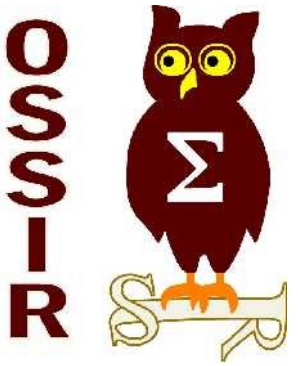
HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet



Compte-rendu du Training BlackHat

« Building, attacking and defending SCADA systems »

13 novembre 2012

Rémi Chauchat <Remi.Chauchat@hsc.fr>

Training BlackHat USA 2012

- Sponsorisé par l'OSSIR (merci !)
- Formation durant l'événement BlackHat USA 2012
- 2 jours complets, avant les conférences BH

- Présenté par :
  - Tom Parker

    → FusionX – Directeur technique (CTO)

  - Jonathan Pollet

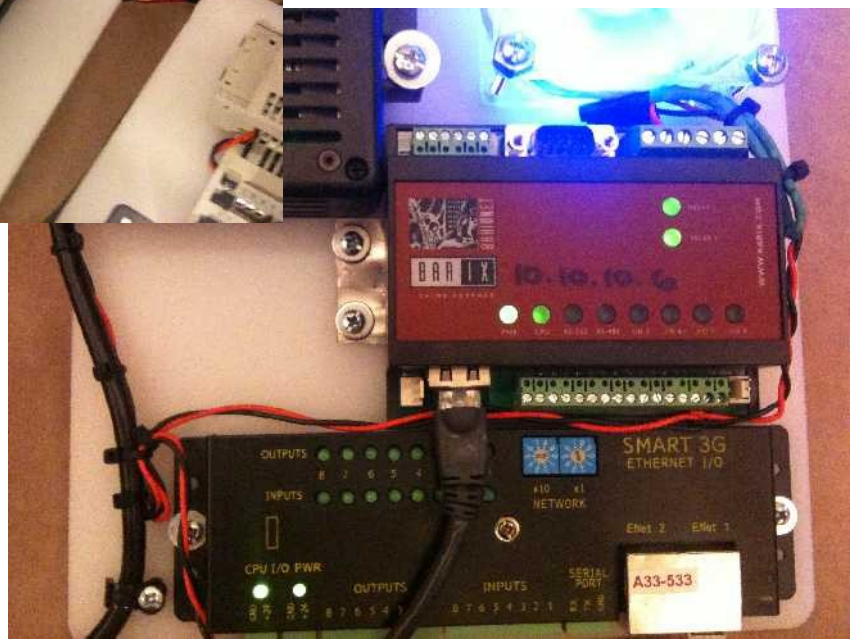
    → Red Tiger Security – Fondateur et consultant principal

Training BlackHat USA 2012

- Plan de formation / Objectifs
  - Introduction et définitions du monde industriel / technologies SCADA
  - Composants et protocoles SCADA
  - Exemples concrets des technologies SCADA
  - Normes
  - Attaques et défenses des infrastructures SCADA

Training BlackHat USA 2012

- Quelques démonstrations et utilisations d'outils



Introduction et Définitions

Introduction et définitions

- Systèmes
  - **ICS (*Industrial Control Systems*)**
  - **SCADA (*Supervisory Control and Data Acquisition*)**
  - DCS (*Distributed Control System*)
  - EMS (*Energy Managements Systems*)
  - MES (*Manufacturing Execution Systems*)
  - AMR / AMI (*Automated Meter Reading / Infrastructure*)
  - BAS (*Building Automation Systems*)

  - Et d'autres...

Introduction et définitions

- Composants SCADA
  - **PLC (*Programmable Logic Controller*)**
  - **RTU (*Remote Terminal Unit*)**
  - IED (*Intellignent Electronic Device*)
  - **HMI (*Human Machine Interface*)**

Termes et définitions (bref)

- PLC (*Programmable Logic Controller*)
  - Automate Programmable Industriel (API)
- SIS (*Safety Instrumented System*)
  - Automate Programmable de Sécurité (APS)

- Réalise un processus industriel programmé
- Communique directement sur des entrées (capteurs) et sorties physiques en fonction de consignes et du processus

Termes et définitions (bref)

