Processus de développement de système contraint par des préconisations de sécurité d'un SI urbanisé

Jacques Simonin
jacques.simonin@telecom-bretagne.eu

Plan de la présentation

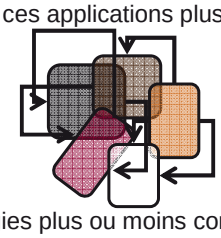
- Urbanisme de SI : un cadre d'architecture d'entreprise
- Conception d'une zone technique dédiée à la sécurité dans un SI urbanisé
- Mise en œuvre d'une zone technique dédiée à la sécurité dans un SI urbanisé
- Perspective

Plan de la présentation

- **Urbanisme de SI : un cadre d'architecture d'entreprise**
- **Conception d'une zone technique dédiée à la sécurité dans un SI urbanisé**
- **Mise en œuvre d'une zone technique dédiée à la sécurité dans un SI urbanisé**
- **Perspective**

Caractéristique d'un SI

- **Complexité du SI**
  - induite par l'évolution continuelle de l'entreprise (marché, technologies, …),
  - et par sa propre évolution
    - des centaines d'applications et…
    - des flux entre ces applications plus ou moins bien maîtrisés,



    - des technologies plus ou moins compatibles

… et de sa sécurité

- … vers une approche unifiée de la sécurité du SI
  - parce que de plus en plus de points sensibles existent
    - terminaux mobiles connectés sur le SI
    - entreprise orientée service
    - …
  - qui nécessitent
    - une stratégie dédiée à la sécurité du SI
    - des technologies de sécurité pertinentes
    - une vision globale de la sécurité du SI

Architecture d'entreprise

- **L'architecture d'entreprise offre des vues sur**
  - les objectifs de l'entreprise
  - l'organisation de l'entreprise
  - les processus métiers de l'entreprise
  - le SI de l'entreprise
  - les applications informatiques dans l'entreprise
  - les choix technologiques de l'entreprise

Architecture d'entreprise et modélisation

- **Architecture d'entreprise et modélisation**
  - Modélisation trop contraignante pour les cadres successeurs du cadre fondateur de l'architecture d'entreprise
    - J. A. Zachman : "A Framework for Information Systems Architecture". IBM Systems Journal 26, no. 3, pp. 276-292, 1987.
  - Création d'un cadre de l'architecture d'entreprise fondé sur une modélisation hiérarchique des vues
    - J. Sassoon : "Urbanisation des systèmes d'information". Hermès, 1998.

Propriétés du cadre d'urbanisation

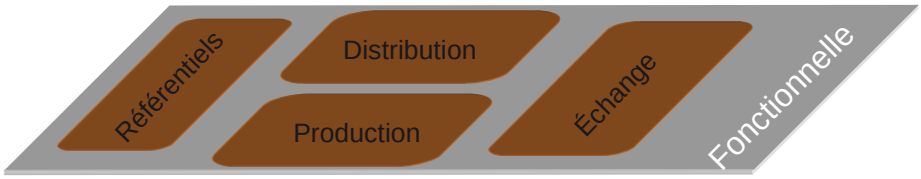
- **Cohérence des vues d'urbanisme avec les différentes architectures d'une application**
  - Vue métier : le « pourquoi ? »
    - quelle activité du processus de facturation de l'entreprise justifie l'application dans le SI ?
  - Vue fonctionnelle : le « quoi ? »
    - Quelles fonctions de facturation et de recouvrement sont réalisées par l'application ?
  - Vue technique : le « avec quoi ? »
    - Sur quelle infrastructure technique est déployée l'application ?
  - Vue applicative : le « comment ? »
    - Quel composant réalisant les fonctions de sécurité des données est conçu dans l'application ?

