Analyse de risques des systèmes dynamiques avec la plate-forme de modélisation Figaro-KB3

Roland DONAT

roland.donat@edgemind.net

Séminaire Maîtrise des Risques et Systèmes Complexes

Vannes, 5 juin 2014

Plan

Plan

Enjeux industriels

Répondre aux contraintes réglementaires

Contraintes réglementaires

Les industries exploitant des systèmes complexes critiques (e.g. énergie, transport, défense) doivent s'adapter à des exigences réglementaires de plus en plus dures

Questions à traiter

- Quelles sont les scénarios de défaillance du système ?
- Quelle est la probabilité de chaque scénario ?
- Quelles sont les répercussions de chaque scénario ?

Conséquences

- Réalisation de nombreuses études afin de démontrer la sûreté des systèmes exploités

⇒ Développement de modèles et outils logiciels supports de plus en plus complexes

Enjeux industriels

Répondre aux contraintes réglementaires

Contraintes réglementaires

Les industries exploitant des systèmes complexes critiques (e.g. énergie, transport, défense) doivent s'adapter à des exigences réglementaires de plus en plus dures

Questions à traiter

- Quelles sont les scénarios de défaillance du système ?
- Quelle est la probabilité de chaque scénario ?
- Quelles sont les répercussions de chaque scénario ?

Conséquences

- Réalisation de nombreuses études afin de démontrer la sûreté des systèmes exploités

⇒ Développement de modèles et outils logiciels supports de plus en plus complexes

Enjeux industriels

Répondre aux contraintes réglementaires

Contraintes réglementaires

Les industries exploitant des systèmes complexes critiques (e.g. énergie, transport, défense) doivent s'adapter à des exigences réglementaires de plus en plus dures

Questions à traiter

- Quelles sont les scénarios de défaillance du système ?
- Quelle est la probabilité de chaque scénario ?
- Quelles sont les répercussions de chaque scénario ?

Conséquences

- Réalisation de nombreuses études afin de démontrer la sûreté des systèmes exploités

⇒ Développement de modèles et outils logiciels supports de plus en plus complexes

Enjeux industriels

Répondre aux contraintes économiques

Contraintes économiques

Le contexte de plus en plus concurrentiel pousse les industriels à optimiser les performances de leurs systèmes

Question à traiter

Comment diminuer les risques de défaillance du système en maîtrisant son coût d'exploitation ?

Conséquences

- Volonté forte d'optimiser les processus industriels (production, maintenance, etc)

$\Rightarrow$ Développement de nouveaux outils d'optimisation et d'aide à la décision pour l'évaluation des stratégies d'exploitation des systèmes

Enjeux industriels

Répondre aux contraintes économiques

Contraintes économiques

Le contexte de plus en plus concurrentiel pousse les industriels à optimiser les performances de leurs systèmes

Question à traiter

Comment diminuer les risques de défaillance du système en maîtrisant son coût d'exploitation ?

Conséquences

- Volonté forte d'optimiser les processus industriels (production, maintenance, etc)

⇒ Développement de nouveaux outils d'optimisation et d'aide à la décision pour l'évaluation des stratégies d'exploitation des systèmes

Enjeux industriels

Répondre aux contraintes économiques

Contraintes économiques

Le contexte de plus en plus concurrentiel pousse les industriels à optimiser les performances de leurs systèmes

Question à traiter

Comment diminuer les risques de défaillance du système en maîtrisant son coût d'exploitation ?

Conséquences

- Volonté forte d'optimiser les processus industriels (production, maintenance, etc)

$\Rightarrow$ Développement de nouveaux outils d'optimisation et d'aide à la décision pour l'évaluation des stratégies d'exploitation des systèmes

Enjeux industriels

Conséquences

Constat général

- Dans de nombreuses industries, les décisions faces aux risques reposent encore uniquement sur des avis d'experts

⇒ Risque : Stratégies en décalage avec la réalité physique du système

⇒ Conséquence : Mise en place de solutions sous-optimales

Objectif : Optimiser l'exploitation des systèmes critiques

- Maîtriser les coûts d'exploitation
- Garantir un niveau de sûreté satisfaisant

Contraintes fortes ⇒ Évolution de l'analyse de risques

1. De l'analyse qualitative à l'**analyse quantitative**
2. Des cas tests aux **cas industriels**
3. Des modèles statiques aux **modèles dynamiques**

Enjeux industriels

Conséquences

Constat général

- Dans de nombreuses industries, les décisions faces aux risques reposent encore uniquement sur des avis d'experts

⇒ Risque : Stratégies en décalage avec la réalité physique du système

⇒ Conséquence : Mise en place de solutions sous-optimales

Objectif : Optimiser l'exploitation des systèmes critiques

- Maîtriser les coûts d'exploitation
- Garantir un niveau de sûreté satisfaisant

Contraintes fortes ⇒ Évolution de l'analyse de risques

1. De l'analyse qualitative à l'**analyse quantitative**
2. Des cas tests aux **cas industriels**
3. Des modèles statiques aux **modèles dynamiques**

Enjeux industriels

Conséquences

Constat général

- Dans de nombreuses industries, les décisions faces aux risques reposent encore uniquement sur des avis d'experts

⇒ Risque : Stratégies en décalage avec la réalité physique du système

⇒ Conséquence : Mise en place de solutions sous-optimales

Objectif : Optimiser l'exploitation des systèmes critiques

- Maîtriser les coûts d'exploitation
- Garantir un niveau de sûreté satisfaisant

Contraintes fortes ⇒ Évolution de l'analyse de risques

1. De l'analyse qualitative à l'**analyse quantitative**
2. Des cas tests aux **cas industriels**
3. Des modèles statiques aux **modèles dynamiques**

Démarche d'analyse des risques

Objectifs

Systèmes complexes critiques

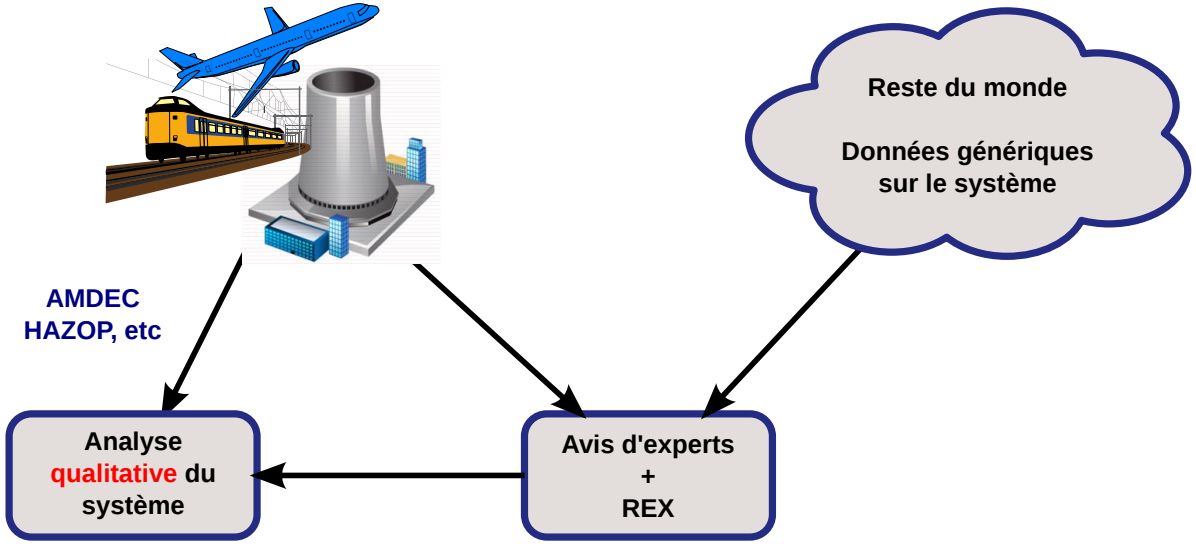
Démarche d'analyse des risques

Objectifs

Objectifs :
- Répondre aux exigences réglementaires
- Améliorer les performances

Démarche d'analyse des risques

Approche qualitative



Analyse de risques qualitative

Démarche d'analyse des risques

Approche quantitative

Reste du monde

Données génériques sur le système

AMDEC
HAZOP, etc

GMAO

Analyse qualitative du système

Données de REX
+
Avis d'experts

Analyse statistique

Choix d'un formalisme de modélisation

Développement d'un modèle système

Exploitation quantitative du modèle

Analyse de risques quantitative

Démarche d'analyse des risques

Approche quantitative

Reste du monde

Données génériques sur le système

AMDEC
HAZOP, etc

GMAO

Analyse qualitative du système

Données de REX + Avis d'experts

Analyse statistique

Choix d'un formalisme de modélisation

Développement d'un modèle système

Exploitation quantitative du modèle

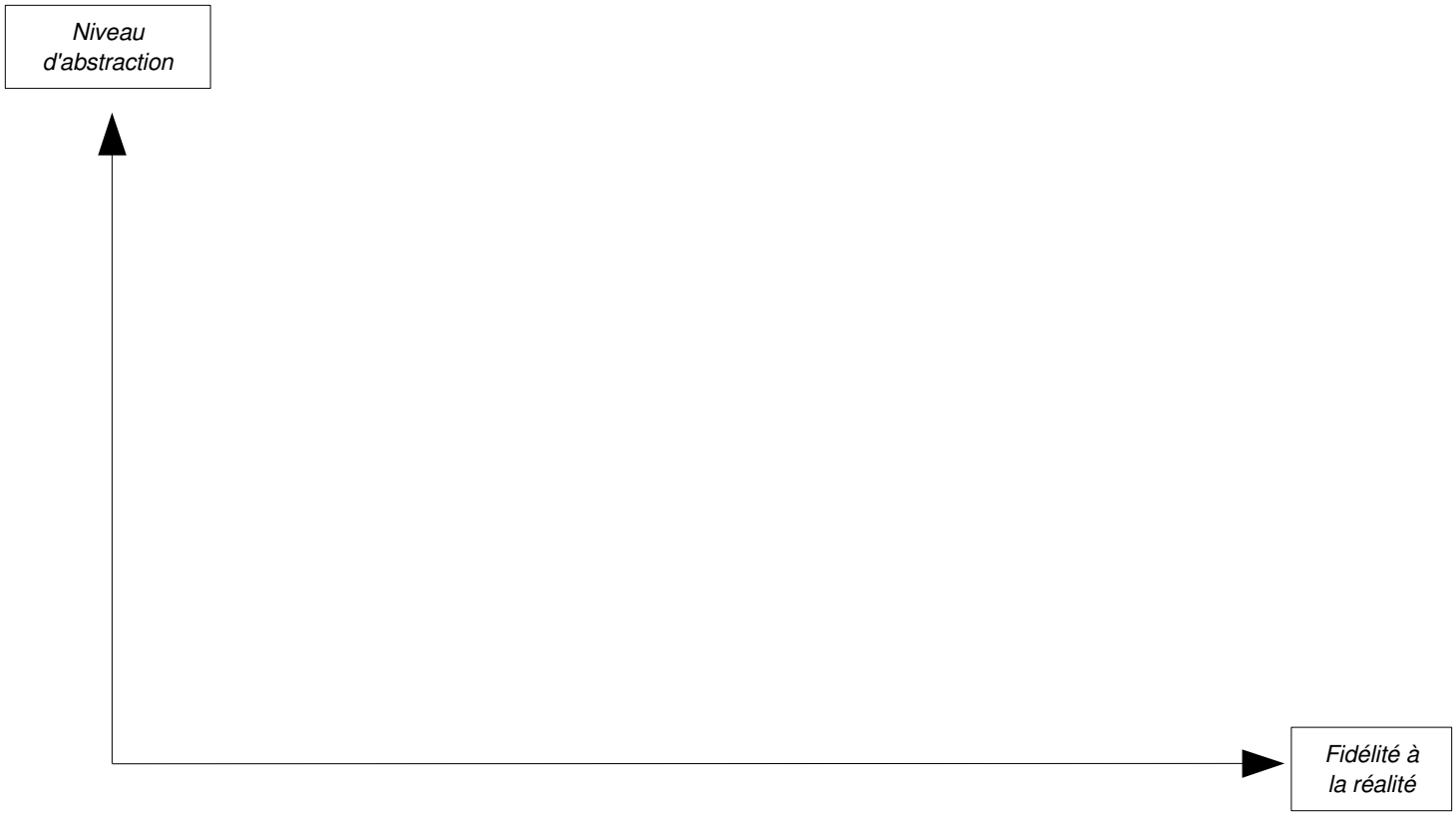
Décisions

Analyse de risques quantitative

Plan

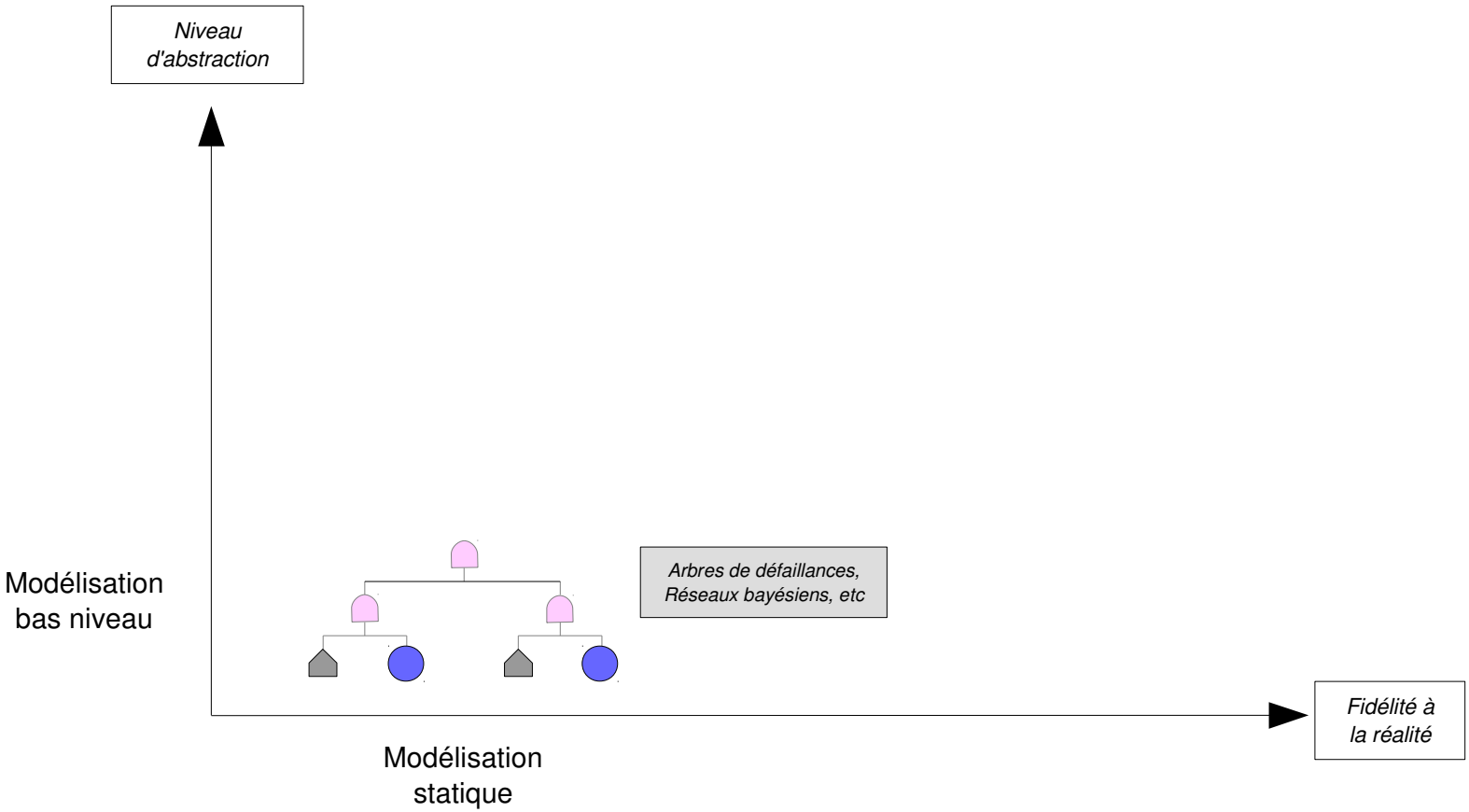
Évolution des techniques de modélisation

