

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

Mohamed NIANG

Bernard RIERA

Alexandre PHILIPPOT



Serge Debernard



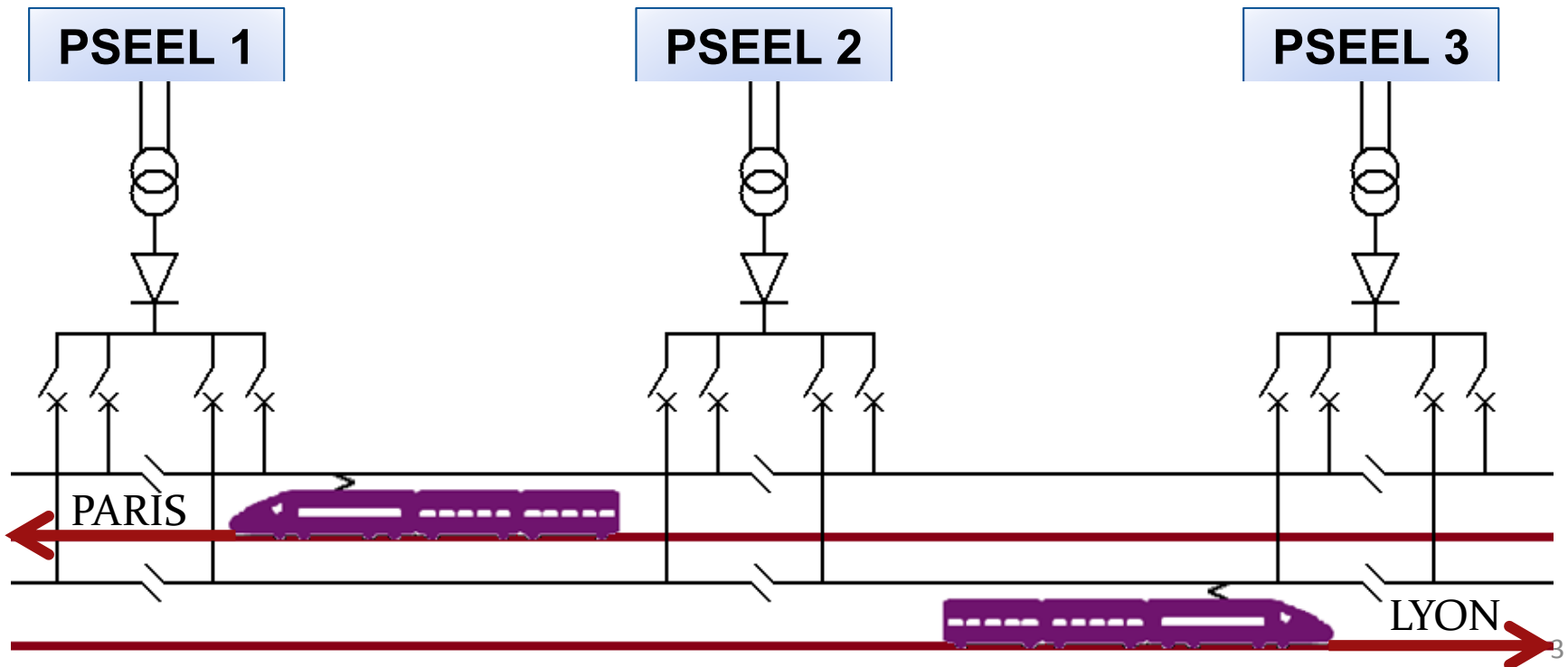
Introduction

- 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



SNCF :

- Management, exploitation et opération de l'infrastructure ferroviaire en France
- 30 000 Km de lignes,
- 560 sous-stations contenant les EALE (Equipements d'Alimentation des Lignes Électrifiées) - 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

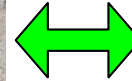
1. Validation of PLC programs through SIL simulations

2. Validation of electric cabinets through HIL simulations

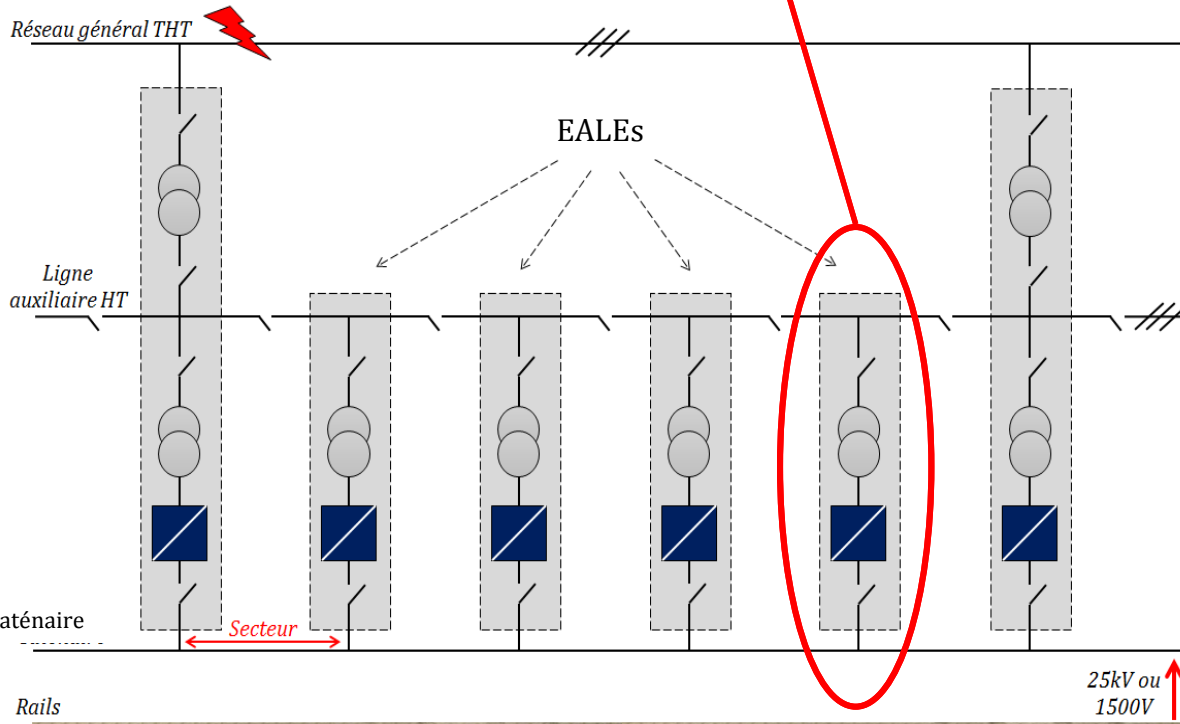
IV. Conclusion

INTRODUCTION

Contexte : Equipements d'Alimentation des Lignes Électrifiées (EALÉ)

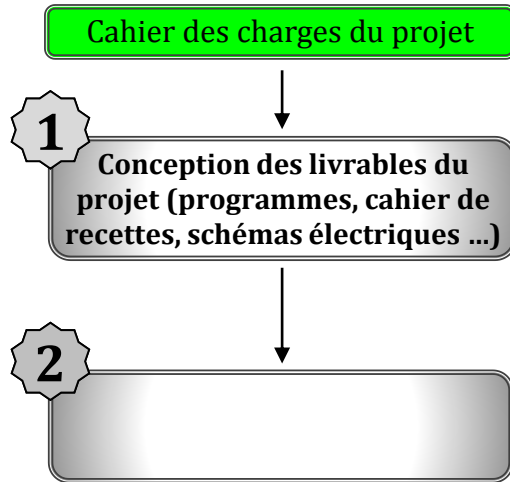


Chargé d'études SNCF



Métier des EALE et problématique

Workflow durant un projet d'automatisation d'EALE



Livrables d'un projet :

- Schémas électriques
- Programmes API
- Cahier de recettes

Procédure de tests N° ##

Fichier Edition Outils Options Aide

Debut: Initial Phase d'initialisation
 LectPara Lecture paramètres en ESPROM
 EcrPara Sortant des paramètres en ESPROM
 AcquiFIP Acquisition des ondes et des réflexes
 AcquiTSD Acquisition des entrées cartes TSD/TSD
 AcquiTSS Acquisition des entrées cartes TSS
 DefautES défaut cartes entrées/sorties

Séquentiel: AIG_S1 Aiguillage sectionneur S1
 AIG_DJGT Aiguillage disjoncteur GT
 AIG_SRB1 Aiguillage sectionneur groupe traction
 AIG_DIR Aiguillage Protection Directionnelle
 CDE_S1 Commande Sectionneur S1 (position)
 CDE_DJGT Commande disjoncteur GT
 CDE_SRB1 Commande sectionneur SRB1
 CDE_DIR Commande protection directionnelle
 DEF_GT Défaut groupe persistant
 MODBUS Envoi trames Modbus
 PGT Gestion PGT
 PGTEven Evénements POT numérique
 TELEGEST Informations Télégestion
 TransSur Traitement des sorties
 PCL_OUT Signalisations PCL
 FIP_OUT Signalisations FIP
 DEF_CT Raz des sorties sur défaut carte ES

Fin: DefaultST (Ladder Diagram)

Référence : GT1SST20
 Auteur : Mr. BLASZCZYK
 Date de création : 27/02/2014 12:54:39
 Numéro de version : 0
 Description : Groupe Traction 1 Sous-Station SSTsansNom

**alarmeGT:= Temp1TR or SF61;
 defTempGT:= defodeD1;
 blocageDefGT:= defTR or SF62;**

EcritureFIP:= ectsstfip[defProtGT1,TSSIMax,TSSRetour,TSSZMin,TSSDir,FALSE,alarmeGT,defTempGT,blocageDefGT,

