Journée Cecilia: Cas d’étude ferroviaire

01/06/2023

DIGITAL LEAF

DIGITAL LEAF

- Consultant indépendant
- 16 ans d’expérience en sûreté de fonctionnement Ferroviaire
- Evaluateur indépendant de la sécurité (ISA)
- Ingénieur Safety
- Facilitateur/Promoteur MBSA

Contexte

Démonstration de faisabilité

Modéliser la fonction « Echange Voyageurs » d'une ligne de métro

Evaluer l'effet des pannes simples et des pannes multiples grâce aux analyses Safety dirigées par les modèles (MBSA).

Mettre en lumière les équivalences et les écarts entre le MBSA et l'état de l'art de la SdF Ferroviaire

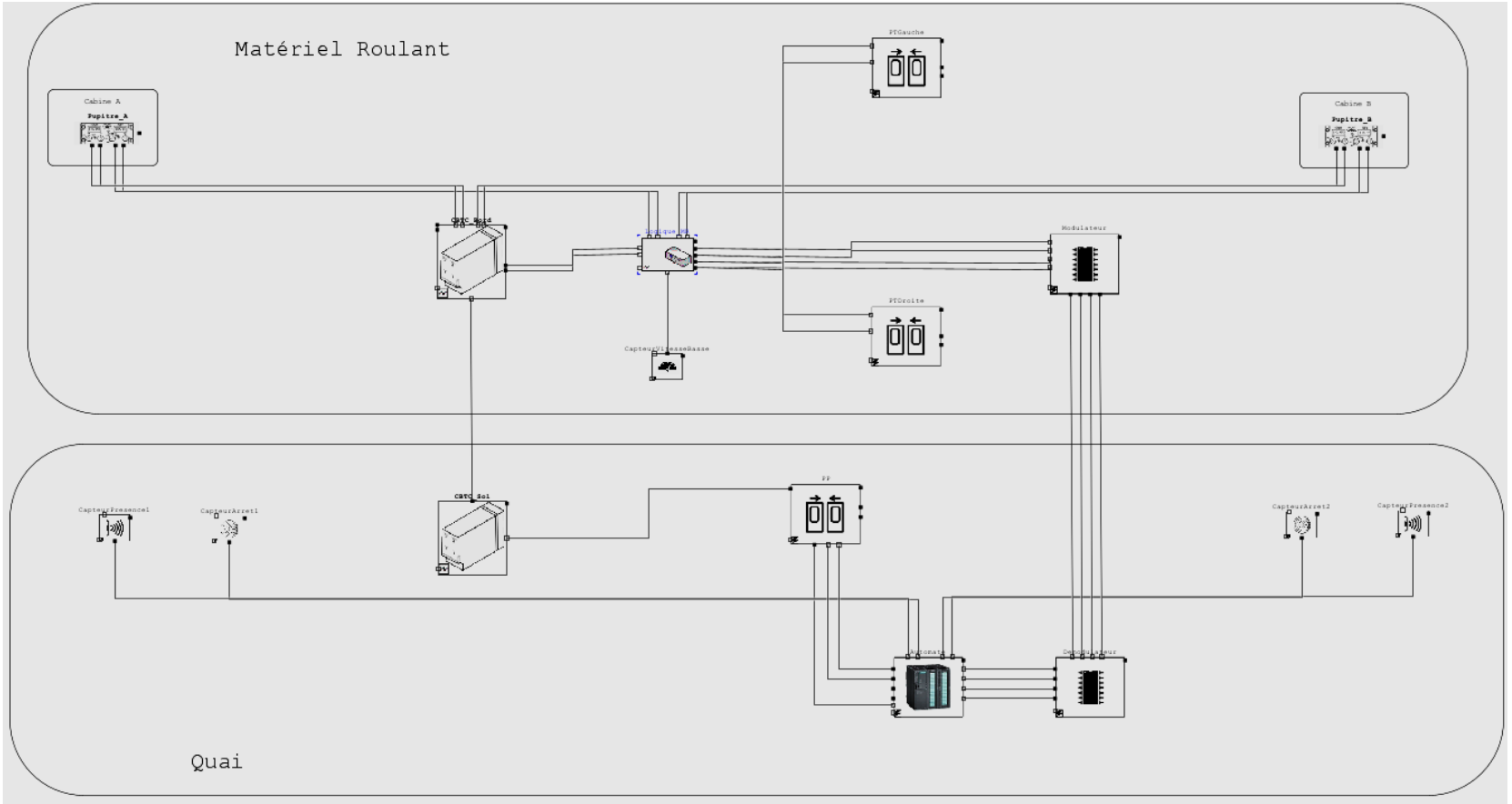
Montrer ce que le MBSA permet de faire, ce qu'il ne fait pas, ce qu'il pourrait faire.

En partenariat avec SATODEV

RATP

SATODEV
SAFETY TOOLS DEVELOPMENT

Echange Voyageurs



Permet la desserte de voyageurs

Des équipements embarqués à bord des trains (CBTC Bord)

Des équipements de voie et en station (CBTC Sol, Portes Palières)

Evénement redouté: Ouverture des portes (train ou palière) alors que le train n’est pas totalement inscrit à quai.