Tendances générales



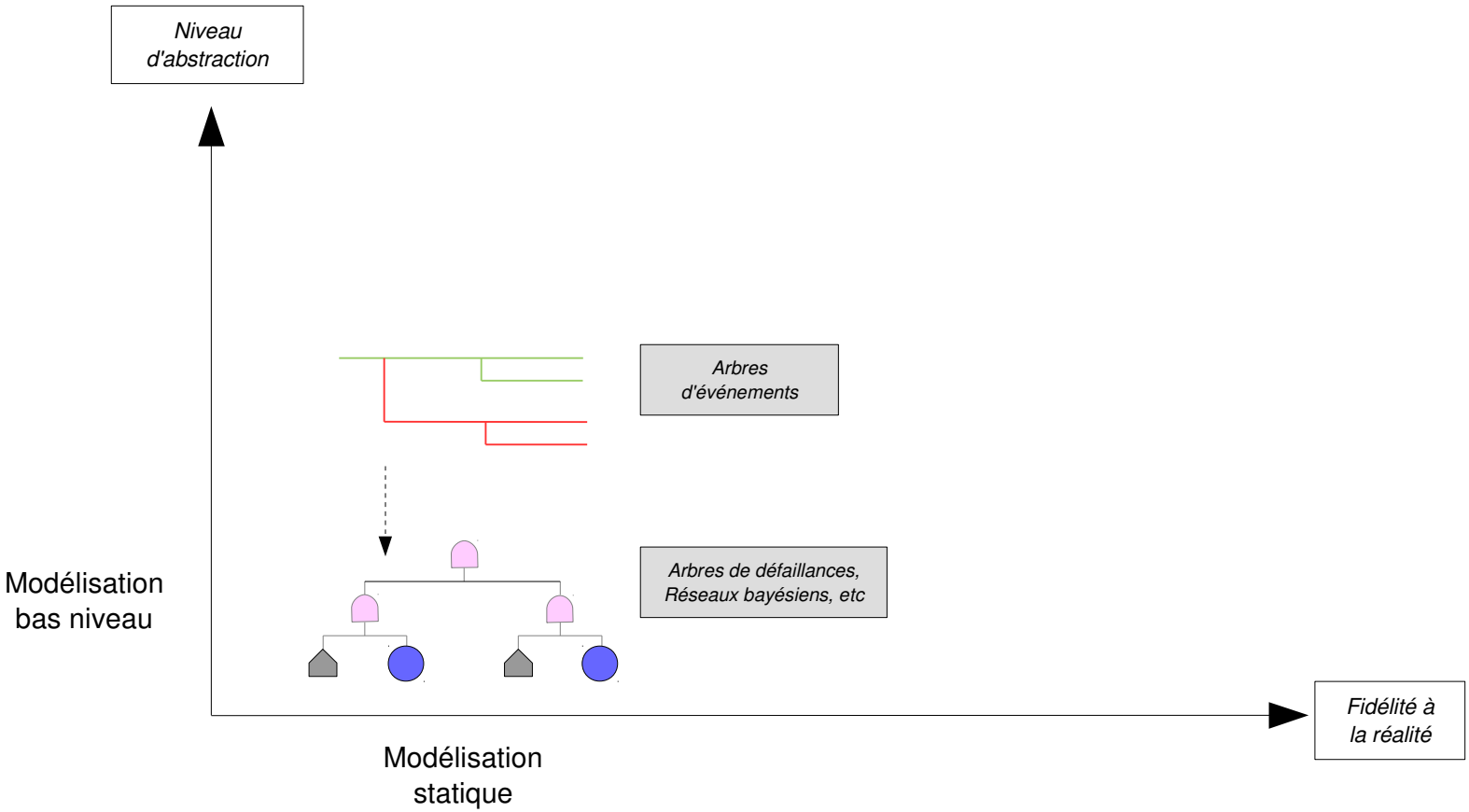
Évolution des techniques de modélisation

Tendances générales



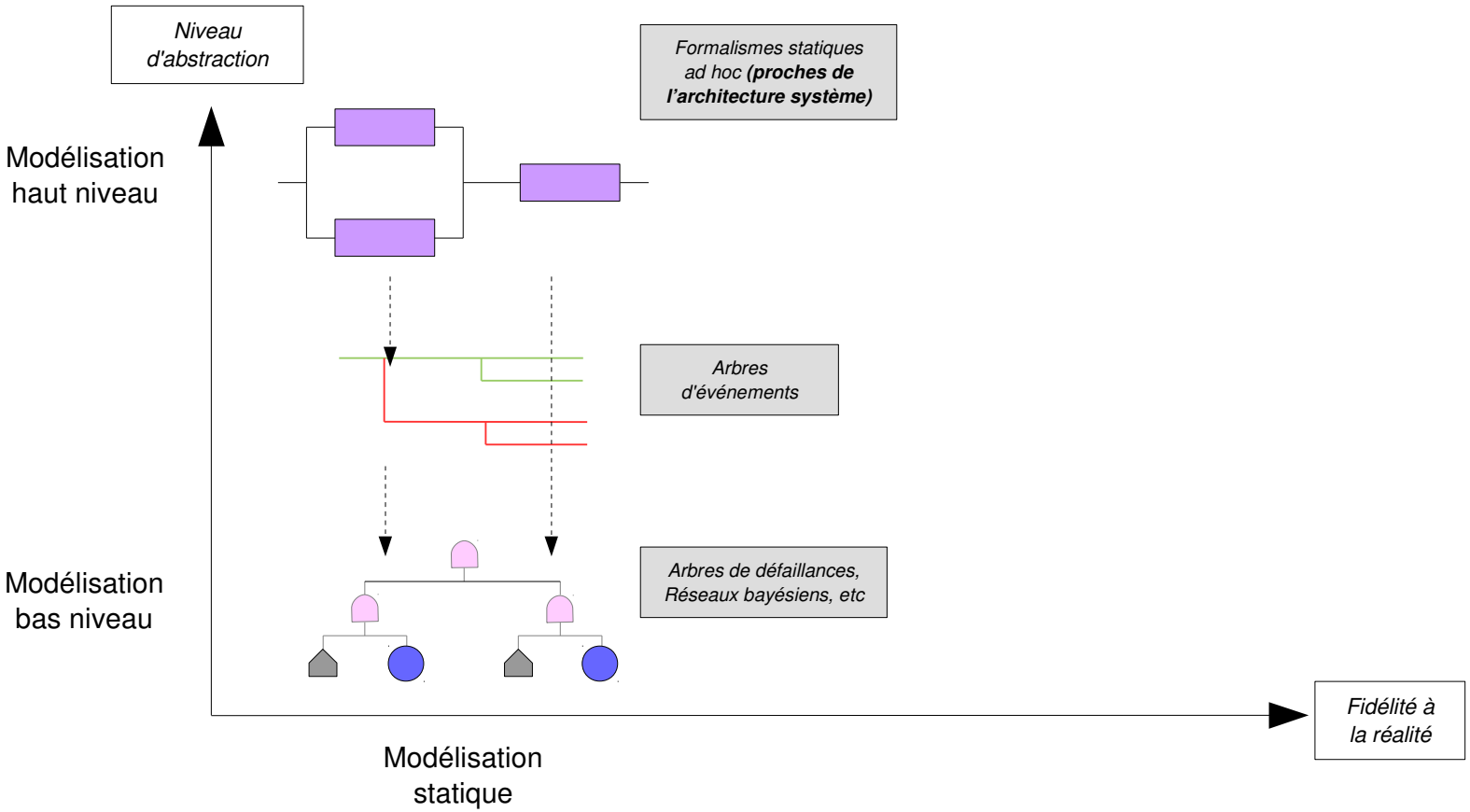
Évolution des techniques de modélisation

Tendances générales



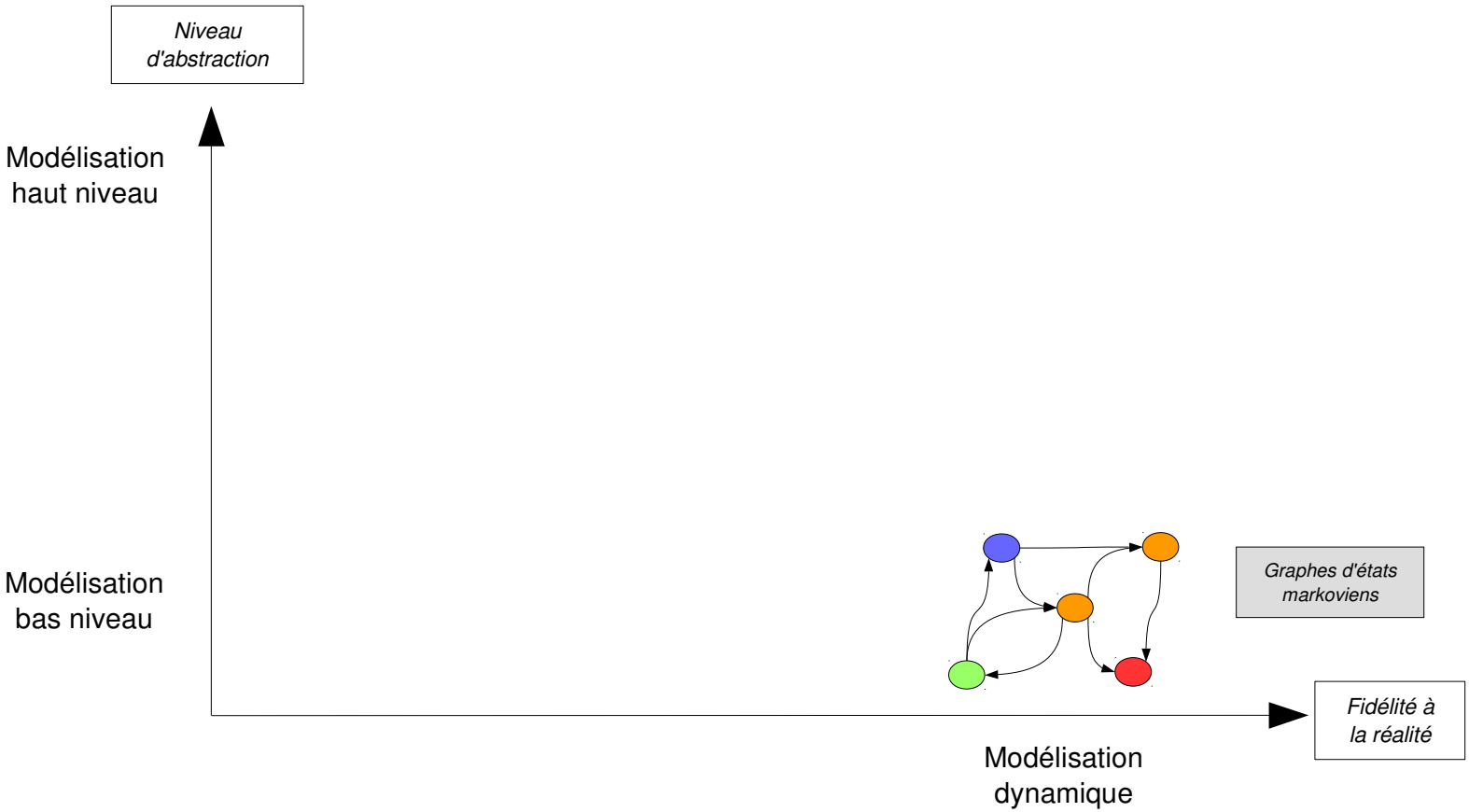
Évolution des techniques de modélisation

Tendances générales



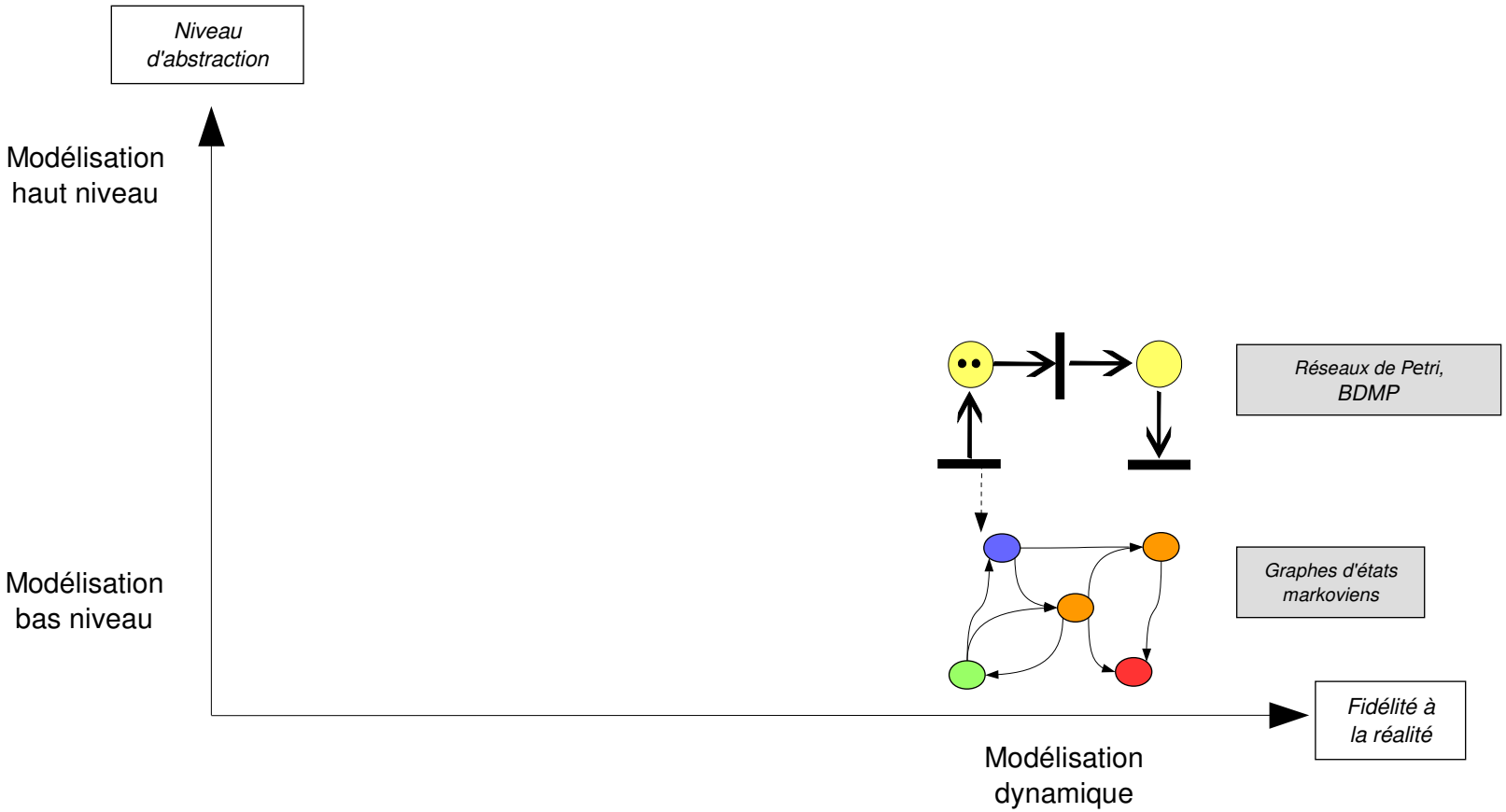
Évolution des techniques de modélisation