- RTU (Remote Terminal Unit)
  - Réalise un processus spécifique pré-configuré
    - Analyse de la qualité de l'eau
    - Calcul de flux
    - Détection de fuite dans une conduite
    - Analyse de qualité de gaz
    - Etc.
  - Par rapport à un PLC
    - Moins flexible
    - Généralement plus compact
    - Moins coûteux en énergie

Termes et définitions (bref)

- IHM (Interface Homme-Machine)
  - Interaction entre l'Homme et la Machine (système industriel)
    - Envoi de commandes aux automates
      - Démarrage
      - Arrêt
      - Modification de données (vitesse / pression / etc.)
    - Réception d'informations de l'environnement industriel
      - État des automates
      - Valeurs des capteurs
      - Etc.
    - Interface de développement
      - Configuration des automates (adressage IP / comptes d'accès / etc.)
      - Programmation des automates

Introduction et définitions

- **Protocoles de communication**
  - Modbus (RTU / RS-232 / RS-485 / TCP/IP)
    - Protocole ouvert
    - Aucun chiffrement ni authentification
  - Profibus
  - DNP
    - Protocole ouvert
    - Chiffrement + authentification mutuelle
  - OPC (OLE for Process Control → Open Platform Communications)
    - Présent dans le « LAN de contrôle »
    - Communication entre les IHM et les contrôleurs
    - Fonctionne avec un serveur et un client

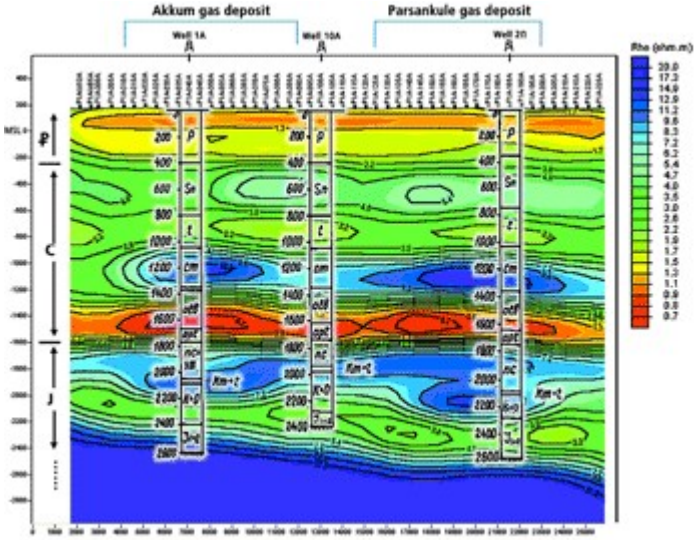
SCADA par l'exemple

SCADA : Pétrole et Gaz

- Exploration
- Forage
- Production
- Transport
- Raffinage
- Distribution

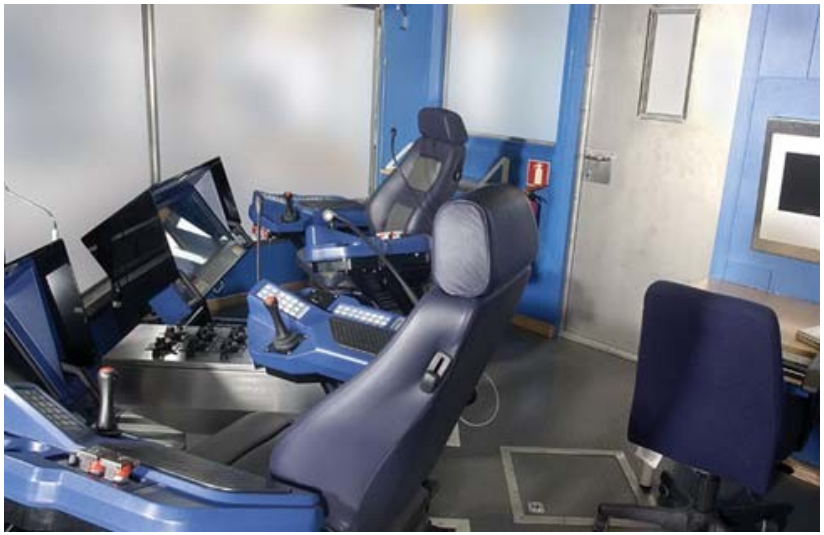
SCADA : Pétrole et Gaz

- Exploration
  - Recherche de ressources sous la roche
  - Explosifs utilisés pour créer des tremblements de terre (génération/propagation d'ondes)
  - Analyse et cartographie 2D / 3D du sous-sol
  - Recherche du point de forage optimal