Evénements Redoutés

Deux événements identifiés:

ER1: Train non inscrit à quai et portes train ouvertes

ER2: Train non inscrit à quai et portes palières ouvertes

Que veut-on analyser ?

- L’effet des pannes simples
- L’effet des pannes multiples
- Adresser les défauts aléatoires et systématiques
- Sous l’angle de vue statique et dynamique

Etat de l’art

- Rappel de l’état de l’art selon la CENELEC EN 50129:2018
- Que veut-on faire avec un modèle ?
- Est-ce équivalent à l’état de l’art ?
- Quelles améliorations possibles par rapport aux analyses traditionnelles ?

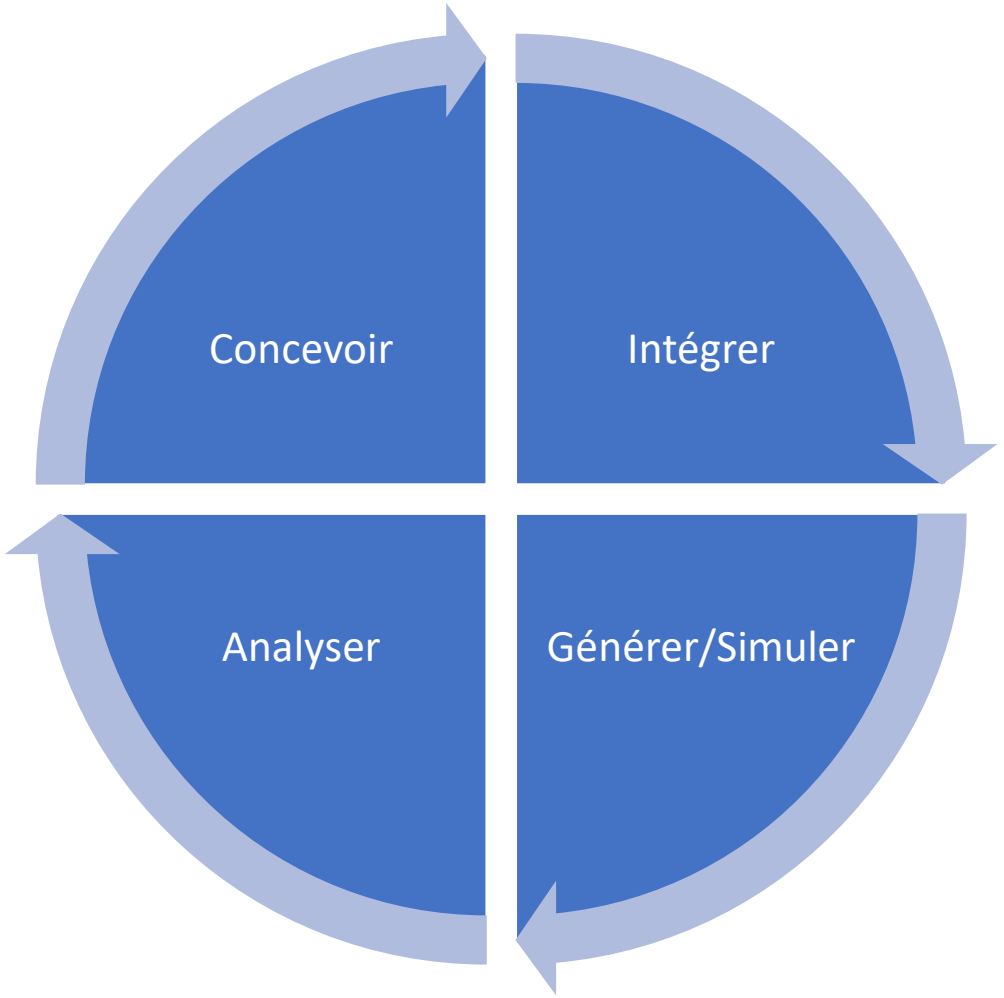
Tableau E.6 — Méthodes d'analyse des situations dangereuses et des défaillances

Techniques/Mesures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Analyse des modes de défaillance et de leurs effets (AMDE)	HR	HR	HR	HR	(a)
2 Etudes de danger et d'exploitabilité (HAZOP)	HR	HR	HR	HR	(b)
3 Analyse par arbre de panne	HR	HR	HR	HR	(c)
4 Graphes de Markov	HR	HR	HR	HR	(d)
5 Diagramme de fiabilité	R	R	R	R	(e)
6 Analyse par zone	R	R	R	R	(f)
7 Analyse des défaillances de cause commune	HR	HR	HR	HR	(g)
8 Analyse des évènements historiques	R	R	R	R	(h)
9 Diagramme Causes-Conséquences	R	R	R	R	(i)
10 Arbre d'évènements	R	R	R	R	(l)

