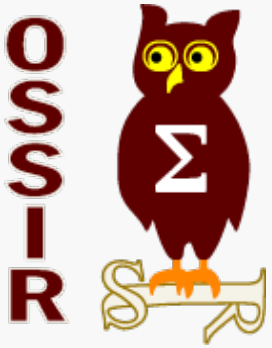
HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet



Sécurité des réseaux industriels Scadastrophe... ou pas

15 Mai 2012

Stéphane Milani <Stephane.Milani@hsc.fr>

Réseaux industriels / SCADA

- Wikipedia
  - 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
- Dans la pratique
  - Télécommande d'équipements industriels (vannes, pompes, moteurs, alarmes, etc.)
    - Processus industriels (plate-formes pétrolière / gaz, usines d'eau potable, stations d'épuration, barrages, écluses, domaine militaire, etc.)
- Évolution de réseaux industriels (bus de terrain) vers des réseaux informatique (Ethernet & TCP/IP)
  - Entraîne toute la problématique liée à la sécurité sur IP
  - Permet la connexion sur Internet (astreinte, maintenance, etc.)
- Population différente du monde informatique

Attaques récentes (Mars - Avril 2012)

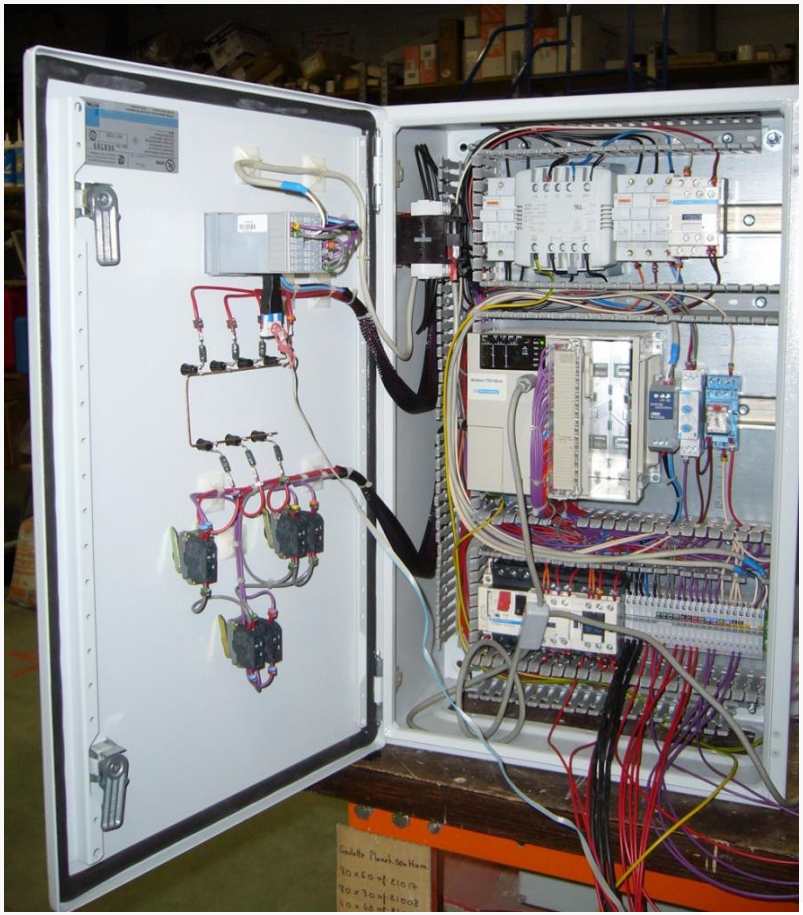
- Attaques sur les pipelines de gaz américains
  - Alertes de l'ICS-CERT du DHS
  - http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf
  - http://www.csmonitor.com/USA/2012/0505/Alert-Major-cyber-attack-aimed-at-natural-gas-pipeline-companies
  - A rapprocher de l'attaque de RSA Inc de Mars 2011 ?
- Attaque sur le réseau pétrolier iranien (control systems of Kharg Island - oil export terminal and Ministry of Petroleum)
  - http://www.guardian.co.uk/world/2012/apr/23/iranian-oil-ministry-cyber-attack
  - http://www.reuters.com/article/2012/04/23/us-iran-oil-cyber-idUSBRE83M0YX20120423

Composants essentiels

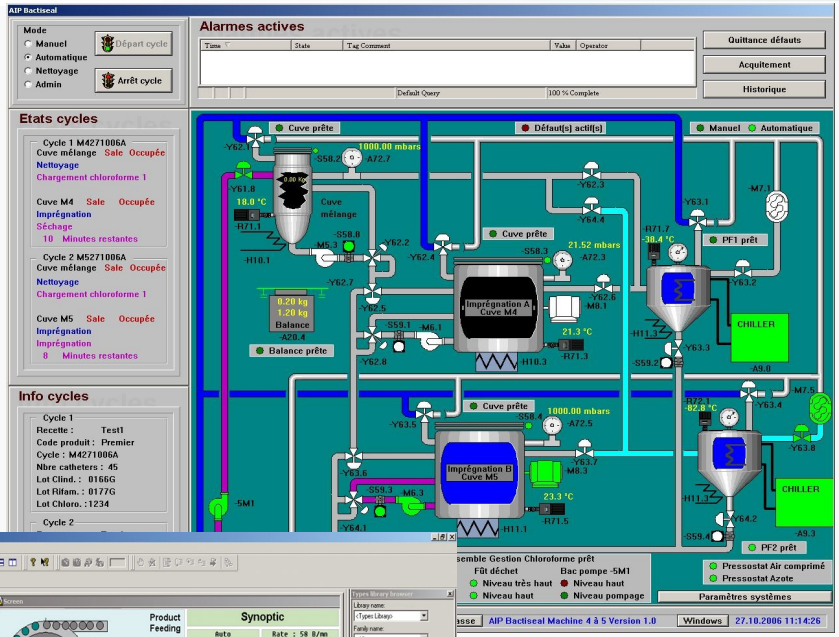
- Organes à commander - vannes, pompes, etc.
- Automates (PLC), boîtiers de télétransmission (RTU), systèmes de sûreté/sécurité (SIS)
- IHM (Interface Homme-Machine)
  - Supervision (WinCC, PC Win, PC Vue, etc.)
  - Programmation (Step7, PL7, Unity Pro, etc.)
- Transmission : protocoles Modbus, S7, IEC 104, CIP, DNP3