SCADA : Pétrole et Gaz

- Forage
  - IHM (écran / joystick) de contrôle
    - envoi d'un signal aux PLC
    - les PLC traduisent ce signal pour modifier la vitesse / la direction / etc.
  - Capteurs de pression
  - PLC de sécurités



SCADA : Pétrole et Gaz

- Production
  - Stockage et contrôle des fluides avant leur transport

Le gaz est utilisé sur place et/ou vendu

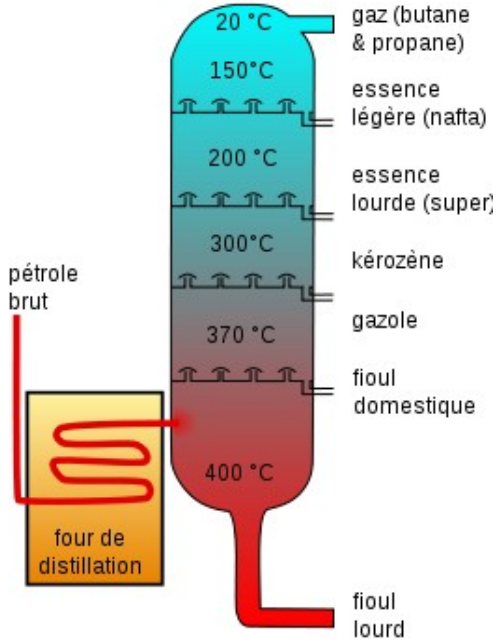
Le pétrole brute avec moins de 3% d'impuretés est mesuré et vendu

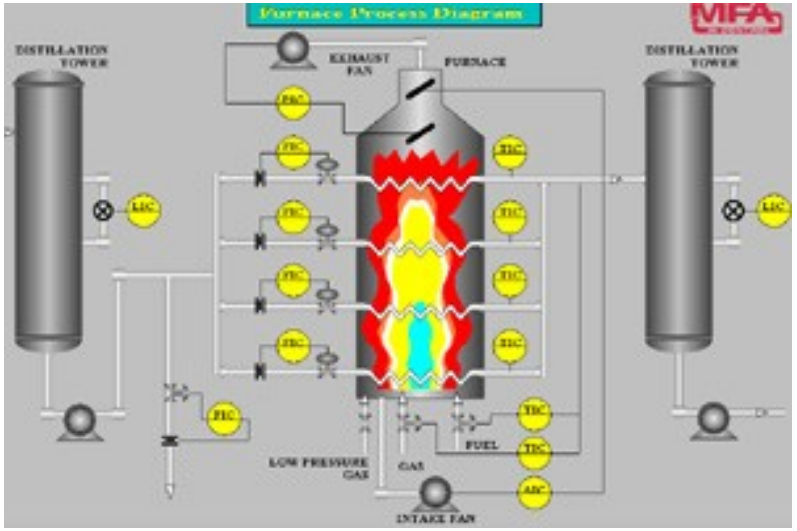
SCADA : Pétrole et Gaz

- Transport via gazoduc / oléoduc (*pipeline)*
  - Déplacement par différence de pression (1 à 6 m/s)
  - Capteurs présents tout le long
    - Contrôle de la pression
    - Contrôle de la vitesse de déplacement
    - Détection de fuites

SCADA : Pétrole et Gaz

- Raffinage
  - Distillation des différents produits hydrocarbonés
  - Contrôle automatique des températures de chauffe





SCADA : Pétrole et Gaz

- Distribution
  - Vente du produit final
  - Acheminé et vendu vers le client/utilisateur final
  - Multiples technologies utilisées
    - RFID
    - GPS
    - Transactions commerciales
    - Payement par carte bancaire
    - Système de communication satellite

