



Setting the Standard for Automation™

District 12 & Qatar Section

ISA99/IEC 62443: a solution to cyber-security issues?

Jean-Pierre HAUET

KB Intelligence

ISA District 12 VP

ISA-France President

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

ISA Automation Conference – Doha (Qatar) - 9 & 10 December 2012

The cyber-security risks

- Cyber-security of control systems relates to the prevention of risks associated with intrusions into systems linked to malicious actions, through computer equipment and communication networks.
- The effect of intrusions may include:
 - Loss of system availability and of production capacity
 - Inferior product quality
 - Publication of sensitive information to unauthorized destinations
 - Equipment damage
 - Personal injury
 - Risk to public health and confidence
 - Violation of legal and regulatory requirements
 - Compromised image, etc.

Cyber-security risks are a reality

Cyber-security is not a paranoia !

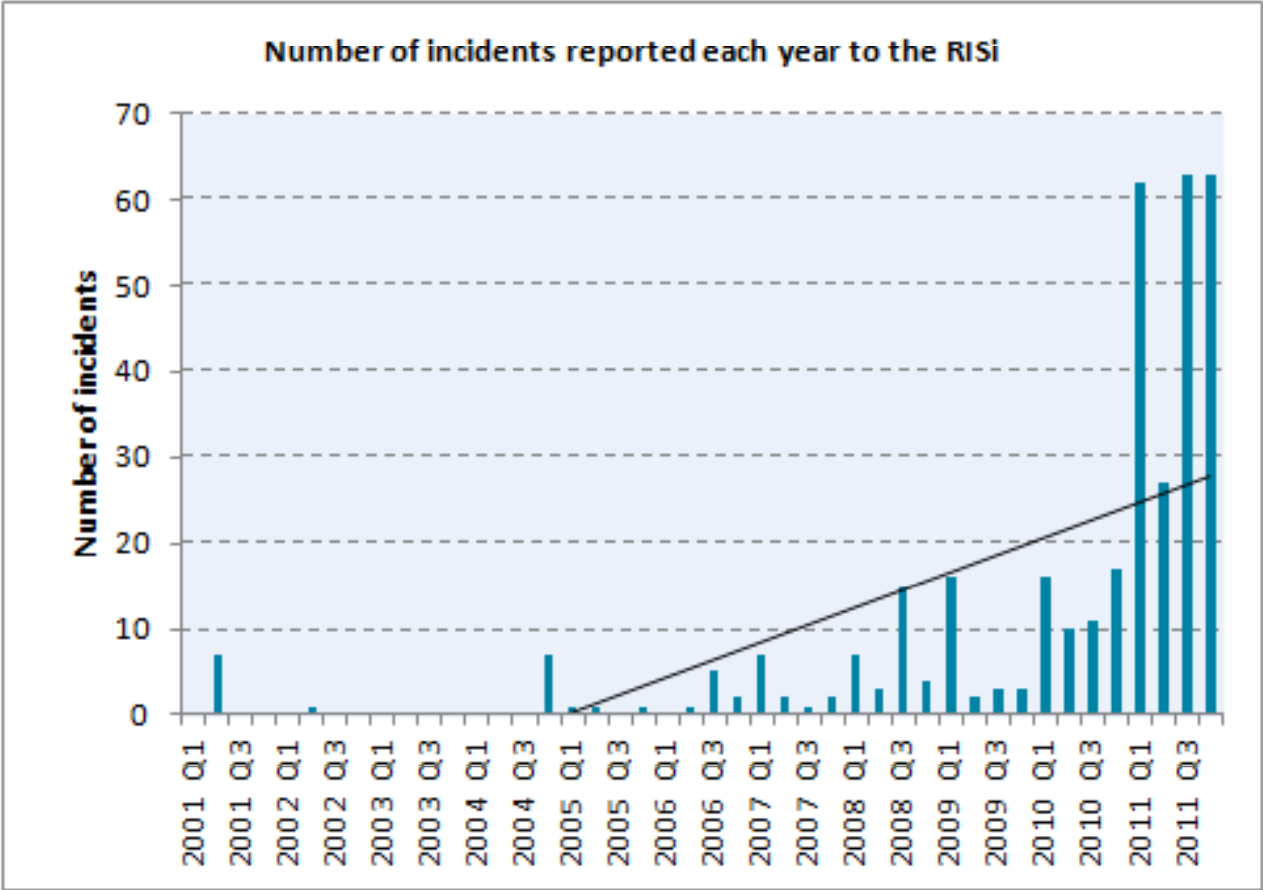


- **Water industry**
 - Maroochy Shire (Australia) sewage spill (disgruntled employee) – 2002
 - Water filtering plant near Harrisburg (USA) - 2006
 - South Houston water utility (proof of concept) - 2011 ,etc.
- **Oil Industry**
 - CIA Trojan causes Siberian gas pipeline explosion (1982)
 - Electronic Sabotage of Venezuela Oil Operations (2009)
 - Slammer impacts offshore platforms (2009)
 - Night Dragon attack against 12 gas-oil and chemical companies - Steal of sensitive information (2009-2011), etc.
- **Power industry**
 - Davis-Besse nuclear power plant (Ohio – USA) - 2003
 - Brown Ferry nuclear power plant (Alabama-USA) – 2006
- **Electrical networks, chemical industries etc.**

▶ **SCADA and ICS are now targets**



Number of reported incidents is increasing



Risi

The Repository of Security Incidents

- HOME
- HOW IT WORKS
- PRODUCTS
- MEMBERSHIP
- ADVISORY PANEL