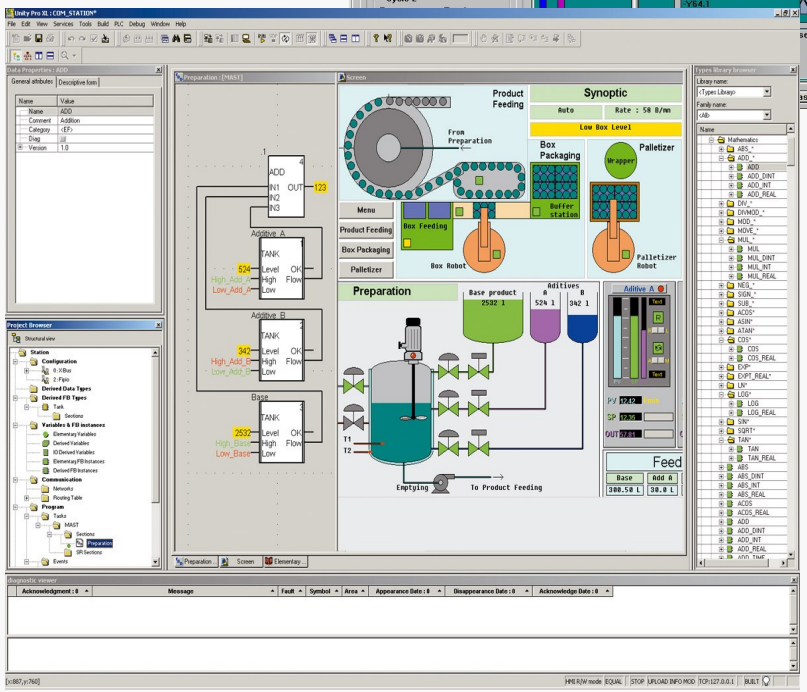
Vannes et automates

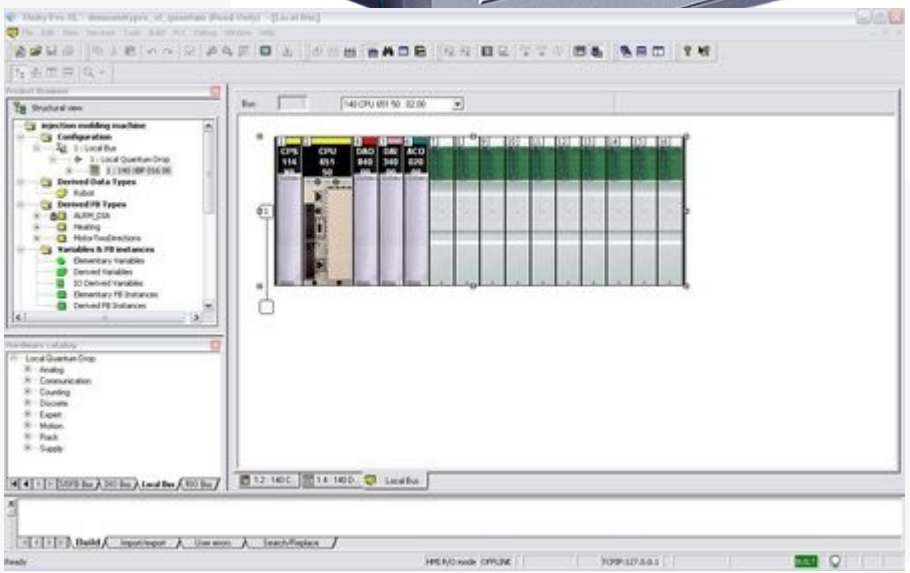
- Organes télécommandés
  - « Simple » dispositif mécanique lié à une commande électrique télécommandable)
- Automates
  - Schneider
  - Emerson
  - Siemens
  - Honeywell
  - Rockwell Automation / Allen-Bradley
  - Yokogawa
  - ABB
  - Wago
  - ...



IHM (Interface Homme-Machine)



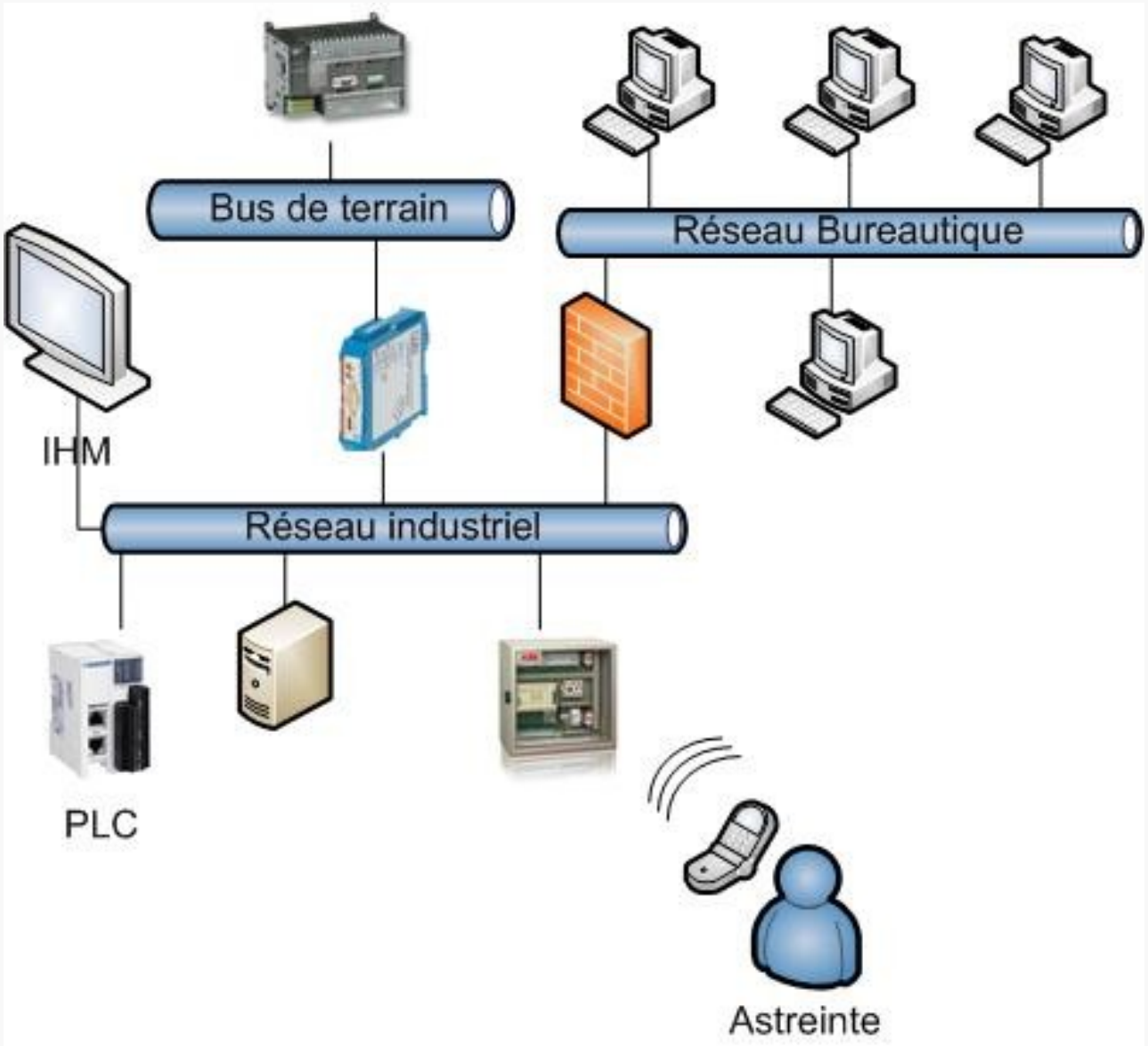




IHM (Interface Homme-Machine)

- Généralement des logiciels installés sur des postes Windows
  - OPC / DCOM / RPC
- 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)
- IHM de supervision
  - Contient un vue partielle ou complète sur l'état du réseau industriel
  - Permet d'envoyer des actions pré-programmées aux automates (arrêt/démarrage, etc.)
  - « Remplace » les «boutons physiques » locaux

