26èmes journées STP du GDR MACS
Clermont-Ferrand, 22-23 novembre 2018

Génération automatique et vérification formelle de programmes d'API sécurisés pour les systèmes de contrôle ferroviaires

Mohamed NIANG
Bernard RIERA
Alexandre PHILIPPOT
Serge Debernard

Introduction

- Concevoir des systèmes plus flexible et plus résilient.
  - Par les nouvelles technologies issues du numérique et des technologies de fabrication.
  - Mais en même temps, l'humain doit rester au centre du processus global de prise de décision et de contrôle.

- HUMANISM project : Développer une méthodologie pour concevoir des systèmes d'assistance coopérative pour soutenir la prise de conscience humaine et la prise de décision

Université Polytechnique HAUTS-DE-FRANCE

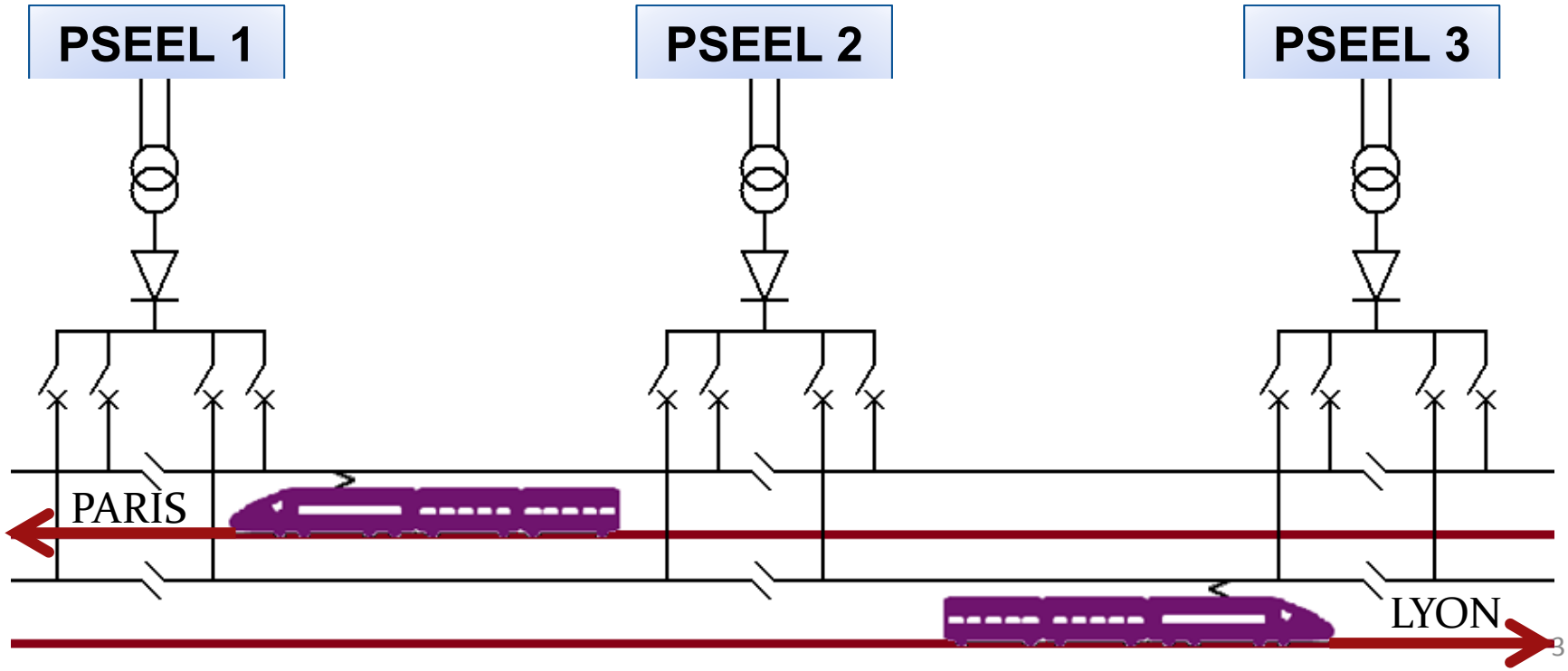
Université Bretagne Sud

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

Humanism

SNCF :

- Management, exploitation et opération de l'infrastructure ferroviaire en France
- 30 000 Km de lignes,
- 560 sous-stations contenant les EALE (**E**quipements d'**A**limentation des **L**ignes **É**lectrifiées) - Power Supply Equipment of the Electric Lines (PSEEL)
  - Disjoncteur, Transformateur, système d'interruption …pour le contrôle et la protection des équipements et des personnes (EN 50126) - (1500 V DC ou 25 KV AC)



OUTLINE

I. Introduction & Background

II. Formal Verification of Recipe book

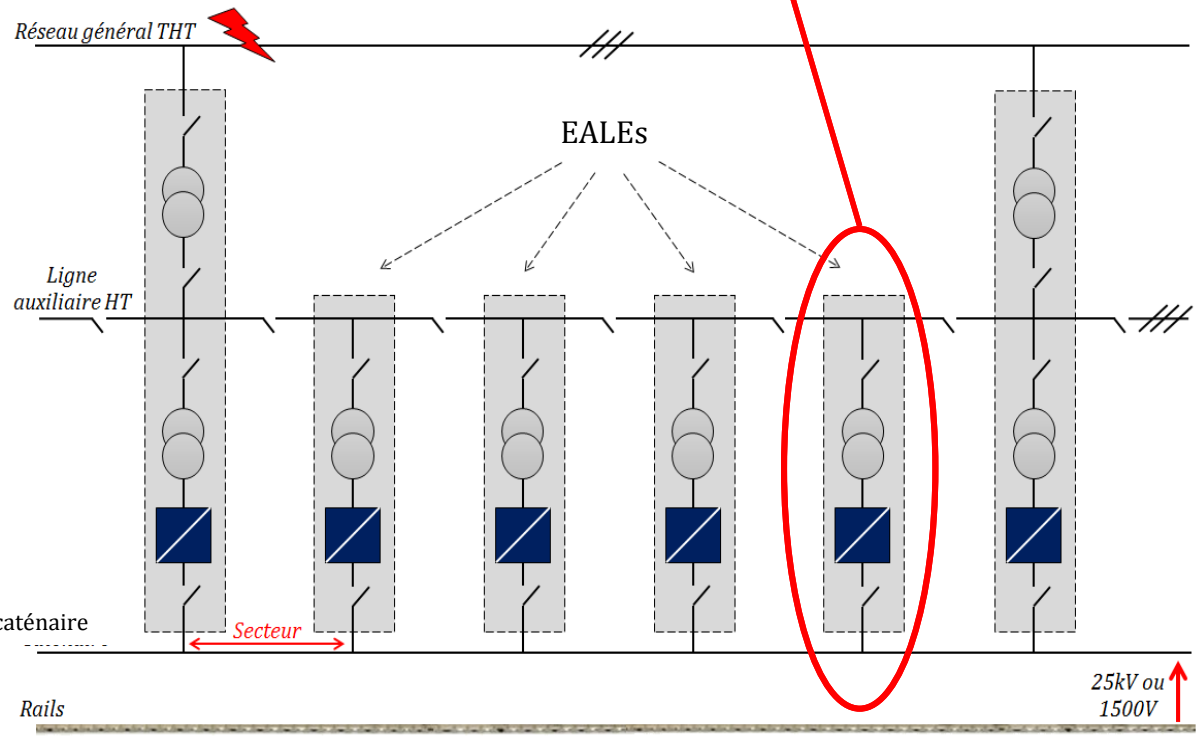
III. Virtual Commissioning

1. Validation of PLC programs through SIL simulations
2. Validation of electric cabinets through HIL simulations

IV. Conclusion

INTRODUCTION

Contexte : **E**quipements d'**A**limentation des **L**ignes **É**lectrifiées (**EALE**)



Chargé d'études SNCF

Métier des EALE et problématique

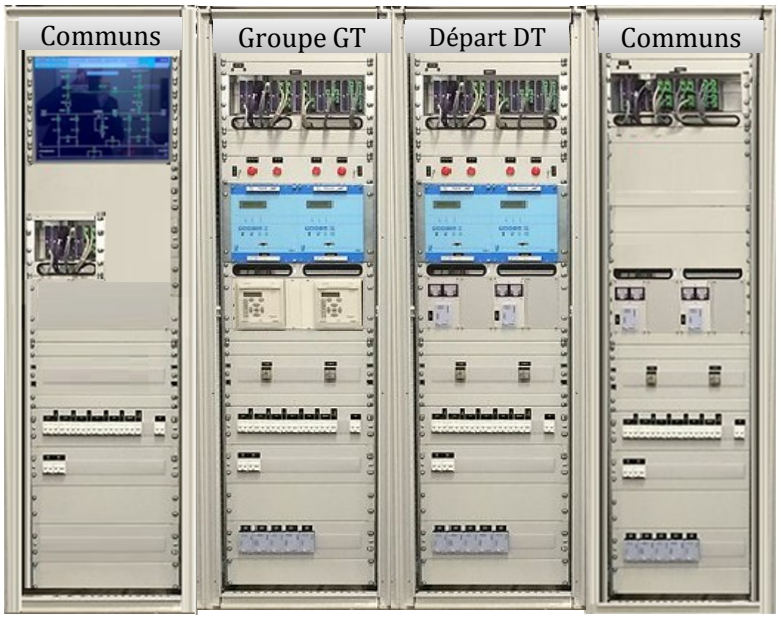
Workflow *durant un projet d'automatisation d'EALE*

Cahier des charges du projet

1 **Conception des livrables du projet (programmes, cahier de recettes, schémas électriques …)**

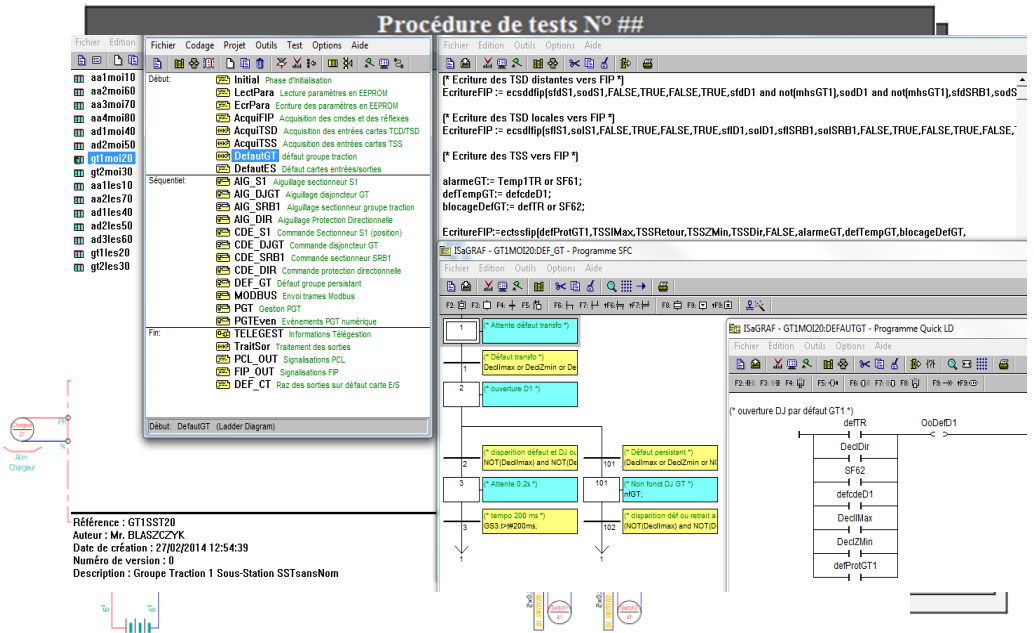
2

Système de Contrôle/Commande/Protection



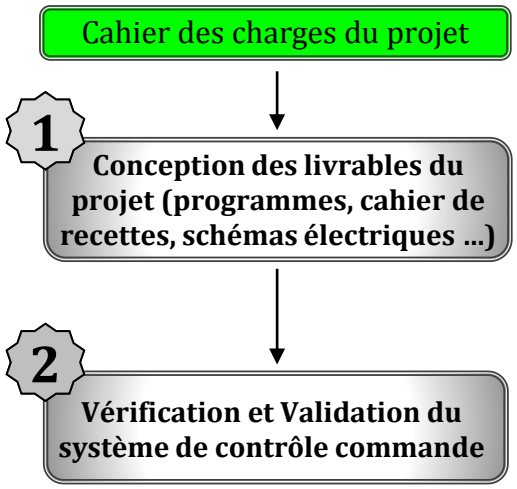
Livrables d'un projet :

- Schémas électriques
- Programmes API
- Cahier de recettes



Métier des EALE et problématique

Workflow *durant un projet d'automatisation d'EALE*



Livrables d'un projet :

- Schémas électriques
- Programmes API
- Cahier de recettes

Vérification et Validation :

- Des programmes API (conformément au CDC) ;
- Du câblage des armoires (E/S, réseau RLI…) ;
- Des réglages de protections numériques.

