Modélisation d'un système de Contrôle-Commande embarqué dans le cadre d'Analyses Fonctionnelle et Dysfonctionnelle

Raphaël SCHOENIG

raphael.schoenig@free.fr
Tony.hutinet@ixi.fr

ONERA Toulouse
21 octobre 2002

Sommaire

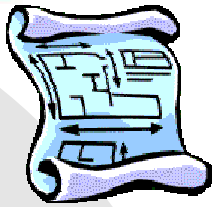
- Introduction
- Objectifs de l'étude
- Présentation du système
- Principes de la modélisation sous OCAS
- Mise en œuvre des Analyses
- Résultats des Analyses
- Conclusion & Synthèse

Introduction

- Cadre de l'étude
  - *Travaux de Thèse sur la définition d'une **Méthodologie de Conception de Systèmes Mécatroniques Sûrs de Fonctionnement***
- Systèmes traités
  - *Systèmes de Contrôle-Commande embarqués dans le secteur des transports (ferroviaire, automobile…)*
  - *Complexité de ces systèmes due à l'intégration de technologies différentes et absence de retour d'expérience*
  - *Besoin de nouvelles méthodes d'Analyse*

Objectifs de l'Étude

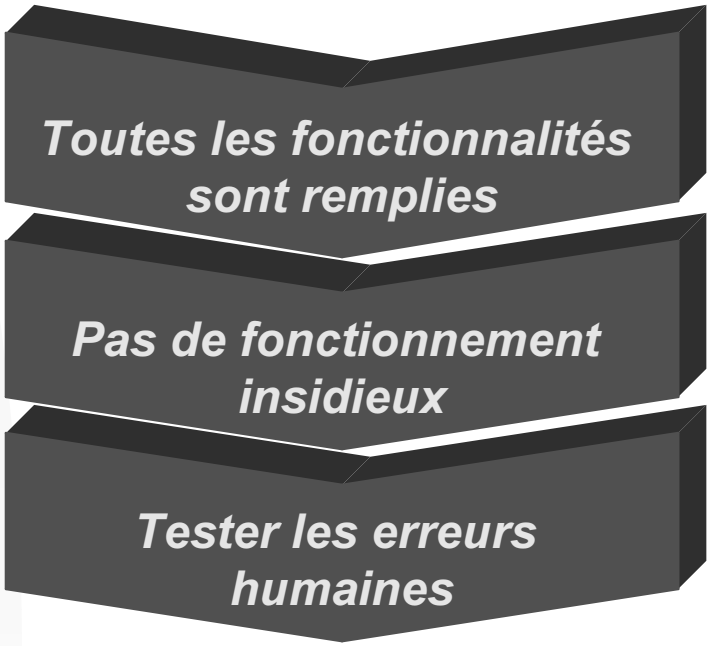
- Réaliser une Analyse Fonctionnelle et Dysfonctionnelle
  - *Système de Contrôle-Commande Embarqué*
  - *Modélisation UNIQUE pour les 2 analyses sous Cécilia OCAS*
- Choix d'un sujet pédagogique
  - *Système de Commande d'Ouverture et Fermeture des portes d'un métro*
- Développement simultané du cas d'étude et de la Méthodologie
- Modélisation Comportementale dans le langage AltaRica



Objectifs de l'Étude

- Analyse Fonctionnelle:

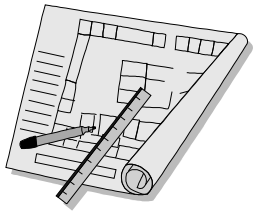
- *Simulation comportementale du modèle à partir d'un profil de mission type*
- *Vérifier que le comportement du modèle est conforme à celui attendu*



Objectifs de l'Étude

- Analyse Dysfonctionnelle:

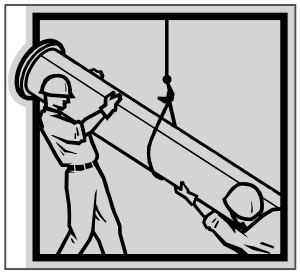
  - *Observer le comportement du système en présence de pannes simples ou multiples*
  - *Identifier les défaillances aboutissant à un ER de Sécurité ou Disponibilité ou à une perte de Fonctionnalité*
  - *Vérifier si les exigences de Sécurité et/ou de Disponibilité sont satisfaites*
  - *Identifier les sous-fonctions critiques vis-à-vis de la SECURITE*



Objectifs de l'Étude

- Exigences et Mise en place d'actions correctives
  - *<u>Exigence qualitative de Sécurité :</u> Aucune panne simple ne doit provoquer **d'Évènement Redouté de Sécurité***

