Méthode et outil pour les études de sécurité en phase de conception - Application à la navigation aérienne

Méthode et outil pour les études de sécurité en phase de conception

➔ Avant propos

- **Retour d'expérience sur la problématique de conception & de rédaction du dossier de sécurité d'un système dans le domaine ATM**
- **Résultats d'une étude réalisée en coopération avec SILOGIC afin de fournir une solution Méthode + Outil en support aux projets internes et aux consultants en mission**
- **Les éléments présentés ont été mis en œuvre dans le cadre d'un projet industriel pour le compte de la DGAC**
- **La méthode définie s'inscrit dans le cadre de nouvelles obligations réglementaires applicables à partir de 2005**
- **Les éléments présentés par la suite constituent un squelette de solution compatible avec plusieurs méthodes développées dans le même cadre réglementaire**
  - SAM : Safety Assessment Method de Eurocontrol
  - ED 78 A : EUROCAE
  - …

Méthode et outil pour les études de sécurité en phase de conception

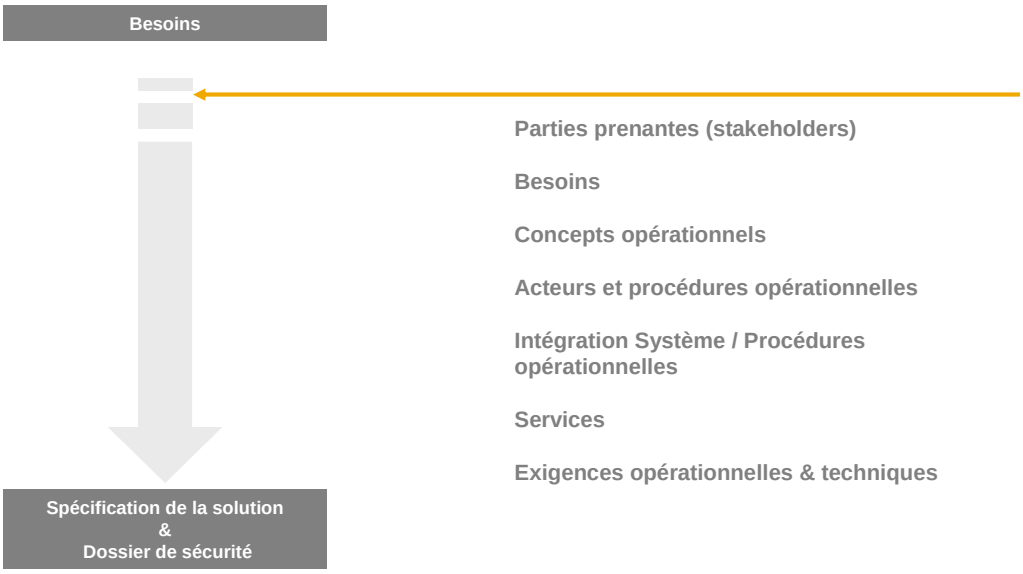
➔ Sommaire

- Périmètre
- Contexte ATM
- Méthode
- Outil
- Conclusion
- Questions

Périmètre
Projet

➔ Étude Amont

- Du besoin à la spécification de la solution intégrée dans son environnement opérationnel
- Productions
  - Dossier de conception
  - Dossier de sécurité



Contexte ATM

➔ Air Traffic Management

- **Domaine complexe**
- **Contraintes de sécurité et de coûts très fortes**
- **Réglementé**

Contexte actuel

- Augmentation du trafic (incidents)
- Évolution des concepts opérationnels
- Évolution de la réglementation