Méthodologie

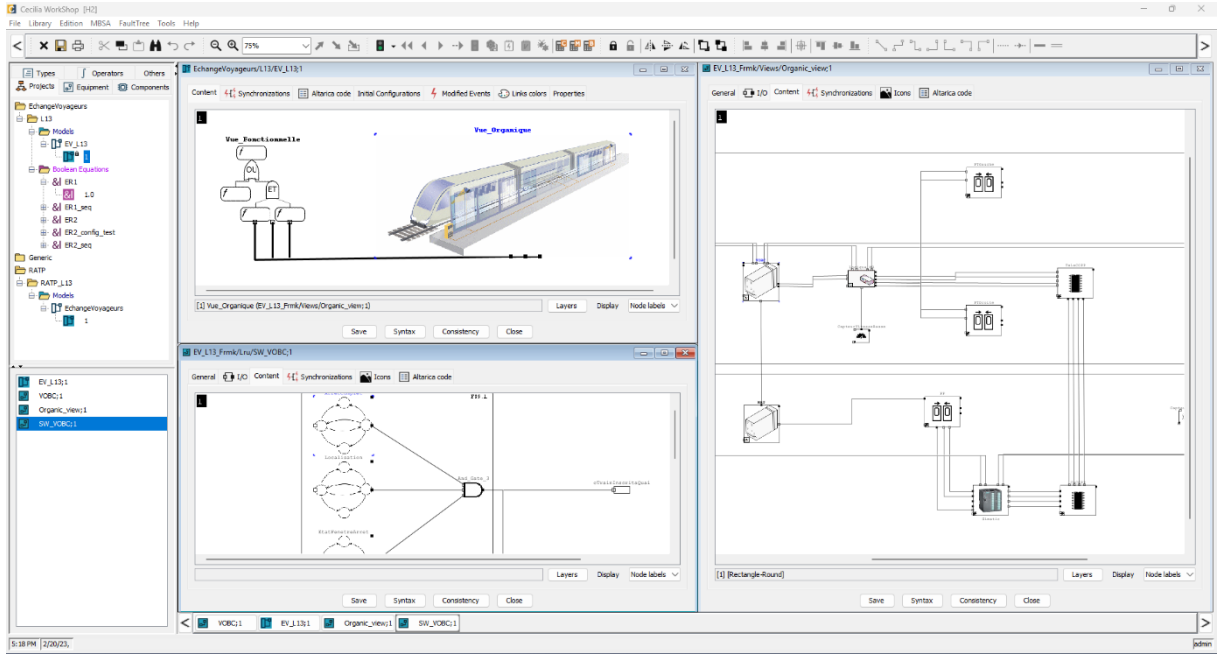
Proposition de méthodologie:

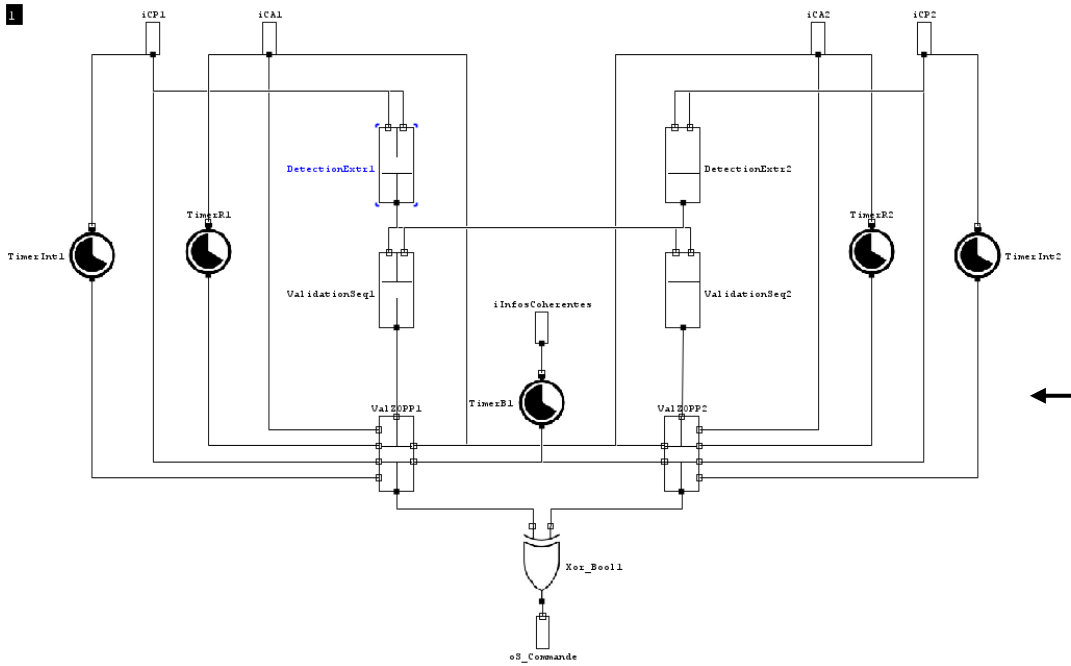
- Donner des perspectives méthodologiques de manière à ce que le client puisse se projeter sur une intégration d'activités MBSA dans un processus respectant les standards en vigueur.
- Cycle itératif.
- Permet de poser un cadre à adapter aux exigences de chaque utilisateur.