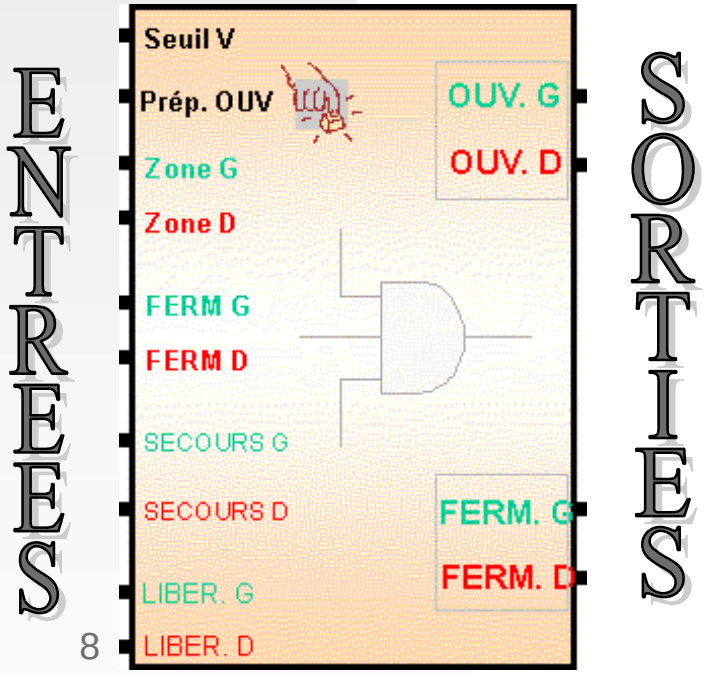
<u>Mise en place de barrières de sécurité:</u>
- ***Introduction de redondances locales***
- ***Sécurisation de certaines commandes***

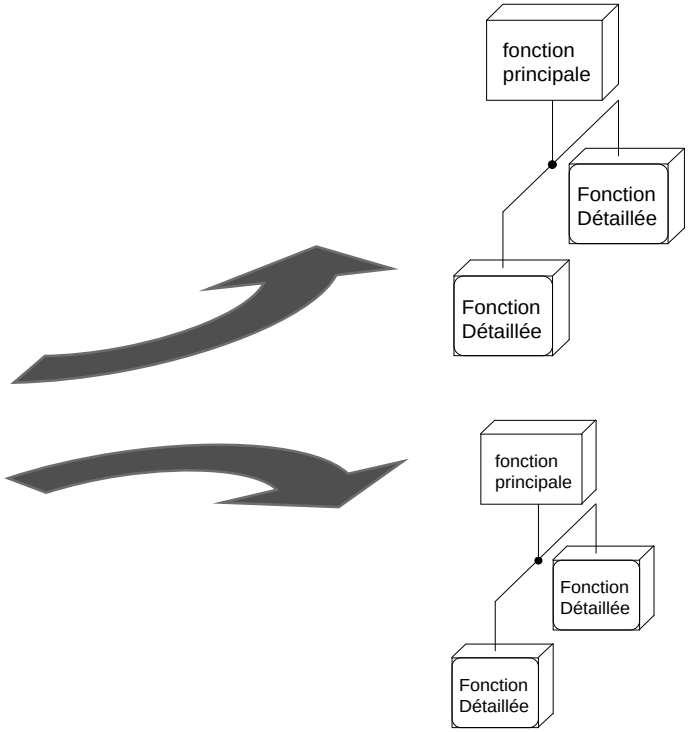


Retour à l'étape d'analyse dysfonctionnelle

Présentation du cas d'étude

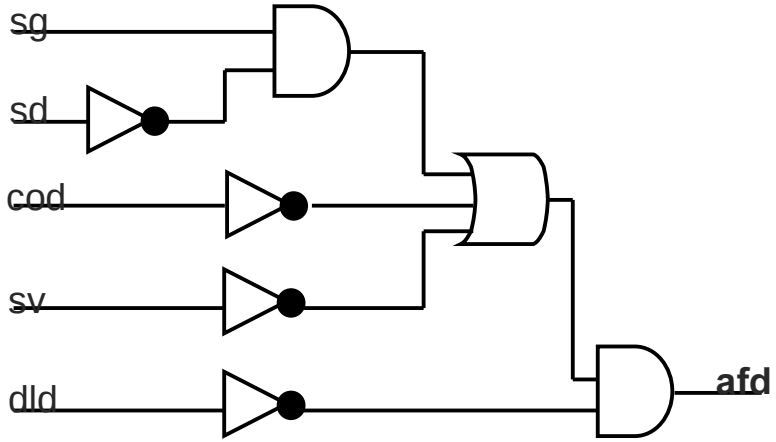
- Système de contrôle-commande **d'ouverture / fermeture des portes d'un métro**
- Décomposition hiérarchique:





Présentation du cas d'étude

- Signaux ENTREES Système: *commandes conducteur, information capteurs, signaux extérieurs au système…*
- Signaux SORTIES Système: *commandes d'ouverture/ fermeture des portes à droite et à gauche*
- Fonctions Principales: OUVRIR / FERMER / SERVICE
- Fonctions Détaillées:



Présentation du cas d'étude

- Commandes de secours à disposition du conducteur en cas de Non Ouverture des portes

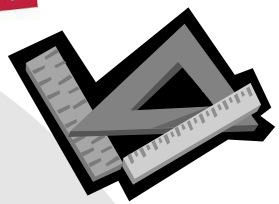
« Demande d'Ouverture de Secours »

Gravité 1

MODES DEGRADES

« Libération des Portes »

Gravité 2



Principes de Modélisation

- Modélisation des Informations: Signaux ENTREES & SORTIES de nature *électrique*

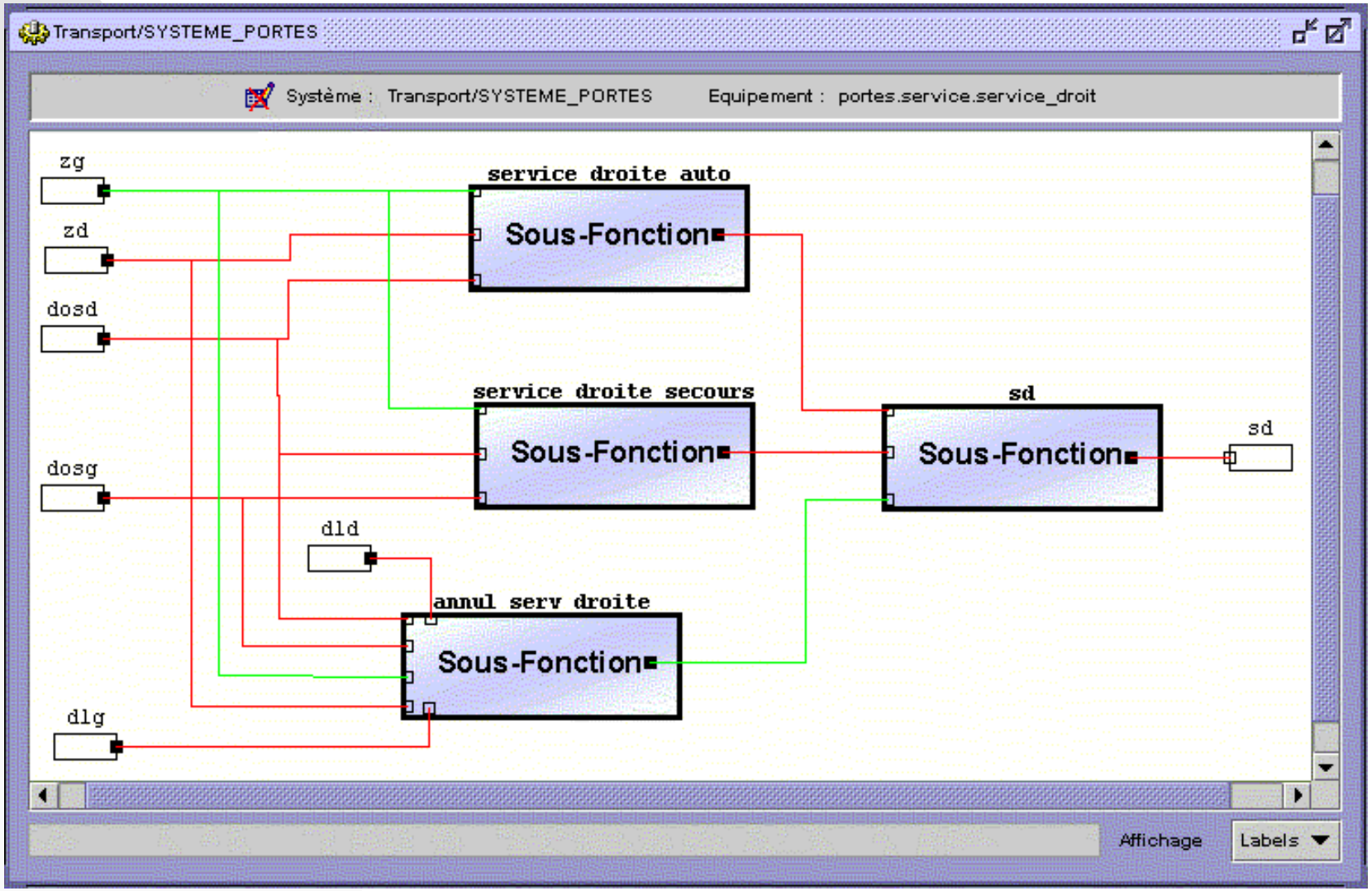
⇨ *Définition de variables de type BOOL dans AltaRica*

