Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

POWER AT SEA

APPLICATION DU GUIDE MODEL-BASED SAFETY & DEPENDABILITY ANALYSIS (IMDR) SUR UN MODÈLE ALTARICA

Frédéric MILCENT

Expert en Sûreté de Fonctionnement
Naval Group

12/12/2025

Application du guide MBSDA (IMdR) sur un modèle AltaRica

GUIDE DE RÉALISATION D'UNE ÉTUDE MBSDA

GUIDE MBSDA
PROJET IMDR

- Projet IMdR réalisé sur une période de 18 mois
- Prise en compte de l'état de l'art
- Confrontation des pratiques des experts des différentes organisations
- Différents outils et langages
- Proposition de définitions et de méthodes communes
- Objectif du guide : **Donner un cadre commun, clair et de confiance pour la réalisation d'études MBSDA afin de garantir la représentativité d'un modèle MBSDA, sa pertinence et son acceptation**
- Guide au format IEC (International Electrotechnical Commission) facilitant la transposition en projet de normalisation

GUIDE MBSDA
GROUPE DE PROJET IMDR

Souscripteurs

AIRBUS PROTECT	Xavier DE BOSSOREILLE
NAVAL GROUP	Frédéric MILCENT
arianeGROUP	Frédéric LOIR
MBDA MISSILE SYSTEMS	Gaëtan PELLOQUIN
DGA	Celia DESPOCQ
RATP	Victor DEBUIRE
EDF	Romain ROY Hassane CHRAIBI
THALES	Emmanuel CLEMENT Joseph MACHROUH

Chefs de projet

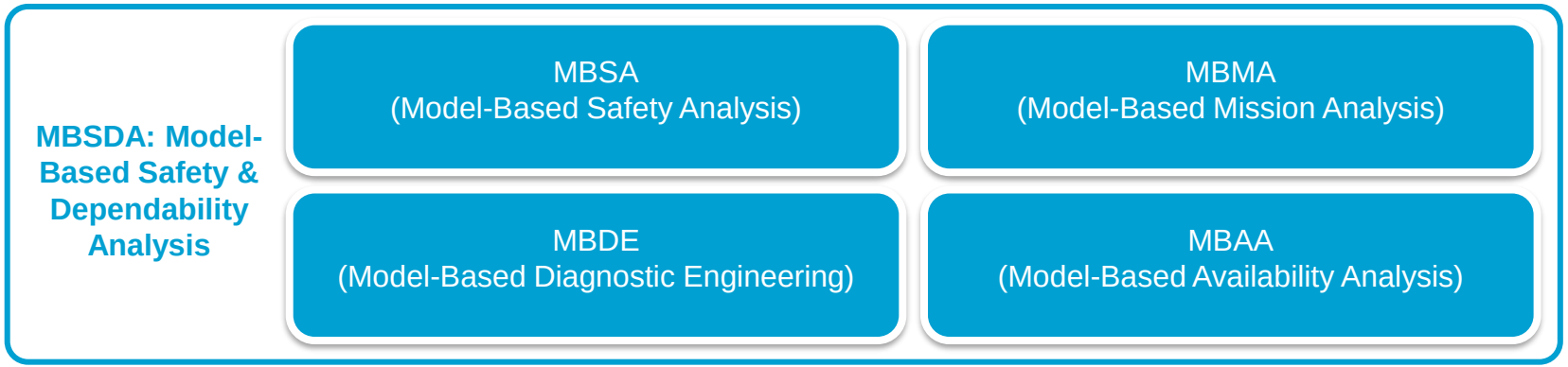
IMdR	Marc BOUISSOU

Equipe support

lgm/	Mustafa MOHAMED ABDALLA Frédéric DESCHAMPS
INSA CENTRE VAL DE LOIRE	Frédéric KRATZ Vincent IDASIAK
isae supméca	Faïda MHENNI Jean-Yves CHOLEY

GUIDE MBSDA
DÉFINITION MBSDA

- 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.
- Ce terme regroupe les différentes analyses FMDS/RAMS réalisées à partir de modèles

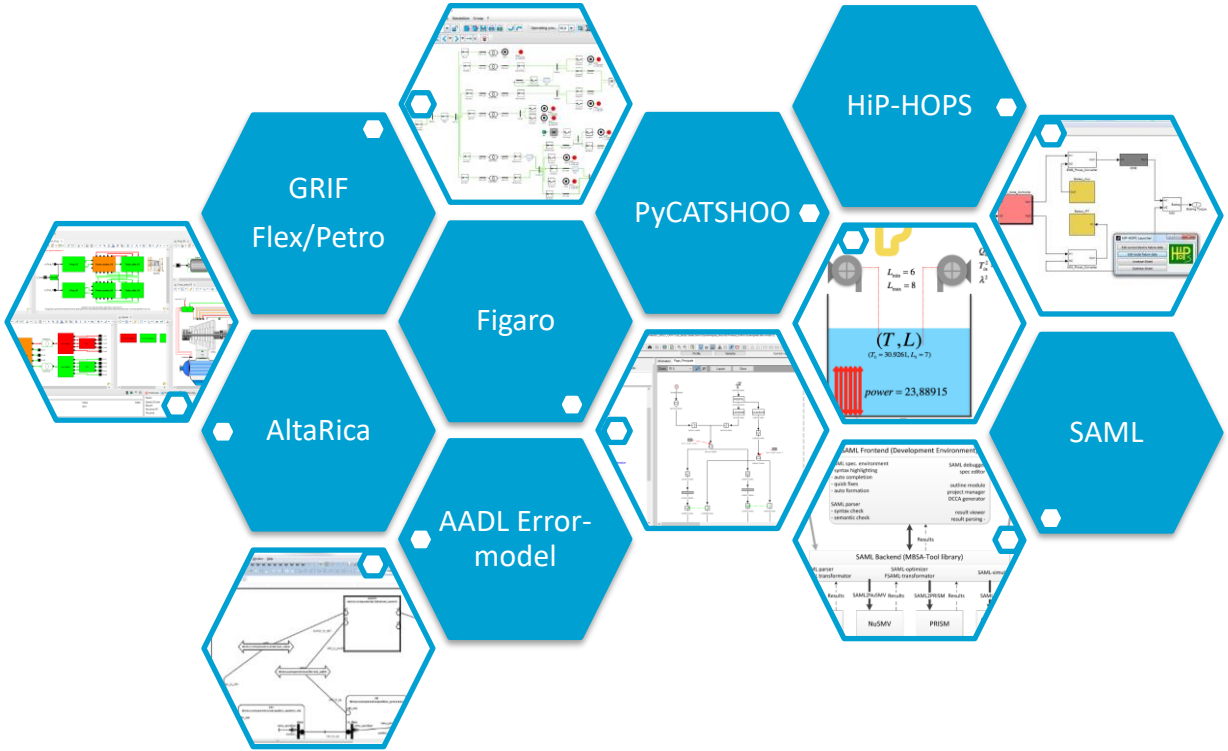


GUIDE MBSDA
PROPRIÉTÉS / CAPACITÉS DU MBSDA

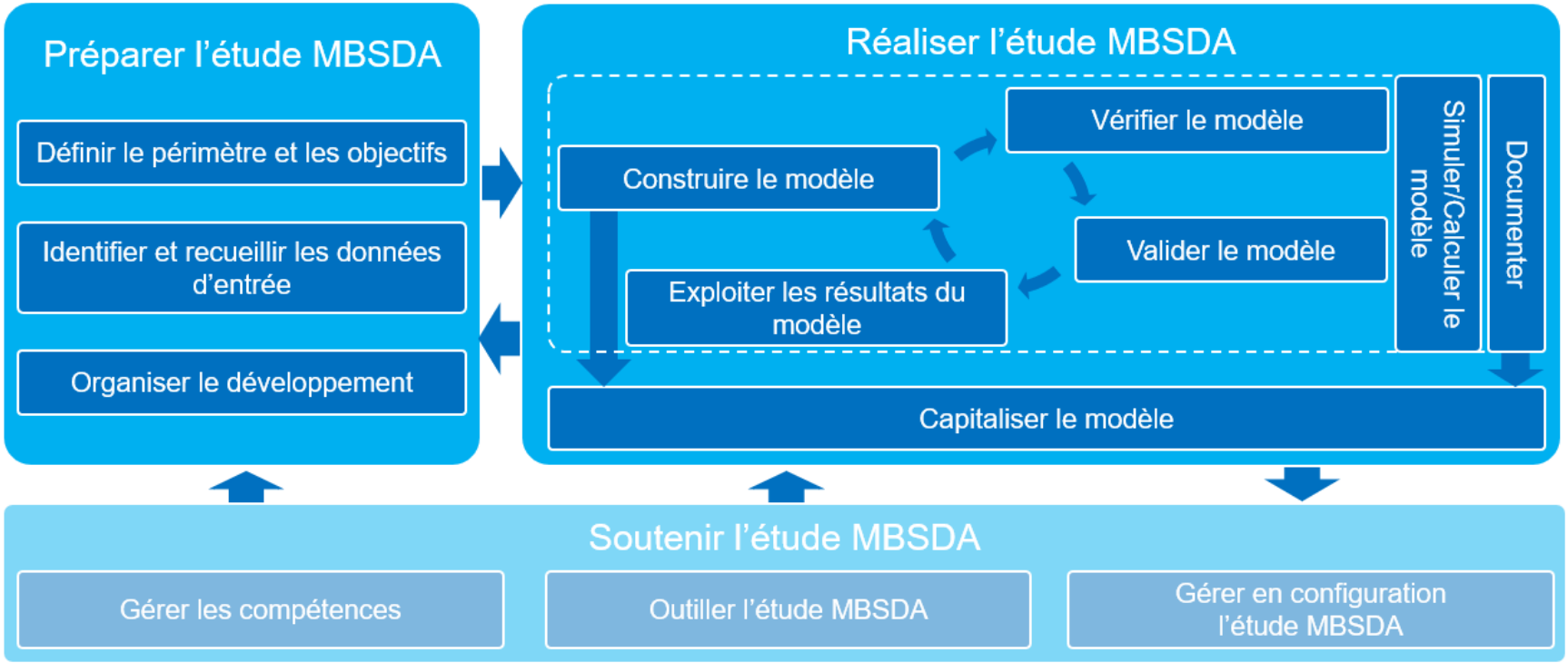
- Modélisation du comportement fonctionnel et dysfonctionnel du système dans le but de réaliser une évaluation de Sûreté de Fonctionnement
- Réalisation de plusieurs analyses de Sûreté de Fonctionnement à partir d'un même modèle en analysant différents descripteurs[1]
- Modélisation de fonctions ou composants 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] : « observer » en AltaRica

MBSDA
QUELQUES LANGAGES / OUTILS



GUIDE MBSDA
CADRE DE RÉFÉRENCE



Sous-processus non abordé dans cette présentation (pas spécifique au cas d'application)

GUIDE MBSDA
CONTENU

- Introduction / Définitions
- Préparer l'étude MBSA
  - Définir le périmètre et les objectifs
  - Identifier et recueillir les données d'entrée
  - Organiser le développement
- Réaliser l'étude MBSDA
  - Construire le modèle
  - Vérifier le modèle
  - Valider le modèle
  - Exploiter les résultats du modèle
  - Calculer / Simuler le modèle
  - Documenter
  - Capitaliser le modèle

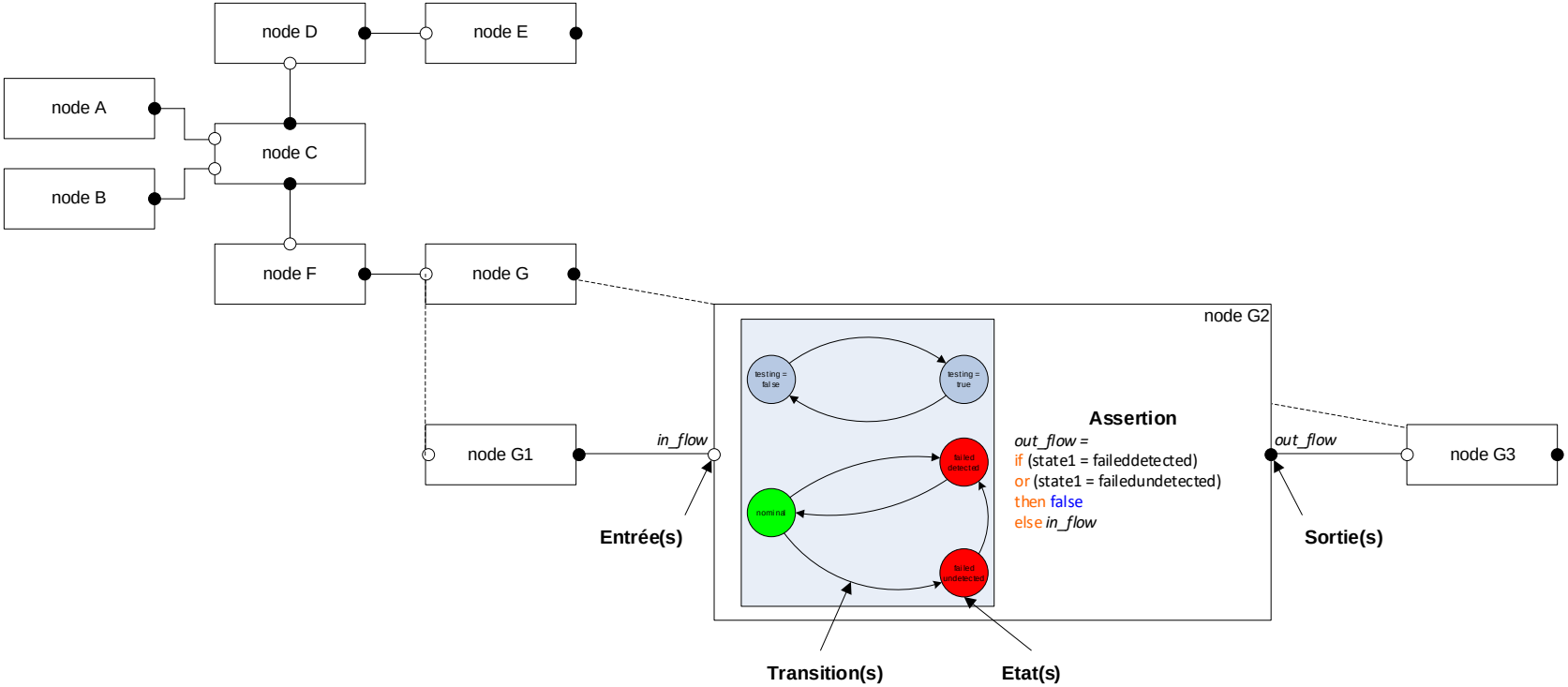
- Soutenir l'étude MBSDA
  - Gérer les compétences
  - Outiller l'étude MBSDA
  - Gérer en configuration l'étude MBSDA
- Cas d'application en annexes

Disponible au téléchargement sur le site de l'IMdR : https://www.imdr.eu/offres/gestion/actus_818_46591-2312/guide-de-realisation-d-une-etude-mbsda-model-based-safety-dependability-analysis.html

Application du guide MBSDA (IMdR) sur un modèle AltaRica

ALTARICA DATAFLOW

ALTARICA DATAFLOW



ALTARICA DATAFLOW

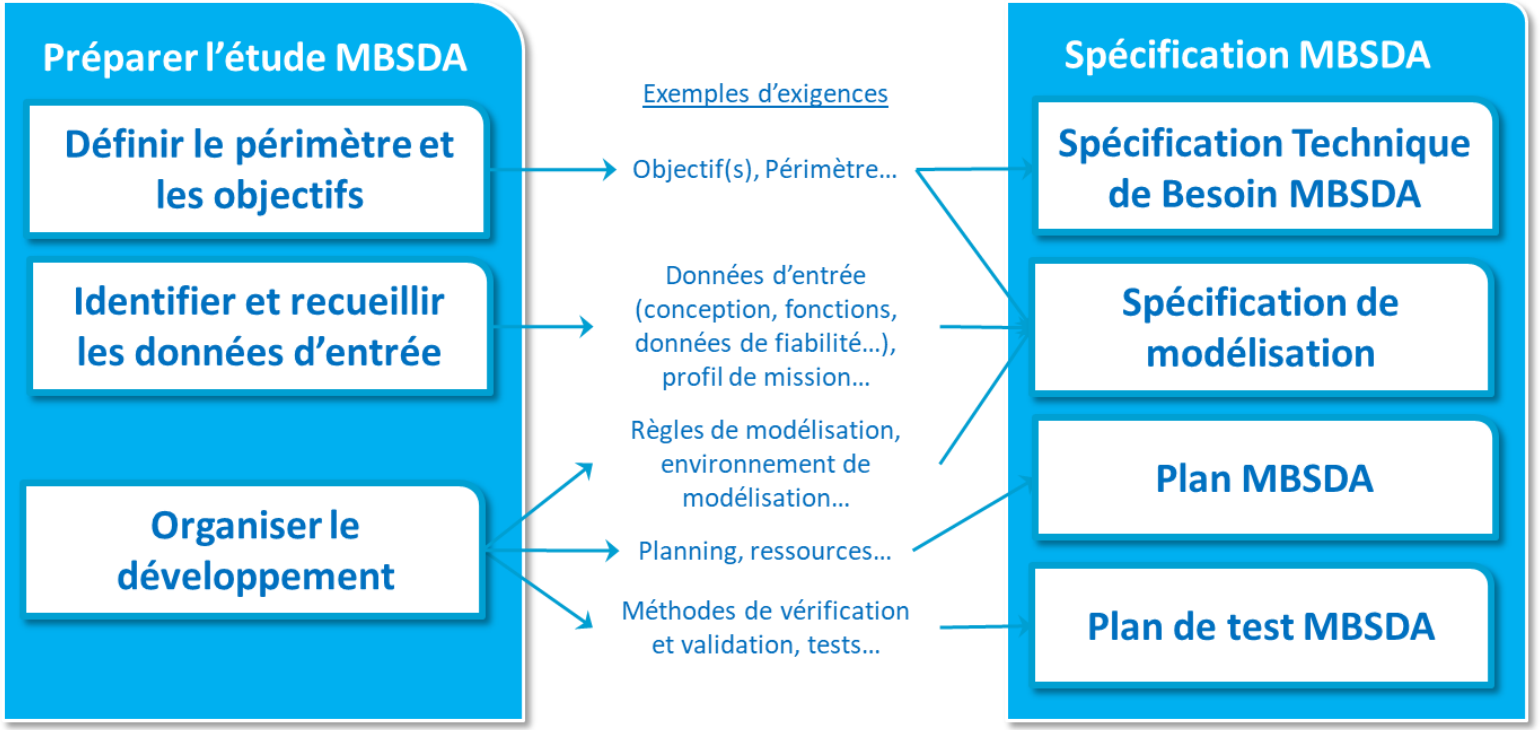
```
domain nominal_failed = {nominal, failed};
node node_G
 flow
        in_flow : nominal_failed : in;
        out_flow : nominal_failed : out;
 sub
        node_G1 : node_G__node_G1;
        node_G2 : node_G__node_G2;
        node_G3 : node_G__node_G3;
 assert
        node_G1.in_flow = in_flow;
        node_G2.in_flow = node_G1.out_flow;
        node_G3.in_flow = node_G2.out_flow;
        out_flow = node_G3.out_flow;
edon
```

```
domain Periodical = {nominal, faileddetected, failedundetected};
node node_G__node_G2
 flow
        in_flow : nominal_failed : in;
        out_flow : nominal_failed : out;
 state
        state1 : Periodical ;
        testing : bool ;
 init
        state1 := nominal;
        testing := false;
 event
        failure;
        repair;
        detection;
        end_detection;
        start_detection;
 trans
        state1 = nominal |- failure -> state1 := failedundetected;
        state1 = faileddetected |- repair -> state1 := nominal;
        (testing = true) and (state1 = failedundetected) |- detection -> state1 := faileddetected;
        testing = true |- end_detection -> testing := false;
        testing = false |- start_detection -> testing := true;
 assert
        out_flow = if (state1 = faileddetected) or (state1 = failedundetected) then failed else in_flow;
 extern
        law <event failure> = exponential(0.000001) ;
        law <event repair> = exponential(1) ;
        law <event detection> = Dirac(0) ;
        law <event end_detection> = Dirac(0) ;
        law <event start_detection> = Dirac(8760) ;
        priority <event detection> = 1;
edon
```

