



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>

- 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)



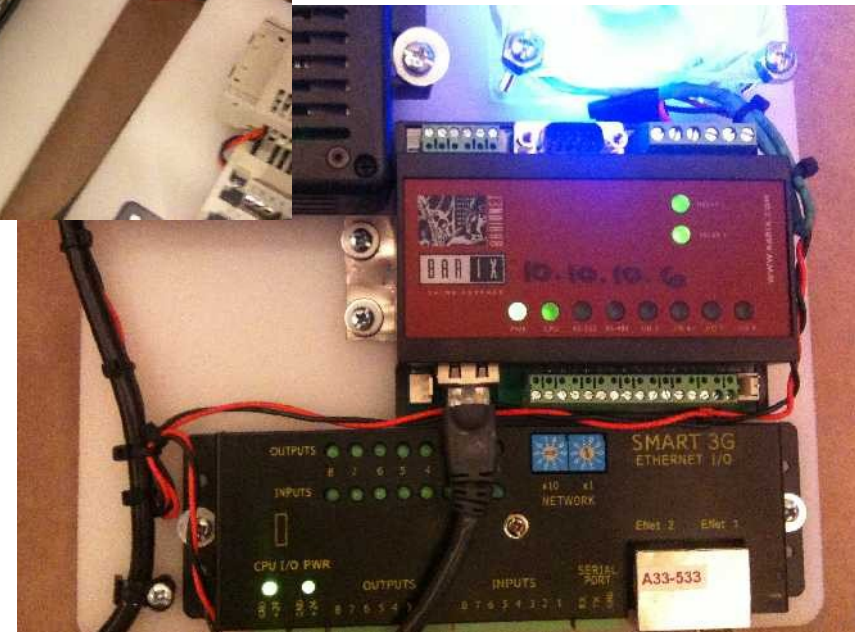
- Jonathan Pollet

→ Red Tiger Security – Fondateur et consultant principal



- 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

- Quelques démonstrations et utilisations d'outils



Introduction et Définitions

- **Systemes**
 - **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...**

- Composants SCADA
 - **PLC** (*Programmable Logic Controller*)
 - **RTU** (*Remote Terminal Unit*)
 - **IED** (*Intelligent 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