ISaGRAF - GT1MOI20DEF_GT - Programme SFC

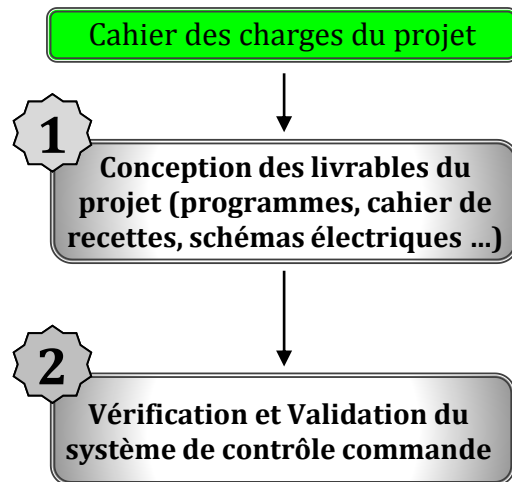
ISaGRAF - GT1MOI20DEFAULTGT - Programme Quick LD

ouverture DJ par défaut GT1

deTR
 DecDir
 SF62
 defodeD1
 DecIMax
 DecZMin
 deProtGT1

Métier des EALE et problématique

Workflow durant un projet d'automatisation d'EALE



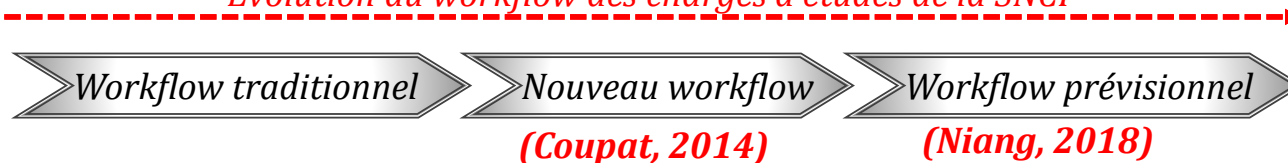
Livrables d'un projet :

- 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



Métier des EALE et problématique

Workflow traditionnel

Nouveau workflow

Workflow prévisionnel

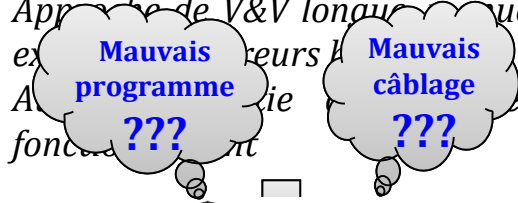
Problématiques du workflow traditionnel :

Etape 1:

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

Etape 2:

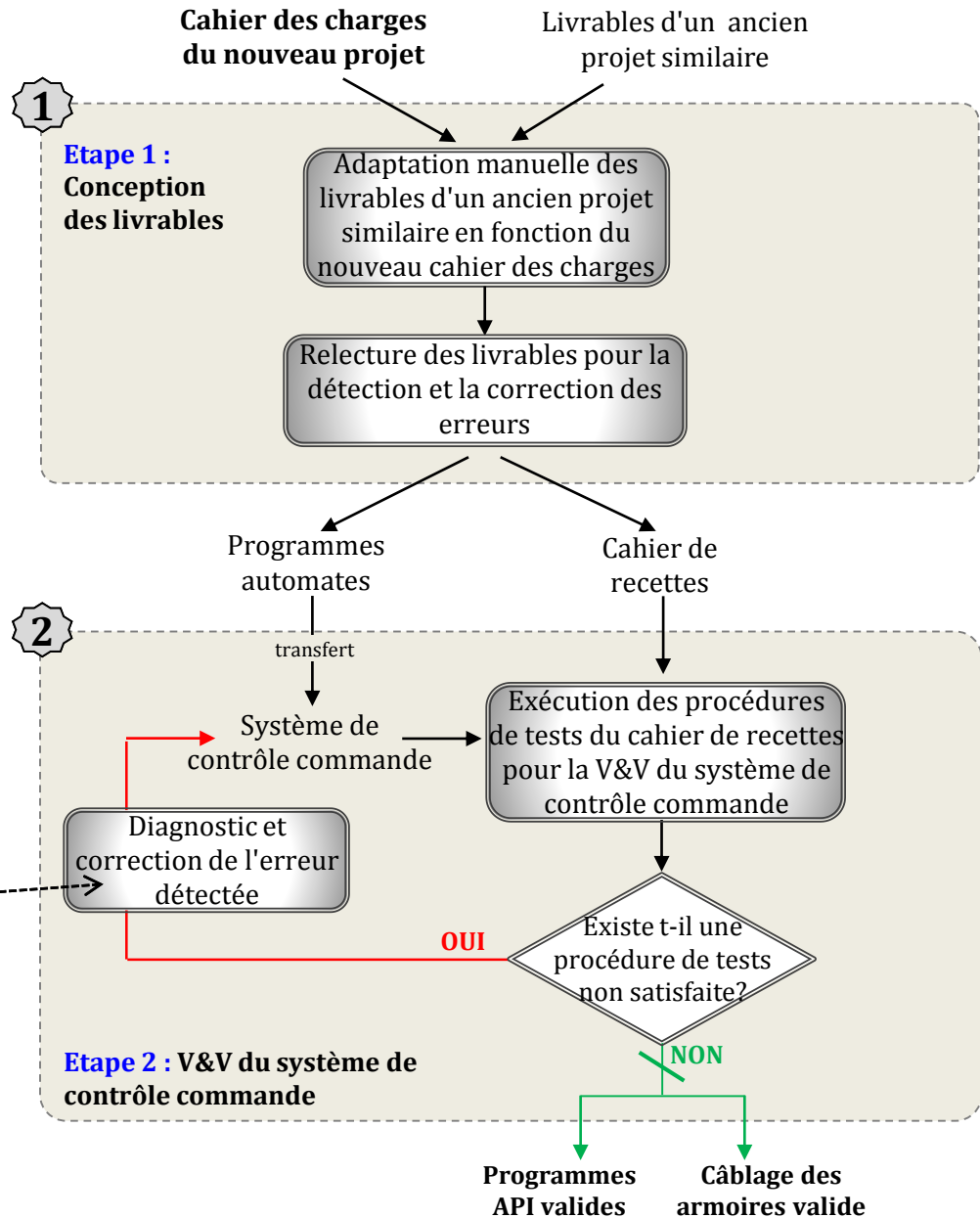
- Vérification des programmes par simple relecture
- Validation simultanément des programmes et du câblage
- Procédures de tests non exhaustives
- Approche de V&V longue et répétitive, et existence de nombreux défauts
- Absence de procédures de tests exhaustives



Ces incertitudes compromettent la fiabilité du contrôle



Les tests montrent l'absence de défauts » fiabilité et sécurité de commande

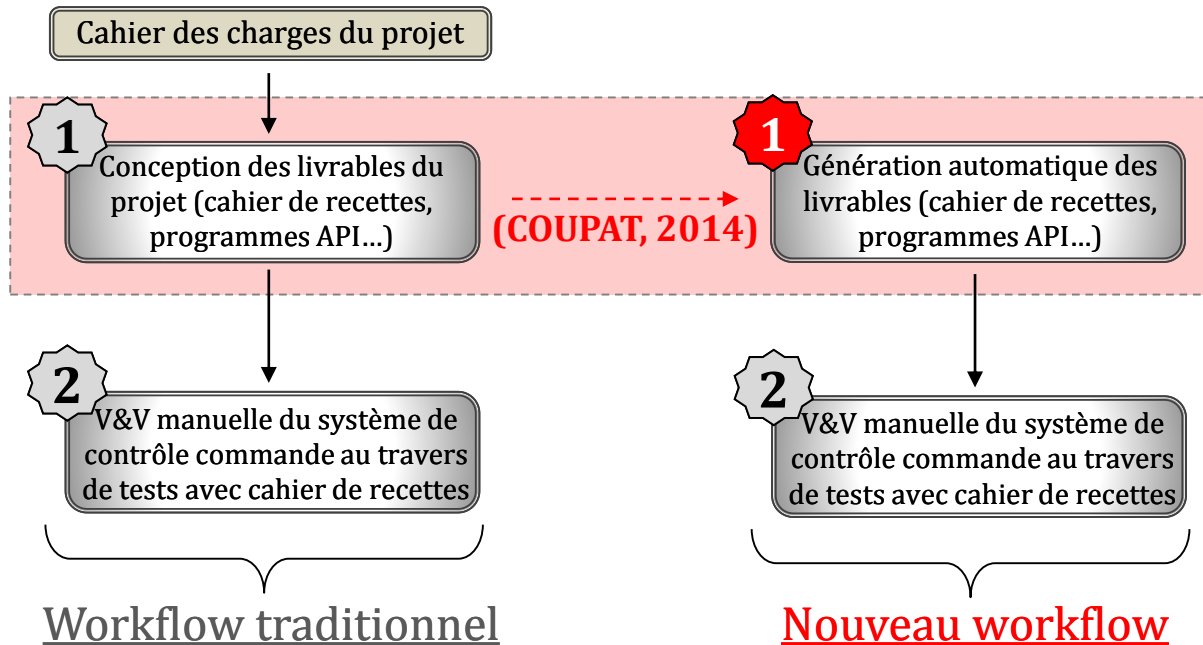


Métier des EALE et problématique

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

Cahier des charges du nouveau projet

Cahier des charges du nouveau projet

Livrables d'un projet similaire

Etape 1 : Génération

Description graphique du projet

Adaptation manuelle des livrables d'un ancien projet en fonction du cahier des charges

Vérification automatique de la cohérence des données saisies dans ODIL

Relecture des livrables pour la détection et la correction des erreurs

Correction manuelle des données d'entrée

NON

CO

Programmes automatés

Cahier de recettes

transfert

Système de contrôle commande

Exécution des procédures de tests du cahier de recettes pour la V&V du système de contrôle commande