Normes

Défenses sur SCADA

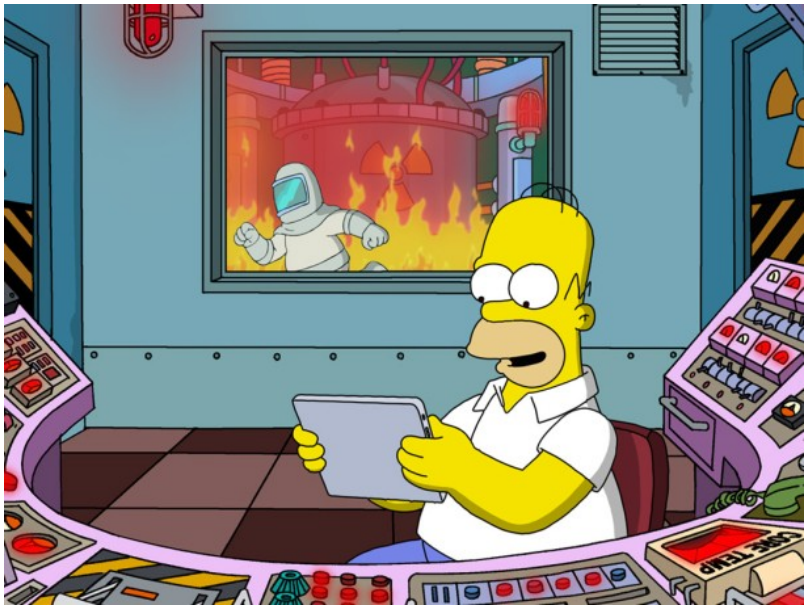
- Norme: NERC CIP (*Critical Infrastructure Protection*)
  - En version 4 – approuvée en avril 2012
    - CIP-002-4 *Critical Cyber Assets*
    - CIP-003-4 *Security Management Controls*
    - CIP-004-4 *Personnel and Training*
    - CIP-005-4 *Electronic Security*
    - CIP-006-4 *Physical Security*
    - CIP-007-4 *Systems Security Management*
    - CIP-008-4 *Incident Reporting and Response Planning*
    - CIP-009-4 *Recovery Plans*

Défenses sur SCADA

- Norme: NERC CIP (*Critical Infrastructure Protection*)
  - CIP-006-4 *Physical Security*
    - Contrôle d'accès physique
    - Droits d'accès
    - Traçabilité des accès
  - CIP-007-4 *Systems Security Management*
    - Prévention contre les logiciels malveillants
    - Gestion des patchs système
    - Règles de maintenances
    - Contrôles des services accessibles
    - Gestion des comptes utilisateurs (revu des comptes / complexité des mots de passe / etc.)

