ALL4TEC

« Safety Architect© : un outil MBSA et son application aux études de sûreté des Systèmes de Combat »

F. Vallée

26 janvier 2016

Forum « Méthodes Formelles et Sûreté de Fonctionnement »

Plan de la présentation

ALL4TEC

- Introduction
- Positionnement MBSA
- Méthode d'analyse de risque
- L'outil Safety Architect
- Avantages
- Démo

Suivie de la présentation de la mise en oeuvre de Safety Architect par DCNS

La société All4tec

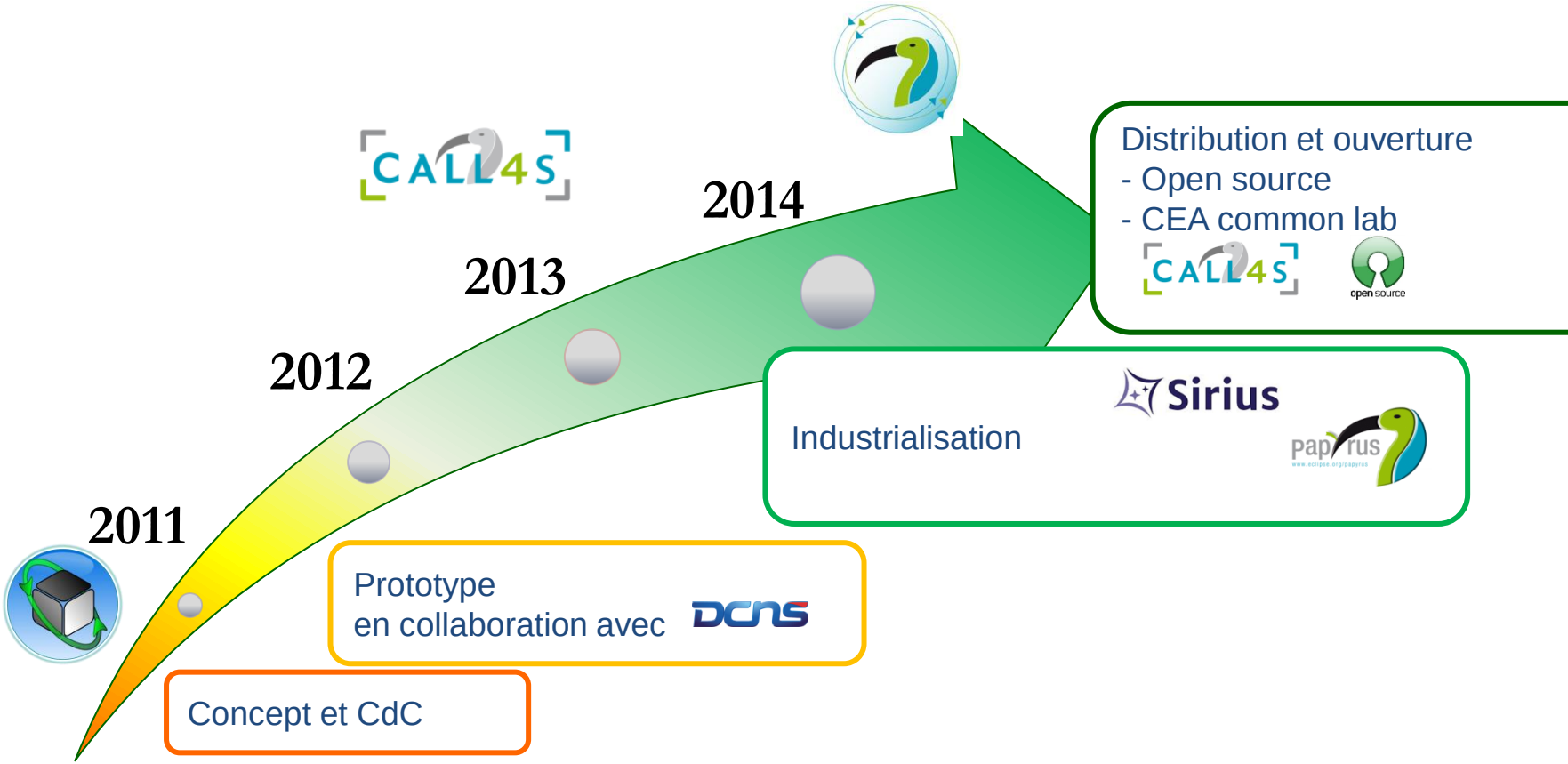
Des solutions dirigées par les modèles

Objectifs de Safety Architect

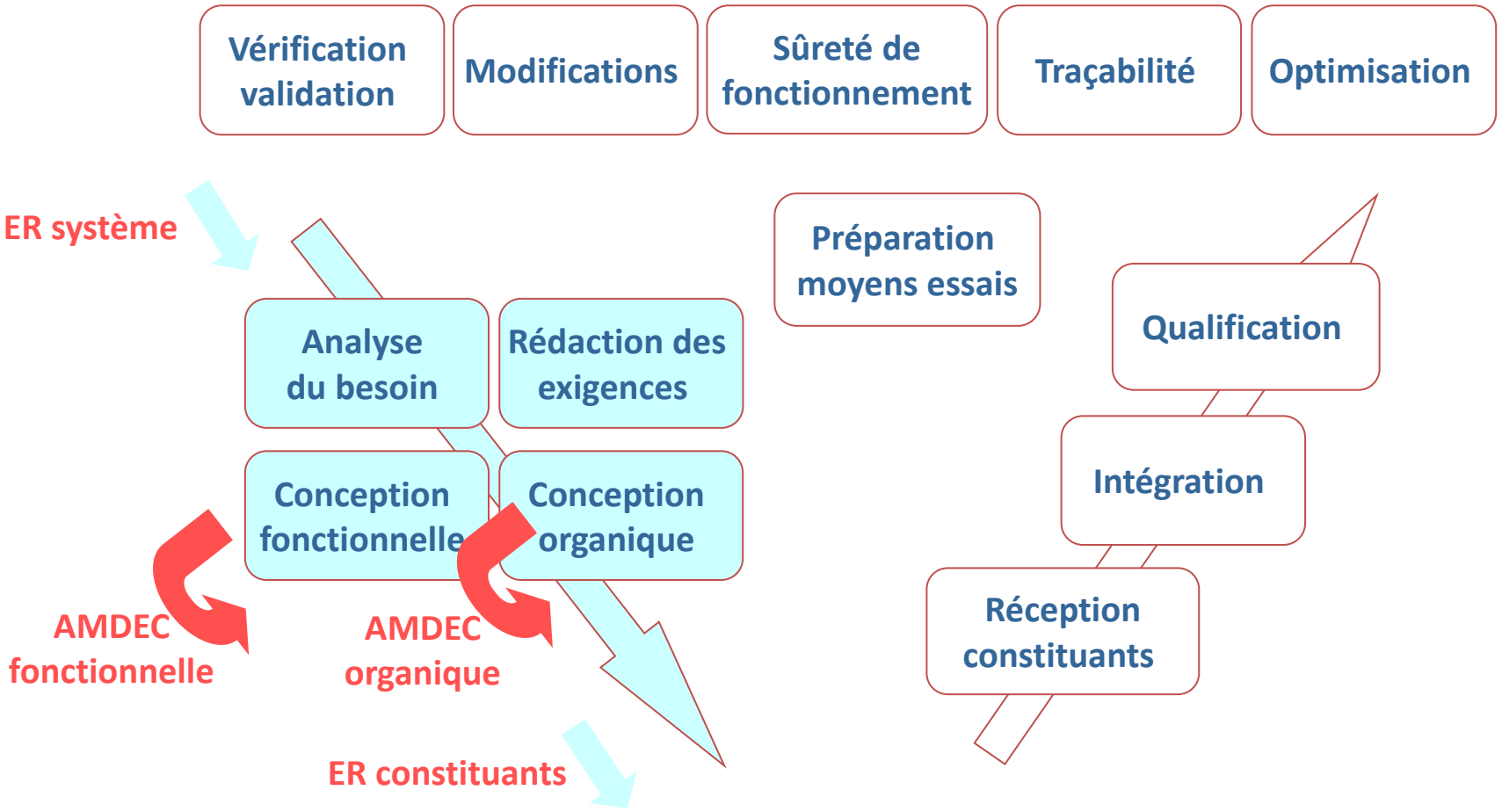
ALL4TEC

- S’appuyer sur les modèles de systèmes/logiciels pour faire les analyses de risque
- Etre indépendant des outils de modélisation
- Automatiser au maximum la démarche d’analyse de risque
- Faciliter les reprises en cas de modifications