- ***VRAI*** *= Signal présent*
- ***FAUX*** *= Signal absent*

⇨ *Analyse de la propagation des signaux dans le système*

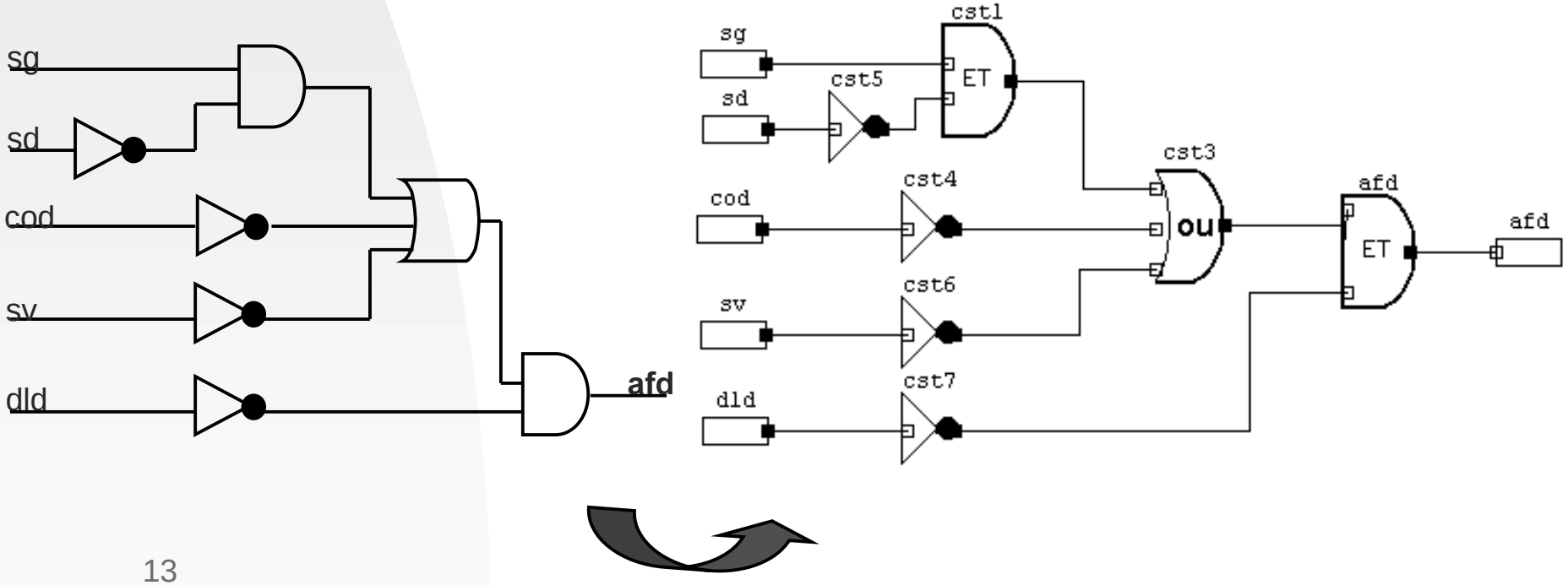
- *Repérage des erreurs de conception ou de saisie*
- *Détection des fonctions critiques*

Principes de Modélisation



Principes de Modélisation

- Modélisation des Sous-Fonctions:

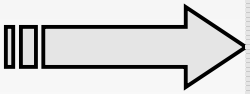


Principes de Modélisation

- Modélisation des Pannes:

Hypothèses: - *2 modes de défaillance pour chaque sous-fonction*

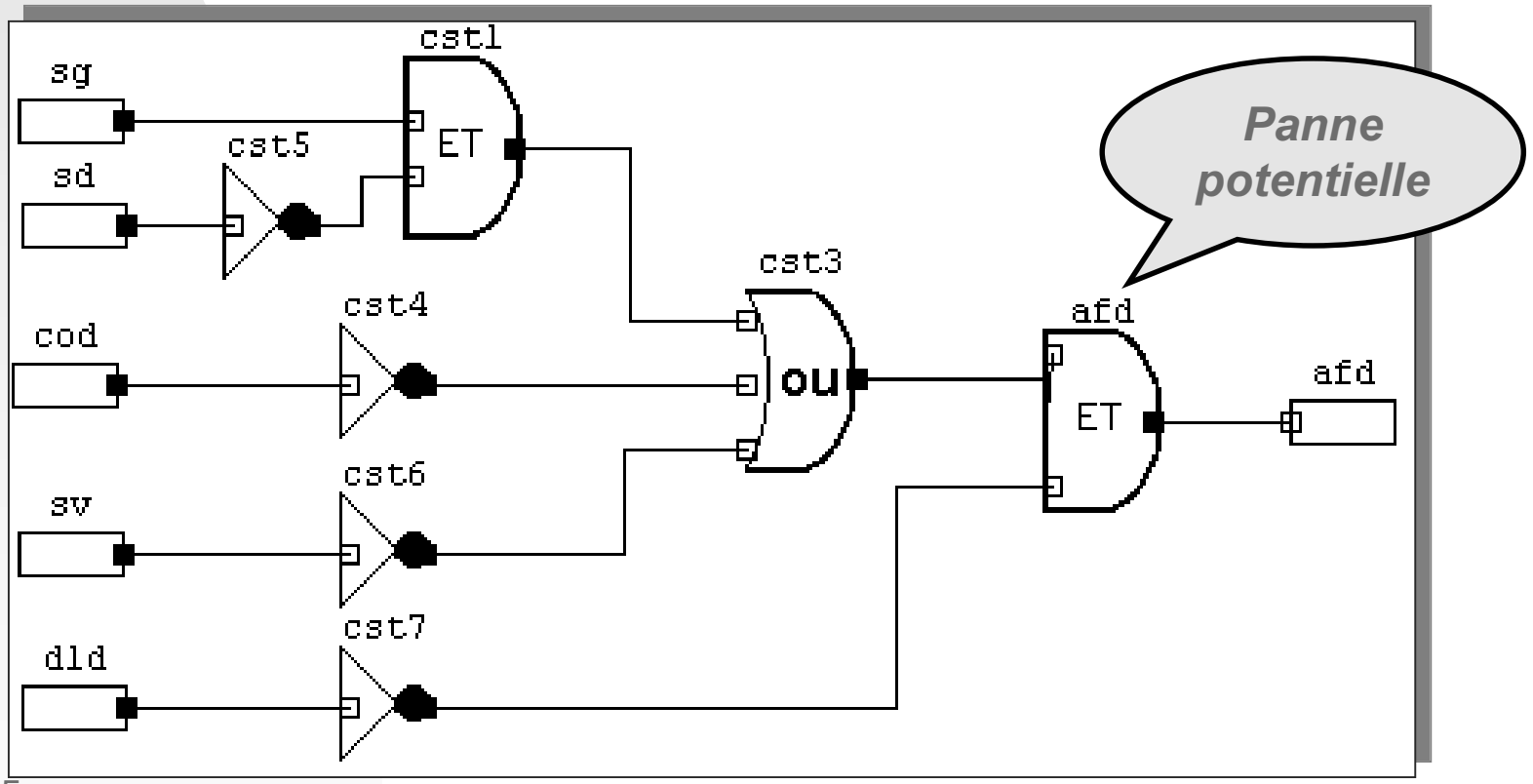
- Collage à 0 de la sortie = *Absence de signal*
- Collage à 1 de la sortie = *Signal intempestif*