Propriétés du cadre d'urbanisation

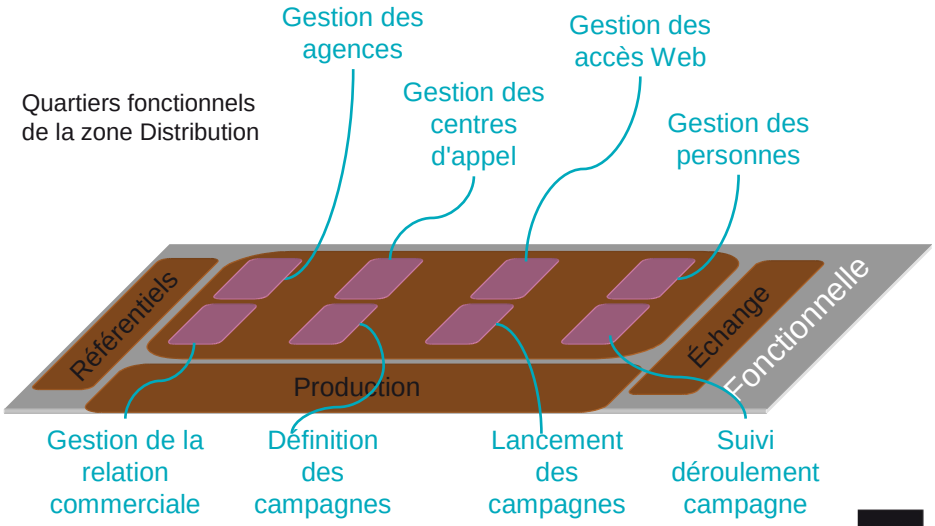
- **Cohérence de la modélisation hiérarchique des vues d'urbanisation avec le PLU (Plan Local d'Urbanisme) des communes (ex POS : Plan d'Occupation des Sols)**
  - Zone
  - Quartier
  - Îlot
  - Parcelle
  - Voie entre îlots

Exemple du PLU standard de la vue fonctionnelle – Zones

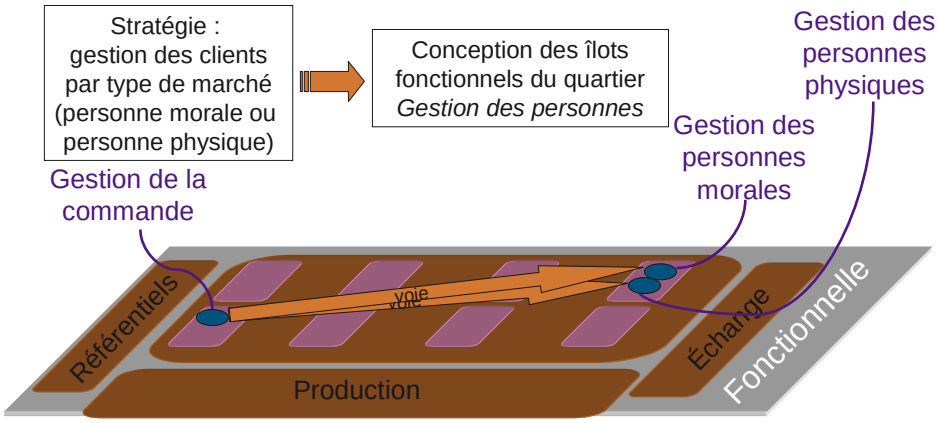
- **Extrait de zones fonctionnelles standards**
  - Zone Référentiels (Catalogue des produits et services, …)
  - Zone Distribution (Gestion de la relation commerciale, …)
  - Zone Production (Gestion des activités de production, …)
  - Zone Échange (Échanges avec un fournisseur, …)



Exemple du PLU standard de la vue fonctionnelle – Quartiers



Exemple du PLU de la vue fonctionnelle spécifique à la stratégie de l'entreprise – Îlots et voies



Conception de voies entre îlots fonctionnels des quartiers
Gestion de la relation commerciale et *Gestion des personnes*

…et dans la pratique ?

- **Une vue métier complète avec**
  - les processus du cœur de métier de l'entreprise
- **Une vue fonctionnelle déduite de la vue métier**
  - et souvent contrainte par les applications du SI
- **Une vue applicative complète avec**
  - les applications et les flux entre applications
- **Une vue technique complète suivant**
  - les infrastructures choisies pour déployer les applications

Plan de la présentation

- **Urbanisme de SI : un cadre d'architecture d'entreprise**
- **Conception d'une zone technique dédiée à la sécurité dans un SI urbanisé**
- **Mise en œuvre d'une zone technique dédiée à la sécurité dans un SI urbanisé**
- **Perspective**