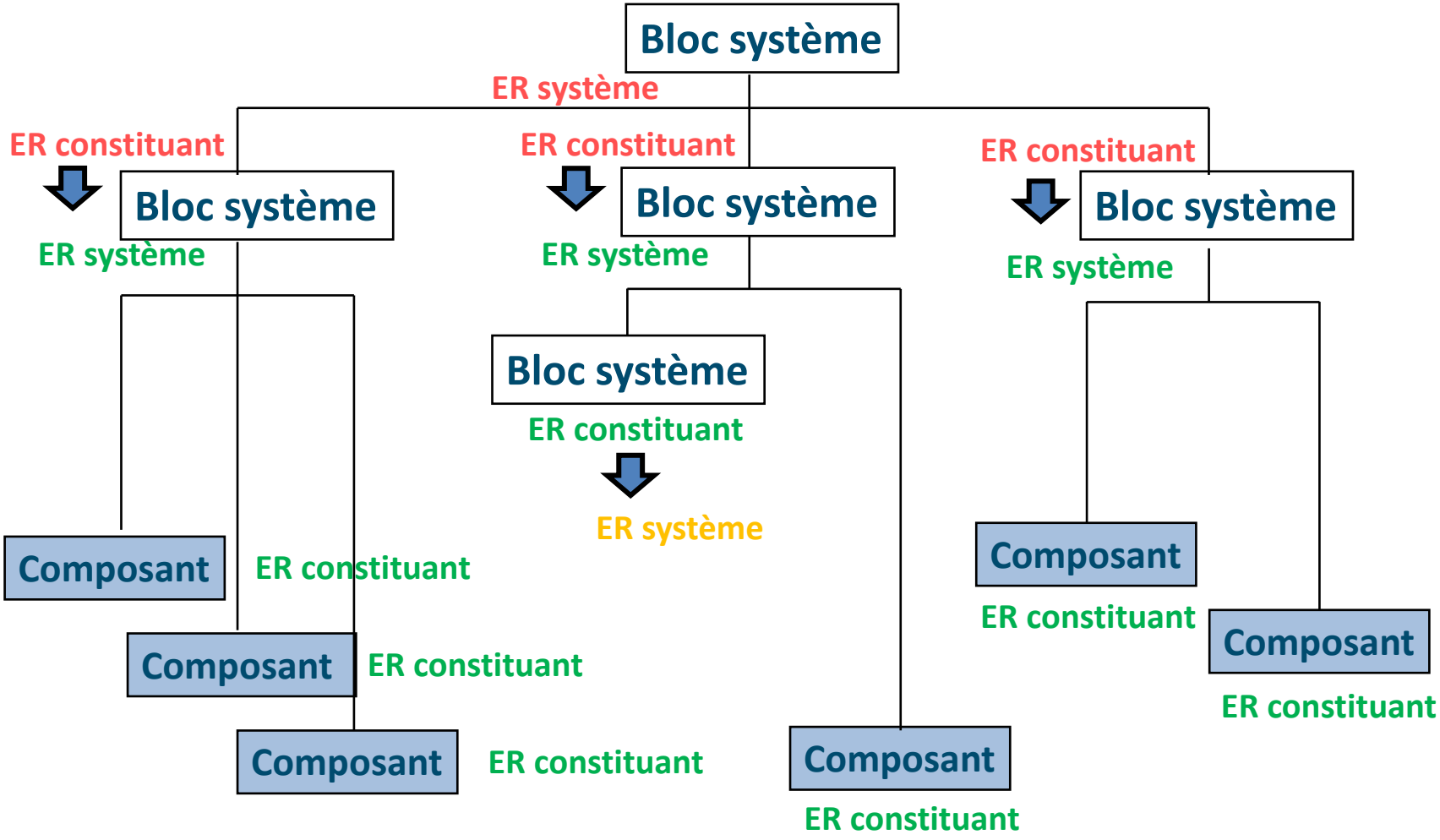
Historique



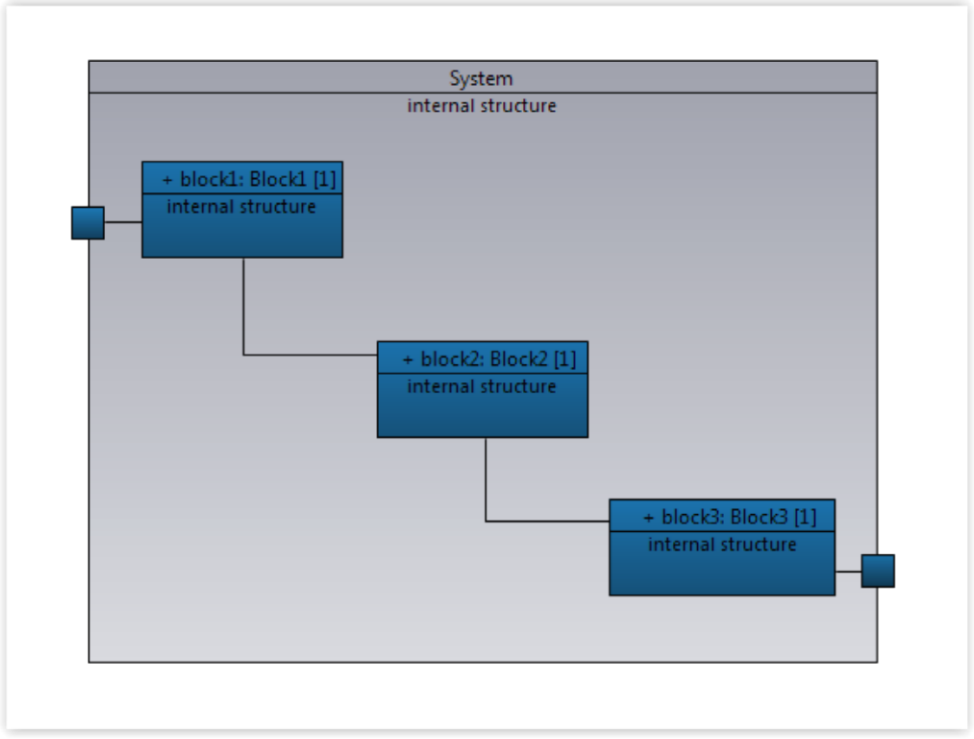
Positionnement IS et MBSA



Itération sur les blocs systèmes



Modèles d'IS utilisés

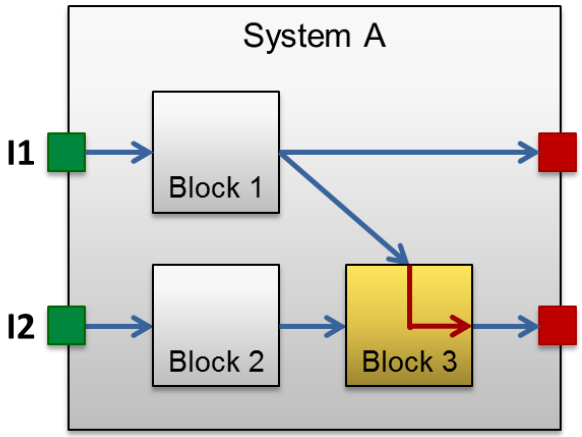


Méthode d'analyse des risques

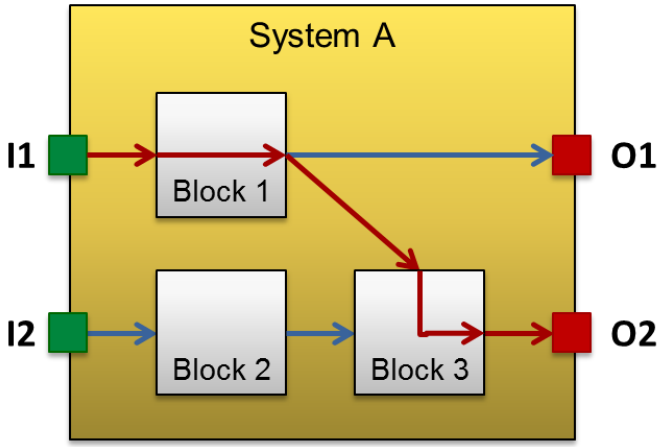
ALL4TEC

❑ Analyse locale

⇨ Association des événements redoutés aux modes de défaillance locaux



❑ Analyse globale par propagation

