Université de Lille

École Doctorale MADIS 6 3 1

Université Gustave Eiffel

Contributions aux activités de sécurité des systèmes complexes critiques ferroviaires

Cadre des systèmes de contrôle-commande avancés

Julie Beugin

Soutenance d'HDR

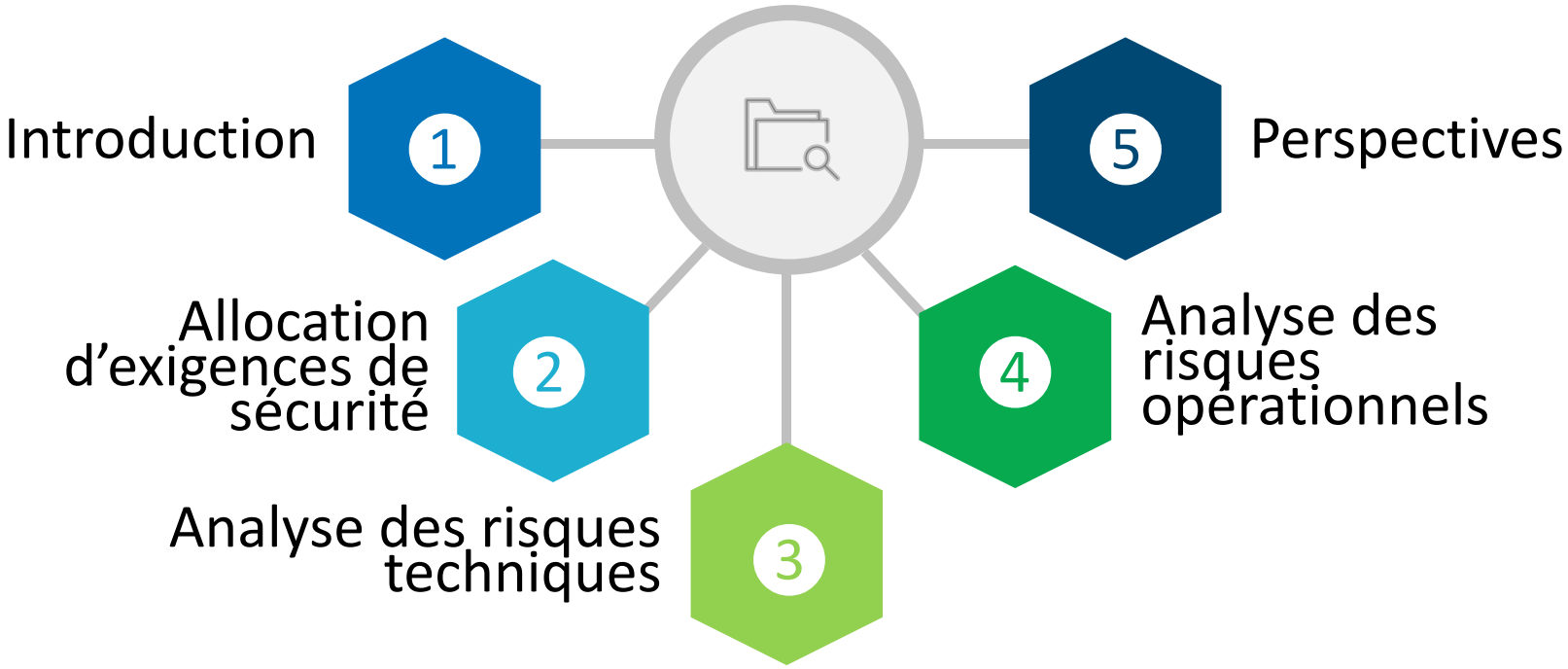
14 novembre 2024

Mohamed Ghazel	DR, Univ. Gustave Eiffel	Garant
Walter Schön	Pr. UTC	Rapporteur
Zineb Simeu-Abazi	Pr. Univ. Grenoble Alpes	Rapporteure
Philippe Weber	Pr. Univ. de Lorraine	Rapporteur
Stefano Ricci	Pr. Sapienza Univ. di Roma	Examinateur
Laurent Cebulski	Directeur de l'EPSF	Invité

Plan

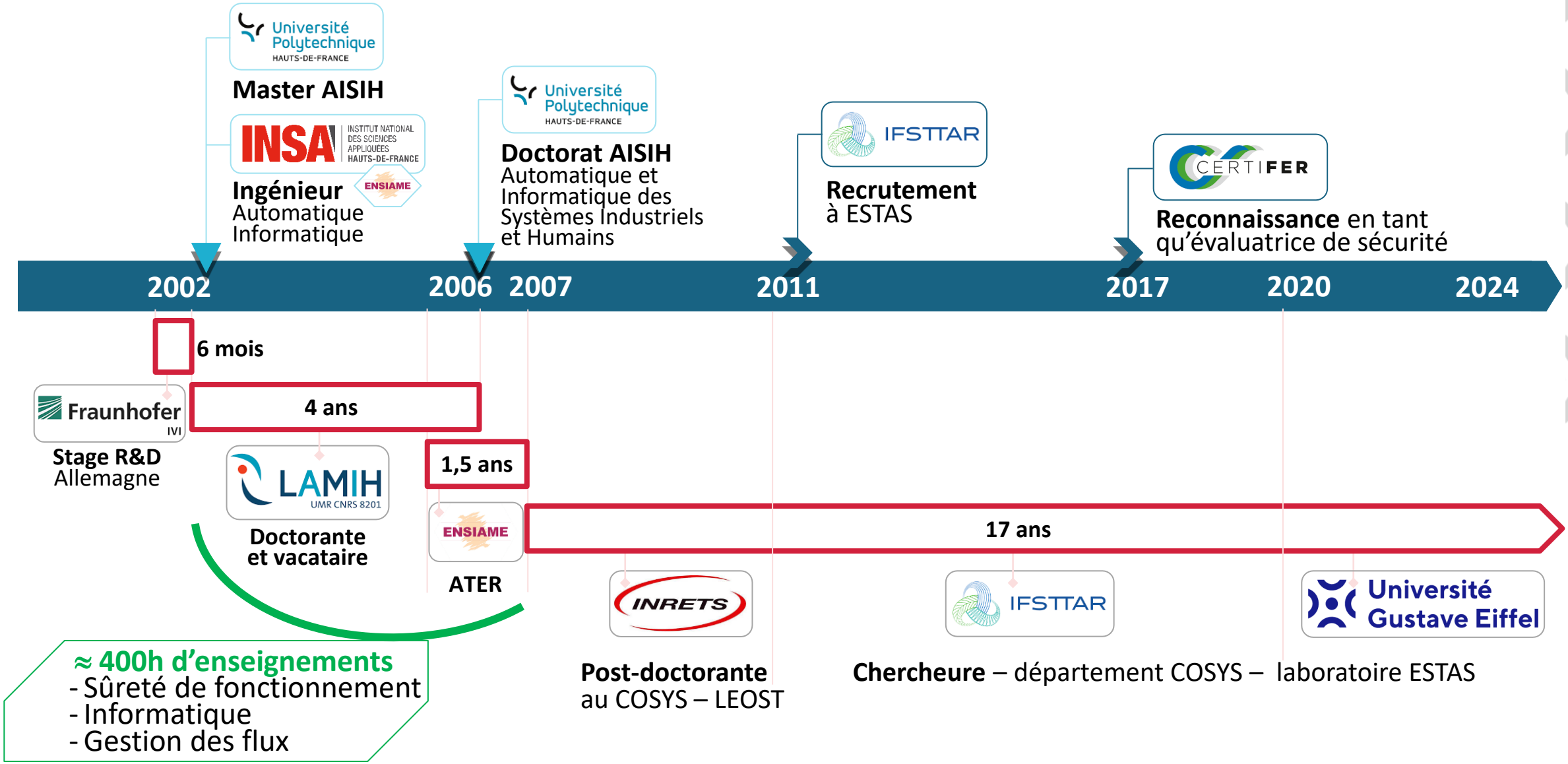
CV

Activités de recherche



Curriculum Vitæ

Diplômes et parcours



Activités de recherche : encadrements et axes

Doctorants

- **Mohammed Chelouati** (2020-2024)
- **Ouail Himrane** (2018-2022)
- **Cyril Legrand** (2012-2016)

Postdoctorant·e·s

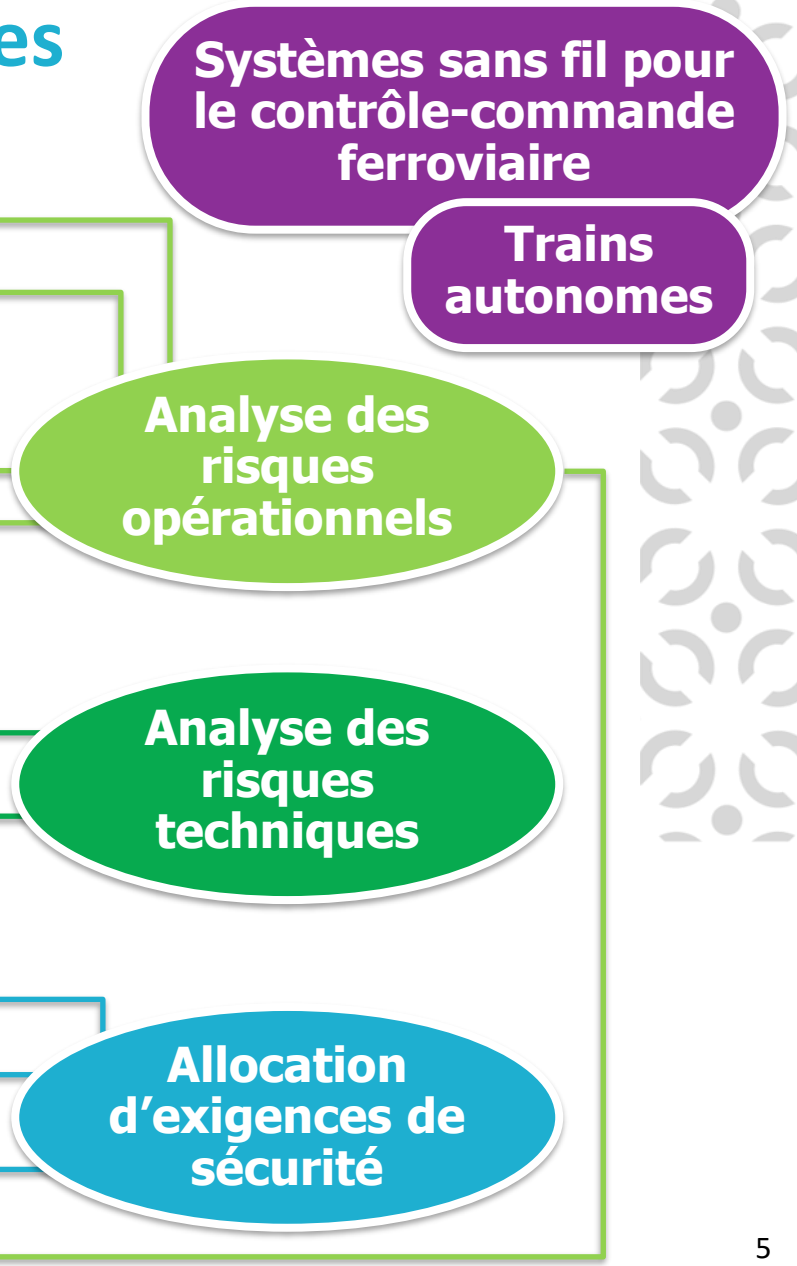
- **Mohammed Chelouati** (1 an)
- **Rim Saddem** (≈1,5 ans)
- **Thi Phuong Khanh Nguyen** (≈3 ans)
- **Kiswendsida Abel Ouedraogo** (≈2,5 ans)

Ingénieur·e·s

- **Insaf Sassi** (≈1,5 ans)
- **Nourdine Aït Tmazirte** (≈6 mois)
- **Abhimanyu Tonk** (≈1 an)

Stagiaires

- 5 stagiaires de M2



Activités de recherche : production et rayonnement

Publications scientifiques

- **17 articles** dans des revues internationales avec comité de lecture
- **44 communications avec actes** dans des congrès internationaux ou nationaux

Participations à des projets

- **18 projets** européens, nationaux et régionaux
- **1 projet national en tant que coordinatrice**
- 21 rapports de recherche
- 1 rapport d'étude, 6 rapports d'expertise

Participations à des jurys

- 6 jurys de thèse en tant qu'examinatrice
- 1 comité de sélection d'enseignant-chercheur
- 1 jury de concours d'ingénieur de recherche

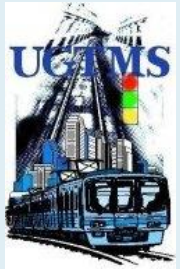
Participation à des projets et à 1 chaire

Chaire « Sécurité des systèmes ferroviaires »
depuis 2022

9 projets européens

Transports guidés urbains (FP5 & FP6)

2002-2004



2005-2006

MODurban

Satellites (EUSPA)

2017- 2019

ERSAT GGC

2016 - 2017

STARS

2012 - 2014

GaLoROI smart railway localisation

2012 - 2014

qualisar

CC ferroviaires (Shift2Rail-IP2)

2020-2023

PERFORMINGRAIL

2020-2023

X2RAIL 4

2017-2020

X2RAIL 2

9 projets nationaux

Mobilité autonome

2018-2023

TRAIN AUTONOME SERVICE VOYAGEURS

2017-2021

TC-Rail

Application de concepts de sécurité

sur 2018 (CPER)
Smarties

2013-2015
SIL

2012-2015
Systuf

2007-2009
TRain MD

GARA sur 2010

2022-2025
Flexy

sur 2016
SatRail

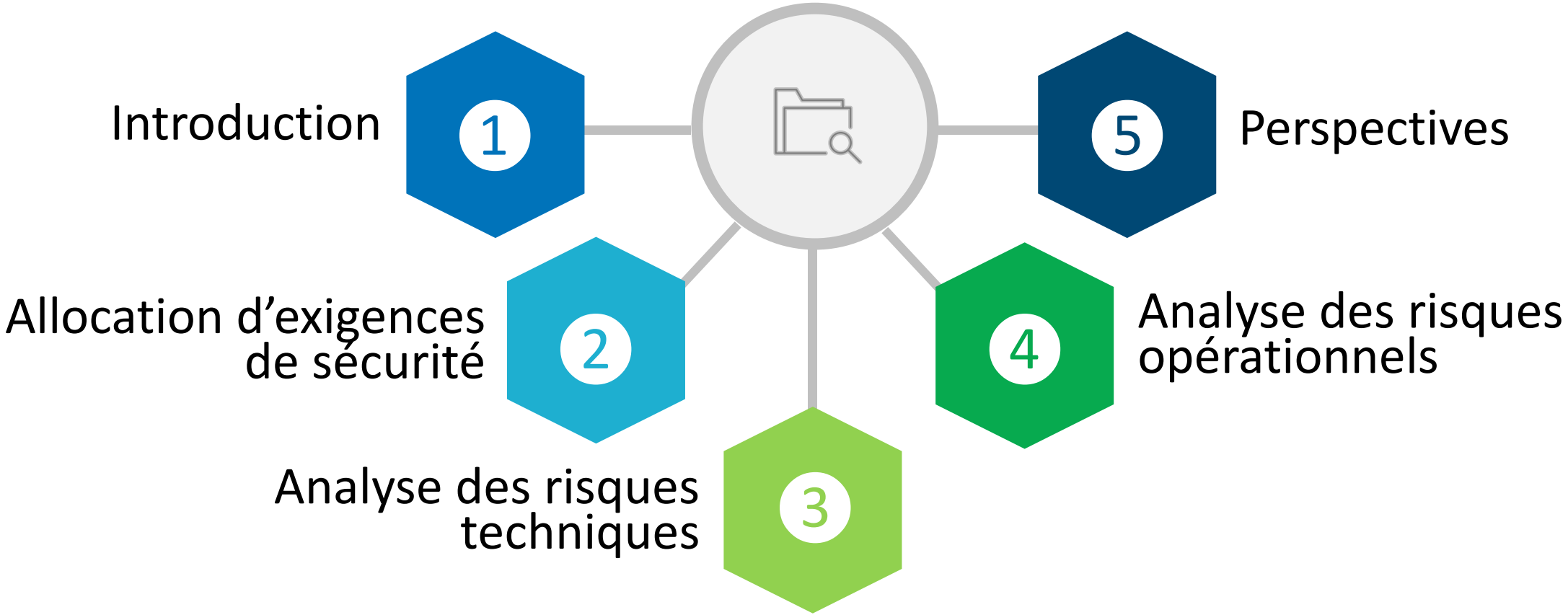
RAILENIUM
RAIL RESEARCH & INNOVATION

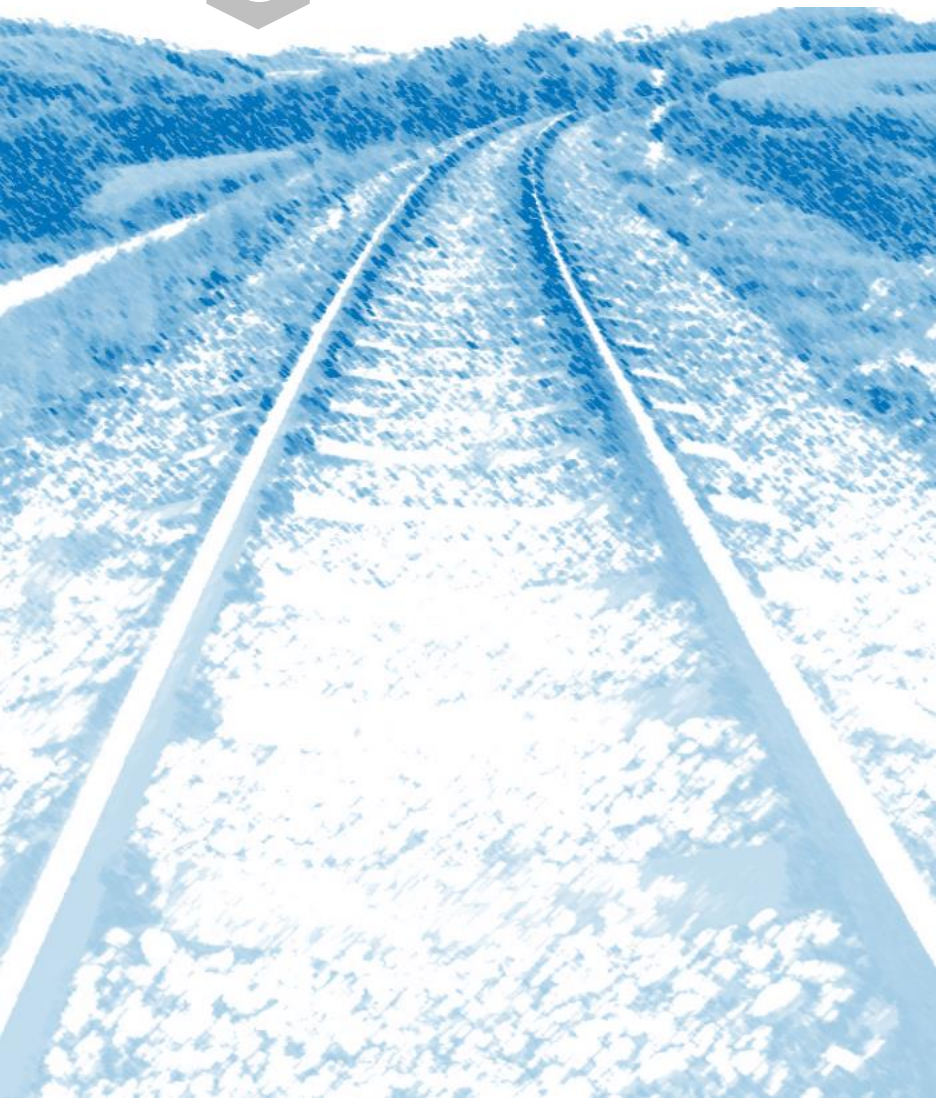
Insertion dans la communauté scientifique