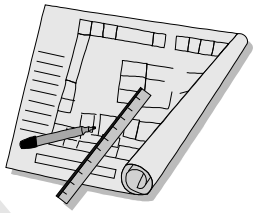


Perte de la fonction affectée d'une défaillance

Principes de Modélisation

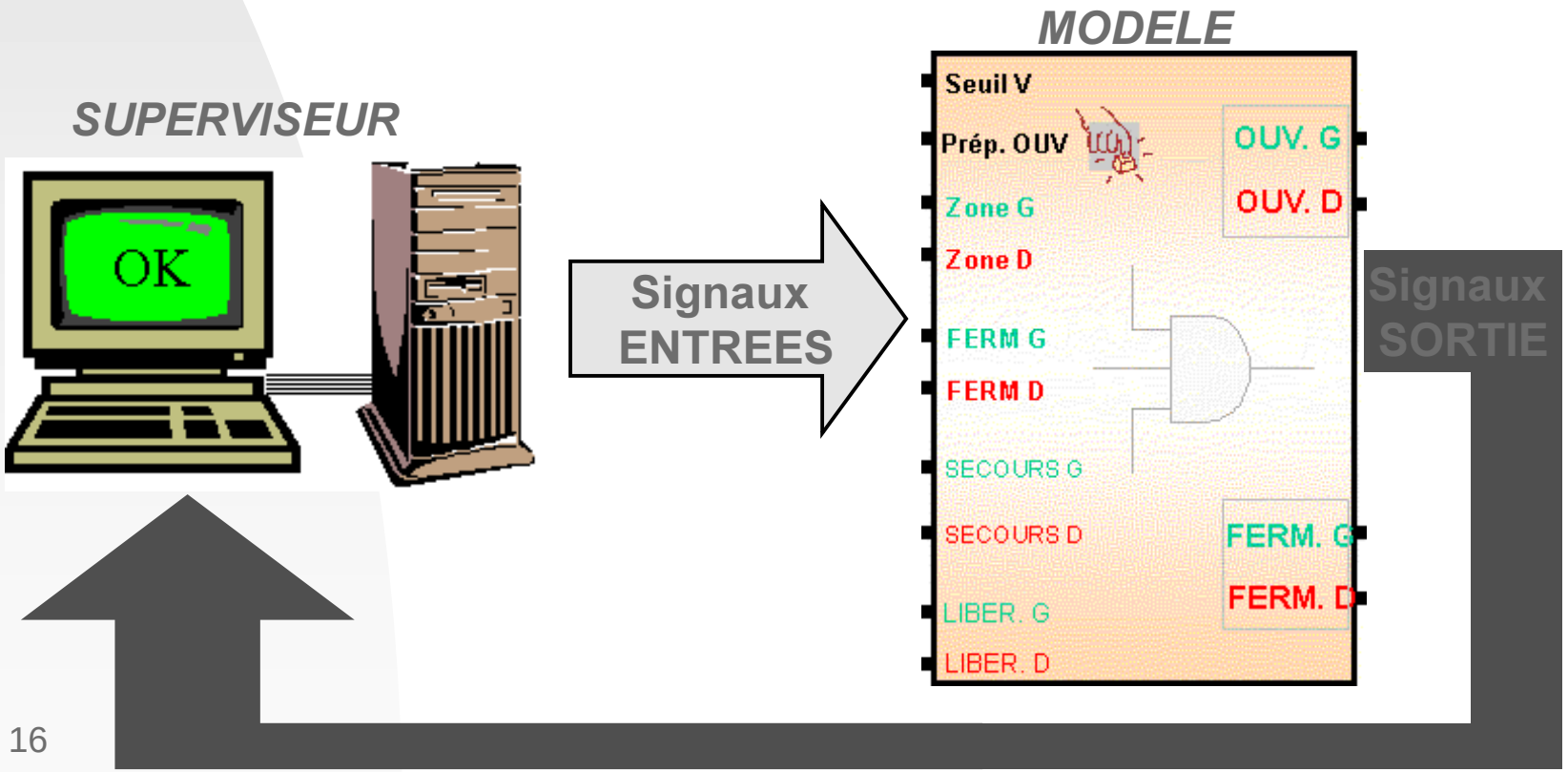
- Modélisation des Pannes:

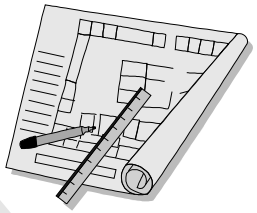




Mise en œuvre des Analyses

- Blocs MODELE & SUPERVISEUR:



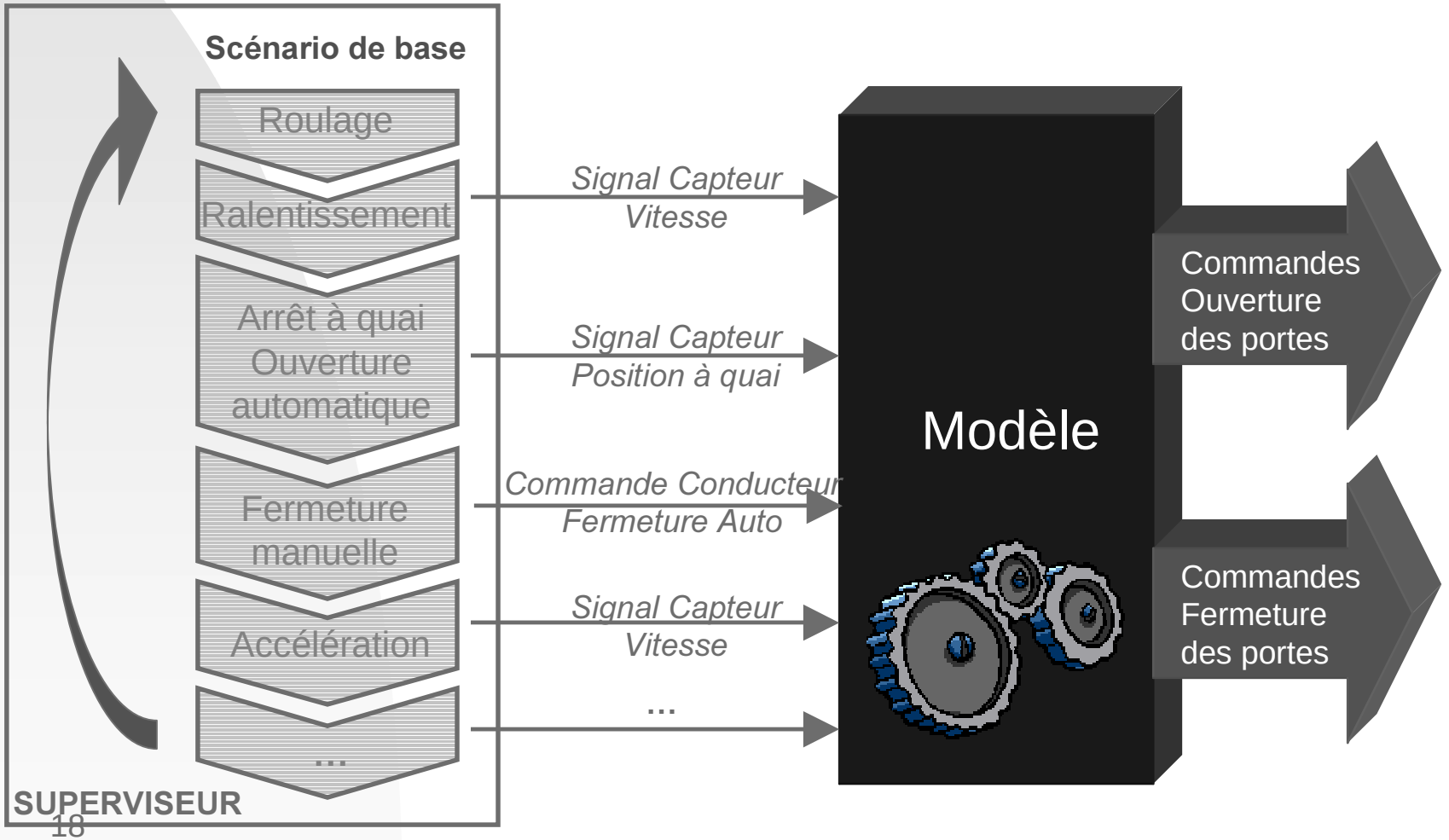


Mise en œuvre des Analyses

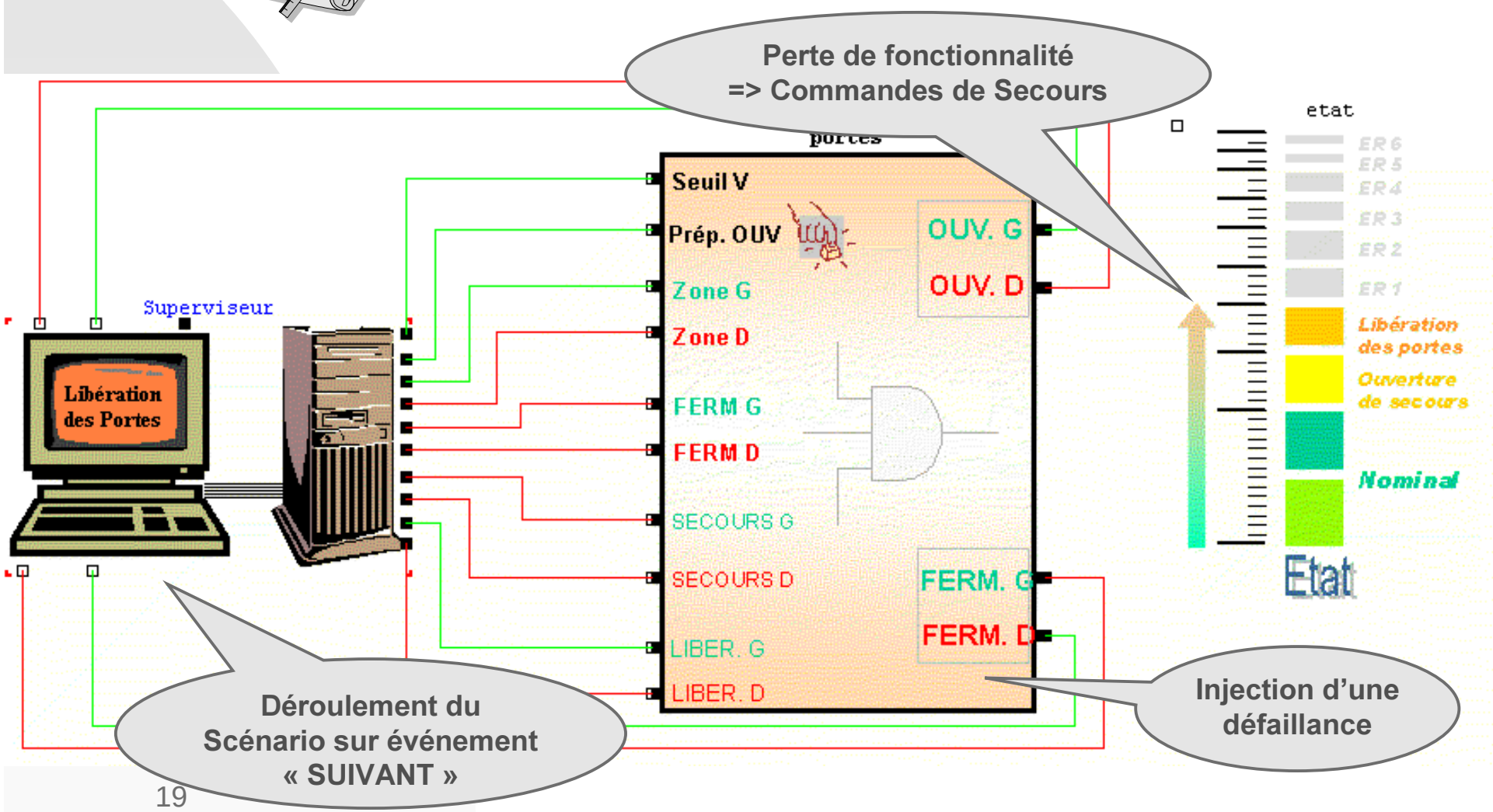
- Rôles du SUPERVISEUR:
  - *Modélisation d'un scénario de base définissant le profil de mission du système (fonctionnement nominal et dégradé)*
  - *Modélisation du comportement humain (envoi de commandes de secours si nécessaire par le conducteur, modélisation des erreurs humaines…)*
  - *Détection des changements d'état : ER de Sécurité, ER de Disponibilité, passages en mode dégradé*