Diagnostic et correction de l'erreur détectée

OUI

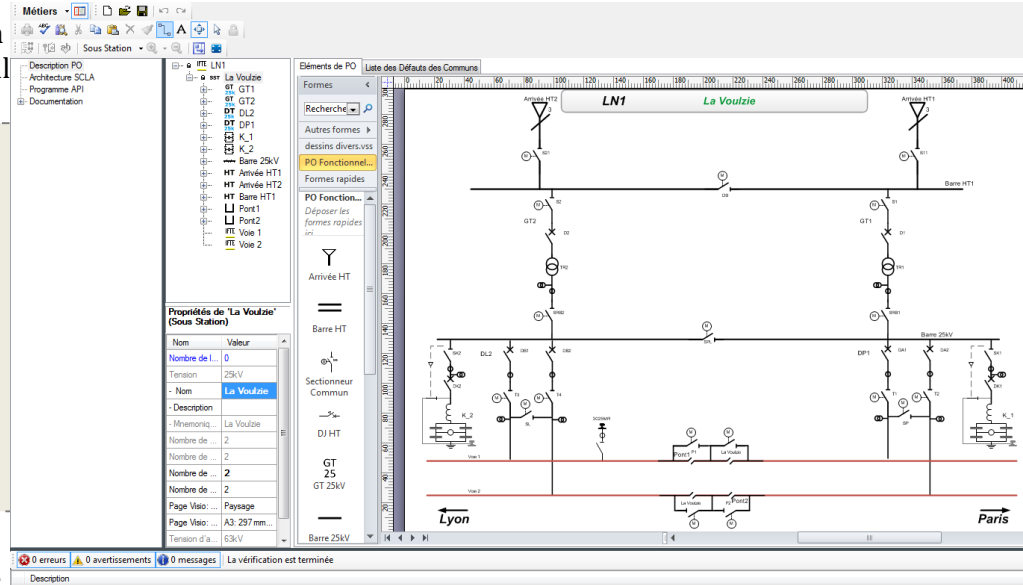
Existe-t-il une procédure de tests non satisfaite?

NON

Etape 2 : V&V du système de contrôle commande

Programmes API validés

Câblage des armoires valide



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

Métier des EALE et problématique

Workflow traditionnel

Nouveau workflow

Workflow prévisionnel

	Workflow traditionnel	Nouveau workflow
Phase 1 : Conception des livrables du projet	<ul style="list-style-type: none"> ○ Réalisation des schémas électriques----- 60h ○ Conception des programmes API----- 50h ○ Rédaction du cahier de recettes----- 40h ○ Relecture et correction des livrables----- 10h <p>Total des heures----- 160h</p>	<ul style="list-style-type: none"> ○ Réalisation des schémas électriques----- 60h ○ Génération des programmes API et du cahier de recettes avec ODIL----- 5h ○ Relecture des livrables générés----- 5h <p>Total des heures ----- 70h</p>
Phase 2 : V&V du système de contrôle commande	<ul style="list-style-type: none"> ○ Vérification du système de contrôle commande en usine ----- 40h ○ correction----- 20h ○ Validation du système de contrôle commande sur site----- 40h <p>Total des heures----- 100h</p>	<ul style="list-style-type: none"> ○ Vérification du système de contrôle commande en usine ----- 40h ○ correction----- 20h ○ Validation du système de contrôle commande sur site----- 40h <p>Total des heures----- 100h</p>

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

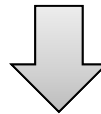
IV. Conclusion

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

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

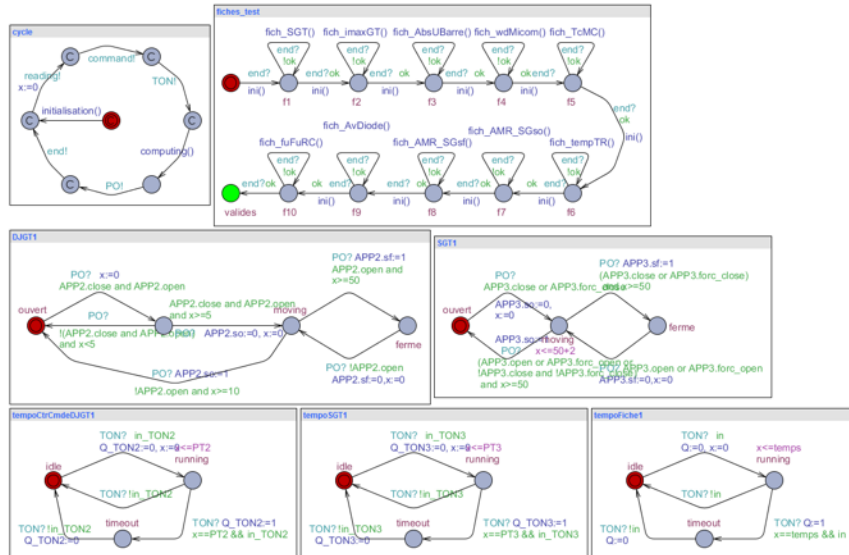
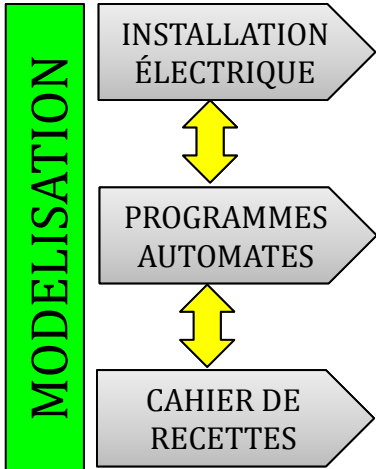
Méthode	Principe	Avantages	Inconvénients
Test	Exécution de procédures de tests	Très largement utilisée ; Facile à mettre en œuvre	Non exhaustive, longue, erreurs humaines...
Virtual Commissioning	Simulateur de Partie Opérative; Procédures de tests	Automatisation des tests, sécurité, traçabilité, gain 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***

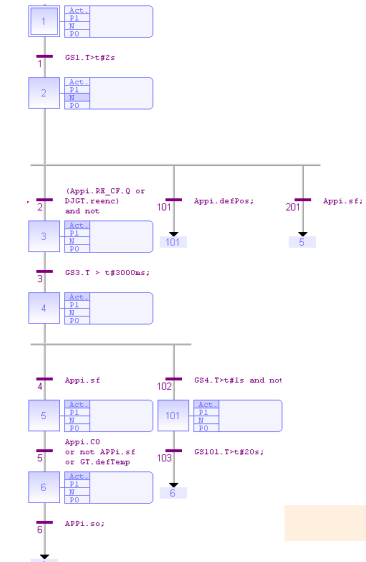
Méthodologie



- 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

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



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

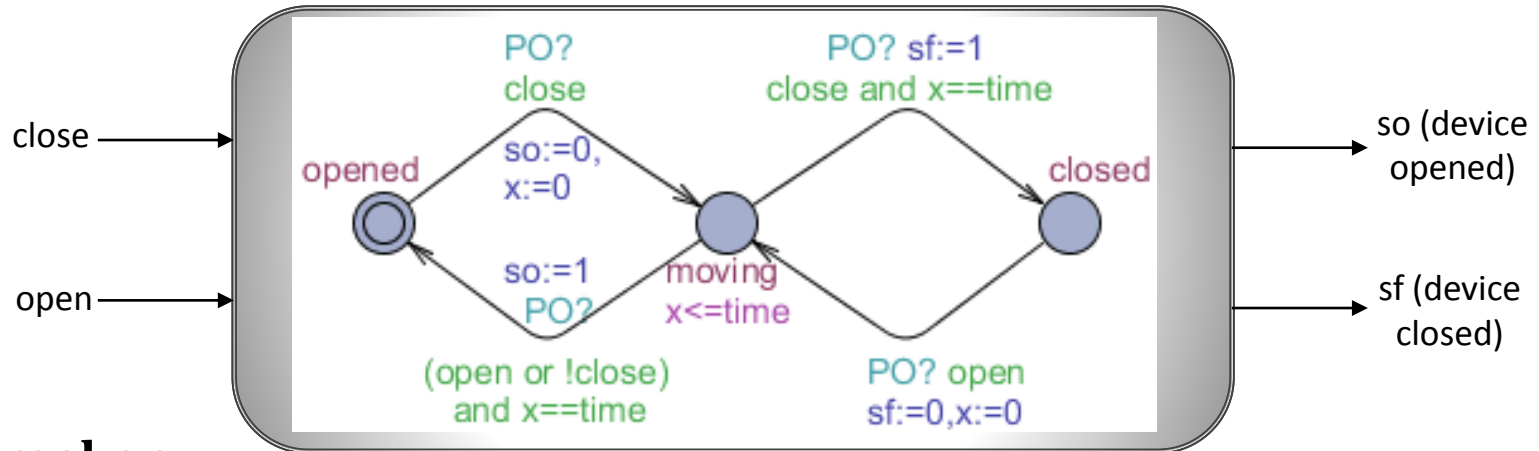
Décisions			
Usine	Correct : <input checked="" type="checkbox"/>	Génant : <input type="checkbox"/>	Bloquant : <input type="checkbox"/>
Site :	Correct : <input checked="" type="checkbox"/>	Génant : <input type="checkbox"/>	Bloquant : <input type="checkbox"/>
Test réalisé par		Usine : RB.ML	N° FFT :
		Site : FCB - ANS - RC	Date du test
			Usine : 25/08/11
			Site : 19/07/16