Responsabilité	– dans l'animation de l'équipe 'Sécurité' d'ESTAS (dep. 2023)
Insertion dans la communauté	– 5 conférences 'invitée' – 7 séminaires (dont 5 pour des groupes de recherche)
Membre de comités de programme	– de conférences en transport / sécurité – présidence de sessions
Évaluatrice	– d'articles (conférences et revues) – 1 projet ANR – axe stratégique (CETU, analyse et maîtrise des risques)
Reconnaissance en tant qu'expert	– Certifer – BNF - localisation par satellites

Plan

Activités de recherche





Introduction

Contexte européen

Enjeu de l'UE pour les transports ferroviaires :

Offre → Performances → Coûts d'infrastructure

Accroître leur **attractivité** et leur **compétitivité**

Levier :

Systèmes de **C**ontrôle-**C**ommande et de **S**ignalisation ferroviaire

➡ **CCS ferroviaires avancés**

Performances Sécurité

Cadre de l'ERTMS

ERTMS – *European Rail Traffic Management System*

le CCS ferroviaire européen : issu de travaux d'harmonisation afin de tendre vers un système ferroviaire **unique** et **interopérable**

➡ Aujourd'hui

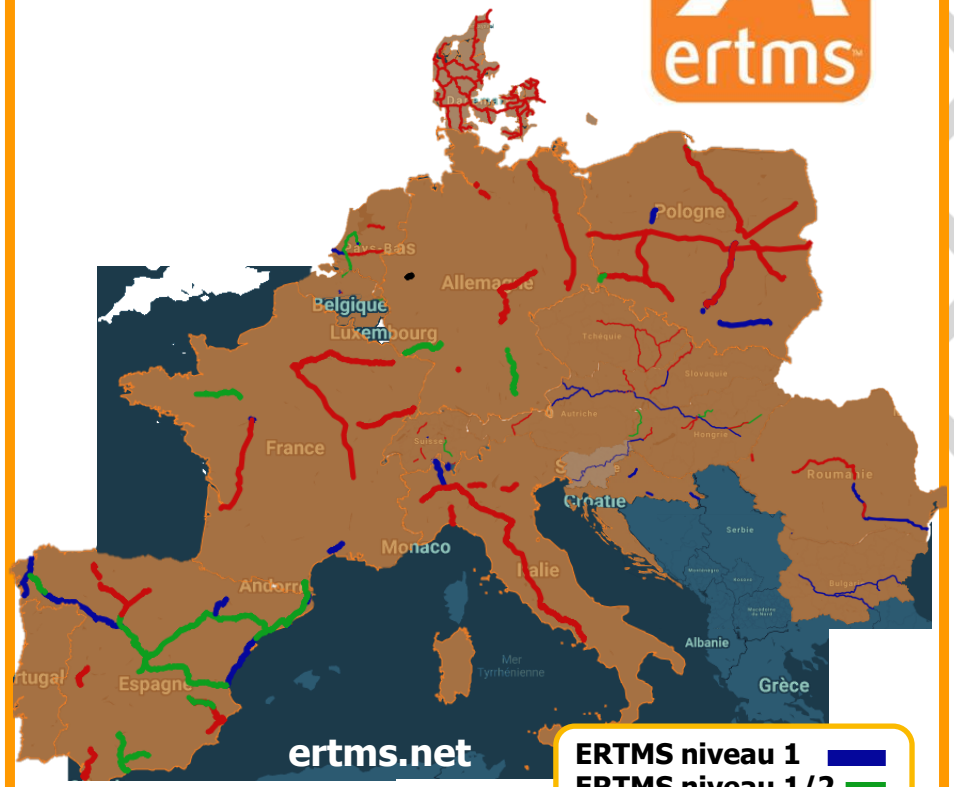
Il est réglementé, possède plusieurs niveaux, et son déploiement est progressif.

➡ Évolutions

Réflexions dans le cadre de projets de recherche européens :

Shift2Rail et Europe's Rail

Déploiement européen actuel



Chiffres estimés pour 2021 :
- **6700 km** de voie équipés
- **5700 véhicules** équipés

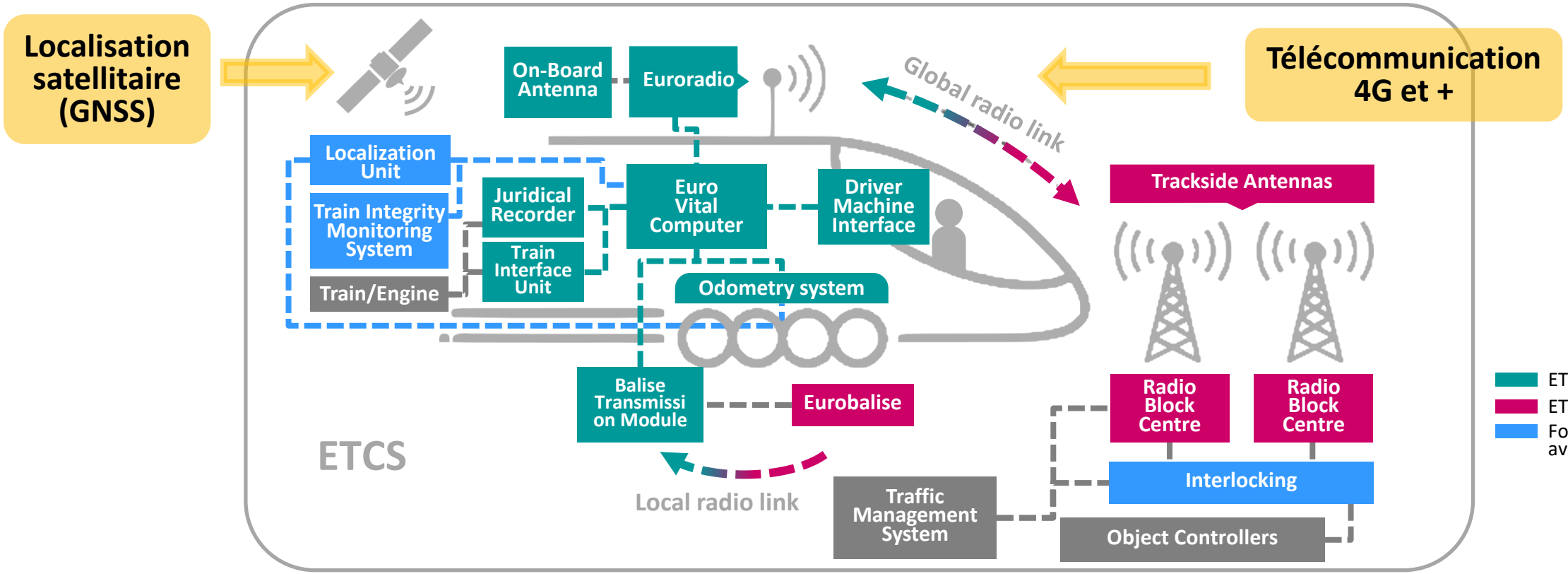
Évolution de l'ETCS : un système complexe critique

ETCS – *European Train Control System*

- Système critique de **protection** automatique des trains d'ERTMS
- survitesse, zone non-autorisée

Améliorations

- Utilisation de **nouvelles technologies sans fil** pour intégrer des fonctionnalités à bord des trains.



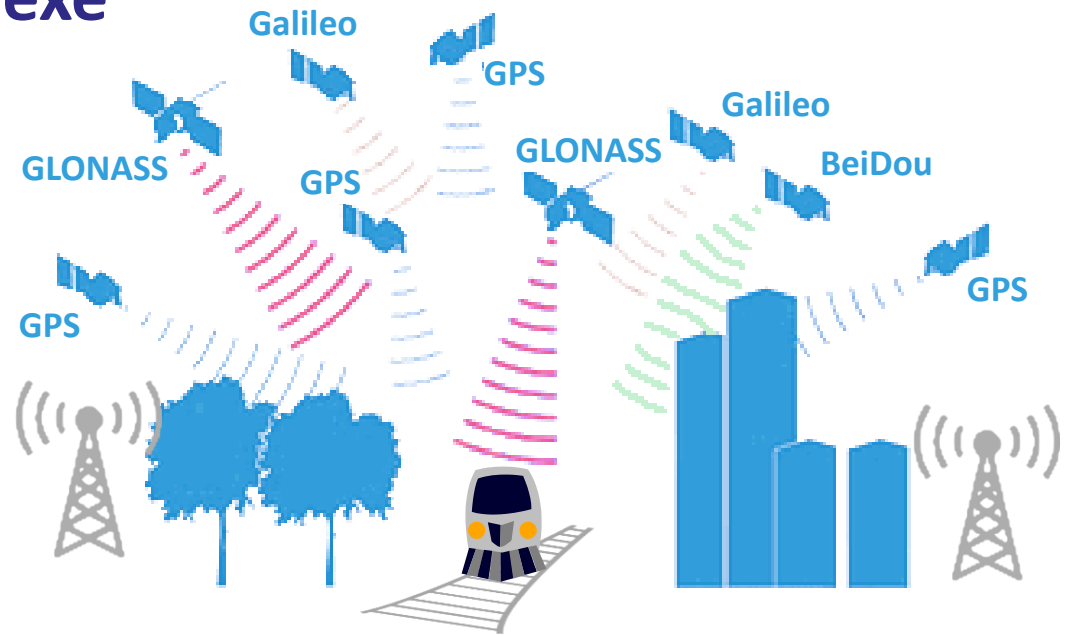
Technologies sans fil : rôle dans la complexité

Nouveaux services numériques dans l'ETCS, nécessaires à la mise en œuvre de nouveaux concepts opérationnels plus performants (ex. cantons mobiles)

Fonctionnement d'ETCS plus complexe

- ↑ fréquence et nombre d'informations
- Accentué par des défauts spécifiques, pas uniquement matériels ou logiciels

➡ Perturbations variables des signaux en milieu ferroviaire



Défi : démontrer la sécurité malgré la complexité

INTERACTIONS

Nombreux éléments de nature variées **interconnectés** et **inter-dépendants**, avec **incertitudes**

COMPORTEMENTS DYNAMIQUES

États de fonctionnement dépendant du **temps**

DIGITALISATION

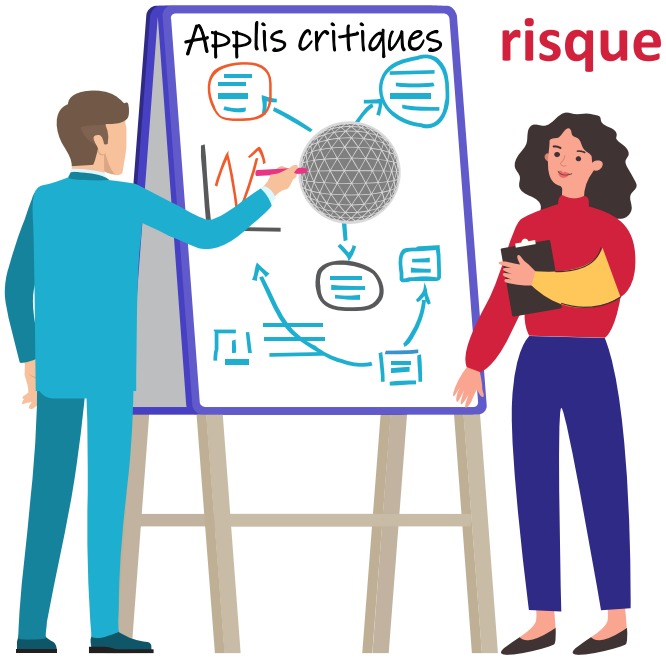
Utilisation de **nouvelles technologies** pour proposer des services numériques et optimiser les performances

ROBUSTESSE

Intégration de **solutions structurelles sophistiquées** pour faire face aux pannes ou aux perturbations internes/externes

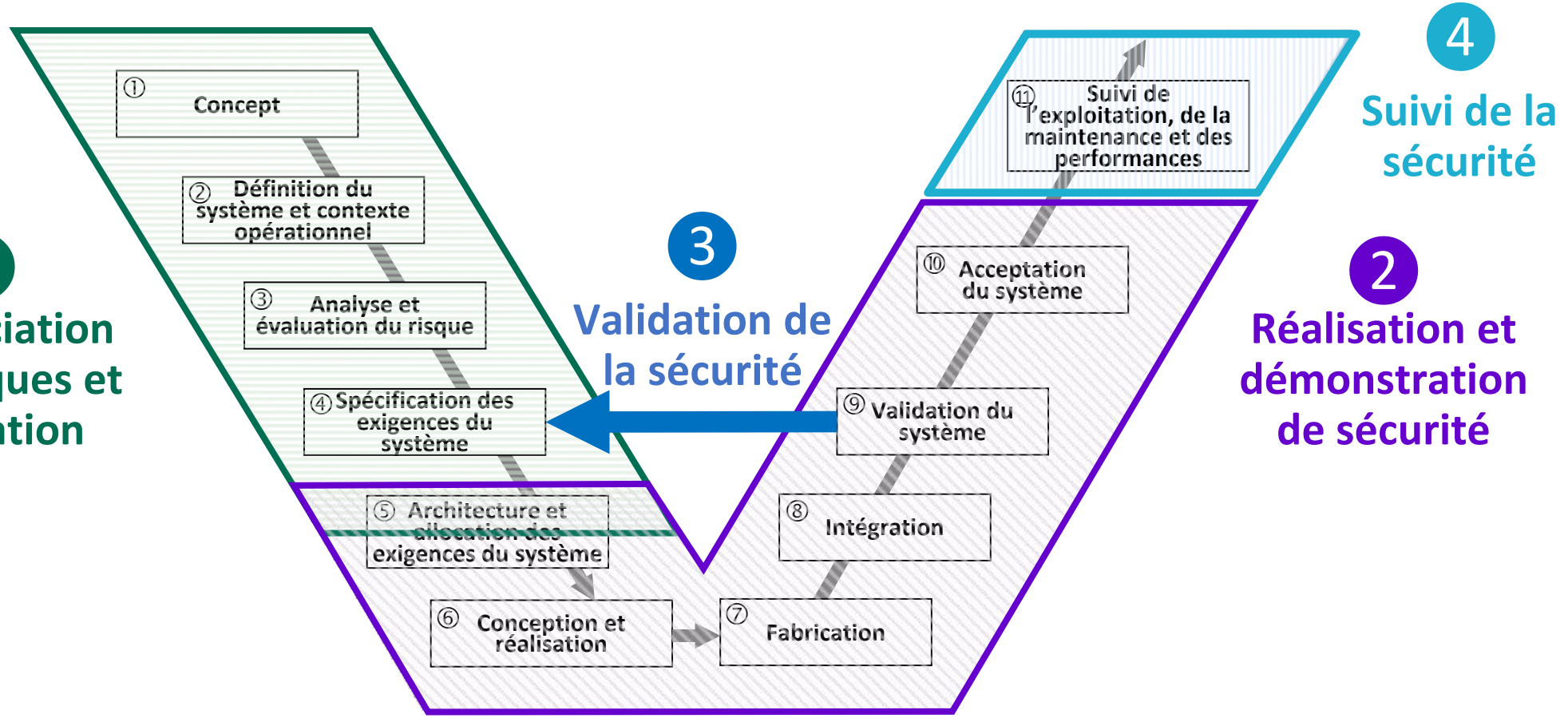
Fonctionnement sûr?