- CONTACT
- FAQ
- ABOUT

US CERT : a reliable source of information



ICS-CERT Advisories and Reports Archive - Windows Internet Explorer

https://www.us-cert.gov/control_systems/ics-cert/archive.html

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME SECURITY PUBLICATIONS ALERTS AND TIPS RELATED RESOURCES ABOUT US GFIRST

Control Systems

- Home
- Calendar
- ICS-CERT
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Secure Architecture Design
- Assessments
- Standards & References
- Related Sites
- FAQ

Control Systems Security Program (CSSP)
ICS-CERT Advisories and Reports Archive

Monthly Monitors | Alerts & Advisories (by Vendor) | Other Alerts & Advisories | Other Reports
Notable ICS-Related Vulnerabilities

MONTHLY MONITORS

2012: September | August | June-July | May | April | March | February | January |
2011: December | November | October | September | July-August | June | May | April

ALERTS & ADVISORIES (BY VENDOR)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z #

ABB

ABB AC500 PLC Webserver CoDeSys Vulnerability, ICSA-12-320-01 (November 15, 2012)
ABB Multiple Components Buffer Overflow (UPDATE), ICSA-12-095-01A (April 10, 2012)

Attacks are getting more sophisticated



- 2000 – 2009 : “conventional” attacks by viruses or worms, Code Red, Nimda, Blaster, Sasser, SQL Slammer, Conficker, myDoom, etc.
- > 2010 : more professional attacks using sophisticated software packages capable of infiltrating ICS, detecting, communicating, replicating, developing
 - July 2010 : Stuxnet – Targeted uranium enrichment infrastructure in Iran - First discovered malware that spies on and subverts industrial systems
 - October 2011 : W32Duqu – Steal of information
 - May 2012 : Flame – Steal of information
 - August 2012 : Shamoon – Data destruction (Aramco – Rasgas)

▶ **Companies in the energy field are now clearly targeted**

Stuxnet (1)