Formal verification of functional requirements

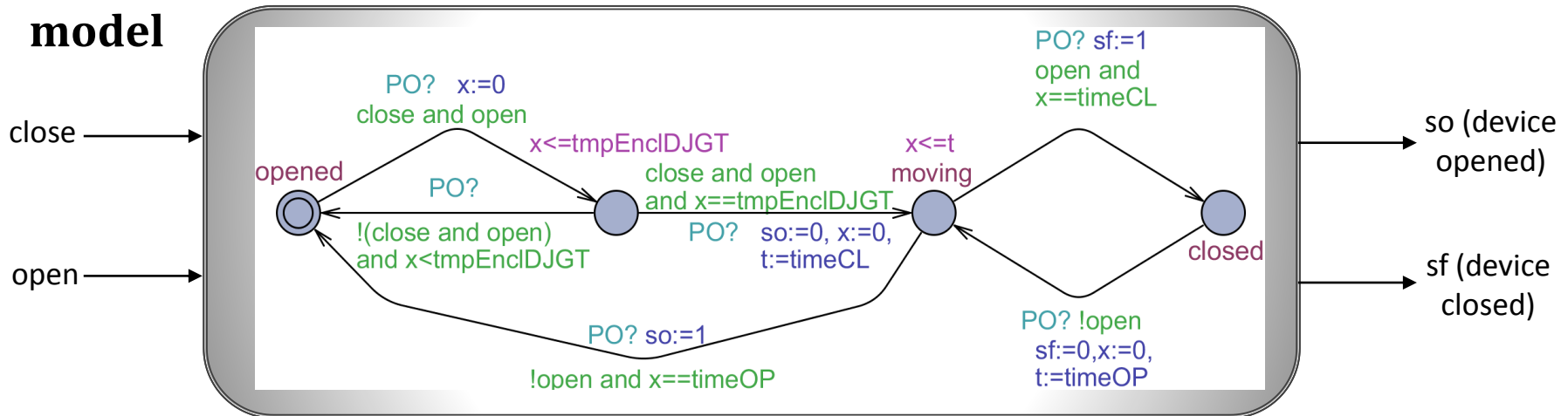
PSEEL's models: Instantiation of devices (20 types of devices) from 4 device categories:

➤ Abstract time discrete-events models

Switch model



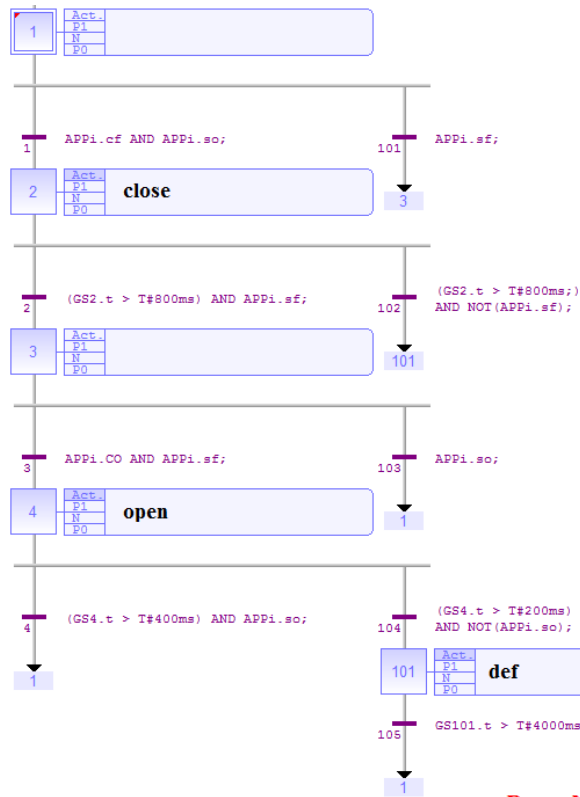
circuit-breaker model



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

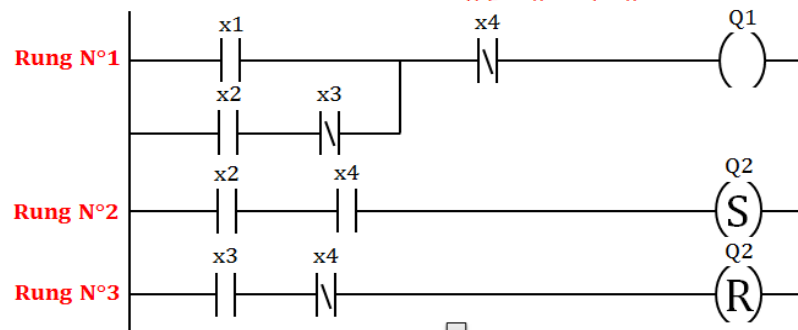
```
ft1 = x1 and so and CF;
ft2 = x2 and sf and Qtmp;
ft3 = x3 and sf and CO;
ft4 = x4 and so and Qtmp;
ft101 = x1 and sf;
ft102 = x2 and !sf and Qtmp;
ft103 = x3 and so;
ft104 = x4 and !so and Qtmp;
ft105 = x101 and Qtmp;
```

// 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

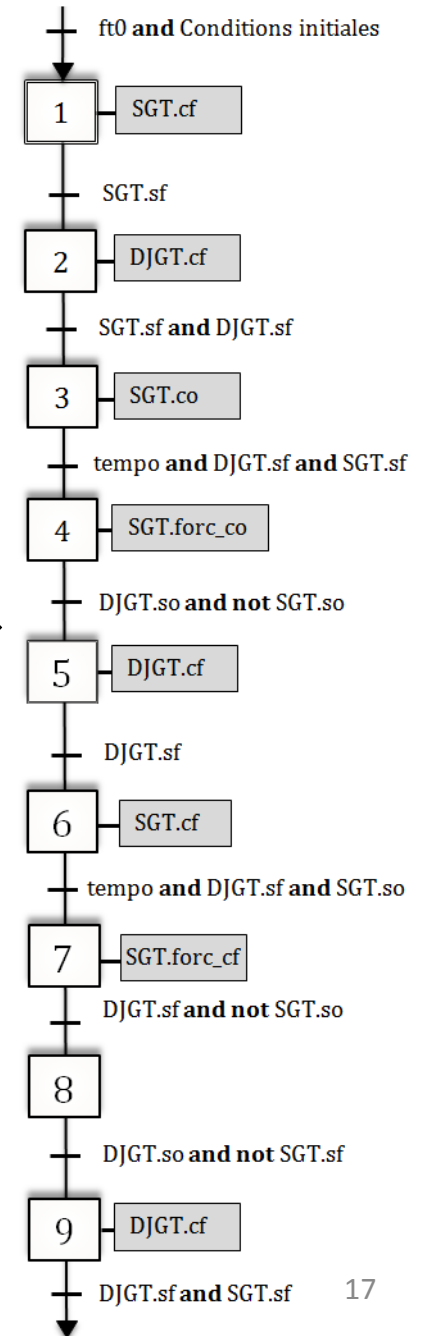
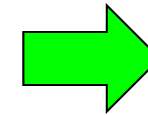
```
Q1 = (x1 or (x2 and not x3)) and not x4;
Q2 = (x2 and x4 ? 1 : Q2);
Q2 = (x3 and not x4 ? 0 : Q2);
```

**Translation of LD into
algebraic equations**

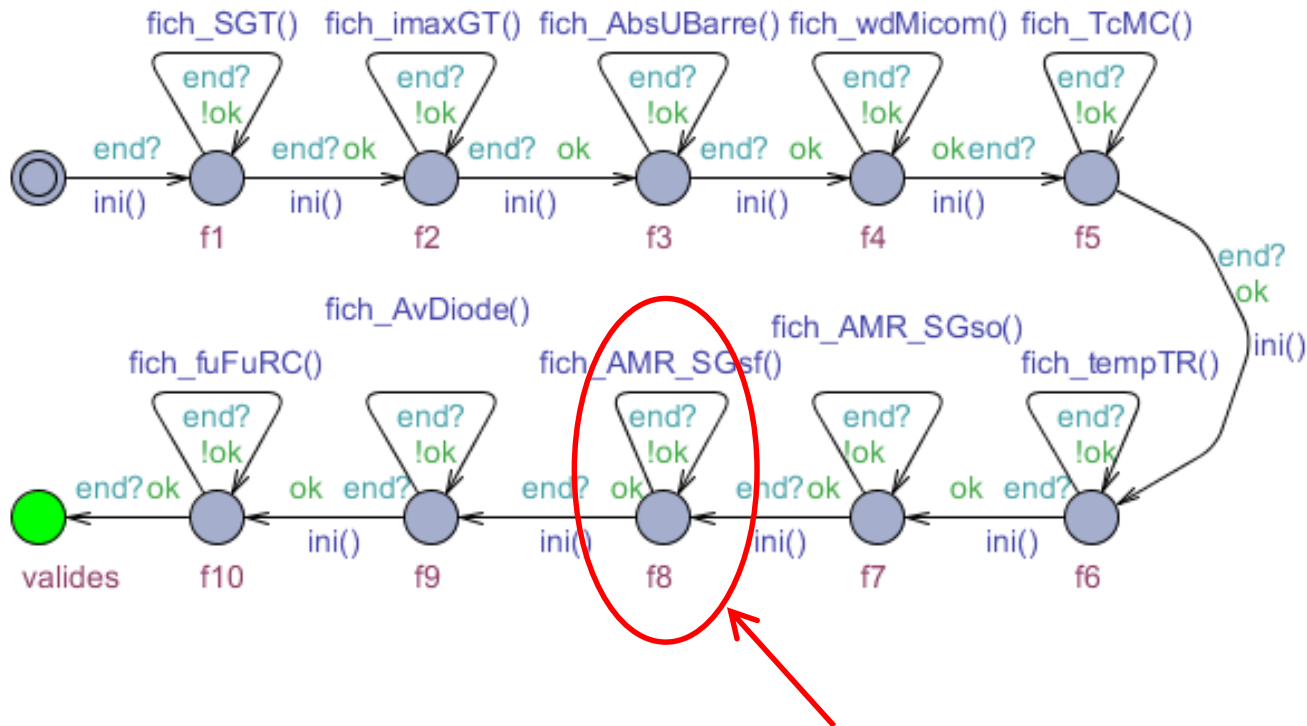
Formal verification of functional requirements