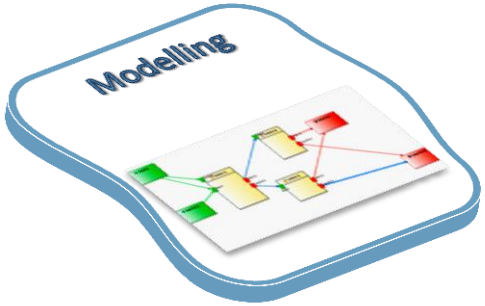


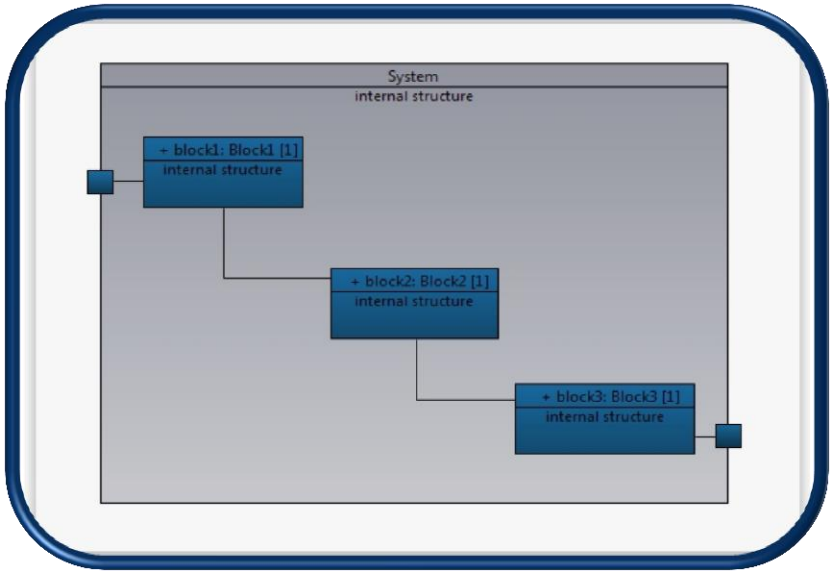
❑ Ajout de barrières et réitération

L'outil Safety Architect

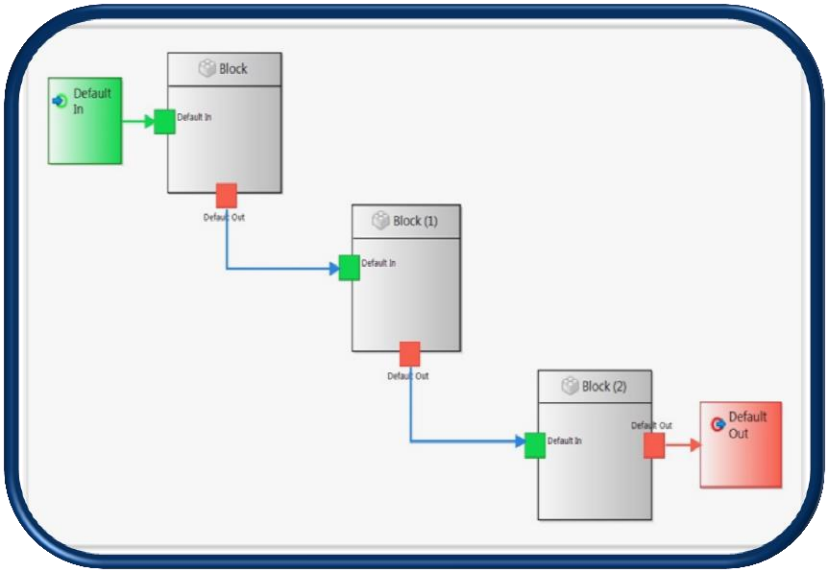
Import

Modélisation



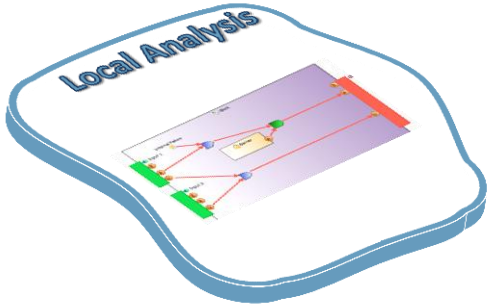


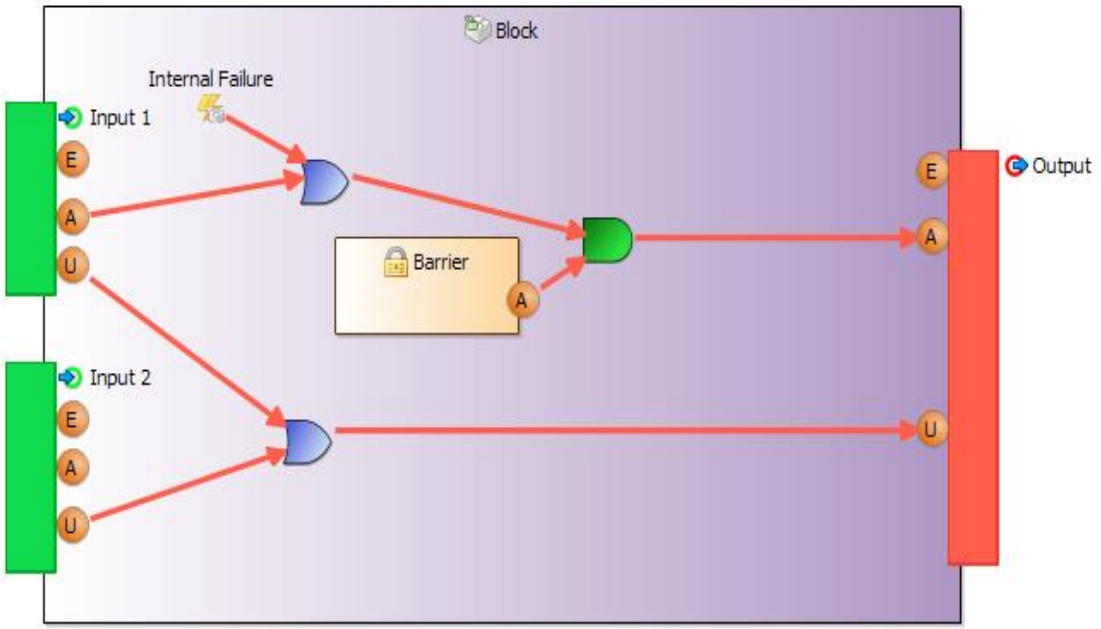
Papyrus



Sirius

Analyse locale





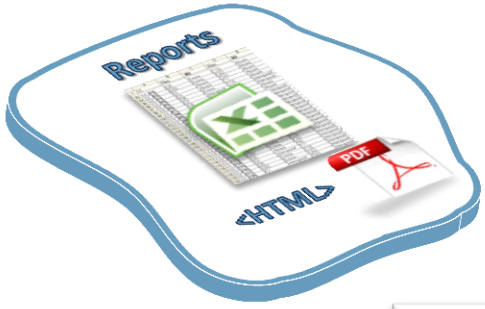
Analyse Globale

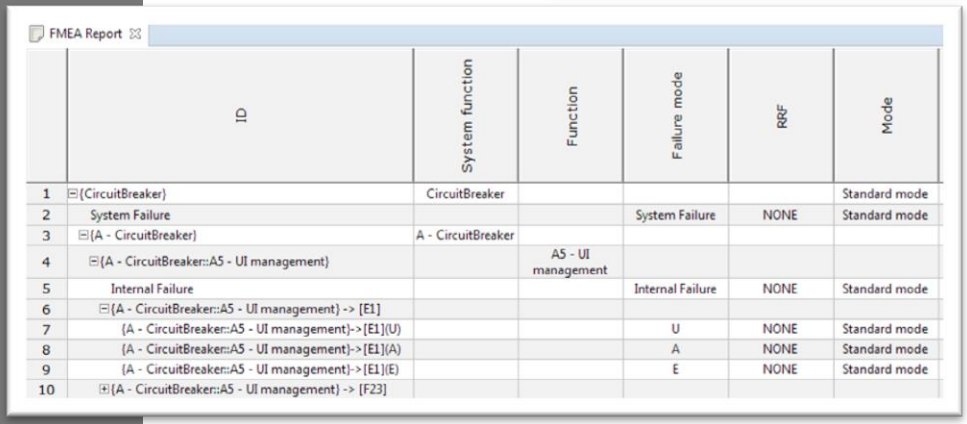
Name
Non broken circuit
{A - CircuitBreaker::A4 - Opening Command::A41 - Quick Opening}->[F412](A)
{A - CircuitBreaker::A4 - Opening Command::A41 - Quick Opening}->[E26](U)
{A - CircuitBreaker::A4 - Opening Command::A41 - Quick Opening}->[F23](A)
{A - CircuitBreaker::A2 - Check Short Circuit::A23 - ShortCircuitDetect}->[F23 - ShortCircuit detected](A)
{A - CircuitBreaker::A4 - Opening Command::A43 - Uncharge relay}->[F43](A)
{A - CircuitBreaker::A4 - Opening Command::A43 - Uncharge relay}->[F411](A)
{A - CircuitBreaker::A4 - Opening Command::A41 - Quick Opening}->[F411](A)
{A - CircuitBreaker::A4 - Opening Command::A41 - Quick Opening}->[E26](U)
{A - CircuitBreaker::A4 - Opening Command::A41 - Quick Opening}->[F23](A)
{A - CircuitBreaker::A2 - Check Short Circuit::A23 - ShortCircuitDetect}->[F23 - ShortCircuit detected](A)