⇨

Caractéristiques des Systèmes ATM

- Équipements techniques
- Procédures
- Personnels

⇨

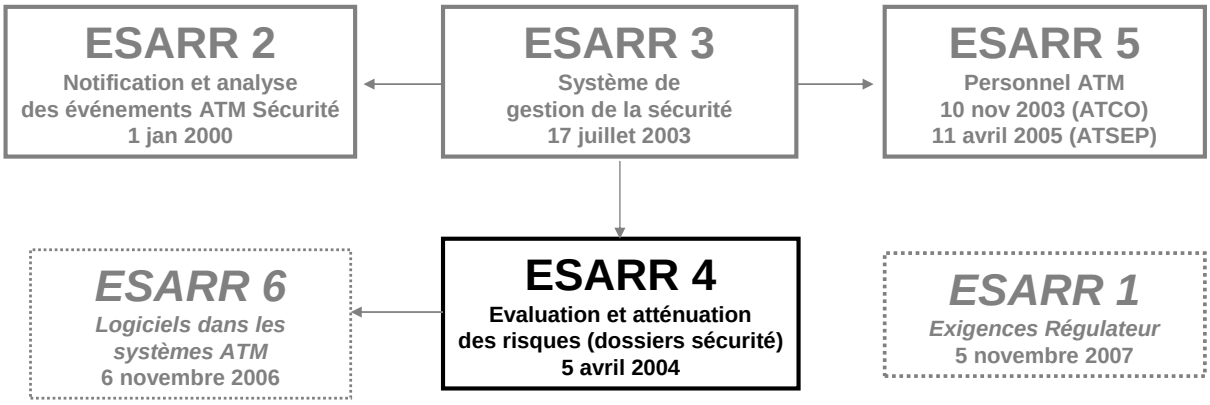
Processus de développement

- Long et coûteux
- Études amont sont primordiales
- Sécurité = Préoccupation de tous les instants à tous les niveaux

Contexte ATM
Réglementation internationale

➔ Eurocontrol Safety Regulatory Requirement (ESARR)

- **A destination de l'ensemble des intervenants du monde ATM**
  - Monde opérationnel
  - Monde technique
- **ESARR 1 ⇨ Autorités de surveillance**
- **ESARR 2 – 6 ⇨ Prestataires de services**
  - textes relatifs à une gestion « a priori » de la sécurité
  - textes relatifs à une gestion « a posteriori » (analyse d'incidents / accidents)



Contexte ATM
Réglementation

➔ ESARR 4 : Dossier de sécurité

- **Objectif**
  - Évaluation et atténuation des risques dans le domaine ATM
- **Champ d'application**
  - Ensemble des prestataires de services ATM
  - Pour tout système ATM (nouveauté & évolution)
    - Pour tout ses éléments (sols et bords)
    - Dans son environnement opérationnel
    - Sur tout son cycle de vie
- **Responsabilité**
  - Le Prestataire doit apporter les **preuves**
    - qu'il a évalué **les risques** liés à la mise en œuvre d'un système ou d'une évolution d'un système
    - qu'il les a rendus **acceptables** par rapport aux niveaux de sécurité approuvés par l'Autorité désignée