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							
<ul style="list-style-type: none"> ◆ 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. 2. Fermer le Disjoncteur DGT1 3. Ouvrir Sectionneur 1500 V SG1 depuis le CLE 4. Ouvrir Sectionneur 1500 V SG1 ⁽¹⁾ 5. Fermer le Disjoncteur DGT1 6. Fermer Sectionneur 1500 V SG1 depuis le CLE 7. Fermer Sectionneur 1500 V SG1 ⁽²⁾				1. Sectionneur 1500 V SG1 fermé 2. Disjoncteur DGT1 fermé 3. Néant 4. Ouverture Disjoncteur DGT1 avant séparation des contacts de puissance du sectionneur 5. Disjoncteur DGT1 fermé 6. Néant 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				⁽¹⁾ Faire une ouverture manuelle du sectionneur SG1			
⁽²⁾ Pour fermer le sectionneur SG1 baisser le compact SG1.S				⁽²⁾ Faire une fermeture manuelle du sectionneur SG1			
Décisions							
Usine	Correct : <input checked="" type="checkbox"/>	Gênant : <input type="checkbox"/>	Bloquant : <input type="checkbox"/>	N° FFT :			
Site :	Correct : <input checked="" type="checkbox"/>	Gênant : <input type="checkbox"/>	Bloquant : <input type="checkbox"/>				
Test réalisé par		Usine : RB. NL	Date du test	Usine : 25/08/15			
		Site : RB. AB. BC		Site : 19/07/16			



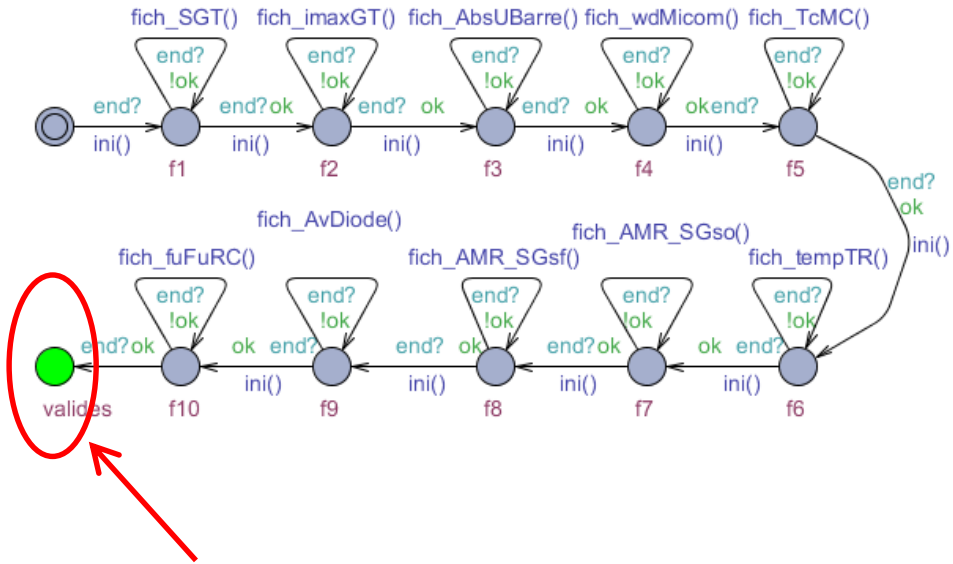
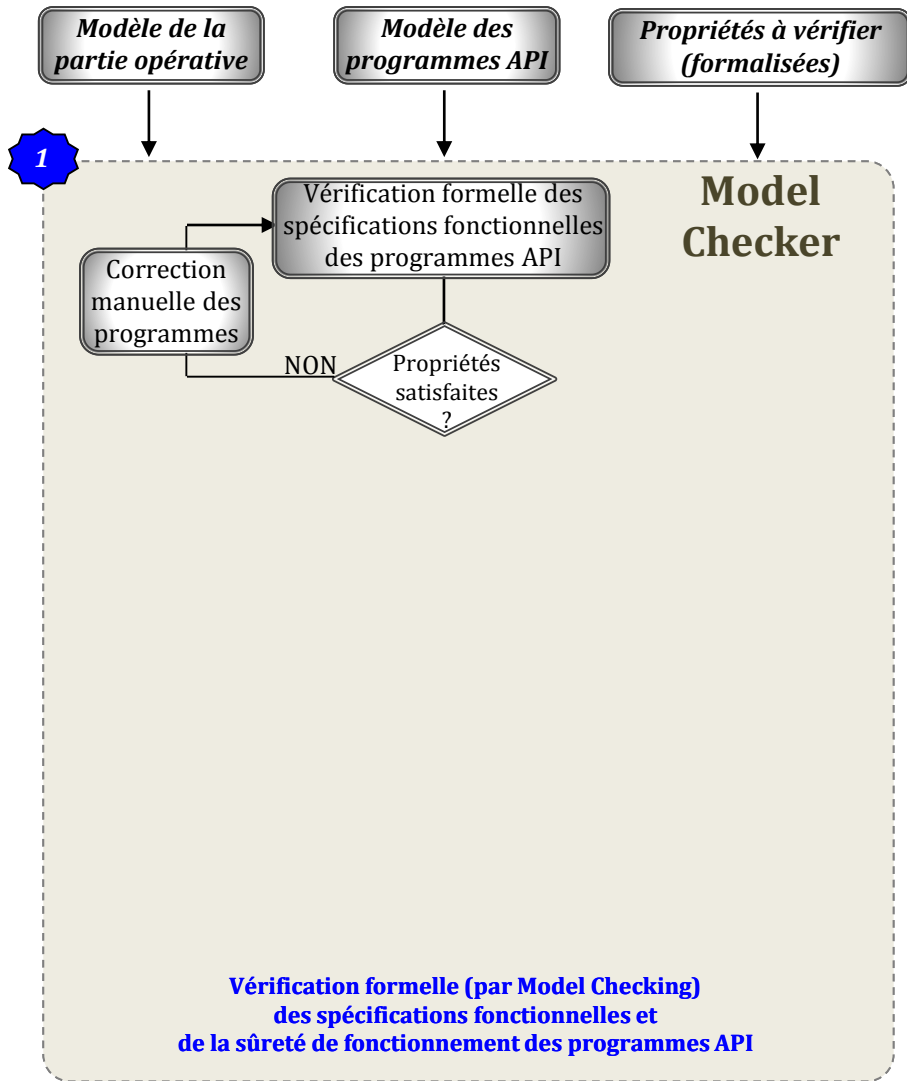
Vérification formelle des programmes API



Fiche de test Réf.						Objet du test	
D	B	01	F	N	U/S	Sectionneur Groupe GT1 SG1	
Condition Initiales							
<ul style="list-style-type: none"> ◆ 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. 2. Fermer le Disjoncteur DGT1 3. Ouvrir Sectionneur 1500 V SG1 depuis le CLE 4. Ouvrir Sectionneur 1500 V SG1 ⁽¹⁾ 5. Fermer le Disjoncteur DGT1 6. Fermer Sectionneur 1500 V SG1 depuis le CLE 7. Fermer Sectionneur 1500 V SG1 ⁽²⁾				1. Sectionneur 1500 V SG1 fermé 2. Disjoncteur DGT1 fermé 3. Néant 4. Ouverture Disjoncteur DGT1 avant séparation des contacts de puissance du sectionneur 5. Disjoncteur DGT1 fermé 6. Néant 7. Ouverture Disjoncteur DGT1 avant établissement des contacts de puissance du sectionneur			
Commentaires							
Usine ⁽¹⁾ Pour ouvrir le sectionneur SG1 baisser le compact SG1.S ⁽²⁾ Pour fermer le sectionneur SG1 baisser le compact SG1.S				Site ⁽¹⁾ Faire une ouverture manuelle du sectionneur SG1 ⁽²⁾ Faire une fermeture manuelle du sectionneur SG1			
Décisions							
Usine		Correct : <input checked="" type="checkbox"/>	Géant : <input type="checkbox"/>	Bloquant : <input type="checkbox"/>	N° FFT :		
Site		Correct : <input checked="" type="checkbox"/>	Géant : <input type="checkbox"/>	Bloquant : <input type="checkbox"/>			
Test réalisé par				Usine : RB. NL	Date du test		Usine : 15/08/11
				Site : (13. AVS. RC			Site : 19/10/11