Sans risque?

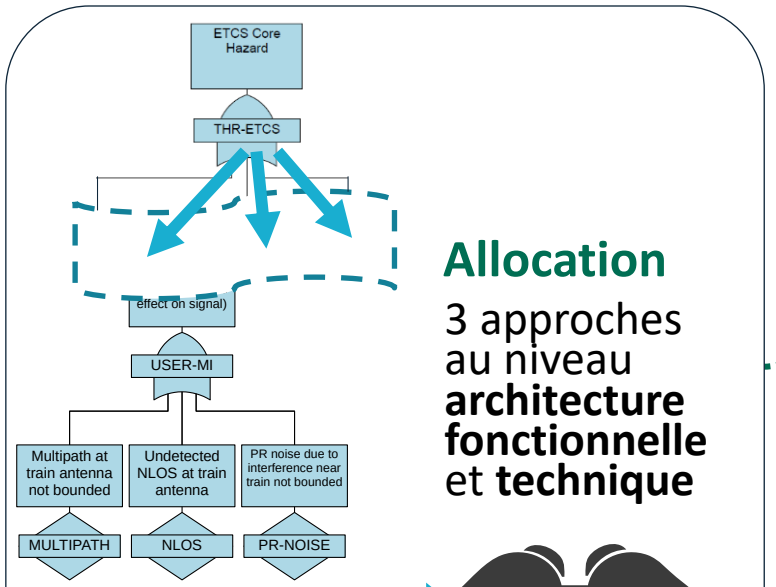


Cadre standard multi-domaines

Activités de sécurité selon 4 macro-phases



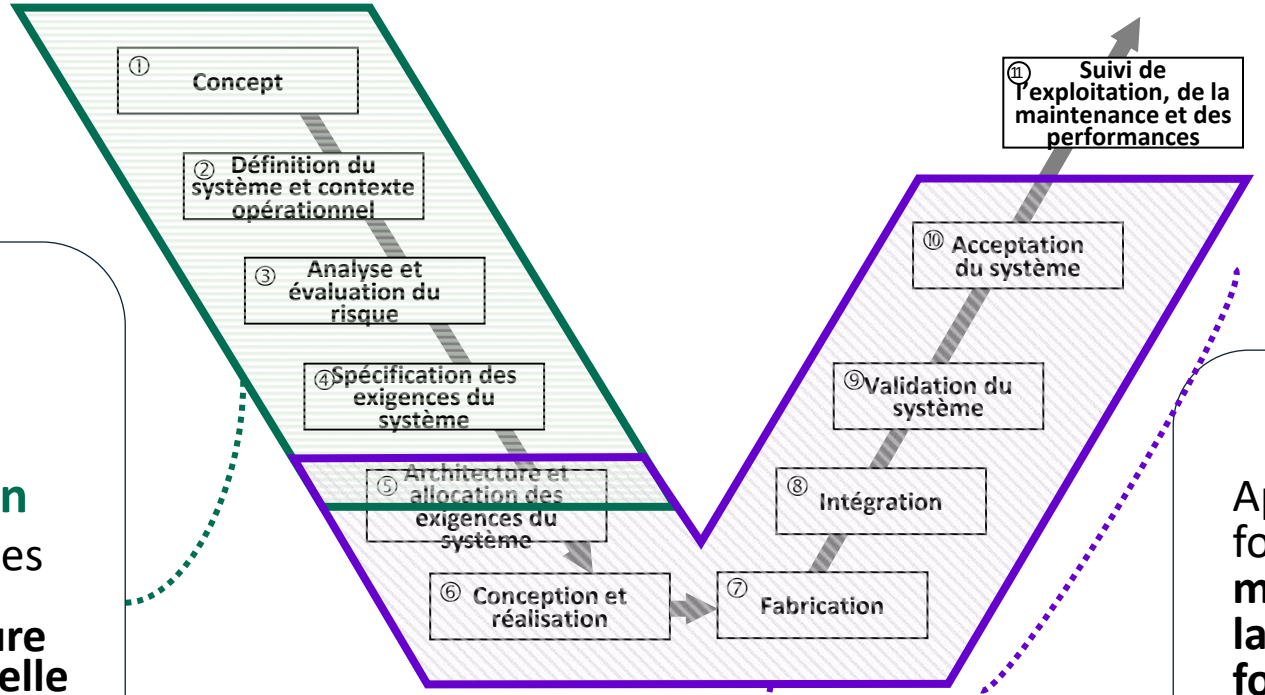
Contributions multi-domaines



Allocation

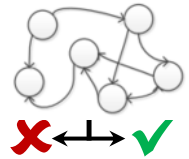
3 approches au niveau **architecture fonctionnelle** et **technique**

imprécisions



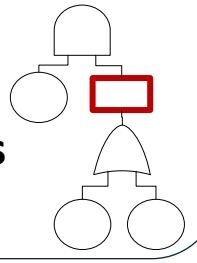
Analyse des risques opérationnels

Approche **générique** fondée sur la **modélisation et la vérification formelle**, puis adaptée au contexte

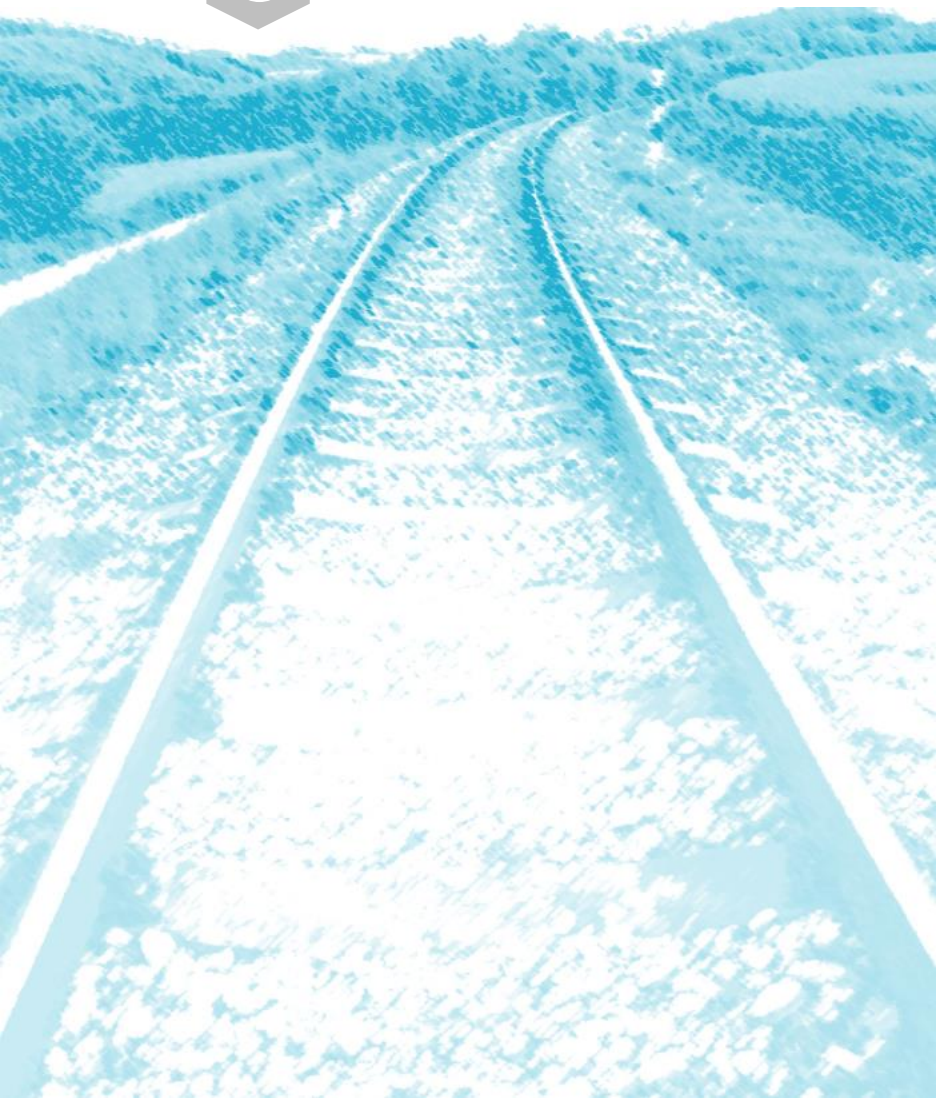


Analyse des risques techniques

- Par arbre de défaillances **étendu**
- Par **évaluations croisées** de critère de sécurité



Allocation d’exigences de sécurité

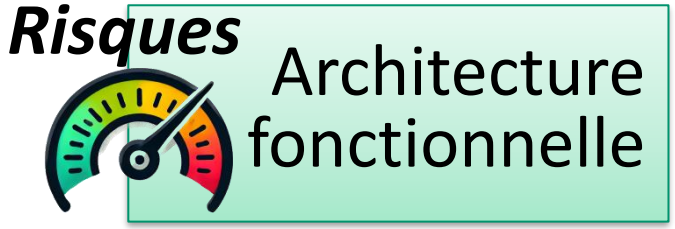


3 contributions d’allocation :

- fonctionnelle
- fonctionnelle, avec imprécision
- technique, avec imprécision

Allocation fonctionnelle : les SIL

➡ *SAFETY INTEGRITY LEVEL*



- **4 niveaux discrets** (SIL1 à SIL4) associés à 4 classes d'exigences de sécurité **qualitatives** et **quantitatives**
- Ils sont alloués **aux fonctions de sécurité** exécutées par des équipements de nature **électronique** ou **numérique**

➡ BESOIN D'UNE MÉTHODOLOGIE STRUCTURÉE ET GÉNÉRIQUE

- Formaliser une **méthodologie d'allocation des SIL**
- Établir un **lien cohérent avec le contexte réglementaire existant**

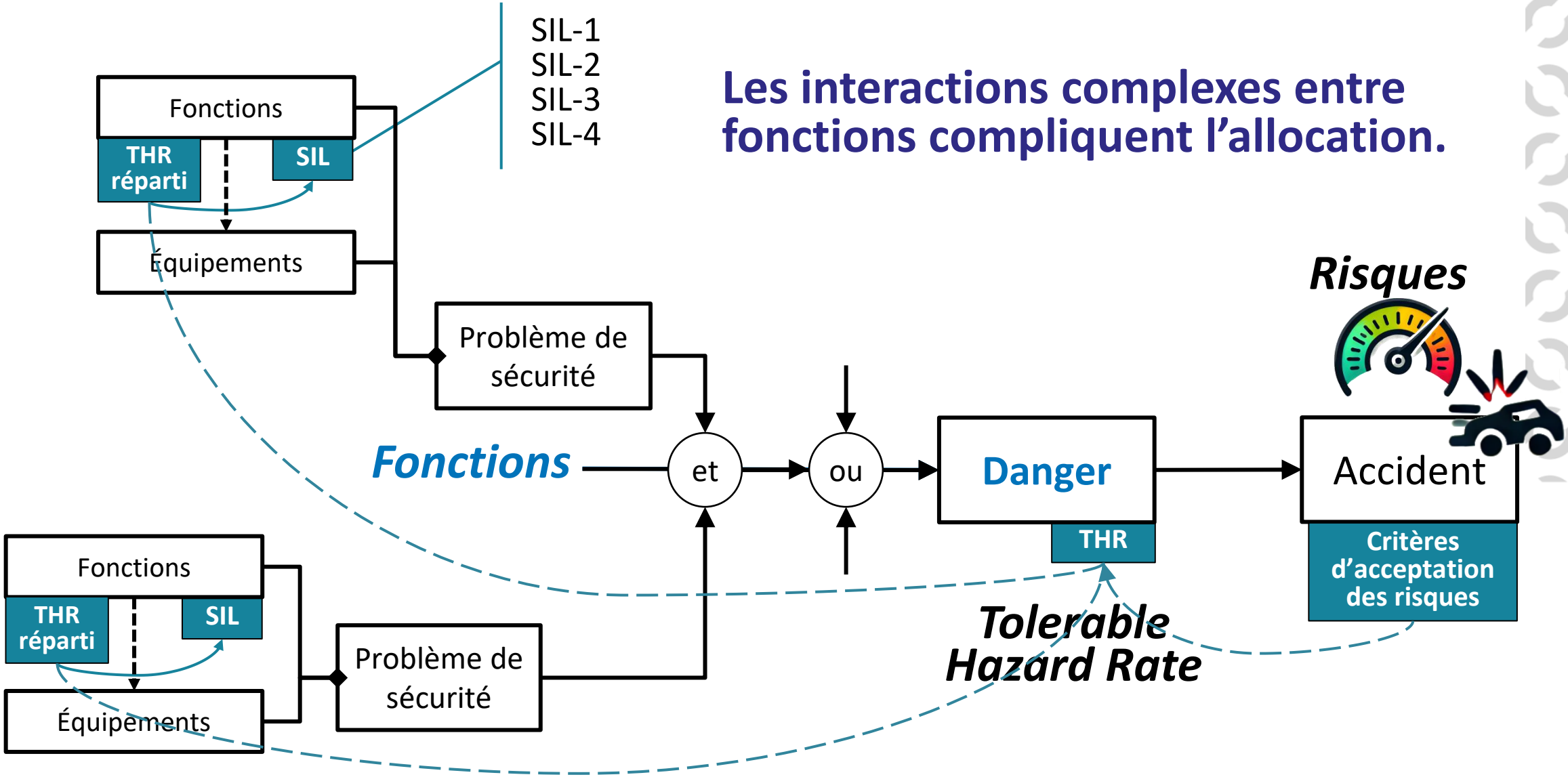
Projet SIL epsf

→ Post-doc A. Ouedraogo
+ coordination

➡ TEXTES RÈGLEMENTAIRES FERROVIAIRES

- Normes européennes (ex. EN 50126)
- Règlements européens (ex. méthodes de sécurité commune)
- Règlements nationaux (ex.: arrêtés liés au RFN)

Articulation Dangers / Fonctions de sécurité



Les interactions complexes entre fonctions compliquent l'allocation.

Méthodologie

Répartition des THR pour obtenir les SIL

1 Règles de répartition des THR

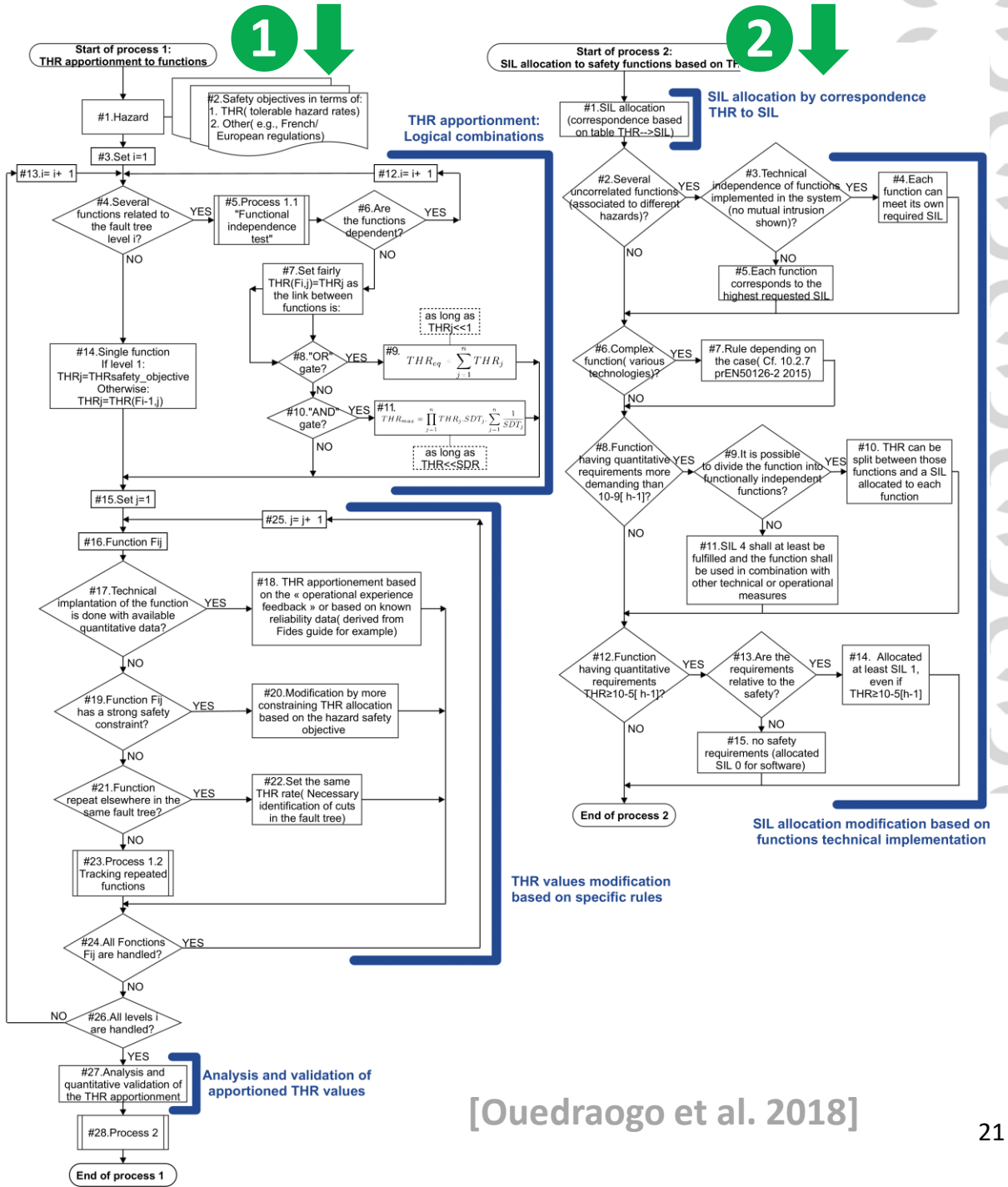
- Combinaisons logiques «ET», «OU»
- Modifications: dépendances, priorités

2 Règles d'allocations des SIL

- Solutions techniques complexes
- Fonction intervenant plusieurs fois
- Réalisation technique des fonctions

Consultations : TÜV, BELGORAIL, ERA, RATP, SNCF, Alstom

Application : X2RAIL 4



[Ouedraogo et al. 2018]

Allocation de THR imprécis

Constat : allouer une **valeur fixe de THR** peut mener à une valeur très contraignante (ex. 10^{-9} /h) quant à la fréquence acceptable d'apparition du danger.