Deux Modèles

Un premier modèle complet statique (modèle de propagation de défaillances).



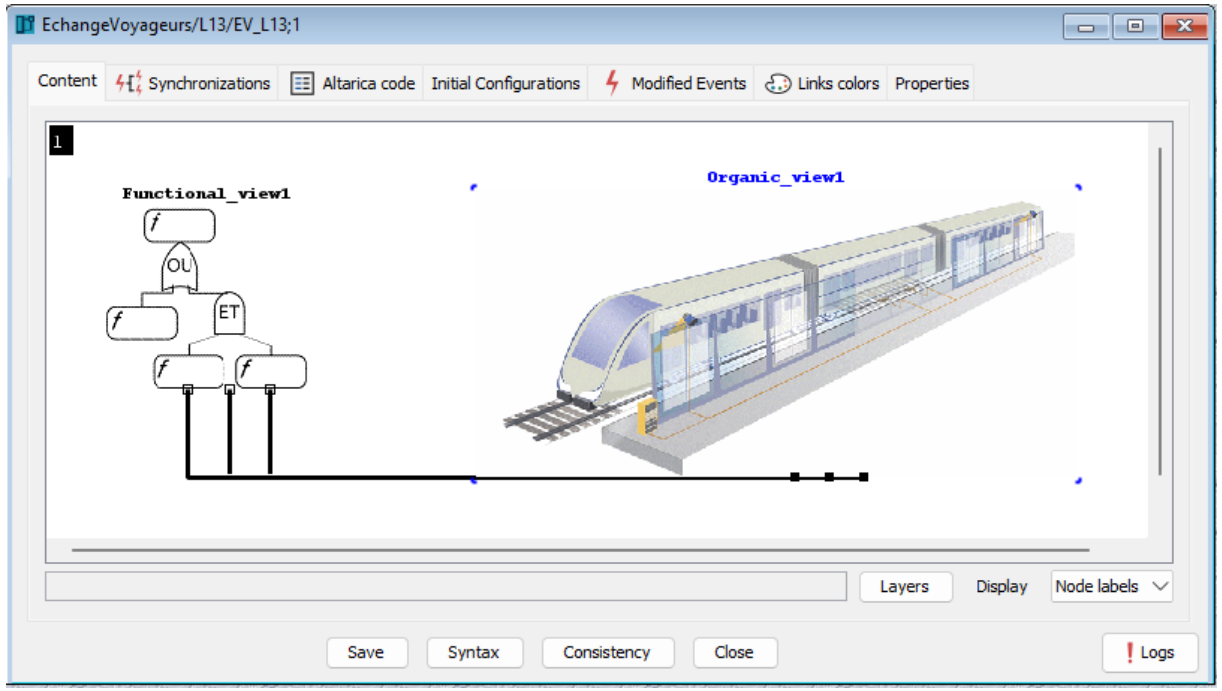


Un second modèle réduit à une problématique précise « dynamique ».

Approche Multi-Vues

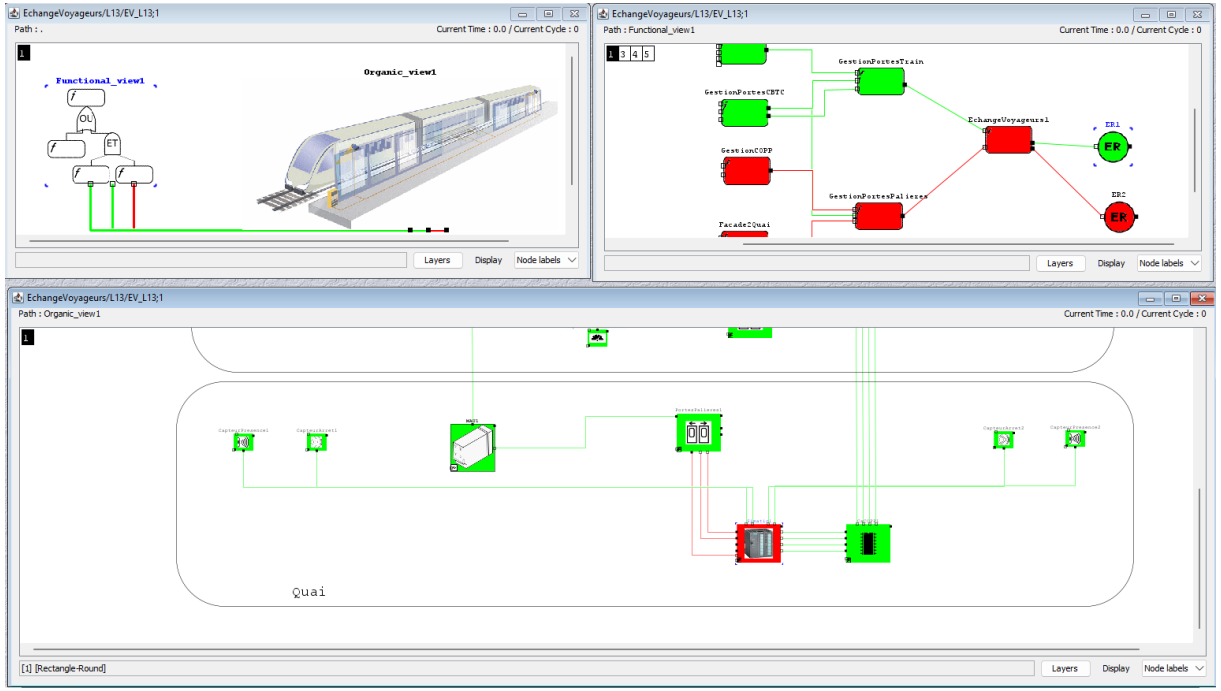
Développement d’un modèle composé de deux vues :

