Simulation de Cas d'accidents Pour l'aide à la décision

« Application au domaine de la sécurité de transport ferroviaire »

Lassaad MEJRI

Ahmed MAALEL

Henda BEN GHEZELA

Sommaire

Diapo

Problématique de l'analyse de sécurité (STA)

-Tâche cruciale indispensable avant la mise en site définitive d'un système de transport automatisé.

- Concerne le système et les automatismes (exemple : Métro VAL).

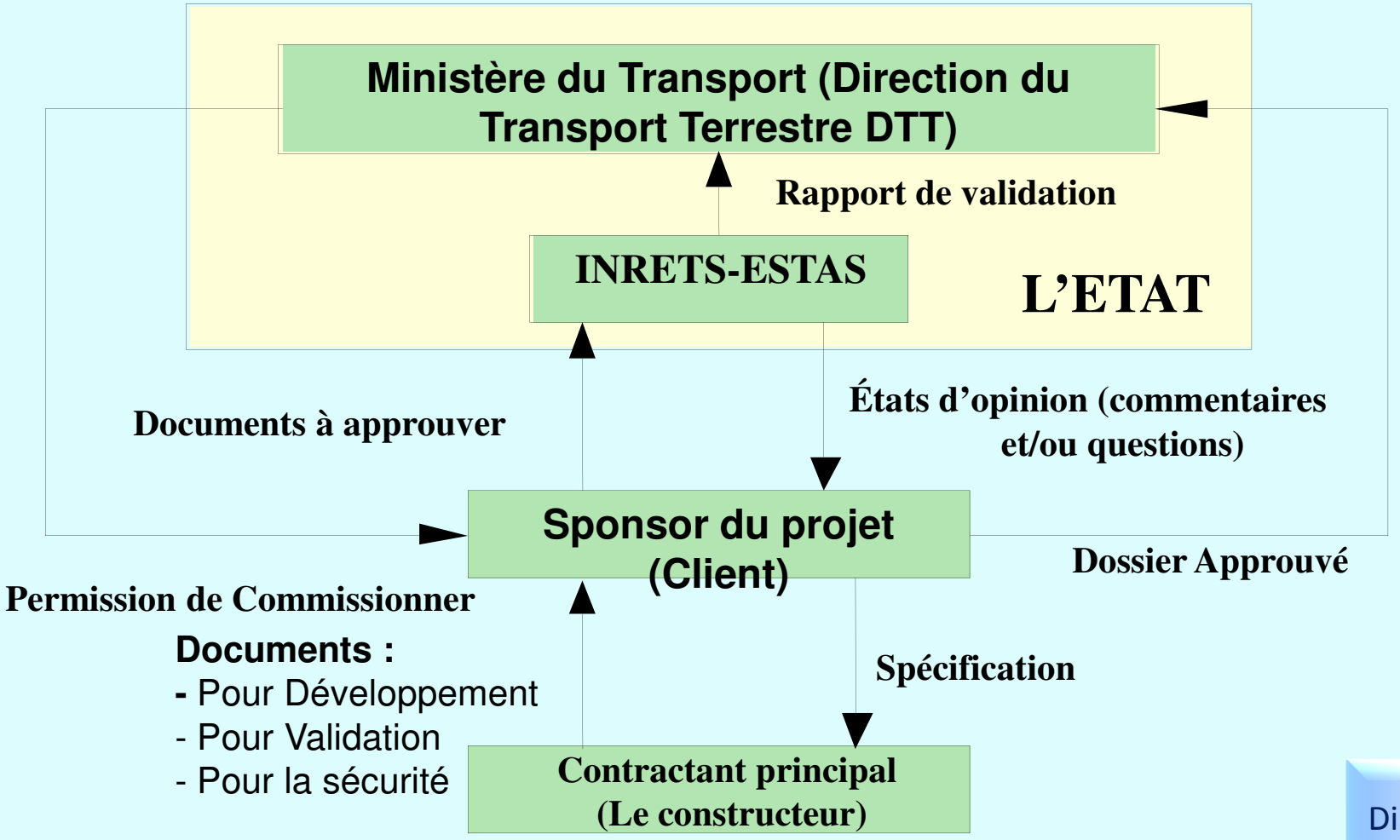
- Plusieurs intervenants (Experts/Constructeur/Exploitant)

- S'assurer de la conformité du système (Matériel & Logiciel) aux exigences de la sécurité.

- Organisme responsable : Institut National de Recherche sur les Transports et leur Sécurité (INRETS-ESTAS)

Diapo

Procédure d'Agrément dans les Systèmes de Transport Automatisés



Diapo

Résultats de l'acquisition de connaissances

- L'analyse de sécurité est une tâche assez complexe qui requiert l'emploi des méthodes et des techniques d'acquisition de connaissances.
- Techniques utilisés (l'interview, les questionnaires, l'analyse de protocoles, le tri conceptuel, la mise en situation réelle, …etc.)
- Cette phase a permis de dégager 3 éléments clés :
  - Identification des acteurs
  - Identification du dossier de sécurité
  - Collection de scénarios d'insécurité

Diapo

Les Acteurs Impliqués dans le processus d'analyse de sécurité

Dossier de sécurité

- Le **constructeur** d'un système de transport automatisé est soumis à l'obligation de fournir plusieurs documents d'ordre technique à la Direction du Transport Terrestre (DTT).

- Le document relatif aux aspects sécurité appelé **dossier de sécurité** est important : Il représente le point de vue du constructeur sur le volet sécuritaire.

- Le dossier de sécurité dans son aspect le plus simpliste pourrait être vu comme un ensemble de scénarios d'insécurité plausibles pouvant mettre en cause la sécurité du système de transport automatisé.

Diapo

Notion de Scénario d'accident

- Un scénario d'insécurité ou encore un scénario contraire à la sécurité représente souvent une situation d'insécurité au niveau du système de transport automatisé.

- Une insécurité, potentielle devrait être résolue par la proposition d'une solution pour pallier au risque qu'elle présente (exemple : collision entre deux rames de métro ou déraillement de la voie …etc.).

- Un scénario est un concours de circonstances pouvant mener à un danger sur le plan de la sécurité. Il est décrit par des attributs de situation et des attributs de solution à adopter pour anéantir ou réduire le risque d'insécurité.