Fonctions connexes

- Définition des événements redoutés
- Possibilité de customisation des modes de défaillance
- Ajout de défaillances système, événements normaux …
- Saisie des informations associées aux modes de défaillance
  - ⇨ Probabilités
  - ⇨ Autres infos AMDEC …
- Lien avec les exigences safety

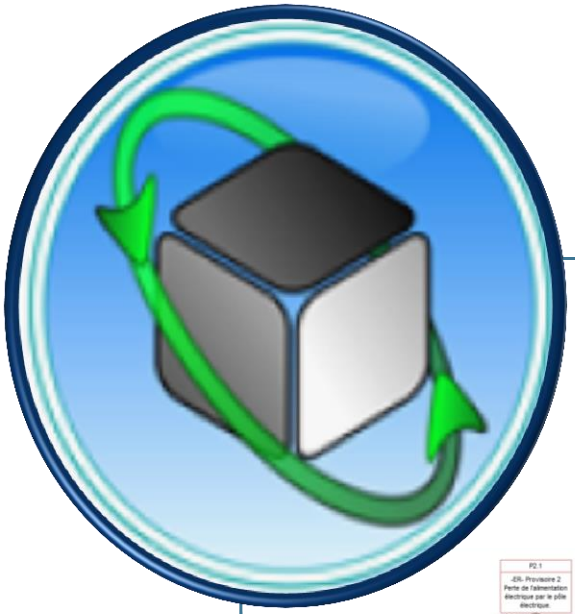
Reporting





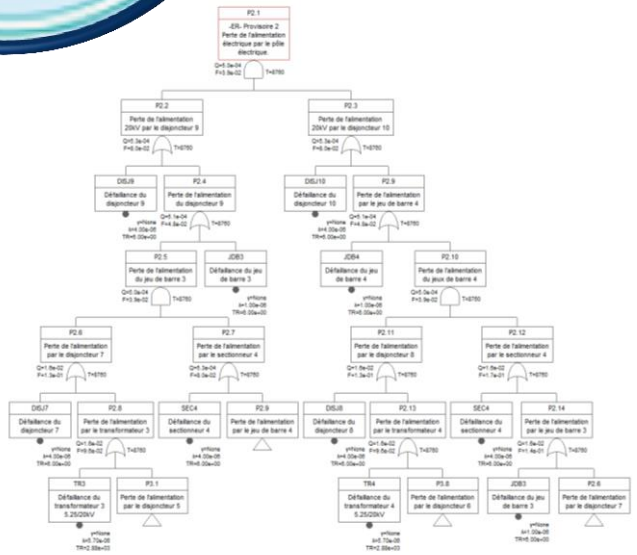
	ID	System function	Function	Failure mode	RRF	Mode
1	⊟{CircuitBreaker}	CircuitBreaker				Standard mode
2	System Failure			System Failure	NONE	Standard mode
3	⊟{A - CircuitBreaker}	A - CircuitBreaker				
4	⊟{A - CircuitBreaker::A5 - UI management}		A5 - UI management			
5	Internal Failure			Internal Failure	NONE	Standard mode
6	⊟{A - CircuitBreaker::A5 - UI management} -> [E1]					
7	{A - CircuitBreaker::A5 - UI management}->[E1](U)			U	NONE	Standard mode
8	{A - CircuitBreaker::A5 - UI management}->[E1](A)			A	NONE	Standard mode
9	{A - CircuitBreaker::A5 - UI management}->[E1](E)			E	NONE	Standard mode
10	⊞{A - CircuitBreaker::A5 - UI management} -> [F23]					

