Secur-ED : retour d'expérience d'une convergence EBIOS-2010/NIST SP800-30

Réunion Club-EBIOS du 12/12/2013

THALES

Agenda

- **Introduction**
  - Le projet SECUR-ED
  - Contexte des PTO
- **Présentation de la méthodologie**
  - Les normes et méthodologies existantes
  - Présentation de la méthodologie pour SECUR-ED
- **Conclusion**
  - Retour d'expérience et bilan des apports EBIOS/NIST
  - Questions

SECured URban Transportation - European Demonstration

L'objectif du projet SECUR-ED

SECUR-ED
www.secur-ed.eu

Des démonstrations

- Paris (RATP - Détection explosive, toxique/chimique et radioactif)
- Madrid (CTM – Outil de gestion d'incidents interopérable entre les opérateurs)
- Milan (ATM – Analyse de flux vidéo pour surveiller les menaces)
- Berlin (DB BAHN - Standards et procédures d'urgence en cas de crise)

Un projet européen

- 42 mois (du 01-04-2011 au 30-09-2014)
- 40 millions euros dont une partie financée par l'EU
- Europe fournit 25 M€, le plus gros projet de sécurité du programme FP7

Ouvrir un nouveau marché

- Ce projet permet la création d'un marché Européen pour fournir des solutions de sécurité adaptées au transport de masse.

SECured URban Transportation - European Demonstration

Définition

Procédures opérationnelles et organisationnelles – Plans

- La résilience des infrastructures
- Approche fondée sur le risque
- Procédures: organisationnel, opérationnel et informatique
- Les plans de sécurité
- Gérer la coopération entre les opérateurs, les premiers intervenants et les passagers
- La planification des interventions en cas d'incident

Implémentation

Infrastructure

- Solutions de protection des Infrastructures
- Video analytics: détection et suivi des menaces
- CBRN-E: détection, dispersion, décontamination
- Systèmes d'information temps-réel interconnectés

Opération

Entrainement et simulation

- Sécurité du train et celui du personnel
- Entrainer les opérateurs de contrôle
- Préparer les passagers aux risques

THALES

Contexte des opérateurs de transport urbain (PTO)

Les enjeux et les contraintes

Fournir des services aux citadins

- Répondre au besoin de mobilité des citadins
- Fournir de nouveaux services connectés

Une infrastructure permettant le transport

- Une infrastructure géographiquement distribuée
- Forte interconnexion entre les opérateurs de transport

Sécurité IT

- Héritage de technologies obsolètes (interopérabilité, coût d'exploitation et de maintenance, etc…)
- Utilisation fréquente des produits sur étagères (COTS)

