EADS INNOVATION WORKS

PROTECTION ET SECURITE DES INFRASTRUCTURES CRITIQUES

ENJEUX DES SYSTEMES SCADA

ADAPTATION DES PRATIQUES DE SECURITE DE L'INFORMATION AUX SAIV/SCADA

Spécificités des infrastructures SCADA
Evolutions et adaptation des pratiques SSI
Particularités

CLUSIF - PARIS
Y.FOURASTIER
Avril 2008

AGENDA
SCADA's security at stake

- **La sécurité des infrastructures critiques**
  - **Introduction à...**
  - **... la dépendance aux sous systèmes SCADA**

- **Spécificités des systèmes de type SCADA**
  - **Architecture générale**
  - **Homologations et normes de sécurité**
  - **Méthodes de construction sûre**
  - **Quand la SSI « classique » entre en scène : COTS/COTS, COTS/CODEC et M2M**

- **Particularités et outils**
  - **Sécurité à niveau composant, à niveau système**
    - **Méthodes existantes et SSI**
    - **Choc des cultures**
  - **Des outils :**
    - **pour modéliser, simuler et représenter virtuellement**
    - **pour intégrer la sûreté à la sécurité, assurance et confiance**

SECURITE DES INFRASTRUCTURES CRITIQUES

Introduction à la protection et à la...

- **Des enjeux vitaux :**
  - **Protéger les infrastructures critiques**
  - **Assurer la continuité des activités économiques, sociales et politiques**
- **Une société moderne :**
  - **Basée sur le "*just in time*"**
  - **Dépendante de biens et de services distribués via des infrastructures critiques**
    - **Électricité**
    - **Fluides : eau, gaz**
    - **Information et télécommunications de façon générale, Internet en particulier**
    - **Réseaux ferrés et Transport : signalisation**
- **Les conséquences de…**
  - **… dysfonctionnements, deviennent plus grave : impacts économiques, voire politiques**
  - **… pannes, deviennent catastrophiques : impacts humains, à potentiel létal élevé**
- **Prévenir, contenir et atténuer : Protection et Sécurité**
  - **Superviser et contrôler le fonctionnement de systèmes durcis et résilients**
  - **Organiser à partir du traitement des alarmes jusqu'aux niveaux très globaux**
- **Au cœur : les infrastructures SCADA**