Vérification formelle des programmes API

VERIFICATION

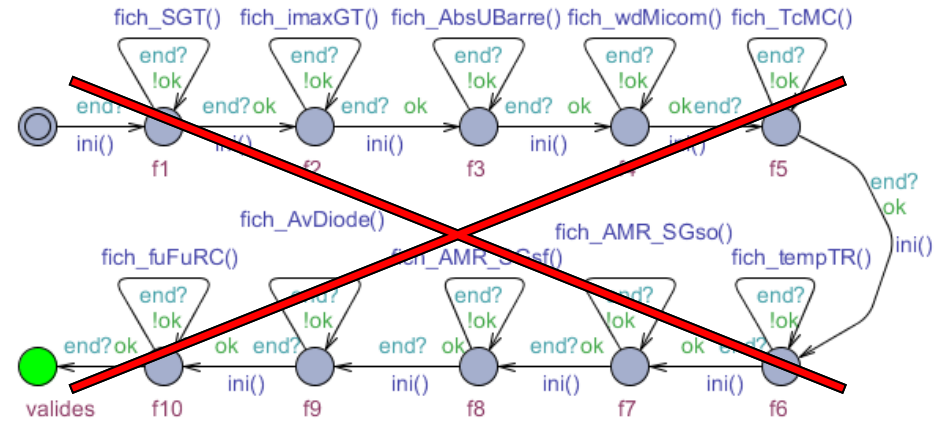
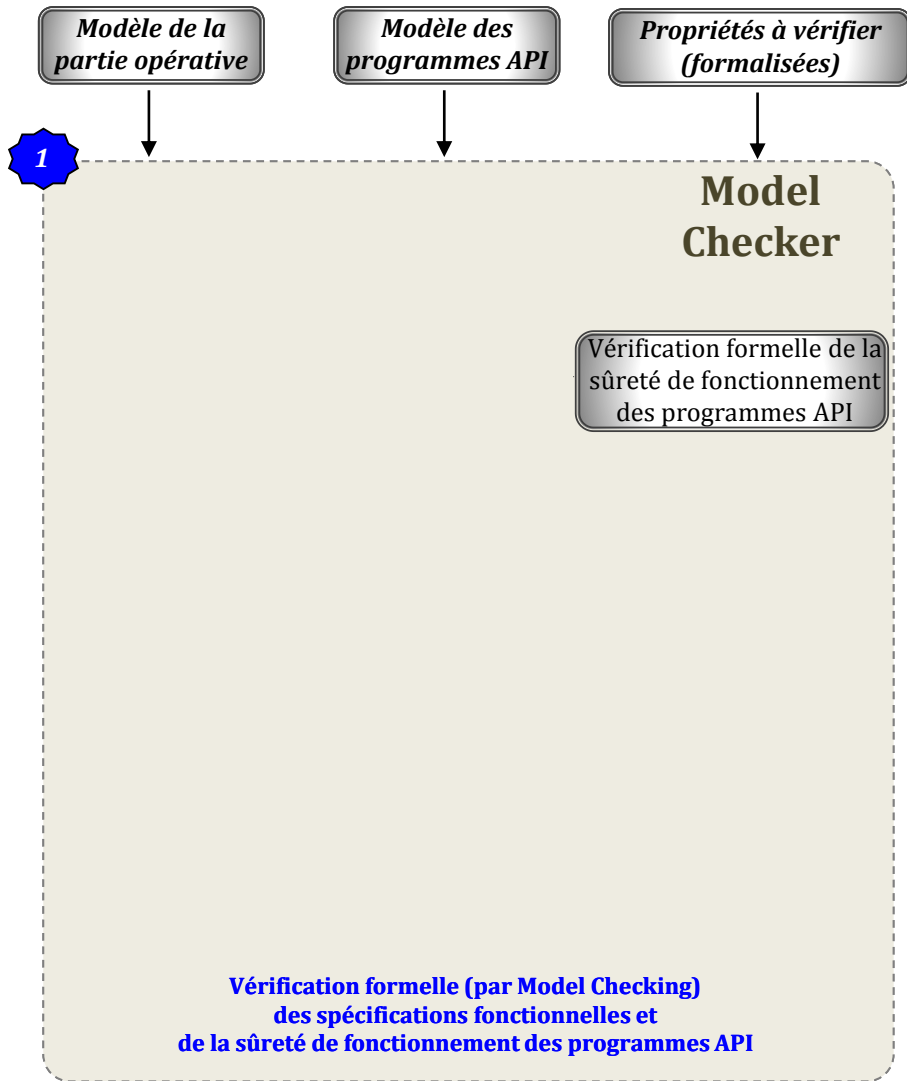


Atteignable ?

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

Vérification formelle des programmes API

VERIFICATION



Vérification formelle des programmes API

Éditeur Simulateur Simulateur concret Vérifieur Yggdrasil

Transitions actives

TON: cycle → tempoCtrCdeDJ2A

Suivant Reset

Trace de la simulation

(, opened, closed, opened, closed, ...)

Fichier de trace:

Préc. Suiv. Rejouer

Ouvrir Enreg. Auto

Global variables >

APP1

- so = 1
- sf = 0
- open = 0
- close = 0
- cod = 0
- cfd = 1
- flagCO = 0
- flagCF = 0
- forc_open = 0
- forc_close = 0
- def = 0

APP2

APP5

APP6

DT1

DT2

AssV1

AssV2

grafCtrCdeDj1AsservFP_C

grafCtrCdeDj2AsservFP_C

grafCmdeIT1

- x1 = 0
- x2 = 1
- x3 = 0
- x4 = 0
- x101 = 0
- flagCO = 0
- flagCF = 0

grafCmdeIT2

grafAsservFPV1_Old

grafAsservFPV2_Old

ReencDJDTV1

- x1 = 1
- x2 = 0
- x3 = 0
- x4 = 0
- x5 = 0

ReencDJDTV2

DJGT1

IT1

DJGT2

IT2

<<Constrains>

The diagrams illustrate the state transitions and constraints for various components in the API verification process. Key elements include:

- cycle:** A circular state machine with states 'initialisation()', 'computing()', and 'end!'. Transitions are labeled with 'reading!', 'command!', and 'PO!'. A constraint $x \leq 20$ is shown.
- DJGT1, DJGT2:** State transition graphs for DJGT1 and DJGT2, showing states like 'opened', 'moving', and 'closed'. Transitions are labeled with 'APP1.close and APP1.open' and 'APP5.close and APP5.open'. Constraints include $x \leq 10$, $x \leq t$, and $t = 50$.
- IT1, IT2:** State transition graphs for IT1 and IT2, showing states like 'opened', 'moving', and 'closed'. Transitions are labeled with 'APP2.close' and 'APP6.close'. Constraints include $x \leq 50$ and $APP2.sf = 1$.
- a1-a8:** Smaller state transition graphs (a1 through a8) showing specific state transitions and constraints for components like DT1, DT2, AssV1, AssV2, APP5, and APP6.

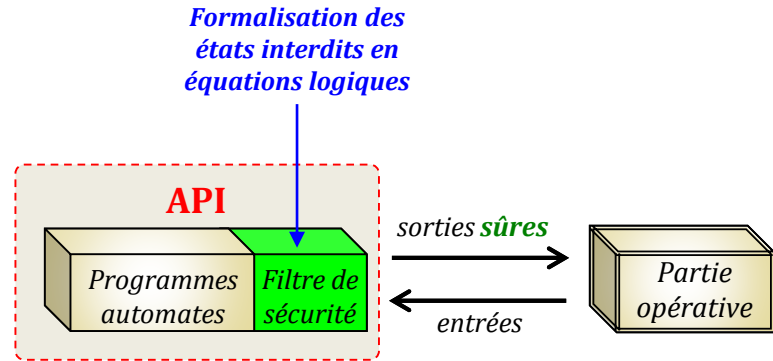
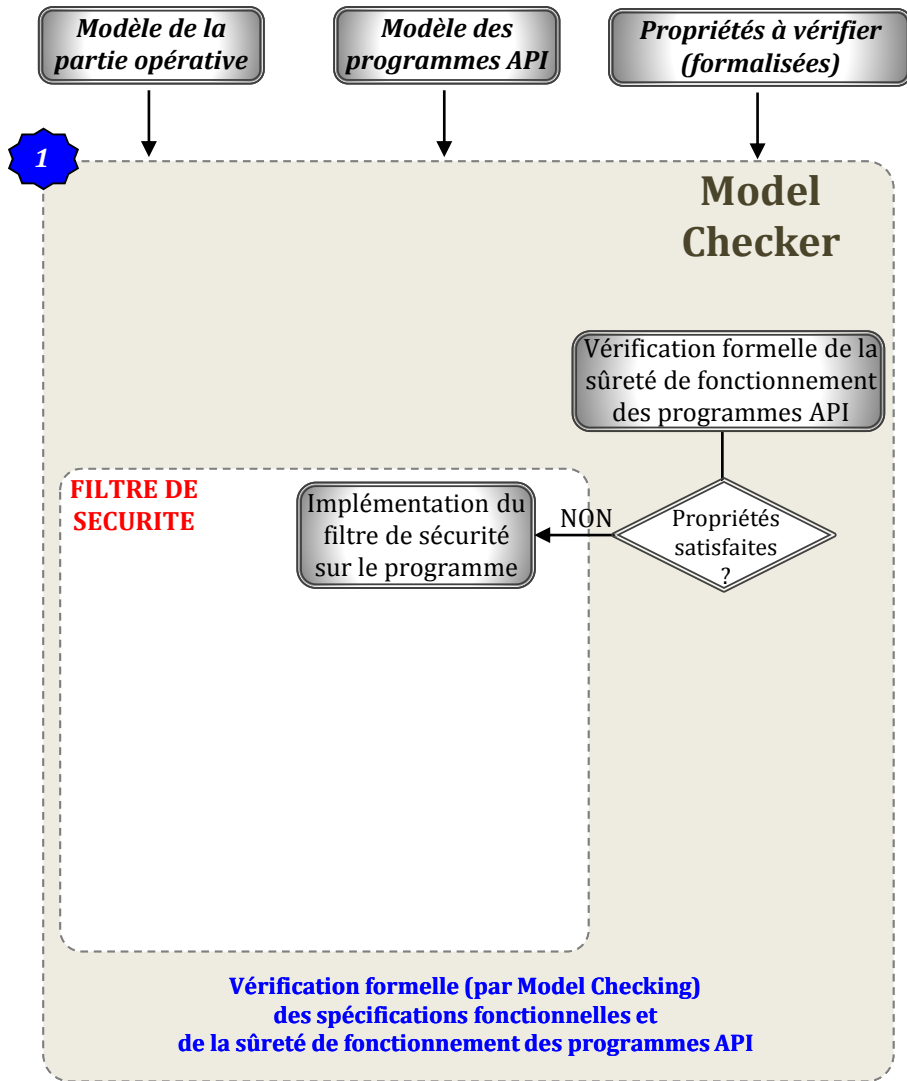
Vérification exhaustive → grande quantité de mémoire utilisée →