Défenses sur SCADA

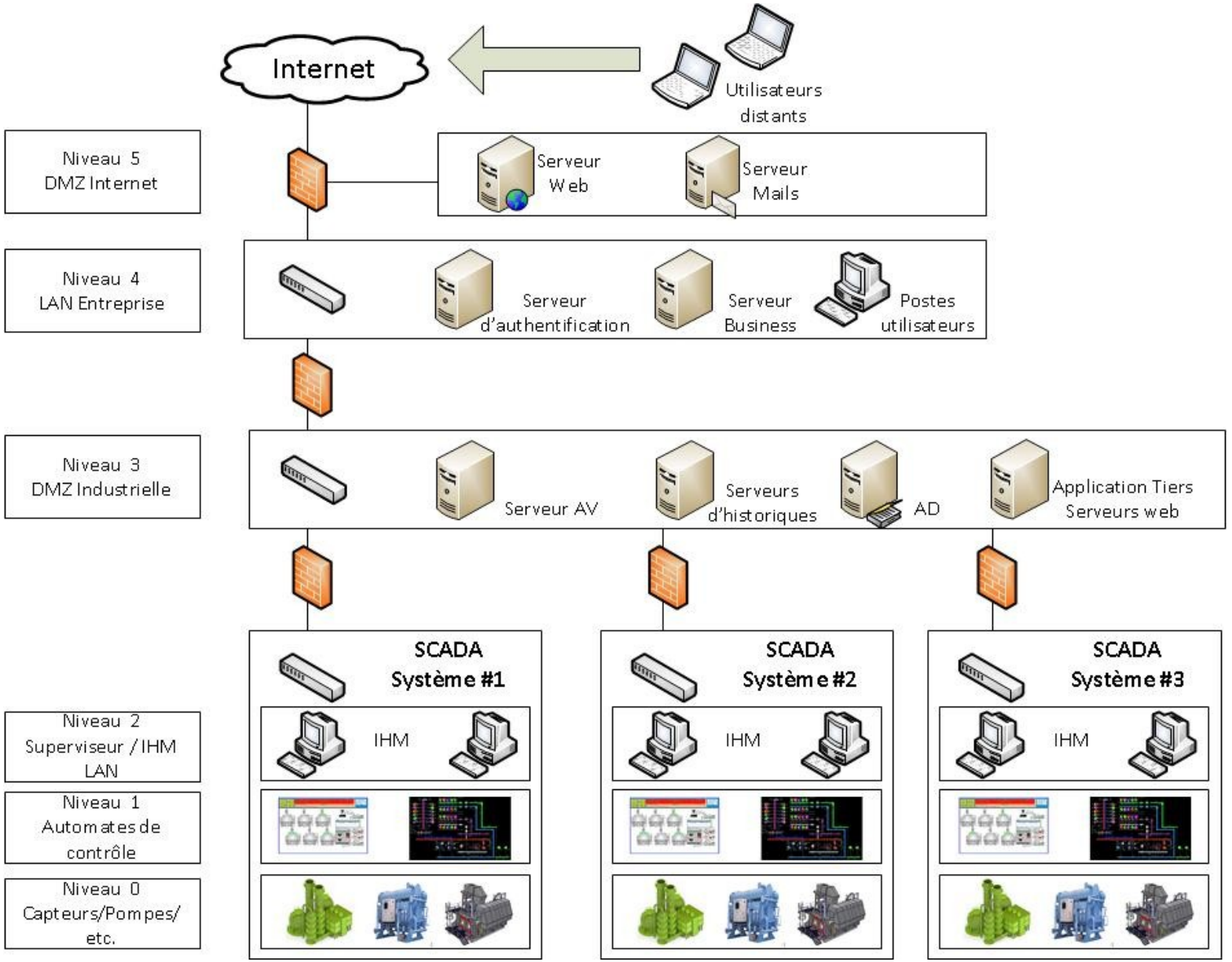
- Norme: NERC CIP – Exceptions (aux États-Unis)
  - Domaine du nucléaire
    - *Nuclear Regulatory Commission* (NRC)
      - Règles de sécurité supplémentaires
      - Préparations en cas d'urgences
      - Plans de communication



  - Domaines chimiques
    - *Chemical Facility Anti-Terrorism Standards* (CFATS)

Attaques SCADA

Attaques SCADA



Attaques SCADA – Points d'entrée

- Niveau 5 – Accès depuis Internet
  - Accès à distance (VPN) pour les utilisateurs et administrateurs
  - Serveurs SSH / FTP / Messagerie
  - Applications web
- Niveau 4 – LAN d'entreprise
  - Vulnérabilité au niveau des utilisateurs
    - Navigateur / plug-ins
    - Emails
    - Etc.
  - Souvent des accès aux IHM (Citrix / VNC / X11 / etc.)