SECURITE DES INFRASTRUCTURES CRITIQUES

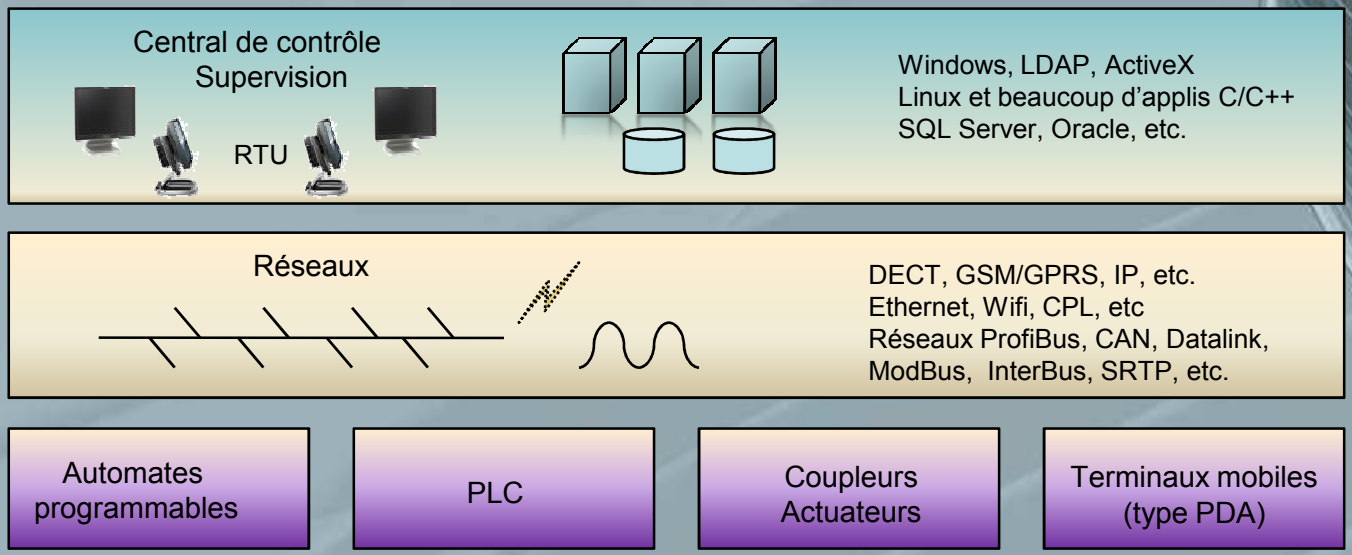
… la dépendance aux sous systèmes SCADA

- **SCADA :**
  - ***Supervisory Control And Data Acquisition***
  - **Un terme <u>générique</u>, commun à de très nombreux secteurs d'activités**
  - **Réseaux de données, de type « informatique industrielle »**
- **Fonctions :**
  - **Télécommande**
  - **Télémétrie**
  - **Gestion automatisée / semi-automatisée**
- **Où trouve t'on des SCADA :**
  - **Production, transport et distribution énergétique**
  - **Traitement et distribution d'eau**
  - **Réseaux de transports : systèmes de signalisation**
  - **Systèmes d'oléoducs et de gazoducs**
  - **Systèmes industriels** (penser qu'AZF était interconnecté avec la SNPE…)
- **Où en trouve t'on dénommés différemment** (facteur d'échelle… et ce n'est pas le propos du jour)
  - **Réseaux vitaux de systèmes complexes : avions, navires, grands bâtiments, etc.**
  - **Satellites et constellations satellitaires**
  - **Etc.**

SPECIFICITES DES SYSTEMES DE TYPE SCADA

Architecture générale et générique... Face à la nécessité d'adaptation

- **Architecture type**



- **Des disciplines scientifiques et technologiques très mûres et expérimentées**
  - **Fiabilité, sûreté de fonctionnement, robustesse, stabilité, maintenabilité, etc.**
  - **Développements prouvés, méthodes formelles, etc.**

- **Des pratiques bien établies :**
  - **Des automates fiables (… très fiables) dotés de grilles de sécurité mais… peu de sûretés informatiques**
  - **Gestion d'incidents et des pannes, gestions préventives… peu de gestion de la sécurité informatique**
  - **Gestion des conséquences systémiques d'incidents**

RTU : Remote Terminal Unit
PLC : Programmable Logic Ontroller

SPECIFICITES DES SYSTEMES DE TYPE SCADA

Quand la SSI classique entre en scène : COTS/COTS, COTS / CODEC et M2M

- **La problématique de standardisation généralisée**

- ***COTS : Components On The Shelf***
  - **au-delà du logiciel à fenêtres renommé…**
  - **… les Legos : des composants génériques prêts à assembler (puces, cartes, logiciels, etc.)**
  - **des composants avec leurs vulnérabilités**

- **Réseaux :**
  - **de COTS, sans ségrégations franche ni cloisonnements (COTS/COTS et COTS/CODEC)**
  - **Interfaces d'encodage avec les réseaux de commande et de contrôle ("propriétaires ")**
  - **M2M (*Machine to Machine*) : interconnexions entre automates**

- **Enjeu de protection :**
  - **la maîtrise du non alignement des vulnérabilités sur la chaine automatisée de traitement**
  - **l'intégration de mécanismes de sécurité au STAD* , à niveau global et localement**
  - **la priorité :**
    - **l'interception de l'action risquée,**
    - **notamment intentionnelle à caractère malveillant**

***STAD : Système de Traitement Automatisé de Données**

SPECIFICITES DES SYSTEMES DE TYPE SCADA

Quand la SSI classique entre en scène : COTS/COTS, COTS / CODEC et M2M

- **Apports de la SSI « classique » : des outils maîtrisés**
- **Des référentiels outillés pour l'analyse de risques « systèmes d'informations »**
  - **Méhari,**
  - **EBIOS**
  - **SVA**
- **Des référentiels de spécifications pour la sécurité :**
  - **ISO27000 pour l'organisation du système de management de la sécurité de l'information**
  - **Critères Communs pour l'assurance sécurité IT**
- **L'approche 'Impact à probabilité d'occurrence égale à 1'**
  - **Si l'attaquant a décidé de réussir quand il en a le temps et les moyens, il atteint sa cible.**
  - **L'effort est de ramener le risque à un niveau de conséquences acceptables et maîtrisées**

***STAD : Système de Traitement Automatisé de Données**

ADAPTATION DES PRATIQUES DE SECURITE DES SYSTEMES D'INFORMATION

Extension du périmètre de la sécurité existant au champ de la sécurité de l'information

