SYNTHESE

Guide de réalisation d'une étude MBSDA (*Model-Based Safety & Dependability Analysis*)

Projet P23-2 pour l'Institut pour la Maîtrise des Risques (IMdR)

Ind A

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

Le 19 août 2025

Rédacteurs

Mustafa MOHAMED ABDALLA
Ingénieur Sûreté de Fonctionnement (LGM)

Vérificateurs

Frédéric MILCENT
Expert Sûreté de Fonctionnement (Naval Group)

Marc BOUISSOU
Expert Sûreté de Fonctionnement (IMdR)

Approbateurs

Frédéric MILCENT
Expert Sûreté de Fonctionnement (Naval Group)

Marc BOUISSOU
Expert Sûreté de Fonctionnement (IMdR)

Historique des évolutions

Version	Date	Évolutions
A	19/08/2025	Création du document

Sommaire

1 Objet du document

Ce document a pour objectif de résumer le guide de réalisation d'une étude MBSDA (*Model-Based Safety & Dependability Analysis*) réalisé dans le cadre du projet P23-2 pour l'IMdR (Institut pour la Maitrise des Risques). Ce guide a été réalisé sur une période de 18 mois en collaboration avec différentes organisations : AIRBUS Protect, Arianegroup, DGA, EDF, INSA, ISAE-SUPMECA, LGM, MBDA, Naval Group, RATP, Thales. Cette initiative a permis à des experts de ces organisations utilisant différents outils et langages de modélisation de comparer leurs pratiques, de proposer des définitions normalisées et d'établir des bases communes pour les méthodes de modélisation.

Ce guide, réalisé à partir du retour d'expérience des membres du projet P23-2 et de l'état de l'art actuel, établit un cadre commun, clair et de confiance pour la réalisation des études MBSDA. Un socle partagé de règles et de bonnes pratiques est mis en avant dans le guide afin de garantir la représentativité d'un modèle MBSDA, sa pertinence et son acceptation par les parties prenantes en relation avec la Sûreté de Fonctionnement.

Le guide, rédigé sous un format de document normatif (IEC (*International Electrotechnical Commission*)), servira de référence à la communauté pour la réalisation d'analyses de Sûreté de Fonctionnement en MBSDA et pourrait constituer la base d'un futur projet de normalisation.

2 *Model-Based Safety & Dependability Analysis* (MBSDA)

Le MBSDA a été défini comme étant une méthode permettant de réaliser des évaluations / simulations statiques ou dynamiques de Sûreté de Fonctionnement (par propagation de défaillances) basée sur un modèle rédigé dans un langage formel et reposant sur une structure modulaire.

Une analyse MBSDA présente notamment les propriétés / capacités suivantes :

- Modélisation du comportement fonctionnel et dysfonctionnel du système dans le but de réaliser une évaluation de Sûreté de Fonctionnement ;
- Réalisation de plusieurs analyses de Sûreté de Fonctionnement à partir d'un même modèle en analysant différents descripteurs[1] ;
- Modélisation de fonctions ou composants organiques d'un système structurellement proches des modèles de la conception ;
- Aspect modulaire permettant de modéliser un système à partir de bibliothèques d'unités de modélisation réutilisables ;
- Comportement global du système obtenu à partir du comportement des unités de modélisation et de leurs interactions.

[1] Suivant les outils/langages, terme équivalent aux suivants : « *observer* », « indicateur » ou « observable »

3 Présentation du processus de réalisation d'une étude MBSDA

3.1 CADRE DE REFERENCE MBSDA

Le guide de réalisation d'une étude MBSDA recommande que toute organisation souhaitant réaliser des études MBSDA établisse un processus interne aligné avec le cadre de référence MBSDA présenté dans la Figure 1. Ce cadre fait partie d'un processus plus large de gestion de la sécurité et de la disponibilité (par exemple, conformément à la norme IEC 60300). Le guide aborde uniquement les aspects spécifiques aux études MBSDA.
Une base partagée de règles et de bonnes pratiques est mise en avant à travers le cadre de référence détaillé, garantissant qu'un modèle MBSDA reflète avec précision sa configuration de référence (c'est-à-dire, les éléments clés du système d'intérêt à prendre en compte, à un instant donné, pour la modélisation, connus sous le nom de « Baseline »).
Le cadre de référence MBSDA, présenté dans la Figure 1, est composé de trois processus principaux :

- Préparer l'étude MBSDA ;
- Réaliser l'étude MBSDA ;
- Soutenir l'étude MBSDA.