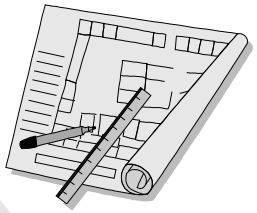
    ⇒ intégration d'un graphe d'état

Mise en œuvre des Analyses



Mise en œuvre des Analyses

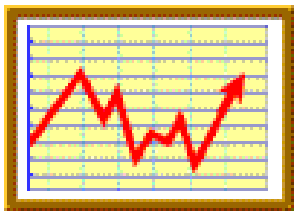




Mise en œuvre des Analyses

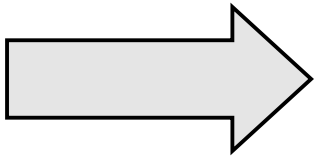
- Modèle vu comme une Boîte Noire
- Injection de pannes au début ou au cours du profil de mission
- Le Superviseur simule les actions humaines

  (déclenchement Commandes de Secours…)
- Détection du moment de l'activation des pannes latentes



Résultats des Analyses

- Analyse Fonctionnelle :

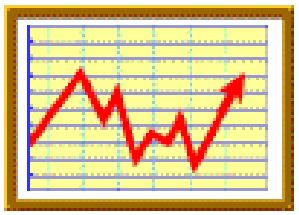


Modification apportée sur le modèle

=> *Simulation OK*

- Simulations des variantes du scénario de base incluant les erreurs humaines

Pas de fonctionnement insidieux détecté

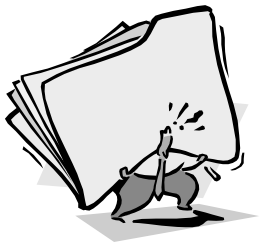


Résultats des Analyses

- Analyse Dysfonctionnelle :

Sur occurrence de pannes simples (54 défaillances potentielles):

	Avant Modifs	Après Modifs	
Sans Effets	24	28	↑
Ouv. Secours	5	5	→
Lib. Portes	2	8	↑
ER Dispo	9	13	↑
ER Sécurité	14	0	↓



Conclusion

- Modifications mineures apportées au système (on évite les redondances massives)

Compromis Disponibilité / Sécurité pendant et après la construction de la Sécurité

- Les simulations dysfonctionnelles ont mis en évidence un mode dégradé supplémentaire non identifié initialement:

le NON MAINTIEN DE FERMETURE

Synthèse

- *Étude du système en tant que Boîte Noire et découpage en 2 blocs: MODELE & SUPERVISEUR*
- *Modélisation Comportementale et visualisation de la propagation des flux dans les niveaux hiérarchiques sous OCAS*
- *Originalité de la méthodologie: Un modèle unique pour l'ensemble des analyses fonctionnelles et dysfonctionnelles*
- *Études réalisées en amont dans le cycle de développement*
- *Respect de la nature hiérarchique des systèmes*