Application du guide MBSDA (IMdR) sur un modèle AltaRica

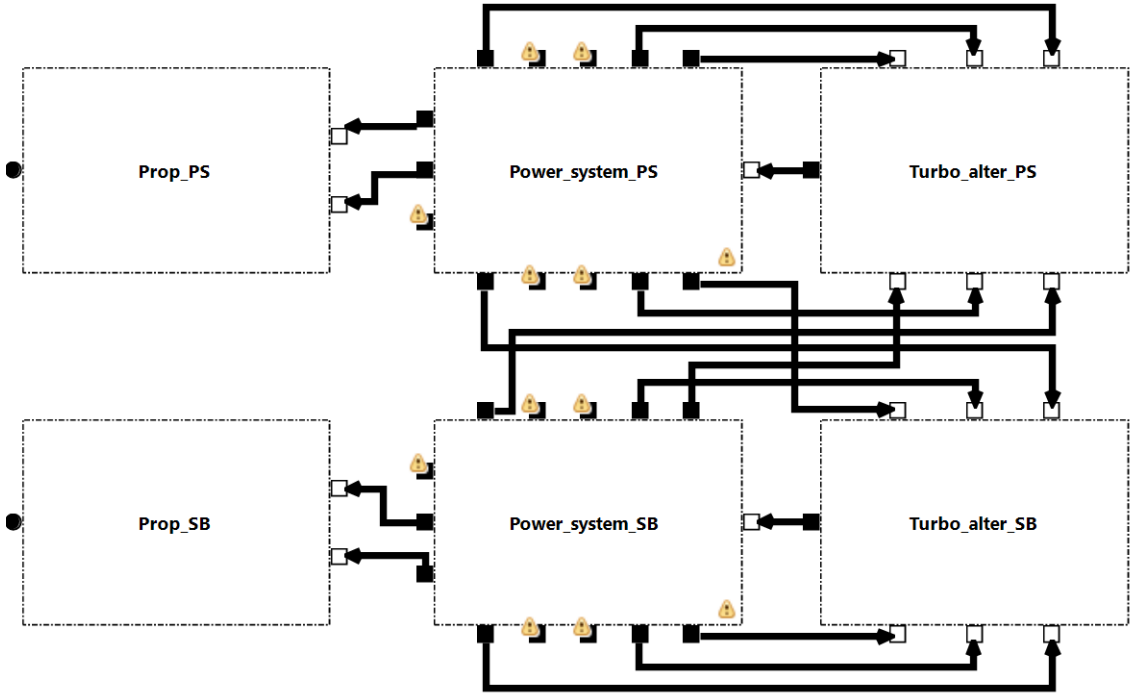
CAS D’APPLICATION

CAS D'APPLICATION
PRÉPARER L'ÉTUDE MBSDA



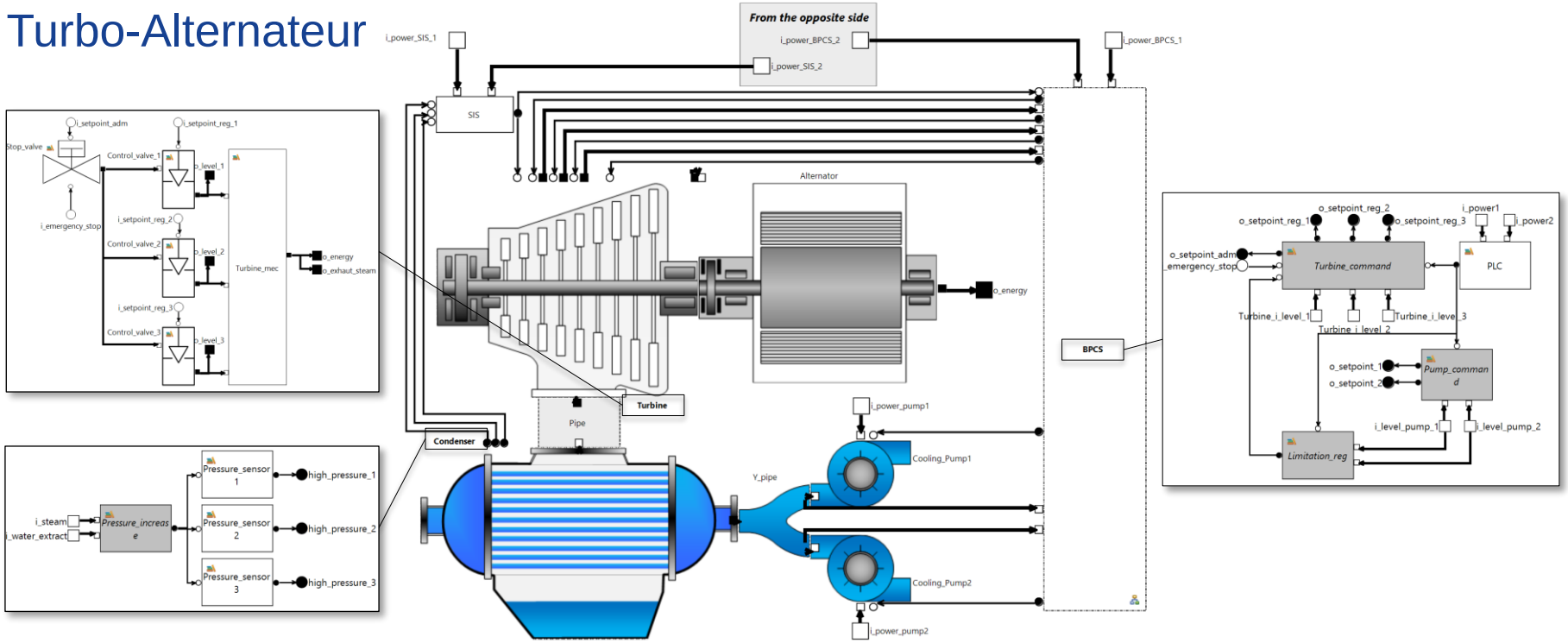
CAS D'APPLICATION
PÉRIMÈTRE

- Système Energie / Propulsion inspiré de systèmes réels (confidentialité)

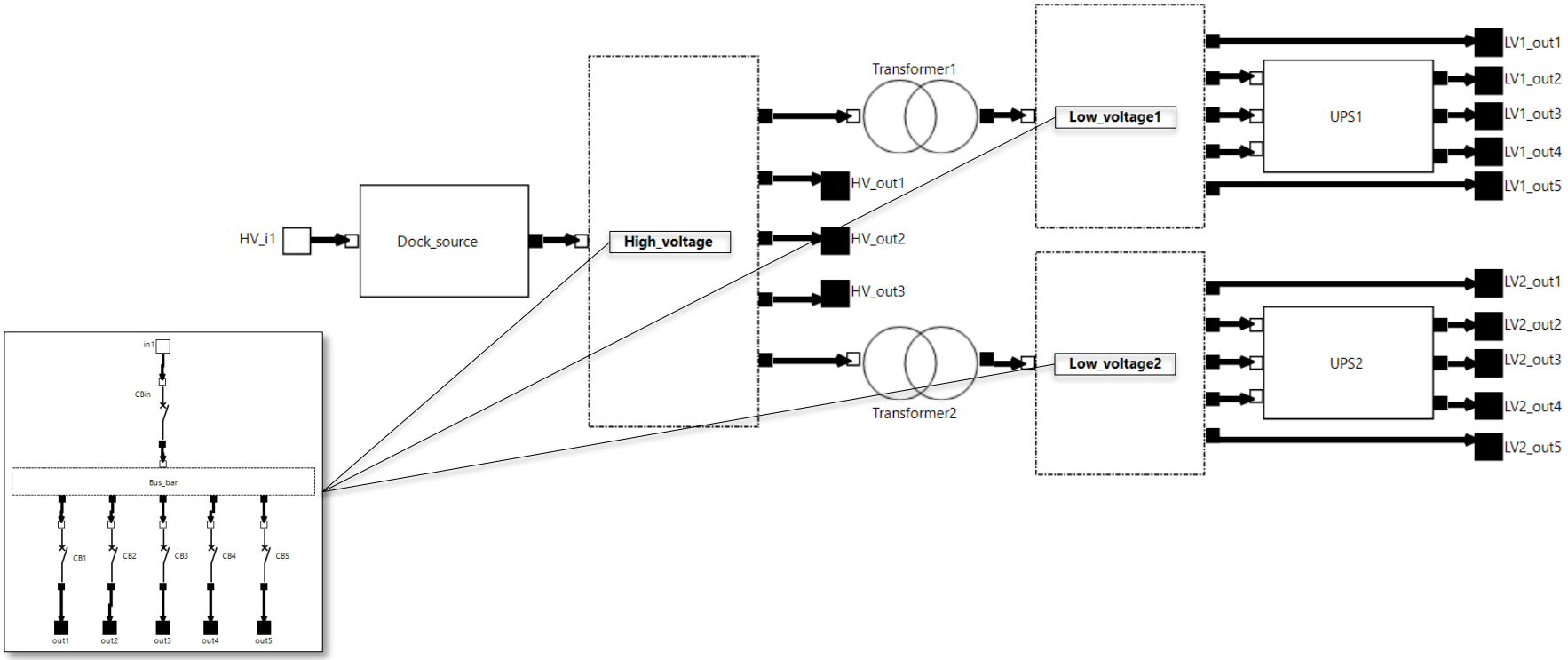


CAS D'APPLICATION
PÉRIMÈTRE - TURBO-ALTERNATEUR

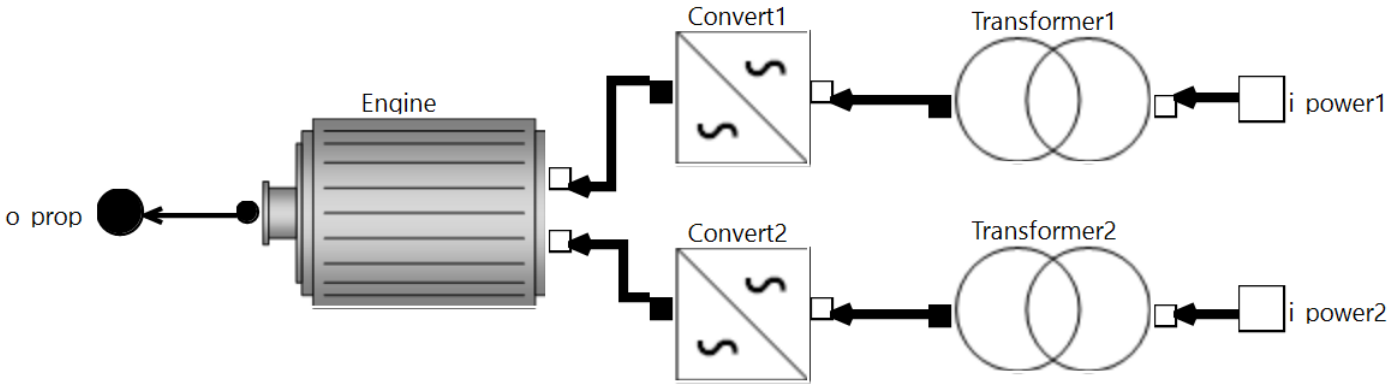
Turbo-Alternateur



CAS D'APPLICATION
PÉRIMÈTRE – DISTRIBUTION ELECTRIQUE



CAS D'APPLICATION
PÉRIMÈTRE - PROPULSION



CAS D'APPLICATION
PRÉPARER L'ÉTUDE MBSDA

- Objectifs :
  - Illustrer la méthode au sein de Naval Group
  - Utiliser les capacités MBSDA : comportement dynamique (reconfiguration, prise en compte des rechanges disponibles en mer), analyse de Sécurité (incluant sécurité fonctionnelle) et de Disponibilité
  - Prendre en compte le guide MBSDA
  - Résultats attendus

    Sécurité : Fréquence annuelle d'occurrence d'une brèche vapeur
    Disponibilité : Probabilité de perte partielle / totale de la propulsion sur une mission de 70 jours

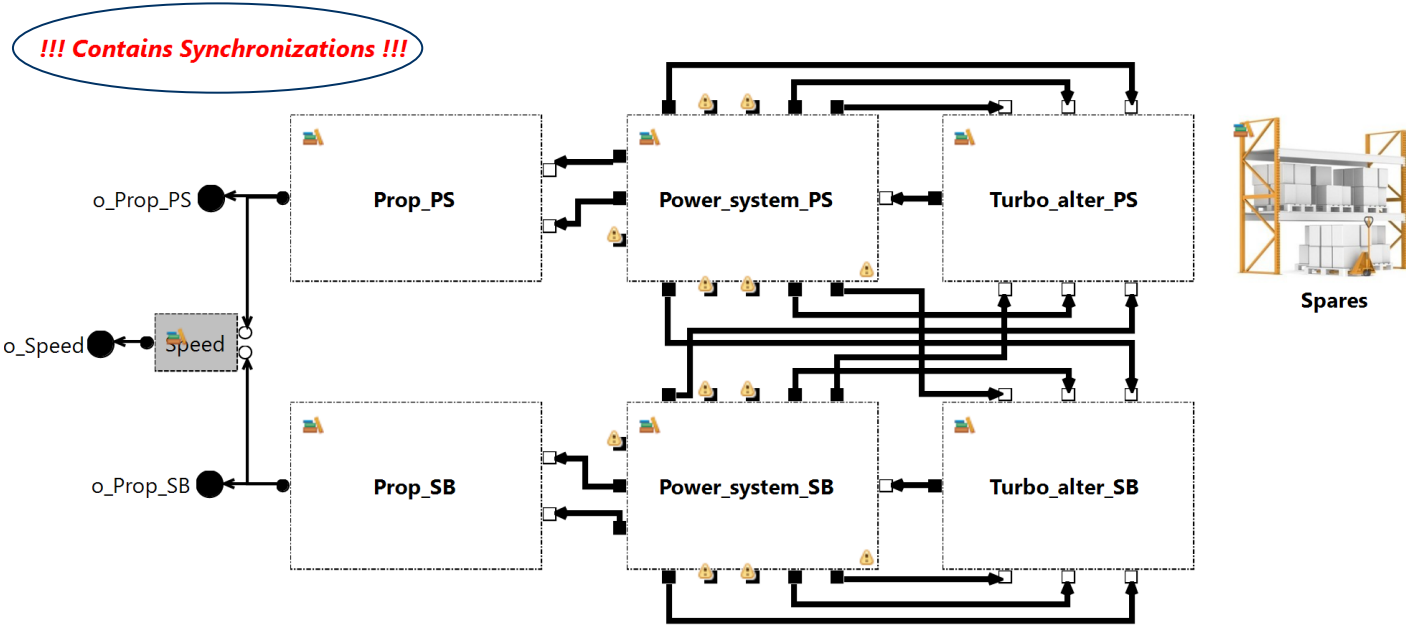
CAS D'APPLICATION
PRÉPARER L'ÉTUDE MBSDA

- Données d'entrée
  - Modèle(s) de systèmes réels équivalents
  - Données de fiabilité (ordre de grandeur)
  - Profil de mission
  - Politique de maintenance

- Instruction Naval Group (confidentielle)
  - Contenant les règles de modélisation
  - Adaptée au logiciel SimfiaNeo
  - Présentant les méthodes de vérification
  - Indiquant les preuves attendues

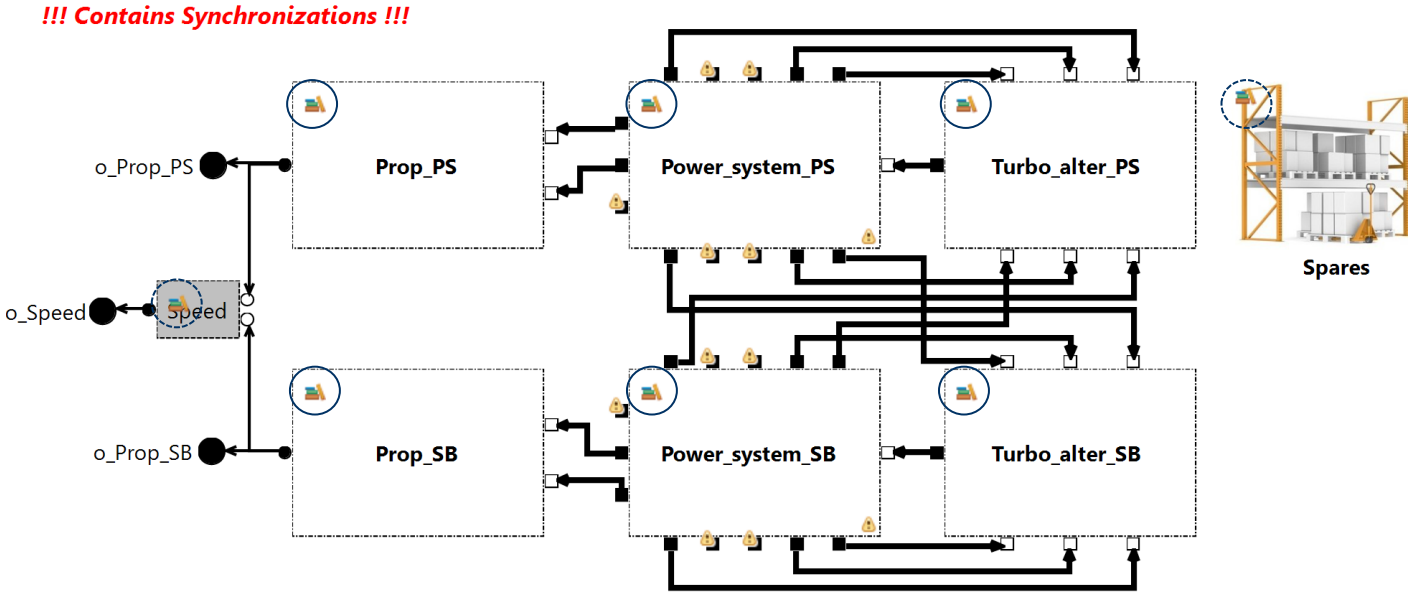
CAS D'APPLICATION
EXEMPLE DE RÈGLE DE MODÉLISATION