Export



RSA

OpenPSA



Résumé des avantages de SA

ALL4TEC

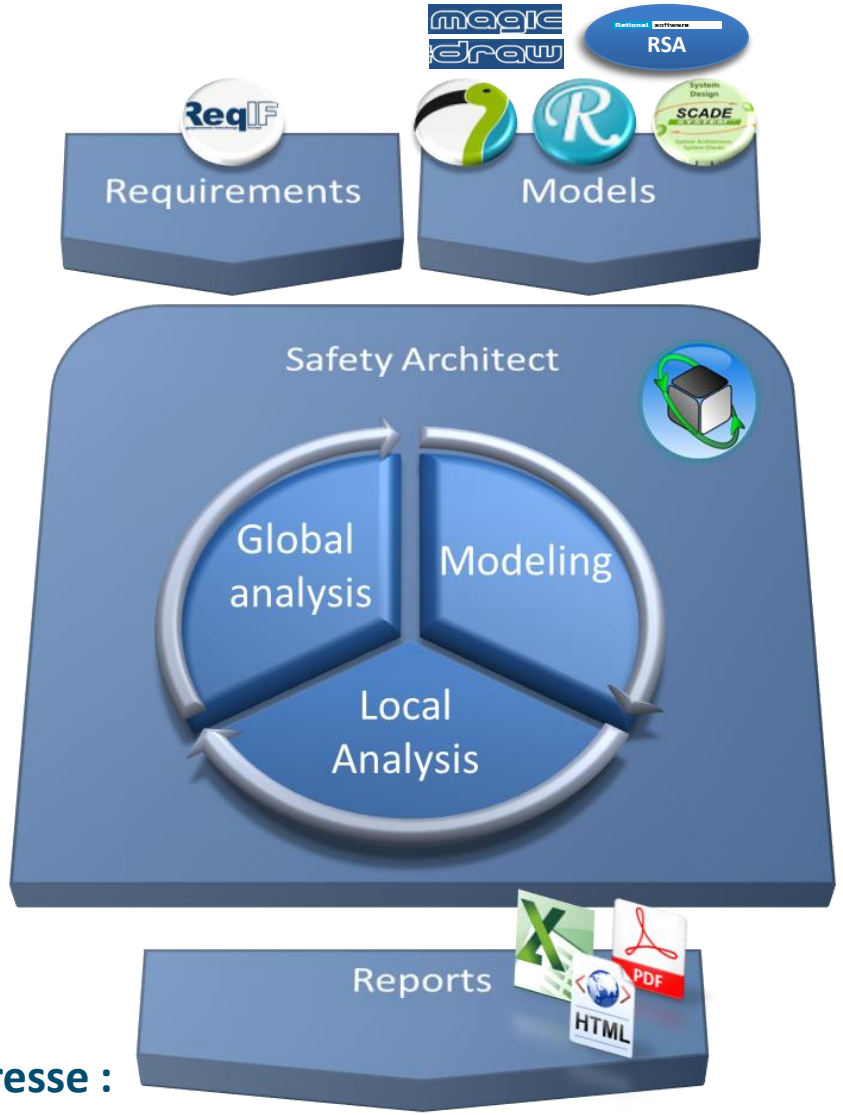
- Utilisable dans toutes les boucles d'ingénierie, depuis les modèles "système" jusqu'aux modèles "logiciel"
- Automatisation de la propagation
- Mise en évidence rapide des composants critiques
- Gains de productivité

Merci de votre attention

ALL4TEC

Démo !

- Integrate safety analysis and design
- Decrease risk of error
- Focus on added value tasks
- Reduce analysis costs



Licence d'évaluation disponible à cette adresse :
http://www.all4tec.net/cat_view/901-safety-architect