Diapo

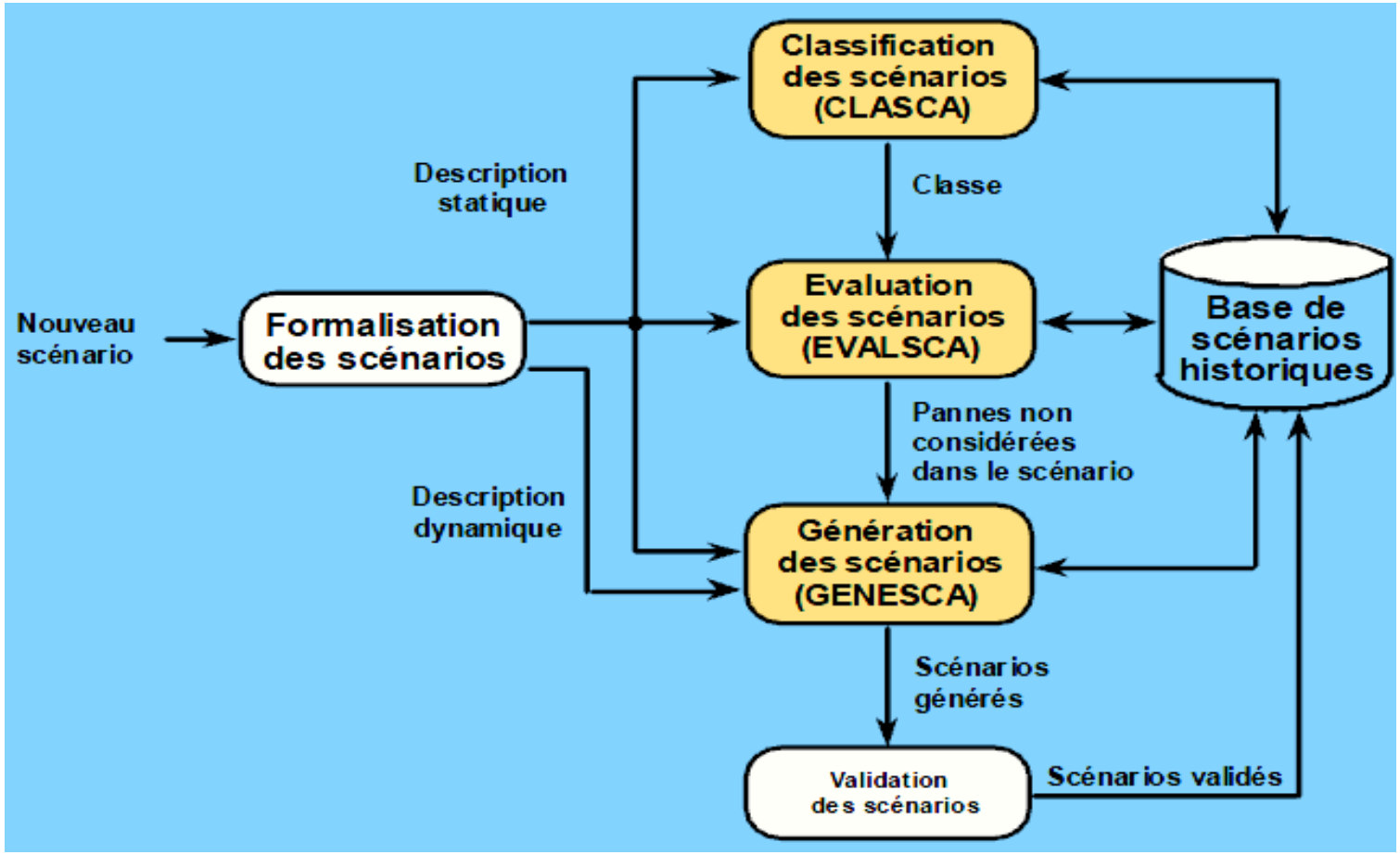
Démarche d'aide à l'analyse de sécurité

Dans l'objectif d'aider les experts dans leur activité d'analyse et d'évaluation de scénarios d'insécurité, notre démarche s'articule autour de deux étapes essentielles complémentaires :

- **Classifier** d'abord automatiquement le scénario d'insécurité dans une classe prédéfinie à l'aide **d'un algorithme de classification**. Ceci afin de cibler sur un cadre de référence qui est la classe de scénarios d'insécurité au lieu de toute la base de scénarios.

- **Evaluer** ensuite le scénario d'insécurité proposé par le constructeur en référence à la classe d'appartenance trouvée dans l'étape précédente.

Le système ACASYA [Mejri 1995, Hadj Mabrouk 94]



Diapo

Critiques et Nouvelles Orientations

- ACASYA s'est limité à exploiter la description statique du scénario d'accident**. Il serait alors naturel de tirer profit de l'ensemble des autres formes de description de scénario : description dynamique, description textuelle et description graphique.**

- Cette description dynamique **se prête bien à la simulation.**

- Le langage de description utilisé dans le volet statique manque de cohérence et ne se réfère à aucune terminologie bien définie du domaine. Il est alors opportun de **mettre en place une ontologie du domaine**.

- ACASYA opère par mécanisme inductif (l'apprentissage). Il serait intéressant de faire appel au **Raisonnement à partir de Cas** et non à un mécanisme purement inductif. En effet, nous considérons le RàPC comme **le moyen du Retour d'expérience (Rex)** dans le domaine de l'analyse de sécurité.

Représentation de connaissances

Un scénario d'accident est représenté par :

- Une description Textuelle (Texte descriptif du déroulement du scénario, de ses causes, et de sa gravité)
- Une description Graphique (Synoptique = Schéma)
- Une description statique (liste d'attributs/valeurs)
- Une description Dynamique (RdP + Tableau de séquencement de Marquage)

Diapo

Description Textuelle Versus Modèle Textuel de Cas

A titre d'exemple, la description textuelle fournie par les experts pour le scénario N°34 porte le nom "***Echec d'effacement d'un élément secouru après dés initialisation***" :

Description *:*

- *Elément A est devenu muet (ne dialogue plus avec le PA : Pilote Automatique) et il est pris en charge par le Pilote automatique du tronçon n nommé PAn qui est en cours de lancer une initialisation par parcours de l'élément B en CM « Conduite Manuelle".*

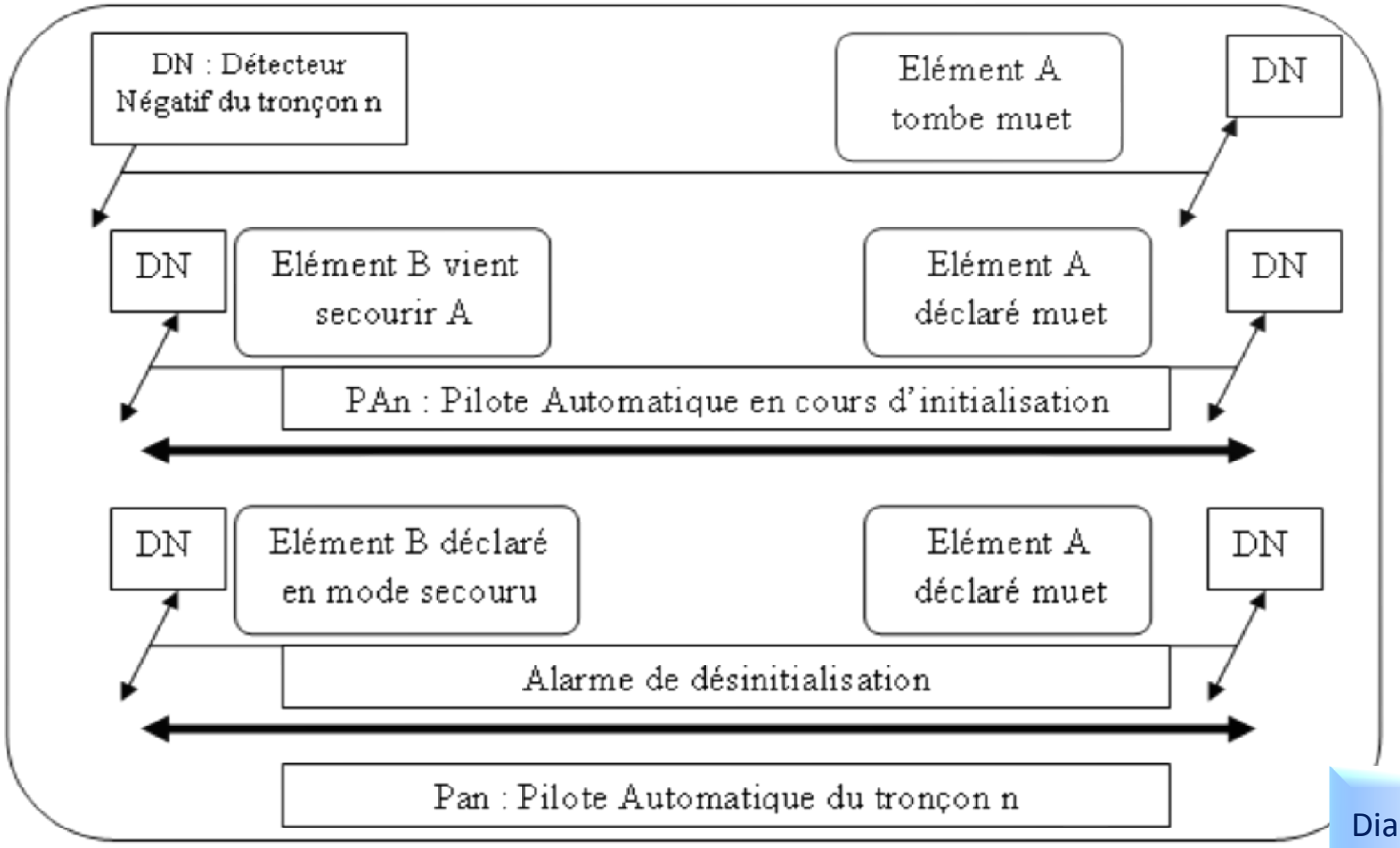
- *L'élément B accoste l'élément A et se met en CMS "Conduite Manuelle Secouru".*