- 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

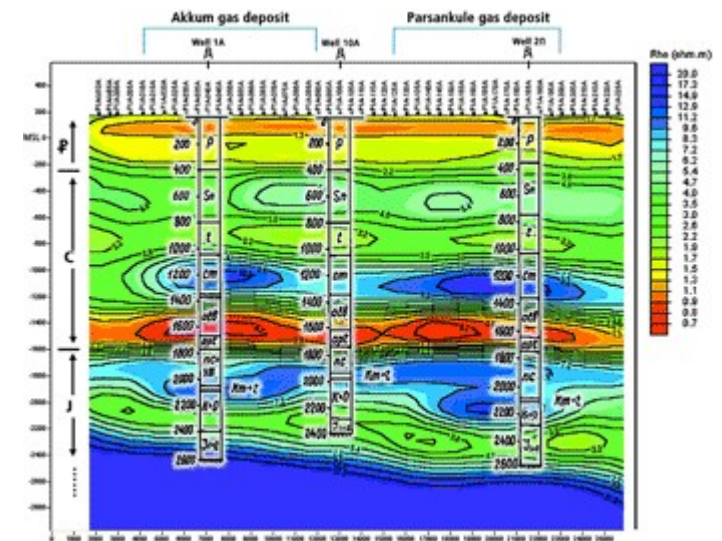
- **Protocoles de communication**

- 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

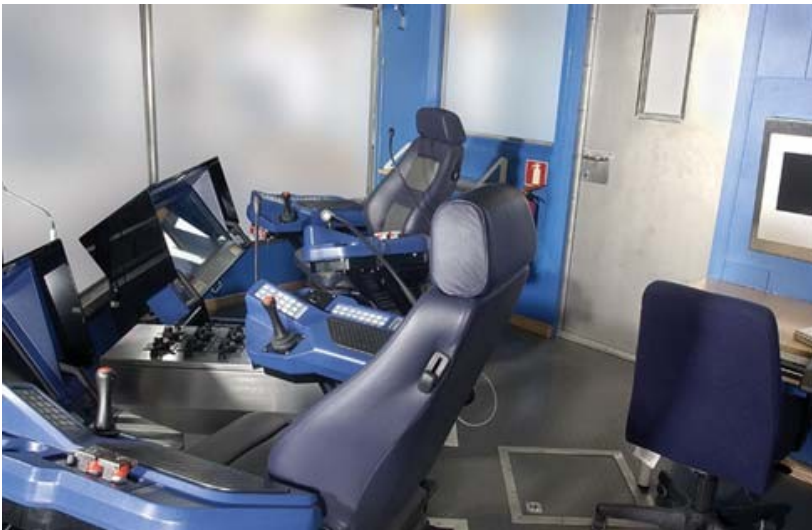
SCADA par l'exemple

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

- 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



- 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



- Production
 - Stockage et contrôle des fluides avant leur transport

Le gaz est utilisé sur place et/ou vendu

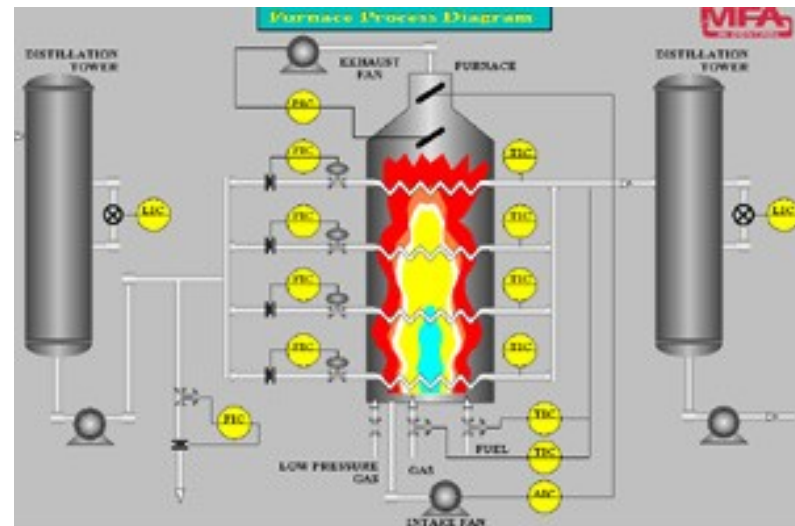
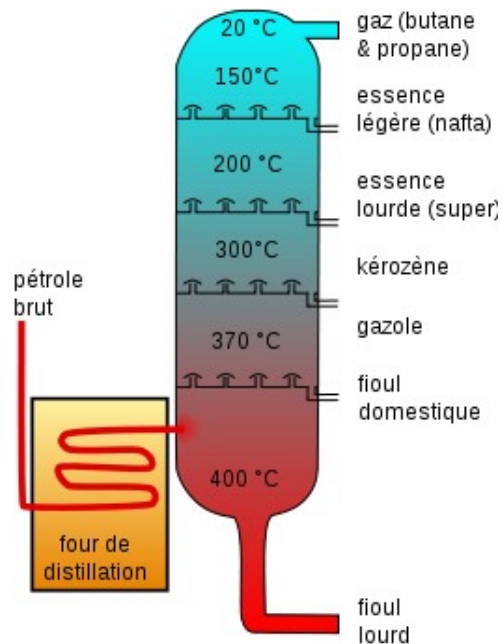


Le pétrole brute avec moins de 3% d'impuretés est mesuré et vendu

- 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



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



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

Normes

- 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*

- 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 patches système
 - Règles de maintenances
 - Contrôles des services accessibles
 - Gestion des comptes utilisateurs (revu des comptes / complexité des mots de passe / etc.)