Illustration de la sécurité dans un SI urbanisé
Cartographie de Télécom Bretagne

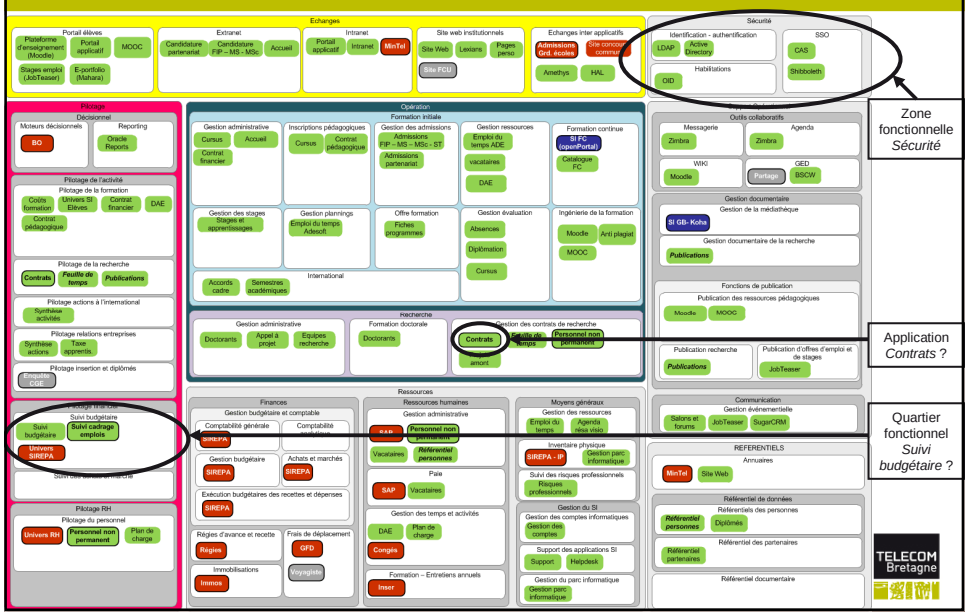
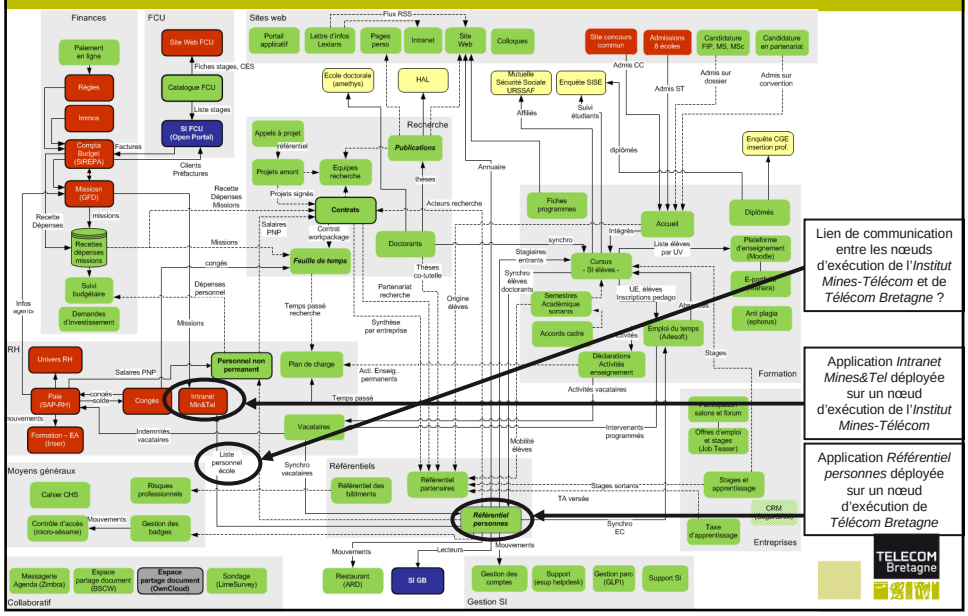