- Une vue fonctionnelle représentant la décomposition fonctionnelle de la fonction « Echange Voyageurs » associée aux événements redoutés sous-jacents.
- Une vue de l’architecture du système implémentant la fonction « Echange Voyageurs ».



Simulation / Génération de résultats / Analyse

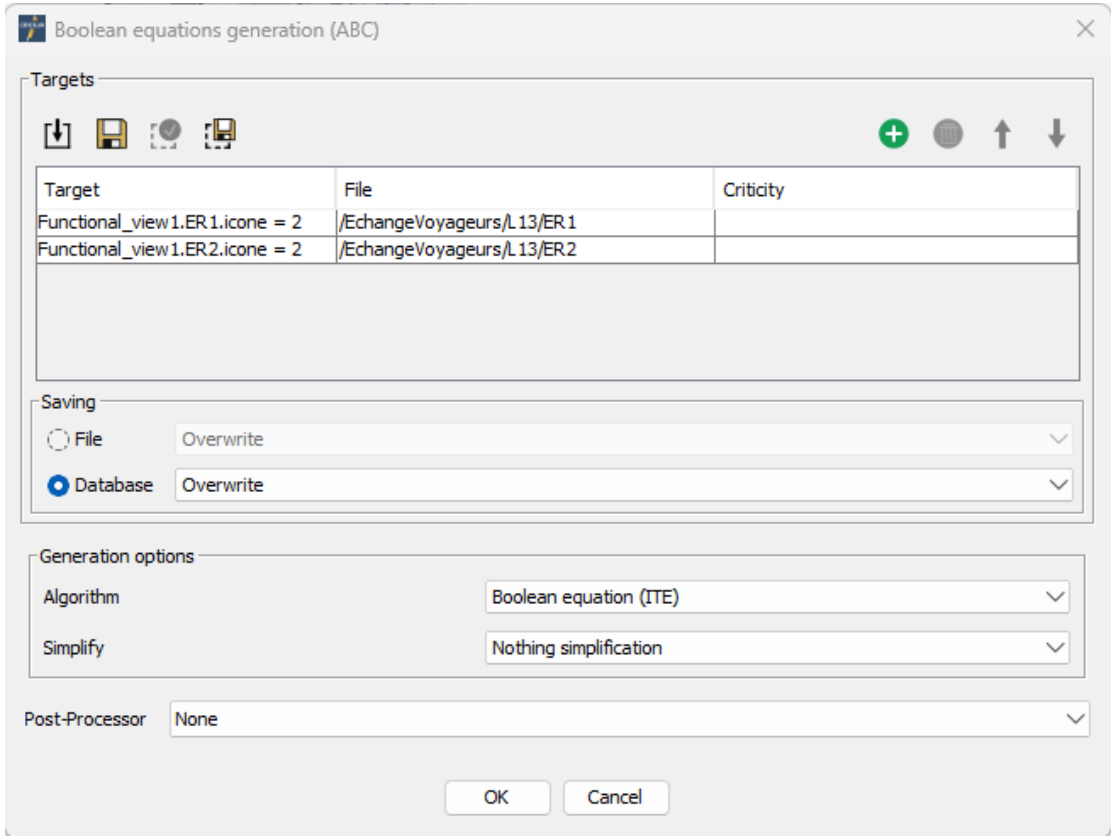
- Génération d’équations booléennes ;
- Génération de FMEA ;
- La génération des coupes (qualitative et quantitative) ;
- La génération de séquence ;
- Model-Checking (ARC).