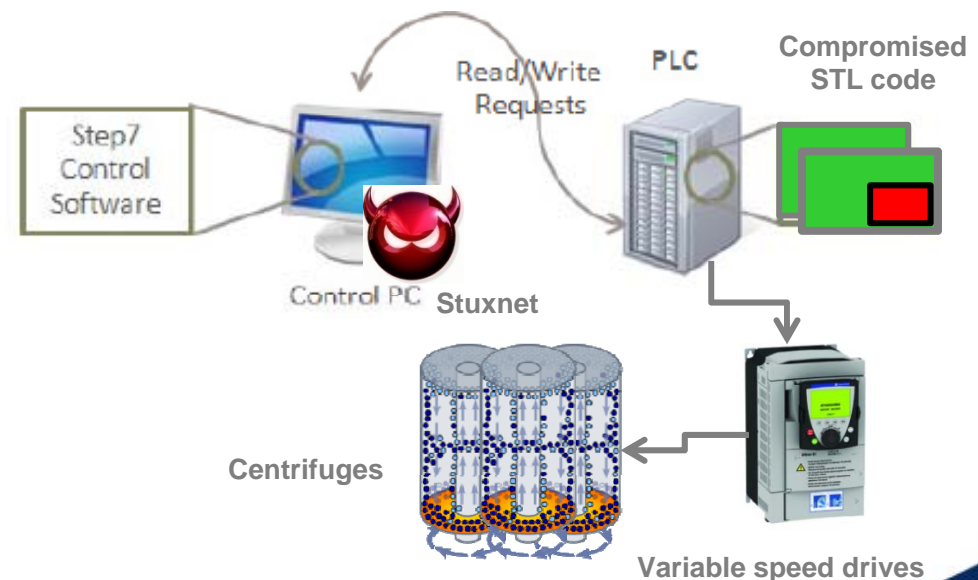
- **July, 2010:** Stuxnet worm discovered
- Attacked Siemens PCS7, S7 PLC and WIN-CC systems
- Infected 100,000 computers
- Infected **at least** 22 manufacturing sites
- Main target, Iran's nuclear enrichment program
- May have destroyed up to 1000 centrifuges (10 percent) sometime between November 2009 and late January 2010



The Stuxnet process



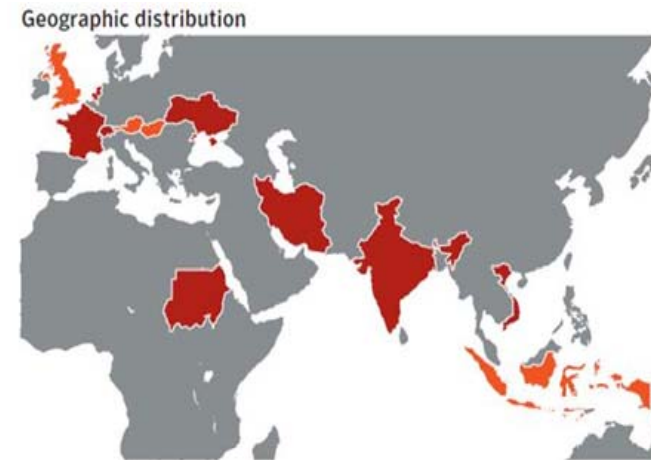
- Initially spread using infected removable drives such as USB flash drives
- Uses zero-day exploits and techniques to infect and update Windows computers inside private networks
- Communicates with distant command and control servers
- Detects Siemens' WinCC/PCS 7 SCADA control software
- Subverts a key communication library of WinCC
- Installs malware into memory blocks of the PLC that monitors the Profibus messaging bus of the system
- Remains hidden by a rootkit
- Periodically modifies the frequency of the VSD



The sons of Stuxnet : DUQU, FLAME et GAUSS



- Duqu (Sept 2011)
 - Malware with large similarities with Stuxnet
 - Trojan horse aiming to capture and exfiltrate information dissimulated in a Jpeg file
 - 12 countries contaminated
- Flame (May 2012)
 - Spyware discovered in Iran in oil and nuclear installations
 - More complex than Stuxnet
 - can record audio, screenshots, keyboard activity and network traffic
- Gauss (August 2012)
 - Design similar to Gauss
 - designed to steal data from several Lebanese banks



Source : Symantec – November 2001



Source : Securelist.com

Shamoon



- Aramco (August 2012)
 - most destructive attack the business sector has seen to date
 - 30,000 computers running on Windows NT infected at Aramco
 - replaced crucial system files with part of an image of a burning U.S. flag
 - Messaging services severely disturbed for several weeks
 - Production officially not directly affected
 - Rasgas (Qatar) hit by an apparently similar virus



The number of US-CERT alerts is increasing



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ALERT


ICS-ALERT-12-020-03B—SCHNEIDER ELECTRIC MODICON QUANTUM MULTIPLE VULNERABILITIES

UPDATE B

April 09, 2012

ALERT

SUMMARY




ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-12-265-01—EMERSON DELTAV BUFFER OVERFLOW

September 28, 2012



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-12-263-01—SIEMENS S7-1200 INSECURE HTTPS CERTIFICATE

September 19, 2012

OVERVIEW

Siemens has reported^a an insecure HTTPS certificate stored on S7-1200 v2.x. Siemens has provided guidance to mitigate this vulnerability, which was exploited remotely.