Évolution du workflow des chargés d'études de la SNCF

Workflow traditionnel → *Nouveau workflow* → *Workflow prévisionnel*

(Coupat, 2014) ***(Niang, 2018)***

Métier des EALE et problématique

Workflow traditionnel | *Nouveau workflow* | *Workflow prévisionnel*

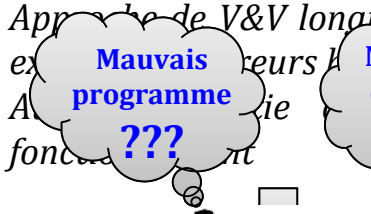
Problématiques du workflow traditionnel :

Etape 1:

- *Des livrables longs et fastidieux à établir*
- *L'existence de tâches répétitives*
- *La présence d'erreurs dans les livrables*

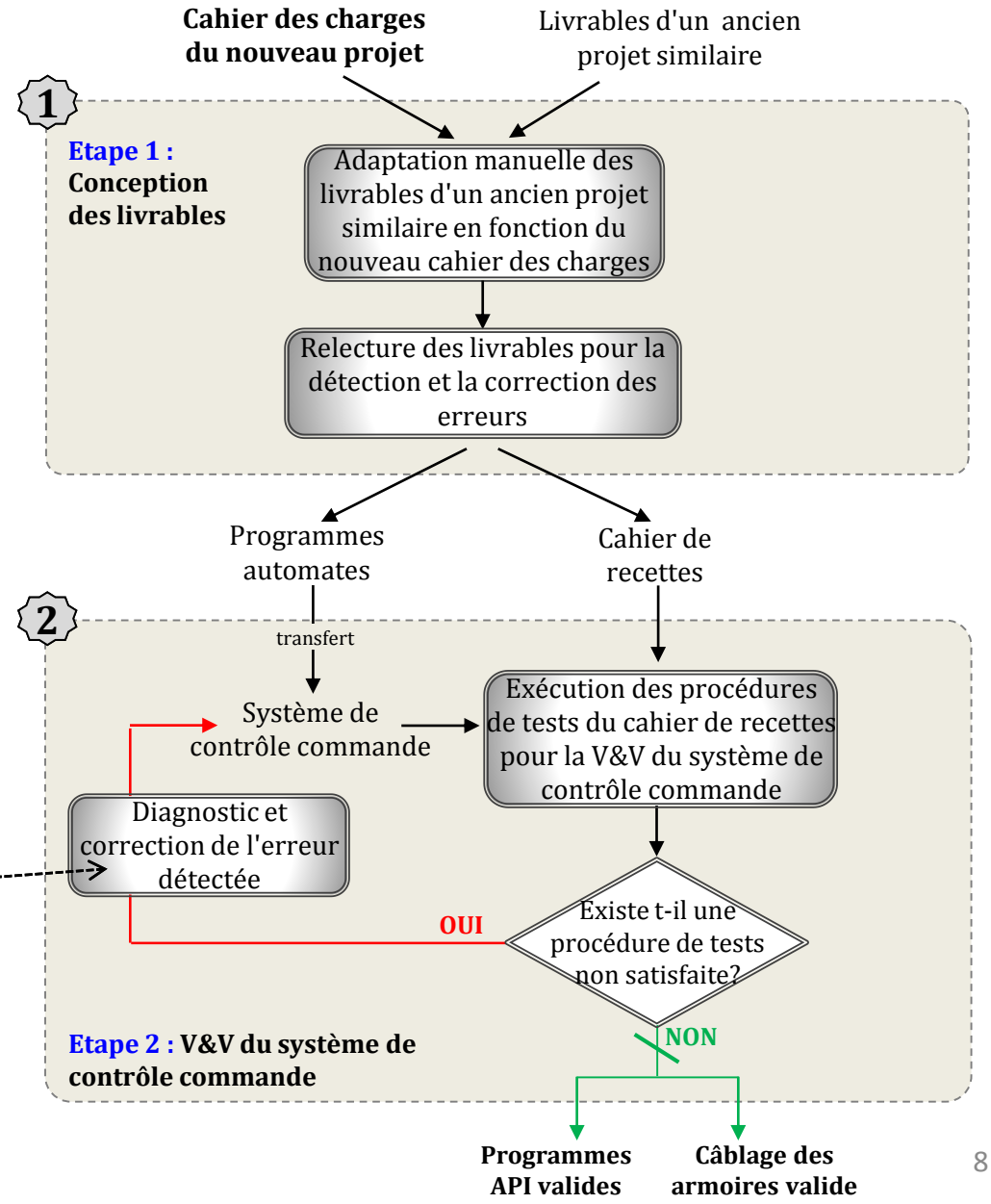
Etape 2:

- *Vérification des programmes par simple relecture*
- *Validation simultanément des programmes et du câblage*
- *Procédures de tests non exhaustives*
- *App[illegible]de de V&V longue[illegible]uelle, et ex[illegible]reurs l[illegible]*
- *A[illegible]ie [illegible]té de fonct[illegible]nt*



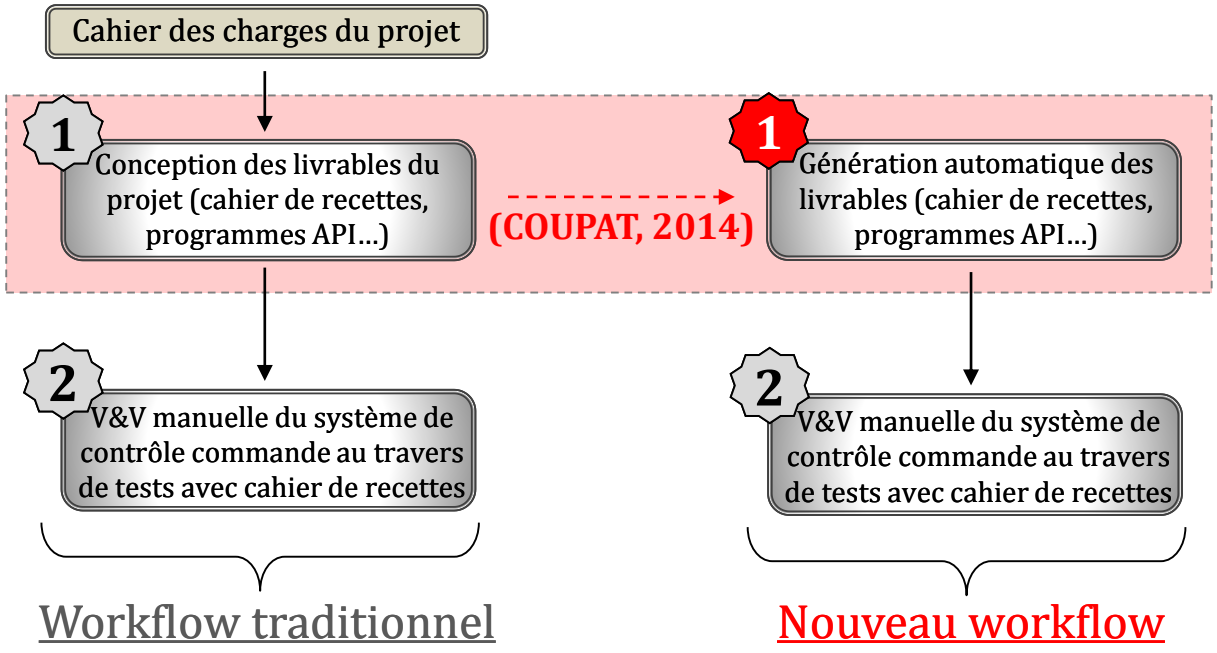
Ces incon[illegible] peuvent compromettre [illegible]acité et la fiabil[illegible]tème de contr[illegible]mande

Edgar W. Dijkstra : « Les tests montrent la présence de défauts » (Buxton 1970)



Métier des EALE et problématique

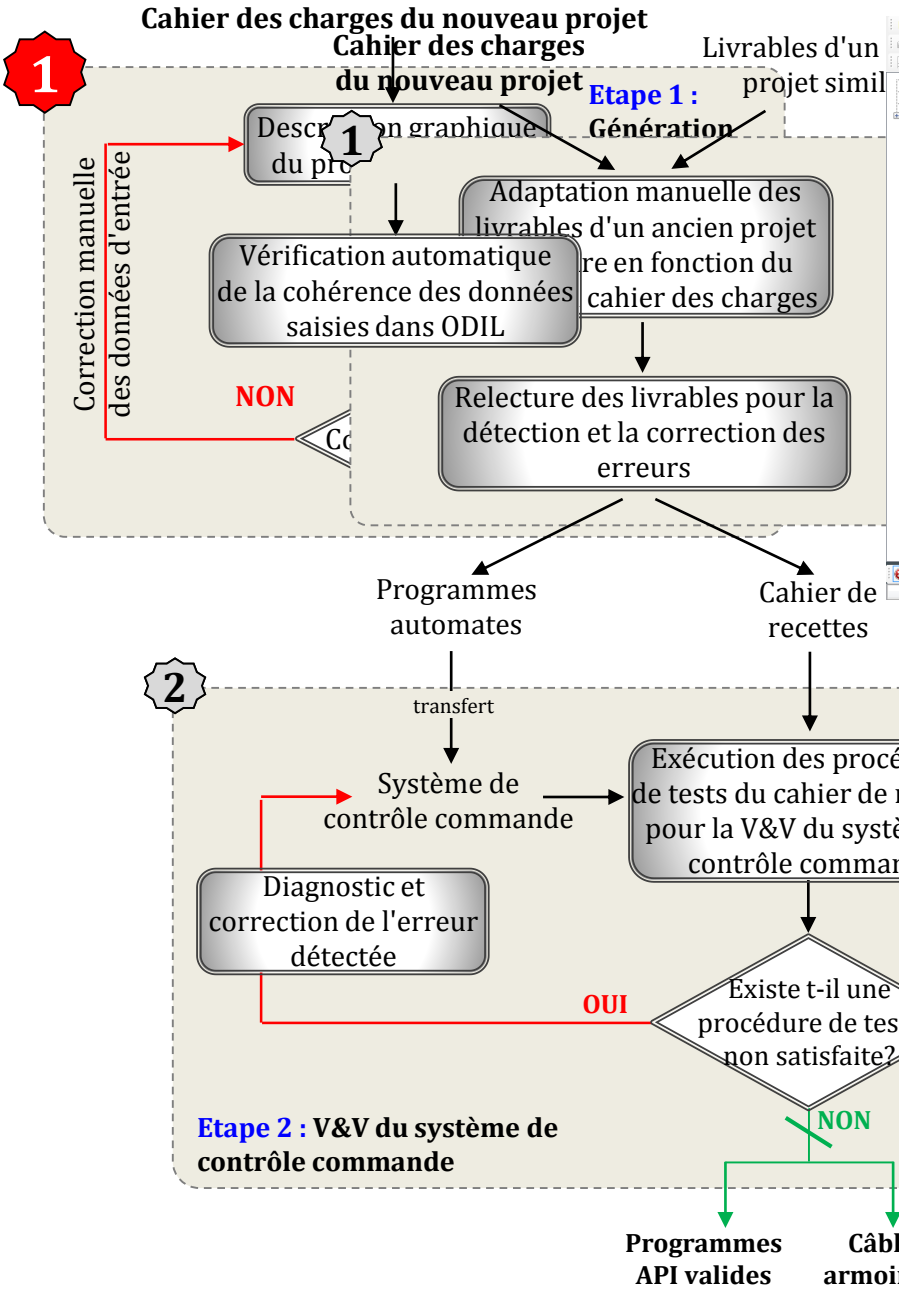
Workflow traditionnel | *Nouveau workflow* | *Workflow prévisionnel*