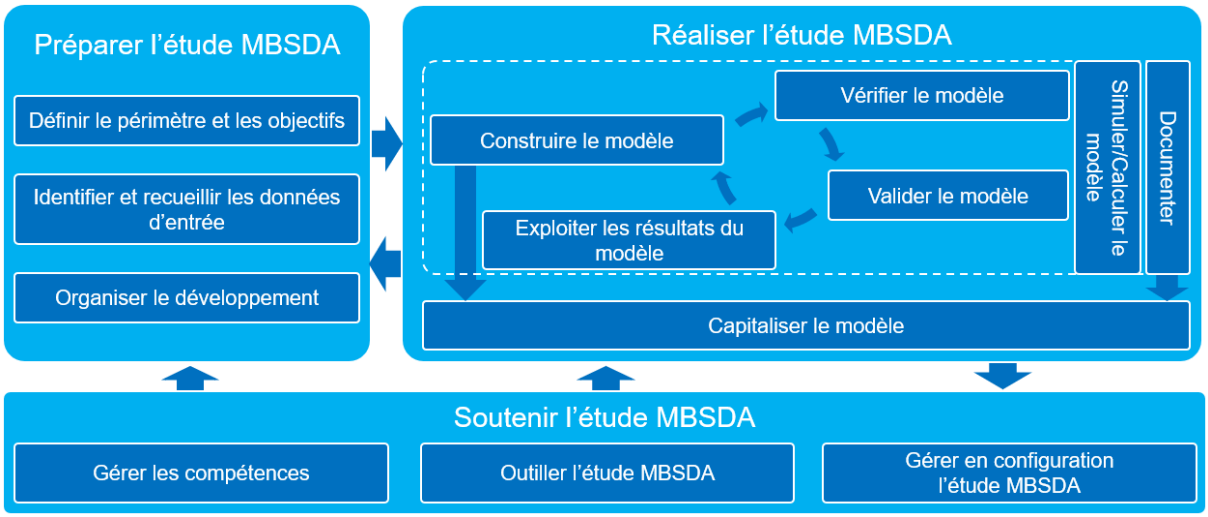

Figure 1 – Cadre de référence MBSDA

Chaque processus et sous-processus est détaillé dans le guide MBSDA. Deux cas d'utilisation mettant en avant des simulations dynamiques et illustrant la méthodologie globale sont également fournis dans les annexes du guide :

- Un système d'alimentation électrique d'urgence pour une centrale nucléaire ;
- Un réservoir chauffé.

Le premier cas d'utilisation démontre des comportements dynamiques (tels que des reconfigurations et une capacité limitée de batterie). Le second cas d'utilisation est un modèle hybride incorporant des variables continues (par exemple, un taux de défaillance dynamique qui varie en fonction de la température).

3.2 PREPARER L'ETUDE MBSDA

La préparation de l'étude MBSDA consiste à fixer les conditions préalables à la mise en œuvre du MBSDA, contribuant à l'efficacité de l'approche. Cette approche est particulièrement adaptée pour les analyses de Sûreté de Fonctionnement de systèmes présentant une composante dynamique impliquant

une dépendance entre les éléments du système : reconfiguration, redondance passive, ressources limitées, influence de l'ordre d'occurrence des événements, prise en compte de phénomènes physiques continus, etc.

Cette étape permet d'établir et de préciser le besoin, de recenser les données disponibles et de planifier l'étude MBSDA tant au niveau organisationnel que technique. La préparation de l'étude MBSDA comprend les trois sous-processus suivants :

- **Définir le périmètre et les objectifs :** La définition du périmètre et des objectifs permet de justifier la réalisation d'une étude MBSDA. Cette phase implique la caractérisation du système à étudier, l'établissement du périmètre de l'étude, la définition des types de résultats attendus et l'identification des contraintes spécifiques au domaine d'application (contexte industriel et/ou normatif).

  Ces activités du sous-processus permettent de formaliser les exigences de besoin MBSDA dans la spécification technique de besoin MBSDA, et d'initier la formalisation des exigences de modélisation dans la spécification de modélisation.