Conséquences : Cela impose des **contraintes fortes de conception** pour l'équipement réalisant la fonction, rendant la conception potentiellement irréalisable.

fonction de localisation avec GNSS

- Les erreurs de position sont **non complètement caractérisées** aujourd'hui en milieu ferroviaire.
- Même s'il y a des fonctions de détections d'erreurs, elles reposent sur des **hypothèses**.

Méthodologie

Objectif : relâcher ces contraintes avec l'utilisation de THR imprécis

➡ plage de fonctionnement pour l'équipement concevoir

Principes :

- Allocation d'**intervalles** de THR pour refléter les incertitudes
- Adaptation des règles de répartition des THR aux intervalles
- Répartition des poids de risques par **propagation d'intervalles** dans un arbre de défaillances

→ Collaboration Railenium / UTC

Combinaison "ET"

$$THR_{max} \approx \prod_{i=1}^{n} THR_i . SDT_i \cdot \sum_{j=1}^{n} \frac{1}{SDT_j}$$

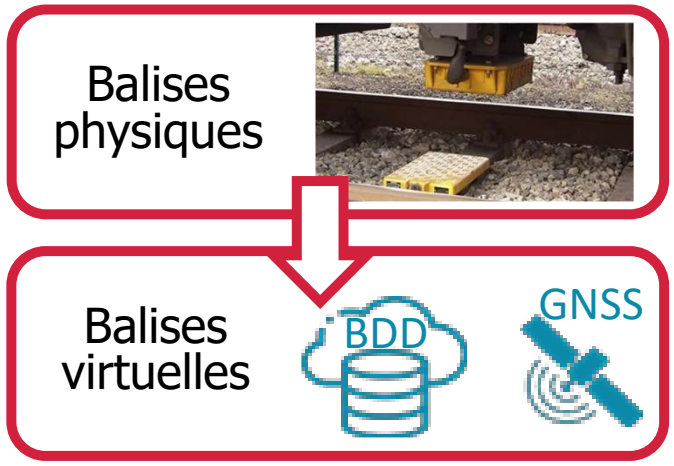
Combinaison "OU"

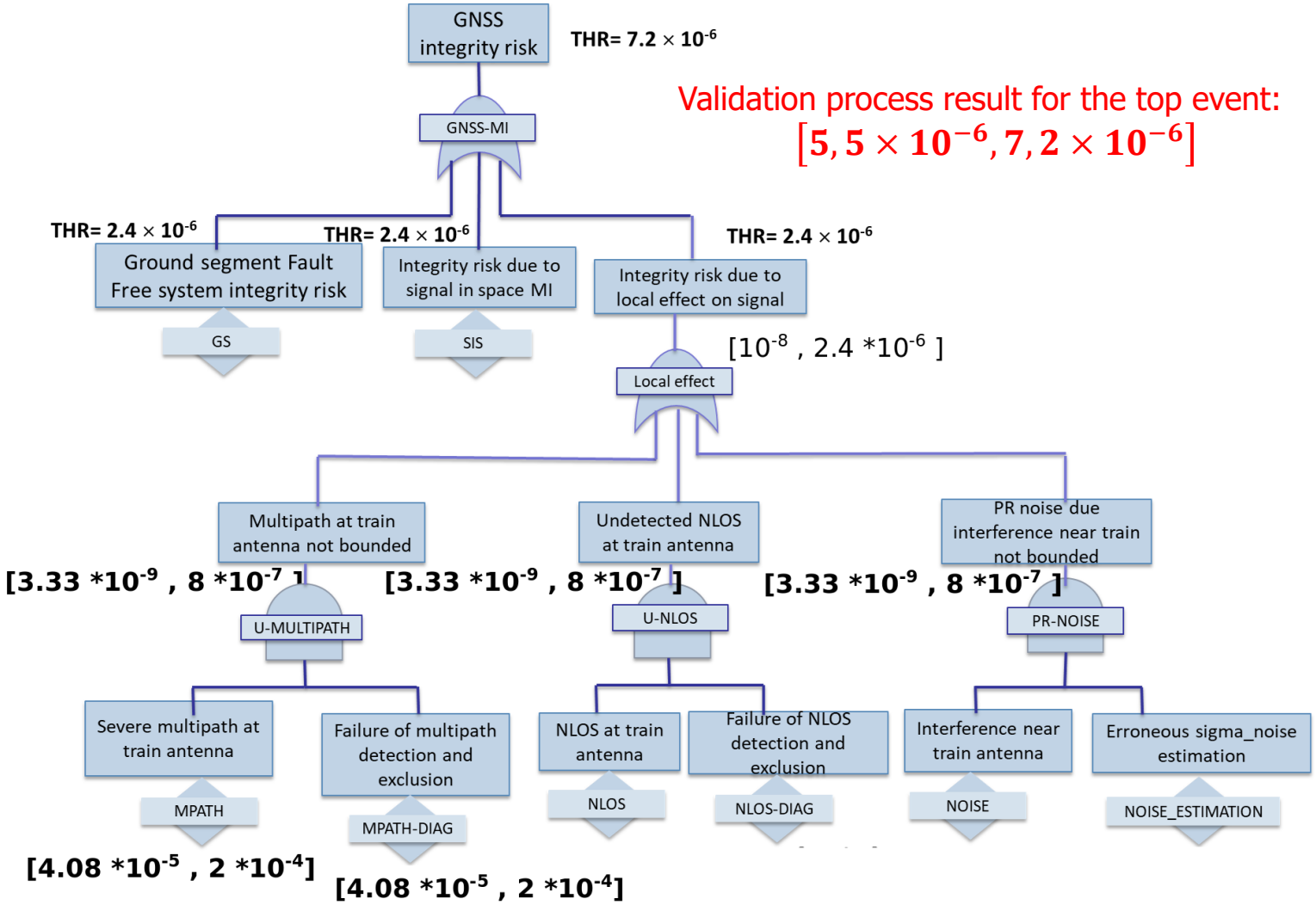
$$THR_{eq} = \sum_{i=1}^{n} THR_i$$

Application

➡ Système de localisation utilisant des balises virtuelles

Réduction d'erreur de l'odométrie embarquée





Validation process result for the top event:
$[5,5 \times 10^{-6}, 7,2 \times 10^{-6}]$

[Sassi et al. 2020]

Allocation technique

→ Post-doc K. Nguyen

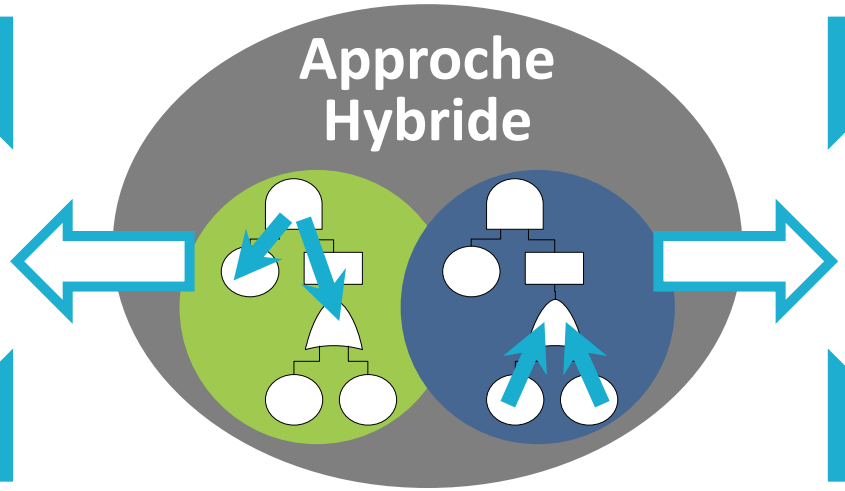
Valorisé au niveau régional

Objectif : allouer un objectif quantitatif à un **équipement spécifique** intervenant dans un système complexe

Application : **Unité de localisation autonome** utilisant les GNSS, celle-ci intervenant au sein de l'ETCS-bord

➡ **Approche d'allocation tenant compte d'incertitudes**

- Décomposer un objectif global jusqu'à un niveau suffisant
- Plusieurs angles de vue globaux



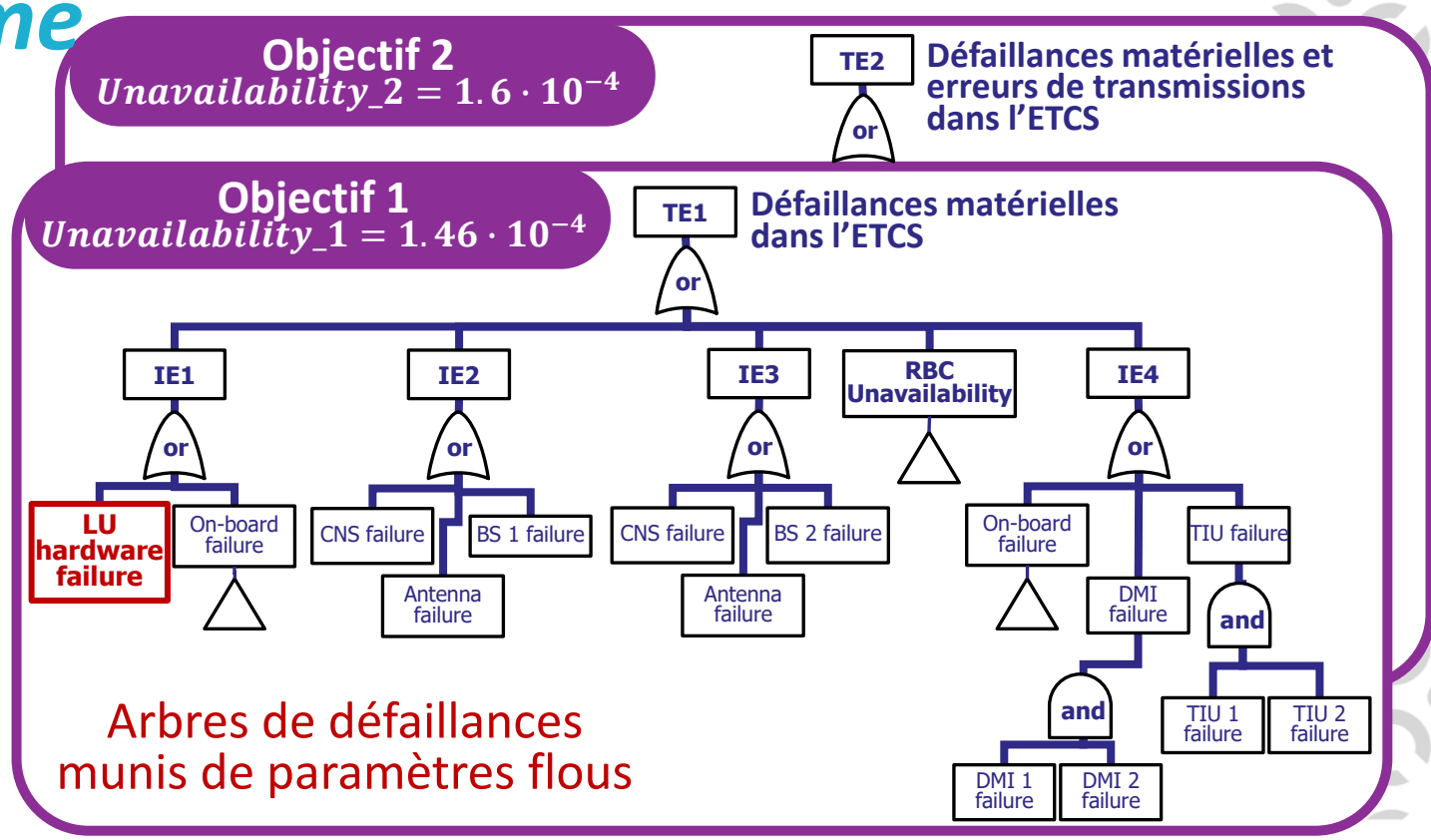
- Utiliser les paramètres de défaillances connus pour certains composants
- Utiliser des valeurs imprécises(infos limitées)

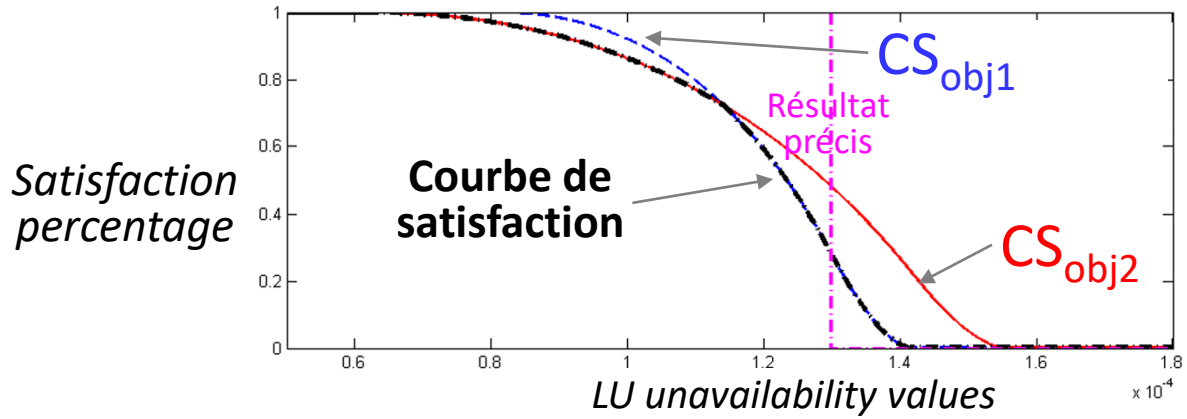
Cas d'étude : *LU autonome*

1. Identification des **objectifs au niveau système**

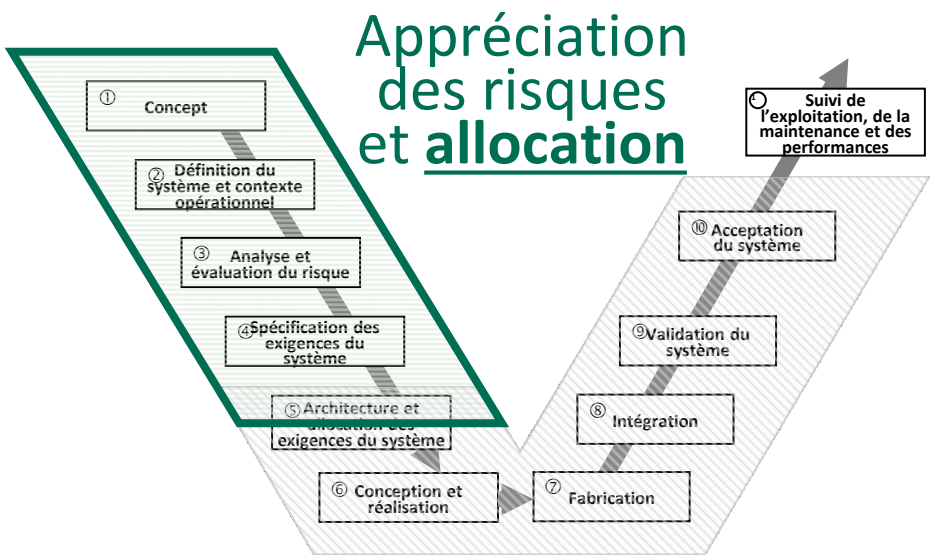
2. Analyse des **causes de défaillance** et **identification de leurs paramètres imprécis**, à l'exception de l'équipement spécifique étudié