Exemple de règles de modélisation : Mettre un avertissement sur le diagramme d'un élément contenant une (ou des) synchronisation(s)



CAS D'APPLICATION
EXEMPLE DE RÈGLE DE MODÉLISATION

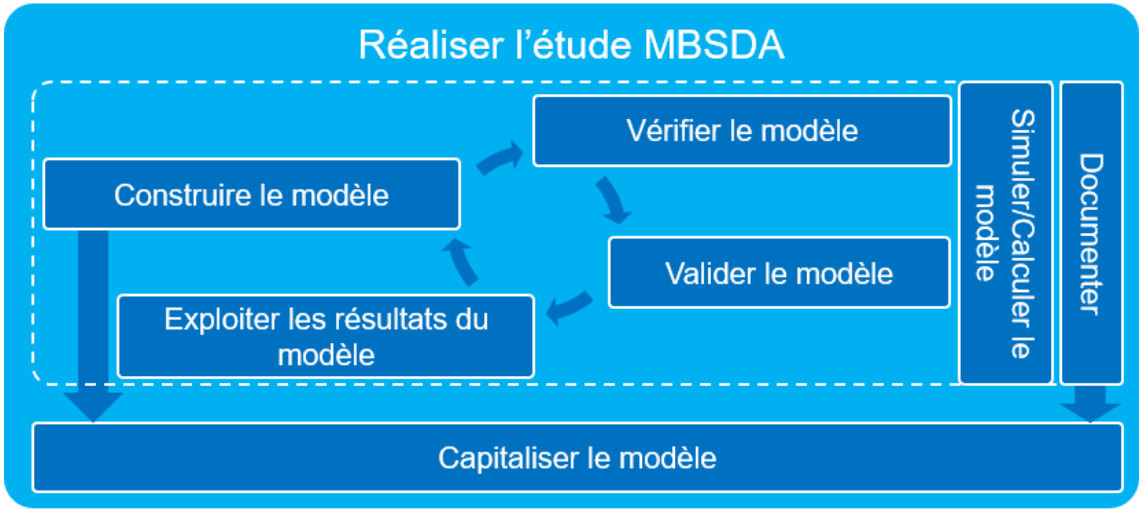
Exemple de règles de modélisation : Tous les éléments répétés doivent être traités en utilisant une classe instanciée autant de fois que nécessaire



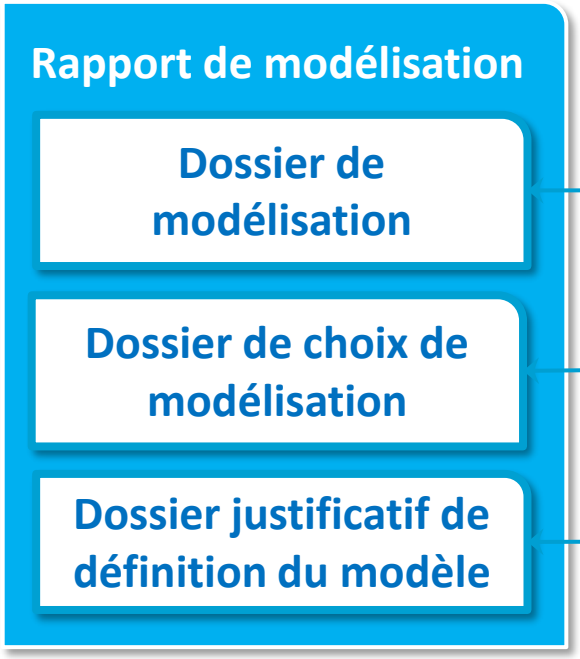
CAS D'APPLICATION
RÉALISER L'ÉTUDE MBSDA

Principal processus

- Itératif
- Construction pas-à-pas
- Au fur et à mesure de la construction du modèle, il faut simuler, vérifier/valider, documenter…



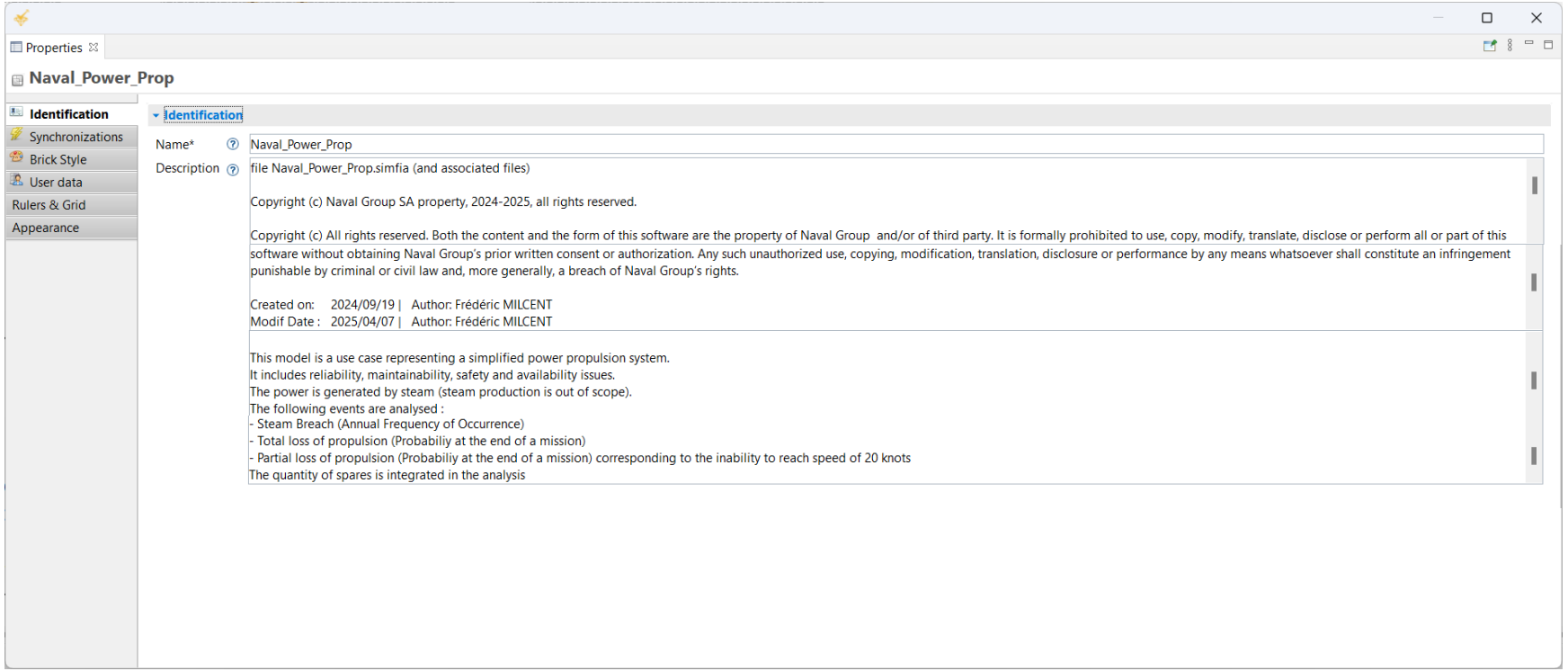
CAS D'APPLICATION
DOCUMENTER LE MODÈLE



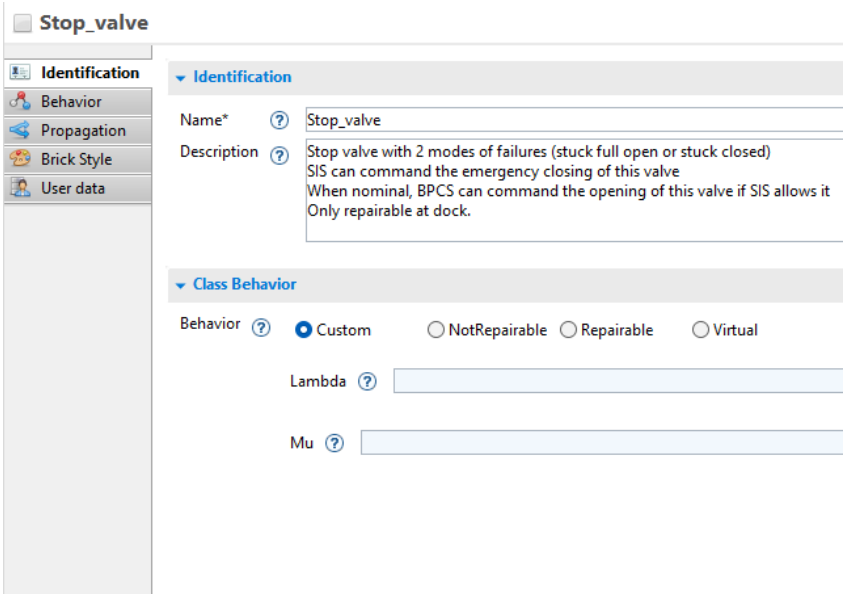
Choix faits pour le cas d'application

- Intégration des éléments de documentation directement dans le modèle
- Edition d'un seul document compilant toutes les informations
- Utilisation de la génération automatique de documentation pour établir la base du rapport de modélisation
- Compléments ajoutés pour expliciter certains comportements

CAS D'APPLICATION
DOCUMENTER LE MODÈLE



CAS D'APPLICATION
DOCUMENTER LE MODÈLE



Domains of Naval_Power_Prop Library

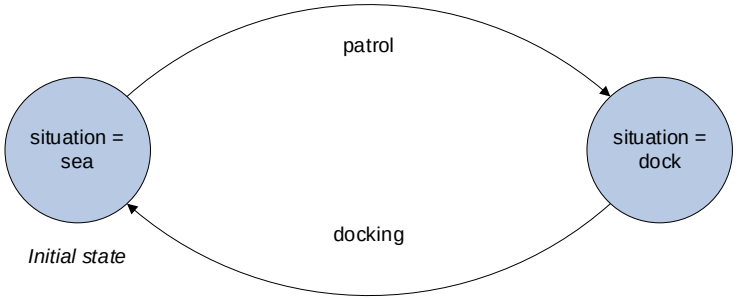
	Name	Domain	Type	Color	Link Style	Description
1	situation_domain				———	Represents ship situation : - waiting used to delay the start of ship - sea - dock
2	dock		Nominal	Blue		
3	sea		Nominal	Green		
4	waiting		Nominal	Yellow		
5	nominal_stuck				———	Domain used for regulation valvle
6	nominal		Nominal	Green		
7	stuck_closed		Failed	Red		
8	stuck_full_open		Degraded	Red		
9	stuck_mid_open		Degraded	Red		
10	nominal_failed_degraded				———	Main domain used for element state
11	nominal		Nominal	Green		
12	failed		Failed	Red		
13	degraded		Degraded	Orange		
14	nominal_failed_dang_safe				———	Specific domain used for SIS element
15	nominal		Nominal	Green		
16	failed_safe		Failed	Red		
17	failed_dang		Failed	Red		
18	colored_capa				———	Strucured domain used to color the float links and ports
19	capa	float				

CAS D'APPLICATION
DOCUMENTER LE MODÈLE

Utilisation d'un état situation (dont les transitions sont synchronisées) pour intégrer la phase dans laquelle se trouve le navire :

Quand le navire est à la mer, la plupart des éléments sont non réparables.

Seuls certains éléments disposent d'un stock limité de rechange à bord permettant des réparations.



Quand le navire est à quai, tous les éléments sont réparables.

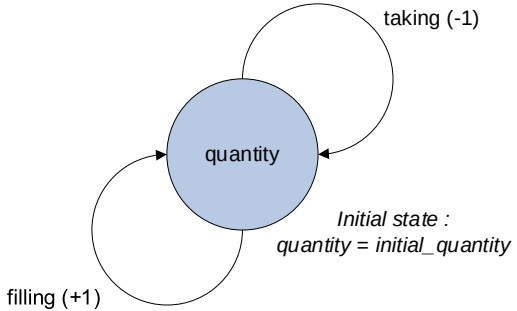
Le stock bord est recomplété.

Le navire est alimenté en énergie électrique par des sources extérieures.

CAS D'APPLICATION
DOCUMENTER LE MODÈLE

Un nœud pour chaque type de composant représentant le stock bord :

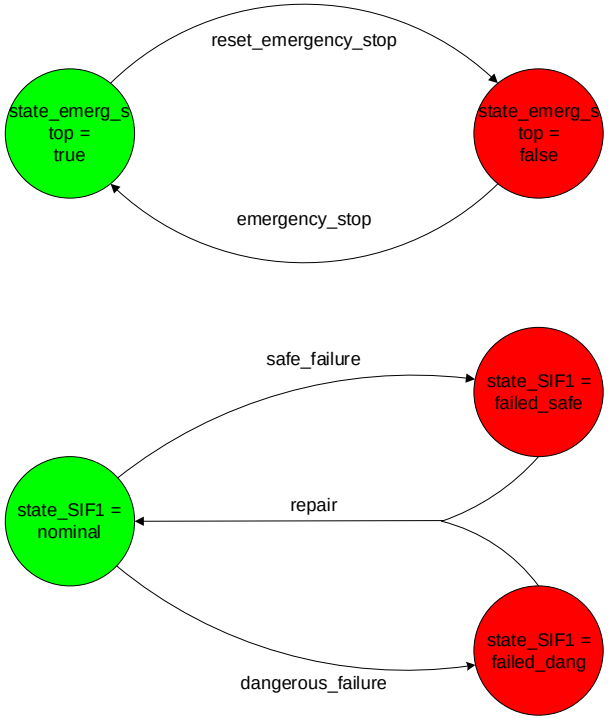
- 3 états :
  - situation,
  - initial_quantity (fixe lors des simulations)
  - quantity
- 2 transitions :
  - taking (synchronisée avec les réparations)
  - filling (possible seulement à quai)



CAS D'APPLICATION
DOCUMENTER LE MODÈLE

SIS (Safety Instrumented System)

- 1 SIF (Safety Instrumented Function) --> Fermer la soupape d'admission vapeur en cas de pression excessive au condenseur (logique 2oo3 sur les capteurs de pression)
- 2 modes de défaillances :
  - dangerous_failure --> arrêt d'urgence impossible
  - safe failure --> arrêt d'urgence intempestif
- Sur perte d'alimentation --> arrêt d'urgence (repli sécuritaire)
- Seulement réparable à quai



CAS D'APPLICATION
DOCUMENTER LE MODÈLE

NAVAL GROUP

Corporate Sensitivity
PUBLIC

3.30 SIS

Safety Instrumented System
1 Safety Instrumented Function --> Close the stop valve (emergency stop) when pressure increases in the condenser (2 out of 3 pressure sensors)
2 modes of failures :
dangerous failure --> emergency stop not available
safe failure --> emergency stop (even if not necessary)
When power supply is lost --> emergency stop (even if not necessary)
Only repairable at dock

3.30.1 Connectors

3.30.1.1 Input

Name	Domain
i_power1	colored_capa
i_power2	colored_capa
i_high_press1	bool
i_high_press2	bool
i_high_press3	bool

3.30.1.2 Output

Name	Domain	Assertion
o_emergency_stop	bool	state_emerg_stop

3.30.2 State variables

Name	Domain	Initial value
state_emerg_stop	bool	false
state_SIF1	nominal_failed_dang_safe	nominal
situation	situation_domain	sea

3.30.3 Events

Event	Guard	Effects	Probabilistic Law
emergency_stop	(state_SIF1 = nominal) and (state_emerg_stop= false) and (((i_high_press1 and i_high_press2) or (i_high_press1 and i_high_press3) or (i_high_press2 and i_high_press3)) or (i_power1=capa+i_power2=capa=0))	state_emerg_stop := true	Dirac(d=0, p=0)

NAVAL GROUP

Corporate Sensitivity
PUBLIC

Event	Guard	Effects	Probabilistic Law
reset_emergency_stop	(state_SIF1 = nominal) and state_emerg_stop and ((i_power1=capa + i_power2=capa) > 0) and not((i_high_press1 and i_high_press2) or (i_high_press1 and i_high_press3) or (i_high_press2 and i_high_press3))	state_emerg_stop := false	Dirac(d=0, p=0)
dangerous_failure	(state_SIF1 = nominal)	state_SIF1 := failed_dang, state_emerg_stop := false	Exp(1.00E-8)
safe_failure	(state_SIF1 = nominal)	state_SIF1 := failed_safe, state_emerg_stop := true	Exp(1.00E-6)
repair	(situation = dock) and ((state_SIF1 = failed_safe) or (state_SIF1 = failed_dang))	state_SIF1 := nominal	Exp(0.1)
patrol	(situation = sea)	situation := dock	Dirac(d=1,680, p=0)
docking	(situation = dock)	situation := sea	Dirac(d=480, p=0)

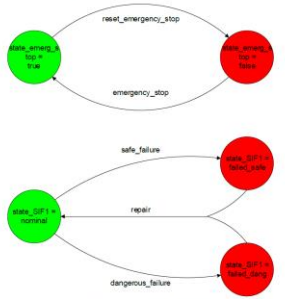


Figure 25 - SIS transitions diagrams

©Naval Group SA property, 2025, all rights reserved.
Siège social : 40-42, rue du Docteur Finlay - 75015 Paris - Tél. : +33 (0)1 40 59 50 00 – www.naval-group.com
Naval Group - SA au capital de 563 000 000 euros - RCS Paris 441 133 808 - SIRET 441 133 808 00135 - APE 3011 Z

CAS D'APPLICATION
VÉRIFIER LE MODÈLE

Vérifications proposées dans le guide :

- Examen syntaxique et sémantique
- Conformité du typage/domaine
- Bon usage de toutes les entrées, sorties et états du modèle
- Conformité des automates à états finis (transitions)
- Respect des règles de modélisation
- Cohérence des événements avec les données d'entrée
- Conformité par rapport au comportement attendu (assertions, visualisation graphique, observers, priorisation des transitions)
- Bonne cohésion des liens entre les éléments du modèle
- Cohérence vis-à-vis d'éventuelles études réalisées par ailleurs

CAS D'APPLICATION
VÉRIFIER LE MODÈLE

Vérifications proposées dans le guide :