- Temps de simulation plus long
- Explosion combinatoire

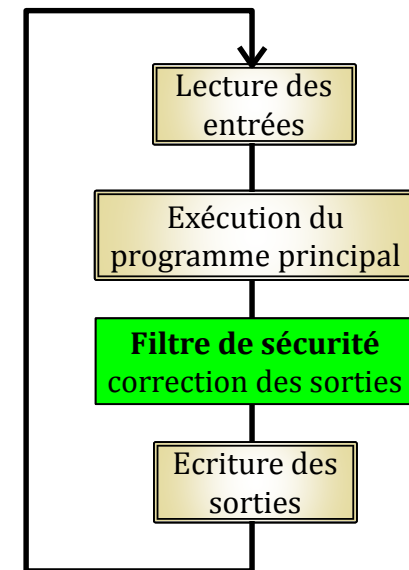
Solution : utilisation d'un super ordinateur combiné au model checker, pour multiplier la puissance de calcul

Vérification formelle des programmes API

VERIFICATION

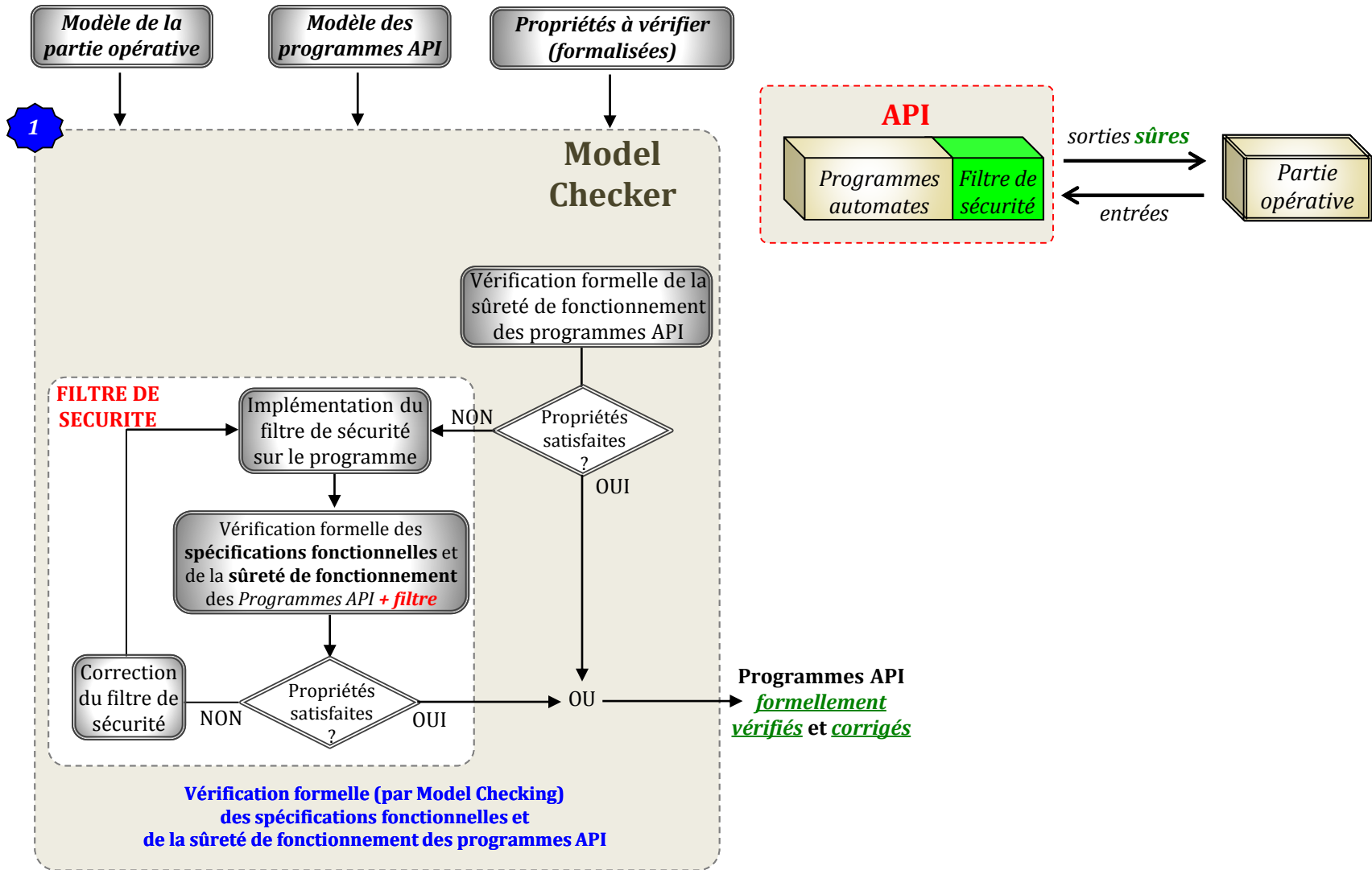


Filtre de sécurité : garantit la sûreté de fonctionnement sans modifier le contenu du programme automate



Vérification formelle des programmes API

VERIFICATION



OUTLINE

I. Introduction & Background

II. Formal Verification of Recipe book

III. Virtual Commissioning

1. Validation of PLC programs through SIL simulations

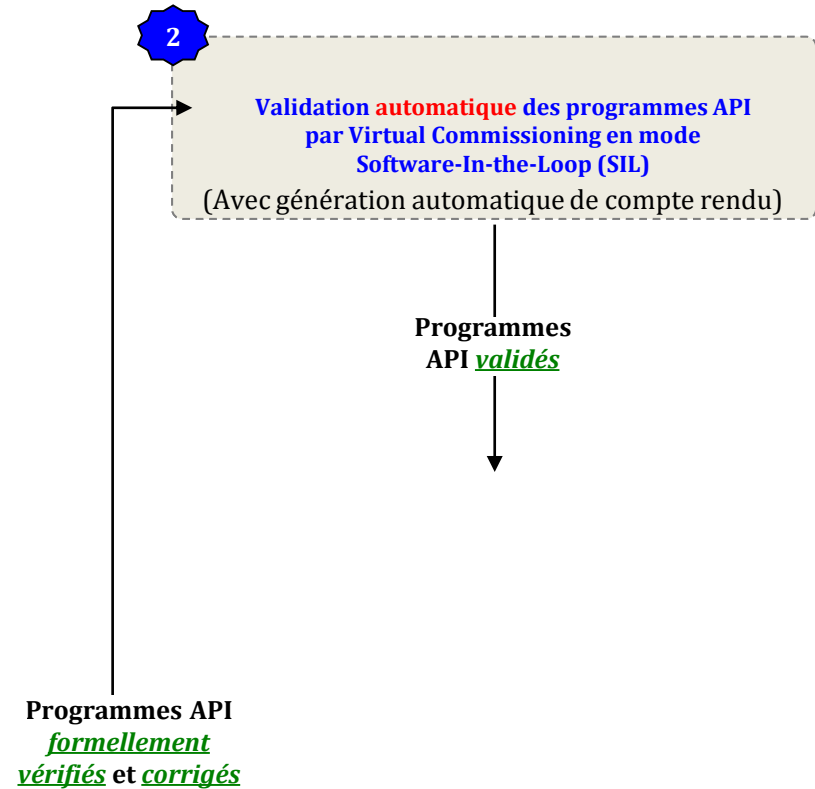
2. Validation of electric cabinets through HIL simulations

IV. Conclusion

Validation automatique des programmes API

←-----**VERIFICATION**----->

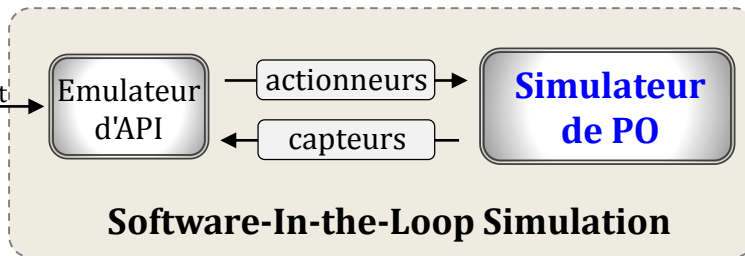
←-----**VALIDATION**----->



Validation automatique des programmes API

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

Programmes API
(à tester)



The screenshot shows the 'SIMULATEUR DE PARTIE OPERATIVE - SOUS-STATION D'ESSAI DE GRANVILLE' interface. It features a 'Barre des menus' at the top and a 'Date et heure' display. The main area is divided into two panels: a 'CAHIER DE RECETTES' (Recipe Book) on the left and a 'Modèle virtuel de l'EALÉ étudiée' (Virtual model of the studied EALÉ) on the right.

CAHIER DE RECETTES

Fiche de recettes exécutée en **mode 1 / semi-automatique**

Objet de test en cours d'exécution
N° 07: AVARIE DIODE TR2 (**non validé**)

Condition Initiale
`DJ2.sf and Sect2.sf and not AbsUHT and not TSS20 and not TSS24 and not default == FALSE`

ESSAIS	
ACTIONS A REALISER	RESULTATS ATTENDUS
1. Av1D := true	1. DJ2.so and TSS20 and TSS24
2. Sect2.coL := true	2. Sect2.so
3. deblocGT := true	3. TSS20 and TSS24 "1 sec"
4. Av1D := false	4. TSS20 and not TSS24
5. DJ2.cfl := true and Sect2.cfl := true	5. Sect2.so and DJ2.so "1 sec"
6. deblocGT := true	6. not TSS20 and not TSS24
7. Sect2.cfl := true	7. Sect2.sf
8. DJ2.cfl := true	8. DJ2.sf

Commentaires utilisateur
`Sect2.coL := true` signifie "activer la commande locale d'ouverture `coL` du sectionneur `Sect2`"

Navigation: < fiche précédente, démarrage, Pause, Arrêter, > fiche suivante

Modèle virtuel de l'EALÉ étudiée

The virtual model shows a power system diagram with components like Sect1, DJ1, Tr1, 25kV HT, DJ5, Sect3, Sect4, Sect6, Voie 1, Voie 2, Voie 3, DJ2, Tr2, DJ3, DJ4, and Sect5. A dialog box for 'DJ2 (TC N°3)' is open, showing control options: Local (selected), distant, LDI, and status indicators for coL, cfl, sol, sfl, coD, cfd, soD, and sfd. It also displays 'Commandes reçues: CO CF' and 'Sorties émises: SO SF'.