Illustration de la sécurité dans un SI urbanisé
Cartographie de Télécom Bretagne



Cartographie de la vue technique d'un SI urbanisé

- **Méta-modélisation utile à la description de la vue technique d'un SI urbanisé**
  - définition des concepts, et de leurs relations, décrivant une vue technique
    - concept de *nœud d'exécution* de la vue technique
  - …ainsi que les relations entre ces concepts et des concepts décrivant les autres vues
    - relation de *déploiement* entre le concept de *nœud d'exécution* et le concept *application* de la vue applicative
- **Cartographie à partir des concepts de la vue technique du SI et de leurs relations**
  - *Serveur_s* instancie le concept de *nœud d'exécution*
  - *Application_a* a une relation de déploiement sur *Serveur_s*

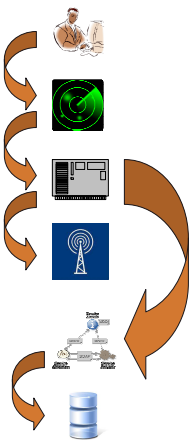
Intégration de la sécurité dans la cartographie d'un SI urbanisé

- **Compléments utiles à la description de la zone *Sécurité* dans le méta-modèle**
  - concepts propres à la sécurité (SecureUML, …)
    - risque, protection, intégrité, confidentialité…
  - concepts en relation avec les concepts propres à la sécurité
    - vue technique : noeud d'exécution, lien de communication, …
    - …mais aussi
      - vue métier : rôle, entité, activité, séquence d'activités, …
      - vue fonctionnelle : quartier fonctionnel, îlot fonctionnel, …
      - vue applicative : application, donnée applicative, …
- **Instances des concepts, et de leurs relations, du méta-modèle lié à la sécurité**
  - Récupération des instances cartographiées dans l'entreprise
  - Ajout des instances spécifiant la zone technique *Sécurité* de l'entreprise

3 illustrations de conception de la zone technique *Sécurité*

- **Méta-modélisation des vues du SI urbanisé, dédiée à la sécurité, fondée sur un processus métier**
  - Référence : échanges sur la propagation d'un risque à partir de la cartographie d'un SI avec la Marine Nationale
- **Spécification d'une règle de sécurité des réseaux conforme au méta-modèle dédié à la sécurité**
  - Référence : adaptation d'un processus de télémédecine à la vue technique le supportant
- **Spécification d'une règle de sécurité des données conforme au méta-modèle dédié à la sécurité**
  - Référence : projet de 3° année sur la conception et l'évolution des systèmes d'information (UV F23B301 à Télécom Bretagne)

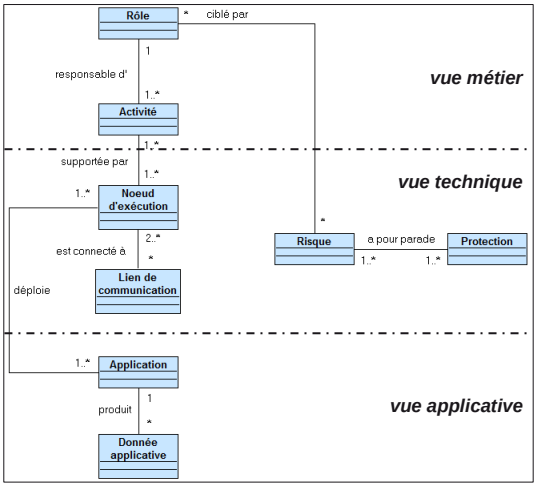
Illustration de méta-modélisation dédiée à la sécurité



- **Choix d'un processus de gestion de propagation d'un risque ciblant un rôle de l'organisation**
  - Un risque associé à un rôle (opérateur radar)
  - … responsable d'une activité (surveillance maritime)
  - …supportée par un nœud d'exécution (équipement de surveillance)
  - …connecté à un lien de communication (réseau MARSUR)
  - … et déployant une application (système de détection et d'identification de navire)
  - …produisant une donnée applicative ou physique (navire identifié)

Illustration de méta-modélisation dédiée à la sécurité

- **Méta-modèle lié à la sécurité déduit du processus de gestion de propagation d'un risque ciblant un rôle de l'organisation**
  - Concepts décrivant la zone technique *Sécurité*
    - Risque
    - Protection
  - Concepts liés à ceux décrivant la zone technique *Sécurité*
  - … et leurs relations