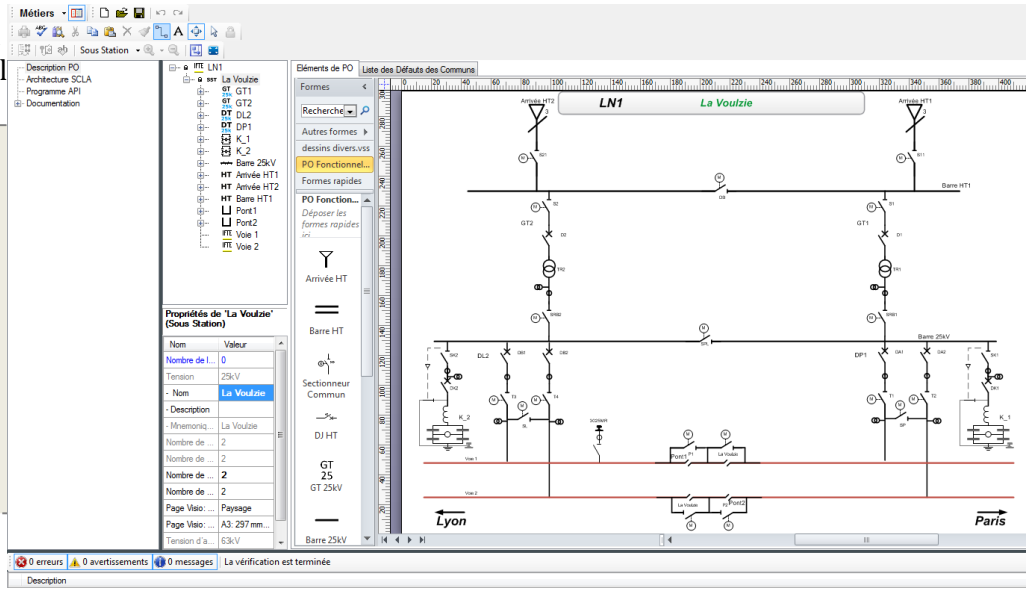


Objectif : *optimiser la phase 1 du workflow d'un projet d'automatisation d'EALE, à savoir la conception des livrables*

Métier des EALE et problématique

Workflow traditionnel | *Nouveau workflow* | *Workflow prévisionnel*





ODIL GREMLINS : Solution de génération automatique de données, basée sur la technologie DSM (Domain Specific Modelling), **développé avec Prosyst**

Métier des EALE et problématique

Workflow traditionnel → *Nouveau workflow* → *Workflow prévisionnel*

	Workflow traditionnel	Nouveau workflow
Phase 1 : Conception des livrables du projet	○ Réalisation des schémas électriques------ 60h ○ Conception des programmes API---------- 50h ○ Rédaction du cahier de recettes---------- 40h ○ Relecture et correction des livrables------ 10h **Total des heures---------- 160h**	○ Réalisation des schémas électriques----- 60h ○ Génération des programmes API et du cahier de recettes avec ODIL---------- 5h ○ Relecture des livrables générés---------- 5h **Total des heures ---------- 70h**
Phase 2 : V&V du système de contrôle commande	○ Vérification du système de contrôle commande en usine ---------- 40h ○ correction---------- 20h ○ Validation du système de contrôle commande sur site---------- 40h **Total des heures---------- 100h**	○ Vérification du système de contrôle commande en usine ---------- 40h ○ correction---------- 20h ○ Validation du système de contrôle commande sur site---------- 40h **Total des heures---------- 100h**

Etape 1 (COUPAT, 2014) :

- ~~*Des livrables longs et fastidieux à établir*~~
- ~~*L'existence de tâches répétitives*~~
- ~~*La présence d'erreurs de recopie dans les livrables*~~

Etape 2 :

- *Vérification des programmes par simple relecture*
- *Validation simultanément des programmes et du câblage*
- *Procédures de tests non exhaustives*
- *Approche de V&V longue, manuelle, et exposée aux erreurs humaines*
- *Aucune garantie de la sûreté de fonctionnement*

OUTLINE

I. Introduction & Background

II. Formal Verification of Recipe book

III. Virtual Commissioning

1. Validation of PLC programs through SIL simulations
2. Validation of electric cabinets through HIL simulations

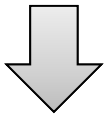
IV. Conclusion

État de l'art sur les techniques de V&V

Récapitulatif des méthodes existantes pour la V&V des systèmes de contrôle commande

Méthode	Principe	Avantages	Inconvénients
Test	Exécution de procédures de tests	Très largement utilisée ; Facile à mettre en œuvre	Non exhaustive, longue, erreurs humaines…
Virtual Commissioning	Simulateur de Partie Opérative; Procédures de tests	Automatisation des tests, sécurité, traçabilité, gain de temps, formation opérateur…	Non exhaustive; Fiabilité des modèles
Méthodes formelles	Vérification formelle basée sur des calculs mathématiques	Vérification exhaustive et automatique Renvoi d'une trace	Explosion combinatoire Fiabilité des modèles

Association des techniques de manière à exploiter les avantages de chacune d'entre elles



Mise en place d'une approche de V&V ***formelle***, ***automatisée***, *et* ***méthodologique***

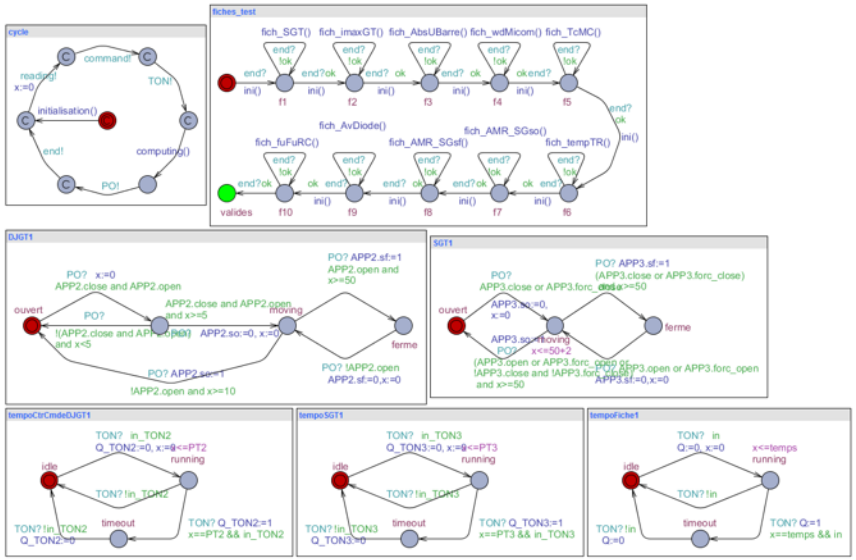
Méthodologie

MODELISATION

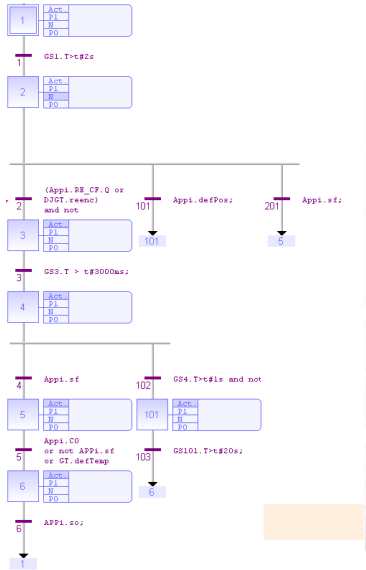
INSTALLATION ÉLECTRIQUE

PROGRAMMES AUTOMATES

CAHIER DE RECETTES



- Modélisation de l'ensemble des données du projet
- Etude du comportement du système à la milliseconde près
- Vérification de propriétés issues du cahier de recettes?
- Vérification exhaustive des programmes
- …



	Objet du test
U/S	Sectionneur Groupe GT1 SG1

né

- Sectionneur groupe SG1 fermé
- Présence tension HT (tension injectée dans le BNU GT1 = 58V~)
- Pas de défauts

Essais

Actions à réaliser	Résultats Attendus
1. Fermer Sectionneur 1500 V SG1.	1. Sectionneur 1500 V SG1 fermé
2. Fermer le Disjoncteur DGT1	2. Disjoncteur DGT1 fermé
3. Ouvrir Sectionneur 1500 V SG1 depuis le CLE	3. Néant
4. Ouvrir Sectionneur 1500 V SG1 (1)	4. Ouverture Disjoncteur DGT1 avant séparation des contacts de puissance du sectionneur
5. Fermer le Disjoncteur DGT1	5. Disjoncteur DGT1 fermé
6. Fermer Sectionneur 1500 V SG1 depuis le CLE	6. Néant
7. Fermer Sectionneur 1500 V SG1 (2)	7. Ouverture Disjoncteur DGT1 avant établissement des contacts de puissance du sectionneur

Commentaires

Usine	Site
(1) Pour ouvrir le sectionneur SG1 baisser le compact SG1.S (2) Pour fermer le sectionneur SG1 baisser le compact SG1.S	(1) Faire une ouverture manuelle du sectionneur SG1 (2) Faire une fermeture manuelle du sectionneur SG1

Décisions

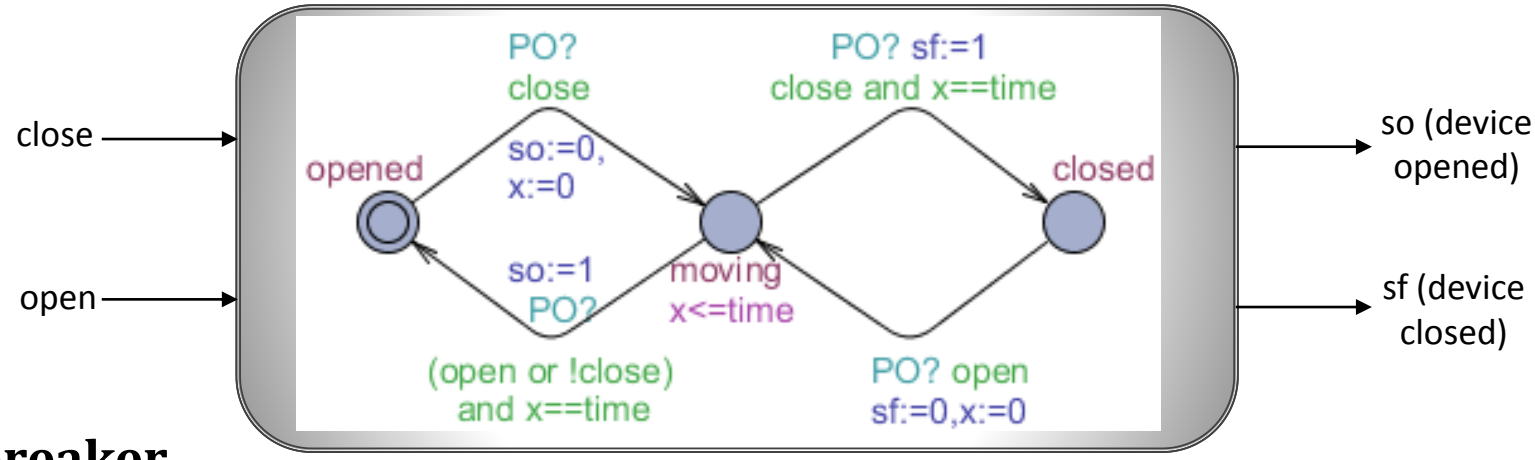
Usine	Correct : ☒	Gênant : ☐	Bloquant : ☐	N° FFT :
Site :	Correct : ☒	Gênant : ☐	Bloquant : ☐	
Test réalisé par	Usine : RB. NL		Date du test	Usine : 25/08/15
	Site : RB. AB. RC			Site : 19/01/16