- Examen syntaxique et sémantique
- Conformité du typage/domaine
- Bonne adéquation des données entrées, sorties et états du modèle
- Conformité des automates à états finis (transitions)
- Respect des règles de modélisation

Vérifié par le logiciel

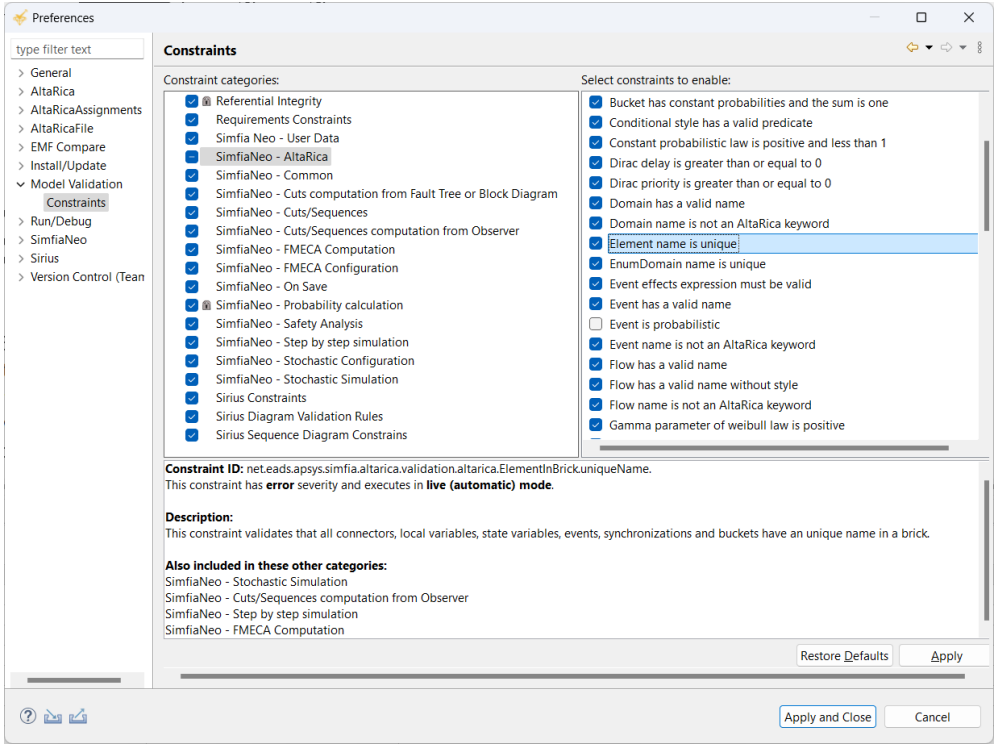
- Cohérence des événements avec les données d'entrée
- Conformité par rapport au comportement attendu (assertions, visualisation graphique, observers, priorisation des transitions)
- Bonne cohésion des liens entre les éléments du modèle
- Cohérence vis-à-vis d'éventuelles études réalisées par ailleurs

CAS D'APPLICATION
VÉRIFICATIONS INTÉGRÉES À SIMFIANEO

Règles implémentées directement

Mais également :

- Détection des boucles
- Mise en évidence des causes et conséquences



CAS D'APPLICATION
VÉRIFICATIONS INTÉGRÉES À SIMFIANEO

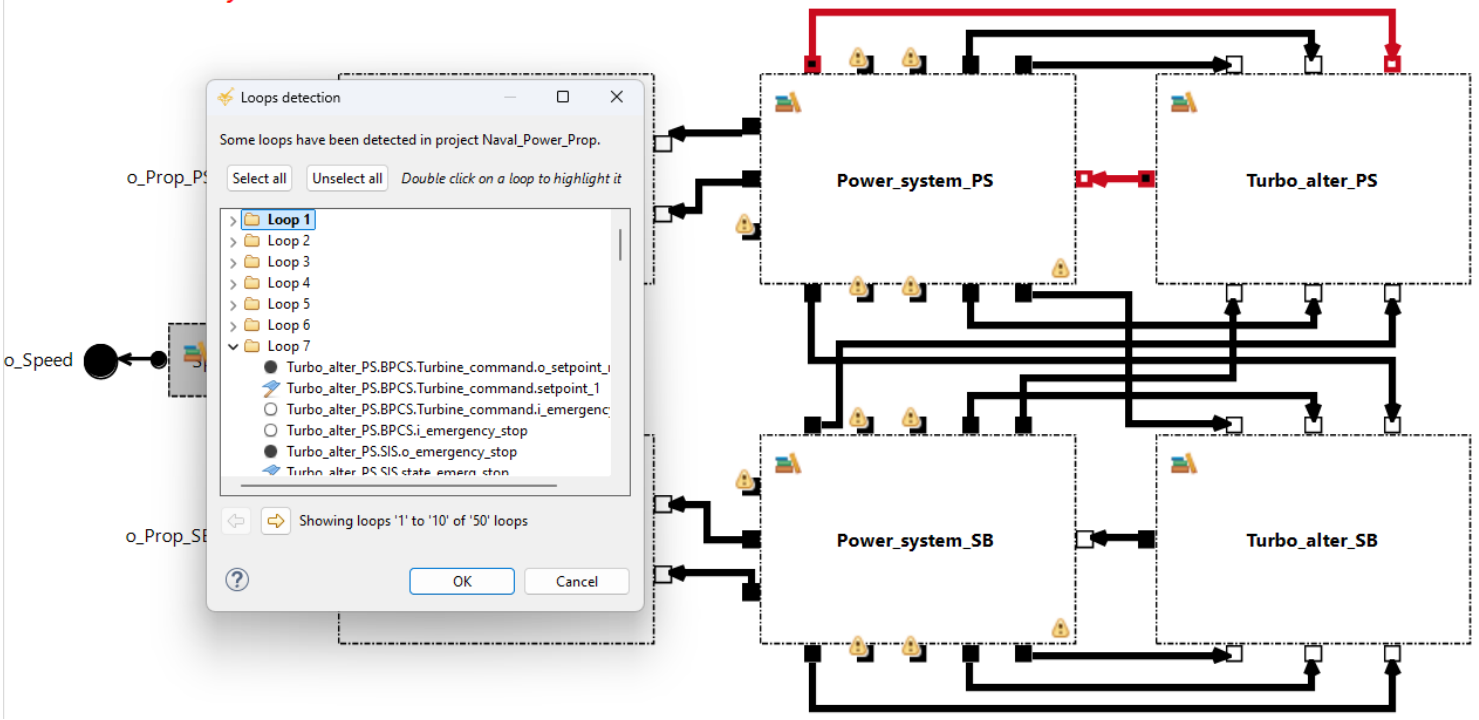
Résultat de ces vérifications intégrées dans un onglet « Validation report »

Properties | Validation report | AltaRica | Images

	Level	Message	Rule name	Project
1	WARNING	In brick Naval_Power_Prop.Power_system_PS: the output connector LV1_out3 does not have any effect	Output connector has effects	Naval_Power_Prop
2	WARNING	In brick Naval_Power_Prop.Power_system_SB: the output connector LV1_out3 does not have any effect	Output connector has effects	Naval_Power_Prop
3	WARNING	In brick Naval_Power_Prop.Power_system_SB: the output connector HV_out3 does not have any effect	Output connector has effects	Naval_Power_Prop
4	WARNING	In brick Naval_Power_Prop.Power_system_SB: the output connector LV2_out3 does not have any effect	Output connector has effects	Naval_Power_Prop
5	WARNING	In brick Naval_Power_Prop.Power_system_SB: the output connector LV2_out4 does not have any effect	Output connector has effects	Naval_Power_Prop
6	WARNING	In brick Naval_Power_Prop.Power_system_PS: the output connector LV1_out4 does not have any effect	Output connector has effects	Naval_Power_Prop
7	WARNING	In brick Naval_Power_Prop.Power_system_SB: the output connector LV1_out4 does not have any effect	Output connector has effects	Naval_Power_Prop
8	WARNING	In brick Naval_Power_Prop.Power_system_PS: the output connector HV_out3 does not have any effect	Output connector has effects	Naval_Power_Prop
9	WARNING	In brick Naval_Power_Prop.Power_system_PS: the output connector LV2_out3 does not have any effect	Output connector has effects	Naval_Power_Prop
10	WARNING	In brick Naval_Power_Prop.Power_system_PS: the output connector LV2_out4 does not have any effect	Output connector has effects	Naval_Power_Prop
11	WARNING	The system Naval_Power_Prop has one or many loops involving a state variable.	System should not have any connectors loop involving a state variable	Naval_Power_Prop

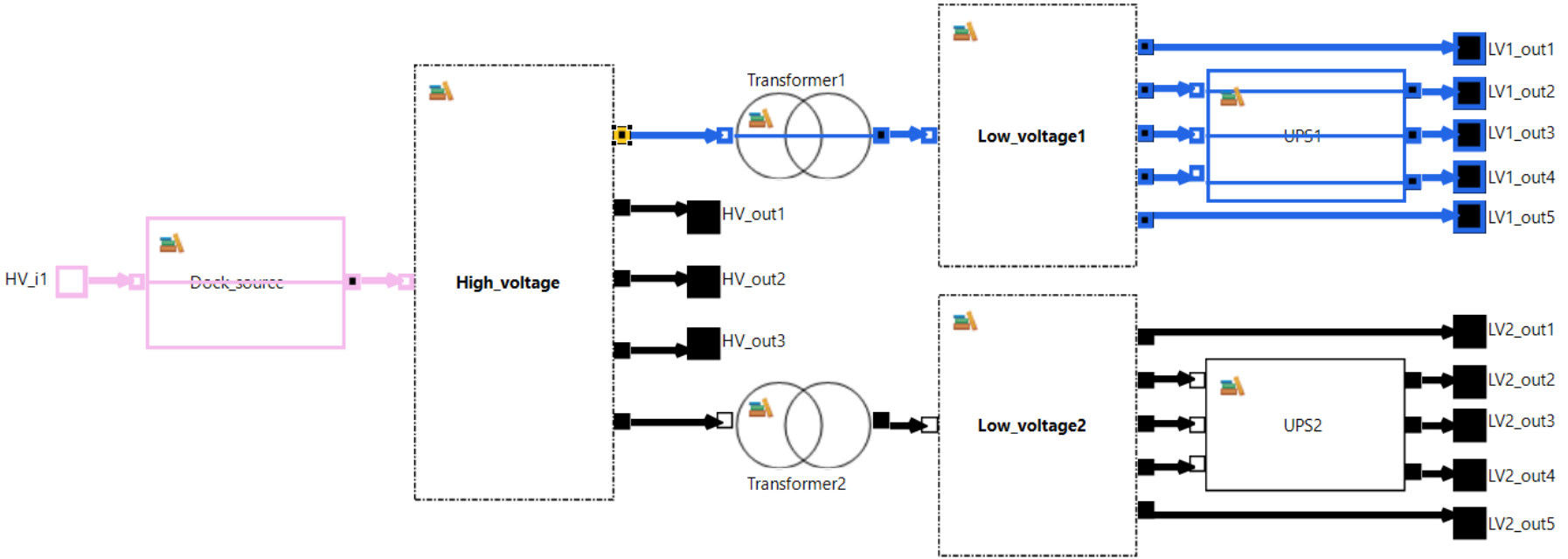
CAS D'APPLICATION
VÉRIFICATIONS INTÉGRÉES À SIMFIANEO

!!! Contains Synchronizations !!!



Spares

CAS D'APPLICATION
VÉRIFICATIONS INTÉGRÉES À SIMFIANEO



CAS D'APPLICATION
SIMULER/CALCULER LE MODÈLE

Permet d'obtenir les résultats attendus de l'étude

Peut servir à vérifier ou valider le modèle

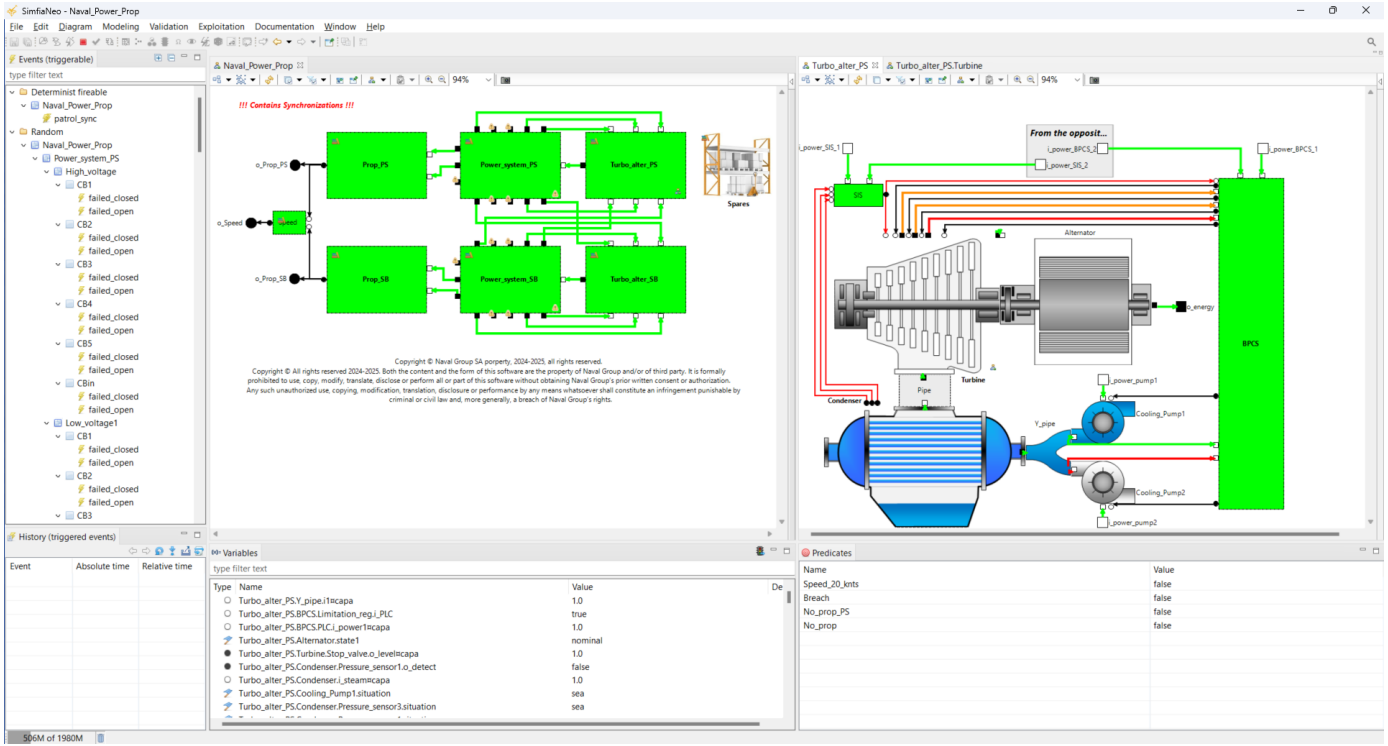
2 types de simulations : interactive (pas à pas) ou systématique (simulation stochastique, génération de séquences)

Sélection et paramétrage des moteurs de calcul

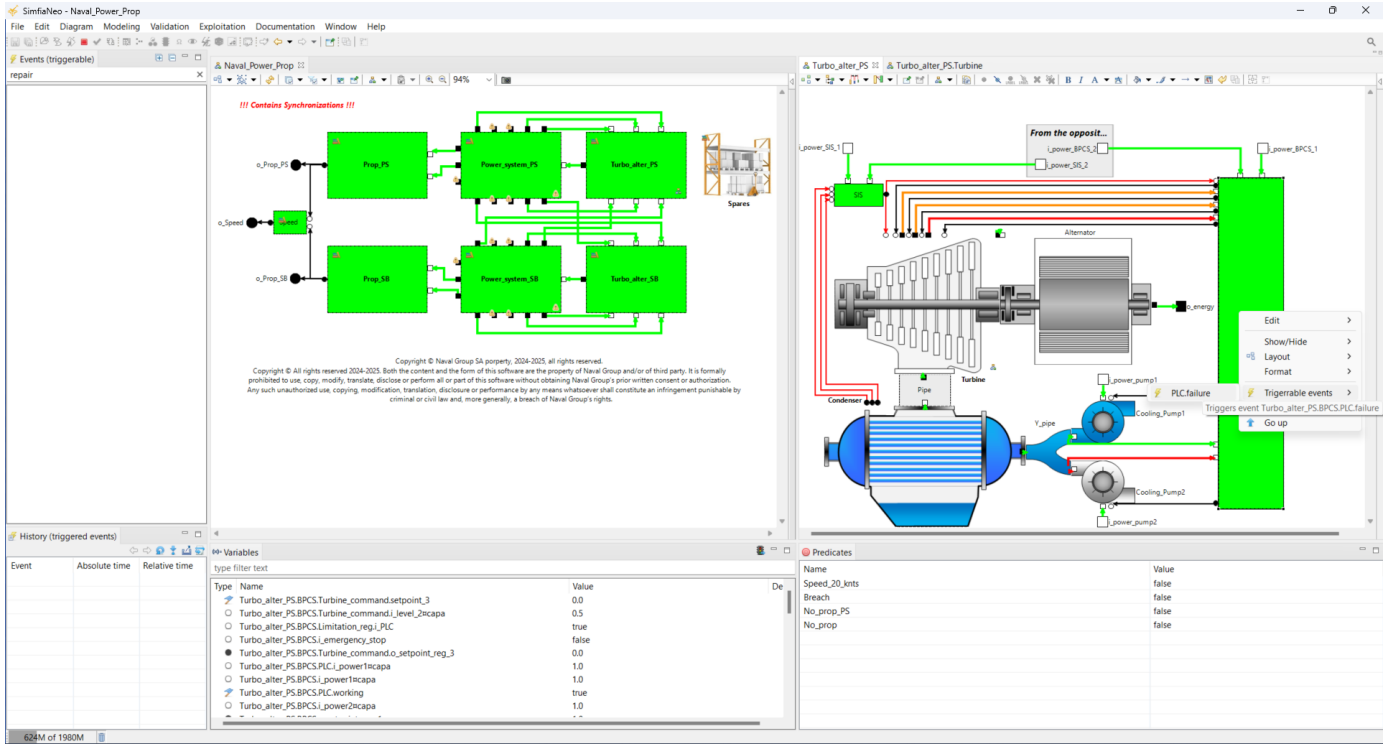
La simulation pas-à-pas est un outil indispensable pour :

- Vérifier le comportement unitaire des nœuds
- Vérifier le comportement du modèle
- Valider le modèle en jouant des scénarios connus ou prévisibles menant aux événements redoutés