- 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

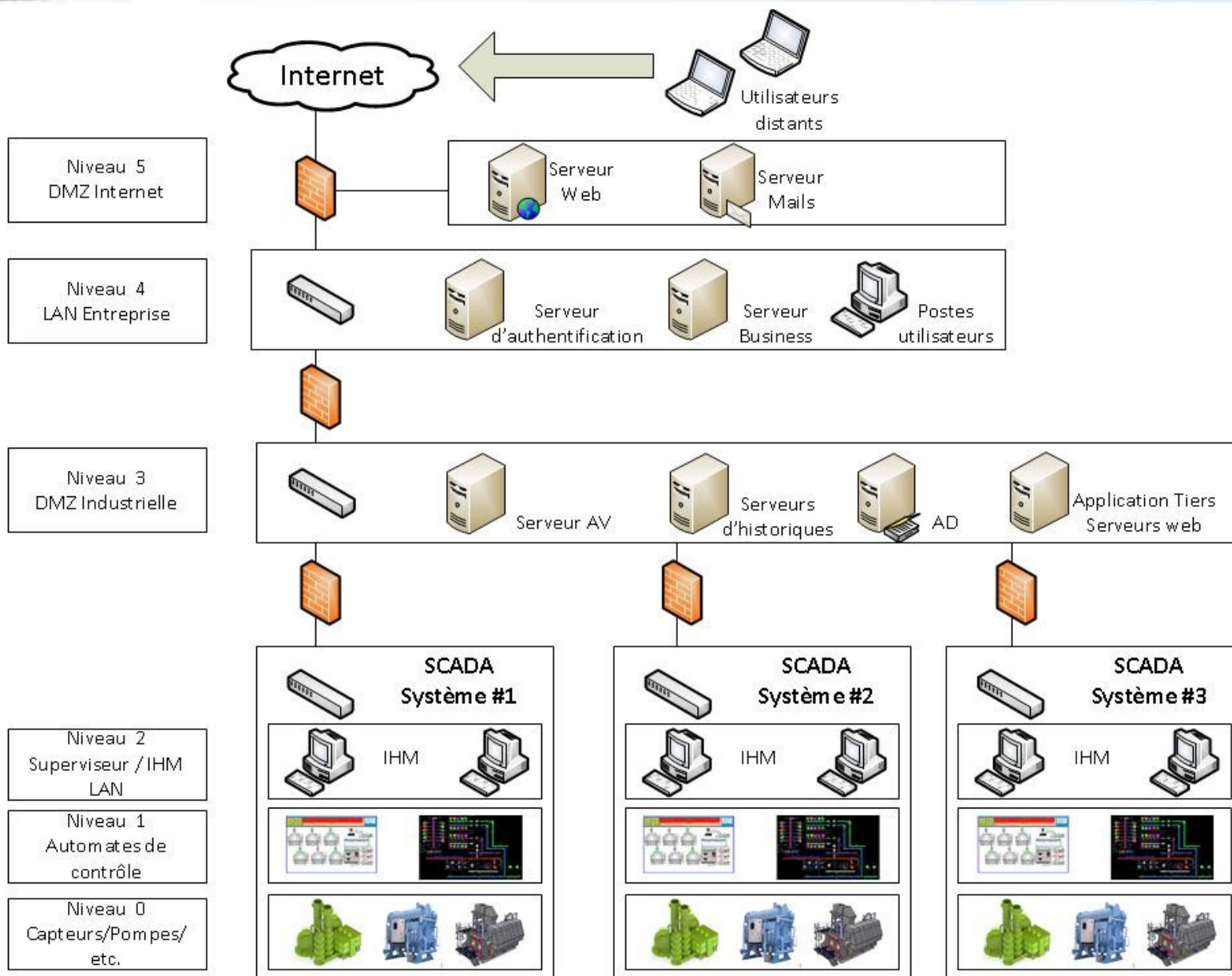


- Domaines chimiques
 - *Chemical Facility Anti-Terrorism Standards (CFATS)*



Attaques SCADA

Attaques SCADA



- 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.)

- Niveau 3 – DMZ « Industrielle »
 - Présence de ressources partagées
 - 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

- Exemple avec ModBus

ModScan32 - [ModSca1]

File Connection Setup View Window Help

Address: 0001 Device Id: 1 Number of Polls: 52
 Length: 100 MODBUS Point Type: 01: COIL STATUS Valid Slave Responses: 52
 Reset Ctrs

00001:	<0>	00037:	<0>	00073:	<0>
00002:	<0>	00038:	<0>	00074:	<0>
00003:	<0>	00039:	<0>	00075:	<0>
00004:	<0>	00040:	<0>	00076:	<0>
00005:	<0>	00041:	<0>	00077:	<0>
00006:	<0>	00042:	<0>	00078:	<0>
00007:	<0>	00043:	<0>	00079:	<0>
00008:	<0>	00044:	<0>	00080:	<0>
00009:	<0>	00045:	<0>	00081:	<0>
00010:	<0>	00046:	<0>	00082:	<0>
00011:	<0>	00047:	<0>	00083:	<0>
00012:	<0>	00048:	<0>	00084:	<0>
00013:	<0>	00049:	<0>	00085:	<0>
00014:	<0>	00050:	<0>	00086:	<0>
00015:	<0>	00051:	<0>	00087:	<0>
00016:	<0>	00052:	<0>	00088:	<0>
00017:	<0>	00053:	<0>	00089:	<0>
00018:	<0>	00054:	<0>	00090:	<0>
00019:	<0>	00055:	<0>	00091:	<0>
00020:	<0>	00056:	<0>	00092:	<0>
00021:	<0>	00057:	<0>	00093:	<0>
00022:	<0>	00058:	<0>	00094:	<0>
00023:	<0>	00059:	<0>	00095:	<0>
00024:	<0>	00060:	<0>	00096:	<0>
00025:	<0>	00061:	<0>	00097:	<0>
00026:	<0>	00062:	<0>	00098:	<0>
00027:	<0>	00063:	<0>	00099:	<0>
00028:	<0>	00064:	<0>	00100:	<1>
00029:	<0>	00065:	<0>		
00030:	<0>	00066:	<0>		
00031:	<0>	00067:	<0>		
00032:	<0>	00068:	<0>		
00033:	<0>	00069:	<0>		
00034:	<0>	00070:	<0>		
00035:	<0>	00071:	<0>		
00036:	<0>	00072:	<0>		