- *Alarme de désinitialisation.*

- ***Solution** : Il faut vider la section de tout élément avant de procéder à une initialisation.*

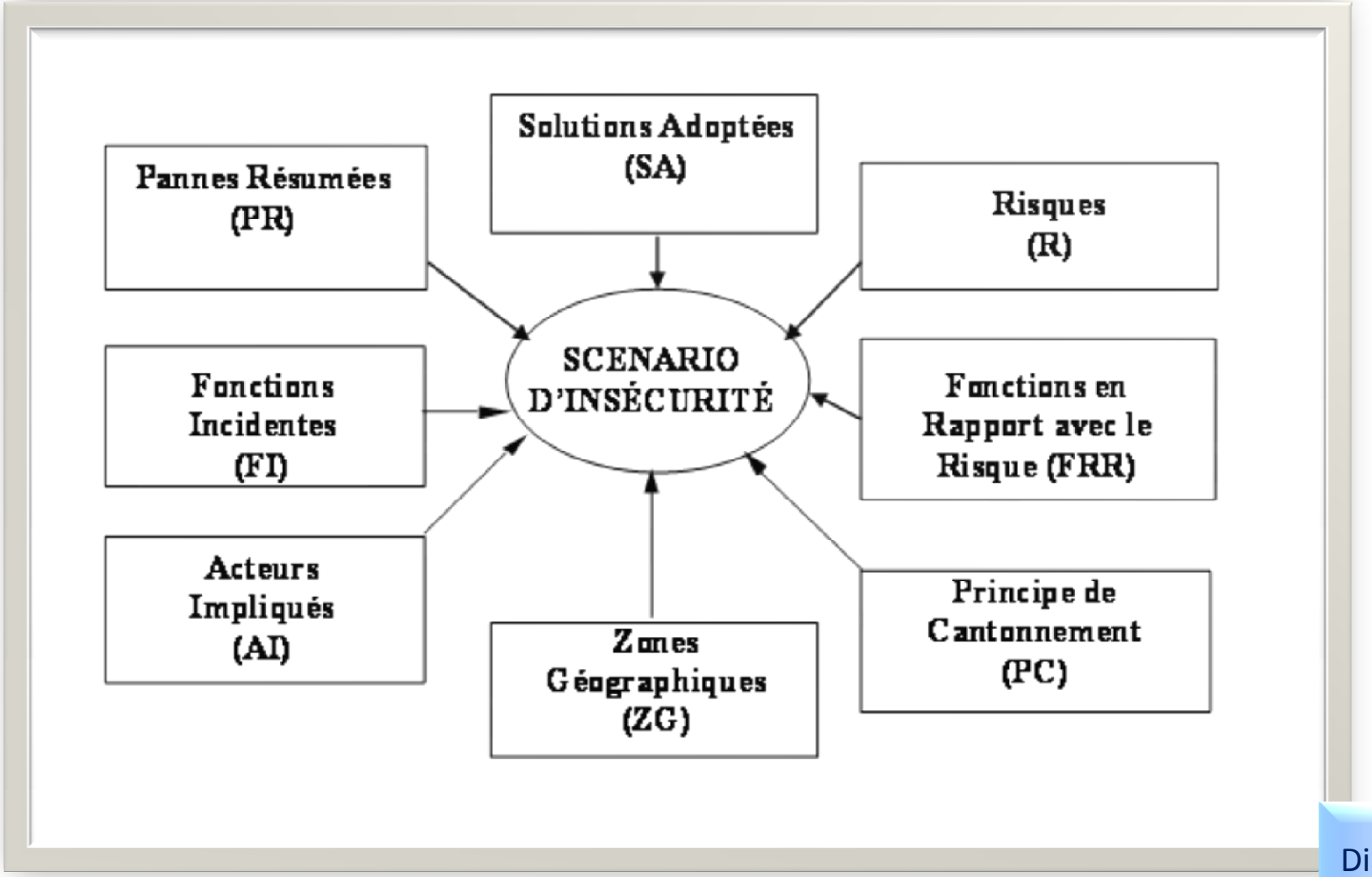
Diapo

Description Graphique



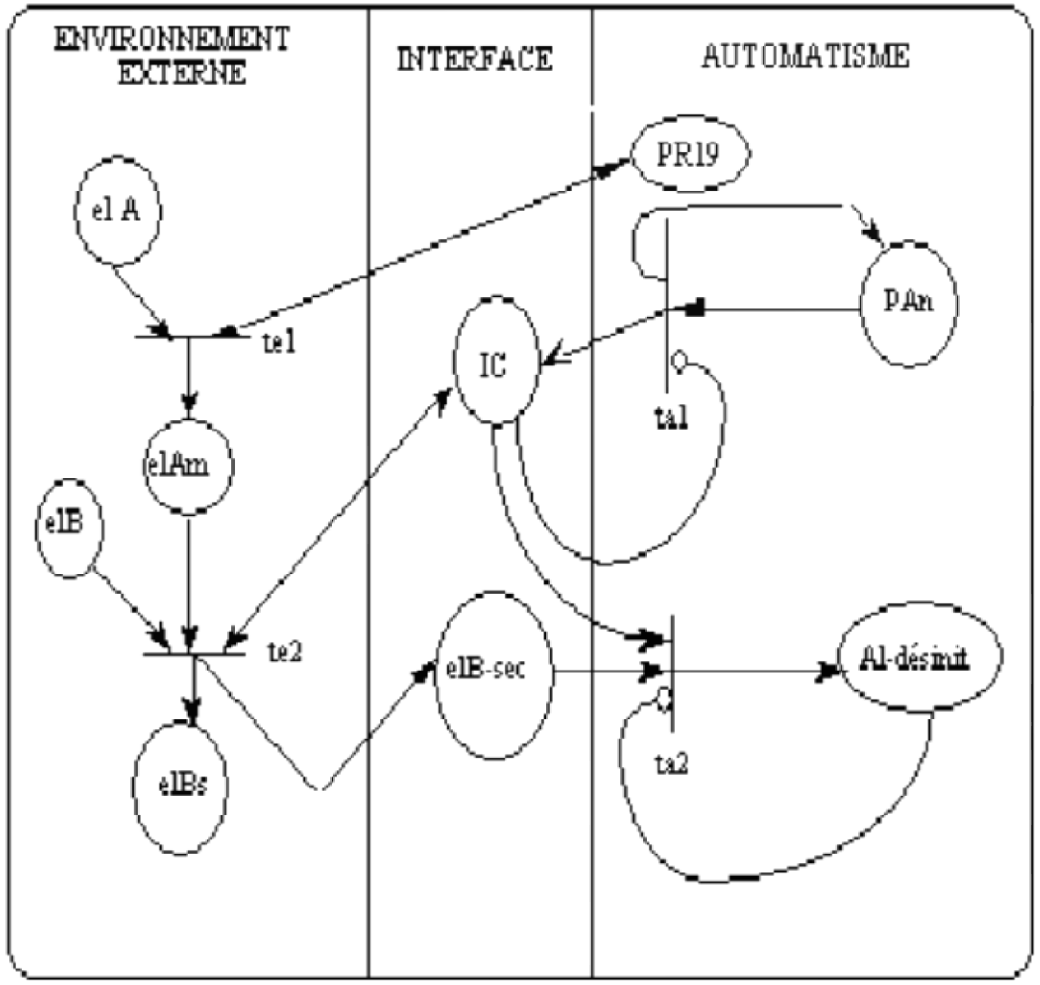
Diapo

Description Statique Versus Modèle Structurel de Cas



Diapo

Description Dynamique Versus modèle conversationnel de Cas