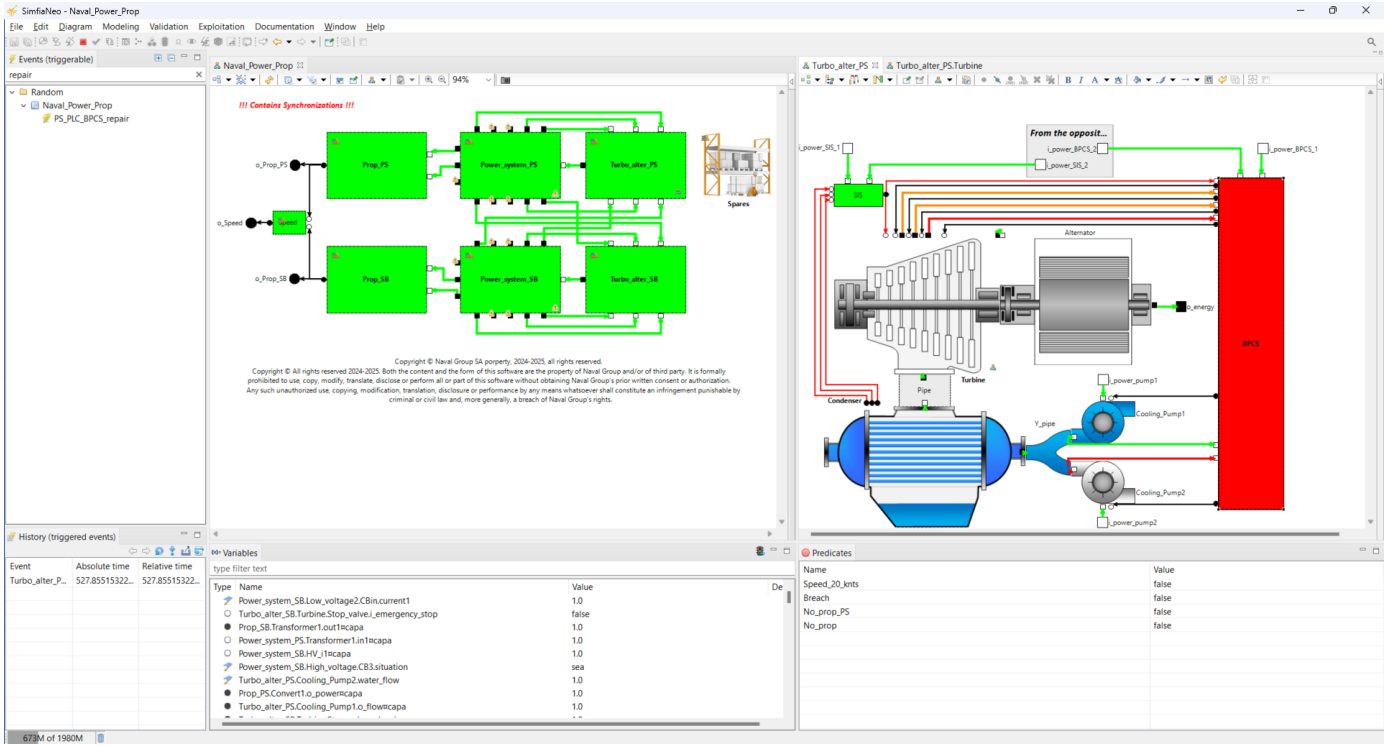
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



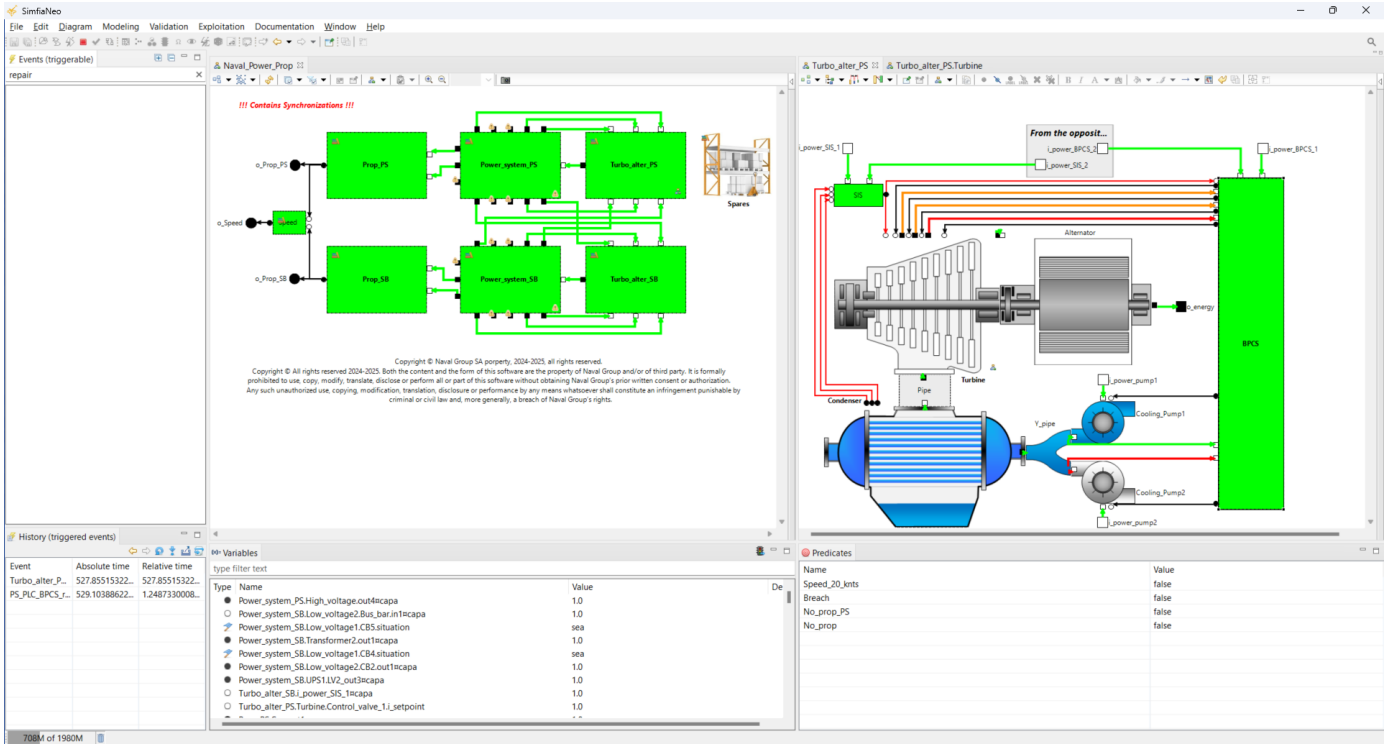
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



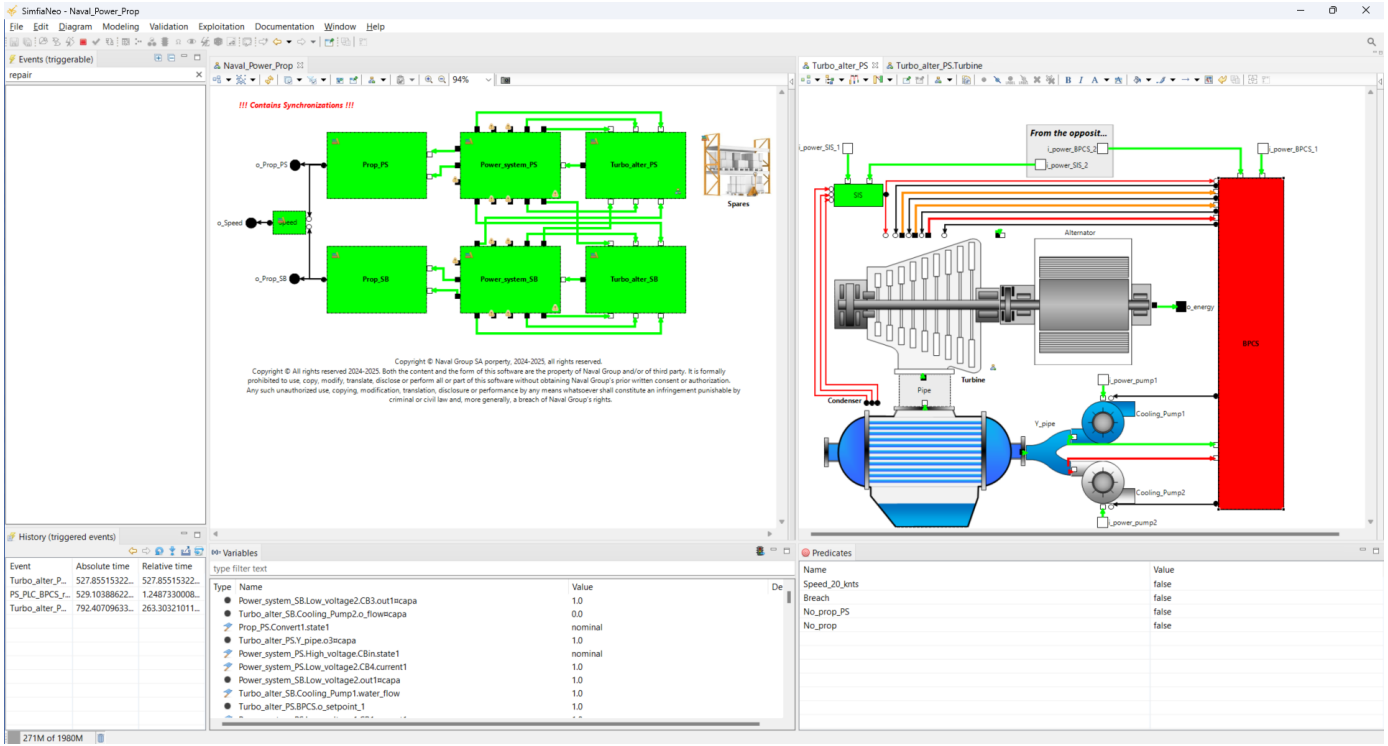
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



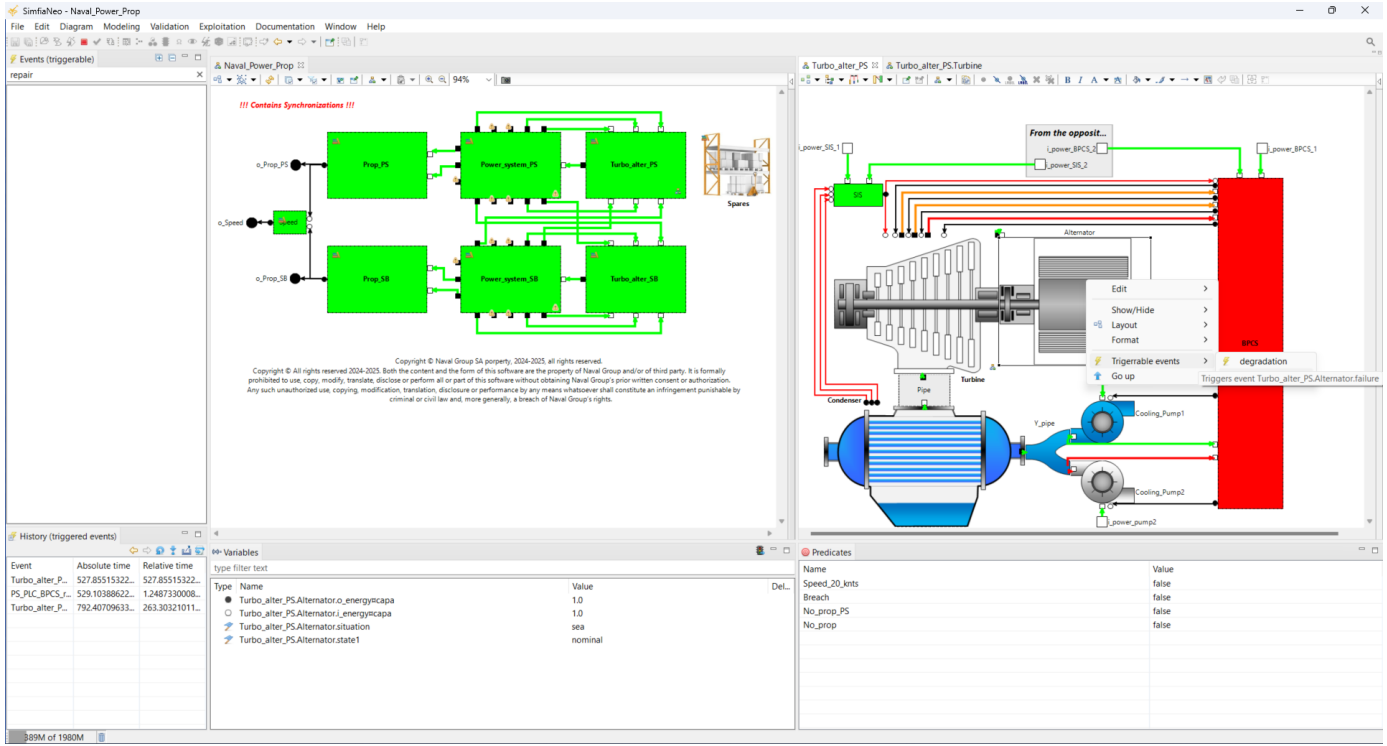
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



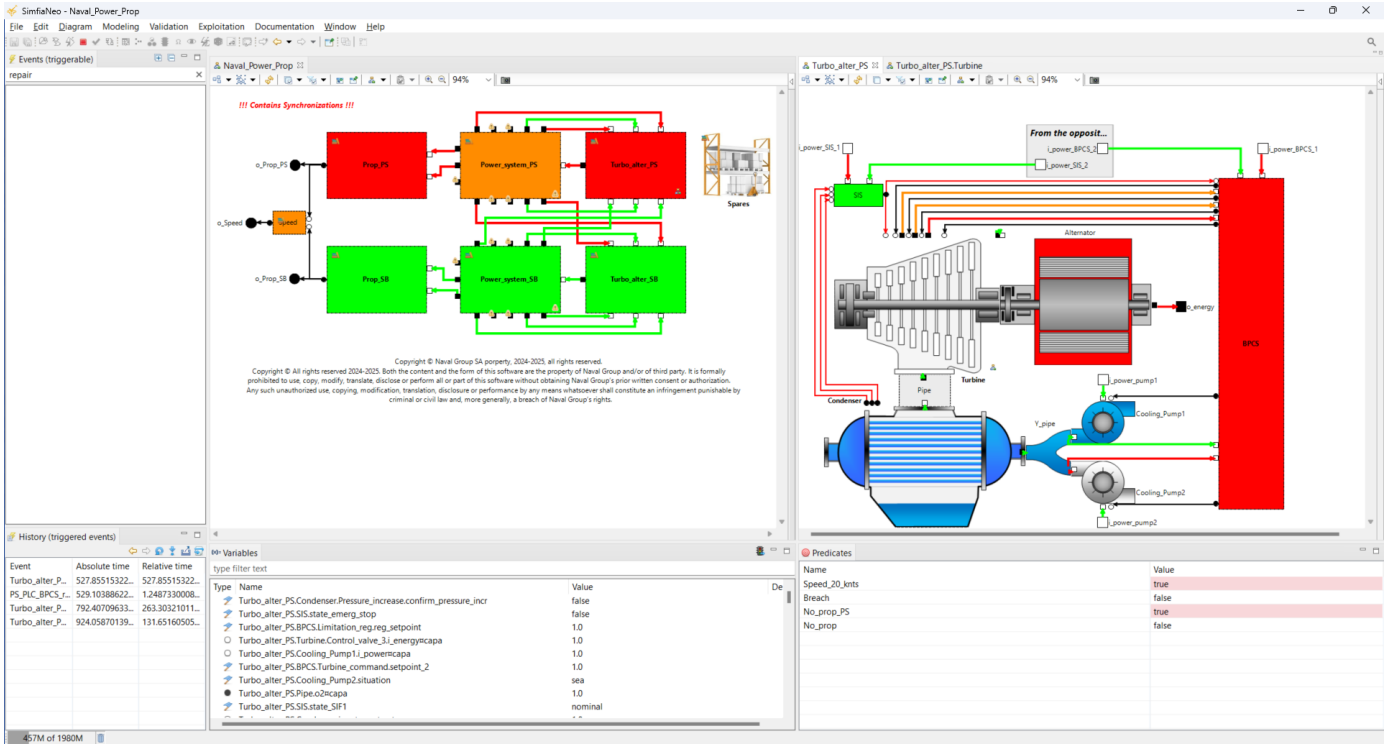
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



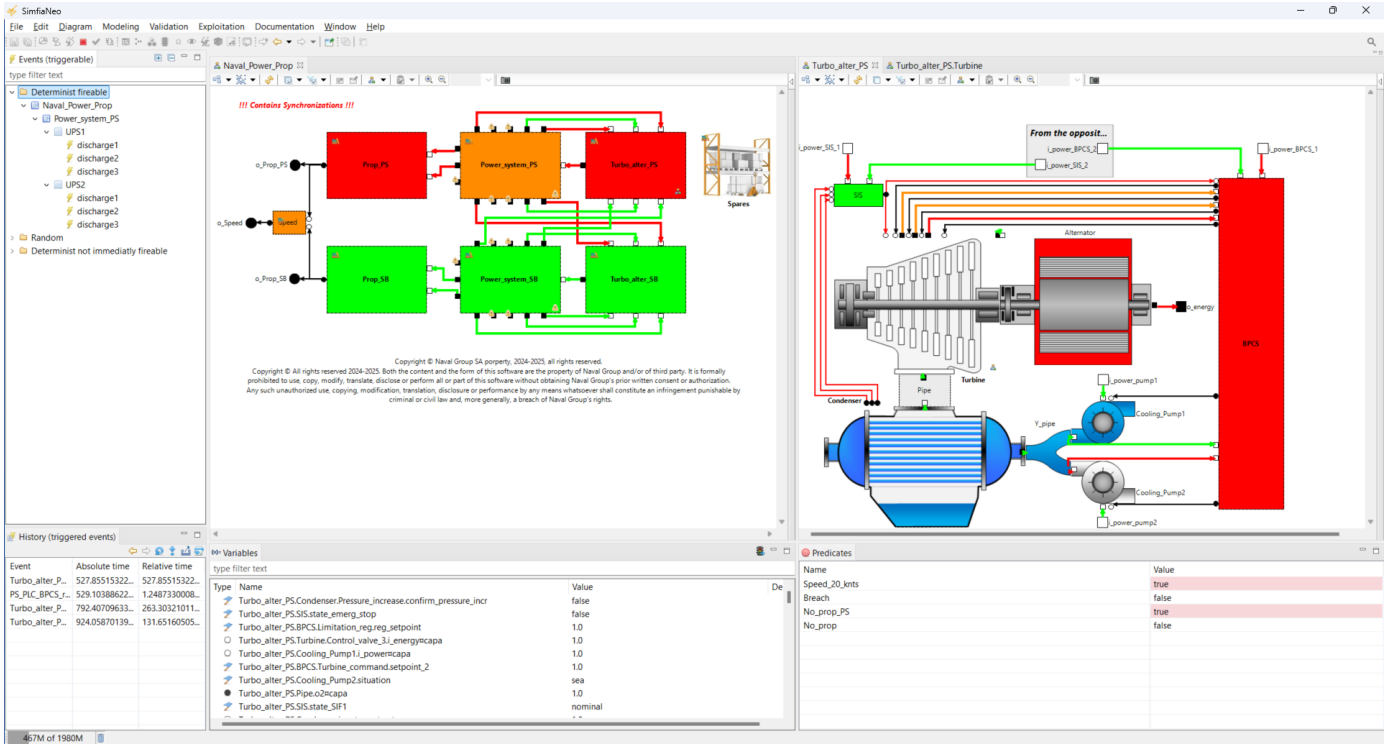
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