Configuration courante - réseau



Protocoles

Protocole Modbus/TCP

- Caractéristiques
  - Spécifications publiques (http://www.modbus.org/specs.php)
  - Port TCP/502
  - Dialogue Maître / Esclave
  - Identifiant Esclave SID (de 1 à 247)
  - 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

Protocole IEC 104

- Ressemble à Modbus
- Caractéristiques
  - Port TCP/2404
  - Relation Maître / Esclave
  - Numéro d'ASDU (*Application Service Data Unit*)
    - de 1 à 65534
  - Pas d'authentification, ni chiffrement
  - Outil public *QTester104*
    - http://sourceforge.net/projects/qtester104/

Protocole S7

- Modbus like
- 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

Protocole EtherNet/IP CIP

- Caractéristiques
  - Ports TCP/44818, UDP/44818, UDP/2222
  - Pas d'authentification, ni chiffrement
  - Envoi de commandes
    - *STOPCPU*
    - *RESETETHER*
    - Etc.
      - *Crash / reboot* du périphérique
    - *ethernetip-multi.rb* is your friend... or foe
      - http://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/auxiliary/admin/scada/multi_cip_command.rb

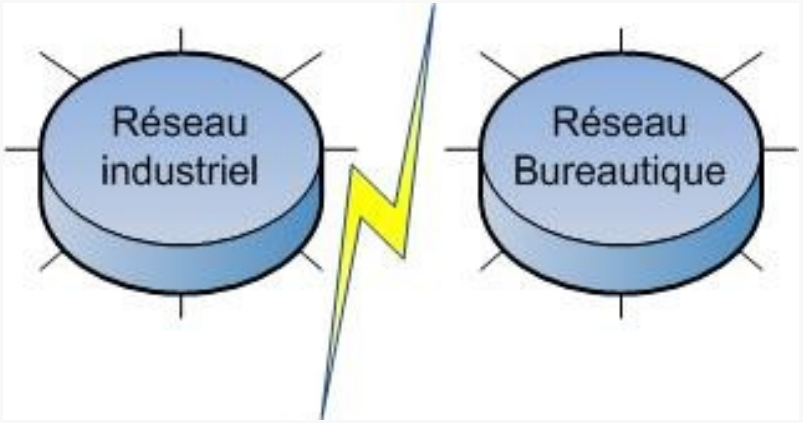
Protocole DNP3 (IEEE Std 1815)

- Caractéristiques
  - http://www.dnp.org/
  - Protocole ouvert
  - 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
    - Chiffrement / Authentification mutuelle
      - HMAC / TLS
      - IEC 62351-5 compliant
        - Data and Communication Security

Sécurité ?

Architecture

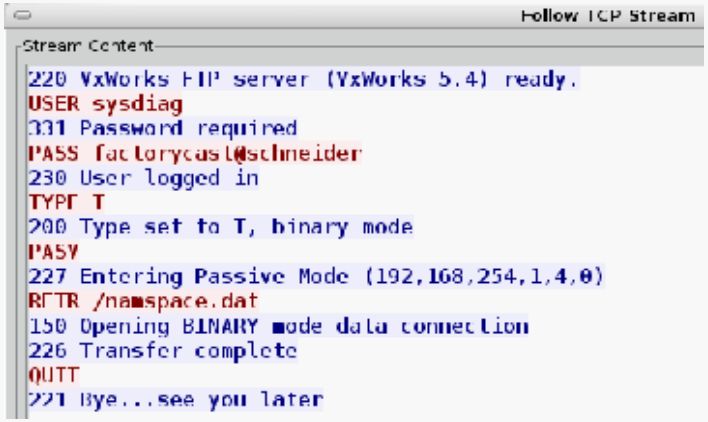
- Architecture souhaitée



- 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)

Automates PLC : exemple Schneider

- Plusieurs ports ouverts
  - 21/TCP, 23/TCP, 80/TCP, 502/TCP, 1864/TCP, 4443/TCP, 5190/TCP, 5566/TCP
- Mots de passe codés en dur
  - Dans le code Java
  - Requête FTP
    - Récupération de *namspace.dat*, *index.gdt*
  - Compte *sysdiag*
    - Permet de se connecter à l 'équipement pour
      - Récupérer les comptes/mot de passe applicatifs (en clair)
        - Fichier *password.rde*, etc.
      - Récupérer/modifier le firmware
      - Extraction de l'arborescence
- Backdoors ? Cf travaux de Rubén « reversemode » Santamarta



Automates

- Les autres marques / modèles sont sensibles aux mêmes types de vulnérabilités
  - Ont généralement des ports ouverts
    - FTP pour la modification du *firmware*
      - mises à jour de fonctionnalité, pas de sécurité
    - Telnet
    - Web (Possibilité d'avoir une mini IHM)
    - Modbus, etc.
    - SNMP

```
webPassword OBJECT-TYPE
    SYNTAX  INTEGER   {
                disabled(1),          -- Password disabled
                enabled(2)            -- Password enabled
              }

    ACCESS  read-write
    STATUS  mandatory
    DESCRIPTION
            "A switch to enable or disable the use of Web passwords:
             disabled(1),          -- Password disabled
             enabled(2)            -- Password enabled
```

Automates

- Plantages
  - *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 ô_O
- Nécessite un reboot manuel

Failles impactant les IHM

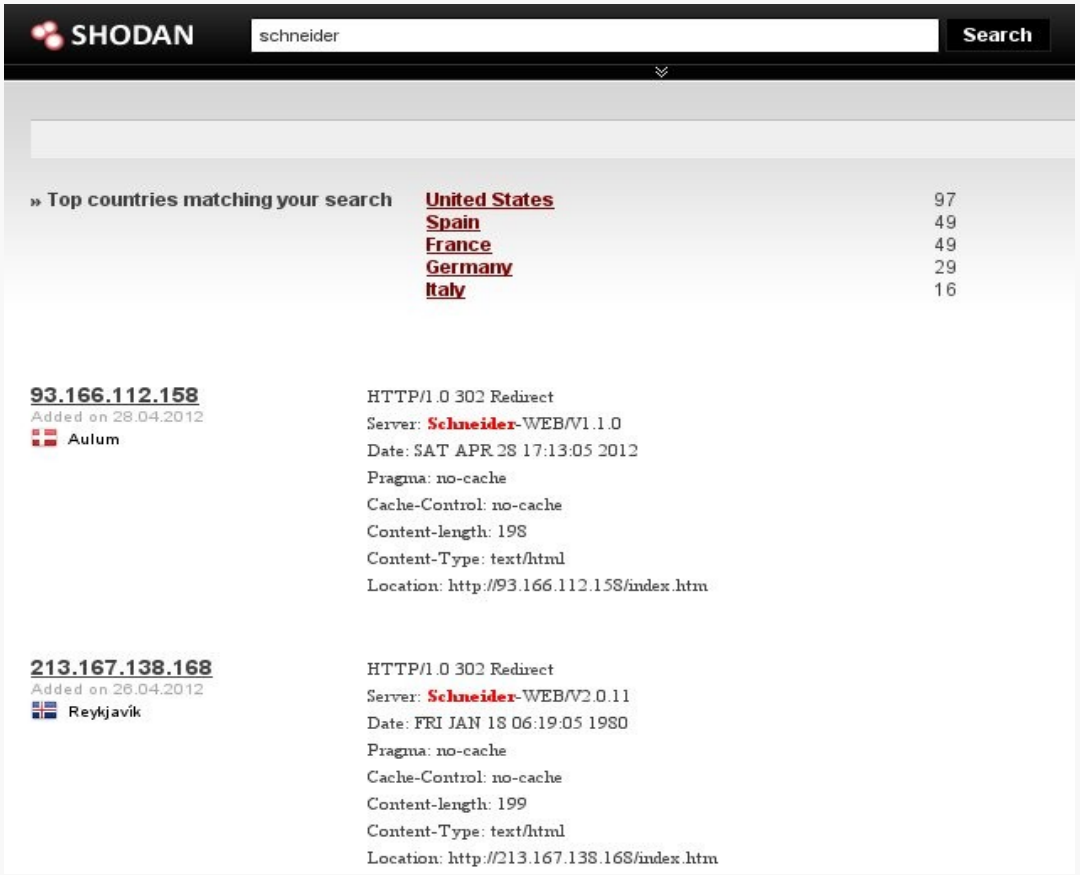
- Stuxnet & WinCC/Step7
  - Mot de passe par défaut sur le SGBD
- Vulnérabilités
  - *Samsung Data Management*
    - Injection SQL , contournement de l'authentification
  - *PC-Vue, CoDeSys, RealWin, etc.*
    - buffer overflow, etc.
  - *BroadWin WebAccess*
    - Exécution de code à distance
  - Etc.
- Systèmes Windows généralement pas à jour