Formal verification of functional requirements

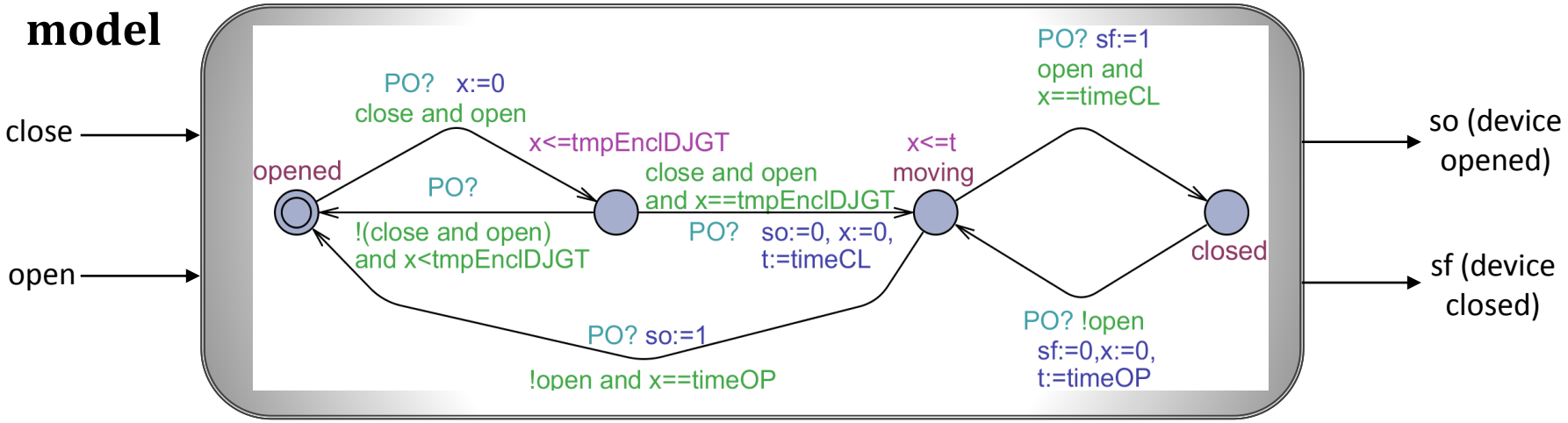
PSEEL's models: Instantiation of devices (20 types of devices) from 4 device categories:

- Abstract time discrete-events models

Switch model



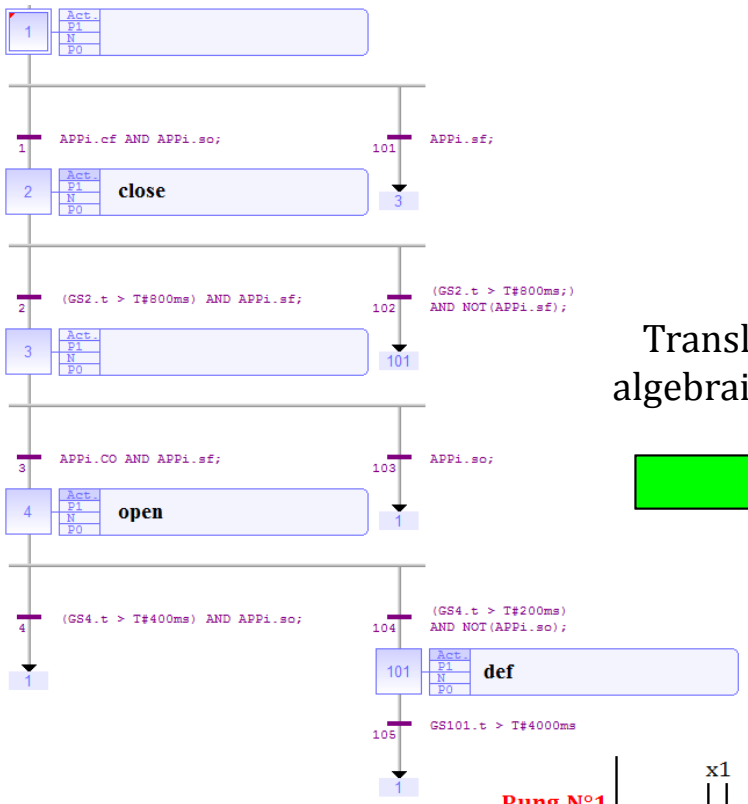
circuit-breaker model



Transformer: structure of Boolean variables representing internal faults: overcurrent, short circuit, overheating, …

Formal verification of functional requirements

PLC programs modeling:



Control program (in SFC) for the switch

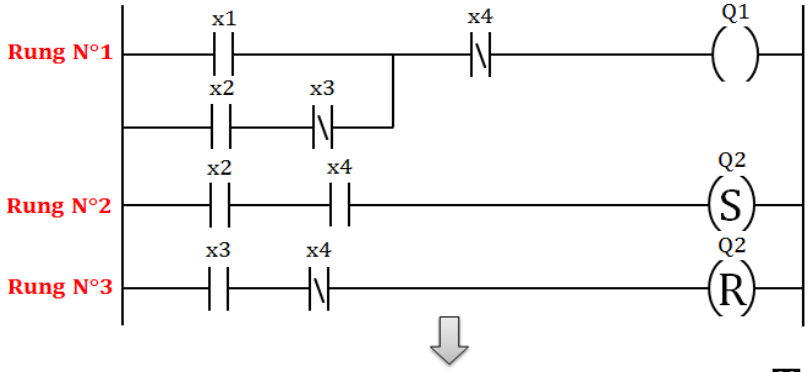
Translation into algebraic equations

```
void CmdAPPi( bool &x1, bool &x2, bool &x3, bool &x4,          // Declaration of variables
              bool &x101, bool &so, bool &sf, bool &CO, bool &CF,
              bool &open, bool &close, bool &def, bool &intmp, bool &Qtmp, int &PT)
{
    bool ft1, ft2, ft3, ft4, ft101, ft102, ft103, ft104, ft105;

 // Equations of transitions
    ft1   = x1 and so and CF;
    ft2   = x2 and sf and Qtmp;
    ft3   = x3 and sf and CO;
    ft4   = x4 and so and Qtmp;
    ft101 = x1 and sf;
    ft102 = x2 and !sf and Qtmp;
    ft103 = x3 and so;
    ft104 = x4 and !so and Qtmp;
    ft105 = x101 and Qtmp;

 // Equations of steps
    x1   = ft4 or ft105 or ft103 or x1 and !ft1 and !ft101;
    x2   = ft1 or x2 and !ft2 and !ft102;
    x3   = ft2 or x3 and !ft3 and !ft103;
    x4   = ft3 or x4 and !ft4 and !ft104;
    x101 = ft104 or ft102 or x101 and !ft105;

 // Timers evolution in steps x2, x4, and x101
    intmp = x2 or x4 or (x101 and !ft104);
    PT=(x2 ?80:PT);  PT:=(x4 ?40:PT);  PT:=(x101 ?400:PT);
```




```
// Translation into algebraic equations
Q1 = (x1 or (x2 and not x3)) and not x4 ;
Q2 = (x2 and x4 ? 1 : Q2) ;
Q2 = (x3 and not x4 ? 0 : Q2) ;
```

Translation of LD into algebraic equations

Formal verification of functional requirements

Recipe book modeling (Specification of functional requirements):

Fiche de test Réf.						Objet du test
D	B	01	F	N	U/S	Sectionneur Groupe GT1 SG1

Condition Initiales

- Disjoncteur DGT1 fermé
- Sectionneur groupe SG1 fermé
- Présence tension HT (tension injectée dans le BNU GT1 = 58V~)
- Pas de défauts

Essais

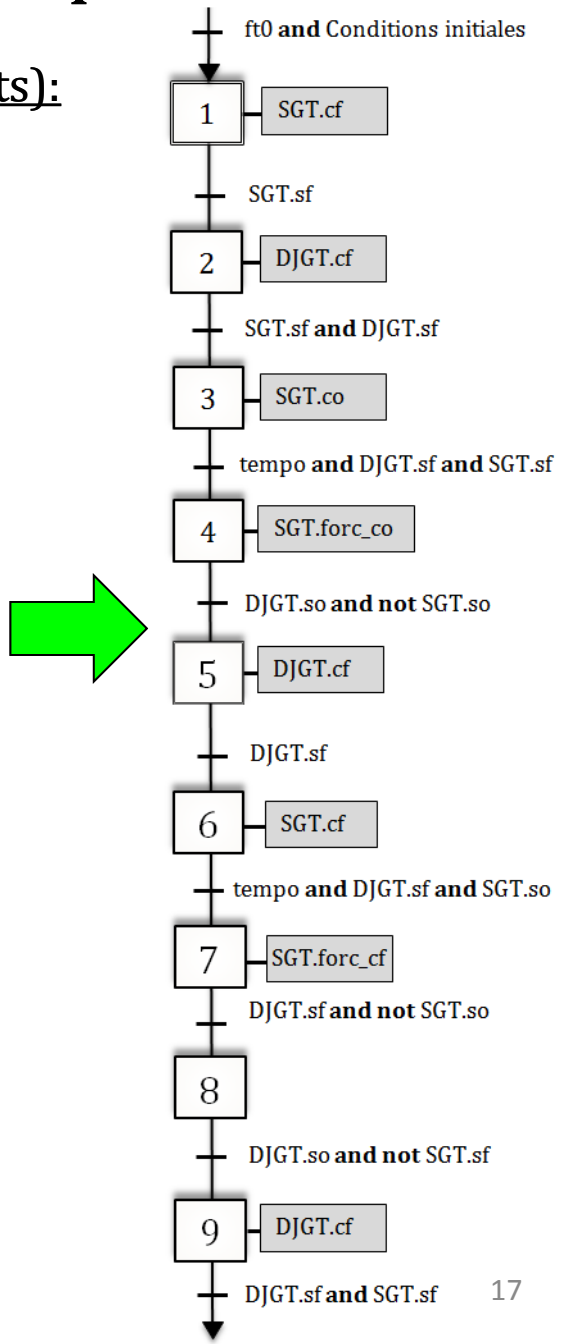
Actions à réaliser	Résultats Attendus
1. Fermer Sectionneur 1500 V SG1.	1. Sectionneur 1500 V SG1 fermé
2. Fermer le Disjoncteur DGT1	2. Disjoncteur DGT1 fermé
3. Ouvrir Sectionneur 1500 V SG1 depuis le CLE	3. Néant
4. Ouvrir Sectionneur 1500 V SG1 (1)	4. Ouverture Disjoncteur DGT1 avant séparation des contacts de puissance du sectionneur
5. Fermer le Disjoncteur DGT1	5. Disjoncteur DGT1 fermé
6. Fermer Sectionneur 1500 V SG1 depuis le CLE	6. Néant
7. Fermer Sectionneur 1500 V SG1 (2)	7. Ouverture Disjoncteur DGT1 avant établissement des contacts de puissance du sectionneur