Légende

elA : élément A

elAm : élément A est muet

elB : élément B

elBs : élément B en conduite manuelle "secouru"

elB-sec : élément B déclaré secouru au niveau du PAn

IC : Initialisation en Cours

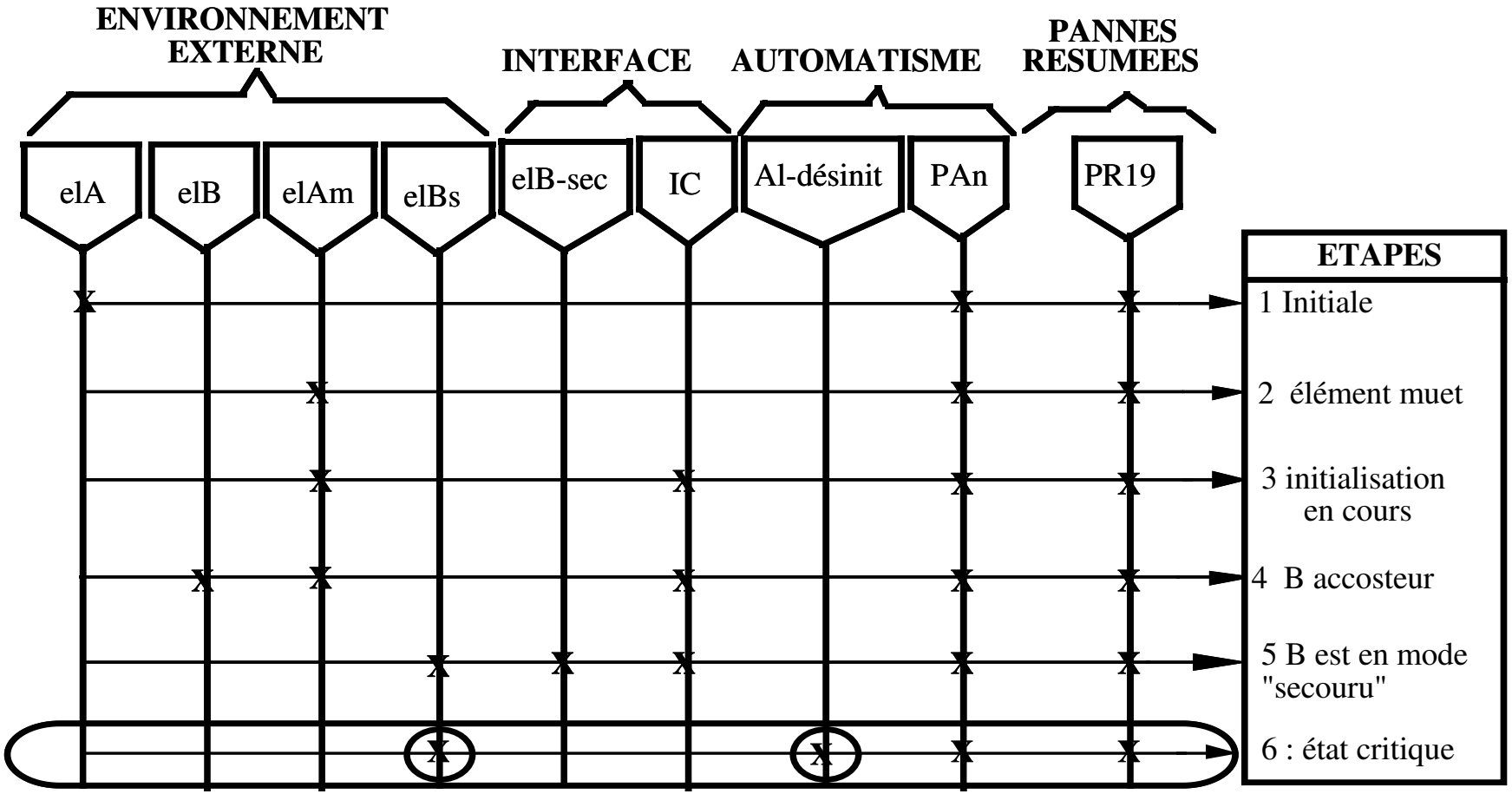
Al-désinit : alarme de désinitialisation

PAn : Pilote automatique de la zone amont (tronçon n) est actif

PR19 : Panne Résumée "élément muet"