Équations booléennes

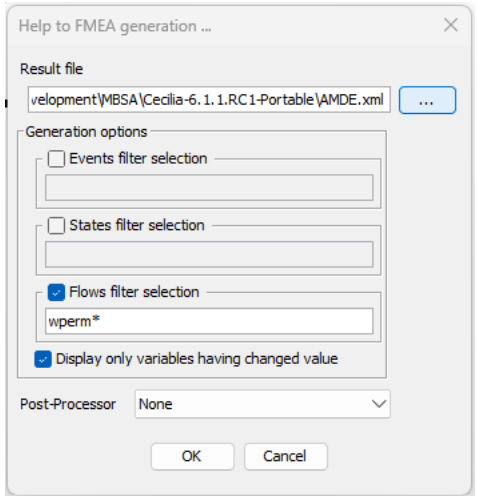
Deux événements redoutés :

- ER1 : Ouverture des portes trains à tort lorsque le train n'est pas correctement inscrit à quai ;
- ER2 : Ouverture des portes palières à tort lorsque le train n'est pas correctement inscrit à quai.

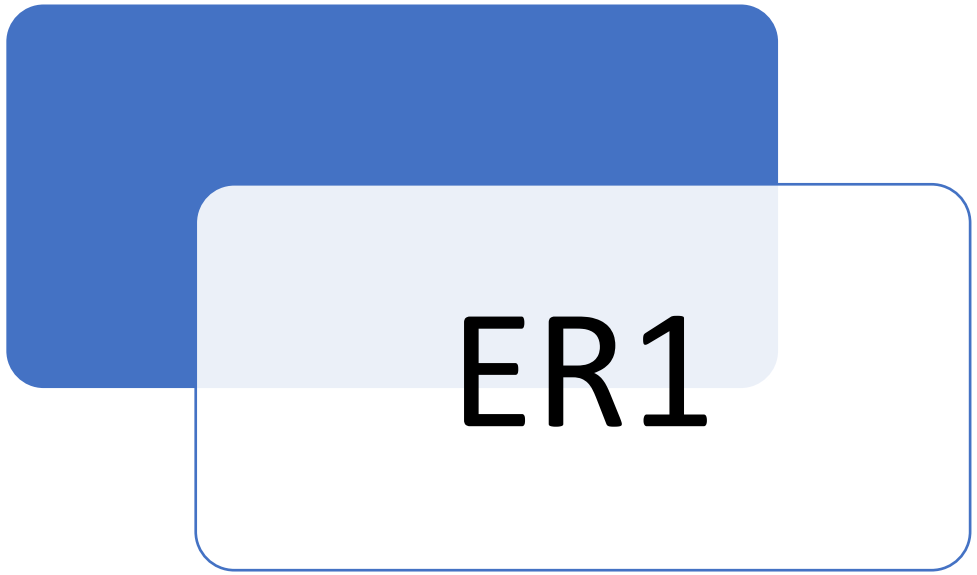


Aides à la génération FMEA

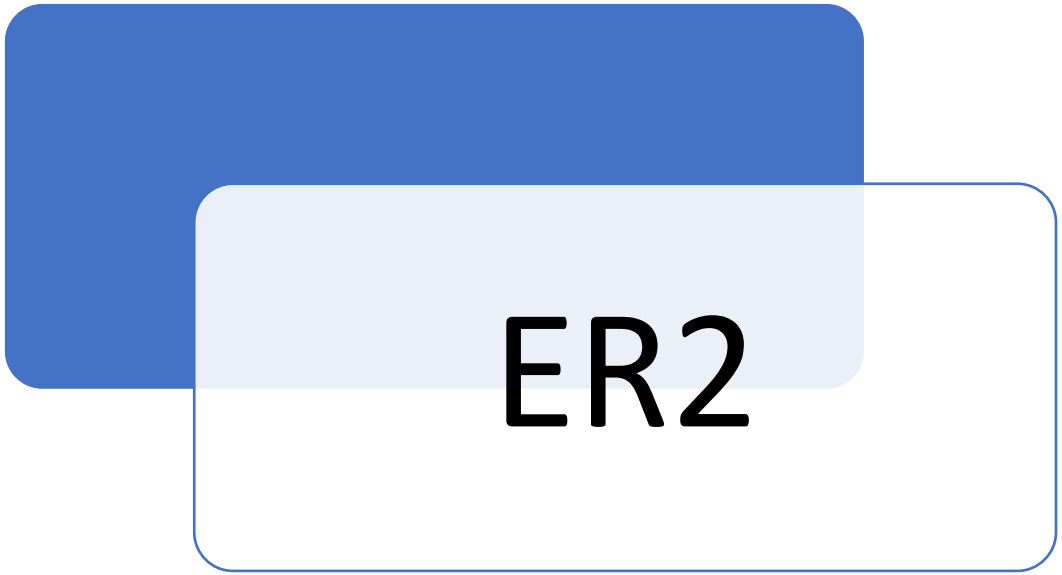
- L’aide à la génération FMEA permet d’extraire la liste des pannes simples et leurs caractéristiques en vue de mener une analyse type AMDE.
- Extraction des événements menant à des flux « permissifs à tort »