Tendances générales



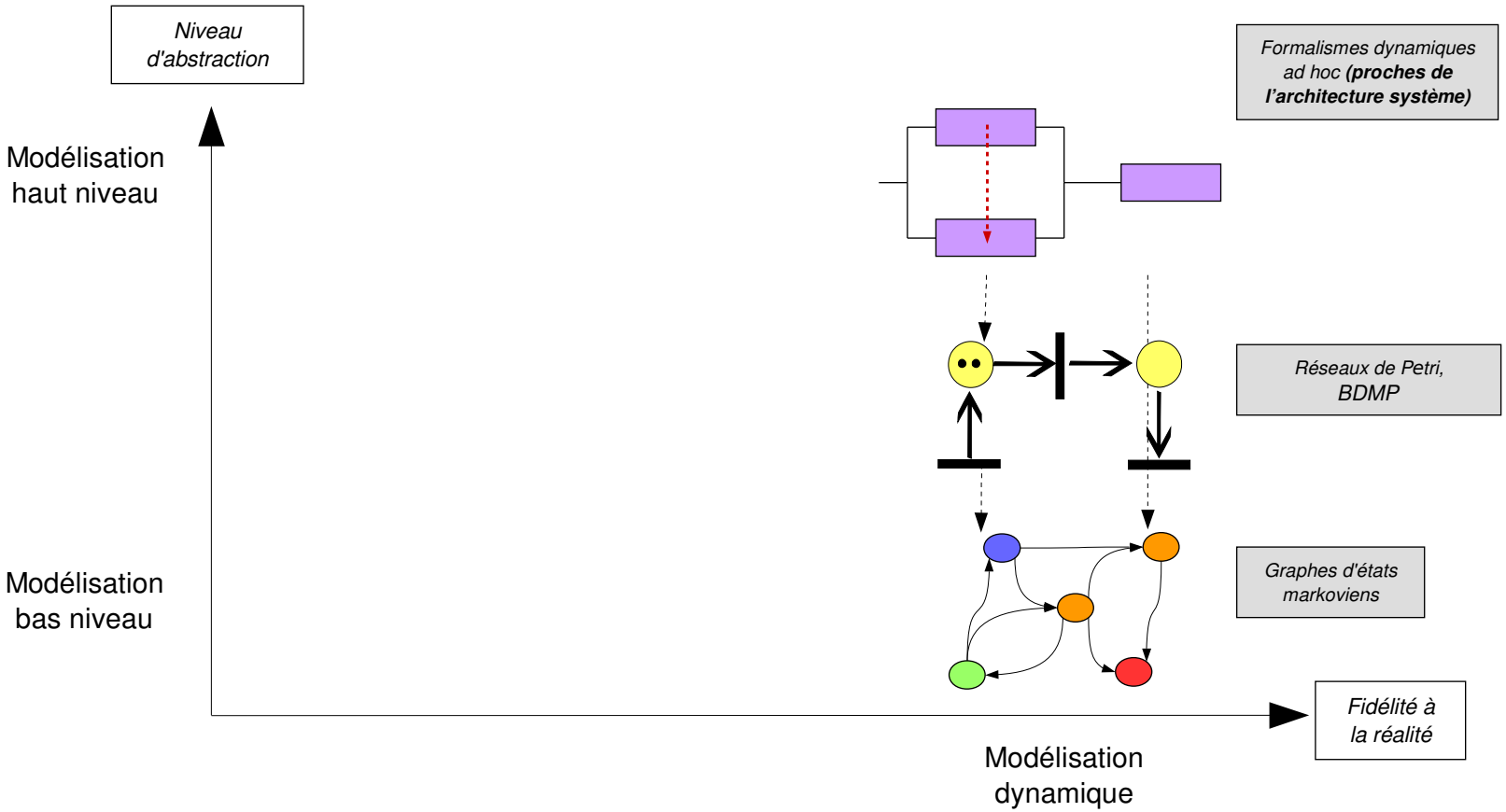
Évolution des techniques de modélisation

Tendances générales



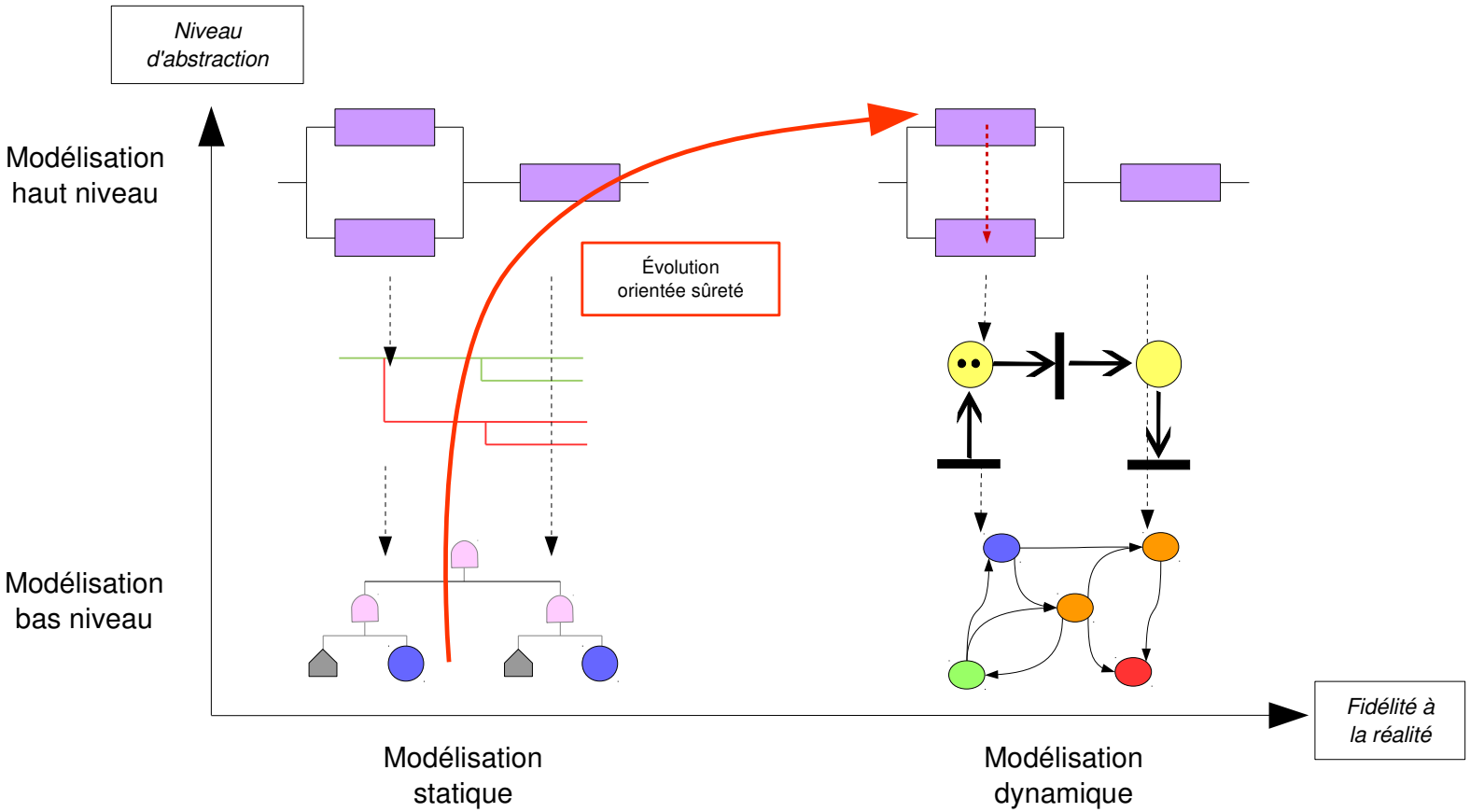
Évolution des techniques de modélisation

Tendances générales



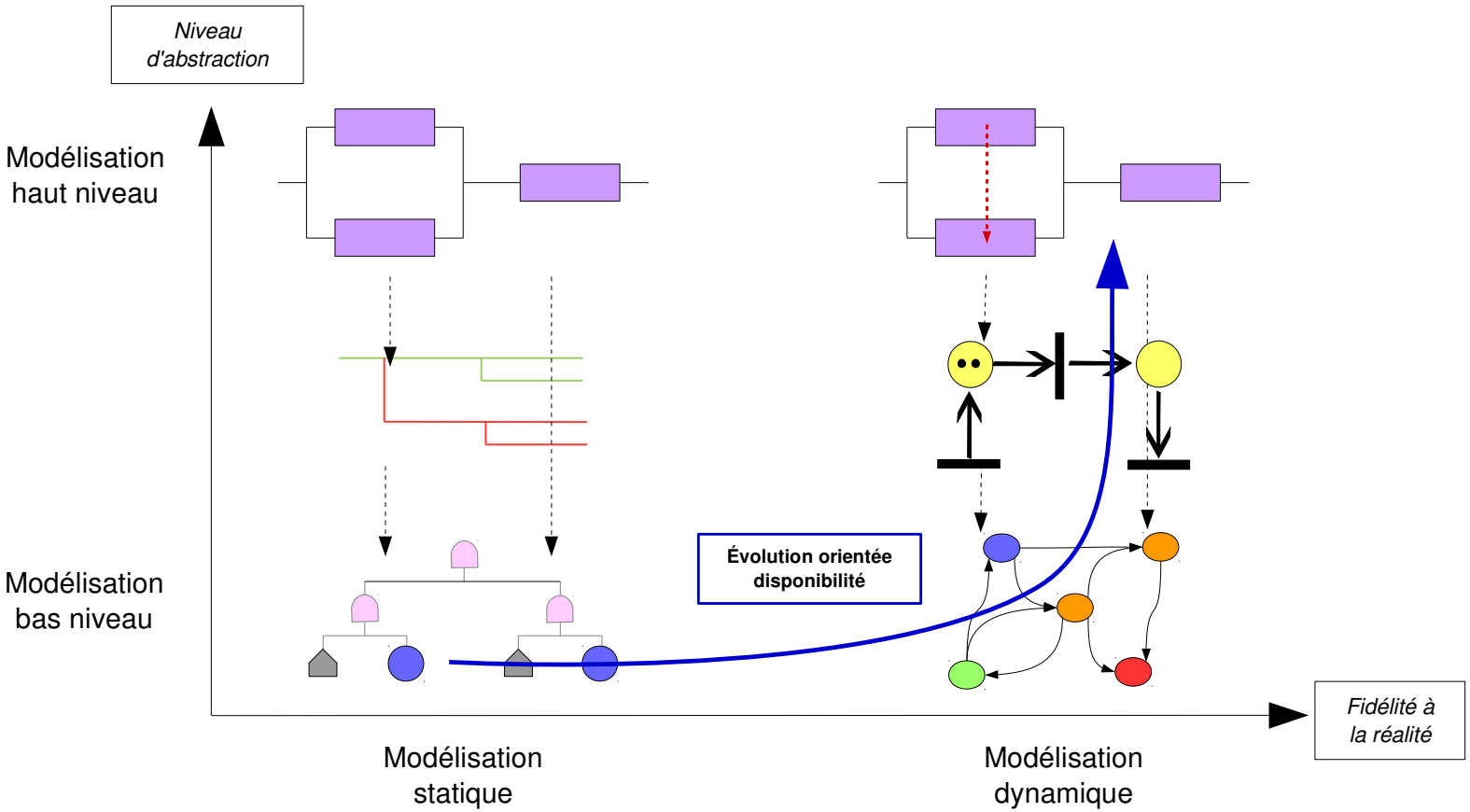
Évolution des techniques de modélisation

Tendances générales



Évolution des techniques de modélisation

Tendances générales



Évolution des techniques de modélisation

Modélisation bas niveau vs haut niveau

Modélisation bas niveau

- ☺ Flexible et non dépendante de la nature du système étudié
- ☹ Difficile de construire et de maintenir de grands modèles
- ☹ Risque d'effets d'auteurs

Modélisation haut niveau

- ☺ Manipulation de concepts proches du métier
- ☺ Aide à structurer et capitaliser la connaissance sur les systèmes
- ☺ Facilite la gestion de la complexité des modèles
- ☹ Nécessite la construction du formalisme adapté aux systèmes étudiés

Évolution des techniques de modélisation

Modélisation bas niveau vs haut niveau

Modélisation bas niveau

- ☺ Flexible et non dépendante de la nature du système étudié
- ☹ Difficile de construire et de maintenir de grands modèles
- ☹ Risque d'effets d'auteurs

Modélisation haut niveau

- ☺ Manipulation de concepts proches du métier
- ☺ Aide à structurer et capitaliser la connaissance sur les systèmes
- ☺ Facilite la gestion de la complexité des modèles
- ☹ Nécessite la construction du formalisme adapté aux systèmes étudiés

Évolution des techniques de modélisation

Modélisation statique vs dynamique

Modélisation statique

- ☺ Bien maîtrisée par les fiabilistes
- ☺ Efficacité des algorithmes de calculs associés
- ☹ Peu fidèle à la réalité fonctionnelle (la plupart des systèmes étant intrinsèquement dynamiques)
- ☹ Analyse quantitative limitée

Modélisation dynamique

- ☺ Approche intuitive et proche du fonctionnement des systèmes étudiés
- ☺ Analyse quantitative riche et détaillée des systèmes au cours du temps
- ☹ Complexité des calculs associés $\Rightarrow$ Limitation de la taille des modèles

Évolution des techniques de modélisation

Modélisation statique vs dynamique

Modélisation statique

- ☺ Bien maîtrisée par les fiabilistes
- ☺ Efficacité des algorithmes de calculs associés
- ☹ Peu fidèle à la réalité fonctionnelle (la plupart des systèmes étant intrinsèquement dynamiques)
- ☹ Analyse quantitative limitée

Modélisation dynamique

- ☺ Approche intuitive et proche du fonctionnement des systèmes étudiés
- ☺ Analyse quantitative riche et détaillée des systèmes au cours du temps
- ☹ Complexité des calculs associés $\Rightarrow$ Limitation de la taille des modèles

Modélisation haut niveau

Apparition des métalangages (1/2)

Constat

- Accroissement de la complexité (taille, comportement à représenter) des modèles associés aux systèmes industriels
- Formalismes génériques de modélisation graphiques inappropriés pour gérer cette complexité

Idée

Développement de métalangages [a] de modélisation

- **Dédiés à l'analyse des risques**
- Capables d'exprimer des comportements aléatoires complexes
- Munis d'une syntaxe intuitive (voire proche du langage naturel)

a. Langage permettant de décrire d'autres formalismes de modélisation

Modélisation haut niveau

Apparition des métalangages (1/2)

Constat

- Accroissement de la complexité (taille, comportement à représenter) des modèles associés aux systèmes industriels
- Formalismes génériques de modélisation graphiques inappropriés pour gérer cette complexité

Idée

Développement de métalangages [a] de modélisation

- **Dédiés à l'analyse des risques**
- Capables d'exprimer des comportements aléatoires complexes
- Munis d'une syntaxe intuitive (voire proche du langage naturel)

a. Langage permettant de décrire d'autres formalismes de modélisation

Modélisation haut niveau

Apparition des métalangages (2/2)

Objectifs

- Construire de nouveaux formalismes de modélisation adaptée à l'étude d'une classe de systèmes donnés (ex : systèmes électriques, barrage, automobile, voies ferrées, etc)
- Assurer traçabilité et transparence dans les modèles développés
- Diminuer les coûts de modélisation à long terme
- Exploiter un socle commun d'outils d'analyses quantitatives

Attention aux métalangages inadaptés

- Risque d'un défaut d'expressivité dans le domaine technique visé
- Difficulté pour réaliser des études quantitatives pertinentes

Modélisation haut niveau

Apparition des métalangages (2/2)

Objectifs

- Construire de nouveaux formalismes de modélisation adaptée à l'étude d'une classe de systèmes donnés (ex : systèmes électriques, barrage, automobile, voies ferrées, etc)
- Assurer traçabilité et transparence dans les modèles développés
- Diminuer les coûts de modélisation à long terme
- Exploiter un socle commun d'outils d'analyses quantitatives

Attention aux métalangages inadaptés

- Risque d'un défaut d'expressivité dans le domaine technique visé
- Difficulté pour réaliser des études quantitatives pertinentes

Modélisation haut niveau

Principaux métalangages en analyse de risques (1/4)

Figaro (Bouissou et al. 1991)

- Créé par le département Maîtrise des Risques Industriels d'EDF R&D au début des années 90
- Toujours maintenu activement par EDF R&D
- Version unique et stable du langage
- Créé à l'origine pour générer les AdD et les modèles dynamiques dans les Études Probabilistes de Sûreté nucléaire