Sans fil ?

- Wi-Fi
  - Dans les salles de supervision ?
  - 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.)
    - Etc.

Moteurs de recherche

- Équipements normalement présents qu'en interne
  - Pas accessible depuis Internet ?
- Moteurs de recherche
  - Shodan
  - Eripp



Sûreté vs sécurité

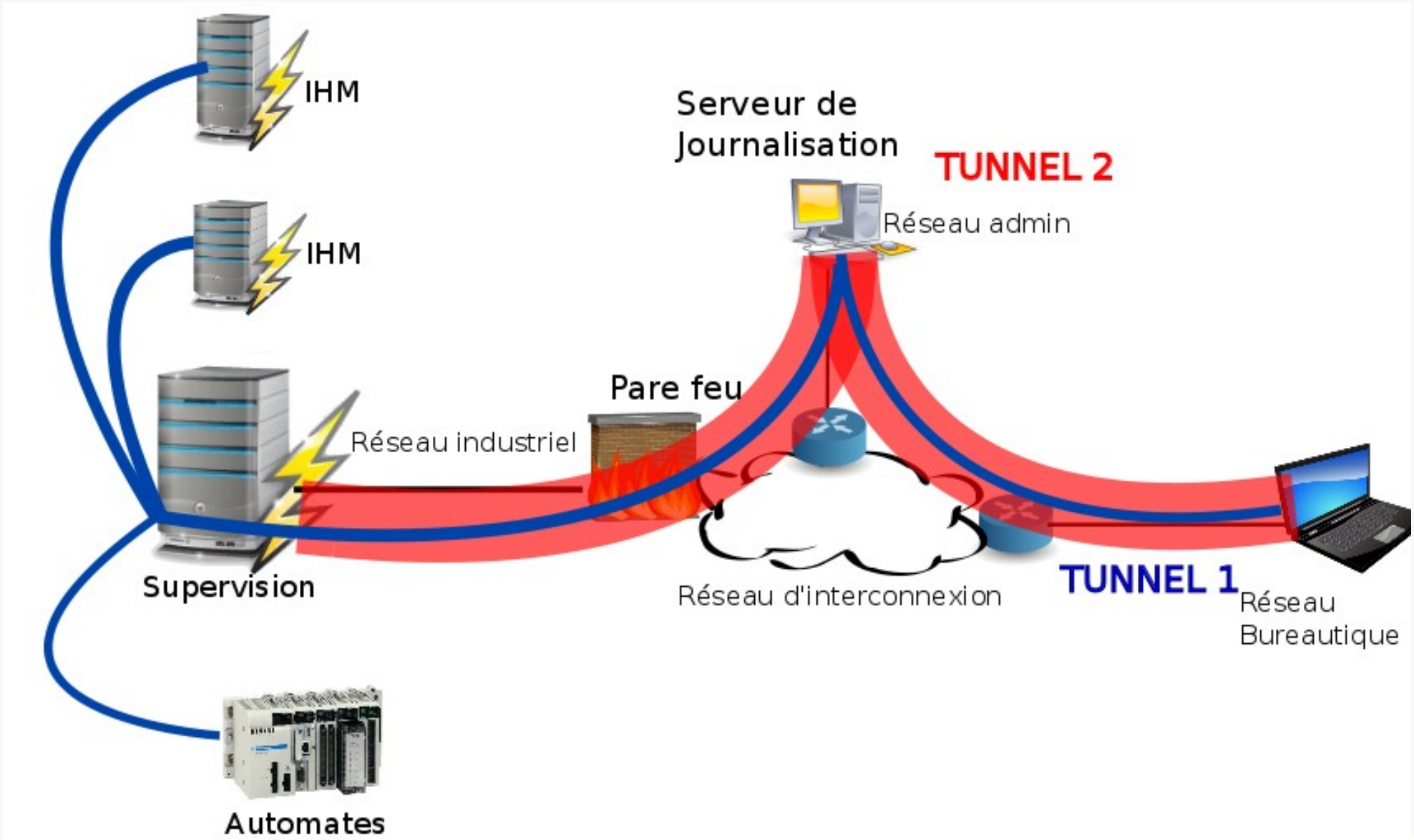
- Sûreté vs sécurité : fonctionnement 24/24, 7/7, 365j/an
  - Pas d'antivirus (cela empêche le bon fonctionnement, ralentissement)
  - Pas de mise a jour (ça va plus marcher)
  - Tout est basé sur la sûreté : des vies sont en jeu
  - Pas de veille techno (sauf pour les nouvelles fonctionnalités)
  - Sécurité = sécurité physique
  - Problème de l'astreinte et des accès distant
- 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 sensibilisées à des risques informatiques : ver/virus, accès externes