3. Détermination de l'**objectif cible** de l'équipement étudié à partir d'une **courbe de satisfaction**





Conclusion partie 2

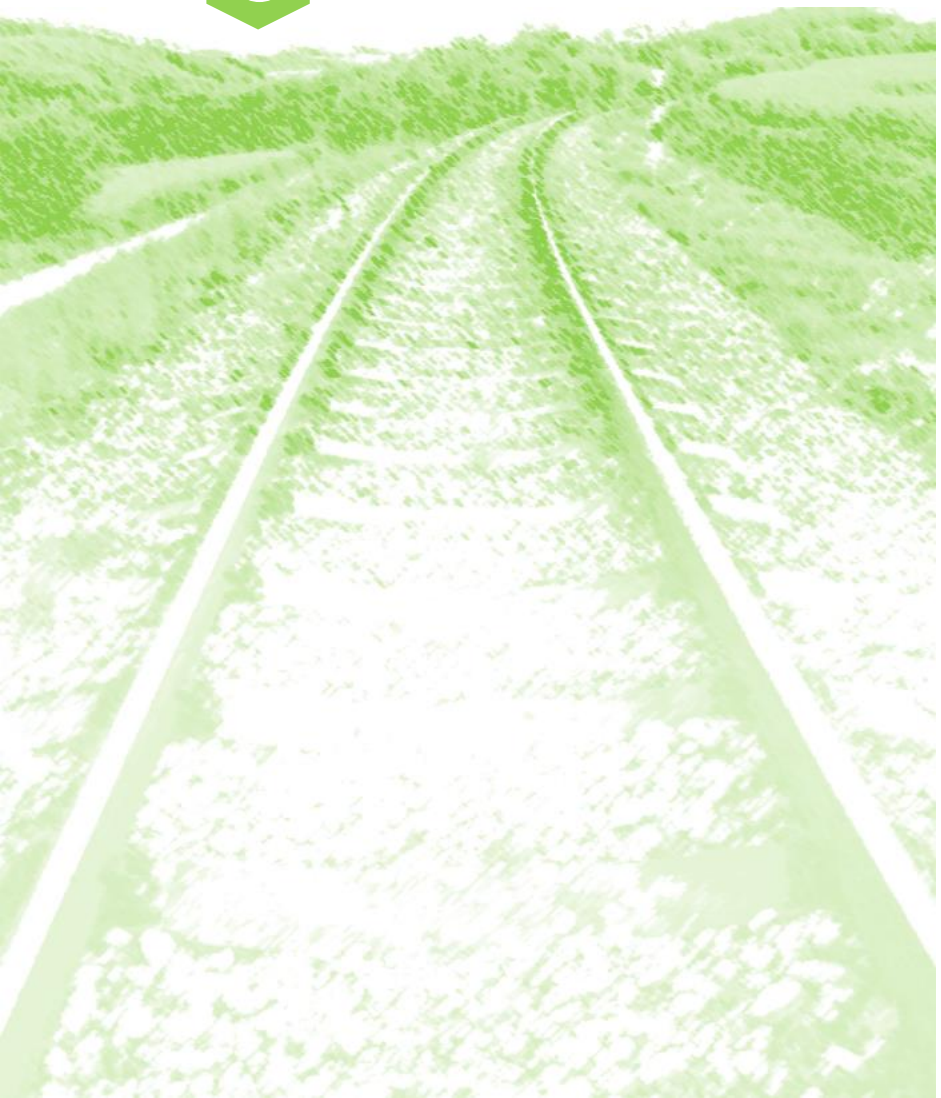


CONTRIBUTIONS

Multi-domaines	CCS ferroviaires avancés
✓ Analyser différentes techniques **d'allocation de niveaux d'intégrité**	✓ **Approches d'allocation** fonctionnelle et au niveau composants
✓ Pour formaliser une **méthodologie** générique ferroviaire	✓ Adaptées aux systèmes de **localisation avec GNSS**

En cohérence avec le cadre de sécurité ferroviaire réglementaire

Analyse des risques techniques

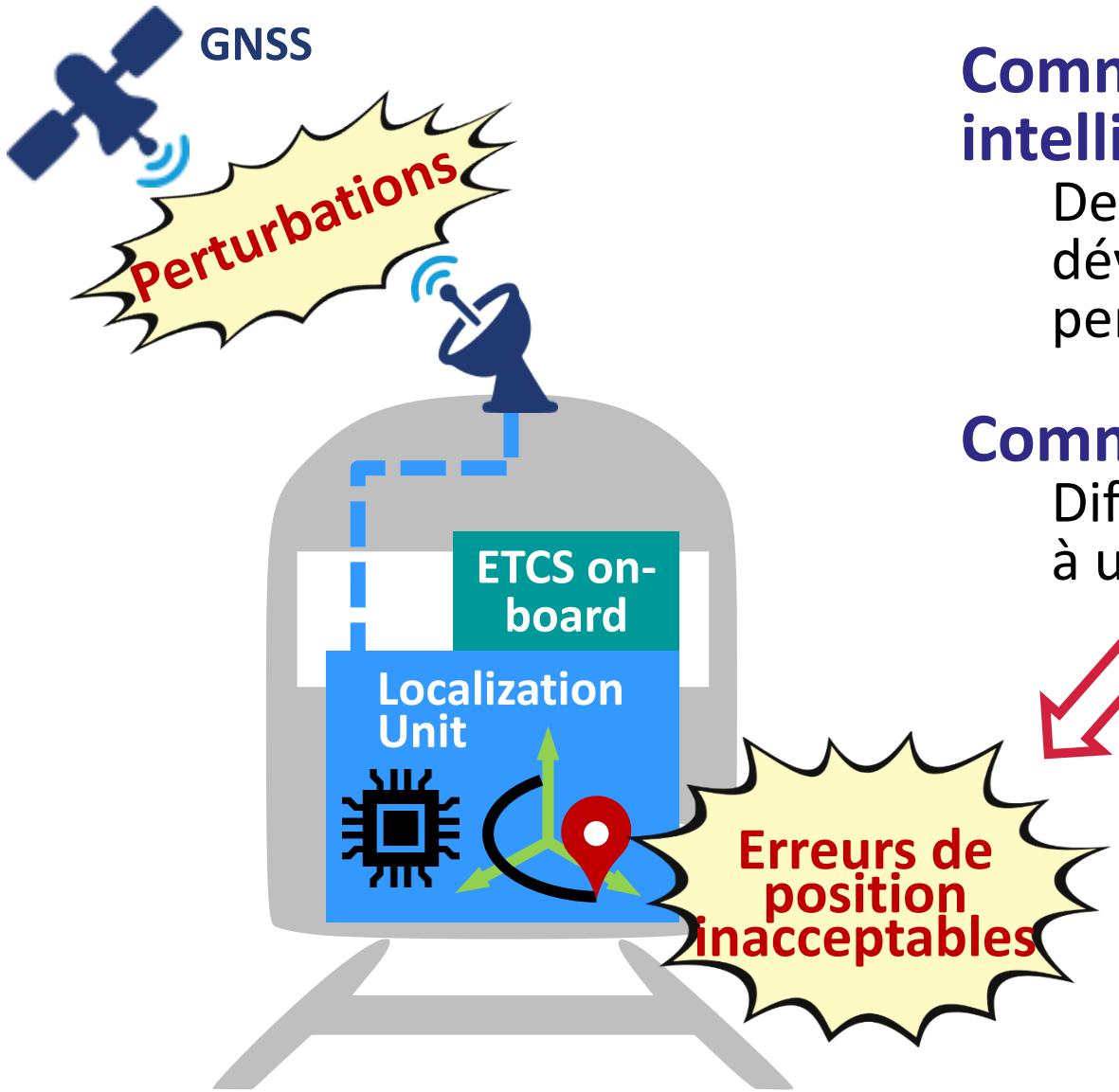


2 approches :

- Arbres de défaillances (AdD) étendus
- Évaluations croisées inter-domaines

➡ Application à des équipements embarqués utilisant les GNSS

Précisions des besoins en termes d'analyse de sécurité



Communautés des GNSS et des transports intelligents :

De **multiples solutions** de localisation développées pour atténuer les impacts des perturbations touchant les signaux GNSS

Communauté de la sécurité des systèmes :

Difficulté pour évaluer les risques associés à une solution

Besoins

(aussi dans d'autres secteurs)

- D'analyser l'évolution dynamique des défaillances d'un système
- De caractériser les défaillances d'un système aux défauts non-observables

Approche par AdD étendu : analyse

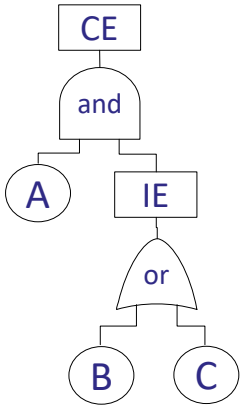
GaLoROI smart railway localisation

→ Post-doc K. Nguyen

➡ **AdD étendu =** modèle qui utilise différentes extensions d'AdD pour représenter graphiquement l'enchaînement de **pannes interdépendantes** et **dépendant du temps**

AdD Classique

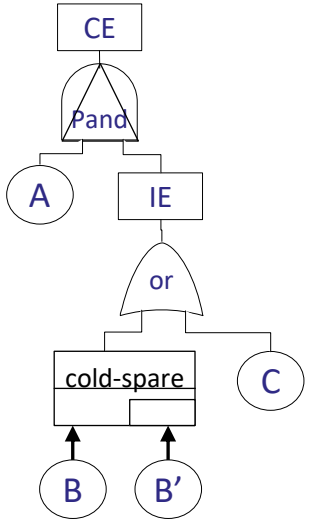
- **États booléens** (fonctionnement ou panne)
- **Évènements indépendants**



Extensions d'AdD combinées

Multi-états
- Composants multi-états
- Dépendance des défaillances
- Composant réparable

Dynamique
- Séquence de défaillances
- Dépendances fonctionnelles entre défaillances (CCF)



Temporel

Ordre chronologique des événements défaillants

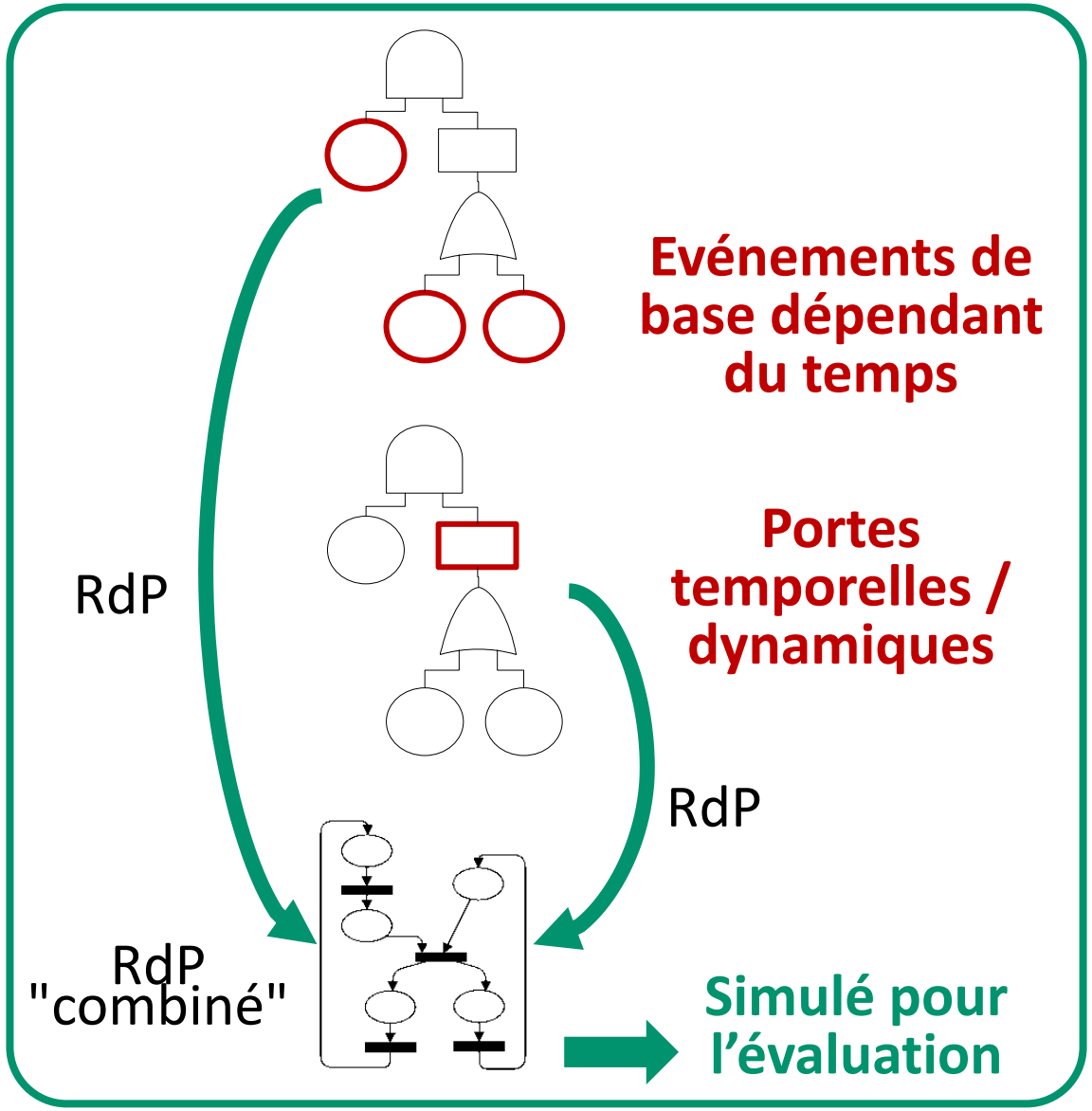
À dépendances temporelles

Délai entre les entrées et la sortie d'une porte causale

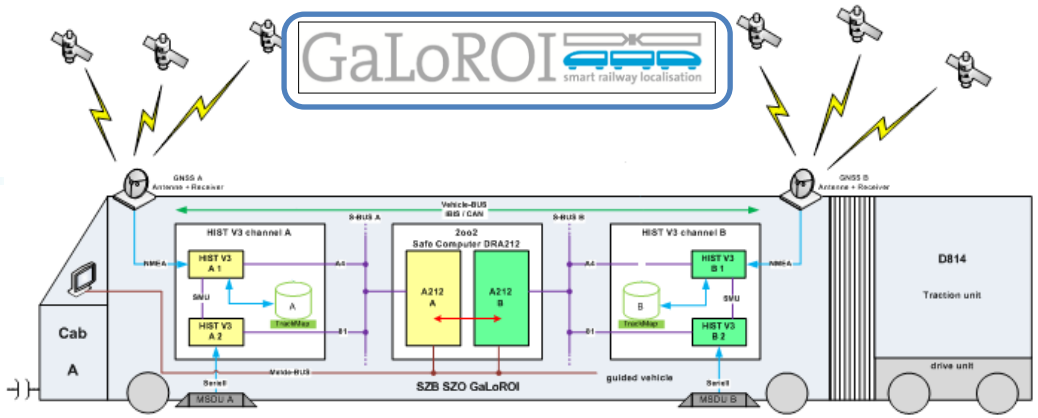
Approche par AdD étendu : évaluation

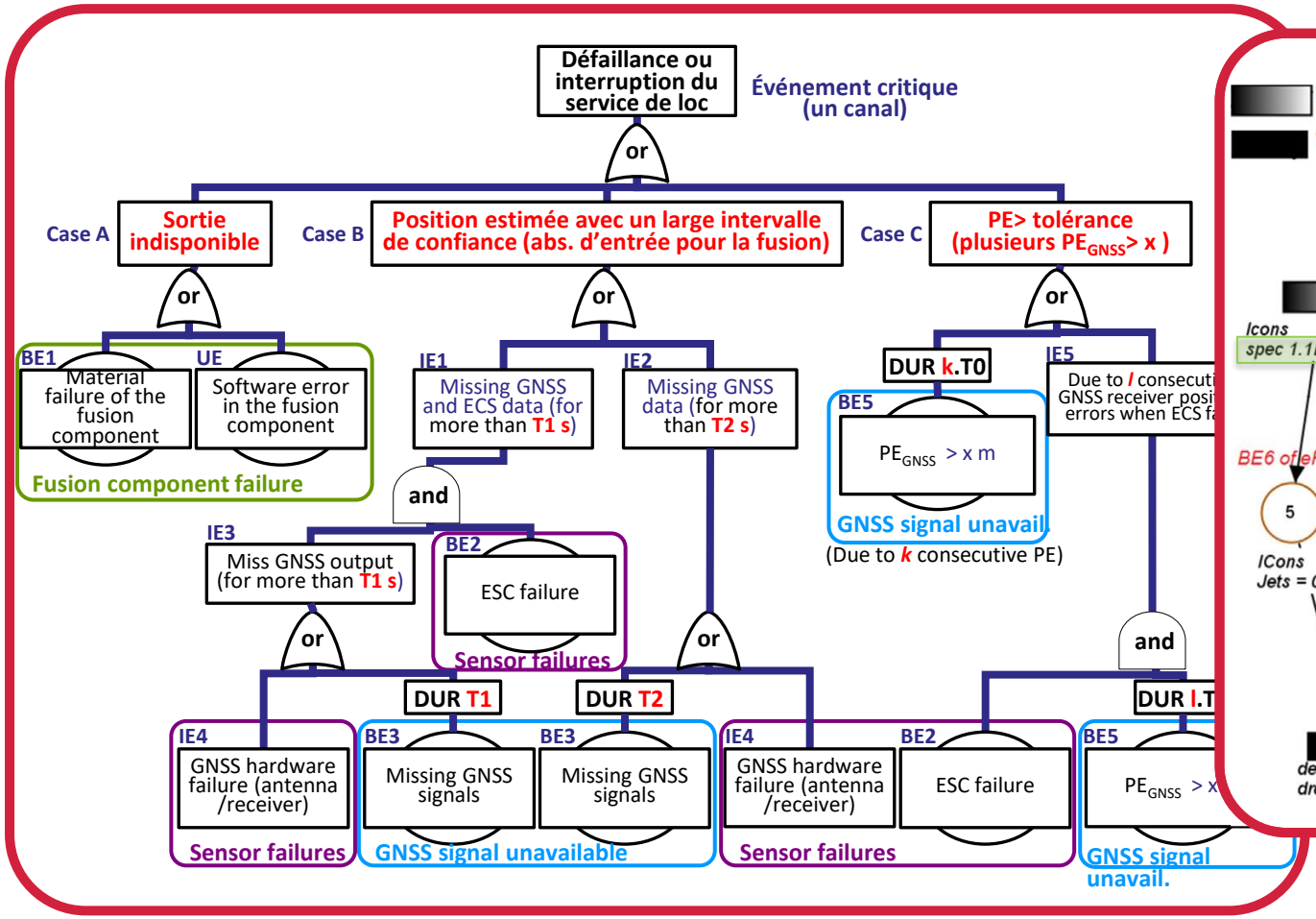
Pour évaluer un modèle d'AdD étendu, certaines parties peuvent être transformées à l'aide de :