Commentaires

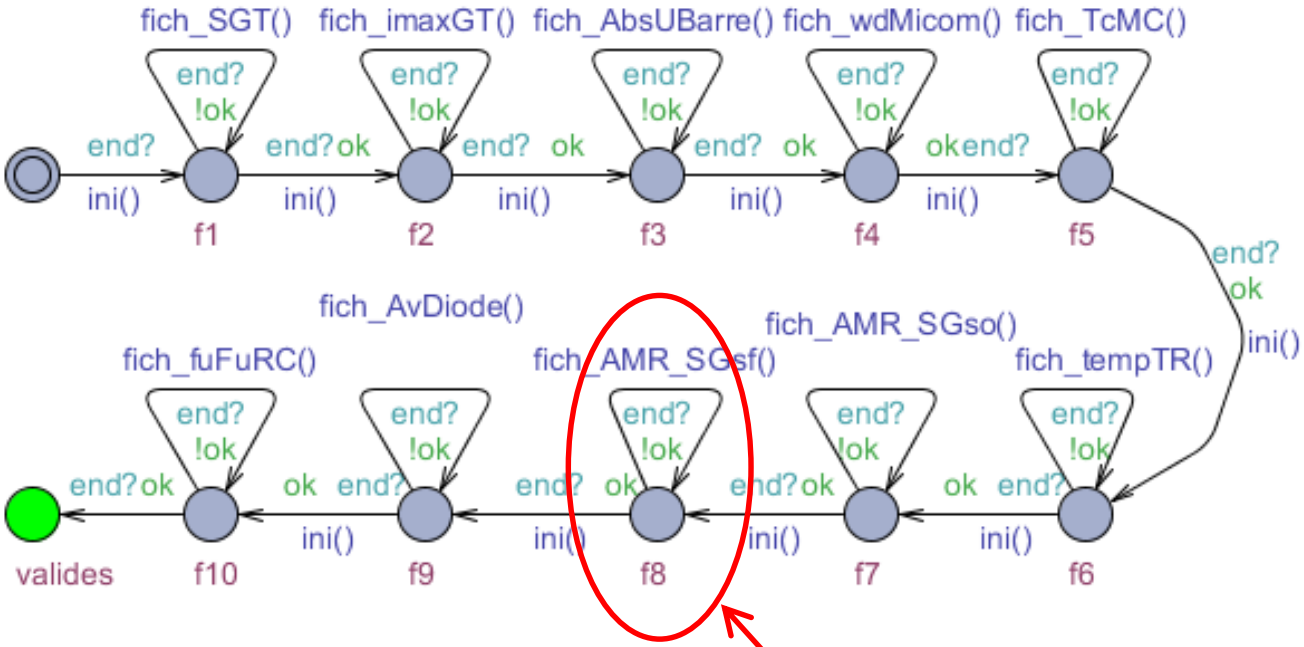
Usine	Site
(1) Pour ouvrir le sectionneur SG1 baisser le compact SG1.S (2) Pour fermer le sectionneur SG1 baisser le compact SG1.S	(1) Faire une ouverture manuelle du sectionneur SG1 (2) Faire une fermeture manuelle du sectionneur SG1

Décisions

Usine	Correct : ☑	Gênant : ☐	Bloquant :☐	N° FFT :	
Site :	Correct : ☒	Gênant : ☐	Bloquant :☐		
Test réalisé par	Usine : RB. NL			Date du test	Usine : 25/08/15
	Site : RB. AB. RC				Site : 19/01/16



Vérification formelle des programmes API



Fiche de test Réf.						Objet du test
D	B	01	F	N	U/S	Sectionneur Groupe GT1 SG1

Condition Initiales

- Disjoncteur DGT1 fermé
- Sectionneur groupe SG1 fermé
- Présence tension HT (tension injectée dans le BNU GT1 = 58V~)
- Pas de défauts

Essais

Actions à réaliser	Résultats Attendus
1. Fermer Sectionneur 1500 V SG1.	1. Sectionneur 1500 V SG1 fermé
2. Fermer le Disjoncteur DGT1	2. Disjoncteur DGT1 fermé
3. Ouvrir Sectionneur 1500 V SG1 depuis le CLE	3. Néant
4. Ouvrir Sectionneur 1500 V SG1 (1)	4. Ouverture Disjoncteur DGT1 avant séparation des contacts de puissance du sectionneur
5. Fermer le Disjoncteur DGT1	5. Disjoncteur DGT1 fermé
6. Fermer Sectionneur 1500 V SG1 depuis le CLE	6. Néant
7. Fermer Sectionneur 1500 V SG1 (2)	7. Ouverture Disjoncteur DGT1 avant établissement des contacts de puissance du sectionneur

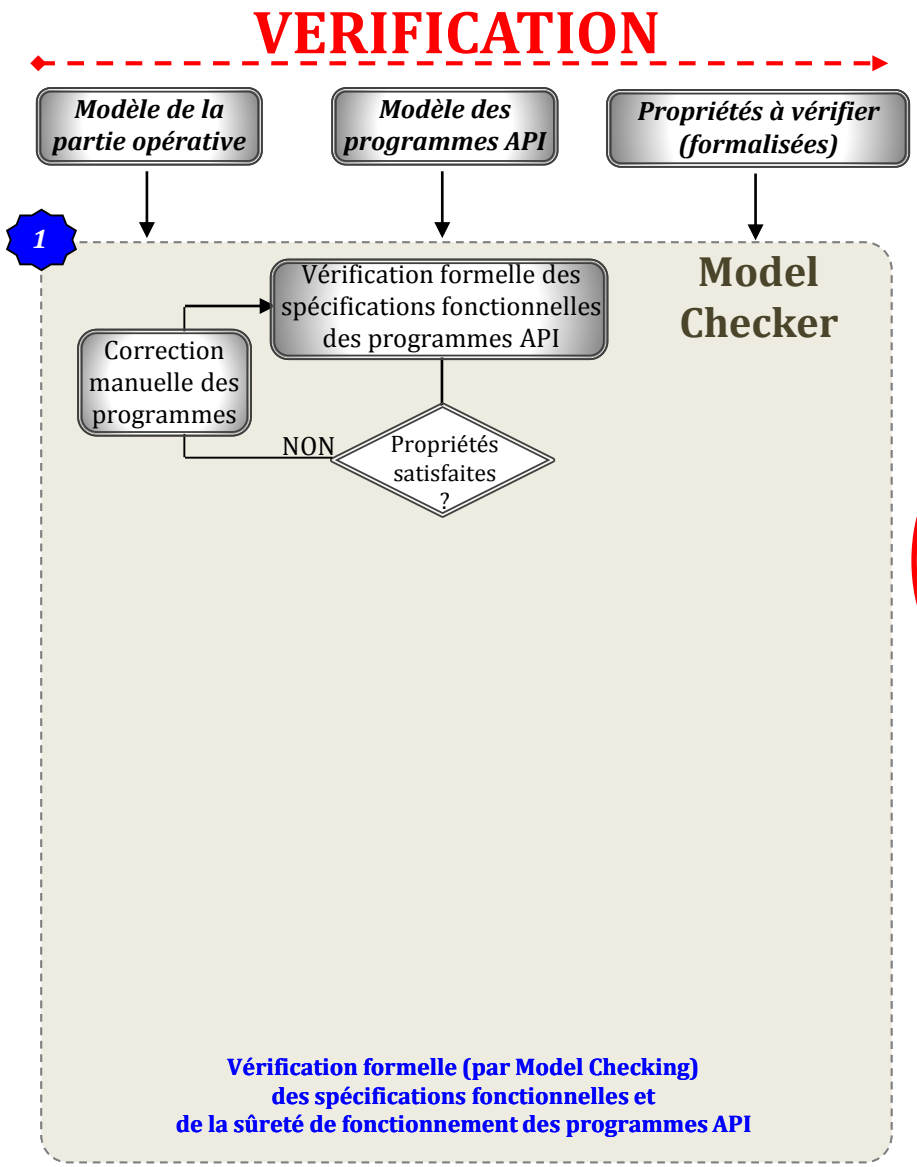
Commentaires

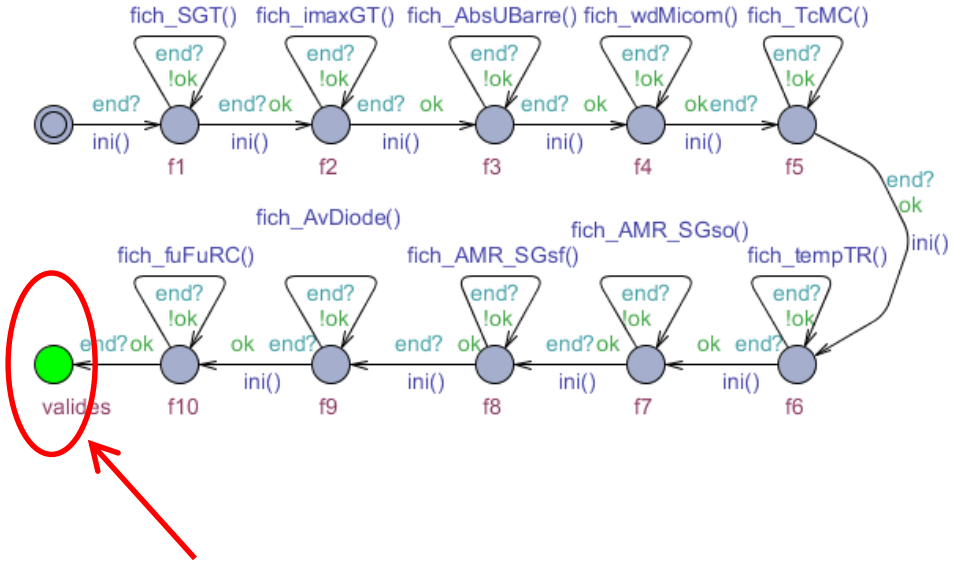
Usine	Site
(1) Pour ouvrir le sectionneur SG1 baisser le compact SG1.S (2) Pour fermer le sectionneur SG1 baisser le compact SG1.S	(1) Faire une ouverture manuelle du sectionneur SG1 (2) Faire une fermeture manuelle du sectionneur SG1

Décisions

Usine	Correct : ☑	Gênant : ☐	Bloquant : ☐	N° FFT :	
Site :	Correct : ☑	Gênant : ☐	Bloquant : ☐		
Test réalisé par	Usine : RB . NL Site : BB . AB . RC			Date du test	Usine : 15/08/17 Site : 19/07/17