De la méta-modélisation dédiée à la sécurité vers la modélisation de la zone technique *Sécurité*

- **Conception du méta-modèle des vues d'urbanisation fondée sur les processus de l'entreprise liés à la sécurité**
  - processus de gestion de propagation d'un risque ciblant un rôle de l'organisation
  - … ?
- **… vers la modélisation des vues du SI intégrant la zone technique *Sécurité***
  - …avec réutilisation de la cartographie existante

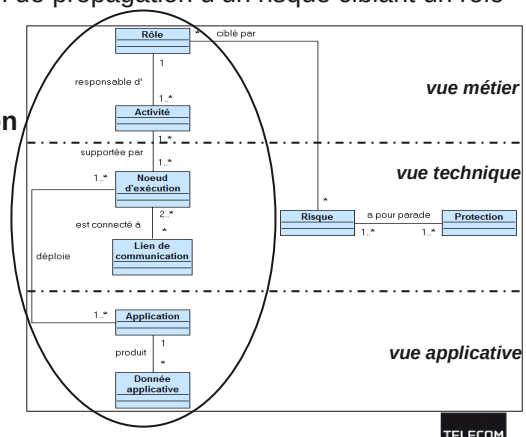
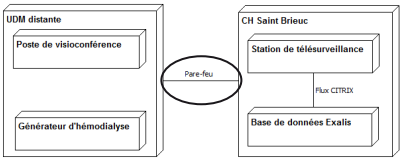


Illustration de spécification d'une règle de sécurité des réseaux

- **Exemple d'un processus de télédialyse**
  - contraint par un lien de communication le supportant



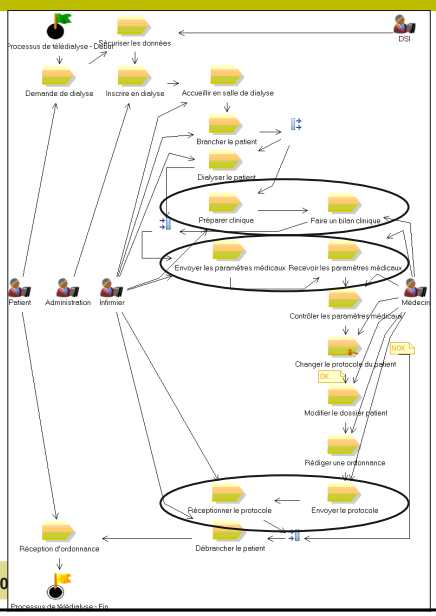


Illustration de spécification d'une règle de sécurité des réseaux

- **Méta-modèle lié à la sécurité déduit du processus de gestion de spécification d'un risque ciblant un lien de communication**

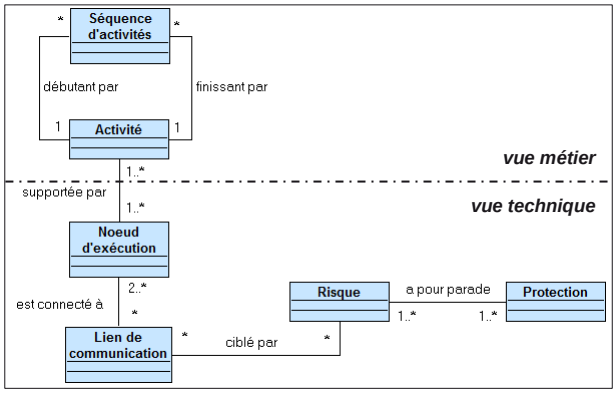
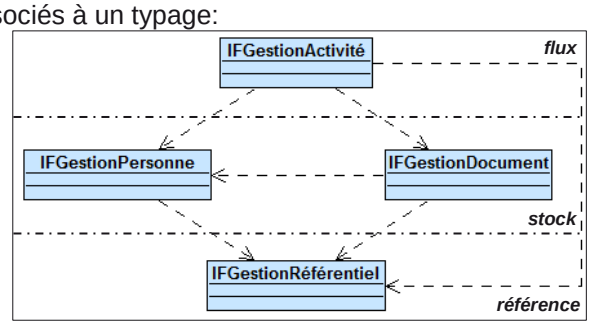