Retours d’expérience
Accès au réseau industriel

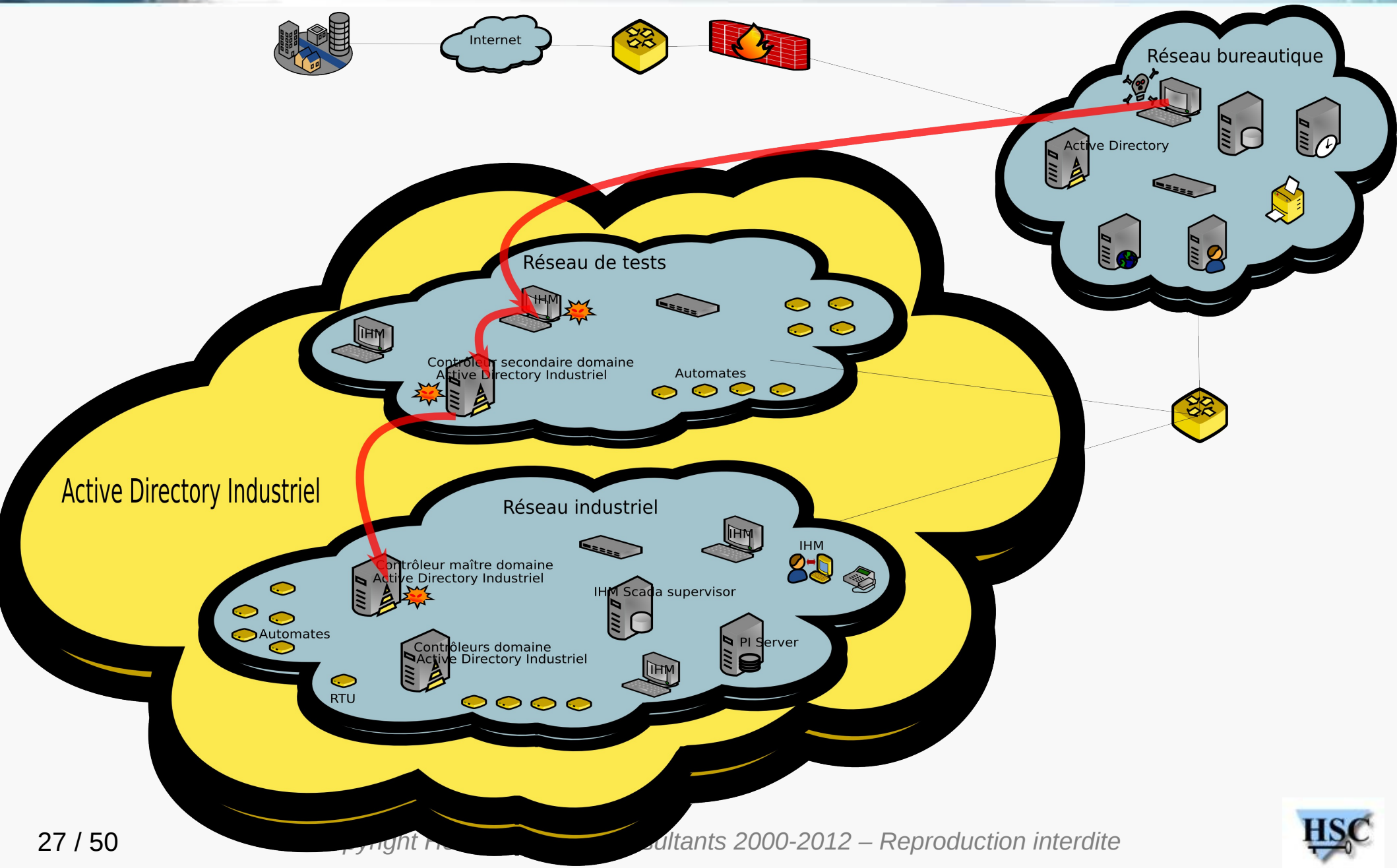
Tests depuis un réseau industriel

- 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

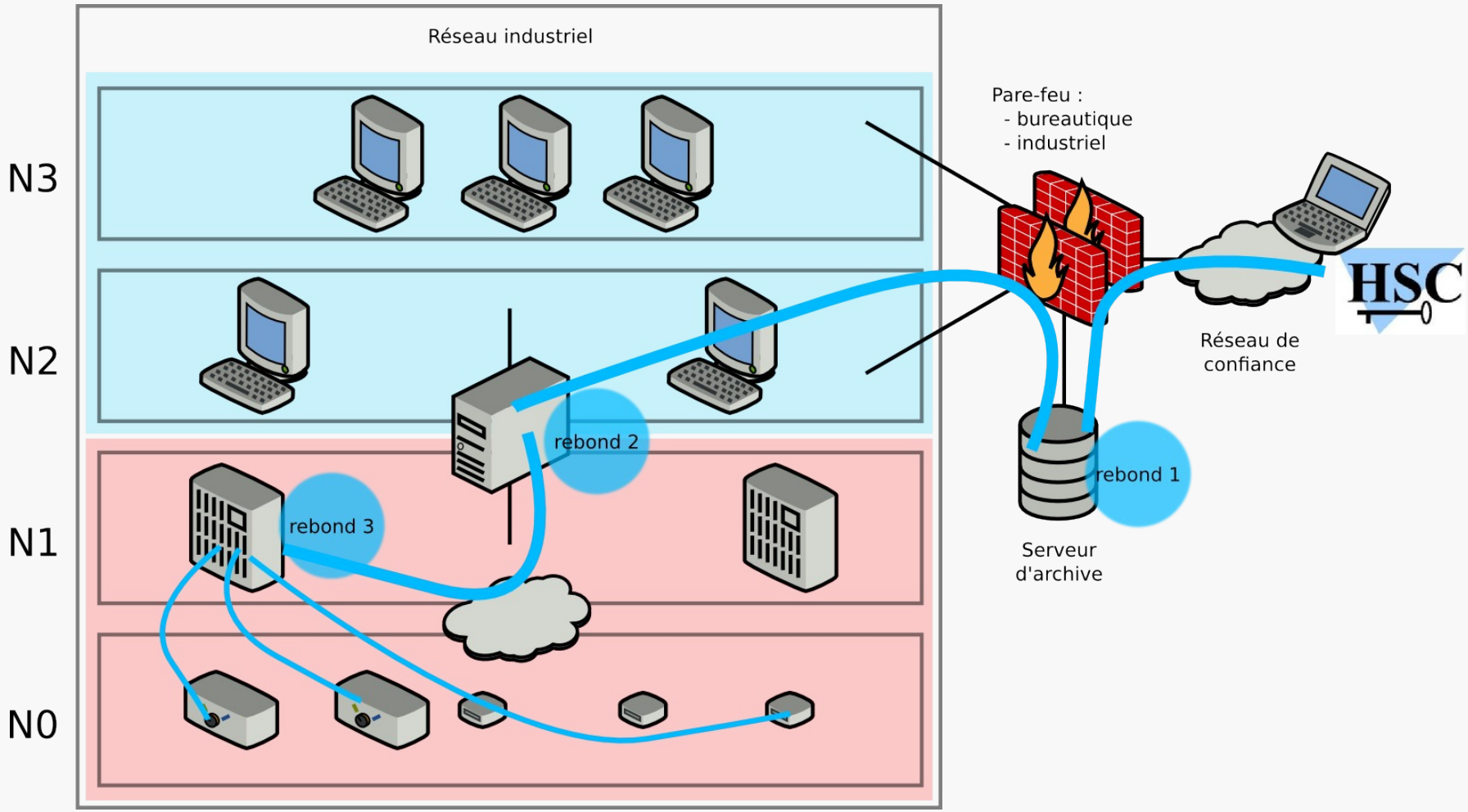
Intrusion depuis un réseau Bureautique



Intrusion depuis un réseau Bureautique



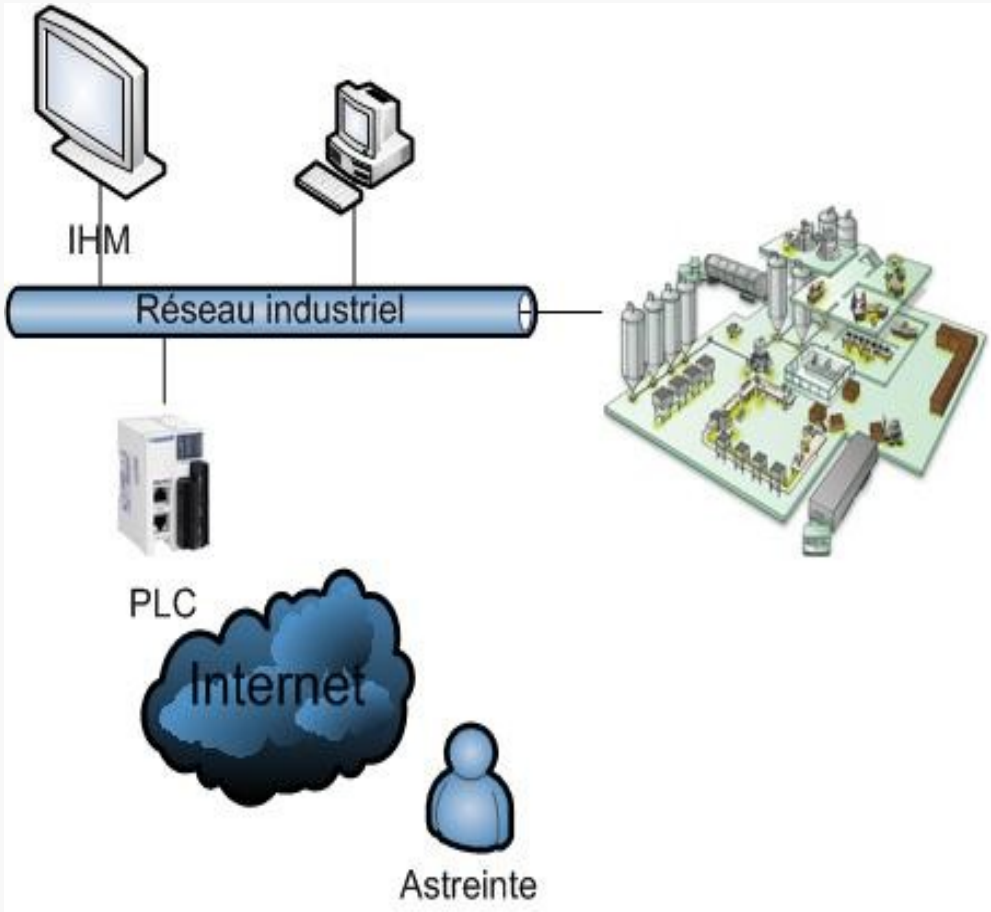
Intrusion depuis un réseau Bureautique

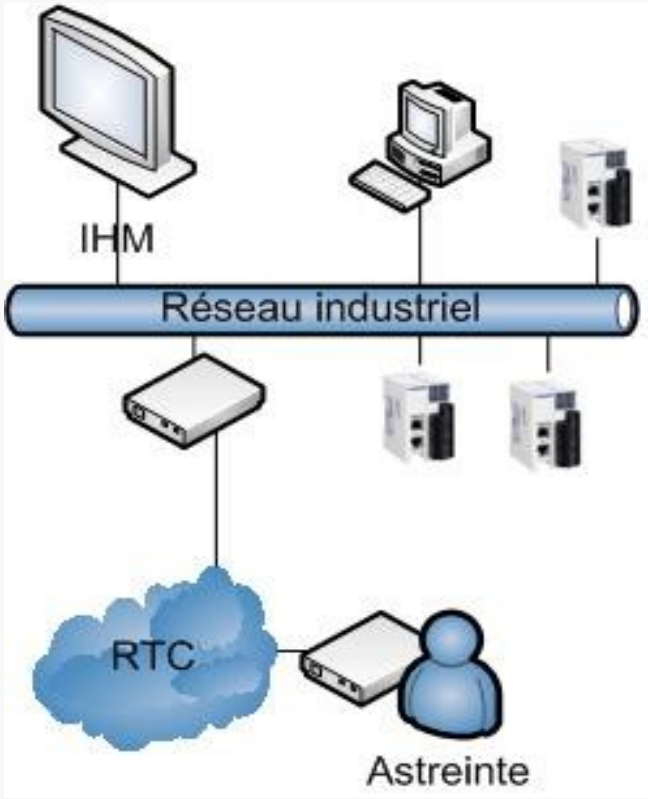


Usines isolées - Accès distants

- Certaines prestations ont montré
  - Automates accessibles sur Internet (directement en Modbus/TCP)
    - 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

Usines isolées - Accès distants





Autres exemples

Attaques ciblées / APT / Ver / Virus

- Compromission du réseau bureautique
  - via *Spear phishing* (fichiers .pdf | .rtf | .xls | .doc | etc. malfaisants)
  - ou via un serveur Web (puis rebond sur le réseau bureautique)
  - Nécessite de pouvoir passer d'un réseau bureautique à un réseau industriel

- Stuxnet, etc.
  - Insertion d'une clé USB directement sur une machine du réseau industriel

Quid des petites infrastructures ?

- Sites ayant des équipements sur Internet
  - Piscines
  - Golfs
  - Écoles
  - Chaufferies
  - STEP
  - Écluses
  - Éoliennes ?
  - Etc.

IP	DNS	Title	Found
93.17.80.135	135.80.17-93.rev.gaoland.net	401 Not Authorized - [redacted] marthe corneille	1 year ago
93.17.79.241	241.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted]	1 year ago
93.17.80.1	1.80.17-93.rev.gaoland.net	401 Not Authorized - [redacted] HAMMEAU DES BROUETTE	1 year ago
93.20.219.188	188.219.20-93.rev.gaoland.net	401 Not Authorized - [redacted] COTONNIER	1 year ago
93.17.94.122	122.94.17-93.rev.gaoland.net	401 Not Authorized - [redacted] RONSARD	1 year ago