Attaques SCADA – Points d'entrée

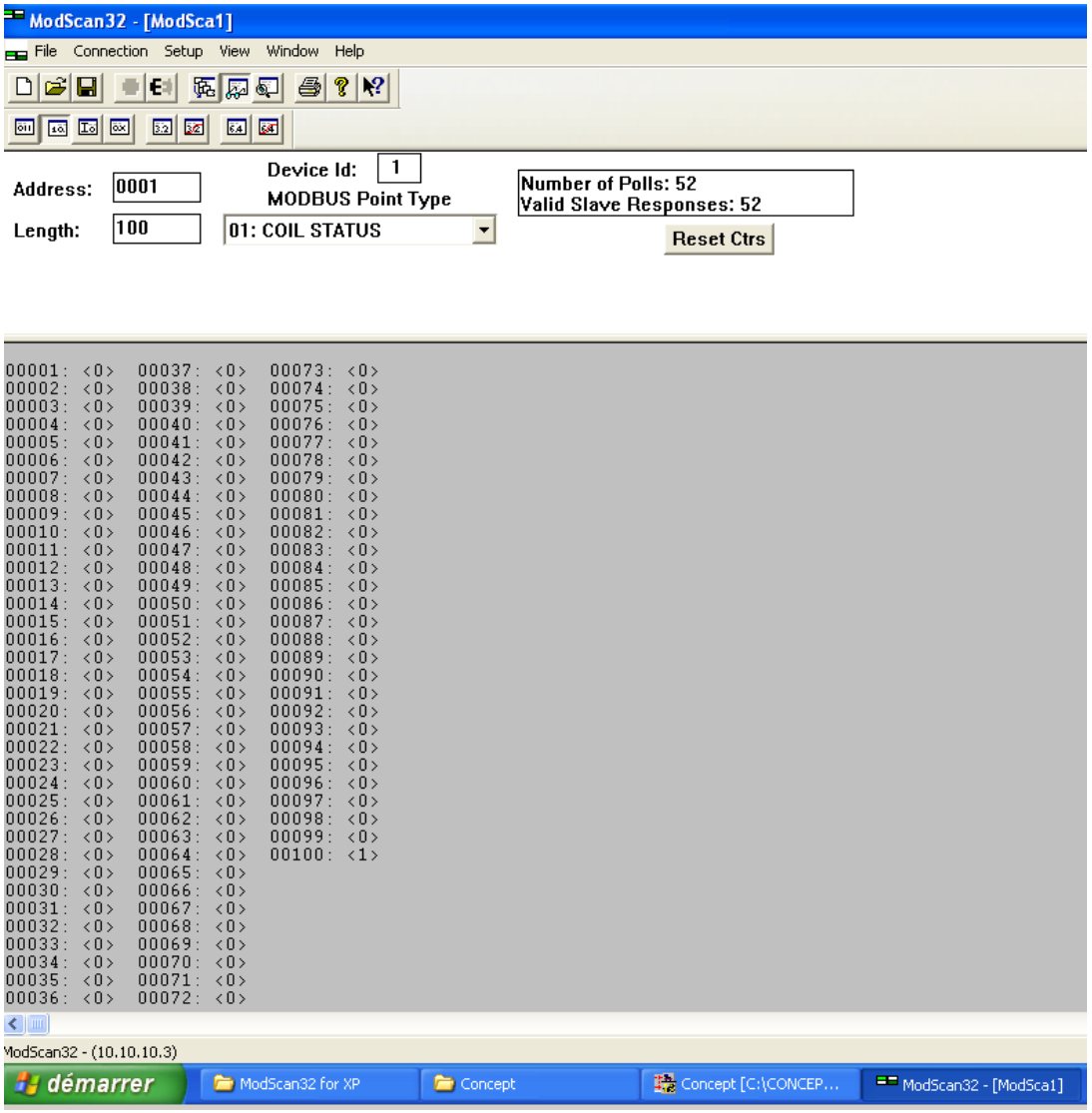
- Niveau 3 – DMZ « Industrielle »
  - Présence de ressources partages
    - AD / serveur d'authentification
    - Serveur de log
    - Centralisation de la surveillance du réseau industriel
    - Serveur de fichiers (commun)
- Niveau 2 – Superviseur / IHM
  - Environnement généralement privilégié pour
    - L'accès aux contrôleurs (lecture d'état / actions sur les automates)
  - Quelques fois connecté à Internet (support / astreintes / etc.)
  - Serveurs à la fois pour la programmation des contrôleurs et la maintenance

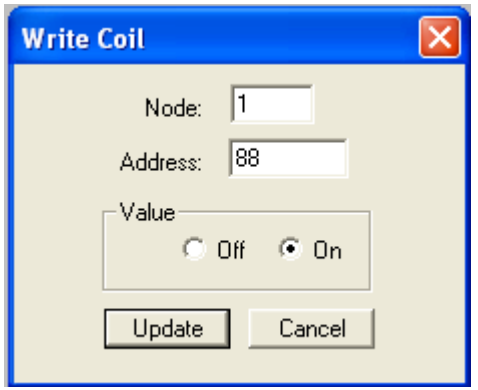
Attaques SCADA – Points d'entrée

- Niveau 1 - Équipement de contrôle
  - Faiblesse de protocoles de communication
  - Pas d'authentification / pas de chiffrement / rejeu possible / etc.
  - Pas/peu de validation des commandes reçues