Diapo

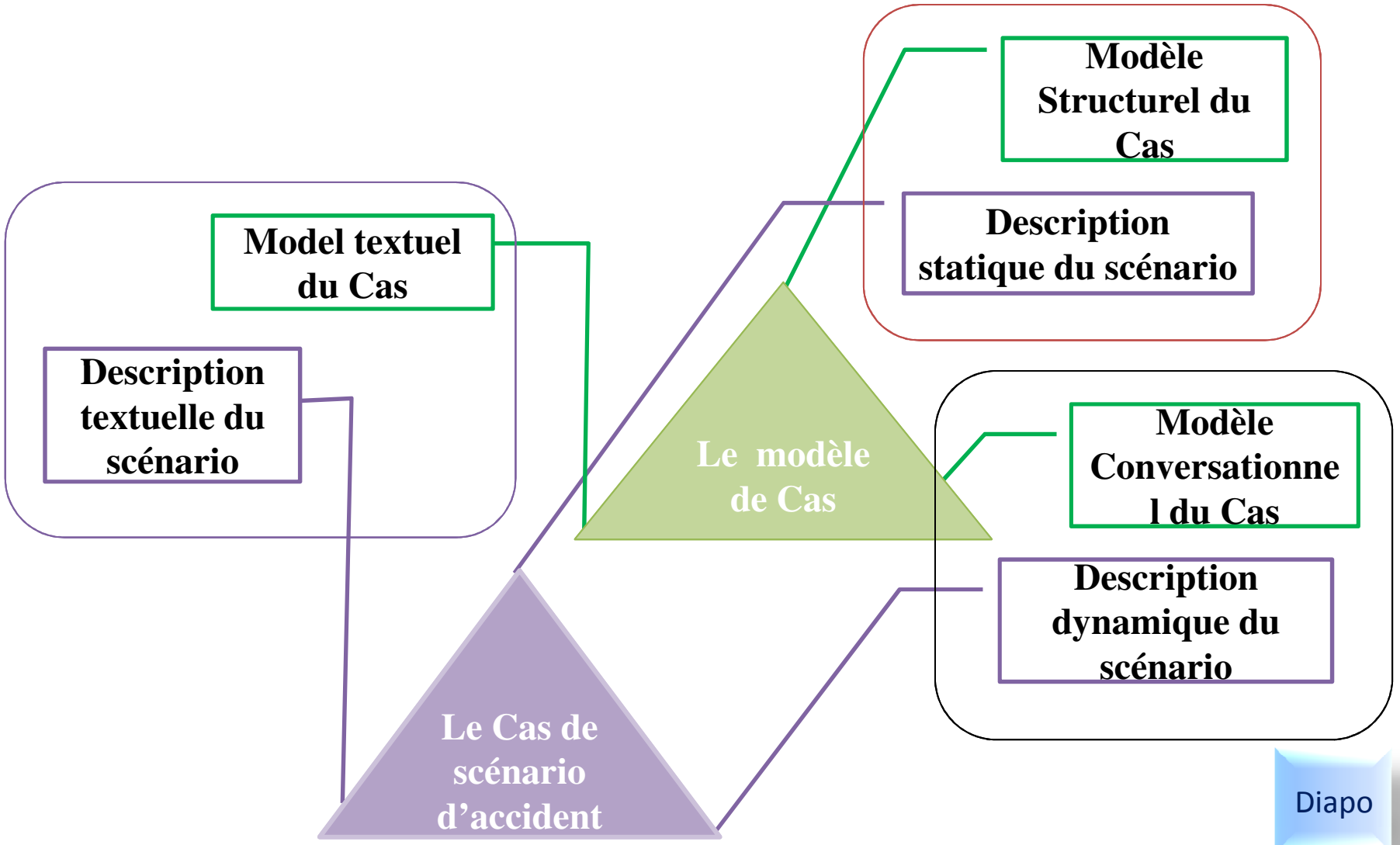
Description Dynamique versus modèle conversationnel de Cas



N.B. : • l'étape encadrée constitue la phase caractéristique (critique)
• les valeurs cerclées représentent les concepts clés