- **Identifier et recueillir les données d'entrée :** Ce sous-processus vise à garantir que toutes les données d'entrée nécessaires au modèle MBSDA sont complètes et traçables. Les données d'entrée peuvent varier selon le type de système et son stade de développement, et peuvent inclure les éléments du dossier de définition, la description des phases de vie du système et de ses missions, les éléments de justification de la définition, les analyses de Sûreté de Fonctionnement antérieures (qualitatives et quantitatives), le concept de maintenance ou détails du soutien logistique, les données définissant l'environnement du système ou encore les données liées à l'ingénierie système.

  Les activités liées à ce sous-processus permettent d'initialiser le sous-processus de gestion de configuration, d'initier la première version de la Baseline du modèle et d'achever la formalisation des exigences de modélisation dans la spécification de modélisation.

- **Organiser le développement :** Ce sous-processus a pour objectif d'organiser le développement de l'étude MBSDA. Dans cette phase, l'environnement de travail doit être choisi, la pertinence de la réutilisation d'unités de modélisation doit être analysée, les travaux d'adaptation doivent être identifiés, les règles de modélisation doivent être définies et les activités MBSDA doivent être planifiées.

  Les activités de ce sous-processus contribuent à la finalisation de la spécification de modélisation en intégrant les exigences de développement et organisationnelles et/ou en établissant une spécification dédiée (telle qu'un plan MBSDA ou un plan de test).

3.3 REALISER L'ETUDE MBSDA

Ce processus englobe les étapes essentielles pour le développement du modèle MBSDA permettant de garantir la représentativité du modèle par rapport à sa Baseline. Ce processus est en partie itératif avec des phases successives :

- **Construire le modèle :** L'objectif de ce sous-processus est de construire tout ou partie du modèle utilisé pour l'étude MBSDA. Il s'agit ici de créer/adapter/instancier les domaines des variables et les unités de modélisation, de connecter les unités de modélisation ou des sous-ensembles d'unités de modélisation pour la constitution du modèle du système, de modéliser les modes communs (ou causes communes) de défaillance du système, de modéliser les reconfigurations du système (y compris leur priorisation) et de modéliser le/les descripteur(s).
- **Vérifier le modèle :** L'objectif de ce sous-processus est de garantir la conformité structurelle et comportementale du modèle par rapport à la configuration de référence du système d'intérêt. Il s'agit ici de vérifier que la construction du modèle est conforme à sa spécification. Les activités de vérification doivent être adaptées à la complexité de l'élément concerné et au formalisme de modélisation utilisé. Les sous-tâches suivantes peuvent être réalisées :
  - Respect des règles de modélisation ;
  - Examen syntaxique et sémantique ;
  - Conformité du typage/domaine des variables de chaque unité de modélisation ;
  - Cohérence des événements du modèle avec les données d'entrée et les paramètres des lois de probabilité ;

- Bon usage de toutes les entrées, sorties et états du modèle ;
- Conformité des automates à états finis (transitions) ;
- Conformité des équations (différentielles ou logiques) en fonction du comportement de l'unité de modélisation attendu ;
- Visualisation graphique affichant les bonnes couleurs et icônes en fonction des états des composants modélisés (dans le cas d'une modélisation utilisant une vue graphique) ;
- Bonne cohésion des liens entre les éléments du modèle (cohérence structurelle, fonctionnelle et/ou organique) ;
- Conformité des comportements locaux du modèle par rapport à d'éventuelles études préliminaires réalisées sur le système d'intérêt étudié ;
- Conformité des équations relatives aux descripteurs du modèle ;
- Correspondance avec le comportement attendu des options prises pour la priorisation des transitions instantanées ou quasi-instantanées (problématique des reconfigurations en cascade correspondant à plusieurs actions de reconfiguration dans un ordre donné et sur une durée très courte).

Des recommandations sur le modèle pour tout non-respect d'une exigence de modélisation (critères non-atteints) doivent être émises.

- **Valider le modèle :** L'objectif de ce sous-processus est de garantir que les résultats générés à partir du modèle, en lien avec la configuration de référence du modèle, sont cohérents et représentatifs du système réel (état des connaissances) dans les limites de l'abstraction retenue. Les tâches à réaliser sont les suivantes :
  - Valider la représentativité du modèle conformément aux exigences des différentes parties prenantes du projet d'ingénierie : Il s'agit de valider la conformité du comportement du modèle global selon les différents scénarios identifiés dans la spécification de modélisation et dans la spécification technique de besoin MBSDA, en collaboration avec les différentes parties prenantes ;
  - Valider la cohérence des résultats générés par le modèle (cohérence des coupes/séquences observées et pertinence des résultats quantitatifs).