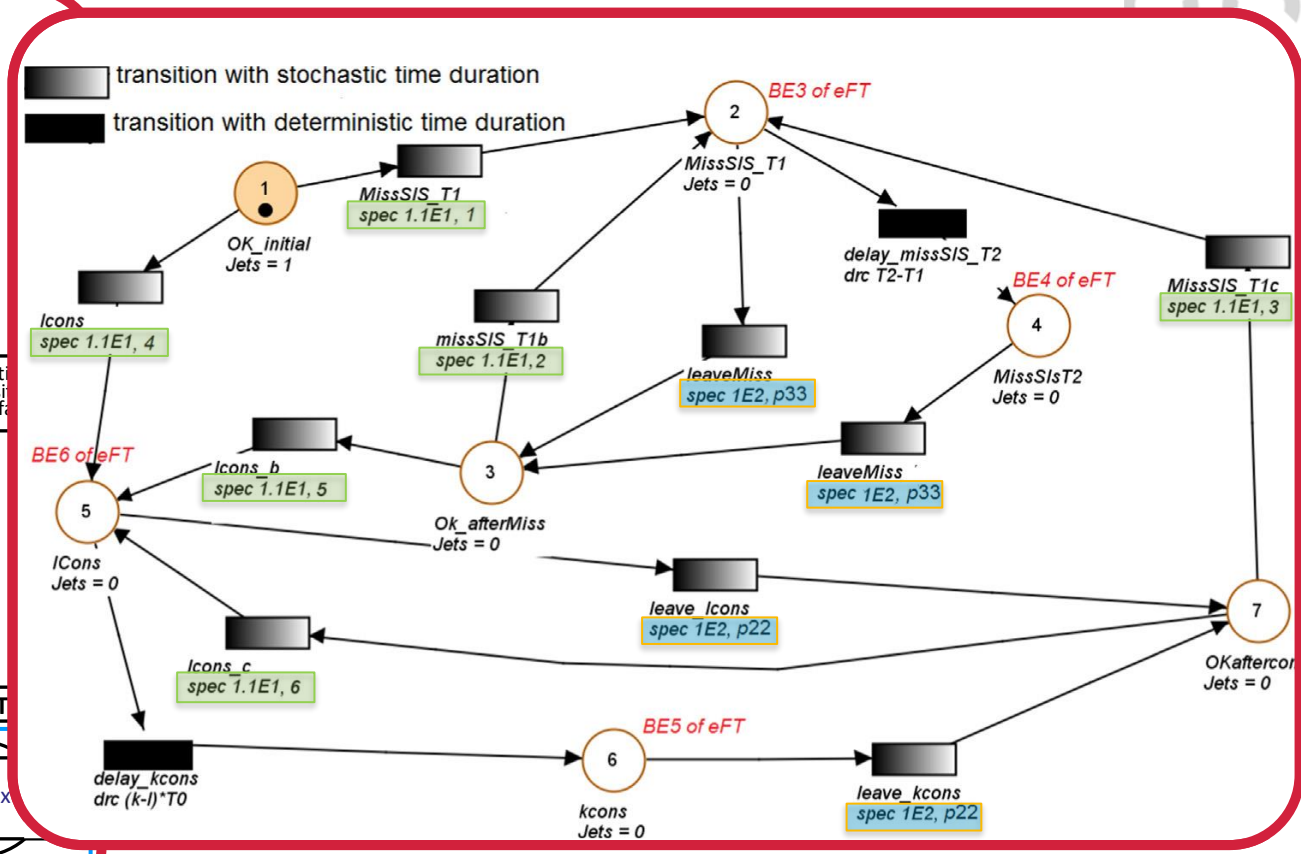
Réseaux de Petri (RdP) déterministes et stochastiques



Cas d'étude

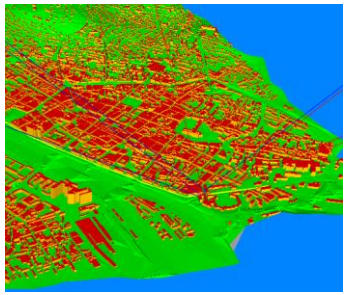

GaLoROI
smart railway localisation
Cab
A
HIST V3 channel A
HIST V3 channel B
2oo2
Safe Computer DRA212
A212
A
A212
B
D814
Traction unit
drive unit
guided vehicle
SZB SZO GaLoROI

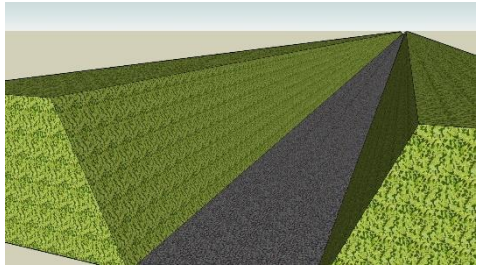

Défaillance ou interruption du service de loc
Événement critique (un canal)
or
Case A
Sortie indisponible
Case B
Position estimée avec un large intervalle de confiance (abs. d'entrée pour la fusion)
Case C
PE> tolérance (plusieurs PE$_{GNSS}$> x)
BE1
Material failure of the fusion component
UE
Software error in the fusion component
Fusion component failure
IE1
Missing GNSS and ECS data (for more than T1 s)
IE2
Missing GNSS data (for more than T2 s)
and
IE3
Miss GNSS output (for more than T1 s)
BE2
ESC failure
Sensor failures
DUR k.T0
BE5
PE$_{GNSS}$ > x m
GNSS signal unavail
(Due to k consecutive PE)
IE5
Due to l consecuti GNSS receiver posi errors when ECS f
DUR T1
DUR T2
DUR l.T
IE4
GNSS hardware failure (antenna /receiver)
BE3
Missing GNSS signals
Missing GNSS signals
Sensor failures
GNSS signal unavailable
IE4
GNSS hardware failure (antenna /receiver)
BE2
ESC failure
Sensor failures
BE5
PE$_{GNSS}$ > x
GNSS signal unavail.

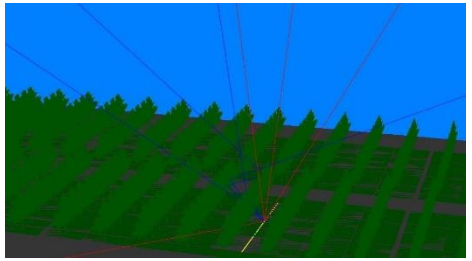

transition with stochastic time duration
transition with deterministic time duration
1
OK_initial
Jets = 1
2
BE3 of eFT
MissSIS_T1
Jets = 0
MissSIS_T1
spec 1.1E1, 1
delay_missSIS_T2
drc T2-T1
BE4 of eFT
MissSIS_T1c
spec 1.1E1, 3
Icons
spec 1.1E1, 4
missSIS_T1b
spec 1.1E1,2
leaveMiss
spec 1E2, p33
4
MissSIsT2
Jets = 0
BE6 of eFT
Icons_b
spec 1.1E1, 5
3
Ok_afterMiss
Jets = 0
leaveMiss
spec 1E2, p33
5
ICons
Jets = 0
leave_Icons
spec 1E2, p22
7
OKaftercor
Jets = 0
Icons_c
spec 1.1E1, 6
BE5 of eFT
delay_kcons
drc (k-l)*T0
6
kcons
Jets = 0
leave_kcons
spec 1E2, p22

Quelques résultats

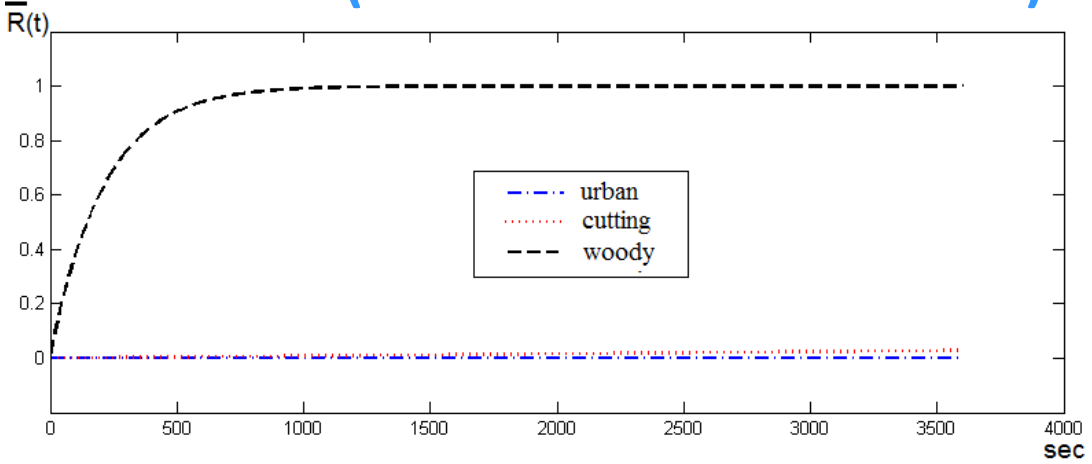
Environnements



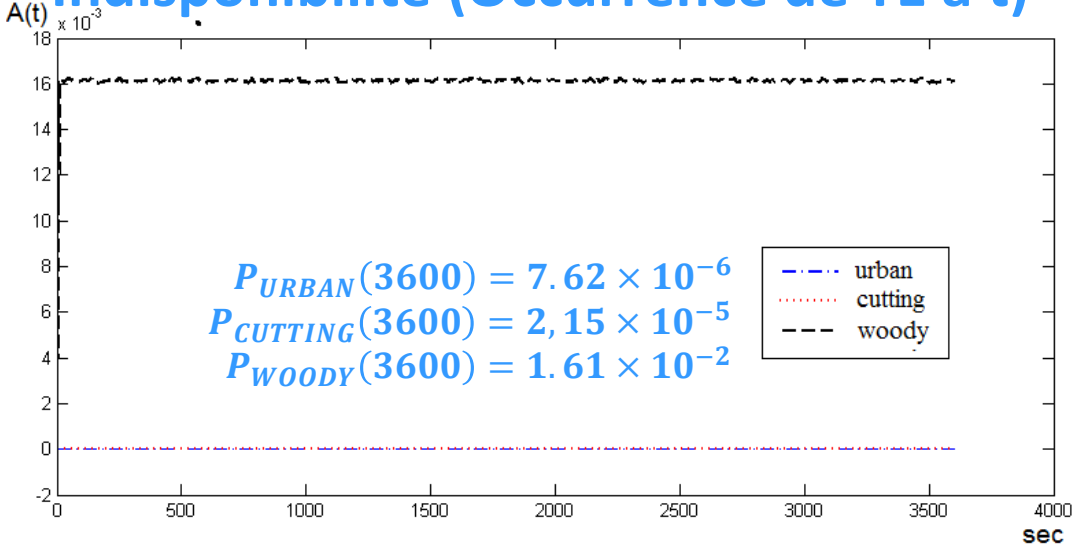




Défiabilité (Occurrence de TE avant t)



Indisponibilité (Occurrence de TE à t)

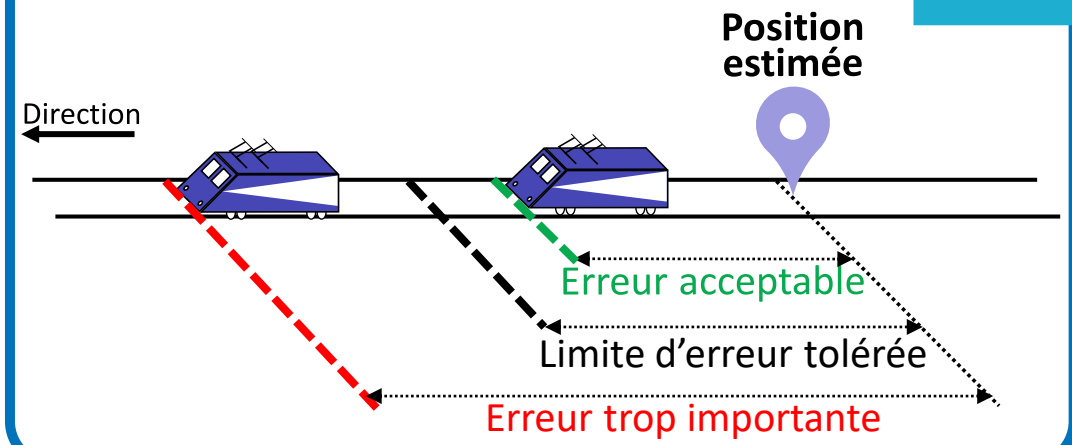


➡ Les résultats d'évaluations permettent d'orienter la conception du système

[Nguyen et al. 2015]

Évaluations croisées inter-domaines

États de localisation



Erreurs trop importantes non-observables mais détectables

Comment ?

Surveillance de l'intégrité de la localisation

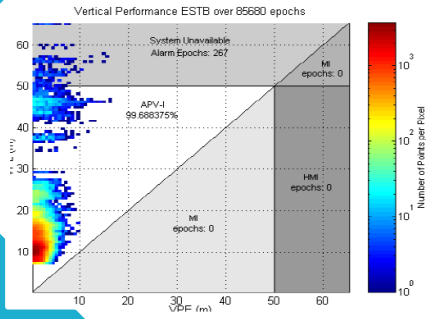
Risques ?

Domaine ferroviaire

➡ Vérification de l'**intégrité de la sécurité** suite à l'allocation d'un **SIL**

Liens

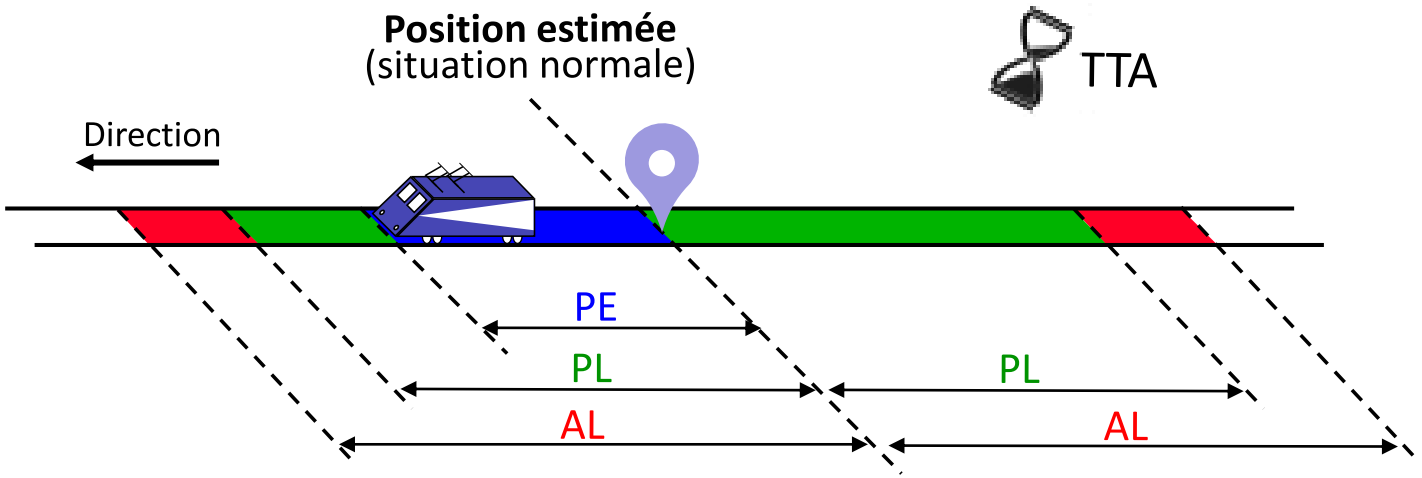
Domaine aéronautique



➡ Évaluation de **l'intégrité de la localisation**

Paramètres des mécanismes de détection

→ Thèse C. Legrand
RAILENIUM
RAIL RESEARCH & INNOVATION



PE: erreur de position (inconnue)

PL: niveau de protection (estimé)

AL: limite d'alerte

TTA: temps d'alerte

Critères associés

Système multi-capteurs avec GNSS

Risque sur l'intégrité
- moyen
- à chaque instant

Situations dangereuses

Non-détection à tort

Pas d'alerte
ET
PL ne borne pas correctement **PE**

Pendant TTA

Relations entre critères

Risque sur l'intégrité de la localisation

Instantané

$$IR_{extend}(t_i) = \prod_{j=i}^{i+int(TTA/T_e)} P(A_{t_j})$$

Moyen

$$IR_{extend\_avg} \approx \frac{\#(A_{t_i},\ldots,A_{i+int(TTA/T_e)}) \text{ is observed on } T_m}{int(T_m/T_e)}$$