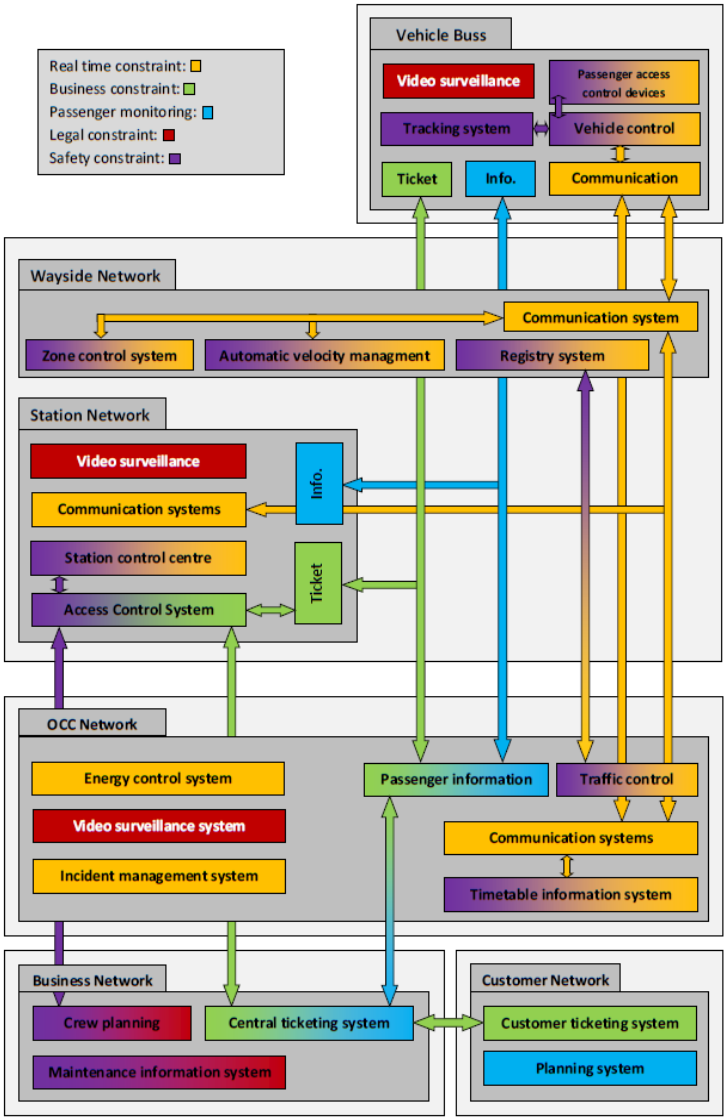
Garantir la sécurité des passagers

- Sureté de fonctionnement
- Sureté et sécurité des passagers

Etre en mesure d'assurer les revenus

- Mise en place d'un système de facturation
- Fournir une infrastructure pour contrôler le paiement des passagers

Contexte des opérateurs de transport urbain (PTO)



- ***Operations control centre (OCC):***

  Ce système permet de surveiller l'ensemble de l'infrastructure et de garder une trace de tous les incidents.

- ***Wayside systems:***

  Ce système communique avec le véhicule afin de contrôler et de surveiller le mouvement du train.

- ***Station systems:***

  Ce système contrôle entièrement l'infrastructure de la station : ascenseurs, escalateurs, passagers, trains, annonces, etc…

THALES

Agenda

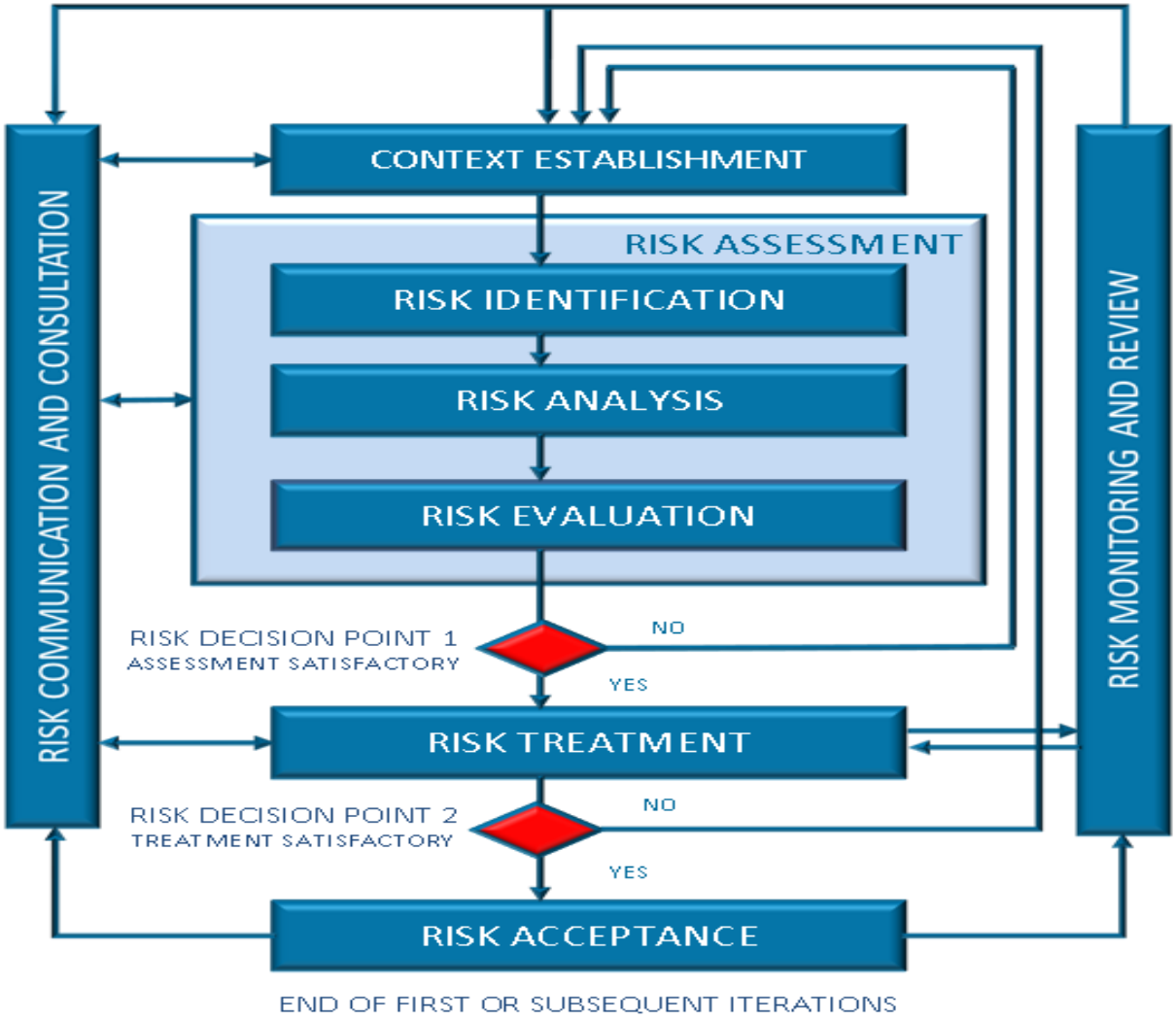
- **Introduction**
  - Le projet SECUR-ED
  - Contexte des PTO
- **Présentation de la méthodologie**
  - Les normes et méthodologies existantes
  - Présentation de la méthodologie pour SECUR-ED
- **Conclusion**
  - Retour d'expérience et bilan des apports EBIOS/NIST
  - Questions