Modélisation haut niveau

Principaux métalangages en analyse de risques (2/4)

AltaRica (POINT 2000)

- Créé par le LaBRI et un groupe d'industriels fin des années 90
- Maintenu et décliné aujourd'hui par différents industriels (ex : Dassault System/Aviation, APSYS) et universitaires (LaBRI)
- Existence de diverses variantes (syntaxe et sémantique)
- Utilisé principalement dans les domaines de l'aéronautique
- Démarrage du projet Altarica 3.0 (PROSVIRNOVA et al. 2013)

Modélisation haut niveau

Principaux métalangages en analyse de risques (3/4)

Caractéristiques techniques

- Langages orientés objets ($\Rightarrow$ notion d'héritage)
- Modélisation reposant sur les concepts d'**attributs**, d'**interfaces** et de **transitions**
- Description du comportement des systèmes cibles à partir de règles déterministes et aléatoires
- Inférence reposant sur la théorie des automates stochastiques à transitions gardées

$\Rightarrow$ Permet de décrire des processus stochastiques à états dénombrables et à temps continu

Comparaison Figaro vs Altarica 2 : (Bouissou et Seguin 2006)

Modélisation haut niveau

Principaux métalangages en analyse de risques (4/4)

Outils d'analyses associés

- Calcul d'indicateurs par simulation stochastique
- Exploration et quantification des scénarios de défaillances
- Vérificateur de modèle
- Génération d'arbres de défaillances

Plan

Langage Figaro

Principes de modélisation

1. Développement de bases de connaissances (BdC)
   - Une BdC = Spécification d'un formalisme de modélisation

   $\Rightarrow$ Une BdC = Une boite à outils de modélisation
2. Modélisation d'un système particulier à partir d'une BdC adaptée
3. Exploitation des modèles Figaro à partir de la plate-forme outils Figaro

Deux types de BdC

- BdC générique : Description d'un formalisme de modélisation général (ex : graphes de Markov, RdP, BDMP, etc)
- BdC *Smart Components* : Description fonctionnelle et dysfonctionnelle d'une classe de systèmes physiques

Langage Figaro

Principes de modélisation

1. Développement de bases de connaissances (BdC)
   - Une BdC = Spécification d'un formalisme de modélisation

   $\Rightarrow$ Une BdC = Une boite à outils de modélisation
2. Modélisation d'un système particulier à partir d'une BdC adaptée
3. Exploitation des modèles Figaro à partir de la plate-forme outils Figaro

Deux types de BdC

- BdC générique : Description d'un formalisme de modélisation général (ex : graphes de Markov, RdP, BDMP, etc)
- BdC *Smart Components* : Description fonctionnelle et dysfonctionnelle d'une classe de systèmes physiques

Exemple d'architecture d'une BdC

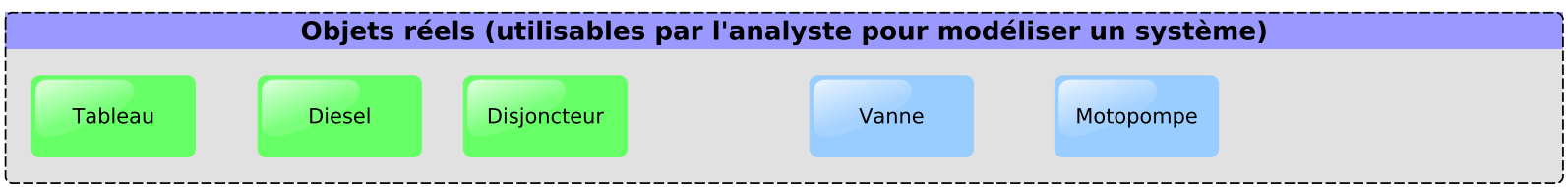
Problématiques

Objectifs

- Construction d'un formalisme de modélisation adapté à la représentation des systèmes électriques et hydrauliques
- Prendre en compte différents modes de défaillances
- Permettre de définir des stratégies de maintenance par type de composant