- **Risk Management**
  - **Intégration de la composante informationnelle**
  - **Des listings d'intervenants…**
  - **… aux données de configuration des grilles de sécurité des automates.**
- **Risque mesuré :**
  - **en vies humaines,**
  - **en impact politiques**
  - **ou économiques majeurs à graves**
- **La menace est profilée et réelle, notamment en ce qui concerne**
  - **Hacktivisme**
  - **Terrorisme**
- **Qu'est ce qui est critique dans une infrastructure critique ?**
  - **Criticité de l'information et classification des données de commande comme de contrôle**
  - **Qualification des composants et *information assurance***

ADAPTATION DES PRATIQUES DE SECURITE DES SYSTEMES D'INFORMATION

Extension du périmètre de la sécurité existant au champ de la sécurité de l'information

- **Adaptation des pratiques opérationnelles de la SSI :**
  - ***Awareness et Training…*** *culture des opérateurs (…fiabilité et disponibilité* **vs** *confiance)*
  - ***Supervision* et *Monitoring…*** *intégration aux centraux existants*
  - ***Incident handling* et *First response…*** *pertinence relative aux risques "industriels"*
  - ***Security Assessments* (techniques)…** par qui et pour qui

↳ **Le mariage de la carpe et du lapin…**

- **Adaptation des recours**
  - ***Emergency* et *Contingency planning* : intégration aux dispositifs préfectoraux**
  - ***Crisis Management* : intégration aux dispositifs sous autorité de l'Etat**
  - ***Continuity planning* : *backup* et *recovery***

↳ **Un univers à part… à intégrer**

SPECIFICITES DES SYSTEMES DE TYPE SCADA

Homologations et normes de sécurité, méthodes de construction sûre

- **Réglementation (dont législation) renforcée**
  - ***Sécurité industrielle et technologique, 2003, 2004, 2006 et 2007***
  - **Régime de certification avec contrôles : Transport, Energie, Industrie (ex. Seveso, etc.)**

- **Nécessité d'homologation :**
  - **Fourniture des éléments permettant à l'autorité de se forger une opinion**
  - **Suivi de l'autorité de tutelle (selon le cas, Transport, Industrie, Défense),**
  - **Rôle des organismes de contrôle : DRIRE**
  - **Responsabilités en rapport de l'homologation**

- **Normes sectorielles de sécurité**
  - **De niveau système puis décliné par domaines technologiques**
  - **Exemple ferroviaire :**
    - **EN50126 (IEC62278), applicable aux réseaux SCADA de signalisation**
    - **Notion de SIL : *Safety Integrity Level***
  - **Exemple aéronautique :**
    - **ARP4761 et ARP4754 pour la sécurité des systèmes aéronautiques**
    - **DO178, systèmes logiciels embarqués, DAL : *Development Assurance Level***