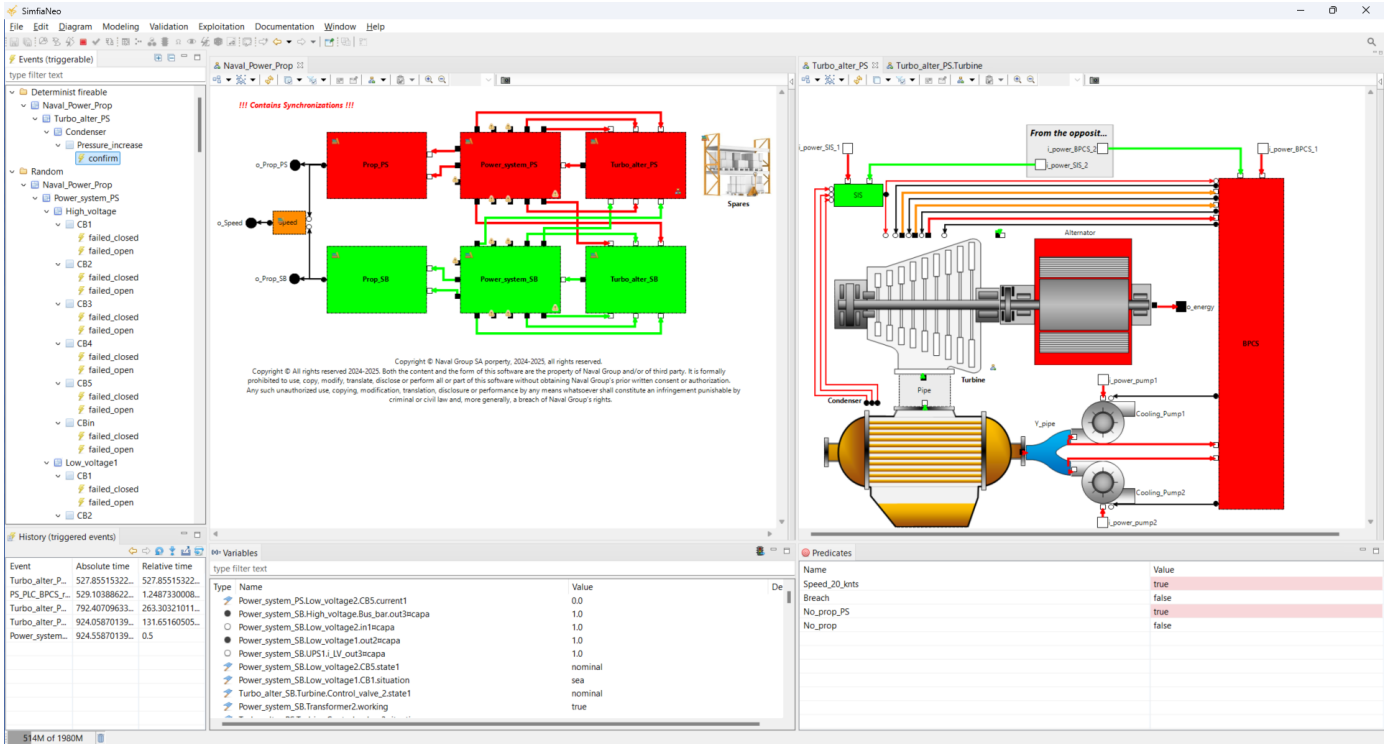
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



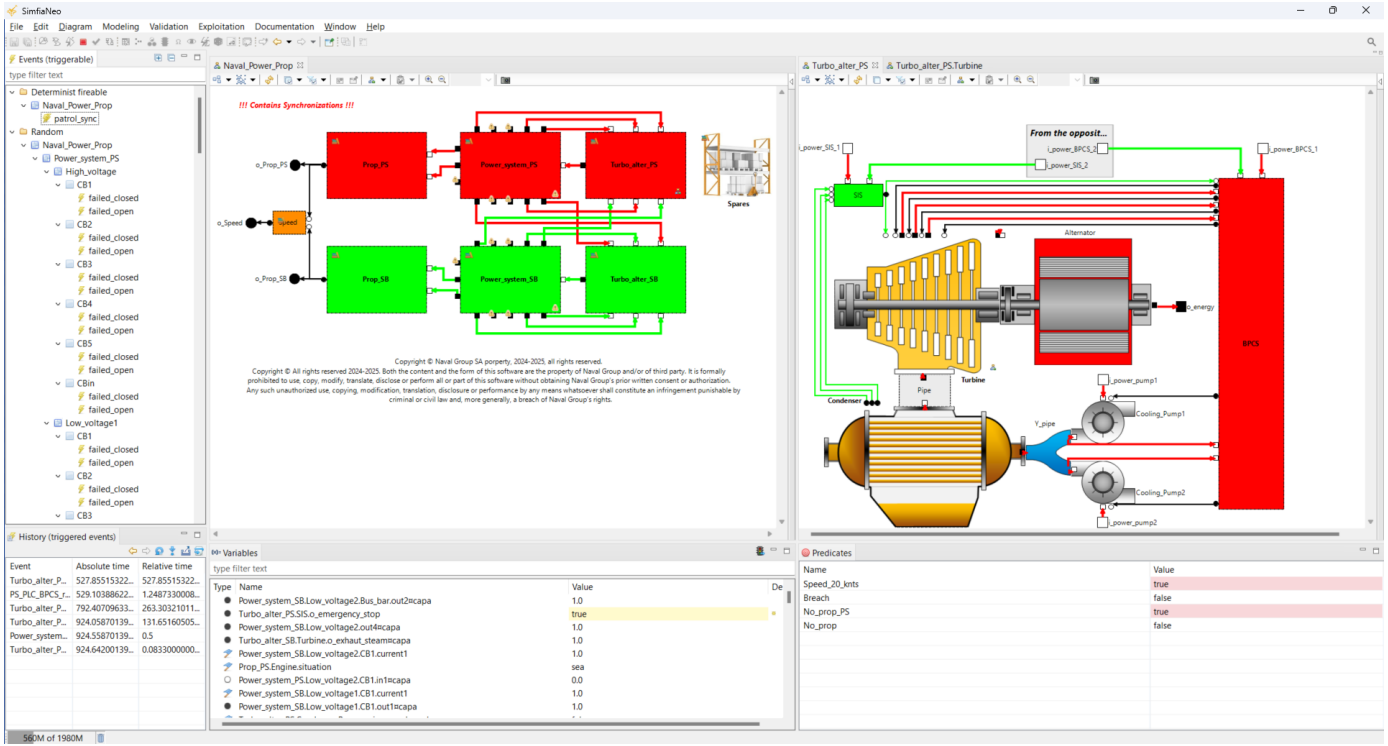
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



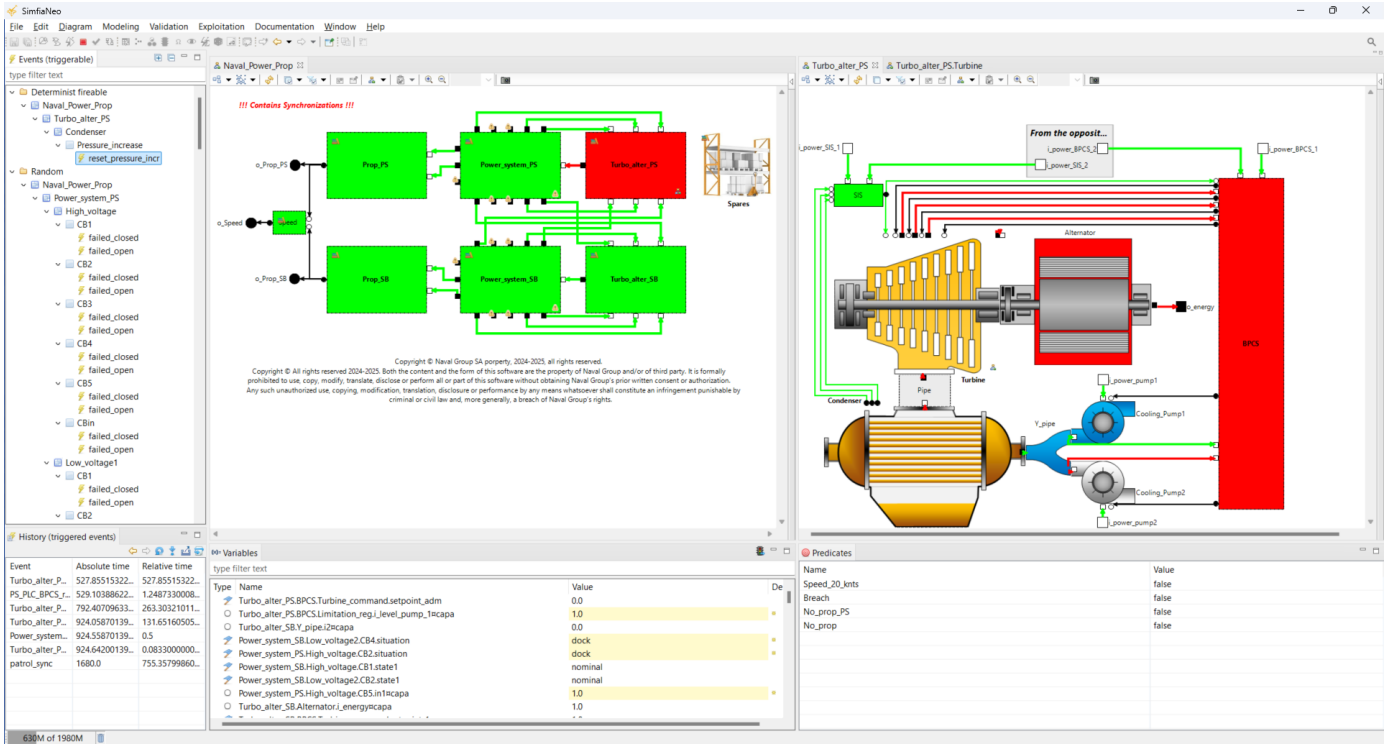
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



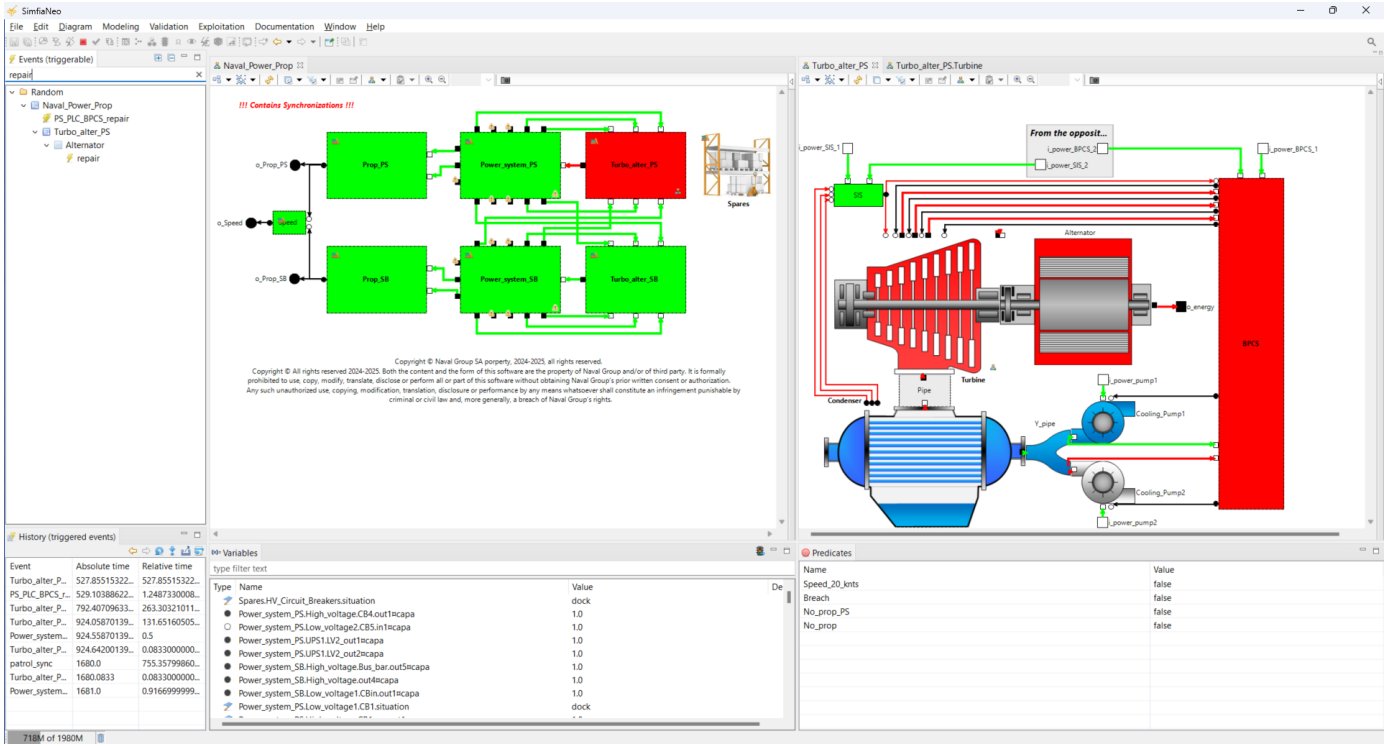
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



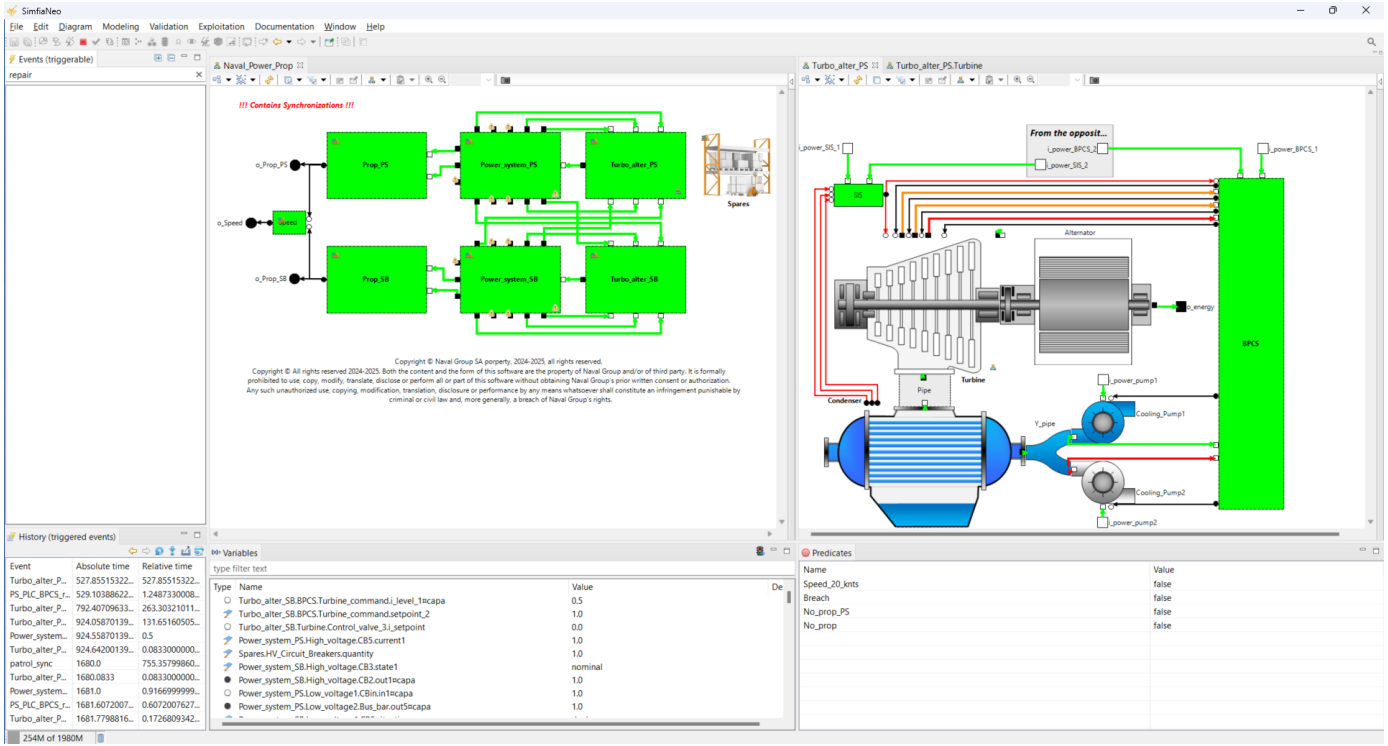
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