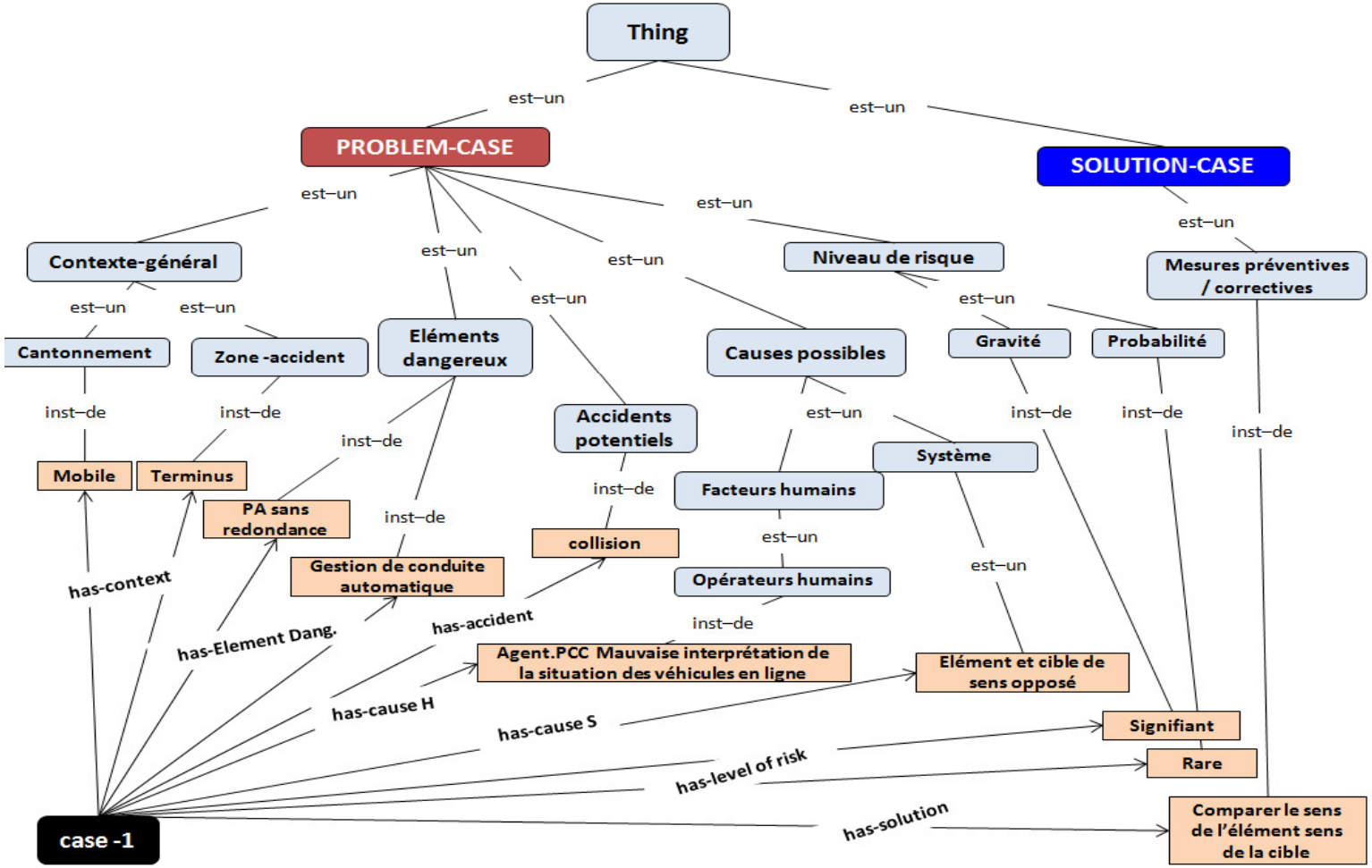
Diapo

Modèle Tridimensionnel du Cas



Diapo

Ontologie du domaine



Diapo

Le retour d'expérience

L'importance de la prise en compte de l'expérience et des leçons du passé

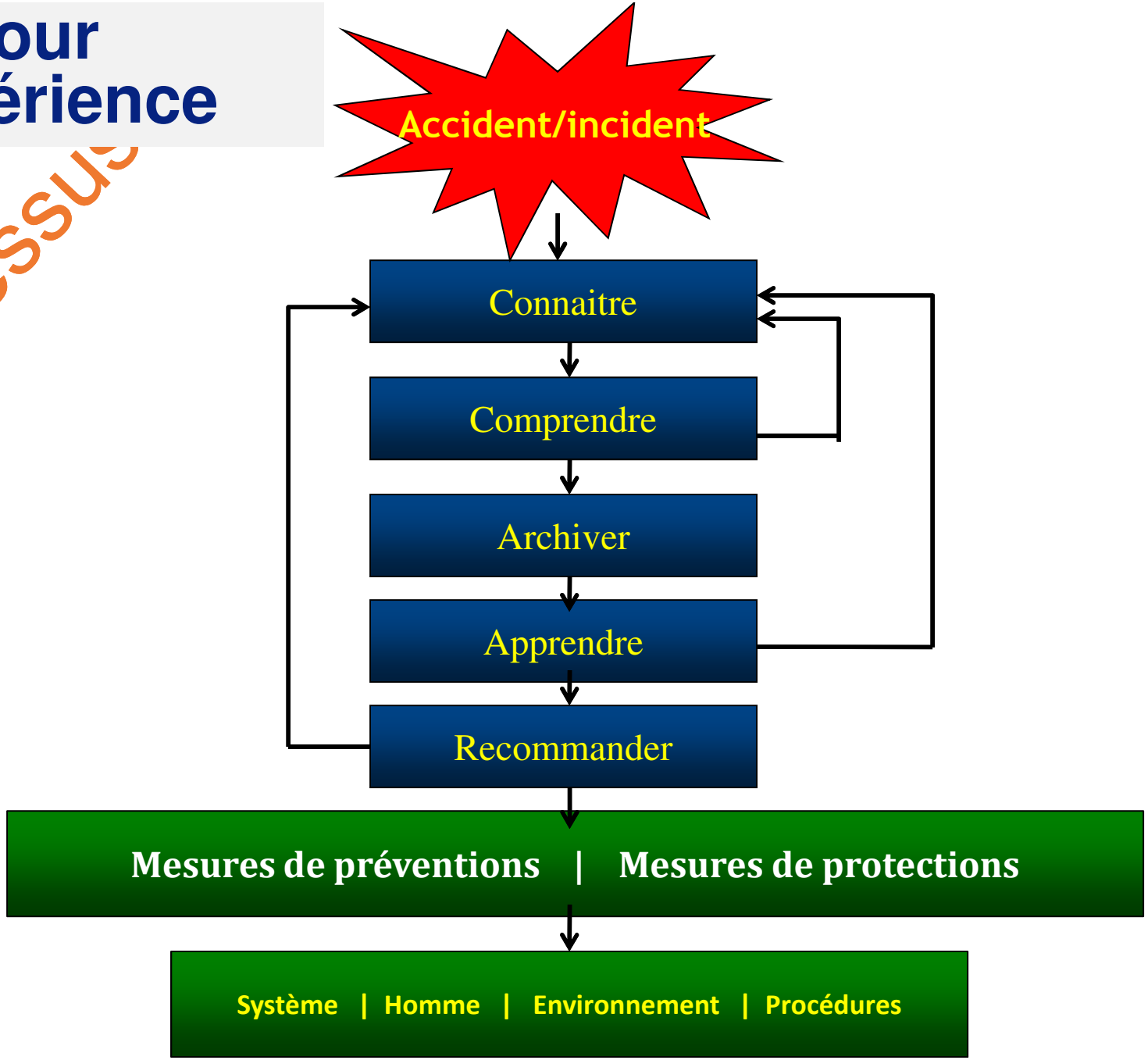
→ **la mise en place d'un système de retour d'expérience (Rex)**

l'un des biais essentiels de nature à promouvoir l'amélioration de la sécurité.
Tirer des leçons d'une expérience vécue pour éviter sa reproduction en mettant en œuvre des mesures préventives et correctives