Illustration de spécification d'une règle de sécurité des réseaux

- **Règle de sécurité**
  - paramétrée par les concepts du méta-modèle lié à la sécurité
    - Mise en œuvre d'un niveau de sécurité plus élevé pour les liens de communication reliant des nœuds d'exécution supportant des activités reliées par une séquence
    - Sécurité des réseaux guidée par les processus métiers dont la conception prend en compte les liens de communication de la vue technique supportant ces processus métiers
  - … et pouvant être mises en œuvre dès la conception de l'architecture technique
    - suivant les exigences de sécurité à satisfaire

Illustration de spécification d'une règle de sécurité des données

- **Exemple d'un pattern d'urbanisme fonctionnel composé de**
  - quatre îlots fonctionnels de gestion (CRUD : création, lecture, mise à jour, suppression) associés à un typage:
    - IFGestionActivité → *flux*
    - IFGestionDocument → *stock*
    - IFGestionPersonne → *stock*
    - IFGestionRéférentiel → *référence*



  - six dépendances associées à des règles paramétrées par les types
    - *flux* dépend de *stock*
    - *flux* dépend de *référence*
    - *stock* dépend de *référence*

Illustration de spécification d'une règle de sécurité des données

- **Mise en œuvre du pattern d'urbanisme fonctionnel pour un système RH de gestion d'embauche d'un employé**
  - Chaque îlot fonctionnel réalise une donnée fonctionnelle associée au type de l'îlot la produisant (*flux*, *stock*, *référence*)

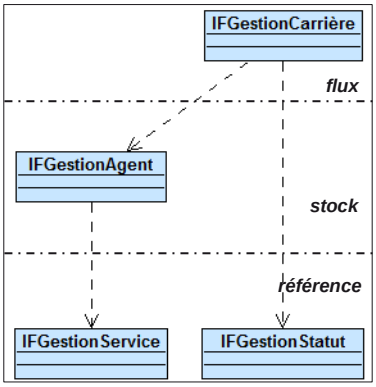


Illustration de spécification d'une règle de sécurité des données

- **Chaque donnée fonctionnelle est réalisée par au moins une donnée applicative associée au type de l'îlot produisant la donnée fonctionnelle (*flux*, *stock*, *référence*)**
- **Le type de chaque donnée applicative peut être associé à un critère non fonctionnel**
  - durée de vie
  - valeur associée

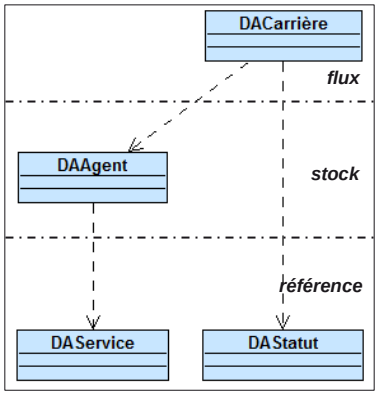


Illustration de spécification d'une règle de sécurité des données

- **Méta-modèle lié à la sécurité déduit du processus de gestion de spécification d'un risque ciblant une donnée applicative**

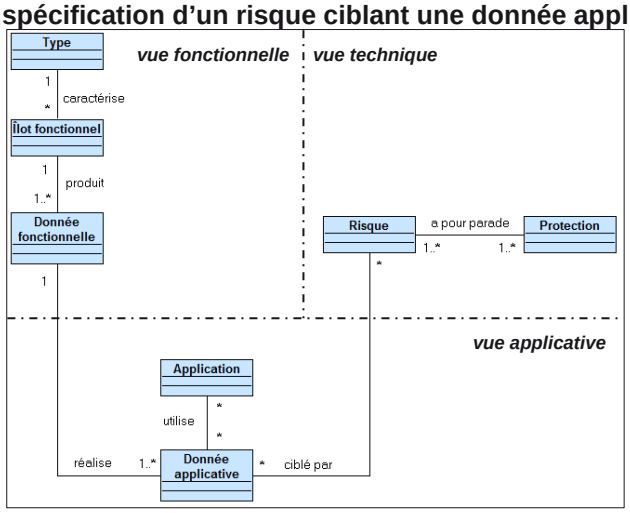


Illustration de spécification d'une règle de sécurité des données

- **Règle de sécurité**
  - paramétrée par les concepts du méta-modèle lié à la sécurité
    - Mise en œuvre d'un niveau de sécurité plus élevé pour les données applicatives réalisant des données fonctionnelles de type *stock* et utilisées par des applications du SI
    - Sécurité des données applicatives produite par des applications du SI et utilisées par d'autres applications du SI de l'entreprise