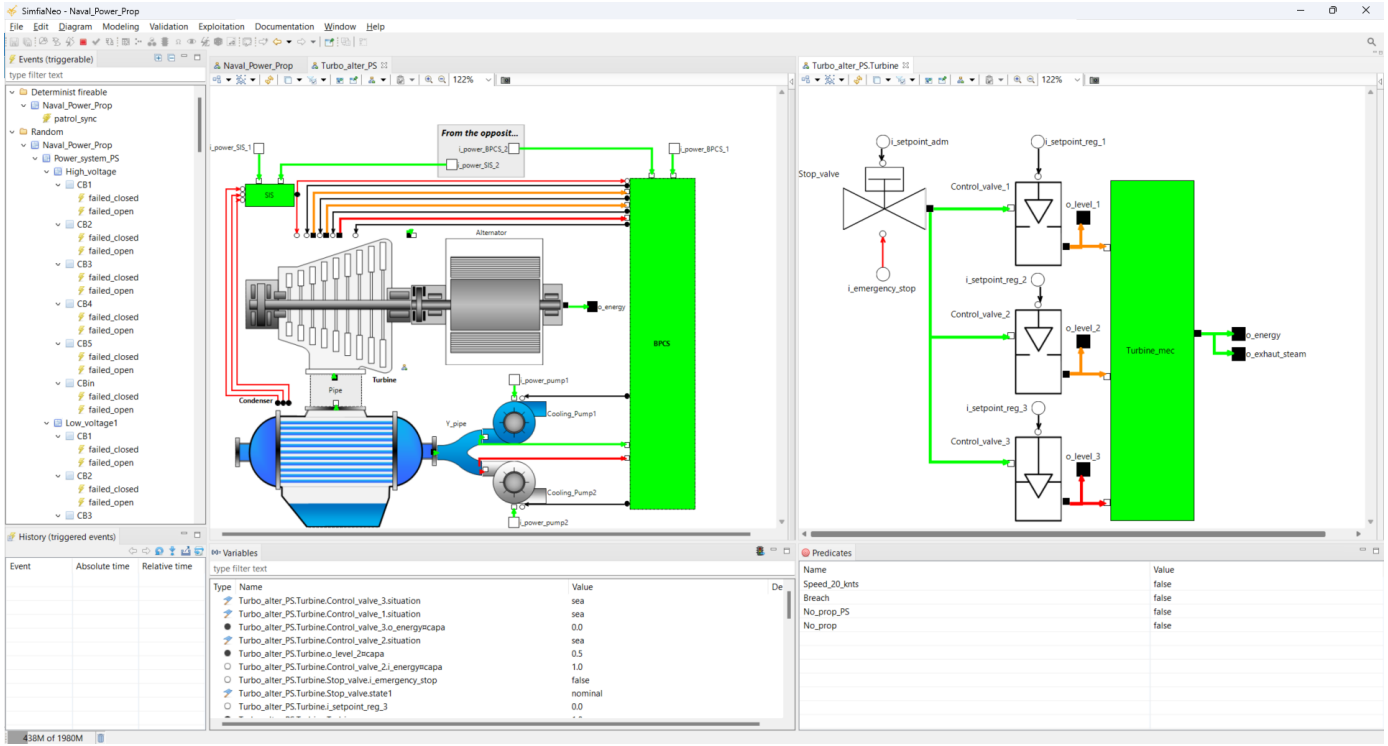
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



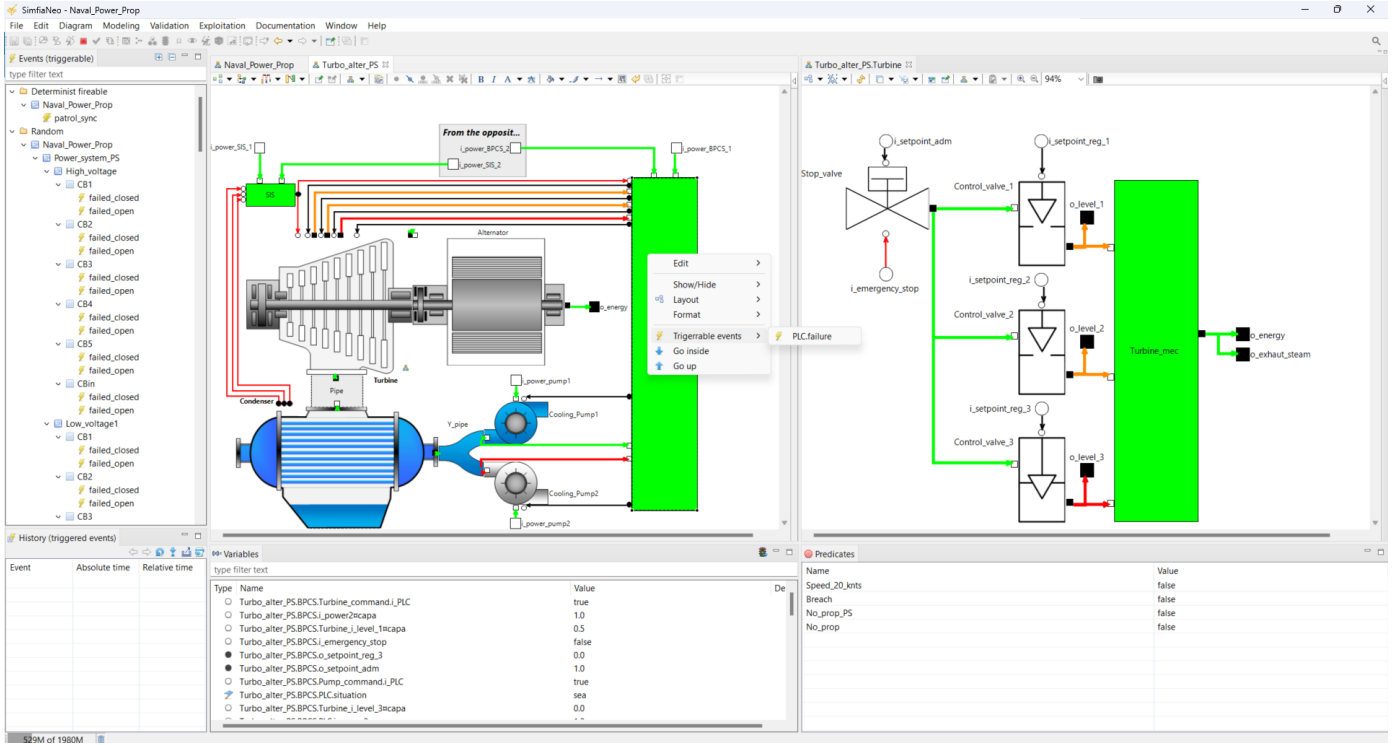
CAS D'APPLICATION
VÉRIFICATION DE LA RÉPARABILITÉ MER / QUAI



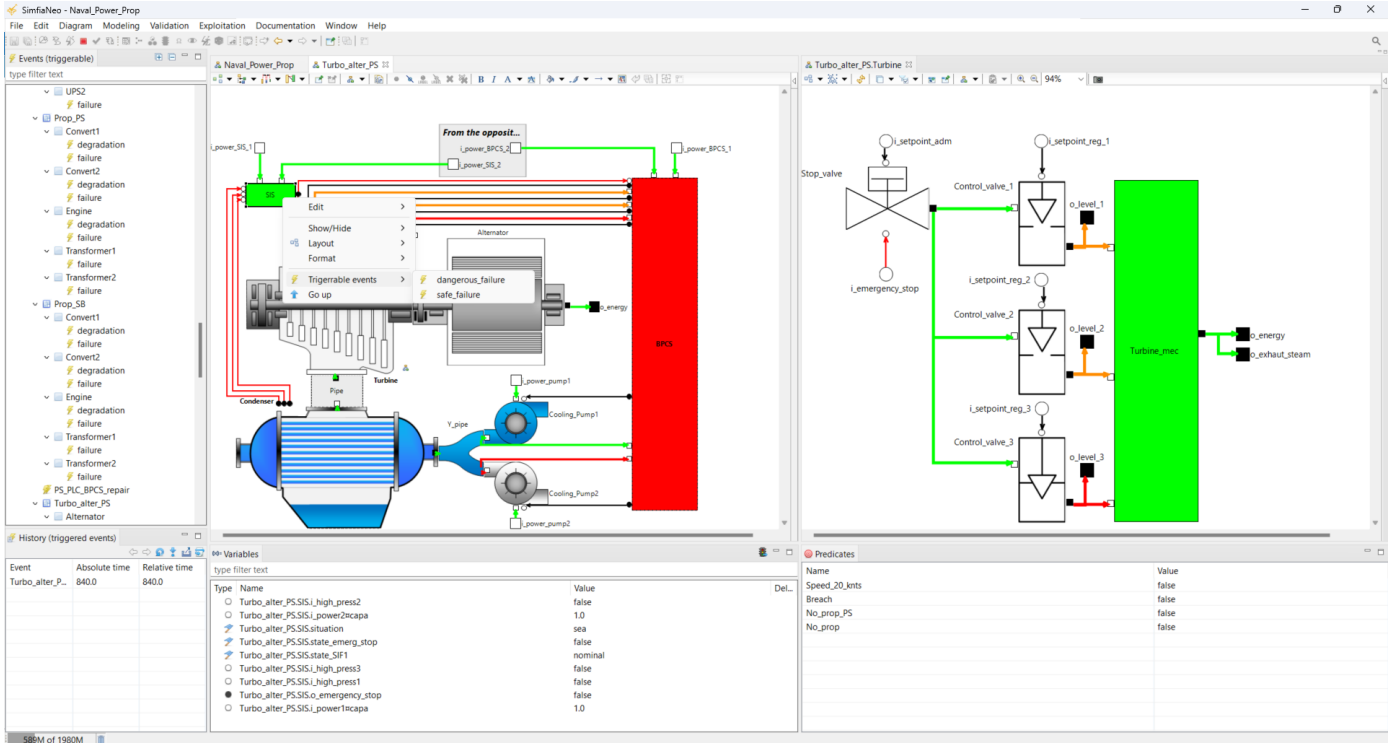
CAS D'APPLICATION
VALIDATION DU MODÈLE – SCÉNARIO BRÈCHE



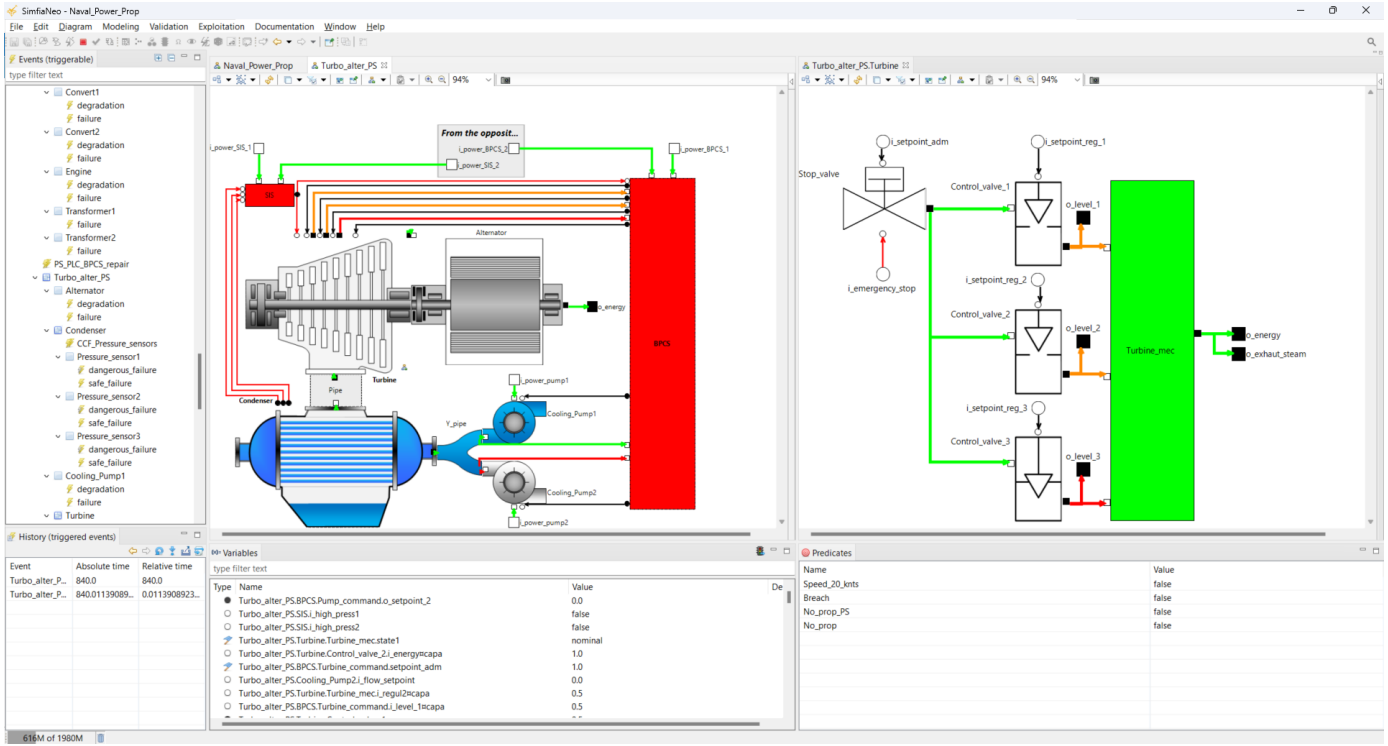
CAS D'APPLICATION
VALIDATION DU MODÈLE – SCÉNARIO BRÈCHE



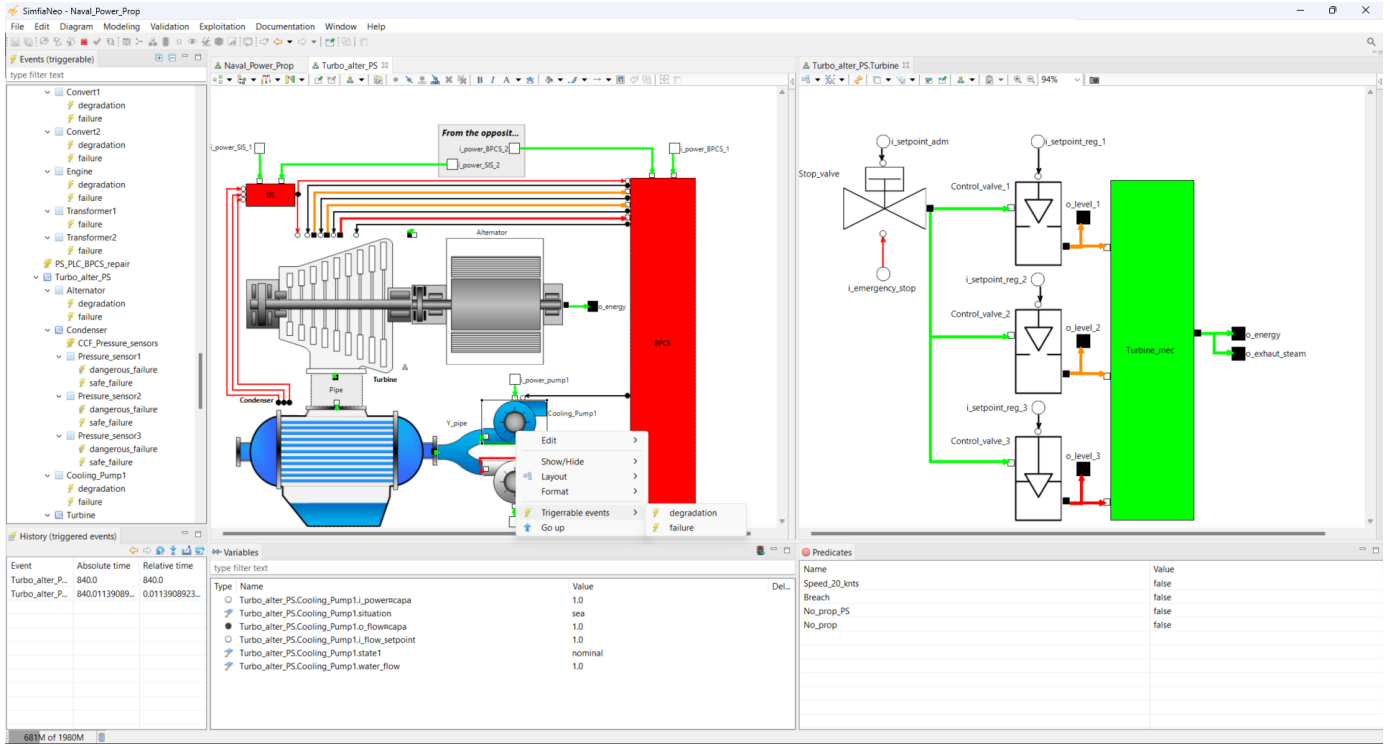
CAS D'APPLICATION
VALIDATION DU MODÈLE – SCÉNARIO BRÈCHE



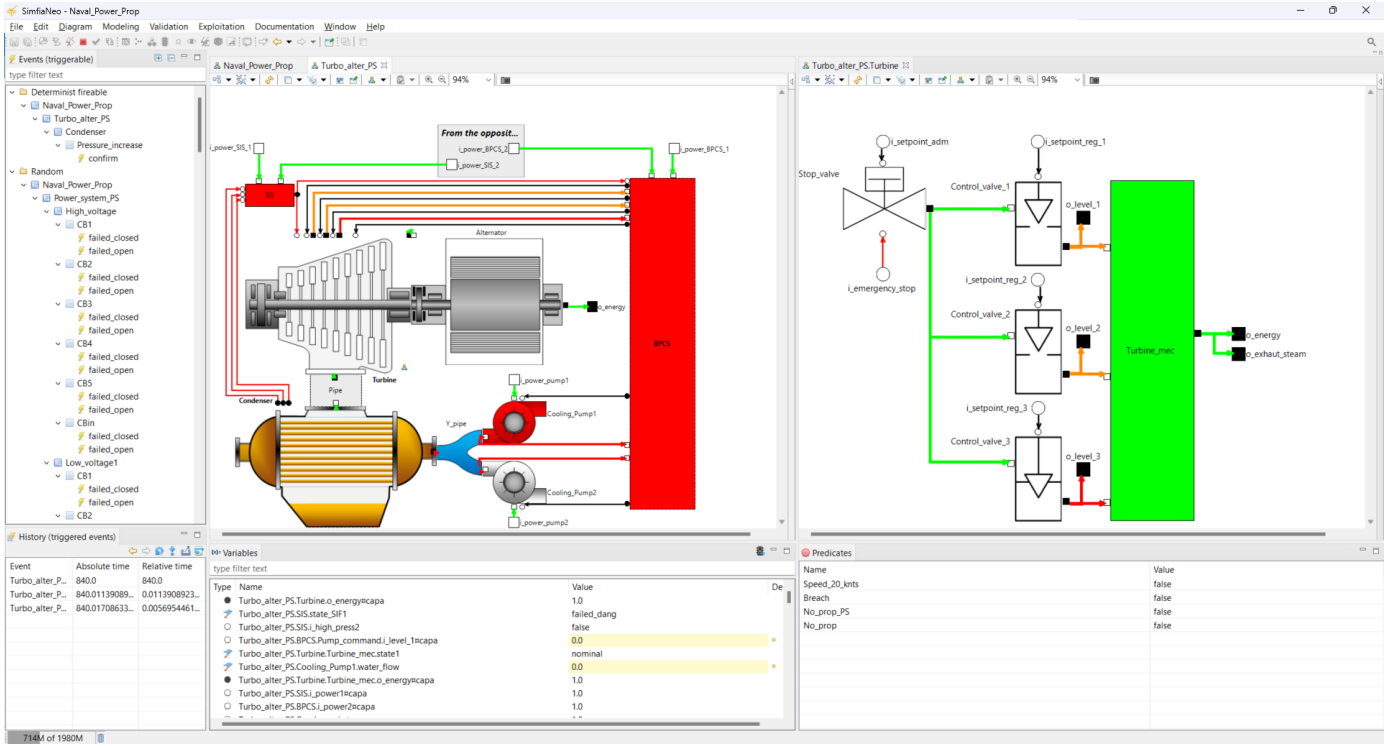
CAS D'APPLICATION
VALIDATION DU MODÈLE – SCÉNARIO BRÈCHE