AFFECTED PRODUCTS

Siemens reports that the vulnerability affects the following



ICS-CERT
Industrial Control Systems
Cyber Emergency Response Team



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Joint Security Awareness Report

JSAR-12-241-01A—Shamoon/DistTrack Malware

UPDATE A

September 27, 2012

OVERVIEW

W32.DistTrack, also known as “Shamoon,” is an information-stealing malware that also includes a destructive module. Shamoon renders infected systems useless by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once overwritten, the data are not recoverable.

Based on initial reporting and analysis of the malware, no evidence exists that Shamoon specifically targets industrial control systems (ICSs) components or U.S. government agencies.

Why are IACS* vulnerable ?

IACS : Industrial Automation & Control Systems

The myth of « air gap » is dead

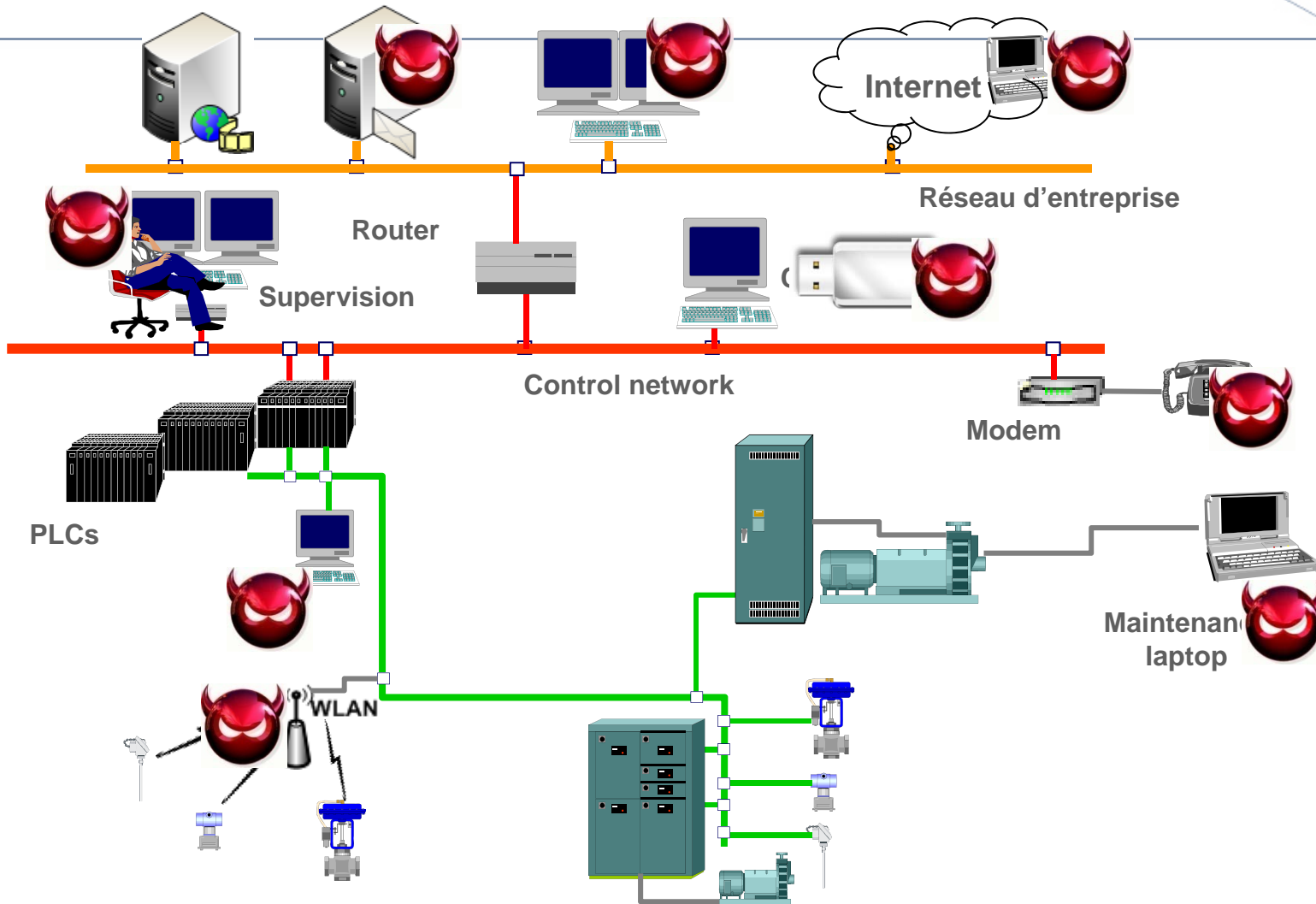


- A modern IACS is highly complex and interconnected
- Multiple potential pathways exist from the outside world to process controllers
- Assuming an air-gap between IACS and corporate networks is unrealistic
- Focusing security efforts on a few obvious pathways (typically the Enterprise/IACS firewall) is a flawed defense