93.17.79.192	192.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted] SEV Jardin des plantes	1 year ago
93.17.73.95	95.73.17-93.rev.gaoland.net	401 Not Authorized - [redacted] Gymnase Grieu	1 year ago
93.20.219.187	187.219.20-93.rev.gaoland.net	401 Not Authorized - [redacted] GYMNASE PELISSIER	1 year ago
93.17.79.231	231.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted] CRECHE PIERRE DE LUNE	1 year ago
93.17.79.229	229.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted] ANATOLE FRANCE 2	1 year ago
93.17.79.225	225.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted]	1 year ago
93.17.79.228	228.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted] Anatole France 1 Synco	1 year ago
93.17.79.227	227.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted] ECOLE ANDRE POTTIER	1 year ago
93.17.79.233	233.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted] Piscine Boulingrin	1 year ago
93.17.79.187	187.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted] PEPINIERE ST JULIEN	1 year ago
93.20.219.189	189.219.20-93.rev.gaoland.net	401 Not Authorized - [redacted] PISCINE DIDEROT	1 year ago
93.17.79.193	193.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted] ECOLE LOUIS PASTEUR	1 year ago
93.17.79.194	194.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted] Gymnase dev	1 year ago
93.17.79.151	151.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted] Ecole Guillaume	1 year ago
93.17.79.166	166.79.17-93.rev.gaoland.net	401 Not Authorized - [redacted] Jean Mulot	1 year ago

- Beaucoup de lignes ADSL *.abo.wanadoo.fr*, *rev.gaoland.net*, etc.
  - A qui appartiennent-elles vraiment ?

iPhone / Android / BlackBerry

- Pilote ta centrale avec ton smartphone

- Application lancée via un VPN ?