Vérification formelle des programmes API

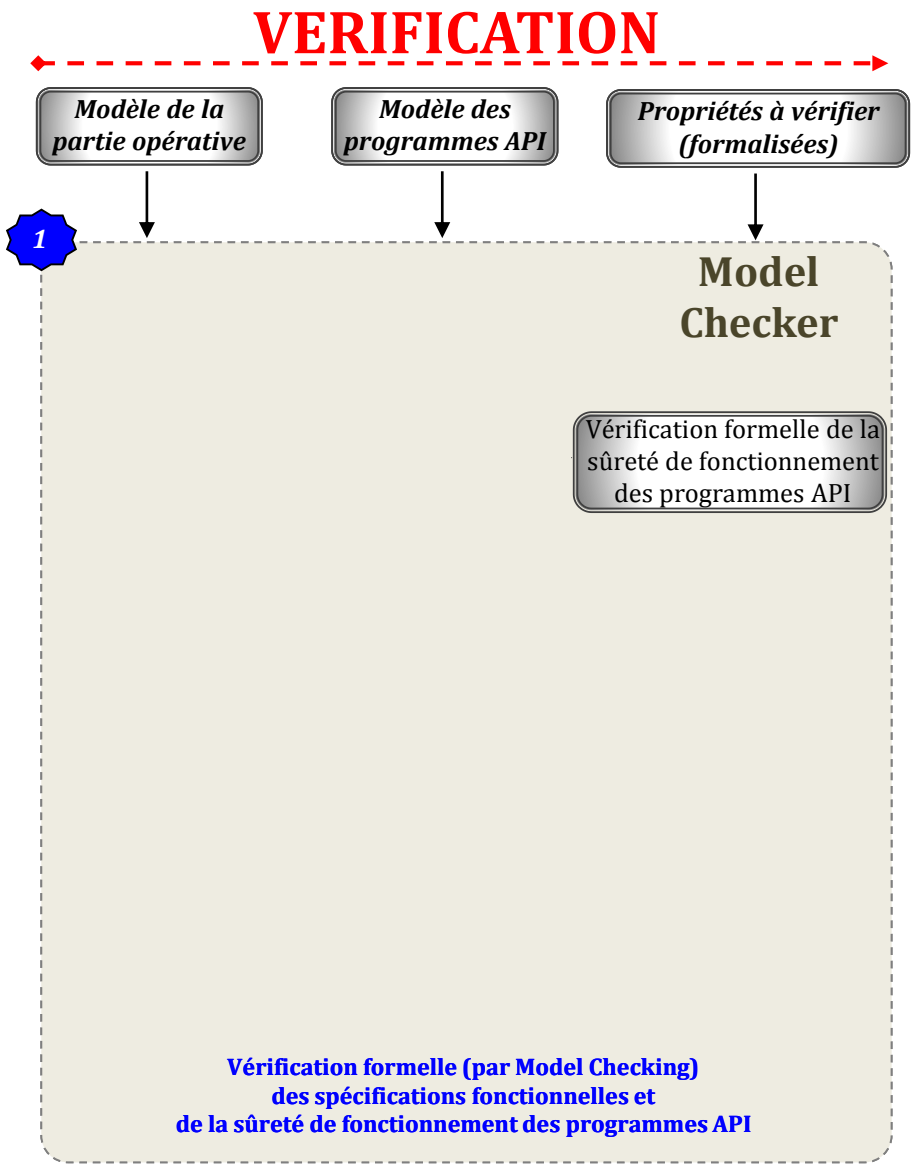


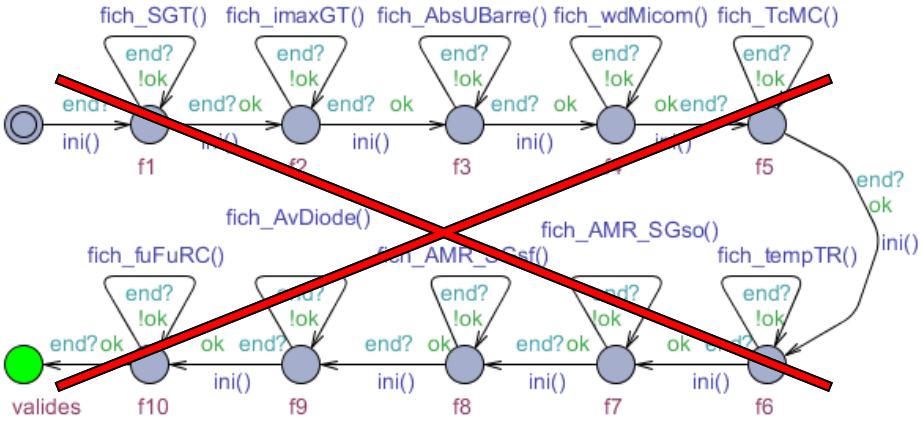


Atteignable ?

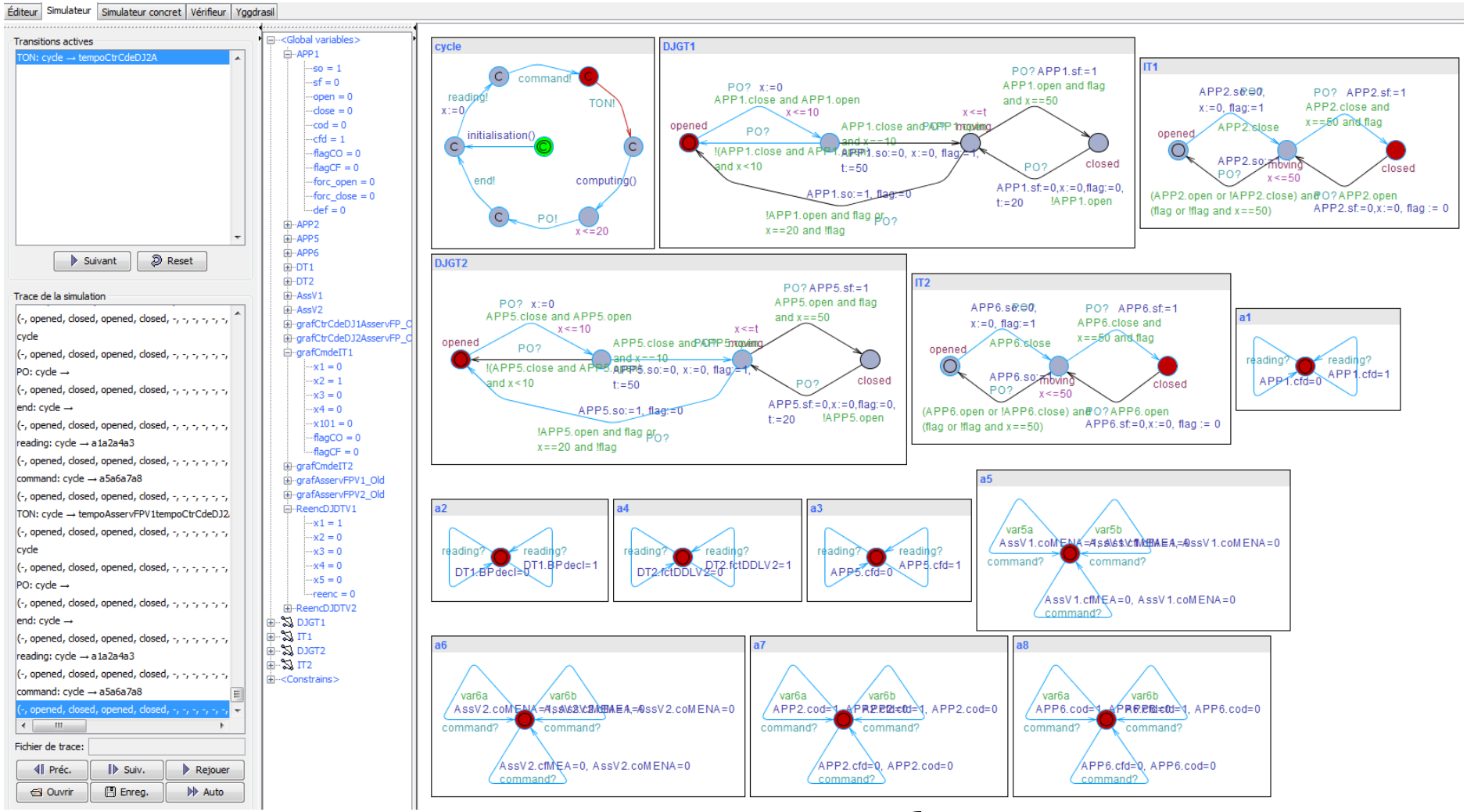
E<> attente_fiche.timeout
(en logique temporelle CTL)

Vérification formelle des programmes API





Vérification formelle des programmes API



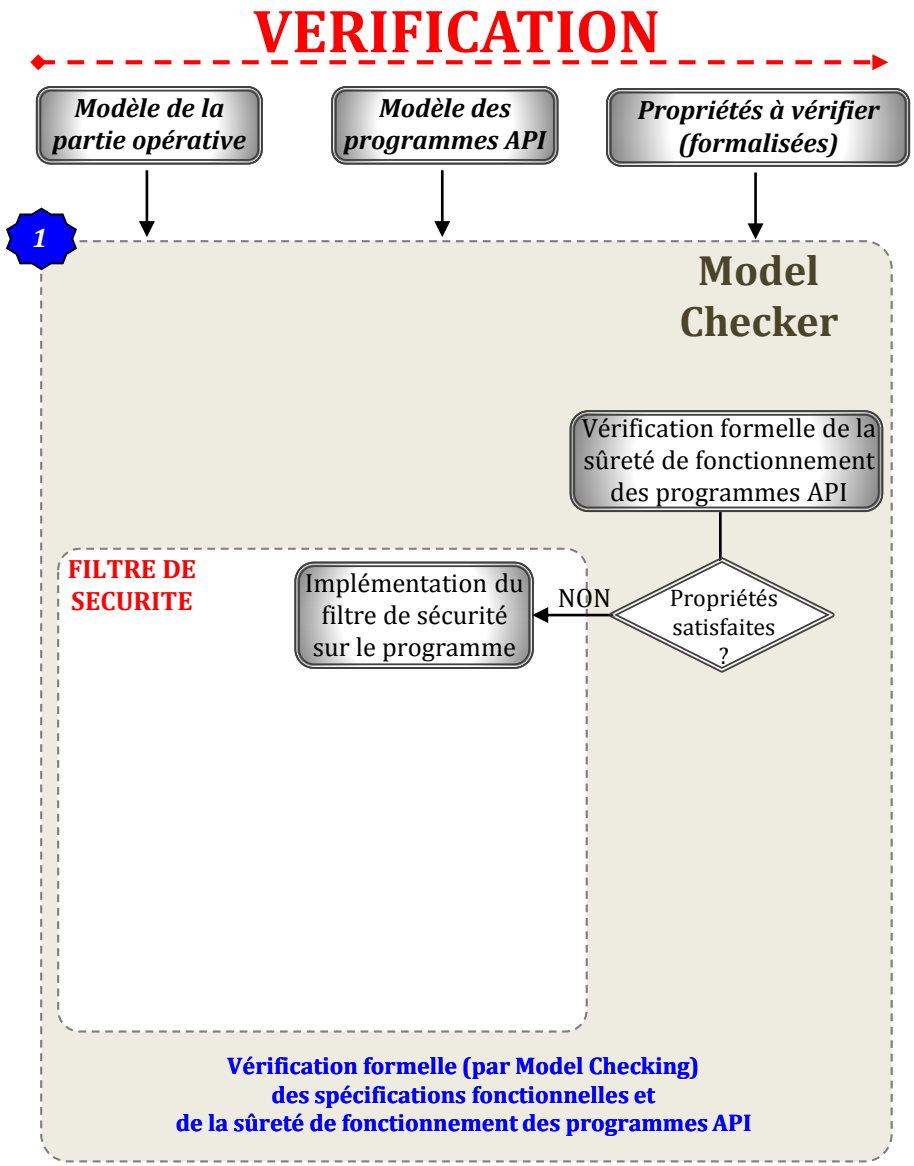
Vérification exhaustive ➔ grande quantité de mémoire utilisée ➔

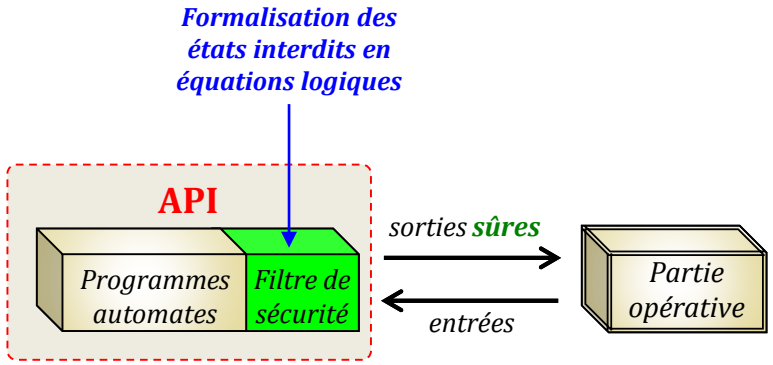
- ***Temps de simulation plus long***
- ***Explosion combinatoire***

<u>Solution</u> : utilisation d'un super calculateur combiné au model checker, pour multiplier la puissance de calcul

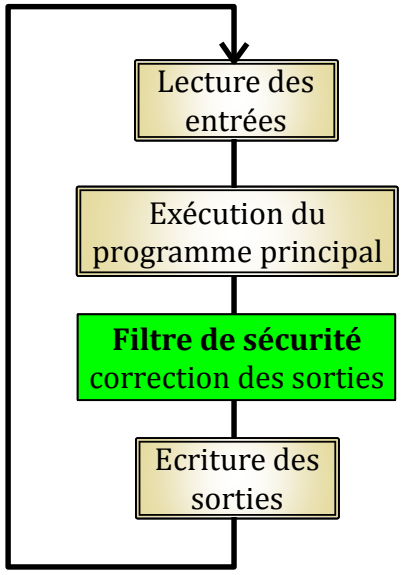
HPC Center ROMEO Centre de Calcul Régional