Three main reasons

- Interconnection of networks
 - Integration between control networks and enterprise networks
 - Remote connections (debugging, maintenance, etc.)
 - « Sneakernets » : USB drives, CD Roms, Laptops, Smart phones
- Use of Commercial off-the-shelf components (COTS)
 - Unsecured protocols
 - Commercial operating systems (operator stations, engineer stations)
 - Applications not regularly patched
- Lack of security policies and procedures
 - Coexistence of two cultures : IT and IC
 - Lack of procedures (wordpasses & antivirus management, etc.)
 - Lack of procedures (access control, patch management, visitors, subcontractors, etc.)
 - Lack of awareness, training, motivation...

Open systems mean more entry points



New remote clients

ScadaMobile
 Logic Controller
 data at your
 fingertips



- Application using Scadamobile on aniPhone (<http://www.sweetwilliams.com/iweb/smhome>)



How to protect IACS? The IEC 62443 (ISA-99) approach

Limits of a conventional IT approach

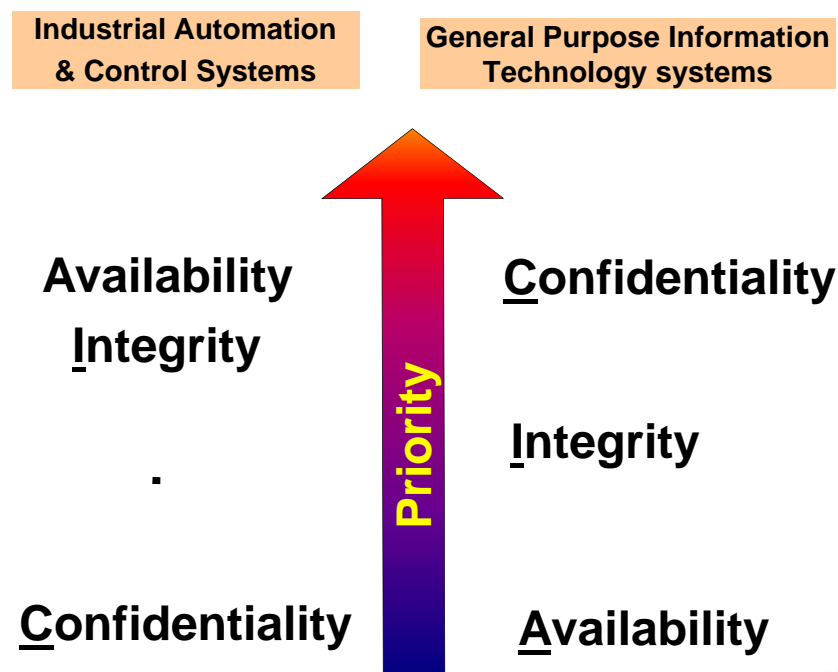
- IACS are complex (mix of technologies, hardware, software, access rights, etc.)
- Architectures different
- Performance criteria different (real time...)
- Priorities different