Calcul de coupes

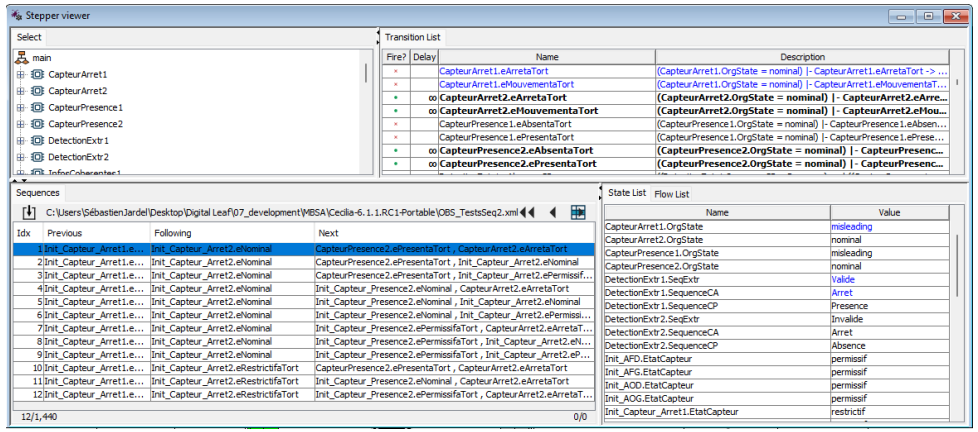


Order	Quantity	Occurrence
1	1	1.0000E-09
2	2	1.0100E-12



Order	Quantity	Occurrence
1	2	2.0000E-08
3	24	4.0866E-11

Evaluation des scénarios issus de la génération de séquences



Exemple de séquence:

```
<seq <tr id="50" evt="Init_Capteur_Arret1.eNominal"/>
        <tr id="6" evt="CapteurPresence1.ePresentaTort"/>
        <tr id="56" evt="Init_Capteur_Arret2.eNominal"/>
        <tr id="70" evt="Init_Capteur_Presence2.ePermissifaTort"/>
        <tr id="58" evt="Init_Capteur_Arret2.ePermissifaTort"/>
        <tr id="52" evt="Init_Capteur_Arret1.ePermissifaTort"/> </seq>
```

Interprétation:

- Détection d'un mouvement par le capteur d'arrêt n°1
- Détection à tort d'une présence sur le capteur de présence n°1 (défaillance du capteur de présence)
- Détection d'un mouvement par le capteur d'arrêt n°2
- Détection d'une présence sur le capteur de présence n°1 (objet devant le capteur de présence)
- Détection d'un arrêt sur les deux capteurs d'arrêt n°1 et n°2

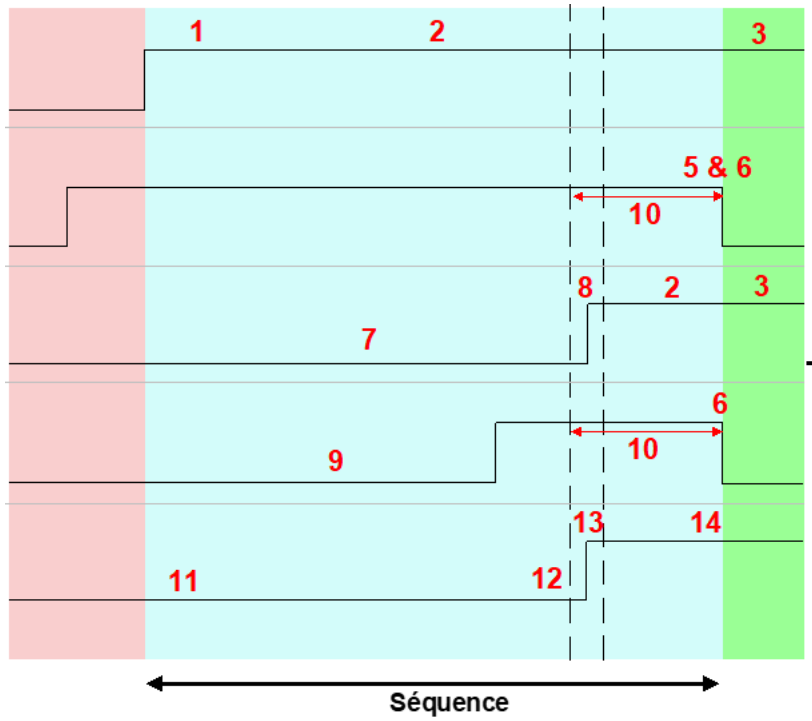
-> Détection à tort d'une séquence d'arrivée correcte du train.