SPECIFICITES DES SYSTEMES DE TYPE SCADA

Homologations et normes de sécurité, méthodes de construction sûre

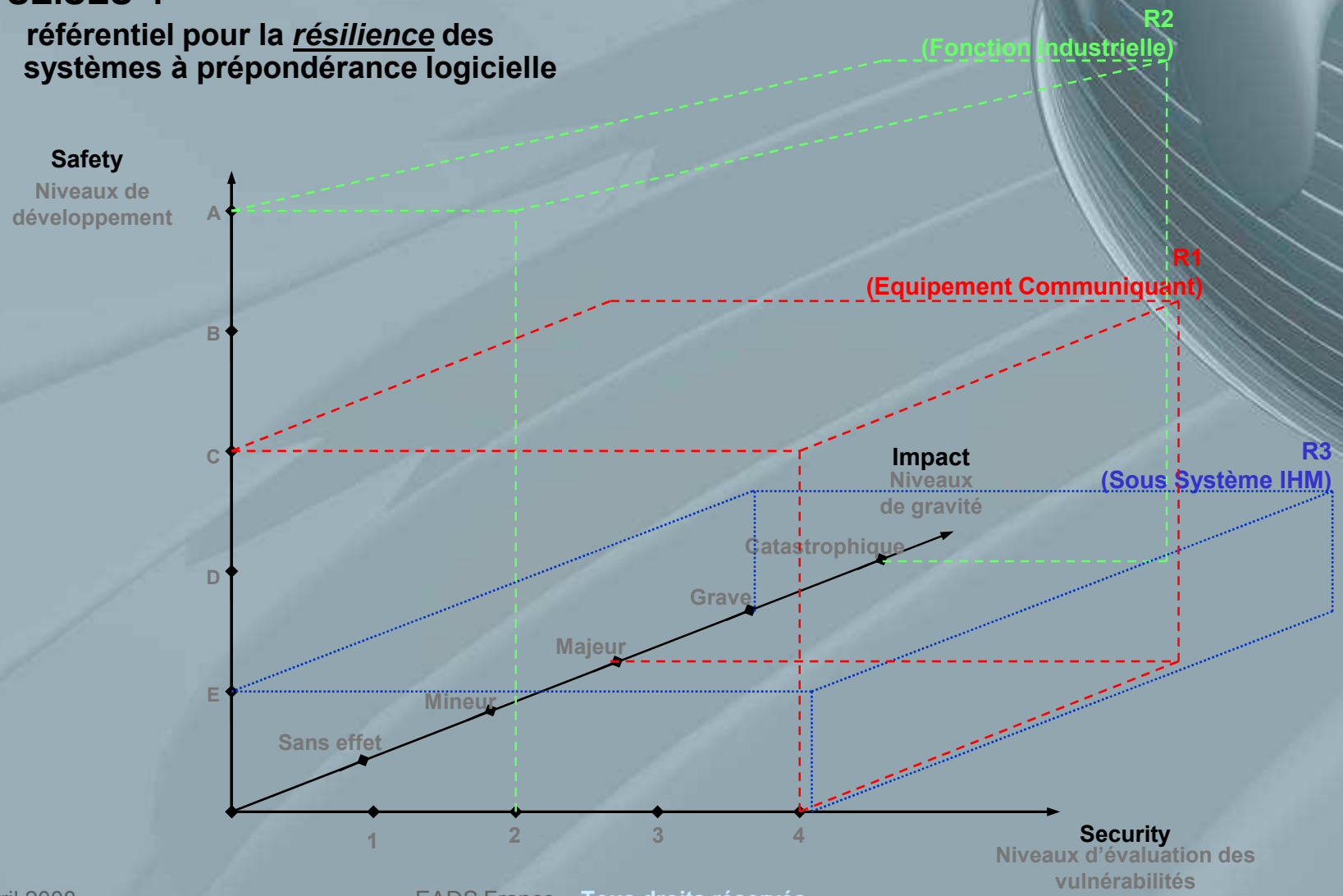
- **Une réalité certaine en ce qui concerne la sécurité des…**
  - **"Systèmes d'Information" : écart culturel important.**
  - **Quand on considère le "système de contrôle de process"…**
  - **… on ne parle pas vraiment des données techniques et de leurs STAD**
- **La conscience de l'acte intentionnel sur l'information / sur les STAD**
  - **A caractère malveillant**
  - **Un enjeu de sensibilisation…**
- **Arrivée de la "génération Internet" et … problèmes de maturité à considérer**
  - **Changement de génération chez les opérationnels : transmission des « savoirs faire métier »**
  - **Maturité des technologies**
- **Maturation du secteur de la sécurité industrielle norme *ISA99* :**
  - **ANSI/ISA-99.00.01-2007 :** ***Security for Industrial Automation and Control Systems: Concepts, Terminology and Models…*** **fin 2007**
  - **ANSI/ISA-TR99.00.01-2007 : Security Technologies for Manufacturing and Control Systems**
  - **Part 2 en cours :** ***Security for Industrial Automation and Control Systems, Establishing an Industrial Automation and Control Systems Security Program…***