Vérification formelle des programmes API

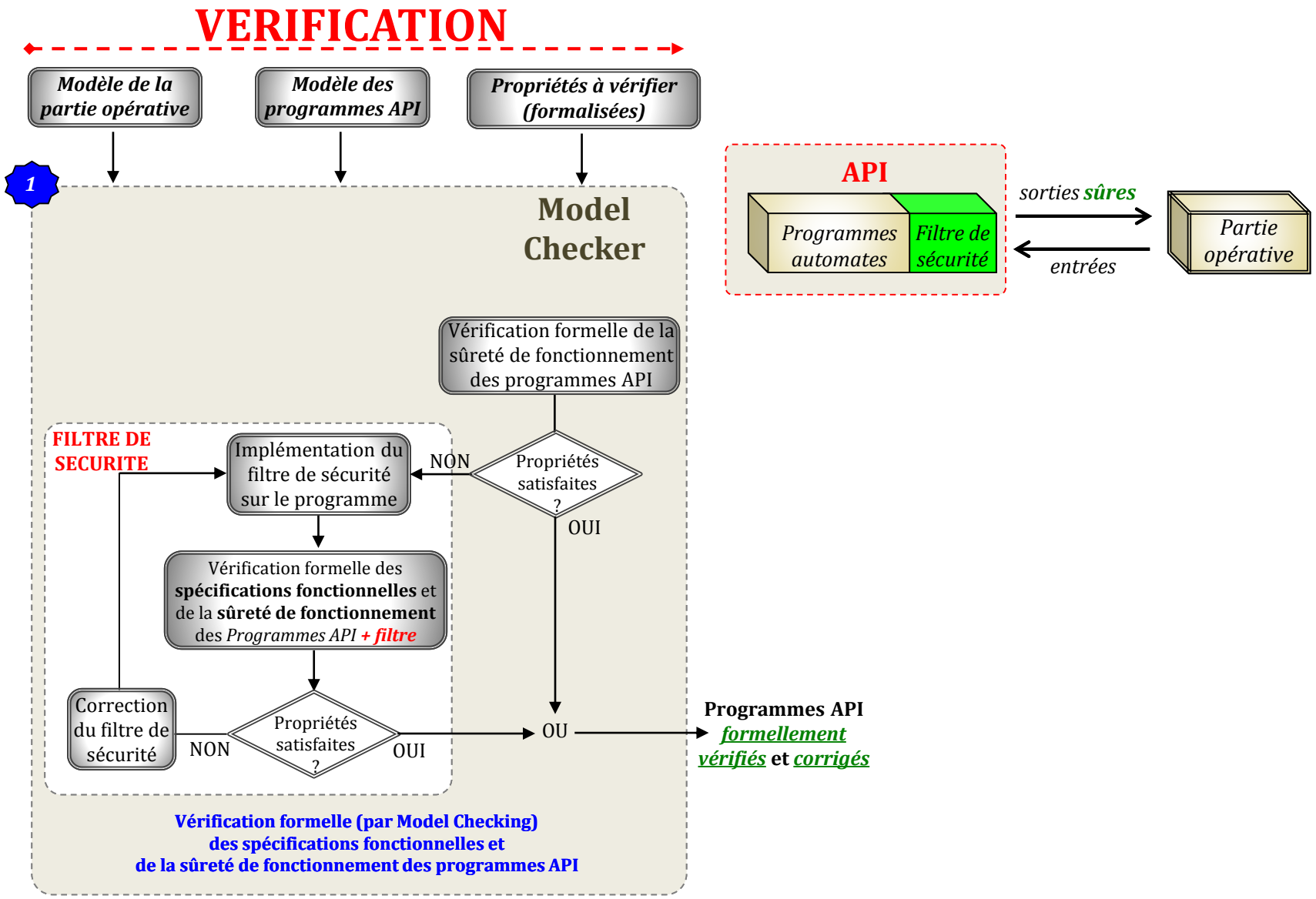




Filtre de sécurité *: garantit la sûreté de fonctionnement sans modifier le contenu du programme automate*



Vérification formelle des programmes API



OUTLINE

I. Introduction & Background

II. Formal Verification of Recipe book

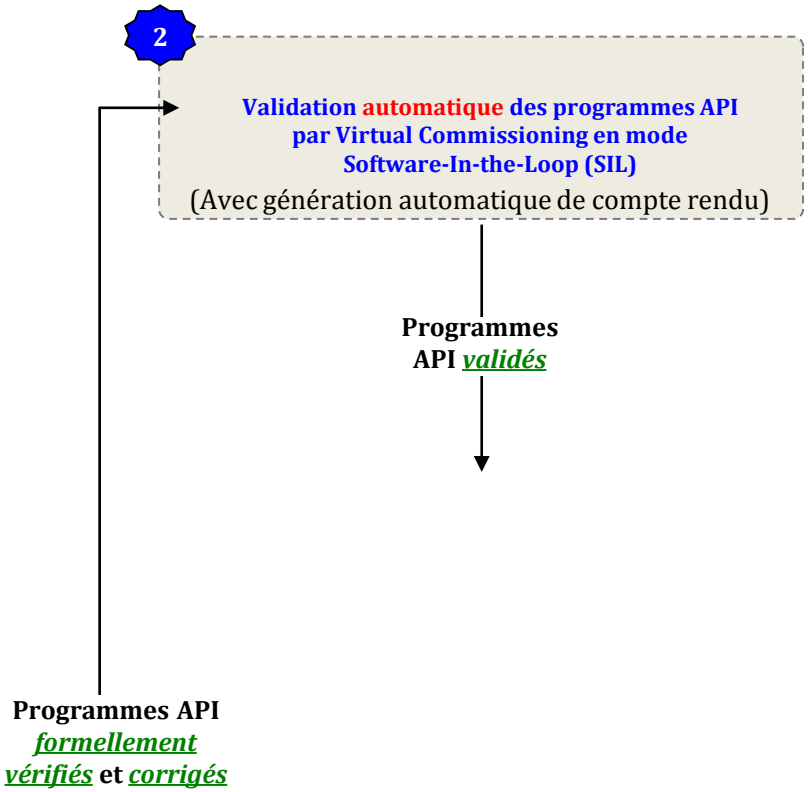
III. Virtual Commissioning

1. Validation of PLC programs through SIL simulations
2. Validation of electric cabinets through HIL simulations

IV. Conclusion

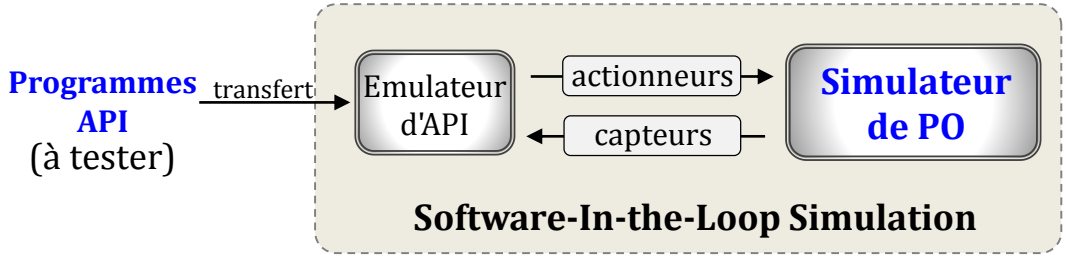
Validation automatique des programmes API