ModScan32 - (10.10.10.3)

Write Coil

Node: 1

Address: 88

Value

Off On

Update Cancel

- ModBus

Capturing from AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler) [Wireshark 1.6.0 (SVN Rev 37592 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: not modbus_tcp.func_code == 1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	10.10.10.3	TCP	62	startron > asa-app1-proto [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_P
2	0.001567	10.10.10.3	10.0.2.15	TCP	60	asa-app1-proto > startron [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=
3	0.001591	10.0.2.15	10.10.10.3	TCP	54	startron > asa-app1-proto [ACK] Seq=1 Ack=1 win=64240 Len=0
5	0.596633	10.10.10.3	10.0.2.15	TCP	60	asa-app1-proto > startron [ACK] Seq=1 Ack=13 win=65535 Len=0
7	0.776587	10.0.2.15	10.10.10.3	TCP	54	startron > asa-app1-proto [ACK] Seq=13 Ack=23 win=64218 Len=0
9	1.598062	10.10.10.3	10.0.2.15	TCP	60	asa-app1-proto > startron [ACK] Seq=23 Ack=25 win=65535 Len=0
11	1.778033	10.0.2.15	10.10.10.3	TCP	54	startron > asa-app1-proto [ACK] Seq=25 Ack=45 win=64196 Len=0
13	2.600337	10.10.10.3	10.0.2.15	TCP	60	asa-app1-proto > startron [ACK] Seq=45 Ack=37 win=65535 Len=0
15	2.779475	10.0.2.15	10.10.10.3	TCP	54	startron > asa-app1-proto [ACK] Seq=37 Ack=67 win=64174 Len=0
17	3.600981	10.10.10.3	10.0.2.15	TCP	60	asa-app1-proto > startron [ACK] Seq=67 Ack=49 win=65535 Len=0
19	3.782347	10.0.2.15	10.10.10.3	TCP	54	startron > asa-app1-proto [ACK] Seq=49 Ack=89 win=64152 Len=0
21	4.602420	10.10.10.3	10.0.2.15	TCP	60	asa-app1-proto > startron [ACK] Seq=89 Ack=61 win=65535 Len=0
23	4.782341	10.0.2.15	10.10.10.3	TCP	54	startron > asa-app1-proto [ACK] Seq=61 Ack=111 win=64130 Len=0
24	4.903420	10.0.2.15	10.10.10.3	Modbus/	66	query [1 pkt(s)]: trans: 1536; unit: 1, func: 5: write coil.
25	4.903899	10.10.10.3	10.0.2.15	TCP	60	asa-app1-proto > startron [ACK] Seq=111 Ack=73 win=65535 Len=0
26	4.906658	10.10.10.3	10.0.2.15	Modbus/	66	response [1 pkt(s)]: trans: 1536; unit: 1, func: 5: write coil.
27	5.082779	10.0.2.15	10.10.10.3	TCP	54	startron > asa-app1-proto [ACK] Seq=73 Ack=123 win=64118 Len=0
29	5.603878	10.10.10.3	10.0.2.15	TCP	60	asa-app1-proto > startron [ACK] Seq=123 Ack=85 win=65535 Len=0
31	5.783792	10.0.2.15	10.10.10.3	TCP	54	startron > asa-app1-proto [ACK] Seq=85 Ack=145 win=64096 Len=0
33	6.606723	10.10.10.3	10.0.2.15	TCP	60	asa-app1-proto > startron [ACK] Seq=145 Ack=97 win=65535 Len=0
35	6.785234	10.0.2.15	10.10.10.3	TCP	54	startron > asa-app1-proto [ACK] Seq=97 Ack=167 win=64074 Len=0
37	7.606721	10.10.10.3	10.0.2.15	TCP	60	asa-app1-proto > startron [ACK] Seq=167 Ack=109 win=65535 Len=0