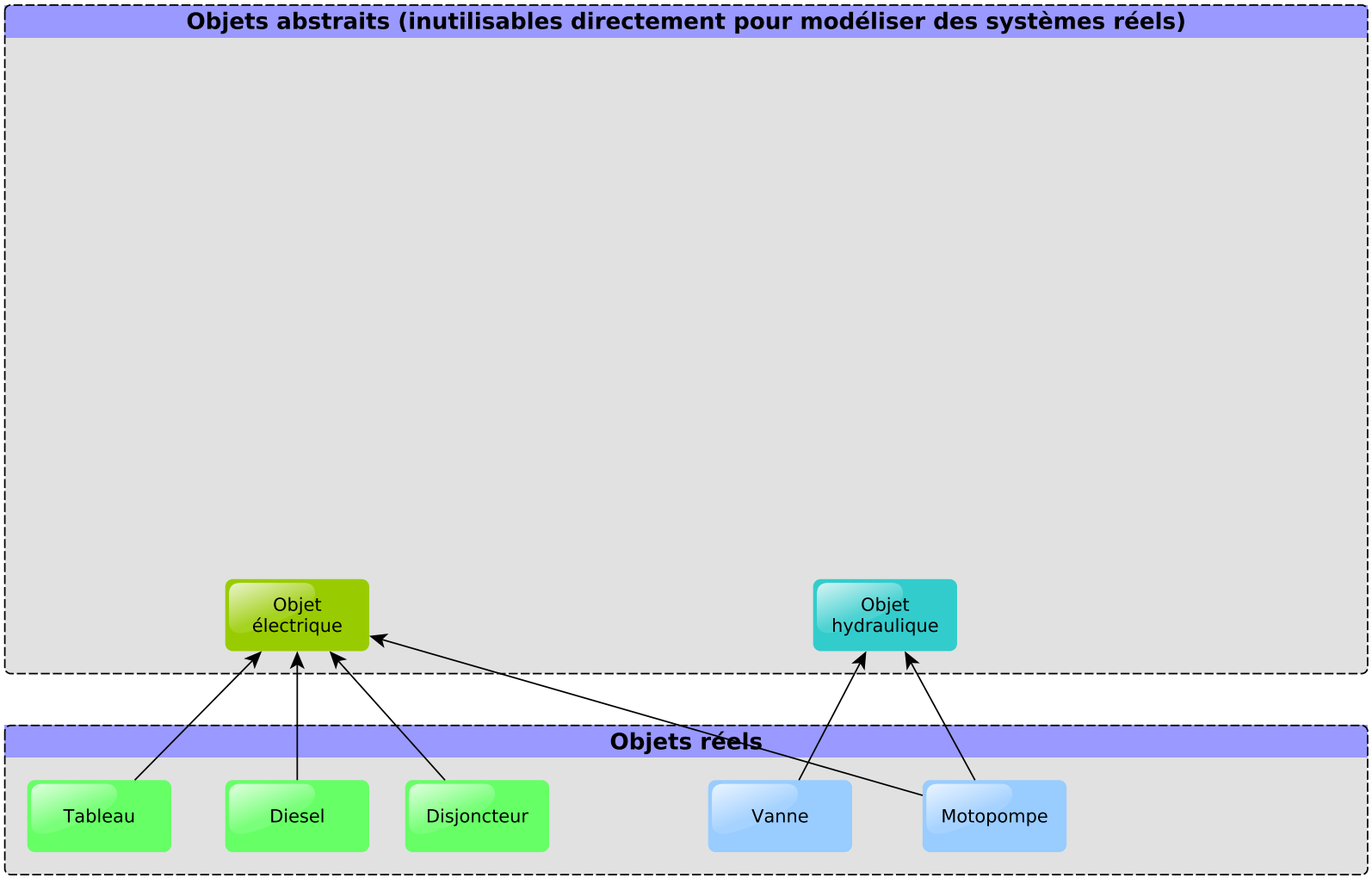
Exemple d'architecture d'une BdC

Éléments d'architecture



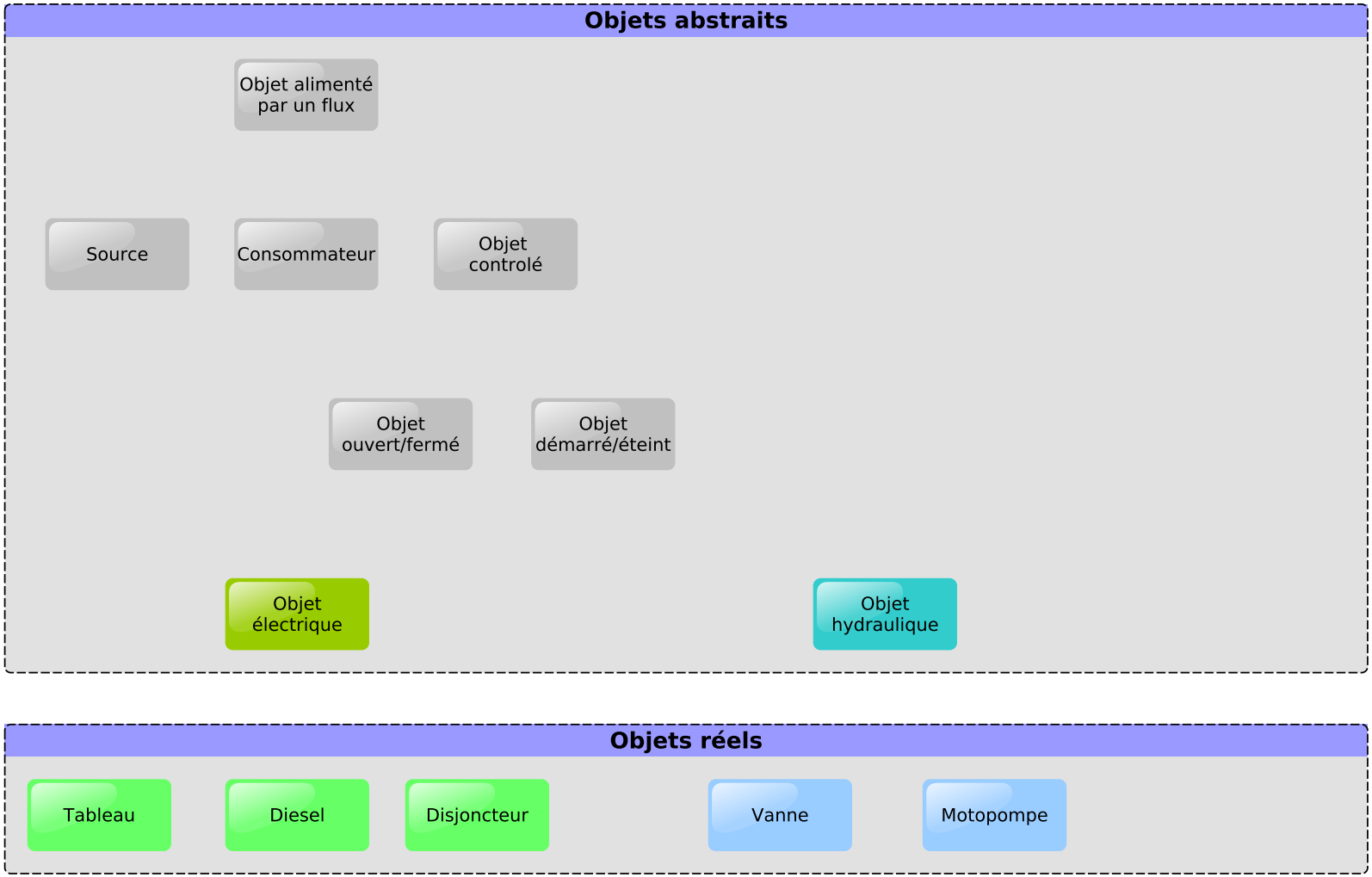
Exemple d'architecture d'une BdC

Éléments d'architecture



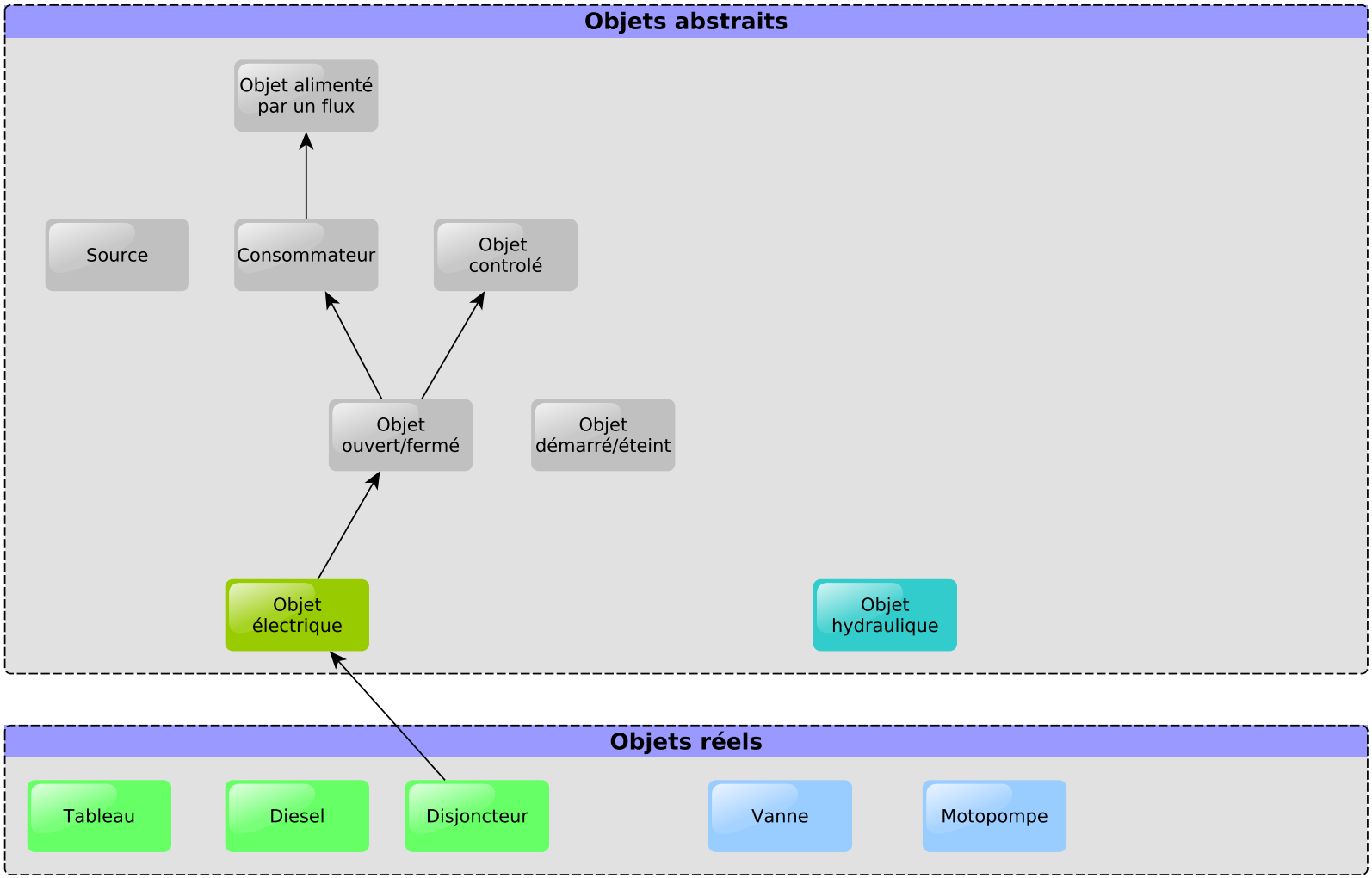
Exemple d'architecture d'une BdC

Éléments d'architecture



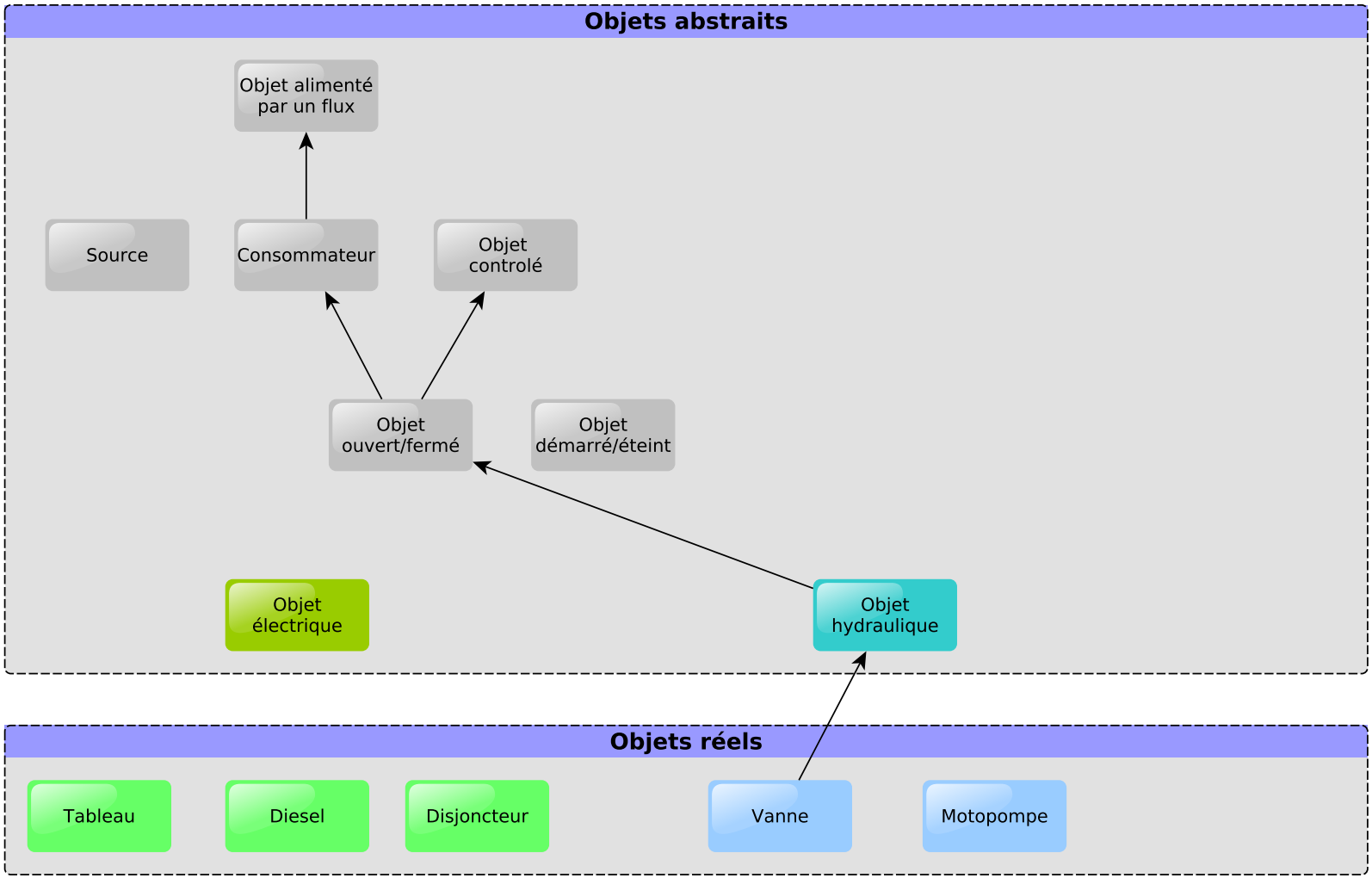
Exemple d'architecture d'une BdC

Éléments d'architecture



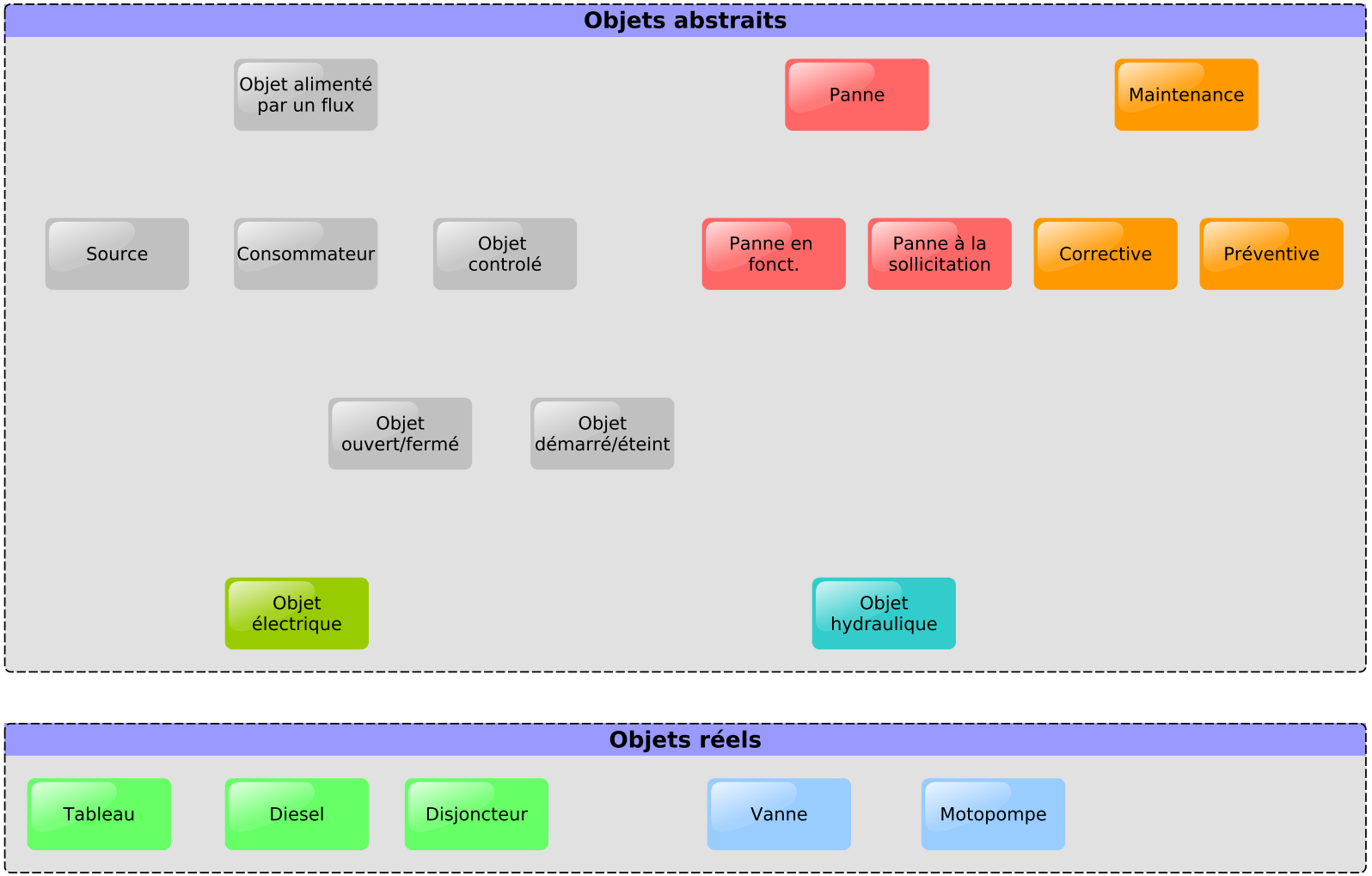
Exemple d'architecture d'une BdC

Éléments d'architecture



Exemple d'architecture d'une BdC

Éléments d'architecture



Exemple d'architecture d'une BdC

Éléments d'architecture

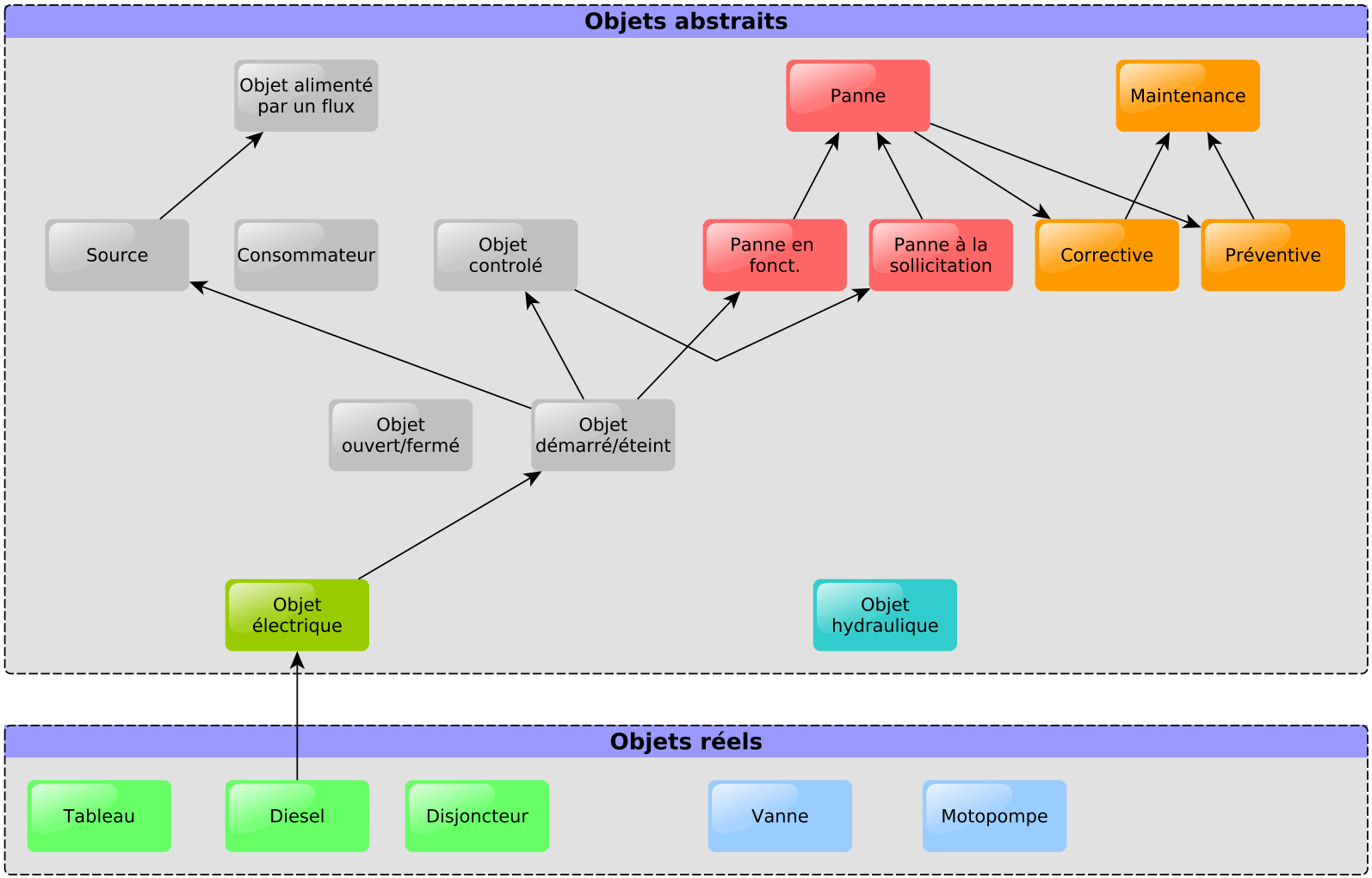


Illustration : système électrique

Schéma du système

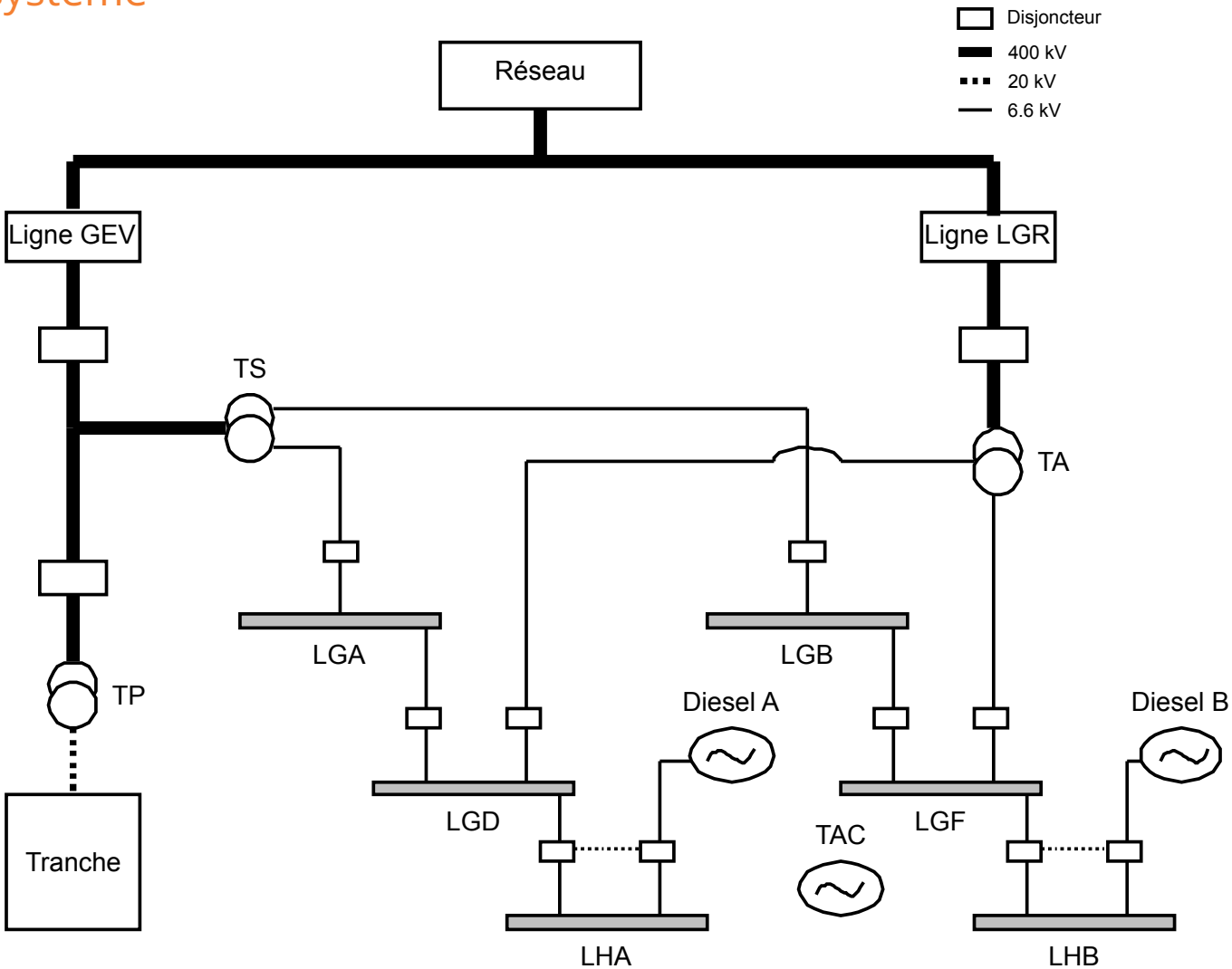


Illustration : système électrique

Approche statique/bas niveau

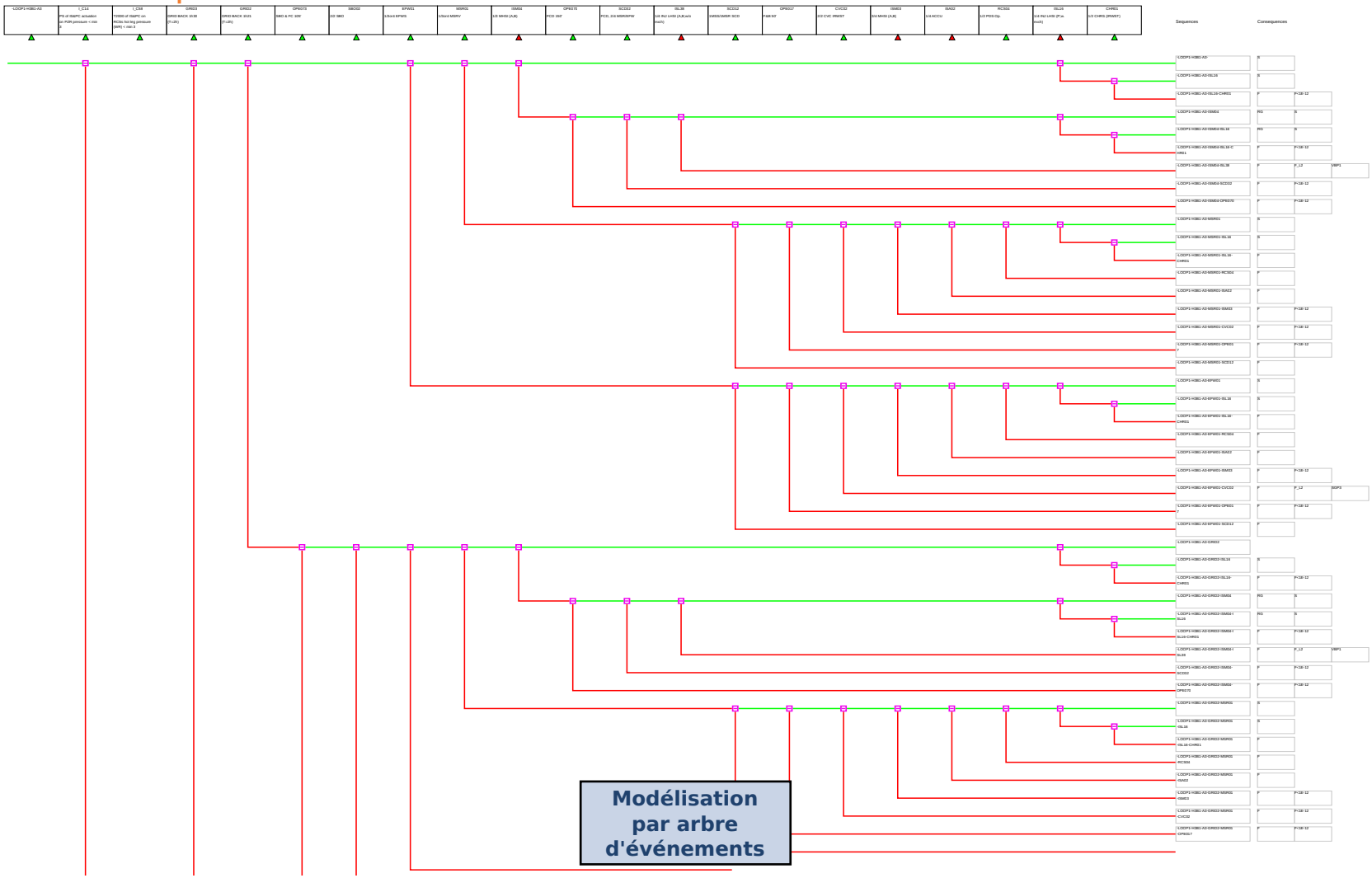


Illustration : système électrique

Approche statique/bas niveau

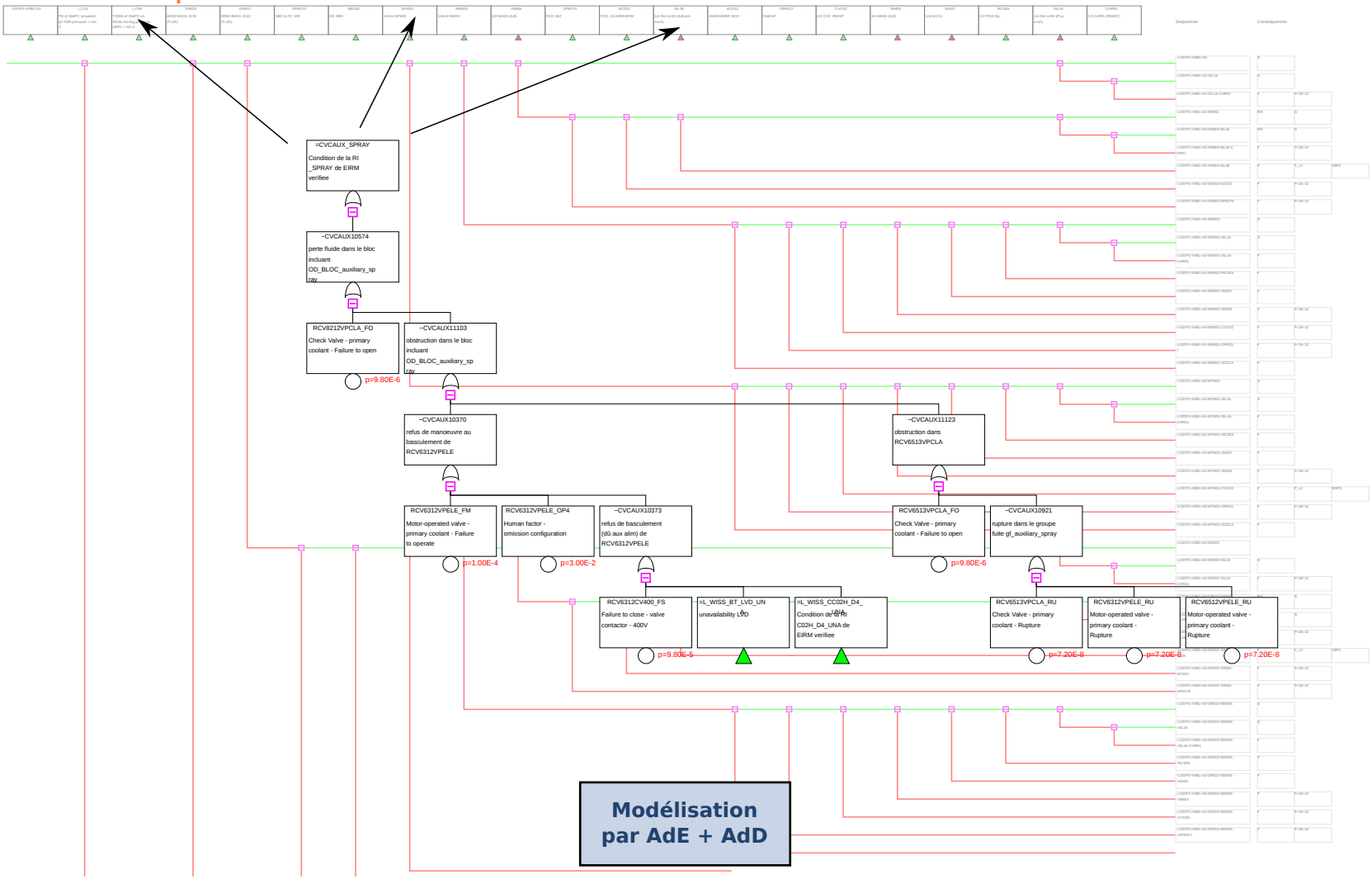
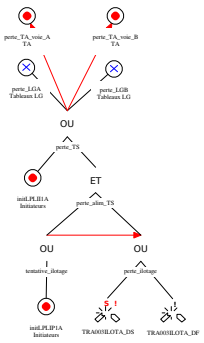
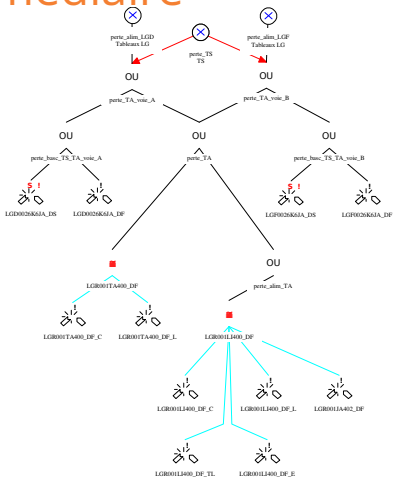
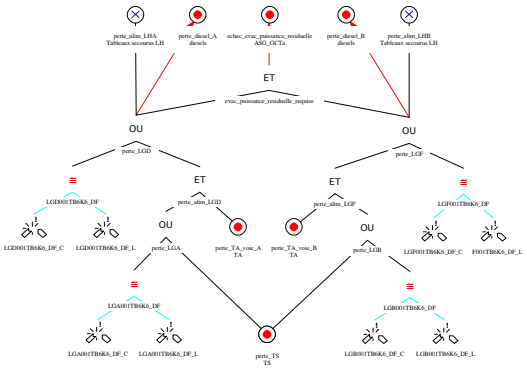