Intégrité de sécurité

P_{wsf} (proba. of wrong side failure)

$$P_{wsf}(t_i) = (IR_{extended}(t_i))^{\frac{1}{int(TTA/T_e)}}$$

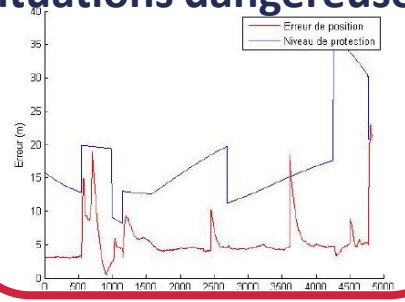
$$P_{wsf\_avg} \approx \frac{\#\text{ of time } A_{t_i} \text{ is observed}}{int(T_m/T_e)}$$

PFH *(freq.of dangerous failure per hour)*

$$PFH = \frac{3600.IR_{extend\_avg}}{T_m}$$

Données

Occurrences des situations dangereuses



Évaluations croisées

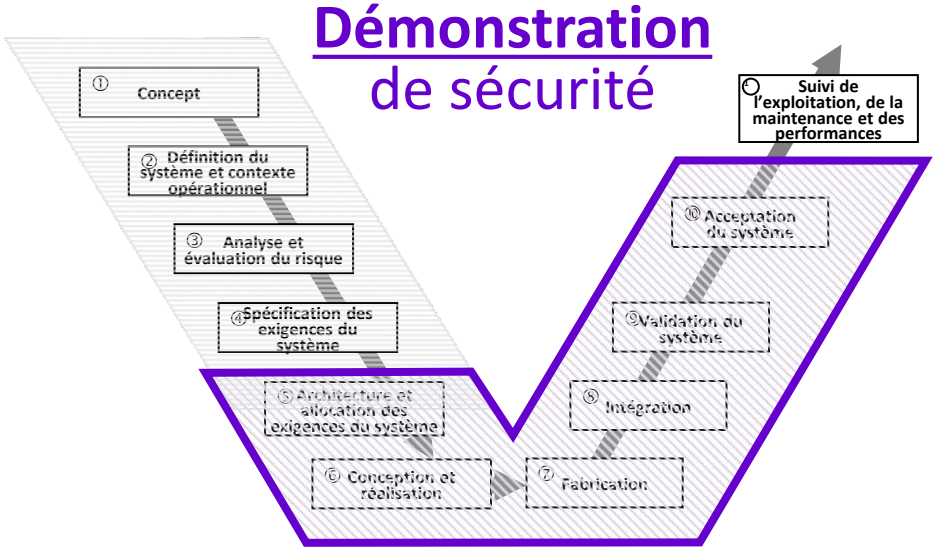
- *$IR(t)$, IR_{avg}*
- *$P_{wsf}(t)$, P_{wsf_avg}*
- *PFH*

	1st data set	2nd data set	Both data sets considered
IR_avg	7.04 E-2	5.65 E-2	6.35 E-2
PFH	3.58 E-2	2.74 E-2	3.16 E-2

[Beugin et al. 2018] [Legrand et al. 2016]

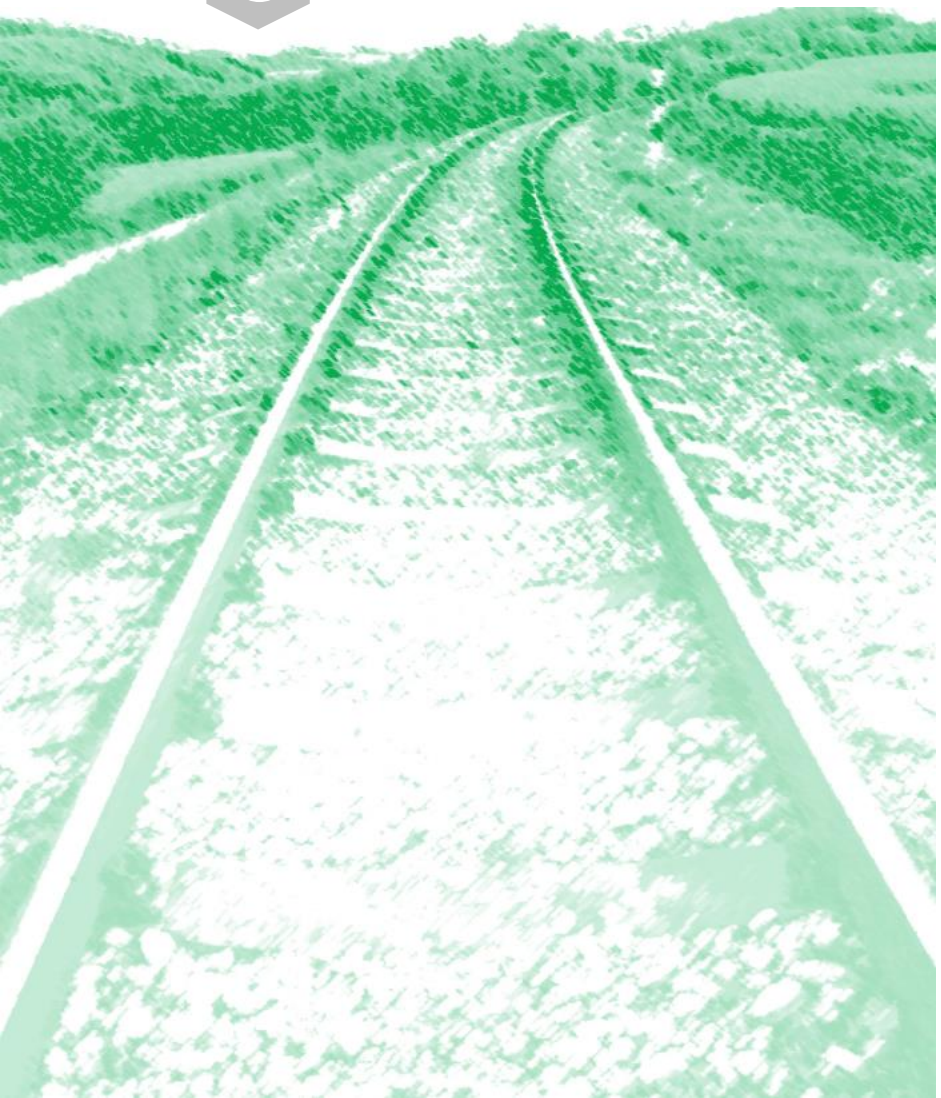
Conclusion partie 3

Contexte technique



CONTRIBUTIONS	
Multi-domaines	**CCS ferroviaires avancés**
✓ Approche d'évaluation pour des systèmes techniques au **comportement complexes**	✓ **Évaluations croisées** entre les domaines **aéronautiques** et **ferroviaires** pour la sécurité de la localisation

Analyse des risques opérationnels



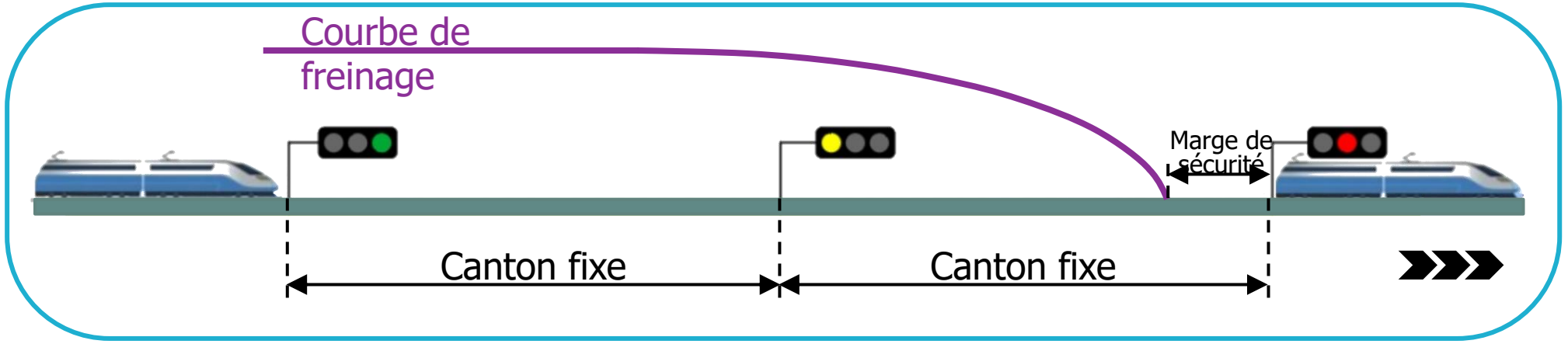
Approche d'analyse formelle

- Principes génériques
- Adaptation aux conditions opérationnelles

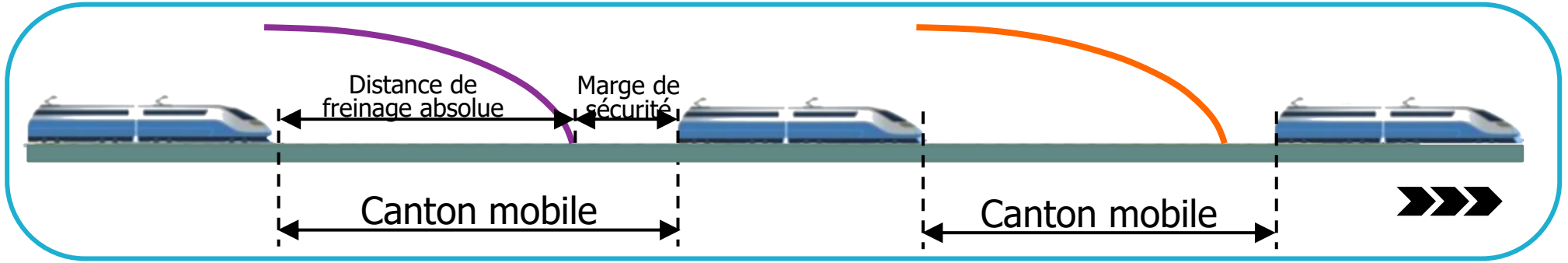
➡ Application à l'ETCS niveau 3

ETCS niveau 3 : vers des cantons logiques

Cantons fixes : découpage géographique, équipements physiques associés



Cantons mobiles / cantons fixes virtuels : découpage logique des lignes



Configurations hybrides : pour la phase de migration

Approche d'analyse formelle

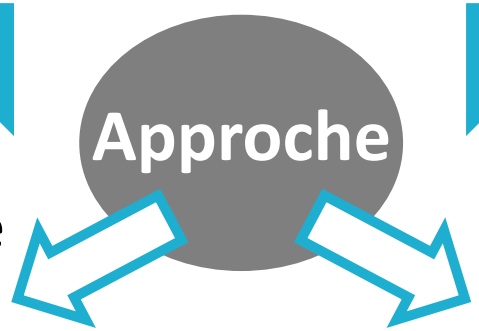
PERFORMINGRAIL

→ Post-doc R. Saddem

Objectif : Analyser la sécurité en tenant compte des **interactions**, des **dépendances**, et des **comportements dynamiques** au sein d'un système complexe aux **configurations multiples**

Modélisation formelle

- Représenter sans ambiguïté ce qui est attendu du système
- S'appuyer sur des notations compatibles avec des traitements automatiques



Vérification formelle

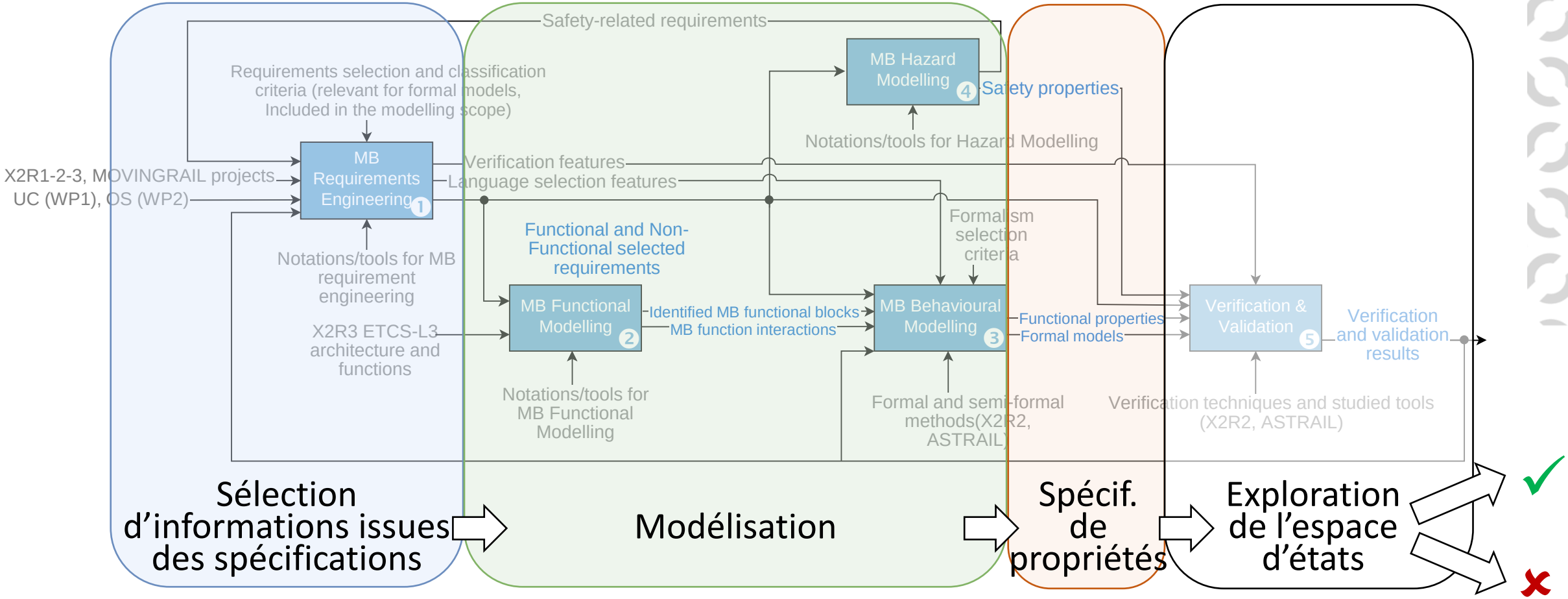
- Vérifier le respect de propriétés par exploration automatique de l'espace d'état
- Identifier des séquences dangereuses d'événements

Méthodologie pour gérer la complexité

[Saddem et al. 2022]

Méthodologie générique

→ Avec 5 étapes pour obtenir des modèles formels paramétrables / modulaires / réutilisables / et adaptés aux techniques de vérification

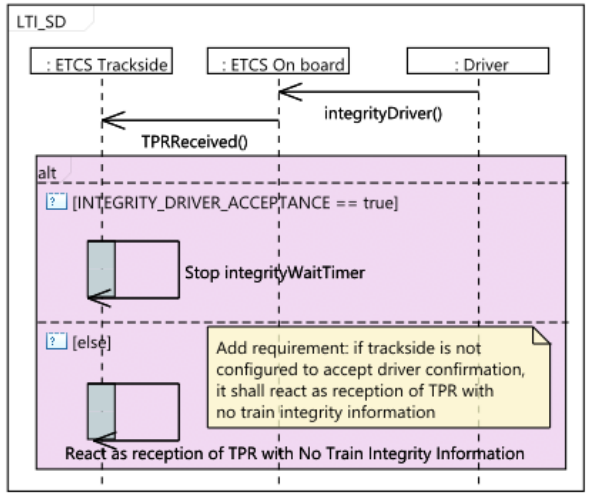


Application à l'ETCS niv.3

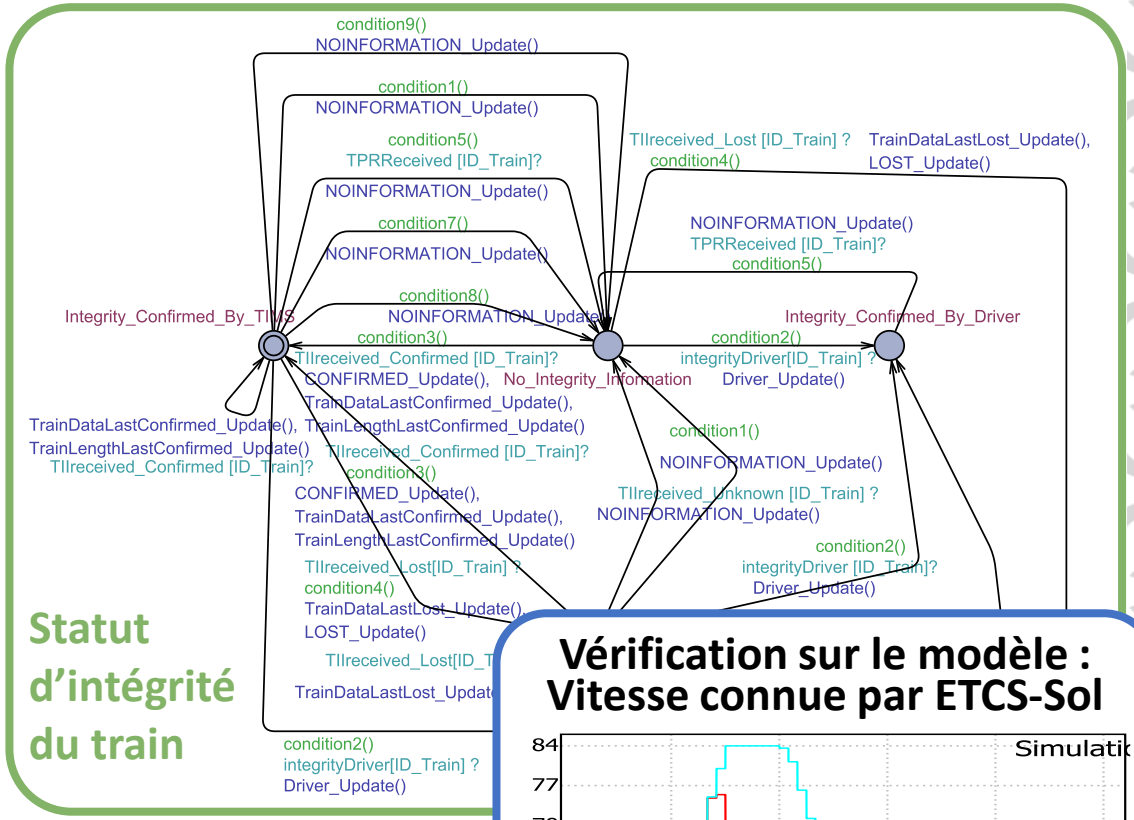
Étape 1 - Exigences sélectionnées

	id : String [1]	/satisfiedBy : NamedElement [*]	text : String [1]
LossTI-1	REQ-LossTI-1	LTI_TIMS_Integrity_SD	When receiving a position report from a train with the information 'Train integrity lost', the L3 Trackside shall change the Track Status Area associated with this train to Unknown.
LossTI-2	REQ-LossTI-2	LTI_TIMS_Integrity_SD	When the L3 Trackside considers that the integrity is lost for a train, the L3 Trackside shall change the Track Status Area associated with this train to Unknown.
LossTI-3	REQ-LossTI-3	LTI_TIMS_Integrity_SD	When the L3 Trackside considers that the Train Integrity is lost for a train, the L3 Trackside shall react as configured.
LossTI-4	REQ-LossTI-4	LTI_TIMS_Integrity_SD	The L3 Trackside shall consider the Train Integrity as lost when 'No train integrity information' is reported longer than a configurable time