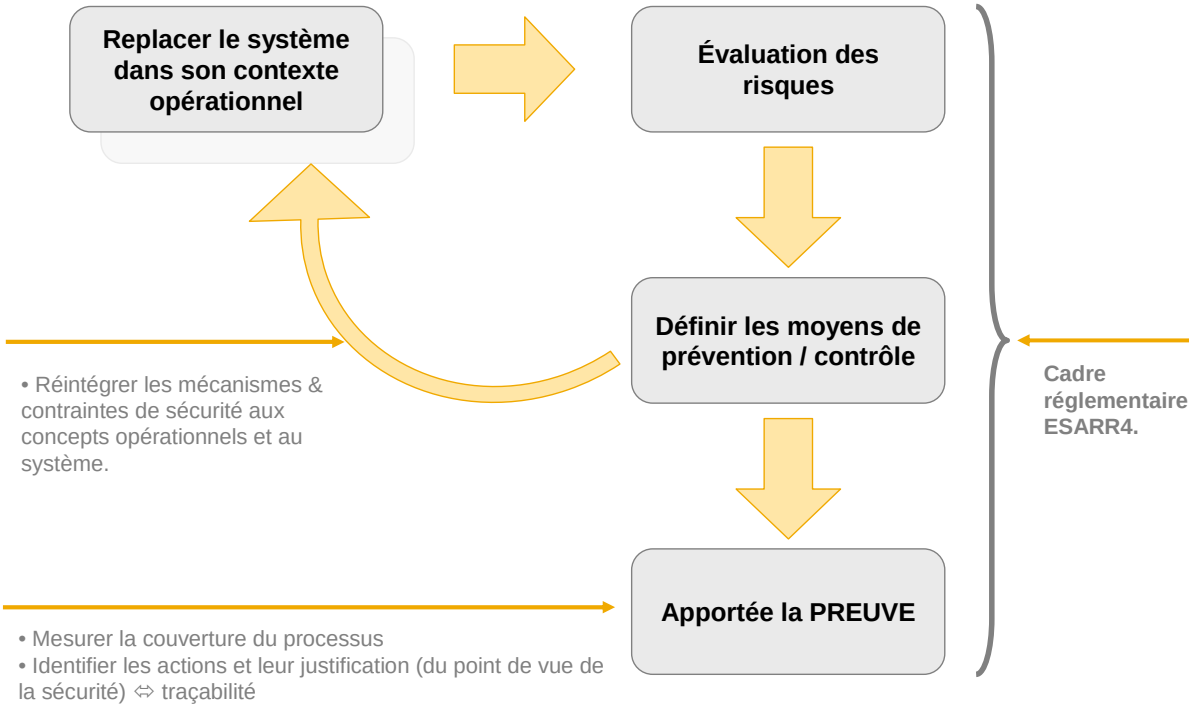
Méthode
Objectifs

➔ Intégrer les approche Conception & Dossier de sécurité

- **Rendre les 2 approches collaboratives**
  - Parce que la conception impacte la sécurité
  - Parce que la prise en compte de la sécurité oriente certains choix de conception
- **Permettre d'adresser les 2 aspects en parallèle et optimiser la collaboration**
  - « Extreme design »
  - Approche itérative
- **Réduire les coûts des études de sécurité**
  - En exploitant au mieux les informations de conception (modèle)
- **Traiter la sécurité tout au long du cycle de conception / développement / validation**
  - Conserver la vue « sécurité » au delà de l'étude initiale
  - Vérifier la bonne prise en compte des objectifs de sécurité
- **Mettre en pratique la méthode sur un projet industriel**