Les normes et méthodologies prises comme sources

- **ISO 27005**
  - Gestion des risques de la Sécurité des Systèmes d'Information
- **EBIOS 2010**
  - EBIOS 2010 - Expression des Besoins et Identification des Objectifs de Sécurité
  - Méthode de gestion des risques portée par l'ANSSI (FR)
- **NIST SP800-30**
  - Guide pour la réalisation d'une analyse de risques portée par le NIST (US)
- **NIST SP800-53**
  - Guide pour la sécurité des systèmes d'information

Présentation de la méthodologie d'analyse de risques

- **Structure générale : ISO 27005**



Présentation de la méthodologie d'analyse de risques

- **Étude du contexte :**
  - Classique et commun à toutes les méthodes
    - Contexte général, périmètre, contraintes, etc.
    - Reprise de la typologie EBIOS-2010 pour les sources de menace
  - Définition des métriques
    - Celles communes aux 2 méthodes (Vraisemblance, Gravité, Niveau de risque)
    - « Catégorisation SI » Vs « Besoin de sécurité »

Présentation de la méthodologie d'analyse de risques

- **Étude des risques :**
  - Reprise du principe EBIOS des 2 branches distinctes
    - Étude des évènements redoutés
    - Étude des scénarios de menace
  - Approche orientée « scénarios » pour les scénarios de menace
    - Besoin de prise en compte d'attaques complexes
    - Utilisation d'arbres d'attaque

Présentation de la méthodologie d'analyse de risques

- **Traitement des risques :**
  - Reprise de l'approche prônée par la SP800-53
    - Catégorisation des SI par niveau de criticité
    - Ensembles prédéterminés de mesures de sécurité (baselines)
    - Ajustement des mesures de sécurité au contexte et aux risques à couvrir

Agenda

- **Introduction**
  - Le projet SECUR-ED
  - Contexte des PTO
- **Présentation de la méthodologie**
  - Les normes et méthodologies existantes
  - Présentation de la méthodologie pour SECUR-ED
- **Conclusion**
  - Retour d'expérience et bilan des apports EBIOS/NIST
  - Questions

Retour d'expérience et bilan des apports EBIOS/NIST

Pourquoi avoir eu besoin d'une méthodologie propre à SECUR-ED?

- Pour des raisons politiques
  - Programme européen donc choix d'une méthodologie nationale = sujet à polémiques
  - Choix de l'ISO 27005 est consensuel
- Pour des raisons techniques
  - L'ISO 27005 reste un cadre, trop vague pour une mise en œuvre opérationnelle directe
  - EBIOS et NIST ont été des sources importantes pour l'ISO 27005
- Pour des raisons culturelles
  - L'approche par les « besoins de sécurité » des « biens essentiels » n'est pas comprise/considérée comme pertinente dans l'étude des évènements redoutés
- Parce qu'il y a du bon dans les différentes approches
  - L'approche des scénarios de menaces par arbres d'attaque
  - L'approche du traitement des risques par utilisation de baselines

Questions ?