  Des recommandations sur le modèle pour tout non-respect d'une exigence de modélisation/besoin MBSDA (critères non-atteints) doivent être émises.
- **Exploiter les résultats du modèle :** Ce sous-processus vise à analyser l'ensemble des résultats générés par le modèle au regard des exigences spécifiées dans la spécification technique de besoin MBSDA.

En support de la partie itérative durant toute la réalisation du modèle, le sous-processus « **Simuler/Calculer le modèle** » permet l'obtention des résultats qualitatifs (coupes et séquences) et/ou quantitatifs (probabilité, nombre, etc.). Cette activité est faite à différents stades de construction, dès lors que la simulation ou les calculs sont possibles afin de fournir les résultats attendus dans le cadre de la réponse aux spécifications ou de vérifier/valider des unités de modélisation, des assemblages de ces unités de modélisation ou le modèle complet. Il est essentiel d'identifier les moteurs de calcul nécessaires et le(s) descripteur(s) sur le(s)quel(s) les résultats générés doivent être exploités, ainsi que de correctement configurer et paramétrer les moteurs de calcul.

En parallèle de la partie itérative, il est nécessaire de « **Documenter** » le modèle durant toute sa réalisation. Les objectifs de ce sous-processus sont les suivants :

- Documenter les informations nécessaires à la bonne compréhension du modèle du système d'intérêt à travers la rédaction d'un dossier de modélisation ;
- Justifier les différents choix de modélisation effectués à travers la rédaction d'un dossier de choix de modélisation ;
- Recueillir les preuves de conformité du modèle du système d'intérêt par rapport aux exigences de la spécification de modélisation et aux exigences de la spécification technique de besoin MBSDA à travers la rédaction d'un dossier justificatif de définition du modèle.

Lorsque le modèle est validé, le sous-processus « **Capitaliser le modèle** » permet de conserver les connaissances et les expériences acquises lors de la réalisation du modèle du système d'intérêt, de rendre accessibles et utiles les connaissances et les expériences pour d'autres modélisateurs, de réduire les coûts et les délais de création de futurs modèles MBSDA en fonction du niveau de similarité entre les architectures ou composants des systèmes étudiés, et d'augmenter l'efficacité de la réalisation

de modèles MBSDA en utilisant les connaissances et les expériences acquises sur des études précédentes.

Les éléments suivants doivent être conservés pour chaque jalon projet spécifique avant d'être transmis ensuite en gestion de configuration : le modèle réalisé, les bibliothèques d'unités de modélisation liées au modèle et la documentation associée au modèle. Pour la capitalisation, il est principalement préconisé d'identifier, parmi ces éléments, les informations pertinentes et les moyens d'accès à toutes ces informations.

Le résultat attendu à l'issue de cette étape est la constitution d'une base de connaissance utile et structurée pour l'analyse de nouveaux systèmes présentant des similitudes avec celui étudié.

3.4 SOUTENIR L'ETUDE MBSDA

Le soutien de l'étude MBSDA consiste à identifier les moyens qui peuvent être mis à la disposition des modélisateurs leur permettant de planifier et de réaliser les modèles. Ce processus comprend les trois sous-processus suivants :

- **Gérer les compétences :** Ce sous-processus vise à acquérir, développer et entretenir les compétences des ingénieurs en Sûreté de Fonctionnement nécessaires pour la réalisation d'une étude MBSDA, et de sensibiliser les ingénieurs en Sûreté de Fonctionnement ainsi que les autres parties prenantes à la démarche et aux règles méthodologiques pour la réalisation d'une étude MBSDA.

  Ceci permettra de disposer de modélisateurs avec un niveau de compétence satisfaisant pour la réalisation d'études MBSDA.

- **Outiller l'étude MBSDA :** L'objectif de ce sous-processus est d'identifier les outils adéquats pour répondre au besoin de l'étude MBSDA.

  Le résultat attendu est la mise à disposition d'outils répondant pleinement aux exigences de l'étude, l'adoption d'un outil répondant partiellement aux exigences, ou la décision de renoncer au besoin si aucun outil adapté n'est disponible.