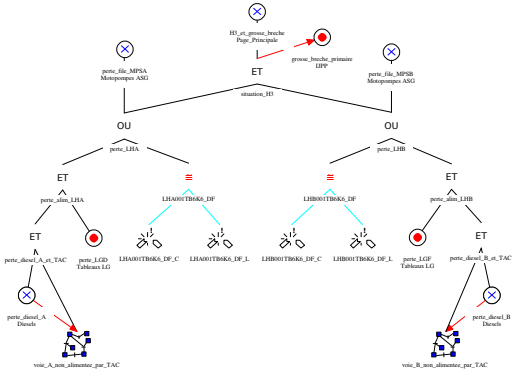
Illustration : système électrique

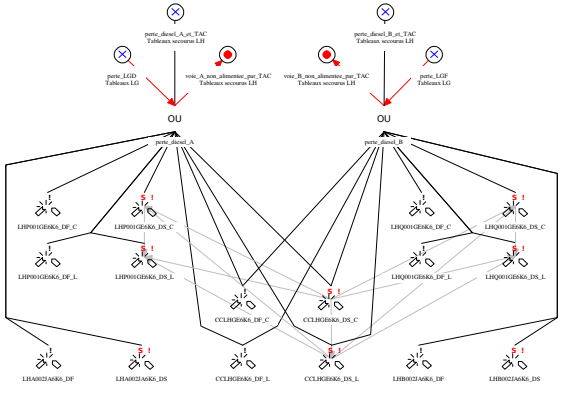
Approche dynamique/niveau intermédiaire

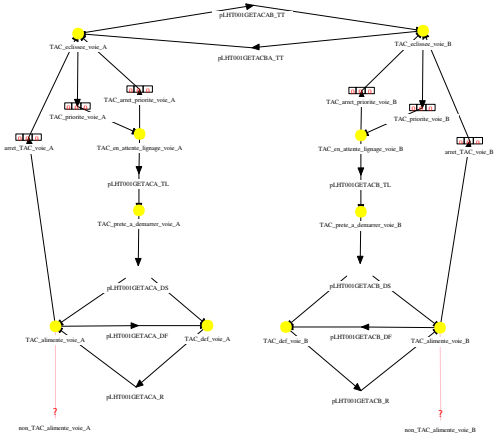








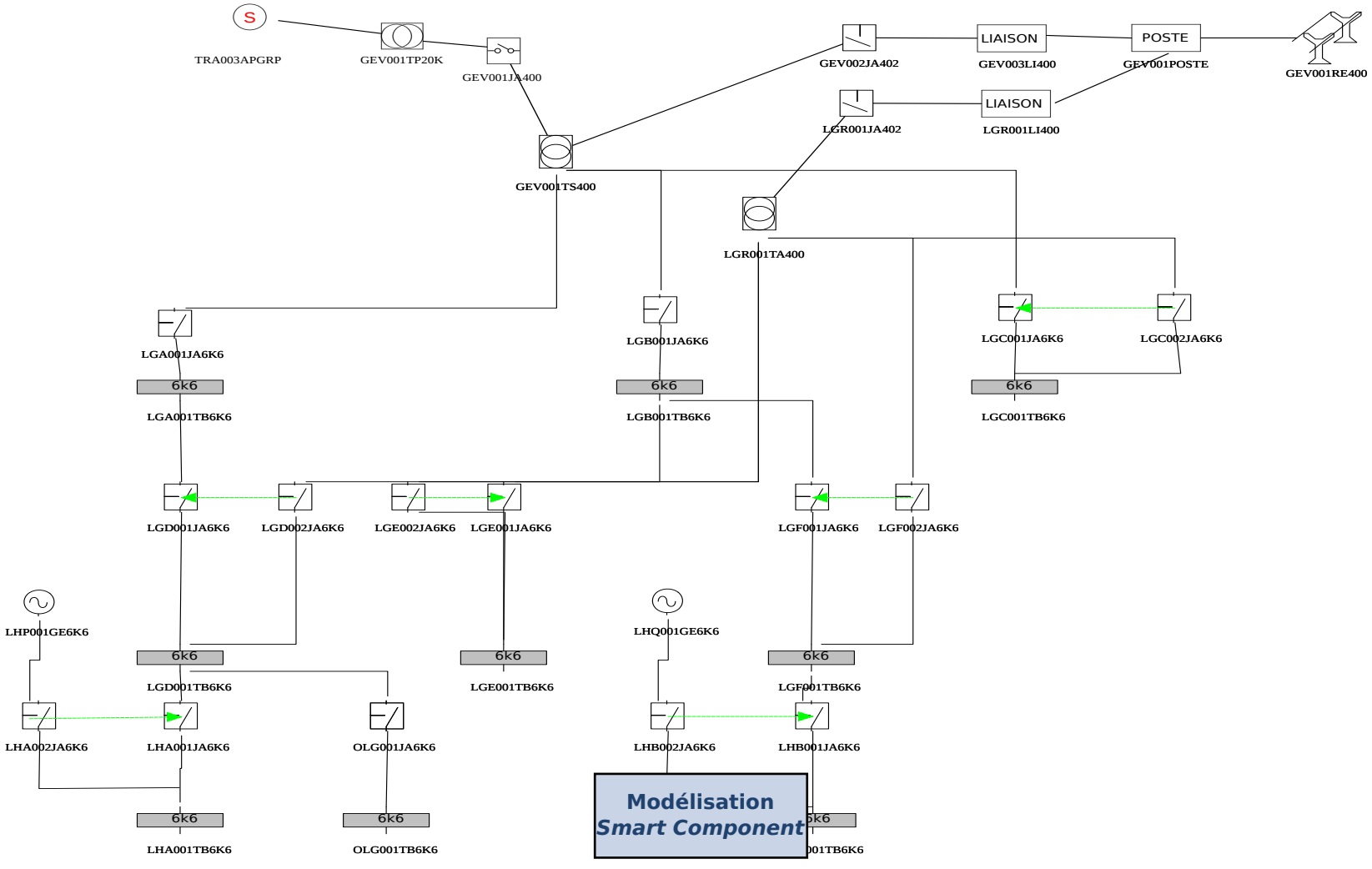




Modélisation BDMP

Illustration : système électrique

Approche dynamique/haut niveau



Illustration

Intérêt de l'approche

Intérêts de l'approche dynamique

- Évite l'utilisation fastidieuse des arbres d'événements
- Modélisation plus naturelle et plus intuitive

Intérêts de l'approche haut niveau

- Modèle proche de l'architecture du système
- Modélisation orientée sur les aspects fonctionnels du système
- Maintenabilité des modèles de systèmes
- Génération automatique des modèles de bas niveau $\Rightarrow$ Utilisation d'outils de quantification efficace
- Traitement de problématiques industrielles complexes

Illustration

Intérêt de l'approche

Intérêts de l'approche dynamique

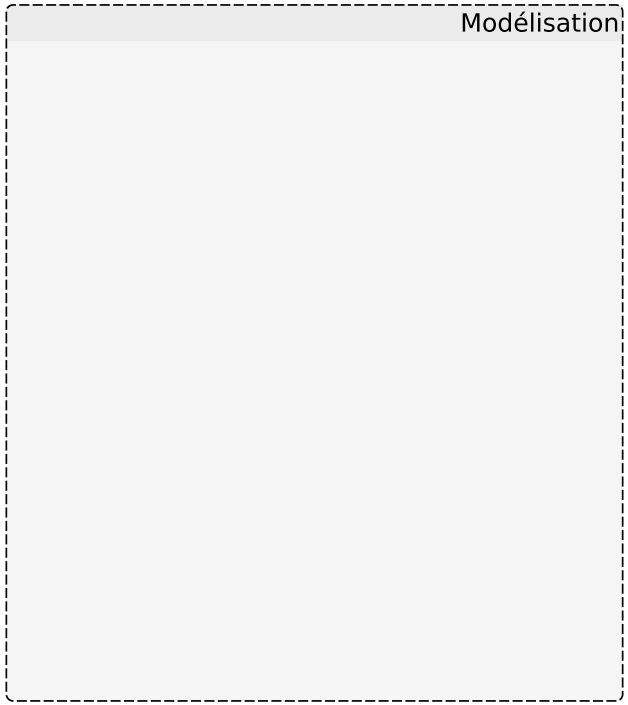
- Évite l'utilisation fastidieuse des arbres d'événements
- Modélisation plus naturelle et plus intuitive