Attaques SCADA – Protocoles

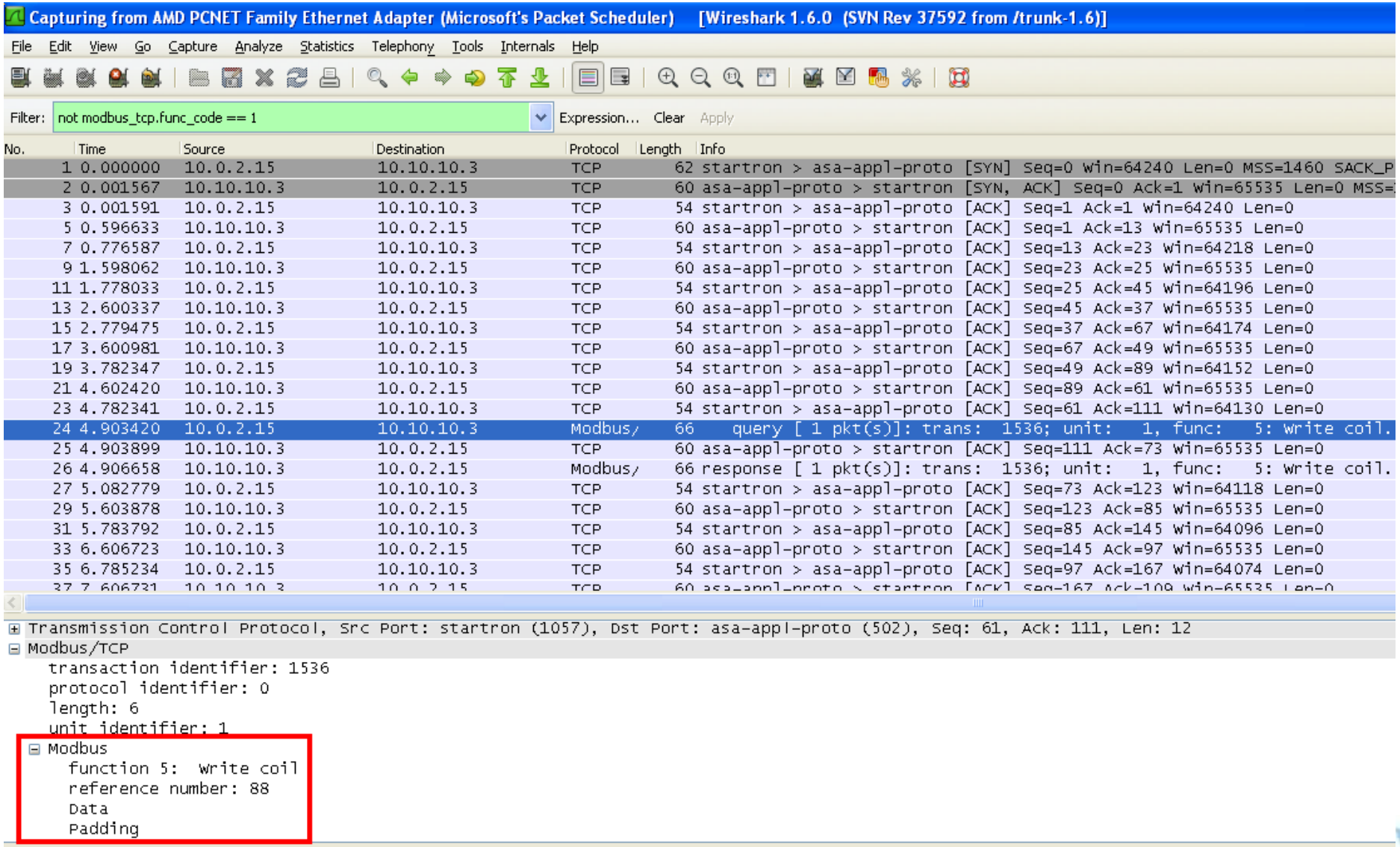
- Exemple avec ModBus





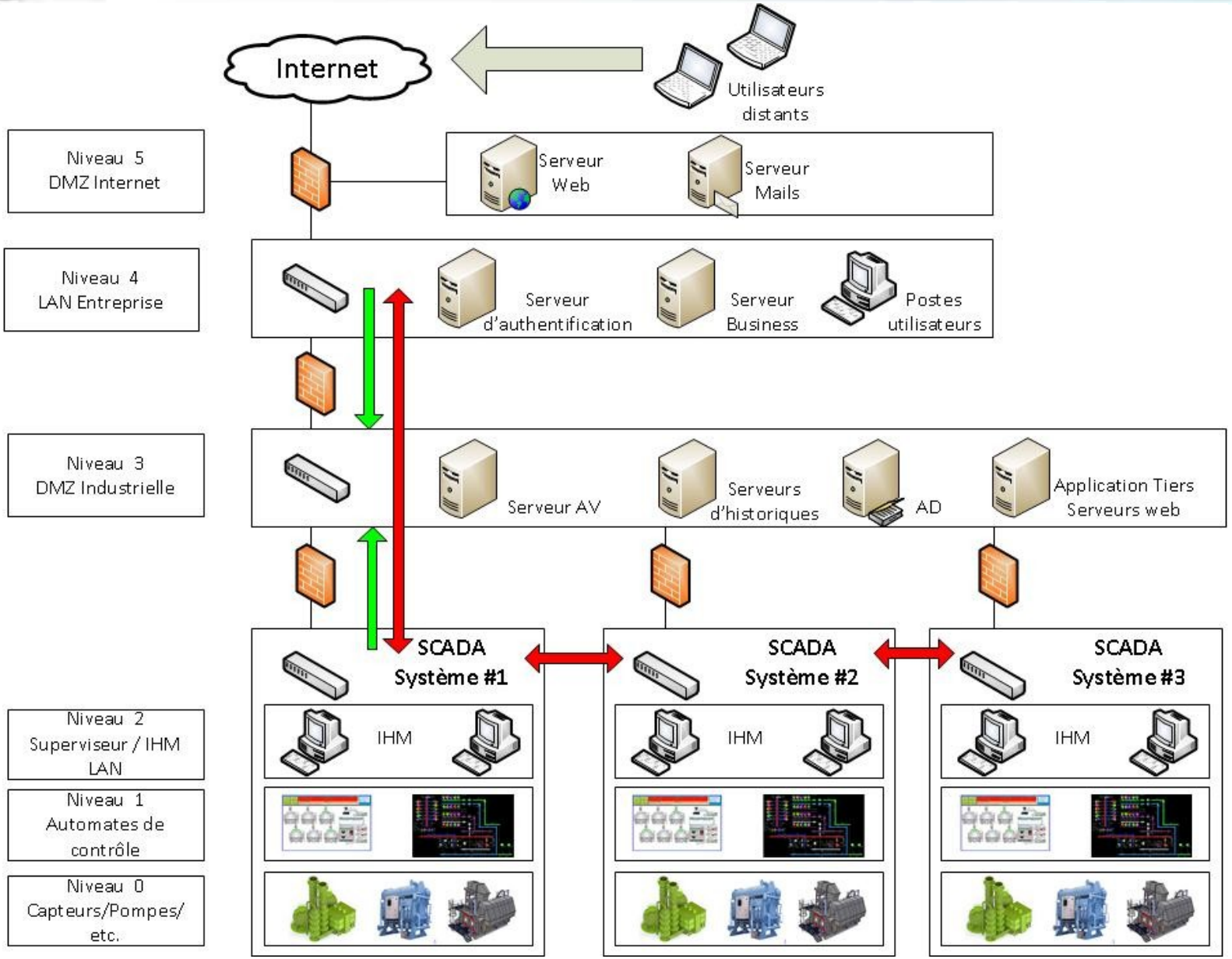
Attaques SCADA – Protocoles

- ModBus



Défenses SCADA

Défenses sur SCADA



Défenses sur SCADA

- Segmentation entre les différents niveaux
  - Distinction entre le réseau d'entreprise et le réseau industriel
  - Filtrage entre tous les niveaux / limiter aux seuls flux nécessaires
  - Utilisation de protocoles chiffrés et authentifiés
- Politiques de sécurité en générale
  - Politique de mot de passe
  - Politique d'accès (physique et logique)
  - Traçabilité
  - Mise à jour des systèmes / antivirus
  - Analyse des flux réseaux (IDS / IPS)

Merci de votre attention

Questions ?