Radio / Capteurs

- Installation distante, problème de câblage
  - Utilisation de liens radio (*VHF* / *UHF* / *microwave*, etc.)
  - Possibilité d'utiliser du chiffrement mais rarement activé
  - Nécessite du matériel spécifique
- Capteurs extérieurs
  - Connectés via réseau IP
  - Problème de l'accès physique au capteur et surveillance
  - Accès au réseau industriel

Etude d'un boîtier de télétransmission (RTU)

Boîtiers de télétransmission (RTU)

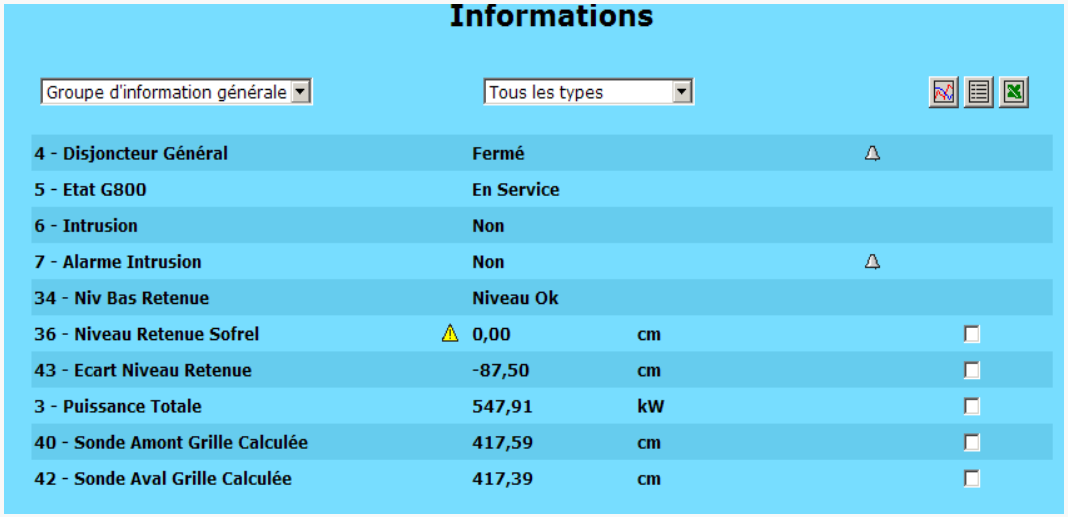
- Pourquoi s'y intéresser ?
  - Boîtiers généralement accessibles depuis l’extérieur
    - GSM, RTC, Internet, …
  - Utiliser par l'astreinte pour obtenir des informations sur l'état des équipements
  - Peut être utilisé pour piloter les équipements
  - Modbus parfois accessible
- Comment les découvrir ?
  - Shodan / Eripp
  - Scan sur Modbus
  - *Wardialing*

Étude de la sécurité d'un RTU

- Boîtiers fortement utilisés en Europe et en France
- Ports ouverts par défaut
  - HTTP
  - FTP
  - Modbus
- Accès restreint par login
  - Pas de mot de passe
  - 4 niveaux d'accès selon le login
  - Logins par défaut très simples
  - Même login pour HTTP et FTP

HTTP RTU

- Serveur HTTP – selon le niveau du login utilisé
  - Permet la visualisation des remontées d'alarmes
  - Permet de lancer des actions si pré-programmées
  - Permet de découvrir des informations
    - architecture, numéros de téléphone d'astreinte, etc.
  - Permet de réinitialiser le configuration



Serveur FTP

- Serveur FTP – selon le niveau du login utilisé
  - Contient la configuration logicielle et industrielle
    - La configuration logicielle contient les mots de passe en clair ...
  - Permet la récupération du Firmware
  - Permet la récupération des journaux
  - Contient la configuration matérielle
- Le serveur FTP est utilisé par l'IHM pour mettre à jour la configuration du boîtier
  - Les configurations sont poussées puis activées
    - Configuration réseau, mots de passe
    - Configuration propre au réseau industriel
      - Accès Modbus, entrées/sorties, ...
  - Le Firmware peut être mis à jour

Firmware

- Reverse du Firmware
  - Contient le système de fichiers
  - OS temps réel propriétaire (*pSOS+*)
  - Architecture *PowerPC*
  - A priori pas de mot de passe stocké en clair (sauf mot de passe par défaut du niveau max mais surchargé dès qu'on le modifie)
- Capacité réseau (très) intéressante
  - Possibilité de le configurer en VPN pour accéder à distance
  - Possibilité de l'utiliser comme routeur
    - Peut donner l'accès au réseau industriel
- Possibilité de modifier le firmware
  - Long à faire (OS propriétaire)
    - Mais la nouvelle version sera basée sur un noyau Linux

Quelques Solutions

Pistes...

- Indispensable : **Défense en profondeur / Cloisonnement réseau**
  - Interdire l'accès au réseau industriel
    - Mise en place d'une DMZ interne
    - Filtrage réseau
      - En entrée du réseau industriel
      - Mais également en sortie !
  - Plusieurs niveaux / zones
    - Ex : niv 0 : capteurs/pompes, niv 1 : automates, niv 2 : serveurs et postes de supervision, niv 3 : postes supervision / archivages / logs
  - Contrôler les accès distants
    - VPN
    - Interdire **impérativement** les IHM / automates connectés sur Internet
  - Utiliser le chiffrement sur les accès réseau