Intérêts de l'approche haut niveau

- Modèle proche de l'architecture du système
- Modélisation orientée sur les aspects fonctionnels du système
- Maintenabilité des modèles de systèmes
- Génération automatique des modèles de bas niveau $\Rightarrow$ Utilisation d'outils de quantification efficace
- Traitement de problématiques industrielles complexes

Plate-forme outils Figaro (Bouissou 2005)

Déroulement de la démarche d'analyse de risques



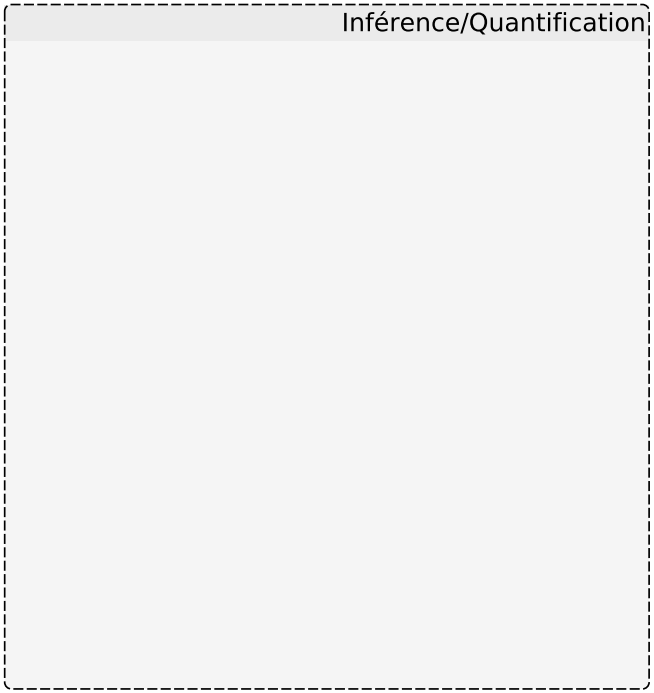
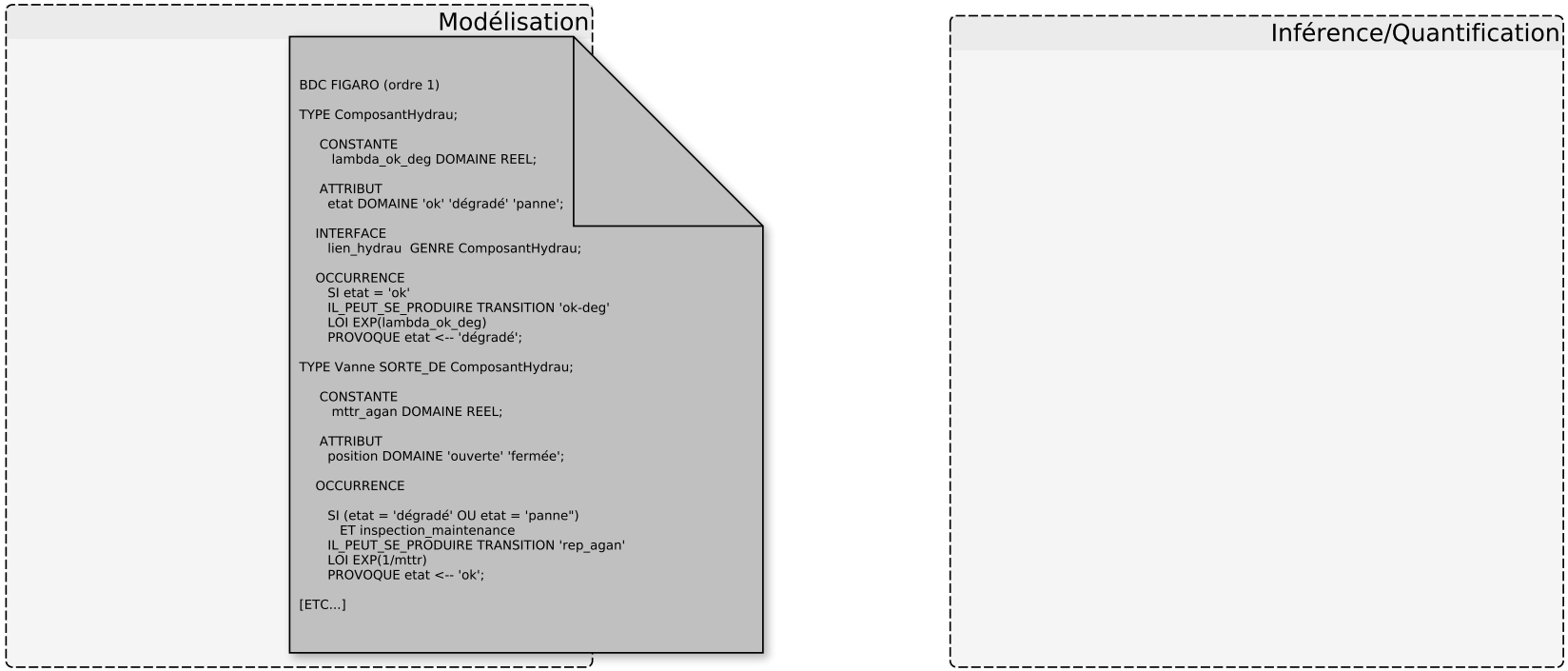


Plate-forme outils Figaro (Bouissou 2005)

Déroulement de la démarche d'analyse de risques

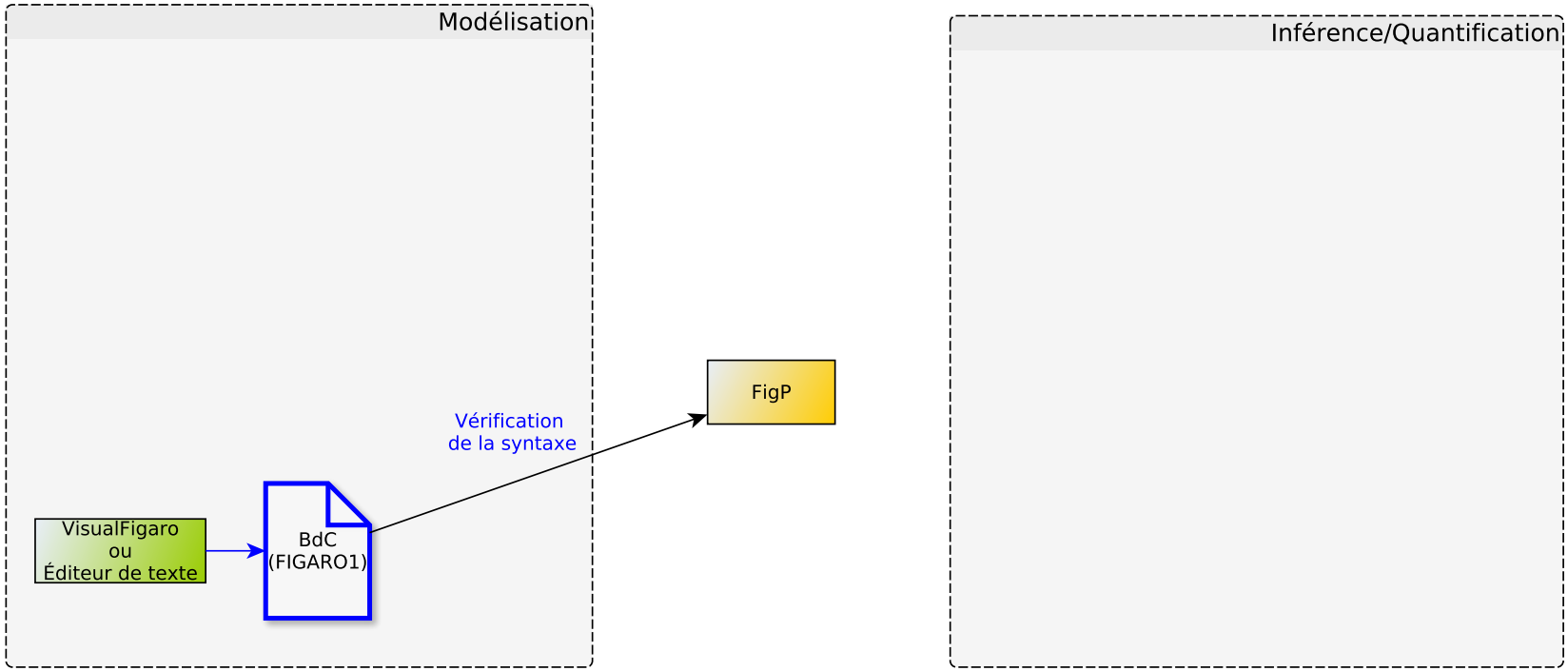


- Si la problématique n'est pas couverte par une base de connaissances existante

⇒ Développement d'une base de connaissances (i.e. du formalisme de modélisation)

Plate-forme outils Figaro (Bouissou 2005)

Déroulement de la démarche d'analyse de risques

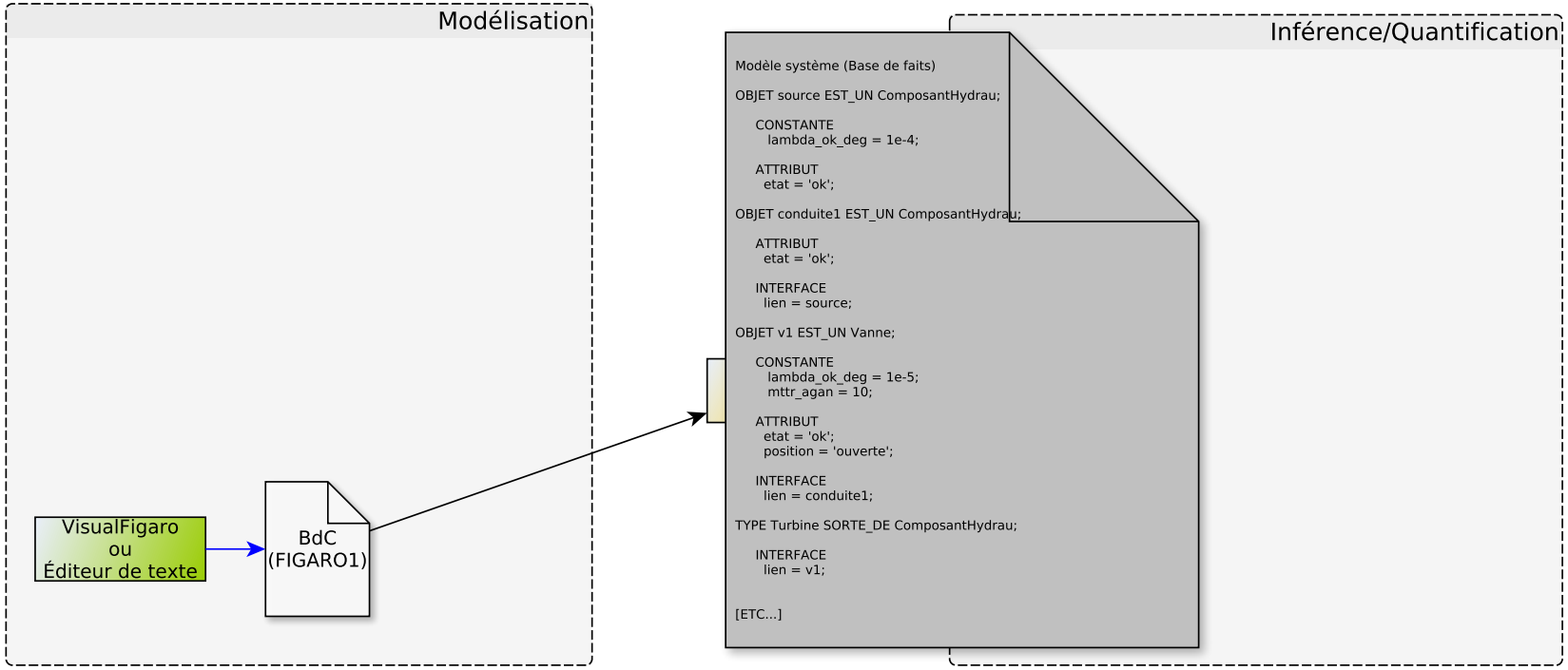


- Si la problématique n'est pas couverte par une base de connaissances existante

⇒ Développement d'une base de connaissances (i.e. du formalisme de modélisation)

Plate-forme outils Figaro (Bouissou 2005)

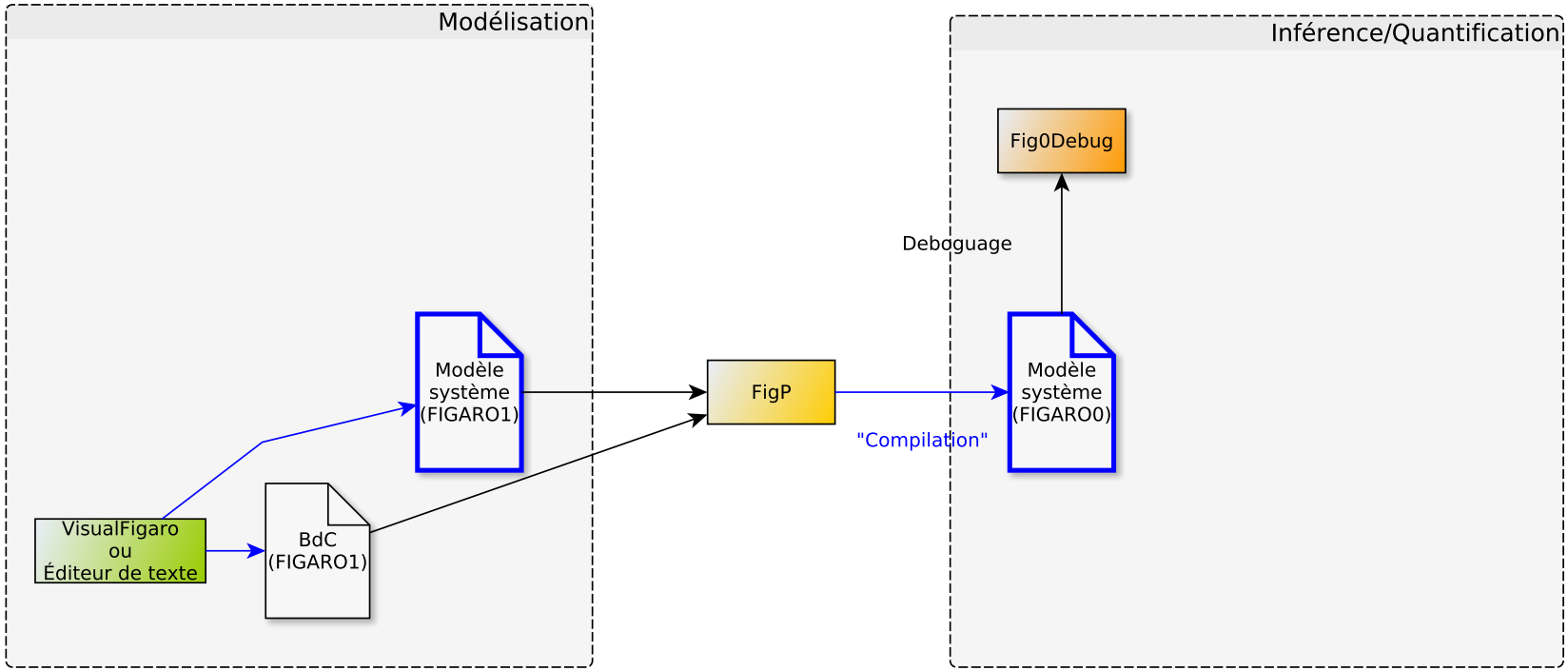
Déroulement de la démarche d'analyse de risques