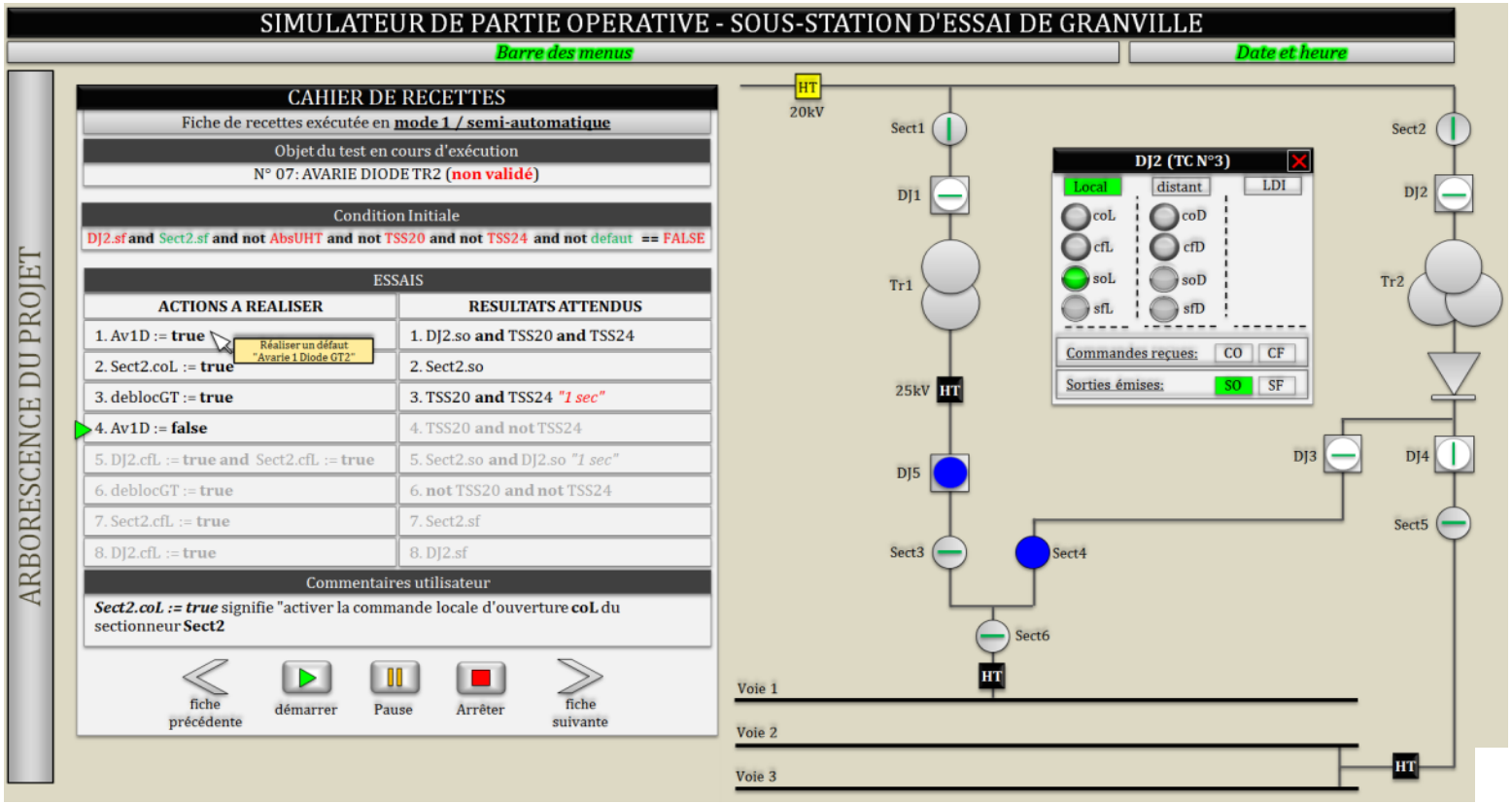
VERIFICATION **VALIDATION**



Validation automatique des programmes API

Solution basée sur l'architecture Software-In-the-Loop





Cahier de recettes numérisé

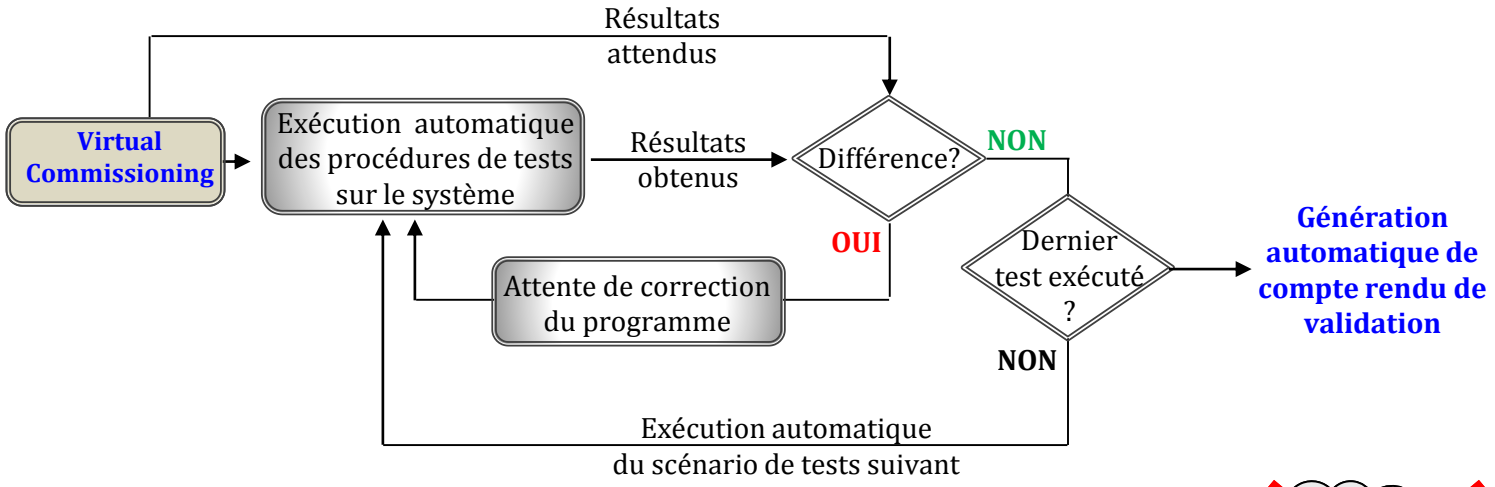
Modèle virtuel de l'EALE étudiée

odil

Validation automatique des programmes API

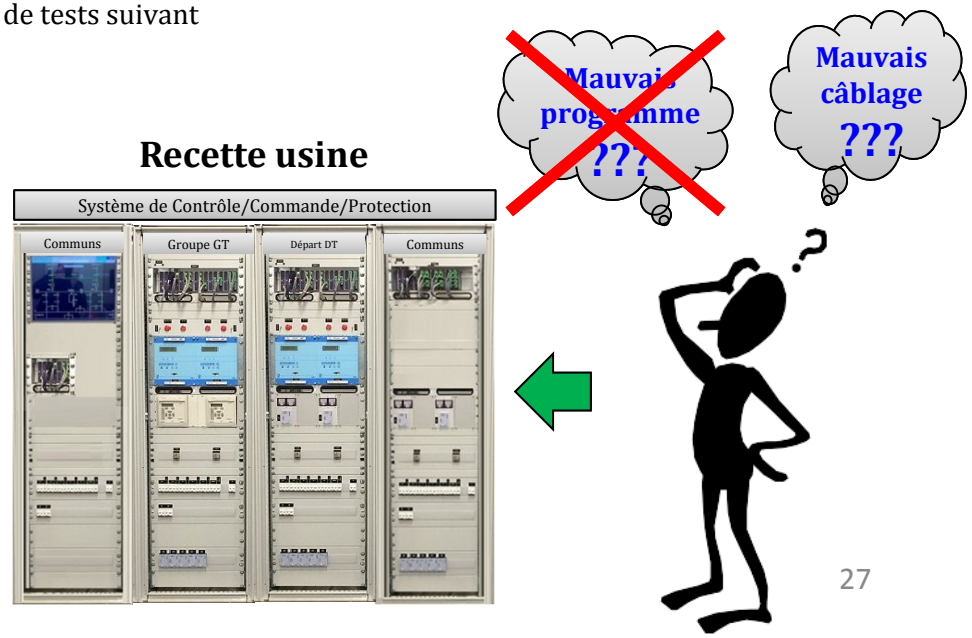
Principe de la validation automatique des programmes API

- ***Mode manuel*** *(commande manuelle de l'installation)*
- ***Mode « cahier de recettes »***



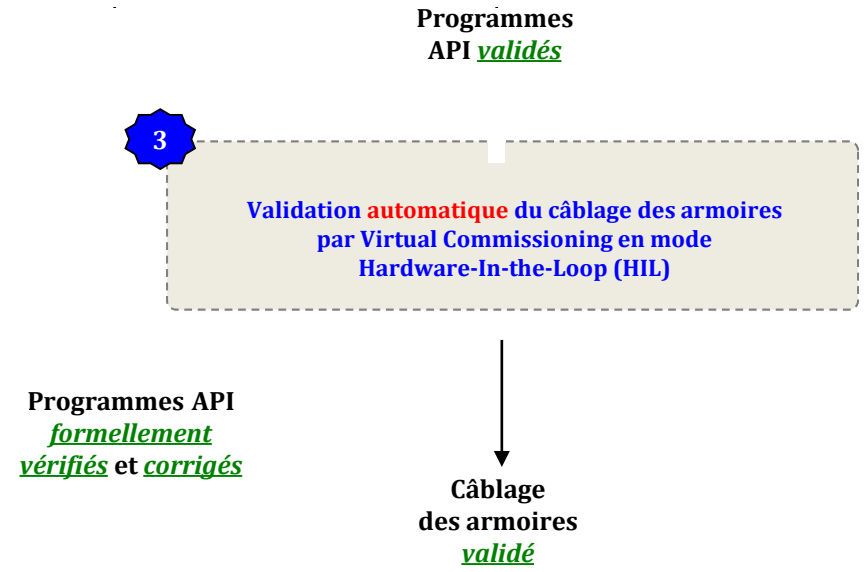
Avantages :

- *Validation en amont des programmes API*
- *Validation automatique (gain de temps…)*
- *Facilite la validation du câblage des armoires en usine*
- *Traçabilité, formation des nouveaux chargés d'études, réduction des coûts…*



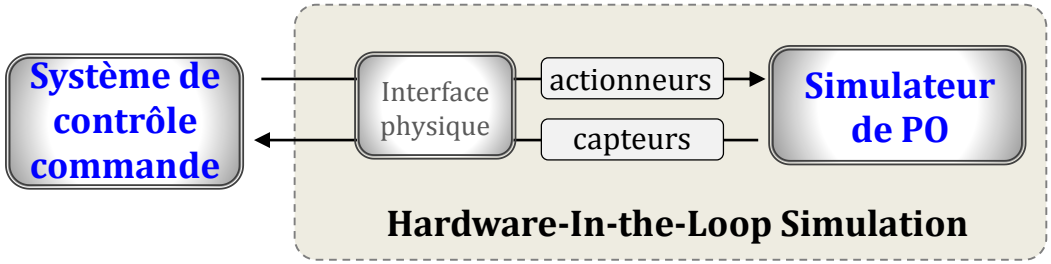
Validation automatique du câblage des armoires

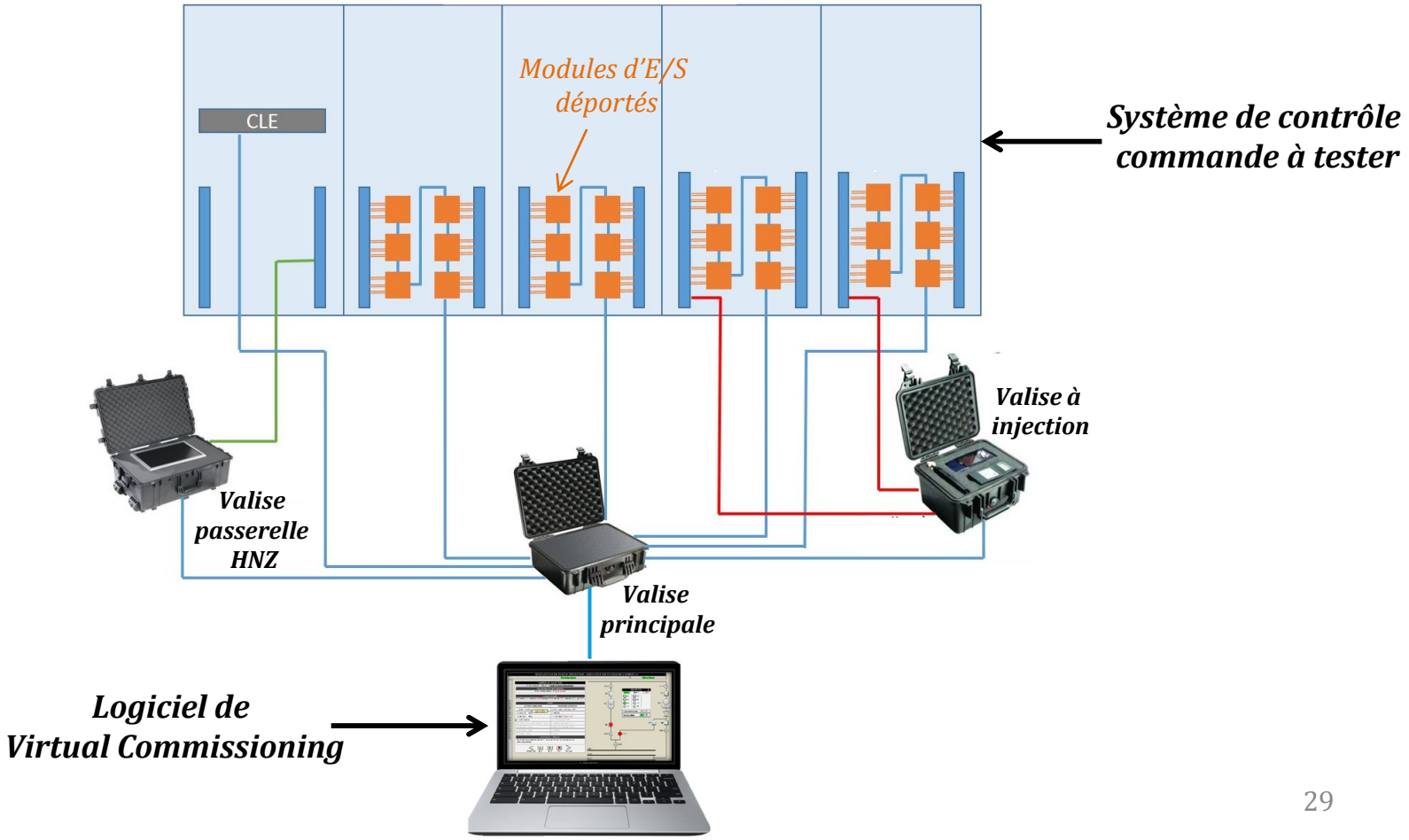
VERIFICATION — **VALIDATION**



Validation automatique du câblage des armoires

Solution basée sur l'architecture Hardware-In-the-Loop





CONCLUSION

Synthèse de la nouvelle approche de V&V formelle, automatisée, et méthodologique

La contribution de ce travail de recherche répond à **trois** objectifs :

- **Sécurité** : grâce à l'exhaustivité et l'automatisation de la V&V
- **Humain** : nécessite moins de temps et de ressources de la part des chargés d'études
- **Économique** : réduction des coûts de prestation, de correction grâce à la validation précoce par Virtual Commissioning

Inconvénient :

Complexité de la modélisation

- *erreurs humaines*
- *temps de modélisation*
- *tâche supplémentaires*

Perspectives :

- Traduction automatique des programmes API lors de la vérification formelle
- Enrichissement du cahier de recettes actuel grâce à la vérification exhaustive
- Application de l'approche méthodologique dans des systèmes manufacturiers

ACKNOWLEDGMENT