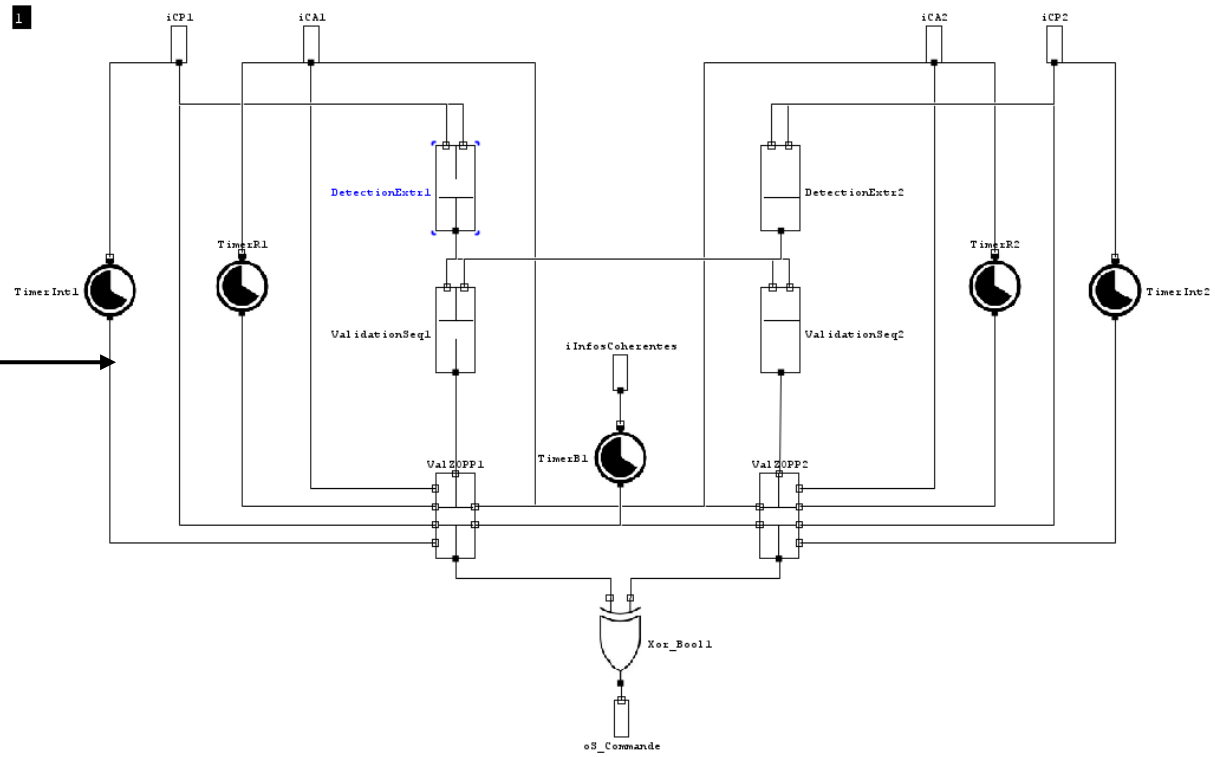
Analyse:

Ce scénario n'est pas suffisant pour atteindre l'ouverture des portes palières. Certes, le train est détecté à quai mais il faut encore une communication correcte issue du train.

Ainsi, la génération de séquence à l'ordre 6 montre que malgré une combinaison de défaillance et d'événements indésirables du à l'environnement du quai, il est très peu probable d'obtenir une ouverture des portes palières.

Modèle Dynamique





ARC : Model-Checker

- Cecilia-Workshop propose une mise à plat du modèle en « Altarica Labri »
- Le “AltaRica Labri” est exploitable par des algorithmes de model-checking permettant de verifier si un modèle satisfait des propriétés de sécurité décrites en logiques temporelles (CTL*): Outil en ligne de commandes ARC développé (et maintenu ?) par le LaBRI
- Les propriétés peuvent être exprimées sous un format de specification Acheck ou MEC 5 (les deux outils principaux)

Objectif: évaluer d’autres modes d’exploration d’un modèle que ceux proposés par Cecilia-Workshop.

```
// Evenement redoute n°1: Il existe une détection de séquence d'arrivée d'un train à
l'extrémité d'un quai alors qu'au moins un capteur n'est pas dans l'état permissif
ER1 := [ (DetectionExtr1^^oSeqExtr=Valide) & (((CapteurPresence1^^oPresence!=permissif)
& (CapteurPresence1^^oPresence!=wpermissif)) |
((CapteurArret1^^oCapteurArret!=permissif) &
(CapteurArret1^^oCapteurArret!=wpermissif))) ];

// Existe-t-il un chemin menant éventuellement à l'ER1 ?
RES1 := ctlspec E [ F ER1];
```

Bilan / Synthèse

- Mise en lumière des apports du MBSA comme:
  - Permet d'acquérir une compréhension approfondie du système (davantage que par analyse linéaire des spécifications).
  - Améliore le partage de la connaissance et le travail collaboratif.
  - Capitalise l'expérience.
- Permet de réaliser des analyses telles que celles présentées par l'état de l'art
  - Effet des pannes simples : Oui
  - Effet des pannes multiples : Oui
  - Causes Communes : Oui
  - Markov: pas évalué
  - Analyse fonctionnelle (séquences, model-checking) : Oui
- Mais des limites existent:
  - Nécessite de nouvelles compétences, notamment une excellente capacité d'abstraction.
  - Passage du format XML à un format plus lisible.
  - L'exhaustivité, c'est bien mais qu'en fait-on ?
  - Model-checker ARC, hors Cecilia-Workshop, en ligne de commande destiné à des érudits avec des écarts conceptuels entre familles de langage AltaRica (dataflow vs Labri).