Plan de la présentation

- Urbanisme de SI : un cadre d'architecture d'entreprise
- Conception d'une zone technique dédiée à la sécurité dans un SI urbanisé
- Mise en œuvre d'une zone technique dédiée à la sécurité dans un SI urbanisé
- Perspective

Mise en œuvre de la vue technique d'un SI urbanisé

- **La vue technique cible dans les entreprises est mise en œuvre lors du développement de système par**
  - des préconisations sur les environnements d'exécution
    - J2EE, JPA, EJB, ...
      - utiles à la génération de code
  - des préconisations sur les nœuds d'exécution
    - conformes aux exigences non fonctionnelles de l'entreprise
      - nombre d'utilisateurs, fréquence d'exécution d'un processus de commande, …
  - des préconisations sur les liens de communication
    - conformes aux exigences non fonctionnelles de l'entreprise
      - réseaux de distribution, quantification des flux de données, …

Illustration d'assistance au processus de développement fondée sur l'extension du méta-modèle de développement

- **Intégration des fonctions techniques de sécurité dans un développement de système**
  - fondée sur l'ingénierie des modèles (dédiée au processus de développement)
  - outillée par des transformations de modèles
    - Transformations d'un modèle d'architecture fonctionnelle en un modèle d'architecture applicative contraintes par les fonctions techniques

Réalisation des fonctions techniques dans les diagrammes de séquence applicative

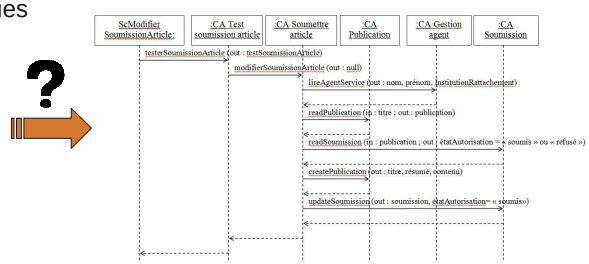


Illustration d'extension du méta-modèle dédié au développement

- **Ajout du concept de fonction technique de sécurité dans le méta-modèle dédié au développement**
  - Fonction technique de surveillance du déroulement des processus métiers composés d'une séquence de deux activités de type émission et de type réception
    - Sécurité des réseaux
  - Fonction technique de surveillance des flux de données applicatives d'un SI entre applications suivant le type de l'îlot fonctionnel produisant la donnée fonctionnelle réalisée par la donnée applicative
    - Sécurité des données
- **Conception de règles de développement intégrant le concept de fonction technique de sécurité**
  - … et conformes au méta-modèle de développement étendu

Plan de la présentation

- Urbanisme de SI : un cadre d'architecture d'entreprise
- Conception d'une zone technique dédiée à la sécurité dans un SI urbanisé
- Mise en œuvre d'une zone technique dédiée à la sécurité dans un SI urbanisé
- Perspective

Conception et mise en œuvre de la zone technique *Sécurité* - Perspective

- **Thèse à vocation à être appliquée dans un cadre industriel**
  - Conception d'un méta-modèle composé des concepts en lien avec les processus métiers de sécurité de l'entreprise
  - Modélisation des vues de l'entreprise conformément au méta-modèle dédié à la sécurité (complétion de la cartographie)
  - Spécification ou adaptation de règles de sécurité utiles au développement de système et paramétrés par les concepts du méta-modèle dédié à la sécurité
  - Extension du méta-modèle dédié au développement avec, par exemple, le concept de fonction technique de sécurité supportant une règle de sécurité
  - Spécification ou adaptation de règles de développement utiles au développement de système et paramétrés par les concepts du méta-modèle, dédié au développement, étendu
  - Expérimentation d'une aide au développement de système intégrant, par exemple les fonctions techniques de sécurité, avec un outil d'ingénierie des modèles