- Modélisation du système à analyser (i.e. instanciation)

Plate-forme outils Figaro (Bouissou 2005)

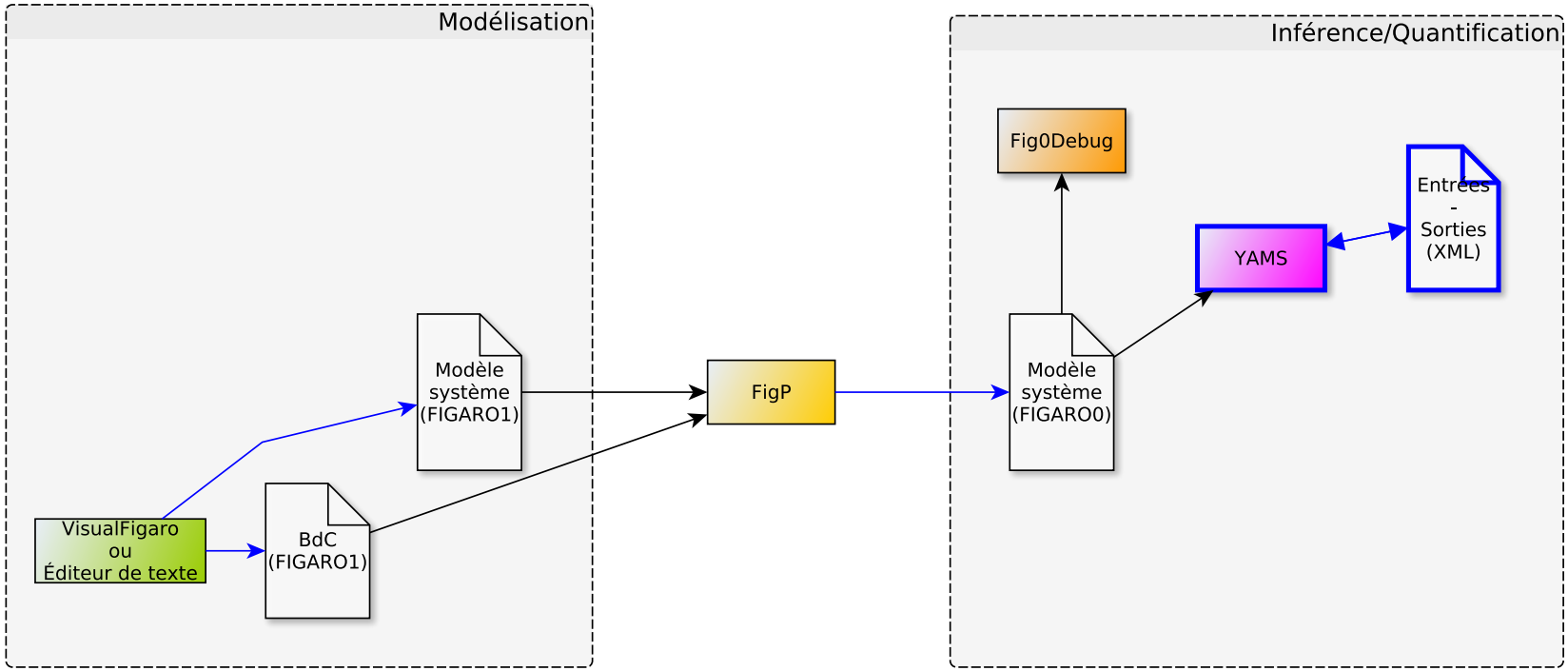
Déroulement de la démarche d'analyse de risques



- Modélisation du système à analyser (i.e. instanciation)
- Compilation du modèle système pour son exploitation

Plate-forme outils Figaro (Bouissou 2005)

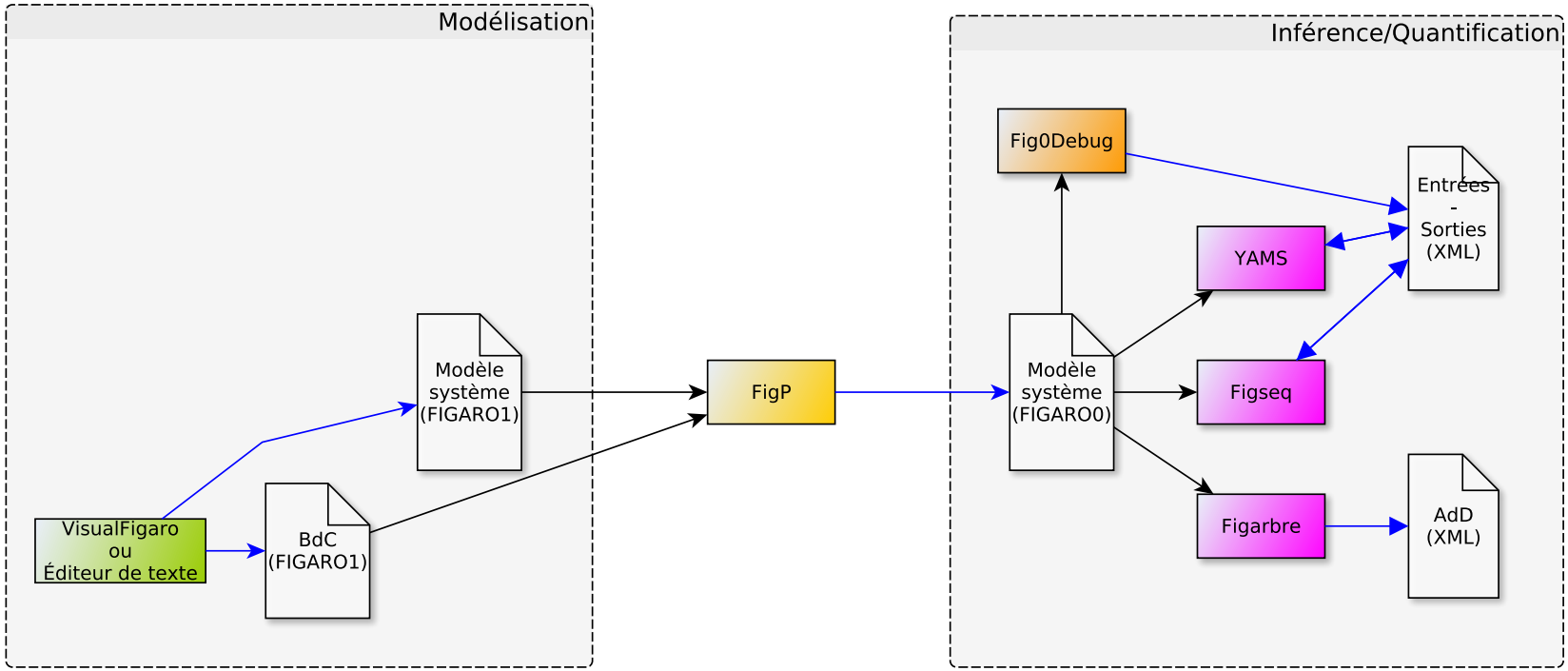
Déroulement de la démarche d'analyse de risques



- Exploitation du modèle
  - Simulation stochastique (Monte-Carlo)

Plate-forme outils Figaro (Bouissou 2005)

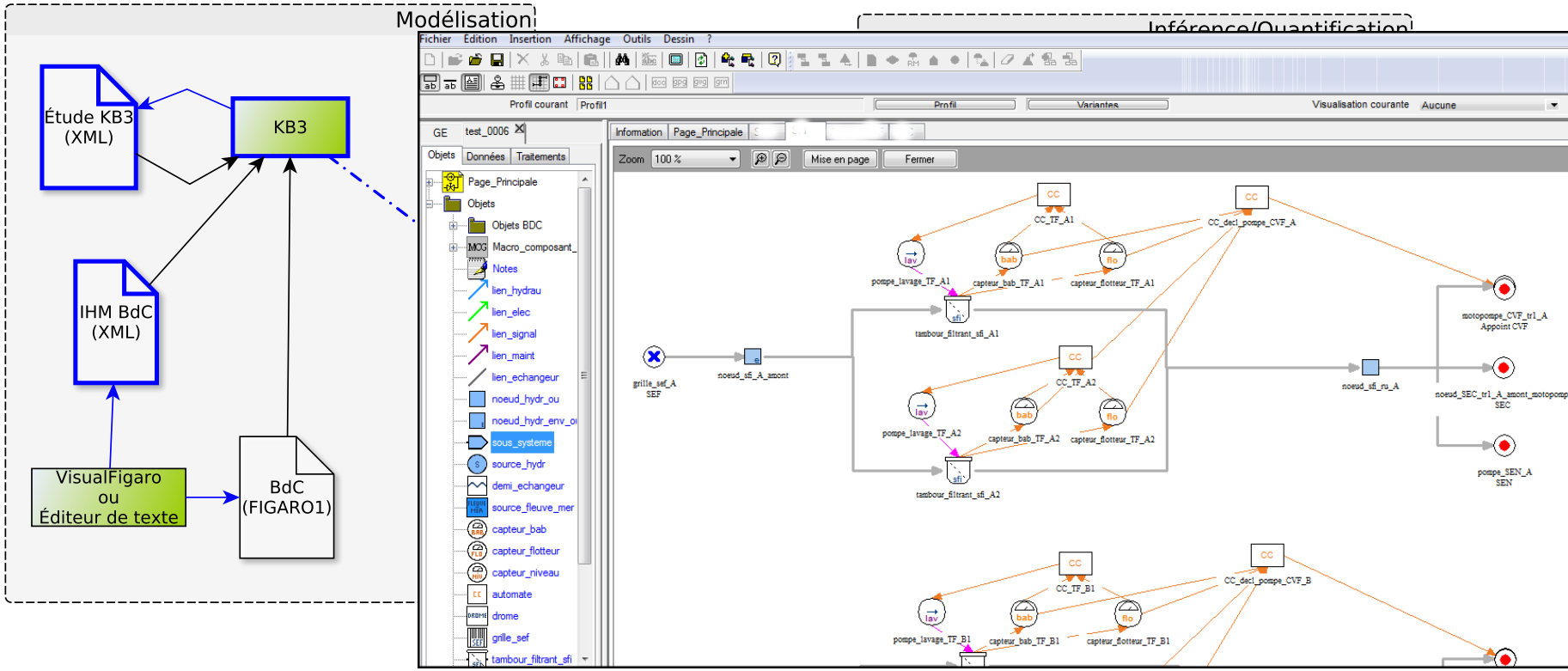
Déroulement de la démarche d'analyse de risques



- Exploitation du modèle
  - Simulation stochastique (Monte-Carlo)
  - Exploration de séquences (systèmes markoviens)
  - Génération d'arbres de défaillances (systèmes statiques)

Plate-forme outils Figaro (Bouissou 2005)

Déroulement de la démarche d'analyse de risques

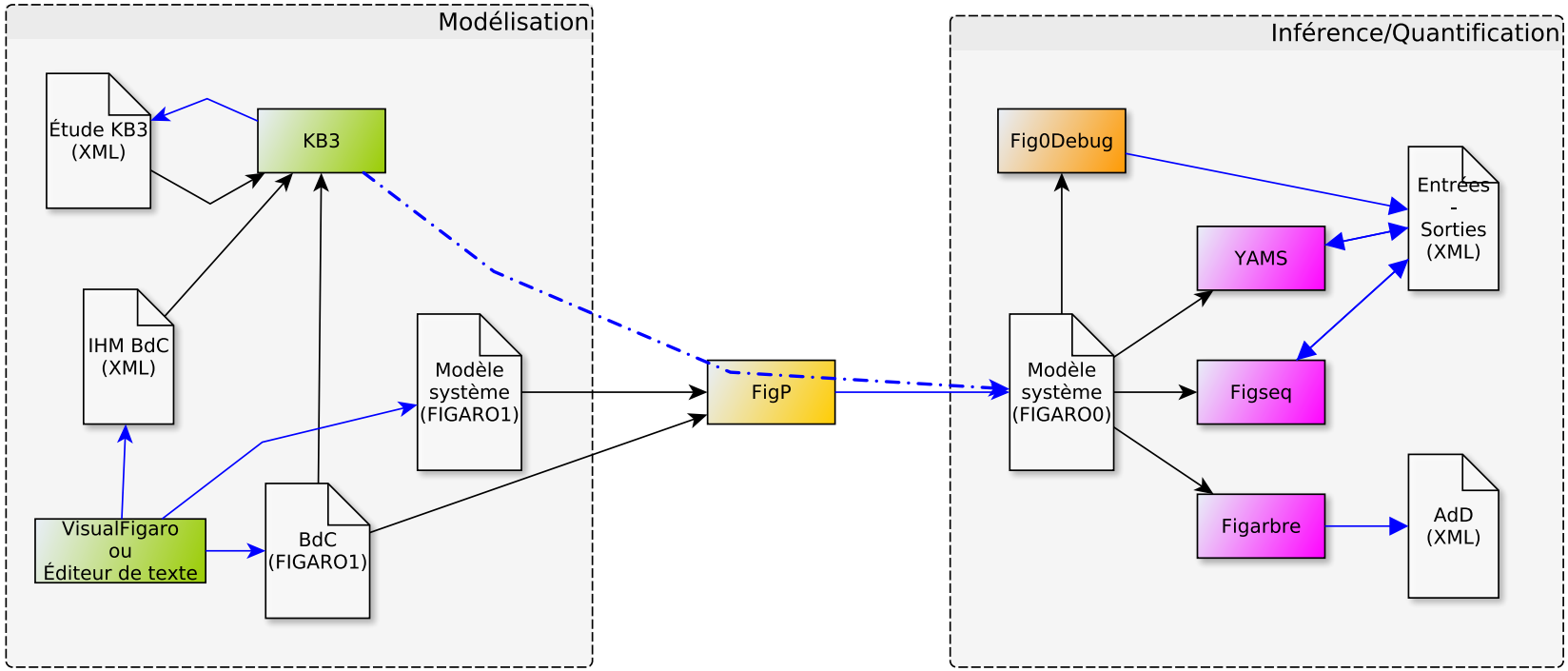


- Développement d'une IHM KB3 associée à la BdC (faculatif)

⇒ Création d'un outil de modélisation graphique adapté aux systèmes cibles

Plate-forme outils Figaro (Bouissou 2005)

Déroulement de la démarche d'analyse de risques



Plan

Conclusion

Approche haut niveau

- Structuration et formalisation de la connaissance métier
- Approche adaptée à chaque domaine spécifique
- Facilite la réutilisation des développements réalisés

Plate-forme outils Figaro

- Construction d'outils de modélisation dédiés à différentes classes de systèmes et de problématiques
- Traitements des modèles à partir d'algorithmes efficaces
- Plate-forme Figaro maintenue et validée en continu par EDF
- Partiellement disponible sur `http://sourceforge.net/projects/visualfigaro`

Plan

Pour en savoir plus...

Quelques références

Bouissou, Marc (2005). "Automated dependability analysis of complex systems with the KB3 workbench : the experience of EDF R&D". Dans : *Proceedings of the International Conference on Energy and Environment (CIEM)*.

Bouissou, Marc et Christel Seguin (2006). "Comparaison des langages de modélisation AltaRica et FIGARO". Dans : *Actes du 14ème congres de fiabilité et maintenabilité de l'IMdR ($\lambda\mu$14)*.

Bouissou, Marc et al. (1991). "Knowledge modelling and reliability processing : Presentation of the FIGARO language and associated tools". Dans : *IFAC/IFIP/EWICS/SRE Symposium*, p. 69–75.

Point, Gérald (2000). "AltaRica : Contribution à l'unification des méthodes formelles et de la sûreté de fonctionnement". Thèse de doct. Université Sciences et Technologies-Bordeaux I.

Prosvirnova, T. et al. (2013). "The AltaRica 3.0 project for Model-Based Safety Assessment". Dans : *Proceedings of 4th IFAC Workshop on Dependable Control of Discrete Systems, DCDS 2013*. York (Great Britain) : IFAC.

Questions ?

Merci de votre attention !
Questions ?