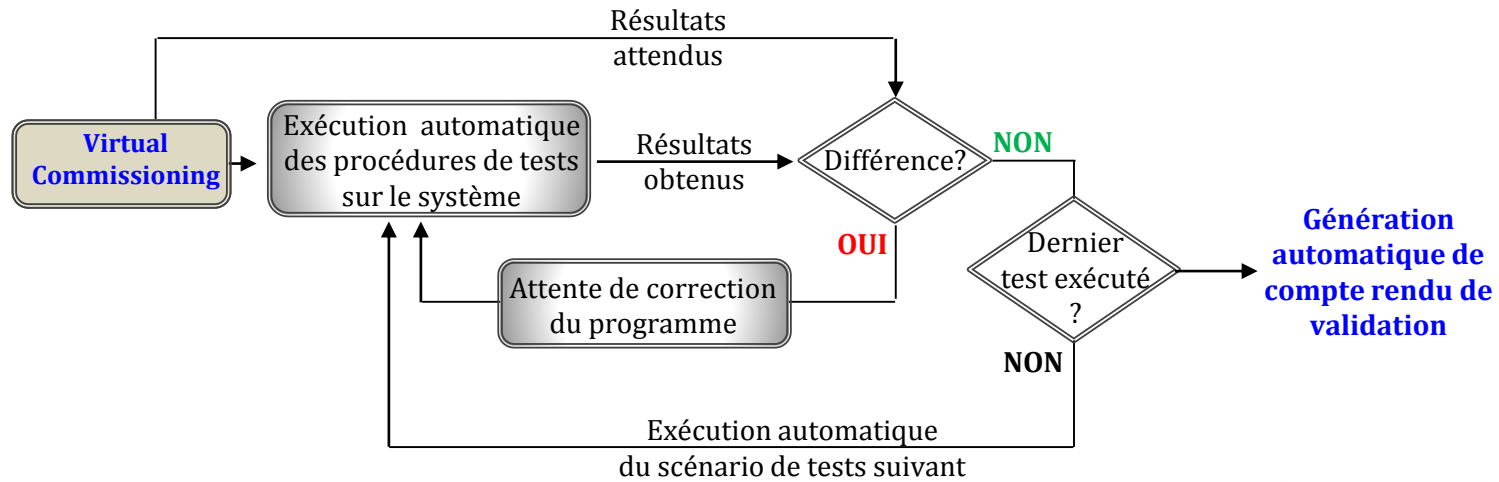
Cahier de recettes numérisé

Modèle virtuel de l'EALÉ étudiée

Validation automatique des programmes API

Principe de la validation automatique des programmes API

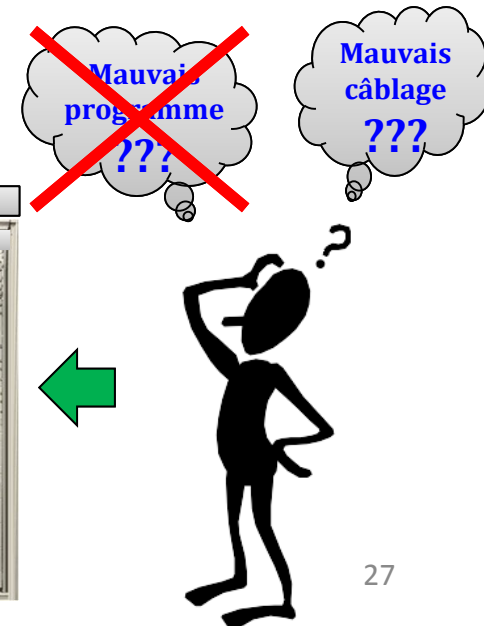
- **Mode manuel** (commande manuelle de l'installation)
- **Mode « cahier de recettes »**



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...

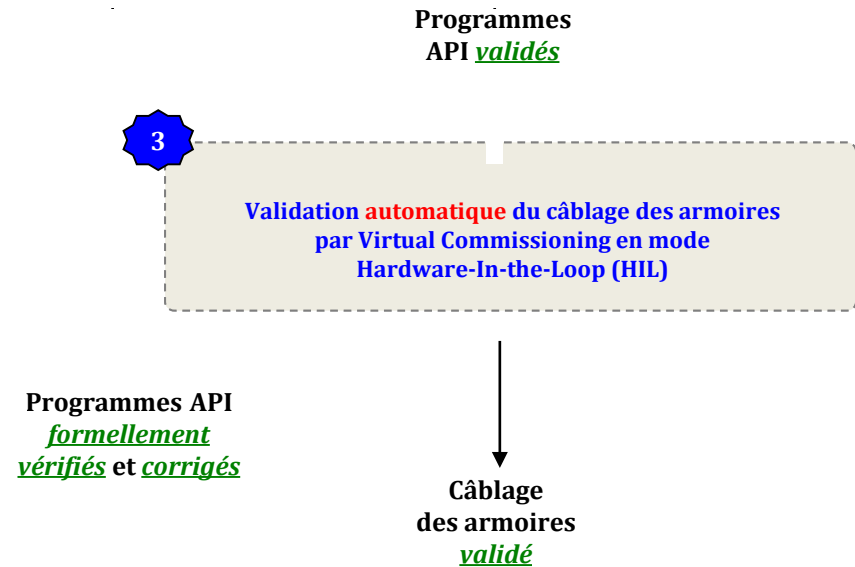
Recette usine



Validation automatique du câblage des armoires

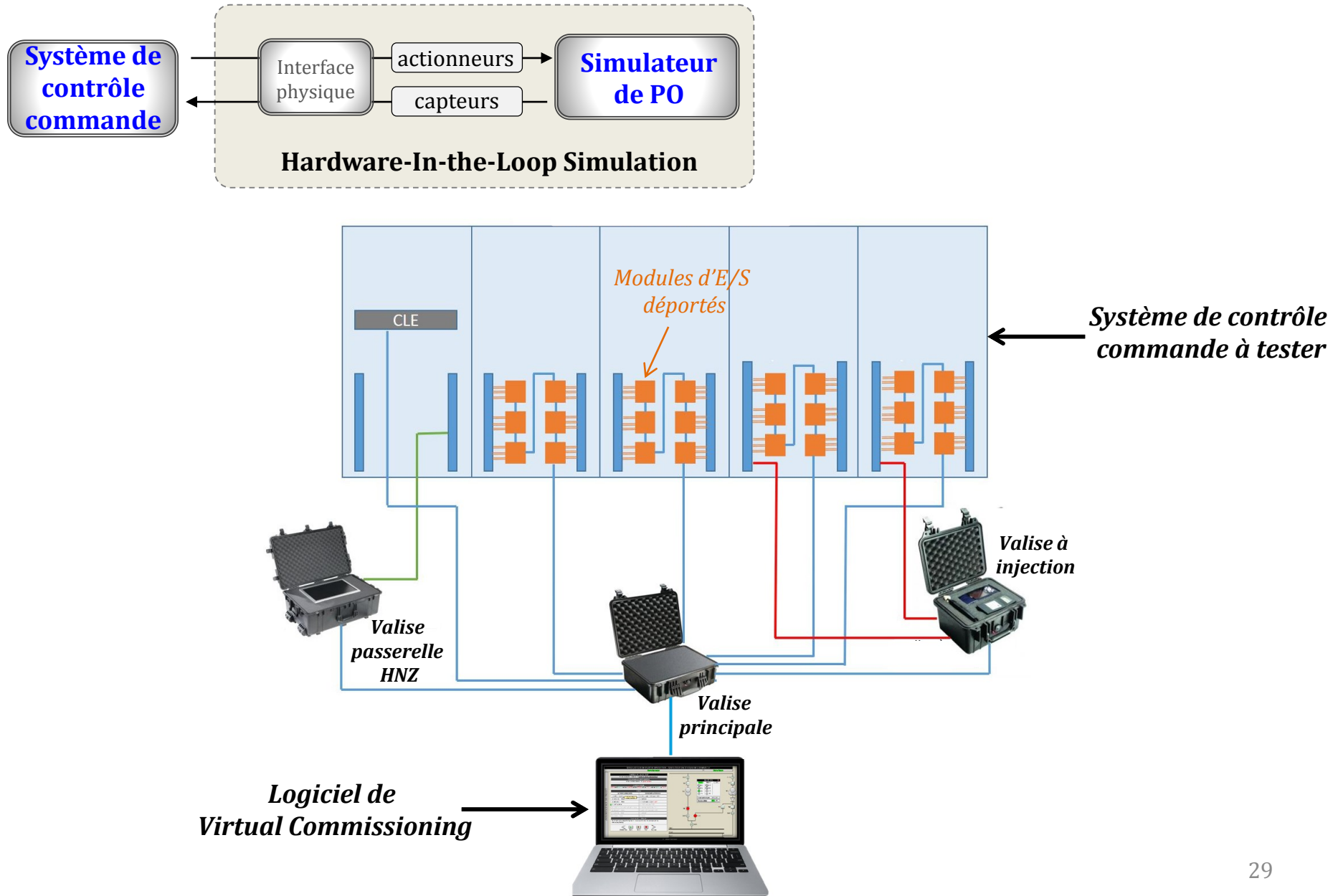
VERIFICATION

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