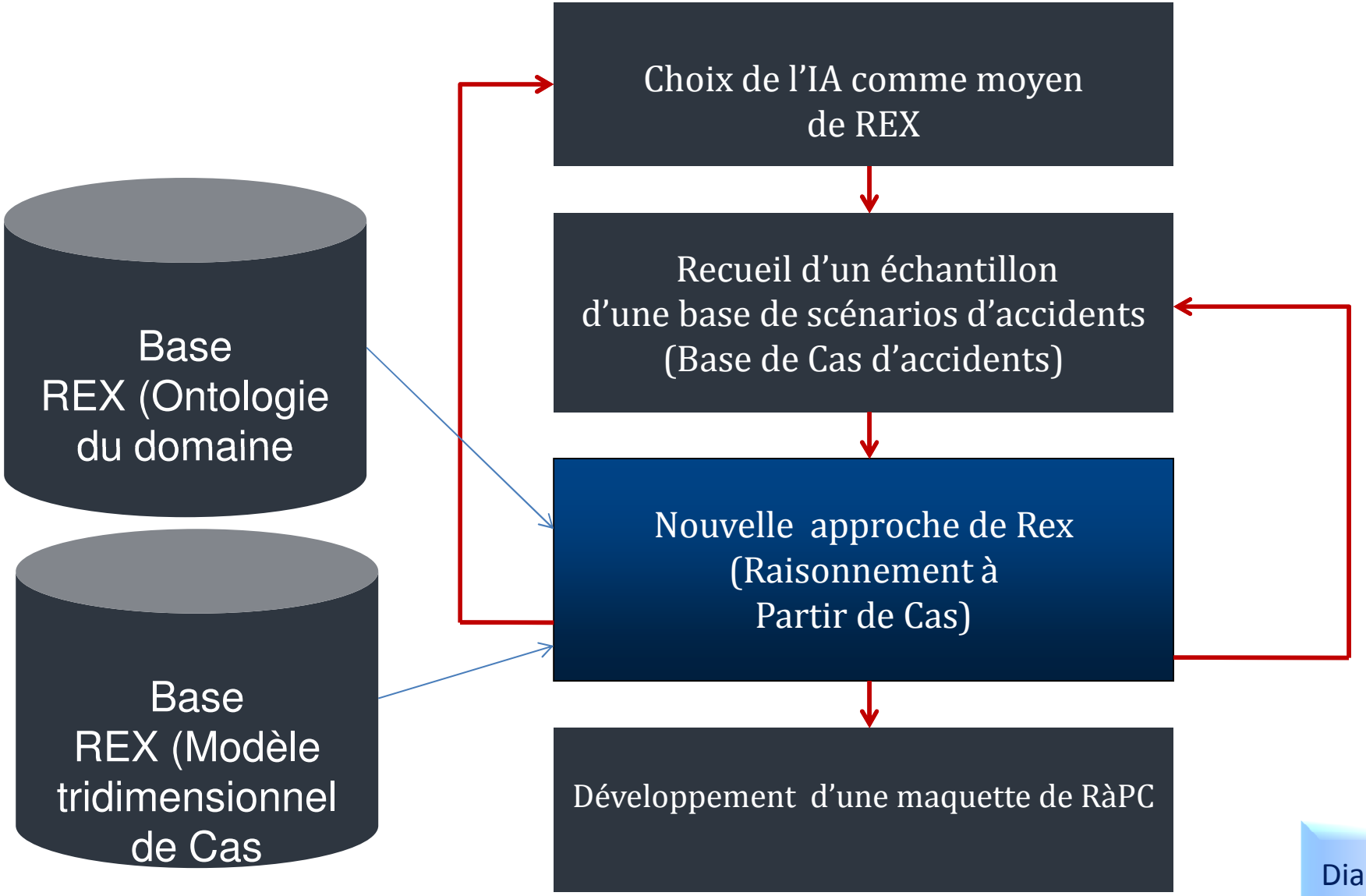
Diapo

Le retour d'expérience

Processus REX



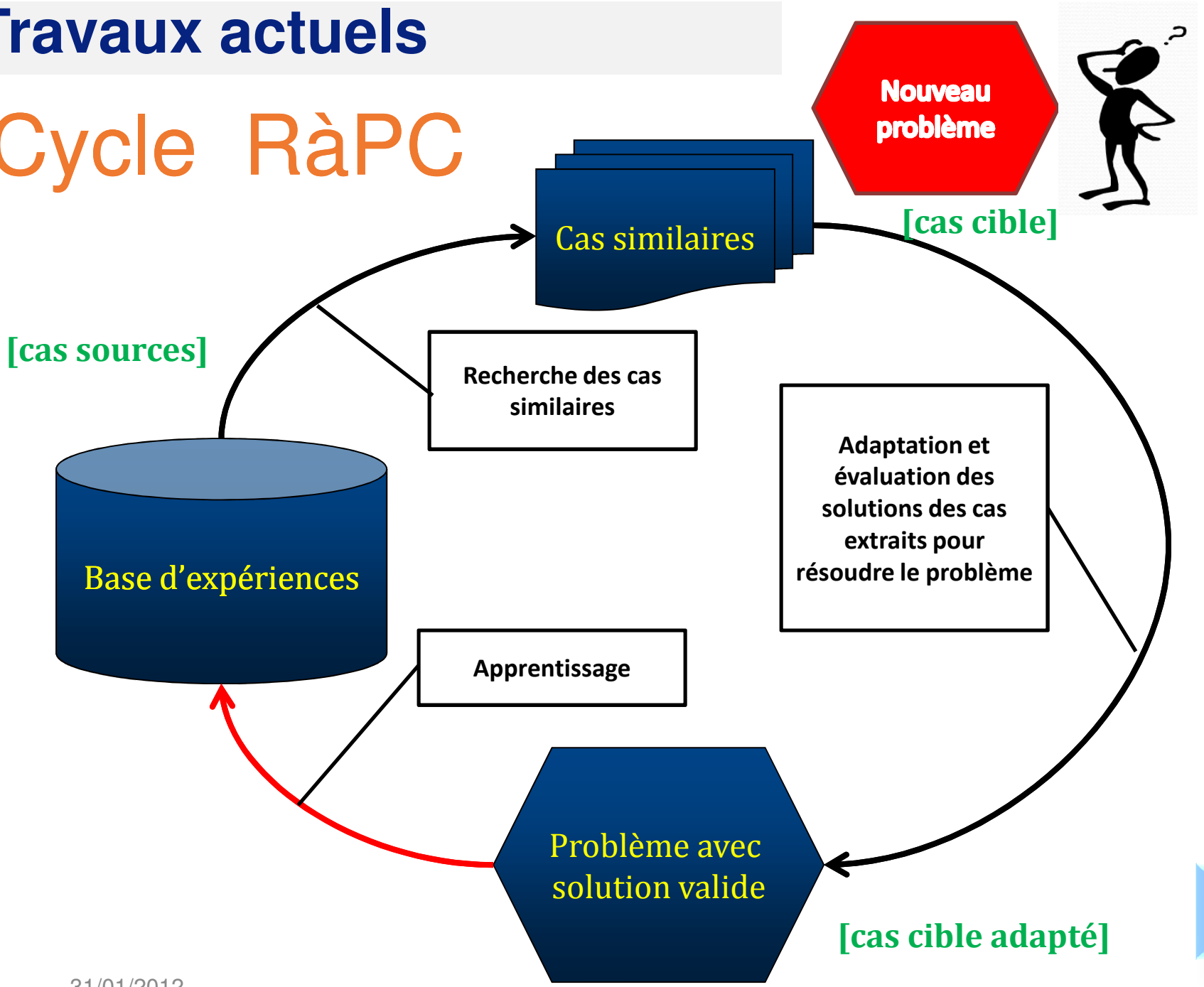
Travaux de recherche Actuelles



Diapo

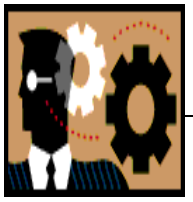
Travaux actuels

Cycle RàPC



Diapo

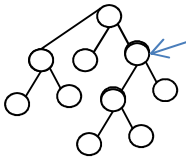
Démarche de réutilisation de cas d'accidents



Connaissances expertes

Retour d'expériences…etc.

Ontologie du Domaine



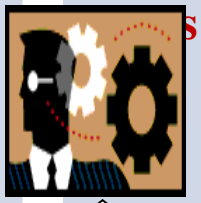
Acquisition et Formalisation des connaissances d'analyse dee sécurité