- **Gérer en configuration l'étude MBSDA :** Les objectifs de ce sous-processus sont de suivre et de contrôler les modifications apportées au modèle et à la documentation associée selon la Baseline du modèle tout au long du cycle de vie du modèle, de savoir quel est à tout instant le référentiel utilisé et d'en connaître ses évolutions, de permettre de remonter à des versions antérieures du modèle pour comprendre l'origine et les conséquences d'une erreur trouvée tardivement, de contribuer à l'assurance que le modèle est en cohérence avec l'objet du modèle (système d'intérêt/besoin de modélisation), de connaître à tout moment le modèle simulé et d'identifier d'éventuels écarts dus à des modifications en cours d'instruction.

  Les résultats de ce sous-processus sont une base de données permettant de stocker les différentes versions des éléments du modèle (y compris les configurations de référence figées), et des états de configuration définis pour les Baselines du modèle servant de points de référence pour les résultats de l'étude MBSDA.

4 Table des livrables d'une étude MBSDA

Le Tableau 1 des livrables présenté ci-dessous recense tous les livrables à prendre en considération dans le cadre de la réalisation d'une étude MBSDA.

Tableau 1 – Livrables d'une étude MBSDA

Livrable	Description du livrable	Processus concerné	Sous-processus concerné
Spécification technique de besoin MBSDA	Exigences de besoin MBSDA	Préparer l'étude MBSDA	Définir le périmètre et les objectifs
Spécification de modélisation (première version)	Première version des exigences de modélisation	Préparer l'étude MBSDA	Définir le périmètre et les objectifs
Spécification de modélisation (deuxième version)	Deuxième version des exigences de modélisation	Préparer l'étude MBSDA	Identifier et recueillir les données d'entrée
Spécification de modélisation (troisième version)	Troisième version des exigences de modélisation	Préparer l'étude MBSDA	Organiser le développement
Plan MBSDA	Organisation générale du développement de l'étude MBSDA	Préparer l'étude MBSDA	Organiser le développement
Plan de test	Stratégie de mise en place de la vérification & validation du modèle	Préparer l'étude MBSDA	Organiser le développement
Dossier de modélisation	Informations nécessaires à la bonne compréhension du modèle du système d'intérêt	Réaliser l'étude MBSDA	Documenter
Dossier de choix de modélisation	Justification des différents choix de modélisation effectués	Réaliser l'étude MBSDA	Documenter
Dossier justificatif de définition du modèle	Preuves de conformité du modèle du système d'intérêt par rapport à la spécification de modélisation et à la spécification technique de besoin MBSDA	Réaliser l'étude MBSDA	Documenter

5 Présentation des cas d'utilisation

5.1 PREMIER CAS D'UTILISATION

Le premier cas d'utilisation concerne un système d'alimentation électrique d'urgence 6,6 kV pour une centrale nucléaire. Ce cas d'utilisation a été modélisé avec le langage AltaRica Data-Flow (outil SimfiaNeo) et le langage Figaro (outil *RiskSpectrum ModelBuilder*). Deux parties ont été modélisées, la partie « *High Voltage* » et la partie « *Low Voltage* » présentées dans la Figure 2 et la Figure 3 :