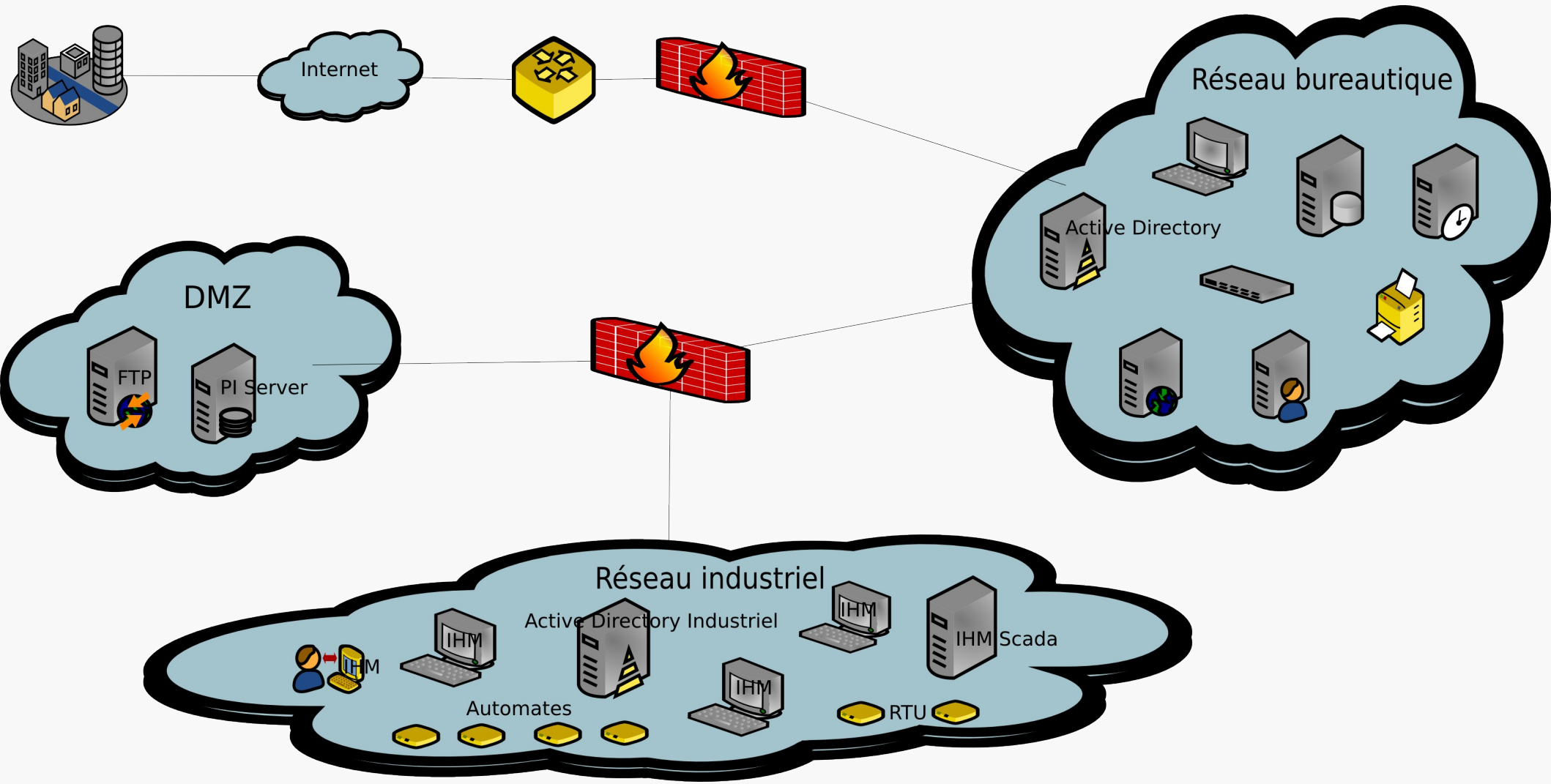
Pistes...

- Politique de mots de passe sur tous les noeuds
  - Serveurs, équipements réseau, automates, modems, etc.
  - Eviter au maximum les mots de passe administrateurs connus et partagés par 100 personnes
    - Essayer de respecter le principe du moindre privilège
- 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, etc.
  - *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 ?

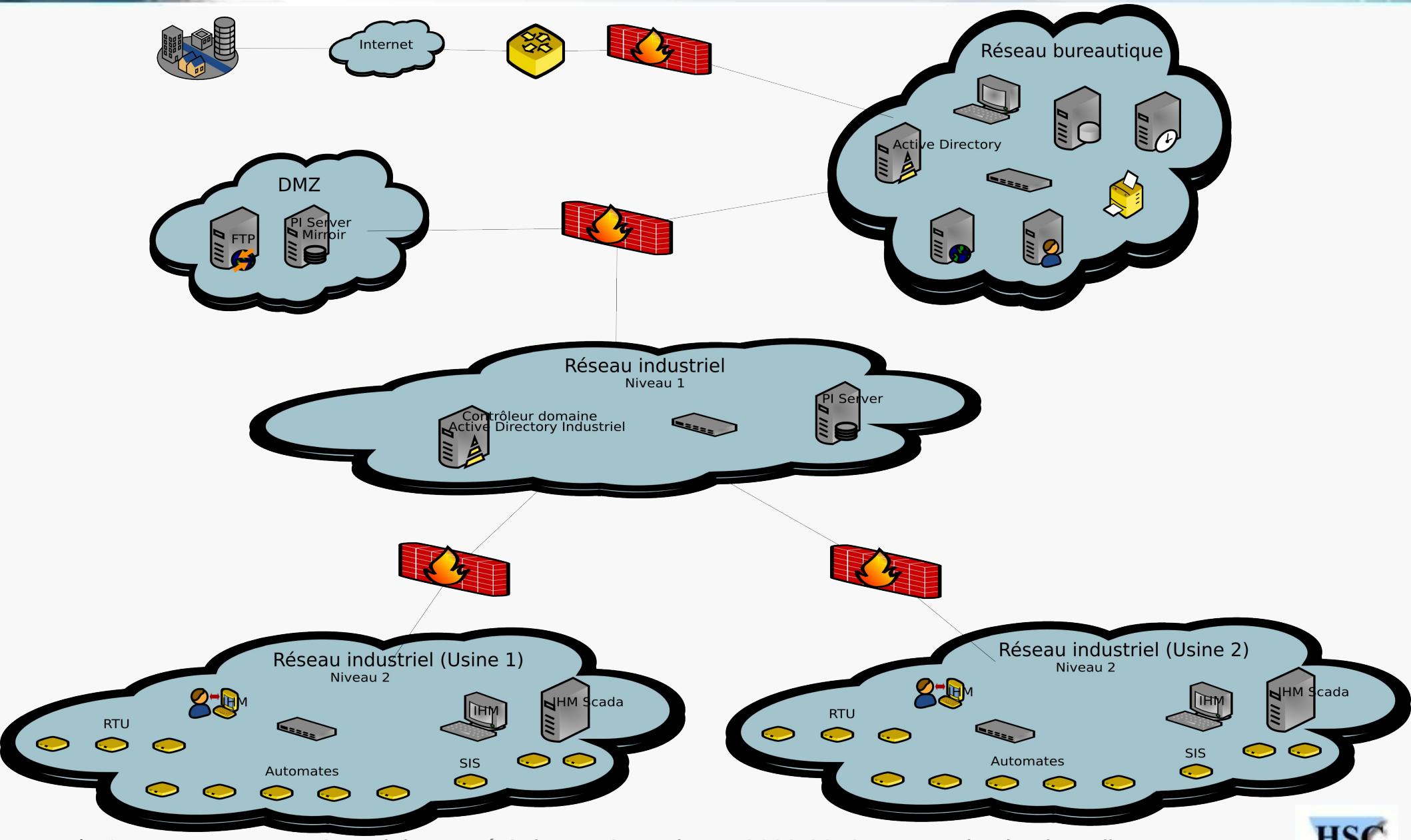
Pistes...

- 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 l'automate
  - 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.

Quelques solutions



Quelques solutions



Docs / Standards / Normes utiles US

- DHS / US-CERT *Defense in Depth*
  - http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf
- SP800-82 *Guide to Industrial Control Systems Security*
  - http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
- IEC 62443 (anciennement ISA 99.03)
  - *Network and system security for industrial-process measurement and control*
- IEC 61511
  - *Functional safety - Safety instrumented systems for the process industry sector*
- IAEA *Computer Security at Nuclear Facilities*
  - http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

Docs / Recommandations ENISA Europe

- *Protecting Industrial Control Systems. Recommendations for Europe and Member States*
  - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states
    - *Protecting Industrial Control Systems Annex I, Annex II, Annex III, Annex IV, Annex V, Annex VI*
- *Protecting Industrial Control Systems. Recommendations for Europe and Member States. Executive Summary in French*
  - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/executive_summary_fr

Merci :-)

Questions ?

Contact : Stéphane Milani <Stephane.Milani@hsc.fr>