PARTICULARITES ET OUTILS

Adaptation des pratiques de SSI… et relation à la maturité de développement

- **SEISES :**

  référentiel pour la *résilience* des systèmes à prépondérance logicielle



PARTICULARITES ET OUTILS
Représentations virtuelles et simulations

Des conséquences d'incidents

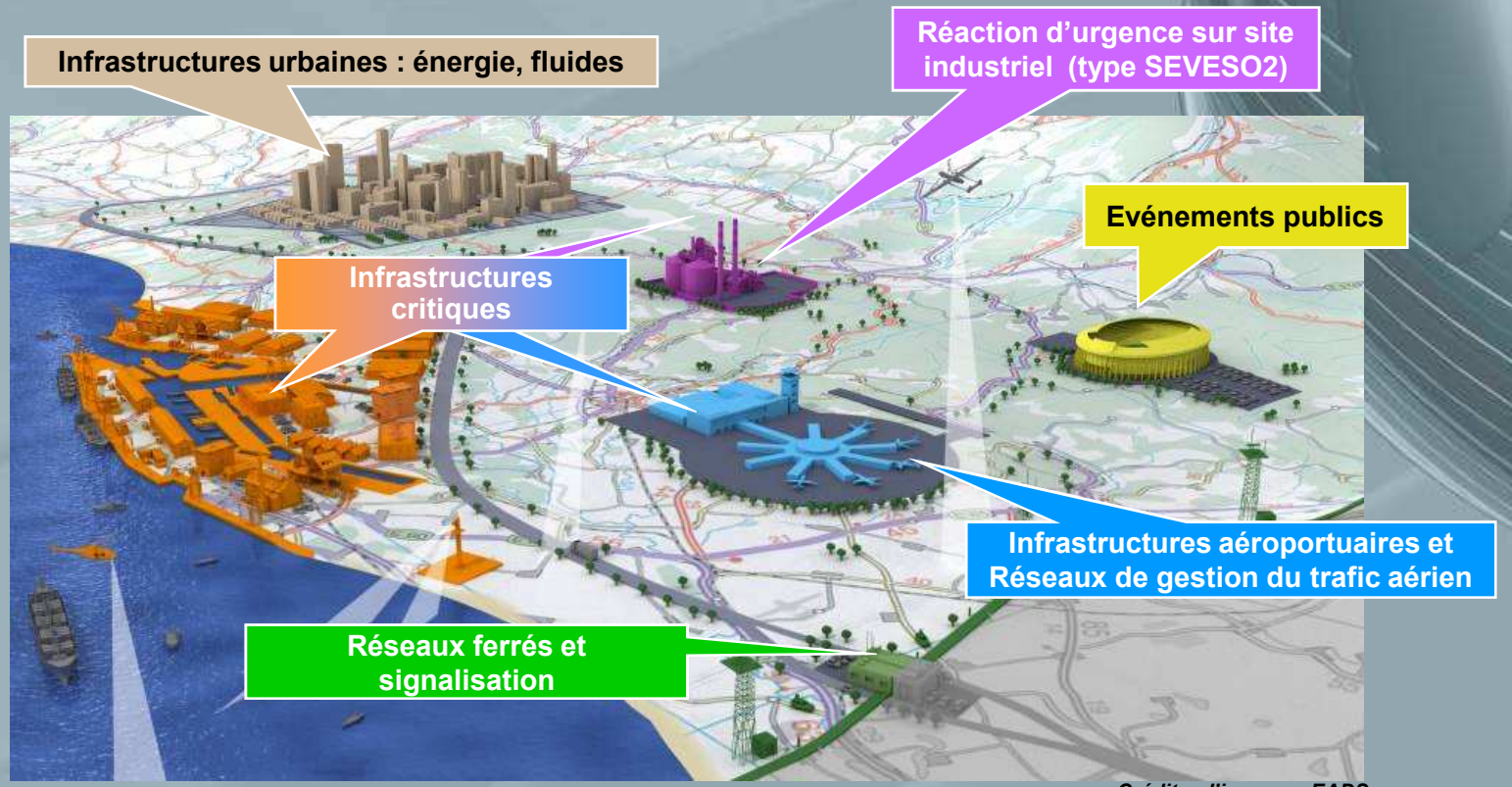
- Rapidement systémiques
- De dimension ample
- Impactant des vies humaines

Scénarios et expérimentations

- Dispositions et systèmes de sûreté (nota : législation des établissements accueillant du public)
- Visualisation de conséquences d'incidents
- *Risk management* intégrant le volet concernant les informations et les données

PARTICULARITES ET OUTILS

Simulations, études des propagations d'erreurs et de conséquences



Crédits d'images : EADS

- **Cartographie et modélisation des interdépendances**
  - Etude des réactions en chaînes
  - Attaques en rebond
  - Débordements
- **Dispositifs de sécurité sur les SCADA**
  - Mode d'implémentation : moyen, implantation
  - Organisation :
    - Security et *Contingency Planning*
    - *Emergency response* et *Backup*

Conclusion

- **Organiser la sécurité des infrastructures critiques**
  - **Dispositions règlementaires récentes (2004, 2007)**
  - **… l'important aujourd'hui :**
    - **Quoi protéger ?**
    - **Qui est responsable de quoi et corollaire, quelles droits et obligations de faire quoi ?**
    - **Quels coûts et son corollaire, qui paye ?**

- **Trois temps :**
  - **Gérer l'existant :**
    - **Cartographier et qualifier les priorités**
    - ***Technical Security assessements* : où risque t'il d'y avoir de vrais problèmes ?**
    - **Corriger l'urgent… pour éviter les catastrophes**
  - **Opérer la transition :**
    - **Intégrer l'organisation de la sécurité dans les contextes opérationnels**
    - **Intégrer l'organisation de la gestion des incidents…**
    - **… en préparant les évolutions de réglementation**
  - **Préparer l'avenir :**
    - **Pratiques de *Security* intégrées à la *Safety***
    - **Infrastructures critiques résilientes par construction**