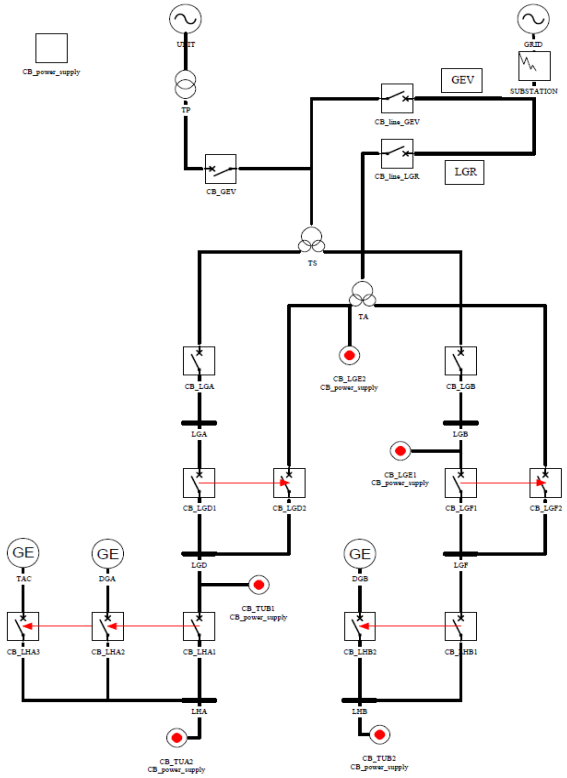

Figure 2 – Partie High Voltage du système d'alimentation électrique 6,6kV

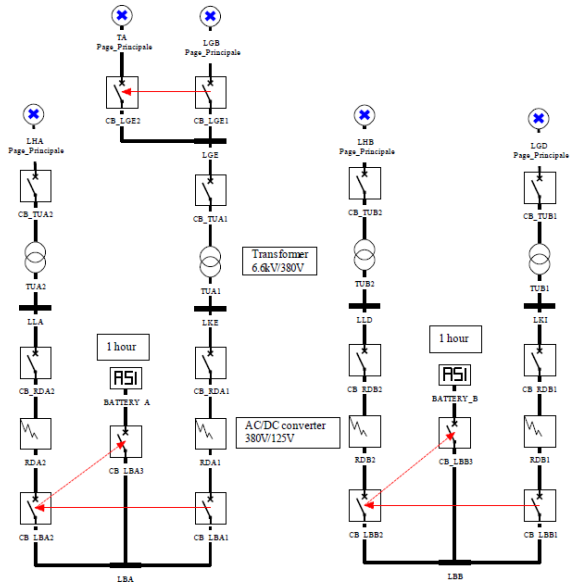

Figure 3 – Partie Low Voltage du système d'alimentation électrique 6,6kV

5.2 DEUXIEME CAS D'UTILISATION

Le deuxième cas d'utilisation concerne un système de réservoir chauffé. Ce système a été représenté en prenant en compte des phénomènes physiques et des phénomènes impliquant des événements ou des états discrets. Le système étudié contient à la fois des variables continues et des variables discrètes. Ce cas d'utilisation a été modélisé avec le langage Python (outils PyCATSHOO et PyCATSHOO Designer).

Le système est composé de deux pompes, d'une vanne, d'un réservoir d'eau (*tank*) et d'une source de chaleur (*fuel*). On peut voir ses caractéristiques sur la Figure 4 :

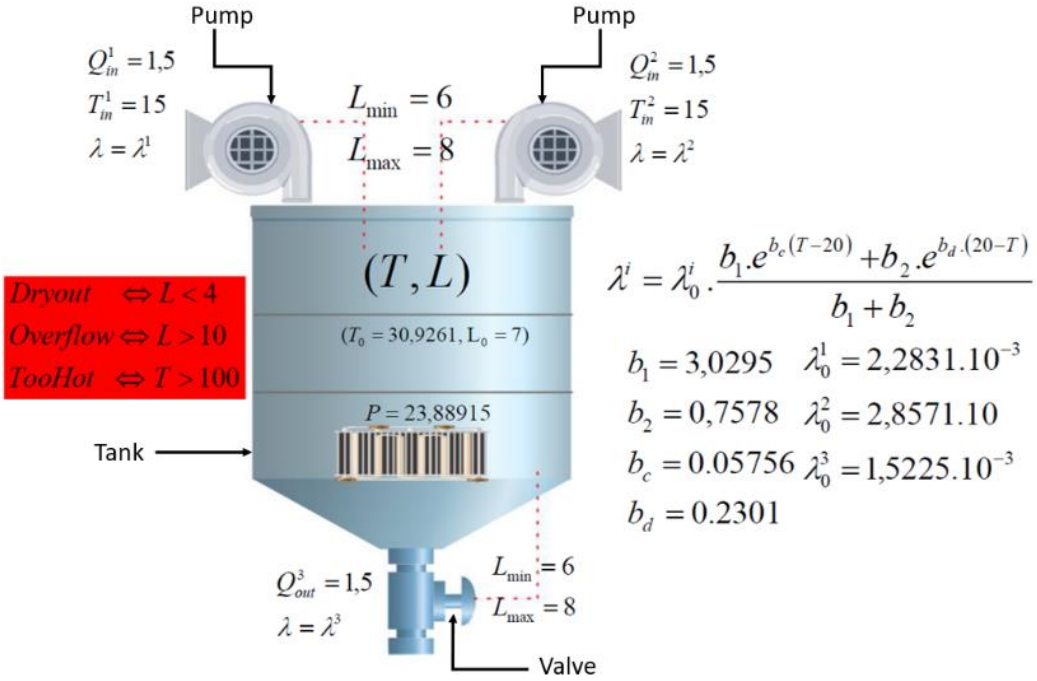

Figure 4 – Représentation du système de réservoir chauffé