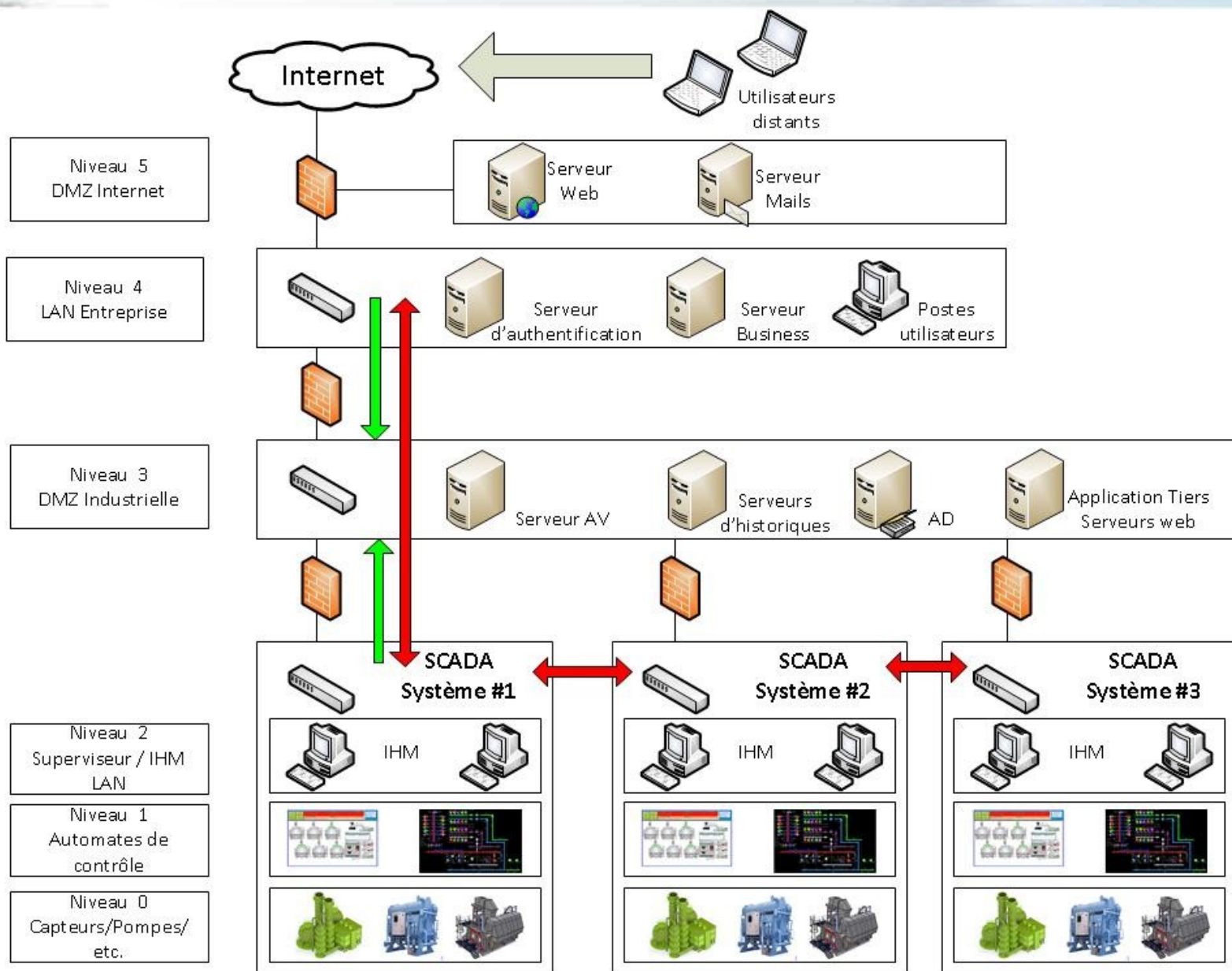
Transmission Control Protocol, Src Port: startron (1057), Dst Port: asa-app1-proto (502), Seq: 61, Ack: 111, Len: 12

Modbus/TCP

- transaction identifier: 1536
- protocol identifier: 0
- length: 6
- unit identifier: 1
- Modbus
 - function 5: write coil
 - reference number: 88
 - Data
 - Padding

Défenses 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 ?