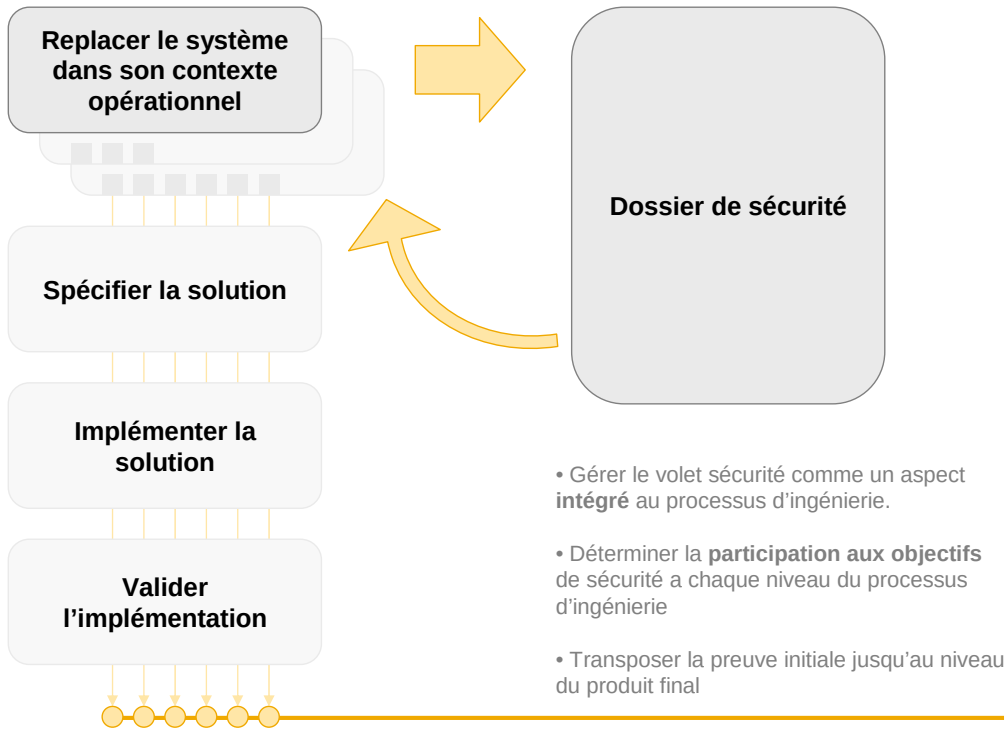
Méthode
Vue globale

➔ **Prise en compte de la sécurité (safety) et Preuve**



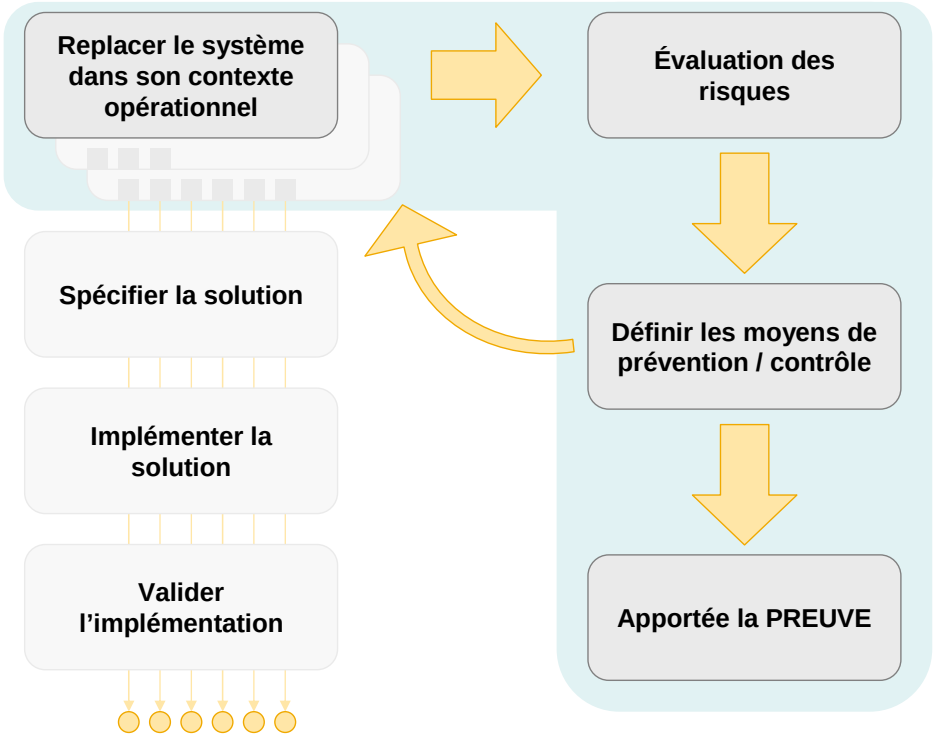
Méthode
Vue globale

➔ **Conserver la preuve au delà de la conception ⇒ faire le pont « Étude de sécurité » ⇔ « Processus d'ingénierie »**