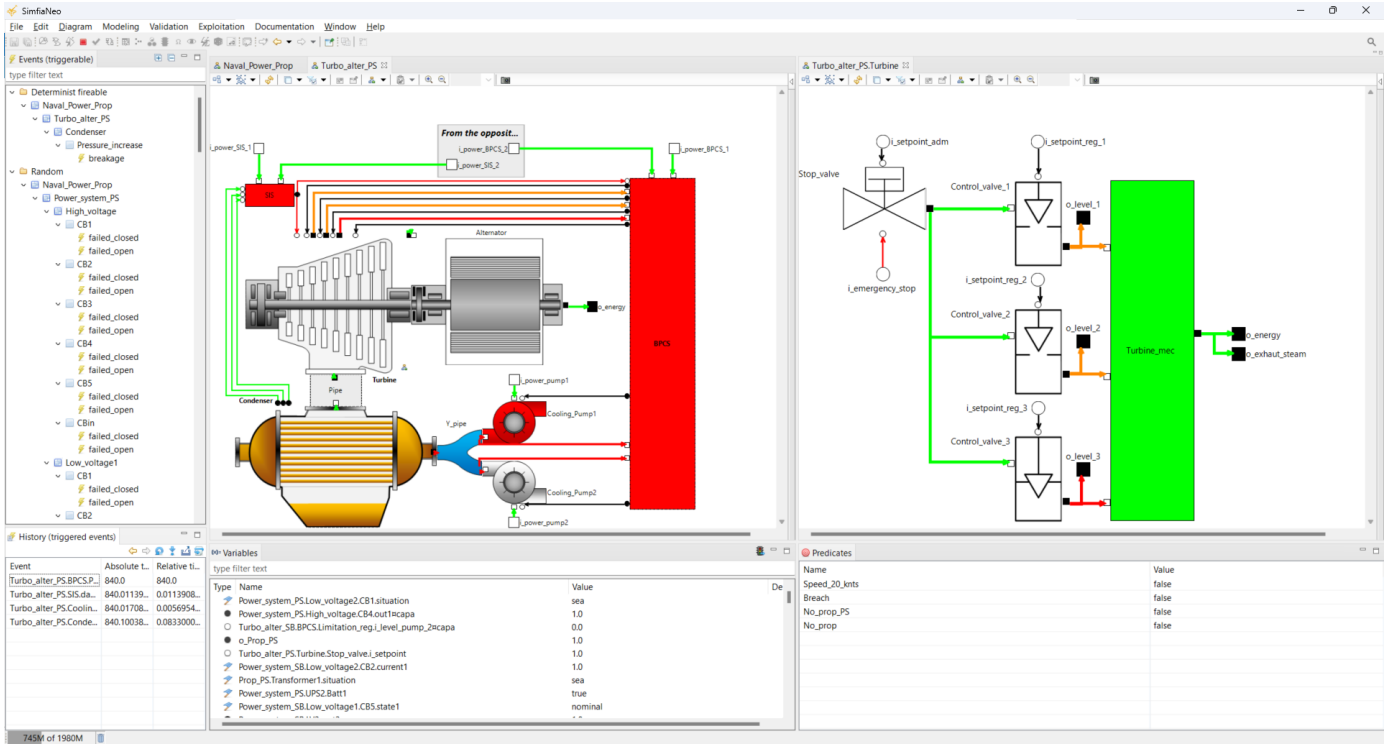
CAS D'APPLICATION
VALIDATION DU MODÈLE – SCÉNARIO BRÈCHE



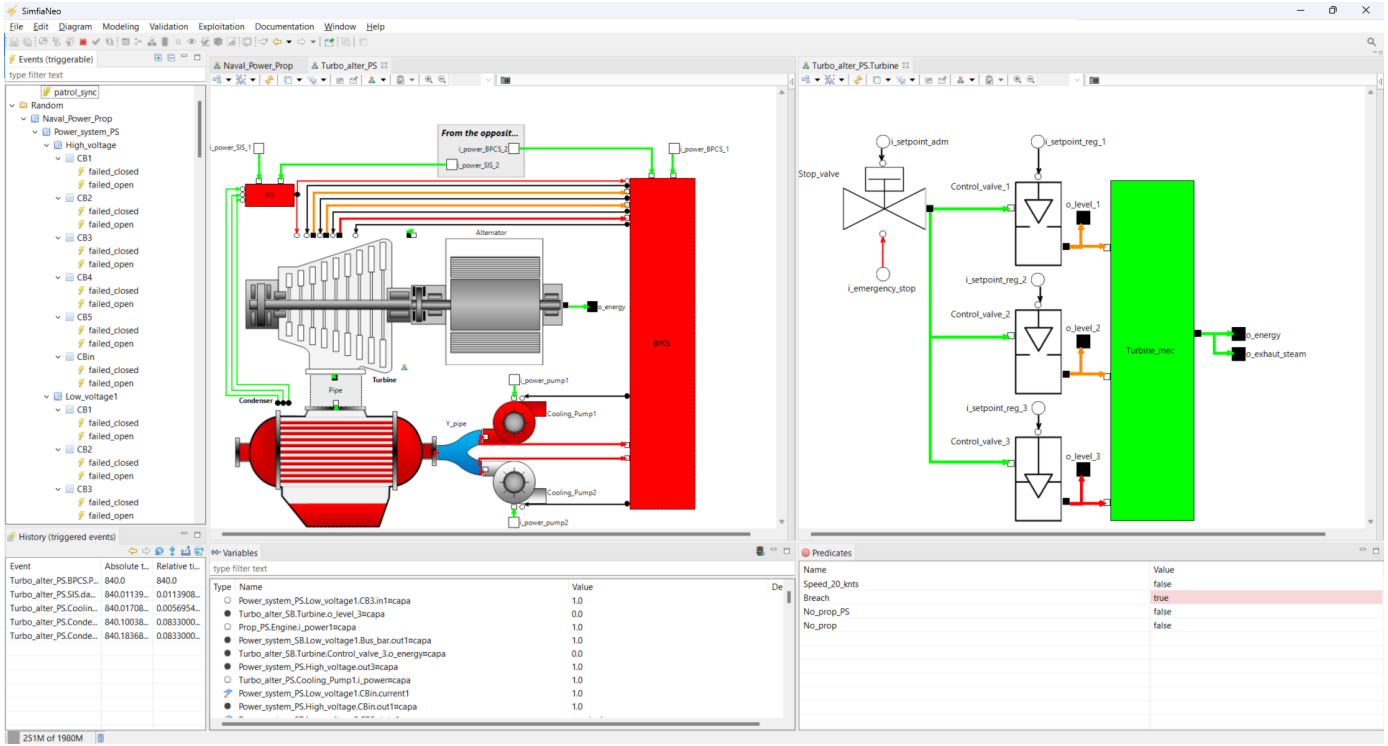
CAS D'APPLICATION
VALIDATION DU MODÈLE – SCÉNARIO BRÈCHE



CAS D'APPLICATION
VALIDATION DU MODÈLE – SCÉNARIO BRÈCHE



CAS D'APPLICATION
VALIDATION DU MODÈLE – SCÉNARIO BRÈCHE



CAS D'APPLICATION
VALIDATION DU MODÈLE – VITESSE DÉGRADÉE

La génération de séquences peut être utilisée pour vérifier que les scénarios menant à l'événement sont corrects

Les premières séquences obtenues s'avèrent tout à fait cohérentes.

Insufficent speed

	Elements	Order
1	Turbo_alter_SB.Alternator.failure	1
2	Turbo_alter_PS.Alternator.failure	1
3	Prop_PS.Engine.failure	1
4	Prop_SB.Engine.failure	1
5	Turbo_alter_SB.Turbine.Stop_valve.spurious_closing	1
6	Turbo_alter_PS.Turbine.Stop_valve.spurious_closing	1
7	Turbo_alter_PS.SIS.safe_failure	1
8	Turbo_alter_SB.SIS.safe_failure	1
9	Power_system_SB.High_voltage.CBin.failed_open	1
10	Power_system_PS.High_voltage.CBin.failed_open	1
11	Turbo_alter_PS.Turbine.Turbine_mec.failure	1
12	Turbo_alter_SB.Turbine.Turbine_mec.failure	1
13	Turbo_alter_SB.Cooling_Pump1.failure & Turbo_alter_SB.Cooling_Pump2.failure	2
14	Turbo_alter_PS.Cooling_Pump1.failure & Turbo_alter_PS.Cooling_Pump2.failure	2
15	Prop_PS.Convert1.failure & Turbo_alter_SB.Alternator.degradation	2
16	Prop_SB.Convert2.failure & Turbo_alter_PS.Alternator.degradation	2
17	Prop_SB.Convert1.degradation & Turbo_alter_PS.Alternator.degradation	2
18	Prop_SB.Convert1.failure & Turbo_alter_PS.Alternator.degradation	2
19	Prop_PS.Convert2.degradation & Turbo_alter_SB.Alternator.degradation	2

CAS D'APPLICATION
VALIDATION DU MODÈLE – SCÉNARIO BRÈCHE

Validation des scénarios brèche par la génération de séquence difficile

- Ordre minimum 5 (notamment à cause des réparations)
- Probabilité faible de chaque séquence

→Temps de calcul important

Pour augmenter l'occurrence des séquences, création d'une phase de calcul spécifique avec :

- Des taux de défaillance 100 fois plus élevés (proportion respectée)
- Les réparations désactivées

CAS D'APPLICATION
VALIDATION DU MODÈLE – SCÉNARIO BRÈCHE

NAVAL GROUP

Phases of Naval_Power_Prop

	Variable	Mission	Annual	High_lambdas
1	Phase name	Mission	Annual	High_lambdas
2	Mission time	1,679.99	8,760	8,760
3	Inactive events	0	0	92
7	Power_system_PS.Dock_source.patrol	Dirac(1,680)	Dirac(1,680)	Dirac(1,680)
8	Power_system_PS.Dock_source.situation	sea	sea	sea
9	Power_system_PS.High_voltage.CB1.current1	1.0	1.0	1.0
10	Power_system_PS.High_voltage.CB1.docking	Dirac(480)	Dirac(480)	Dirac(480)
11	Power_system_PS.High_voltage.CB1.failed_closed	Exp(5.00E-7)	Exp(5.00E-7)	Exp(5.00E-5)
12	Power_system_PS.High_voltage.CB1.failed_open	Exp(5.00E-7)	Exp(5.00E-7)	Exp(5.00E-5)
13	Power_system_PS.High_voltage.CB1.patrol	Dirac(1,680)	Dirac(1,680)	Dirac(1,680)
14	Power_system_PS.High_voltage.CB1.repair	Exp(2)	Exp(2)	*Exp(2)*
15	Power_system_PS.High_voltage.CB1.situation	sea	sea	sea
16	Power_system_PS.High_voltage.CB1.state1	nominal	nominal	nominal
17	Power_system_PS.High_voltage.CB1.update_current1	Dirac(0)	Dirac(0)	Dirac(0)
18	Power_system_PS.High_voltage.CB2.current1	1.0	1.0	1.0
19	Power_system_PS.High_voltage.CB2.docking	Dirac(480)	Dirac(480)	Dirac(480)
20	Power_system_PS.High_voltage.CB2.failed_closed	Exp(5.00E-7)	Exp(5.00E-7)	Exp(5.00E-5)
21	Power_system_PS.High_voltage.CB2.failed_open	Exp(5.00E-7)	Exp(5.00E-7)	Exp(5.00E-5)
22	Power_system_PS.High_voltage.CB2.patrol	Dirac(1,680)	Dirac(1,680)	Dirac(1,680)

Breach

	Elements	Order ▲	Probability
1	Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.Condenser.CCF_Pressure_sensors & Turbo_alter_PS.Cooling_Pump1.failure	3	4.00E-8
2	Turbo_alter_SB.SIS.dangerous_failure & Turbo_alter_SB.BPCS.PLC.failure & Turbo_alter_SB.Cooling_Pump1.failure	3	8.00E-8
3	Turbo_alter_PS.Condenser.CCF_Pressure_sensors & Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.Alternator.failure	3	3.00E-8
4	Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.Condenser.CCF_Pressure_sensors & Turbo_alter_PS.Cooling_Pump1.degradation	3	4.00E-8
5	Turbo_alter_SB.BPCS.PLC.failure & Turbo_alter_SB.Condenser.CCF_Pressure_sensors & Power_system_SB.High_voltage.CBin.failed_o...	3	1.00E-8
6	Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.SIS.dangerous_failure & Turbo_alter_PS.Cooling_Pump1.failure	3	1.20E-7
7	Turbo_alter_SB.BPCS.PLC.failure & Turbo_alter_SB.Condenser.CCF_Pressure_sensors & Turbo_alter_SB.Cooling_Pump1.failure	3	5.00E-8
8	Turbo_alter_SB.SIS.dangerous_failure & Turbo_alter_SB.BPCS.PLC.failure & Turbo_alter_SB.Alternator.failure	3	6.00E-8
9	Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.SIS.dangerous_failure & Turbo_alter_PS.Alternator.failure	3	5.00E-8
10	Turbo_alter_PS.SIS.dangerous_failure & Power_system_SB.Low_voltage2.CB1.failed_open & Turbo_alter_PS.Alternator.failure	3	1.00E-8
11	Power_system_PS.Low_voltage2.CB1.failed_open & Turbo_alter_SB.Condenser.CCF_Pressure_sensors & Turbo_alter_SB.Alternator.fai...	3	3.00E-8
12	Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.SIS.dangerous_failure & Turbo_alter_PS.Cooling_Pump1.degradation	3	1.40E-7
13	Turbo_alter_SB.BPCS.PLC.failure & Turbo_alter_SB.Condenser.CCF_Pressure_sensors & Turbo_alter_SB.Cooling_Pump1.degradation	3	4.00E-8
14	Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.Condenser.CCF_Pressure_sensors & Power_system_PS.Low_voltage1.CB2.failed_o...	3	1.00E-8
15	Turbo_alter_SB.SIS.dangerous_failure & Turbo_alter_SB.BPCS.PLC.failure & Turbo_alter_SB.Cooling_Pump1.degradation	3	1.10E-7
16	Turbo_alter_SB.Alternator.degradation & Turbo_alter_PS.SIS.dangerous_failure & Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS....	4	1.00E-8
17	Turbo_alter_SB.Condenser.CCF_Pressure_sensors & Prop_PS.Convert2.failure & Turbo_alter_SB.BPCS.PLC.failure & Turbo_alter_SB.Al...	4	1.00E-8
18	Turbo_alter_PS.Turbine.Stop_valve.stuck_opening & Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.Turbine.Control_valve_1.stuc...	4	1.10E-7
19	Turbo_alter_PS.BPCS.PLC.failure & Prop_SB.Convert1.failure & Turbo_alter_PS.SIS.dangerous_failure & Turbo_alter_PS.Cooling_Pum...	4	1.00E-8
20	Turbo_alter_PS.Turbine.Control_valve_2.stuck_in_the_middle & Turbo_alter_PS.Turbine.Stop_valve.stuck_opening & Turbo_alter_PS.B...	4	1.00E-8
21	Turbo_alter_PS.SIS.dangerous_failure & Turbo_alter_PS.Turbine.Control_valve_2.stuck_opening & Turbo_alter_PS.BPCS.PLC.failure & ...	4	1.00E-8
22	Power_system_SB.Low_voltage2.CB4.failed_closed & Turbo_alter_SB.BPCS.PLC.failure & Turbo_alter_SB.Condenser.CCF_Pressure_se...	4	1.00E-8
23	Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.Condenser.CCF_Pressure_sensors & Turbo_alter_SB.Cooling_Pump1.degradation ...	4	2.00E-8
24	Prop_SB.Convert2.failure & Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.Condenser.CCF_Pressure_sensors & Turbo_alter_PS.C...	4	1.00E-8
25	Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_SB.Condenser.CCF_Pressure_sensors & Turbo_alter_SB.BPCS.PLC.failure & Turbo_alte...	4	2.00E-8
26	Prop_PS.Convert1.failure & Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.SIS.dangerous_failure & Turbo_alter_PS.Cooling_Pum...	4	1.00E-8
27	Turbo_alter_PS.BPCS.PLC.failure & Turbo_alter_PS.Condenser.CCF_Pressure_sensors & Prop_PS.Convert2.degradation & Turbo_alter...	4	1.00E-8

CAS D'APPLICATION
VALIDATION DES CALCULS STOCHASTIQUES

NAVAL GROUP

Stochastic configurations of Naval_Power_Prop

	Name	Phase	Number of stories	Seed	Last launch date	Up-to-date
1	Mission	Mission	10,000,000	123,456,789	01/12 08:59	
2	Annual	Annual	10,000,000	123,456,789	01/12 08:44	

Mission

	Observer	Type	Value	Standard deviation	95% confidence min value	95% confidence max value
1	Breach_count	Count	1.00E-6	1.00E-3	3.8019E-7	1.6198E-6
2	No_prop_PS_final	FinalValue	0.0498	0.2175	0.0497	0.0499
3	No_prop_final	FinalValue	3.1234E-3	0.0558	3.0888E-3	3.158E-3
4	Speed_20_knts_final	FinalValue	0.0498	0.2175	0.0497	0.0499
5	Speed_avg	WeightedValue	28.5419	3.1215	28.54	28.5438

Annual

	Observer	Type	Value	Standard deviation	95% confidence min value	95% confidence max value
1	Breach_count	Count	4.50E-6	2.1213E-3	3.1852E-6	5.8148E-6
2	No_prop_PS_final	FinalValue	4.083E-3	0.0638	4.0435E-3	4.1225E-3
3	No_prop_final	FinalValue	8.16E-5	9.0329E-3	7.6001E-5	8.7199E-5
4	Speed_20_knts_final	FinalValue	4.083E-3	0.0638	4.0435E-3	4.1225E-3
5	Speed_avg	WeightedValue	28.7454	1.4379	28.7445	28.7463

RETOUR D'EXPÉRIENCE

Préparation de l'étude → Optimise la modélisation (identification du besoin et des attendus)

Vérification / validation et de documentation :

- Prise de recul par rapport au modèle
- Opportunité de détecter des erreurs de modélisation

L'utilisation massive / systématique des classes représente un gain de temps de vérification et de mise à jour du modèle

Du travail supplémentaire … mais pas forcément conséquent (notamment grâce à la génération automatique)

Réel gain en termes de confiance dans les résultats

PERSPECTIVES

Expérimentation dans les entités respectives des membres du projet

Compilation des retours

Portage du guide sous forme de norme

- Facilité par le format utilisé
- D'abord au niveau français
- Puis à l'international (si possible)
- Discussions en cours sur le positionnement
  - Probablement groupe d'expert joint UF56 (Sûreté de Fonctionnement) / UF65 (Mesure et commande dans le processus industriel)
  - Passerelle vers l'ISO/IEC JTC 1/SC 7 (Ingénierie du logiciel et des systèmes)


NAVAL
GROUP