- Cas Structurels
– Cas Textuels et
- Cas Conversationnels

Classification par ACASYA de cas d'accidents structurels

Evaluation & Consolidation du cas conversationnel

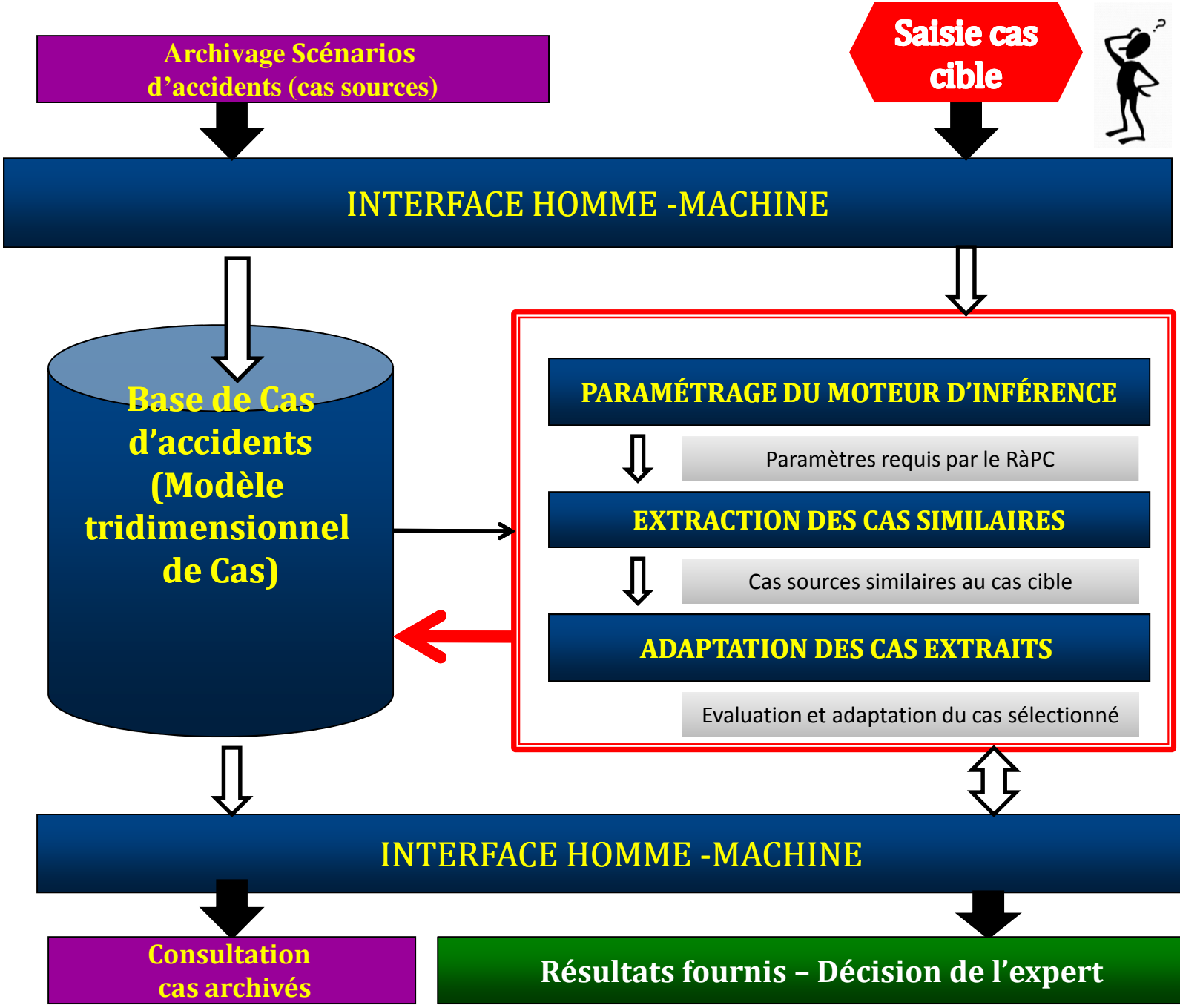
- Elaboration d'un Cas conversationnel généralisé par classe
- Simulation du cas généralisé
- Révision & Apprentissage du cas Conversationnel obtenu



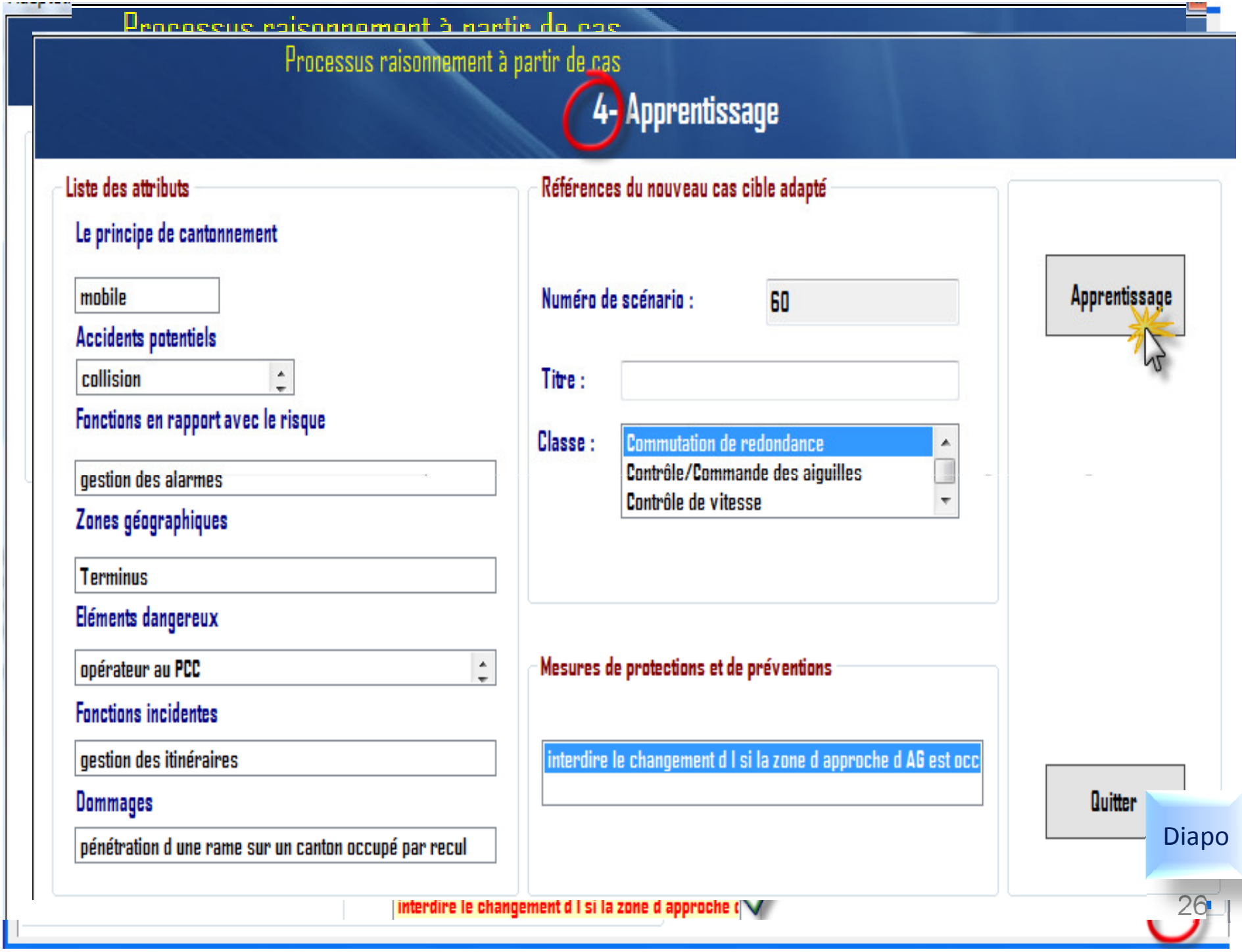
Evaluation & Consolidation structurel

- Remémoration du cas d'accident le plus proche de la classe du nouveau cas
- Adaptation du cas source remémoré de la classe
- Révision & Apprentissage du cas source structurel adapté

Diapo



Architecture fonctionnelle de la maquette


Processus raisonnement à partir de cas
4- Apprentissage
Liste des attributs
Le principe de cantonnement
mobile
Accidents potentiels
collision
Fonctions en rapport avec le risque
gestion des alarmes
Zones géographiques
Terminus
Eléments dangereux
opérateur au PCC
Fonctions incidentes
gestion des itinéraires
Dommages
pénétration d une rame sur un canton occupé par recul
Références du nouveau cas cible adapté
Numéro de scénario :
60
Titre :
Classe :
Commutation de redondance
Contrôle/Commande des aiguilles
Contrôle de vitesse
Mesures de protections et de préventions
interdire le changement d l si la zone d approche d AG est occ
Apprentissage
Quitter
Diapo
interdire le changement d l si la zone d approche d
26

Limites et Perspectives

La validation du bien fondé de la maquette nécessite :

- Choix d'un autre cas industriel
- Améliorations d'ordre technique
  - Enrichissement de la base de connaissances
  - Amélioration des algorithmes et les stratégies d'adaptation
- Comment utiliser les trois modèles de cas d'une manière conjointe et complémentaire

MERCI POUR VOTRE ATTENTION

Diapo