Méthode
Ingénierie Système & Étude de sécurité

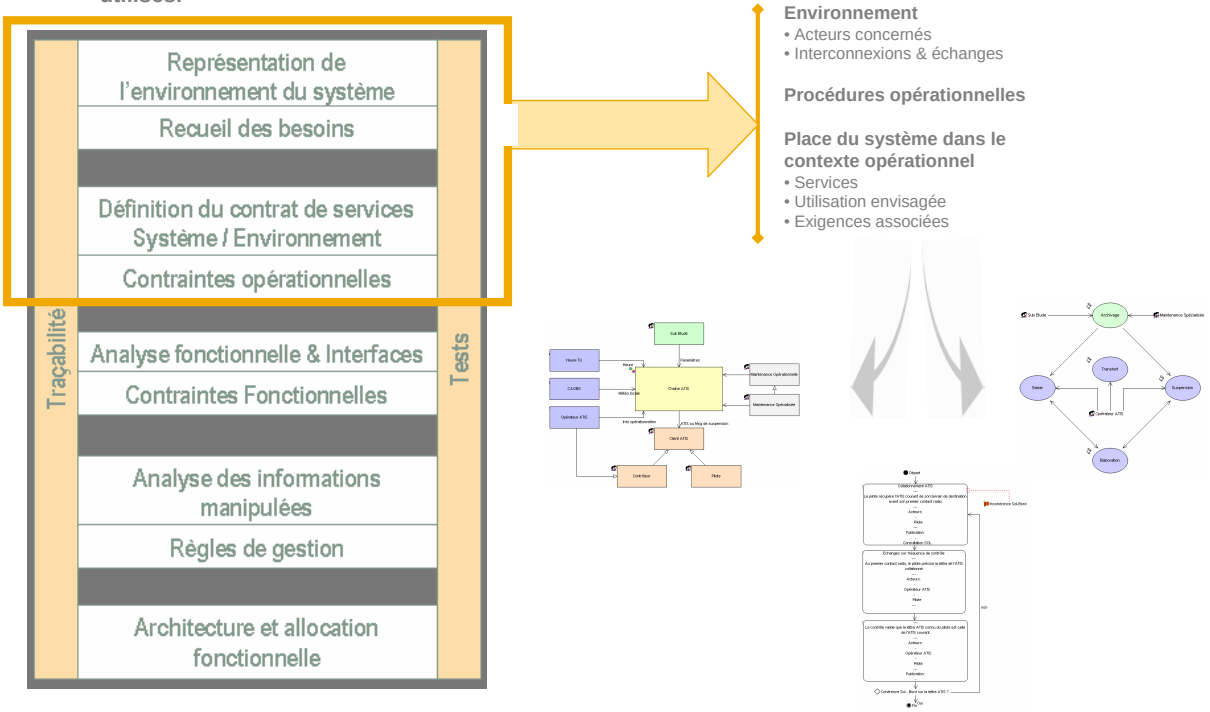
➔ **Périmètres respectifs**



Méthode
Replacer le système dans son contexte opérationnel

➔ **Poser les bases de l'étude de sécurité**

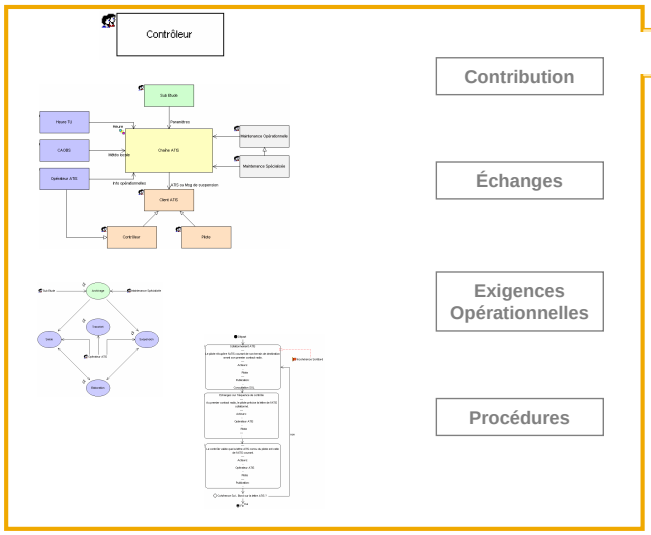
Se faire une idée précise des services fournis par le système et des conditions dans lesquelles ils seront utilisés.



Méthode
Évaluation des risques

➔ Identification : Événements redoutés

- **Danger affectant la fourniture de services ATM et ayant un impact sur la sécurité**
  - Peut être d'origine humaine, procédurale et/ou technique
  - Doit être vu du point de vue utilisateur
  - Doit être relativement précis pour évaluer la gravité des effets/conséquences (étendue, durée, …)
- **Les éléments de conception fournissent le cadre initial**
- **L'utilisation de ce cadre permet de faire le pont entre conception & étude de sécurité**



Identification & Allocation d'événements redoutés

- Description
- Fréquence d'occurrence
- Conséquences
- Gravité

Méthode
Évaluation des risques

➔ Analyse : Identification des effets

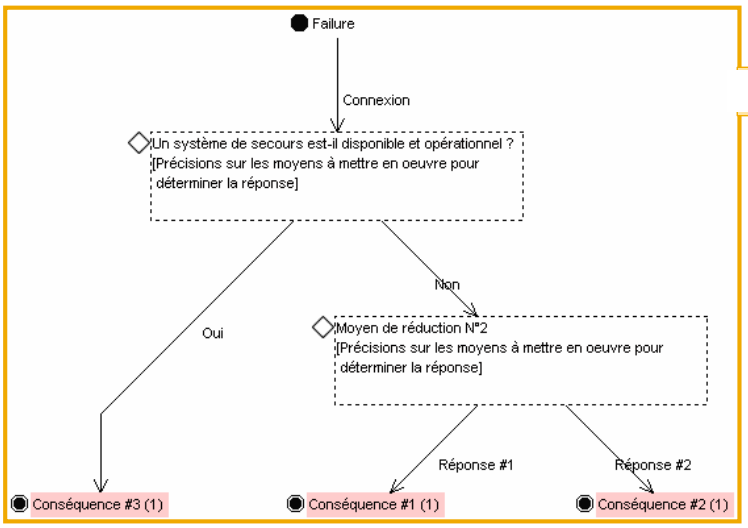
Utilisation du modèle de conception en support

- **Évaluation des effets / conséquences des événements redoutés**
  - ⇨ **Analyse en profondeur d'un ER dans son contexte**
    - Chaque événement fait l'objet d'une analyse conduisant à l'identification / qualification des

Maîtrise de la situation

      - Moyens de réduction du risque
      - Conséquences / Effets
    - Chaque services / systèmes / procédures … impliqué dans un moyen de réduction du risque est explicitement identifié

Conséquences opérationnelles



Approche quantitative

L'arbre d'analyse permet de déterminer le niveau de gravité de l'ER en fonction:

- De la gravité des effets
- Du nombre de moyens de réduction
- De la nature des moyens de réductions (procédure humaine, support système, …)

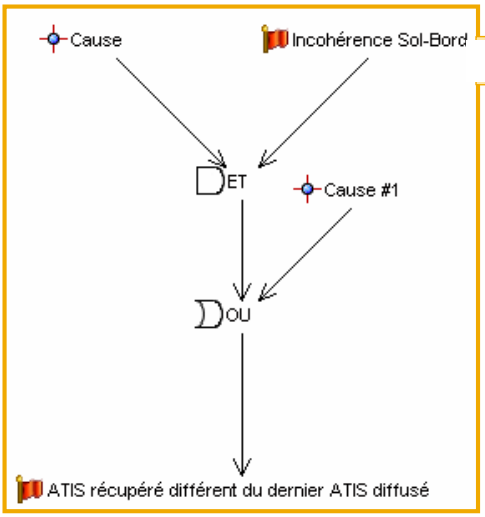
Méthode
Évaluation des risques

➔ Analyse : Identification des causes et des connexions logiques

- **Évaluation des causes des événements redoutés**
  - ⇨ **Analyse transversale des relations logiques entre ERs**
    - Identification des causes
    - Identification des dépendances entre événements redoutés

Utilisation du modèle de conception en support

- **Les éléments de conception justifiant les causes & relations logiques doivent être explicités**
  - Analyse d'impact « conception / sécurité » automatisée



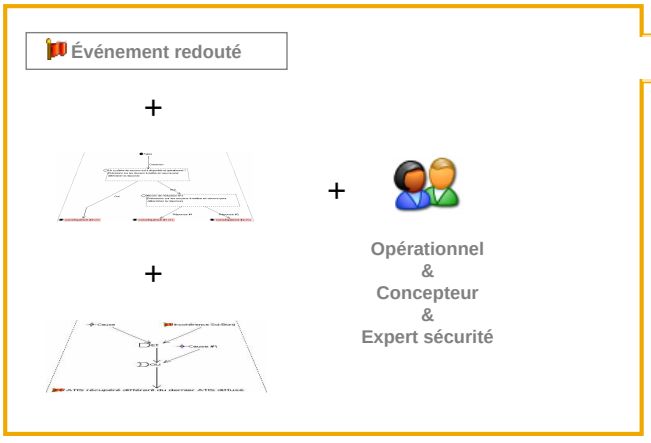
Approche quantitative

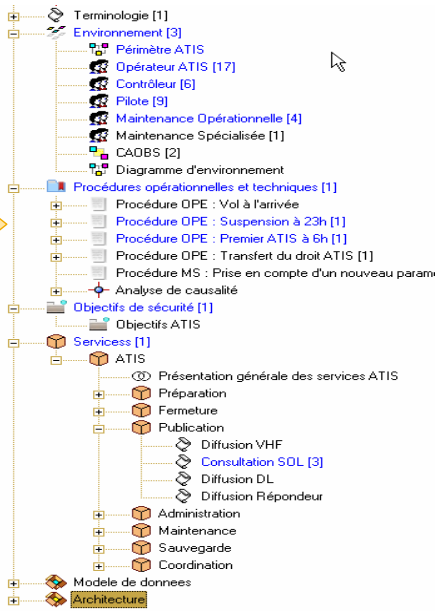
Utilisé comme complément de l'arbre d'analyse pour déterminer la gravité des événements redoutés.

Méthode
Prévention et contrôle

➔ Contrôler les risques et les rendre acceptables

- **Définition d'objectifs de sécurité & déclinaison de ces objectifs en fonction du système**
  - ⇨ **Analyse globale et définition d'exigences opérationnelles / techniques de sécurité**
    - Définition des objectifs de sécurité
      - Justification ⇔ Traçabilité OS / ER
      - Périmètre ⇔ Liens ER analyse / Conception
    - Ré intégration des moyens de contrôle au modèle de conception
      - Exigence opérationnelle de sécurité
      - Procédure opérationnelle complémentaire
      - Services de prévention et d'urgence additionnels
      - Exigence techniques de sécurité (sur des services)

