 6.6 kV emergency power supply system for a nuclear power plant. This use case was modelled using the AltaRica Data-Flow language (SimfiaNeo tool) and the Figaro language (RiskSpectrum ModelBuilder tool). Two parts were modelled: the 'High Voltage' part and the 'Low Voltage' part, as shown in Figure 2 and Figure 3:

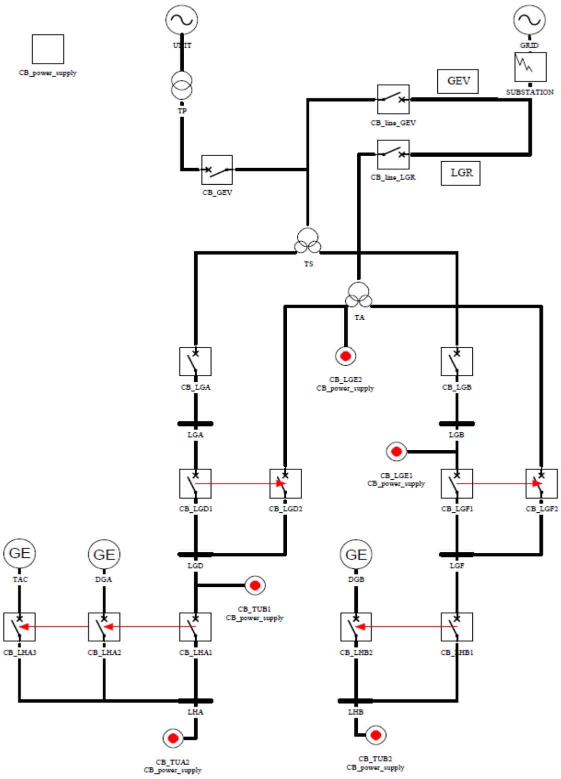

Figure 2 – High Voltage part of the 6.6kV power supply system

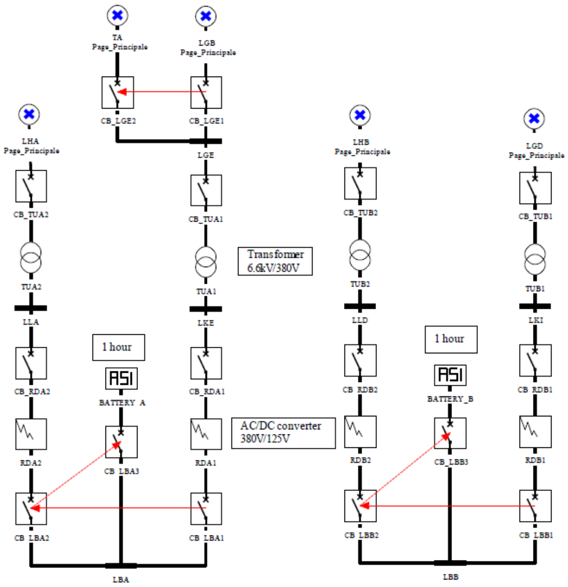

Figure 3 – Low Voltage Part of the 6.6kV Power Supply System

5.2 SECOND USE CASE

The second use case concerns a heated tank system. This system was represented by considering both physical phenomena and phenomena involving discrete events or states. The studied system contains both continuous and discrete variables. This use case was modelled using the Python language (PyCATSHOO and PyCATSHOO Designer tools).

The system consists of two pumps, a valve, a water tank, and a heat source. Its characteristics can be seen in the Figure 4:

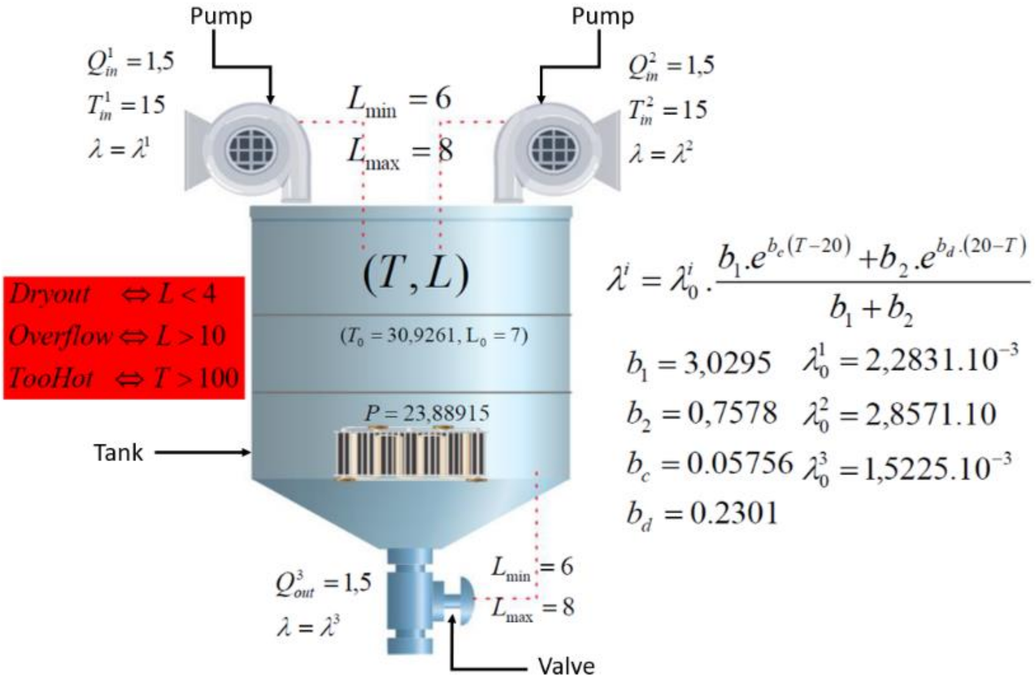
Pump
$Q_{in}^1 = 1{,}5$
$T_{in}^1 = 15$
$\lambda = \lambda^1$
Pump
$Q_{in}^2 = 1{,}5$
$T_{in}^2 = 15$
$\lambda = \lambda^2$
$L_{\min} = 6$
$L_{\max} = 8$
(T, L)
$(T_0 = 30{,}9261, L_0 = 7)$
$P = 23{,}88915$
$Dryout \Leftrightarrow L < 4$
$Overflow \Leftrightarrow L > 10$
$TooHot \Leftrightarrow T > 100$
Tank
$\lambda^i = \lambda_0^i . \frac{b_1.e^{b_c(T-20)} + b_2.e^{b_d.(20-T)}}{b_1 + b_2}$
$b_1 = 3{,}0295$ $\lambda_0^1 = 2{,}2831.10^{-3}$
$b_2 = 0{,}7578$ $\lambda_0^2 = 2{,}8571.10$
$b_c = 0.05756$ $\lambda_0^3 = 1{,}5225.10^{-3}$
$b_d = 0.2301$
$Q_{out}^3 = 1{,}5$
$\lambda = \lambda^3$
$L_{\min} = 6$
$L_{\max} = 8$
Valve

Figure 4 – Representation of the heated tank system