Étape 2 - Interactions de haut niveau



Étape 3 - Modèle formel paramétrable



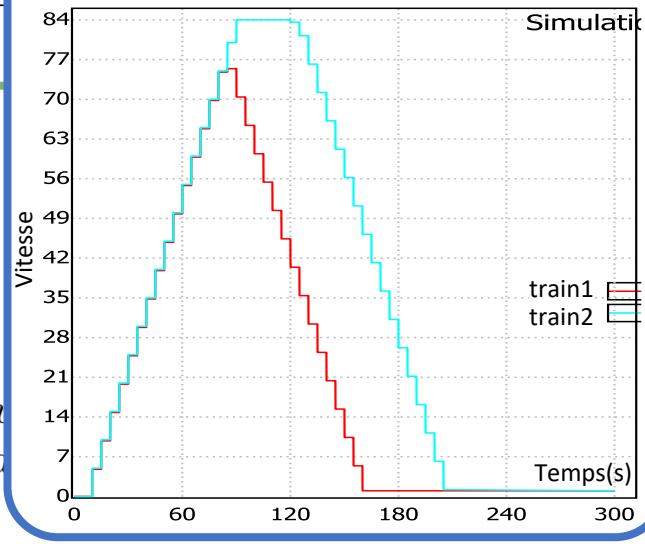
Étapes 4 et 5

Exemple de propriétés vérifiables :

- **Atteignabilité de l'état** $Lost\_By\_TIMS$:
  $E <> IIM\_Process\_A.Lost\_By\_TIMS \;\&\&$
  $LOC\_AbsTime > 60$

- **Vitesse connue par ETCS-Sol** :
  $simulate[LOC\_AbsTime <= 300; 1]\{(msgTPRRecei$
  $positionReport.V\_TRAIN) * 0.1,\ (msgTPRReceive$
  $positionReport.V\_TRAIN) * 0.1\}$

Vérification sur le modèle : Vitesse connue par ETCS-Sol



Adaptation de l'approche

→ Thèse O. Himrane

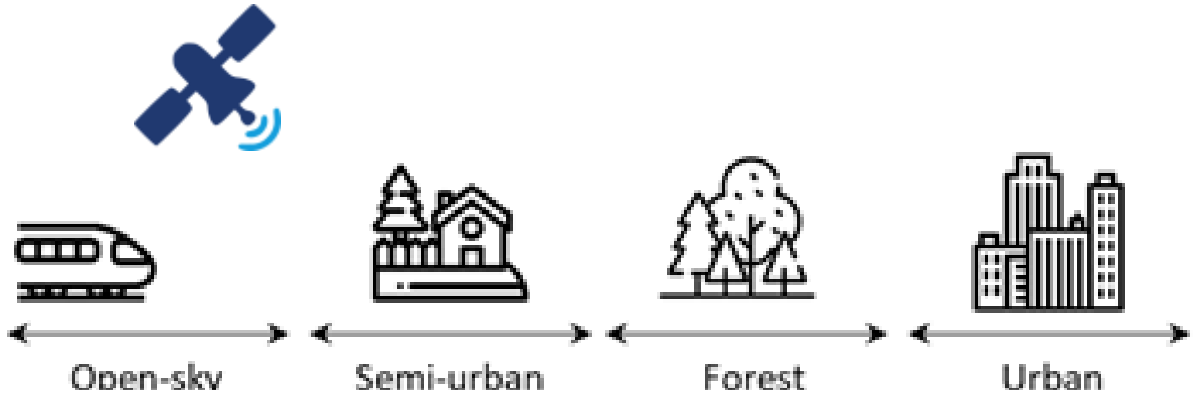
Région Hauts-de-France

→ En intégrant l'influence du contexte opérationnel sur le système

Objectif : tenir compte des comportements spécifiques de la fonction de localisation des trains avec GNSS

Paramétrage supplémentaire pour intégrer les impacts variables sur le système :

- De l'évolution d'un train
- Des conditions environnementales changeantes

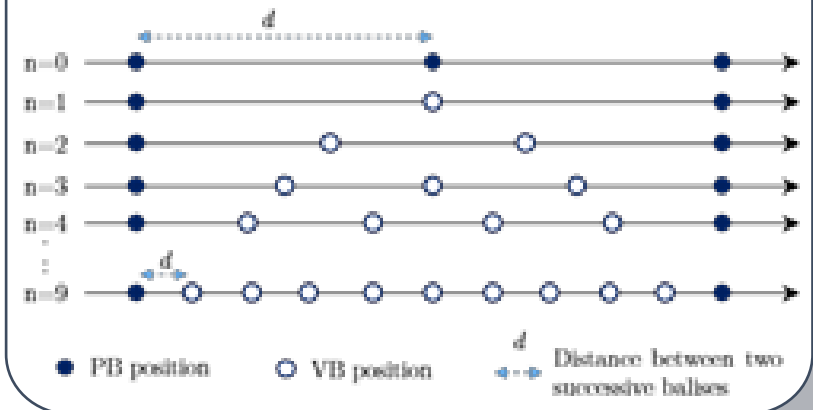


Variables additionnelles :

- Position/vitesse du train
- D'**incertitudes de position** liées à l'environnement

Application à l'ETCS niveau 3 avec balises virtuelles

Parameters related to the balise location



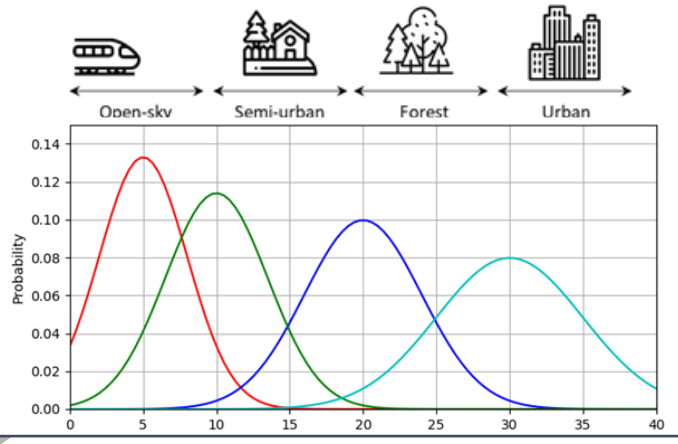
Train dynamics parameters

Acceleration parameter depending on:

- Train braking characteristics
- Track characteristics (e.g. gradient)
- Train traction capabilities

Parameters related to PL

Distribution parameters depending on environmental classes

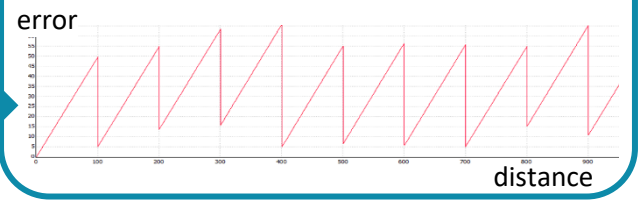


Model of the localization behavior

- **Train dynamics**
- **Evolution/modification of the error bound**
- **Balise activation**

Monitored output

Maximum allowed bound on the train position uncertainty



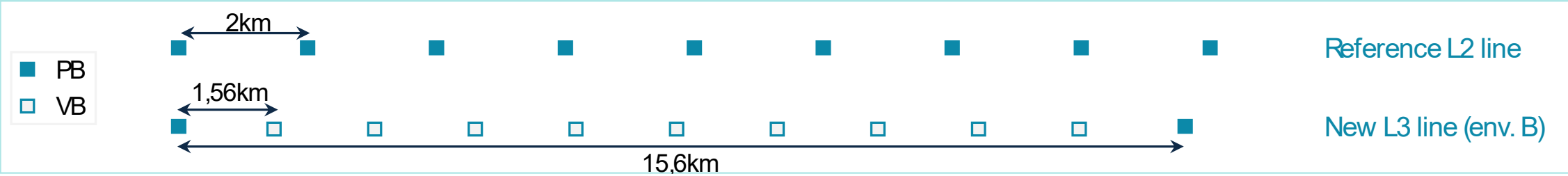
Résultats de vérification obtenus

Utilisation de techniques de SMC (*Statistical Model Checking*)

Exploitation des modèles (avec paramétrage)

⟶ Preuve que l'on peut passer de 10 PB à 1 PB (+ 9 VB) pour un environnement GNSS donné

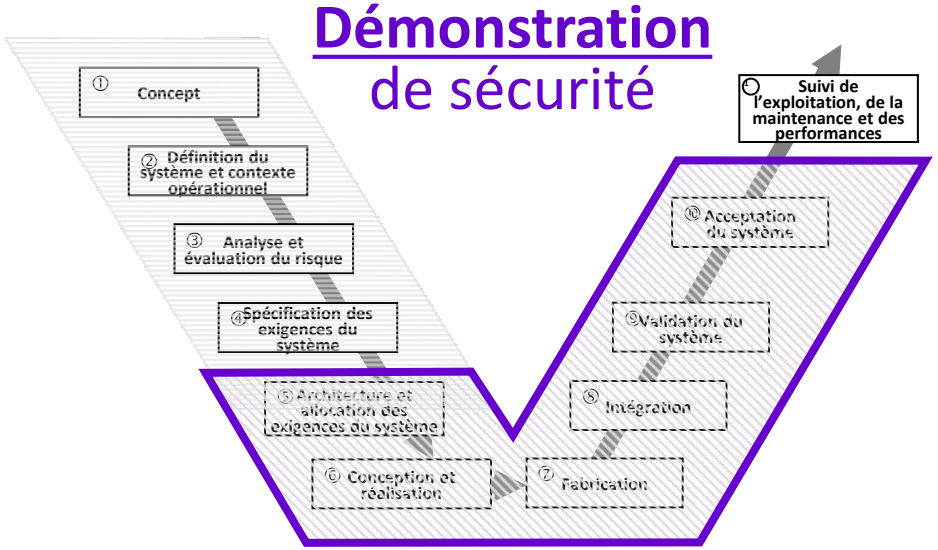
⟶ Avec garantie (intervalle de confiance par SMC) que cette configuration est sécuritaire et conforme aux spécifications



[Himrane et al. 2023]

Conclusion partie 4

Contexte opérationnel



CONTRIBUTIONS	
Multi-domaines	**CCS ferroviaires avancés**
✓ **Approche d'analyse formelle générique** pour analyser des scénarios opérationnels complexes	✓ Adaptation de l'approche pour une analyse tenant compte de la **variabilité du contexte opérationnel** ferroviaire

Perspectives

- Évolution d’approches MBSA
- Sécurité des trains autonomes

Des approches prometteuses face à la complexité

Communauté de la sûreté de fonctionnement

- *Fault tree*
- *Block diagrams*
- *Event tree*
  (etc.)

Analyses prévisionnelles des défaillances

M
B
S
A

***M**odel-**B**ased **S**ystem **E**ngineering*

Communauté de l'ingénierie système

Modélisation pour l'aide à la conception

Communauté de l'ingénierie de la sécurité

Model-**B**ased **S**afety **A**ssessment

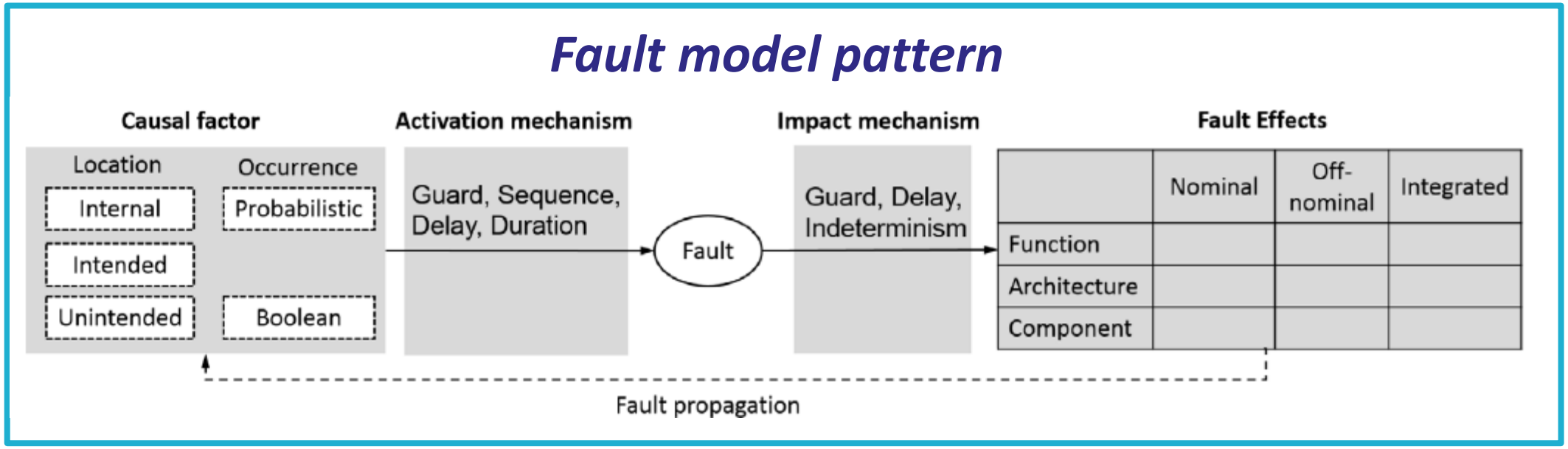
➡ Automatiser les analyses de sécurité

➡ Optimiser les analyses de sécurité

➡ Concentrer l'effort sur les aspects dysfonctionnels et dangereux

Évolution des approches MBSA

Prendre en compte les conditions environnementales et les comportements dynamiques



➡ Adaptation aux spécificités techniques et contextuelles des **technologies sans fil de localisation et de communication**

Expertise

Université Gustave Eiffel — Département COSYS

Pour continuer l'analyse des systèmes critiques ferroviaires

Intégrer les réflexions sur les MBSA, à court terme, dans le cadre :

– Des approches orientées modèles pour l'ETCS exploité à l'aide de cantons mobiles

Thèse

Chaire « Sécurité des systèmes ferroviaires »

CERTIFER Groupe apave

LIS LABORATOIRE D'INFORMATIQUE & SYSTÈMES

Université Gustave Eiffel — Laboratoire ESTAS

– De véhicules légers hybrides route / rail

Projet **FLEXY**

RAILENIUM RAIL RESEARCH & INNOVATION

SNCF

– Solution de signalisation "*trackside*"

HITACHI

Sécurité des trains autonomes

Pourquoi les TA : ils contribuent aussi à augmenter la compétitivité du transport ferroviaire, et requièrent des efforts communs en termes de sécurité

Objectif : contribuer à l'établissement d'un cadre d'assurance sécurité lié à l'introduction de l'autonomie dans les trains

→ Thèse M. Chelouati
Défendue en 2024

RAILENIUM
RAIL RESEARCH & INNOVATION

TRAIN AUTONOME
SERVICE VOYAGEURS

Plusieurs aspects déjà approfondis :

- L'argumentation de sécurité
- L'analyse dynamique des risques
- La prise en compte des risques dans les processus de prise de décision des TA

Vers la mise en service de TA sûrs ?

Équipe Sécurité d'ESTAS

Adaptation du processus d'appréciation des risques des TA à ≠ niveaux

Système / Logiciel / Composants à base d'IA

Nouvelles approches de démonstration

ex. fondées sur STPA

Travaux méthodologiques

Formations

Chaire « Sécurité des systèmes ferroviaires »

Appui aux organismes réglementaires et de certification

Collaborations scientifiques

STRMTG

CERTIFER

epsf

RAILENIUM RAIL RESEARCH & INNOVATION

heudiasyc

Eisenbahn-Bundesamt

Deutsches Zentrum für Schienenverkehrsforschung

Merci pour votre attention !

Université Gustave Eiffel

Merci aux collègues pour leur collaboration, leur soutien, et leur sympathie !