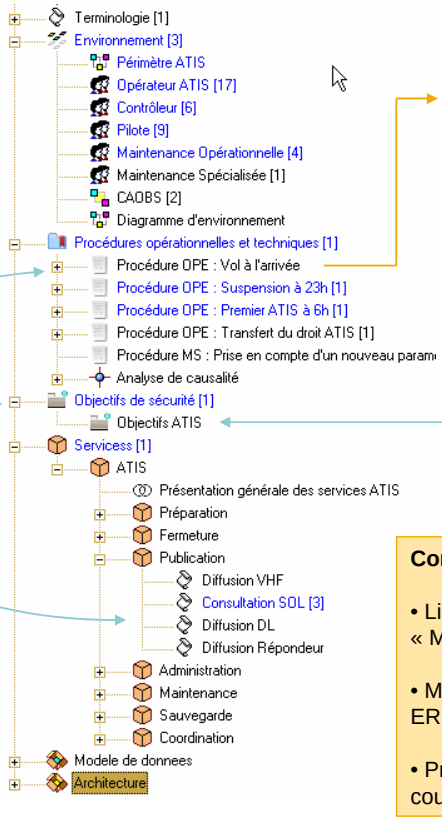


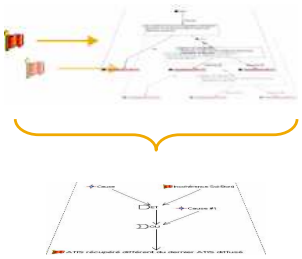


Méthode
Preuve

➔ Par l'intégration Conception / Sécurité & la Traçabilité (outil)

- Exigences opérationnelles de sécurité
- Procédures de prévention & d'urgence





Évaluation

Contrôle

- Exigences techniques de sécurité
- Services de surveillance et d'urgence

Construction de la preuve

- Lien permanent « Etude de sécurité » / « Modèle de conception »
- Mémoire du processus (traçabilité)
  ER ⇨ OS ⇨ Exigences additionnelles
- Production automatisée de matrice de couverture & traçabilité.

Outil

➔ Caractéristique globale du processus mis en oeuvre

- **Intégré**
  - Ingénierie & Étude de sécurité
- **Itératif**
- **Traçable**
  - Impose la traçabilité comme base de la preuve
- **Mesurable**
  - Associé à des métriques
    - matérialisation de la preuve

Mise en oeuvre

Support d'un outil

- Pour l'intégration ⇨ doit implémenter
  - Le **processus de conception**
  - Le **processus des études de sécurité**
- Afin de
  - Fournir à chaque domaine la **représentation la plus adaptée**
  - **Réutiliser** les travaux réaliser par ailleurs
  - Gérer la **traçabilité intra et inter domaine**
  - **Structurer l'information** pour pouvoir produire des métriques
  - **Générer les documents** de conception et le dossier de sécurité

Outil
S-Miner

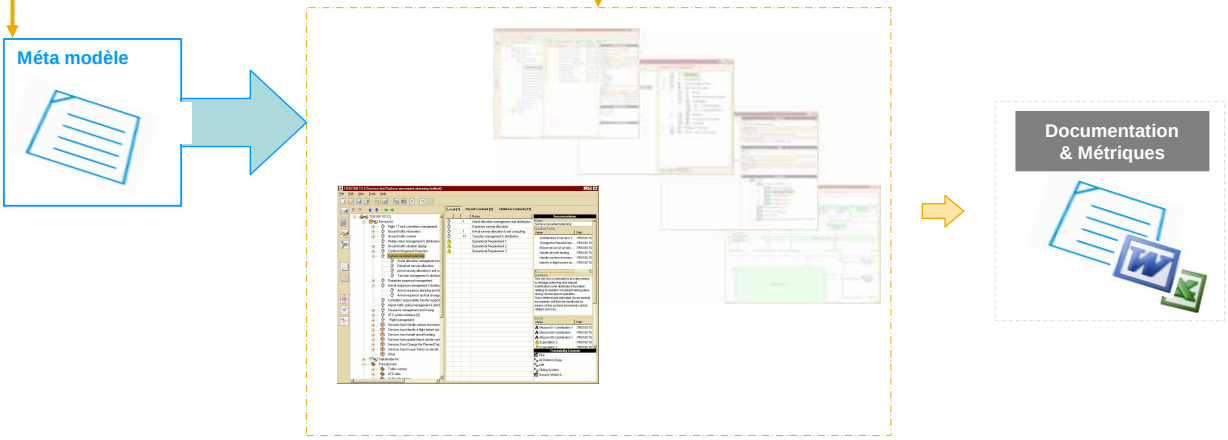
➔ Présentation globale

Méta modèle ⇨ document XML décrivant

- les concepts utilisés dans le cadre de la méthode.
- les relations logiques entre ces concepts
- les représentations utilisées
- les règles de modélisation et leur documentation

S – Miner ⇨ Environnement intégré d'ingénierie

- permettant la réalisation de modèles conformes à une méthode décrite dans un méta modèle.
- prenant en charge la gestion de la traçabilité (en fonction de la méthode)
- permettant de générer des documents & métriques dont le contenu peut être adapté à la cible.

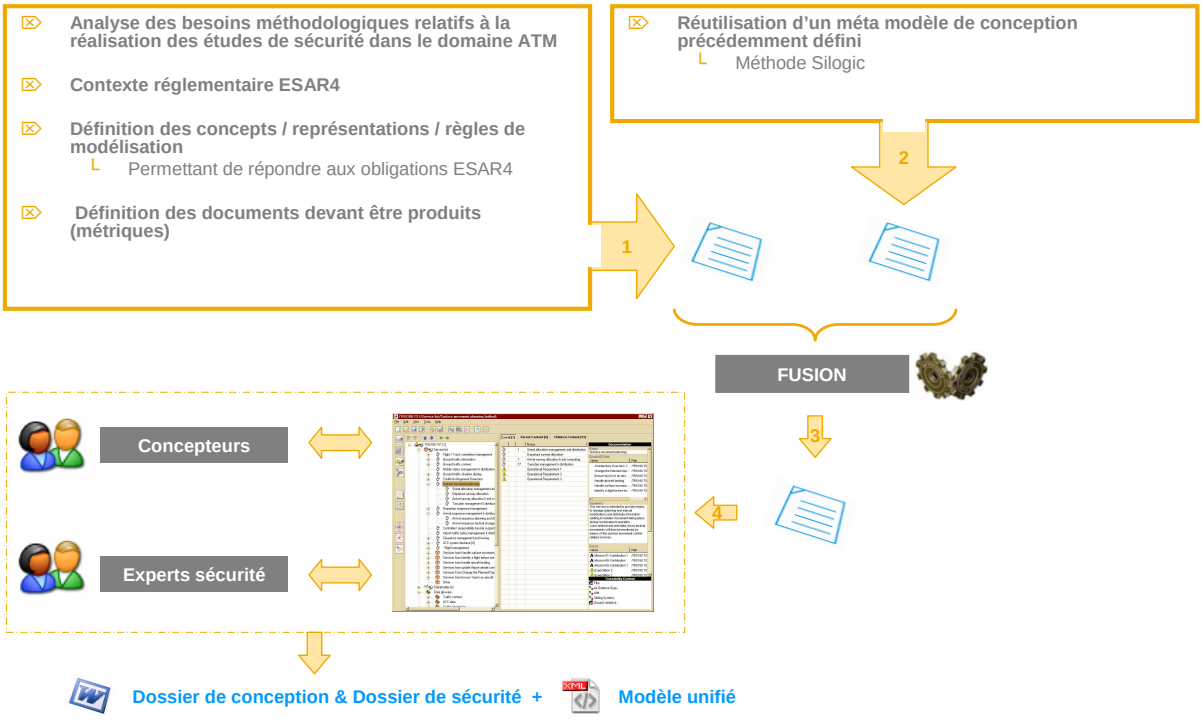


Outil
S-Miner

➔ Intégration Conception & Étude de sécurité

- **Analyse des besoins méthodologiques relatifs à la réalisation des études de sécurité dans le domaine ATM**
- **Contexte réglementaire ESAR4**
- **Définition des concepts / représentations / règles de modélisation**
  - Permettant de répondre aux obligations ESAR4
- **Définition des documents devant être produits (métriques)**

- **Réutilisation d'un méta modèle de conception précédemment défini**
  - Méthode Silogic



Conclusion

➔ Résultats

- **Définition d'un processus Ingénierie + Étude de sécurité**
  - Respectant la culture interne ⇨ prise en compte de la méthode de conception interne
  - Répondant aux exigences réglementaires ⇨ intégration du volet sécurité sur la base ESARR4
- **Réelle mise en place de la méthode par la fourniture d'un ensemble Méthode + Outil**
- **… sans surcoût par la prise en charge automatique de la traçabilité et de l'intégrité ⇨ Outil ⇨ S – Miner**
- **Rapprochement des experts Conception & Sécurité**

Questions ?

S Miner © 1999 - 2006

Eric Britz (ericbritz@s-miner.com) – FORUM " Systèmes & Logiciels pour les NTIC dans le Transport " – Paris 18 mai 2006