– **IT**

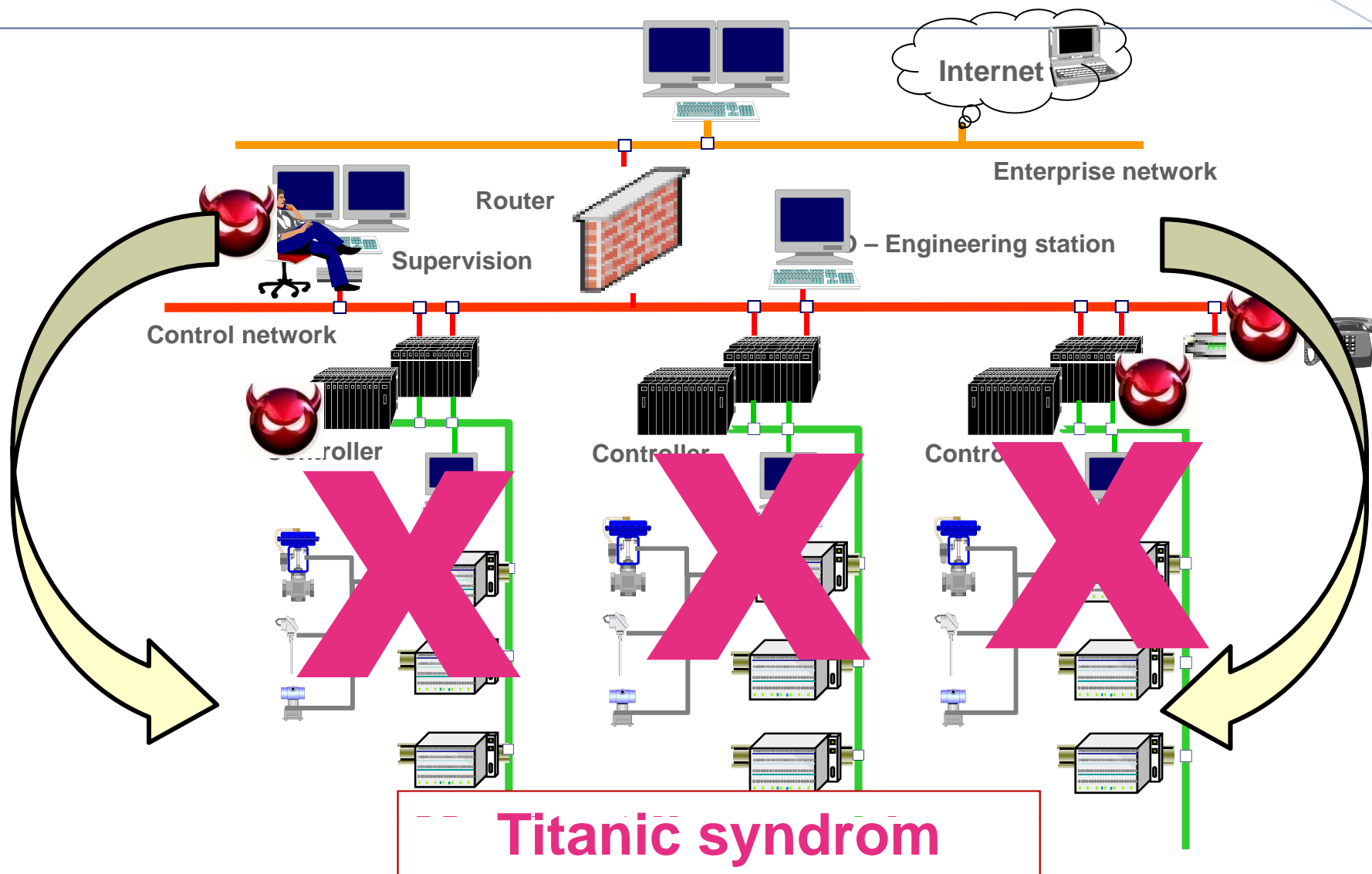
- Confidentiality first
- large servers to be protected

– **IC**

- Availability and Integrity first
- Numerous critical points to protect



The firewall illusion








IEC 62443 approach



- The only comprehensive set of security standards specifically dedicated to IACS
- Directly results from the ISA-99 committee initiative(International Society of Automation) : ISA-99
- Four levels of documents
 - General (Terminology, Concepts and Models)
 - Asset owners (Establishing and Operating an IACS Security Program)
 - System integrators (Security Technologies, Zones & Conduits Security)
 - Components providers (Product Development Requirements)
- Coherent with ISO 27000
- May be supplemented by specific standards
 - CIP requirements (Critical Infrastructure Protection) (NERC)
 - Guide to Industrial Control System Security (NIST – 2008)
 - Computer Security at Nuclear facilities (IAEA – 2011)

CEI 62443 – State of completion



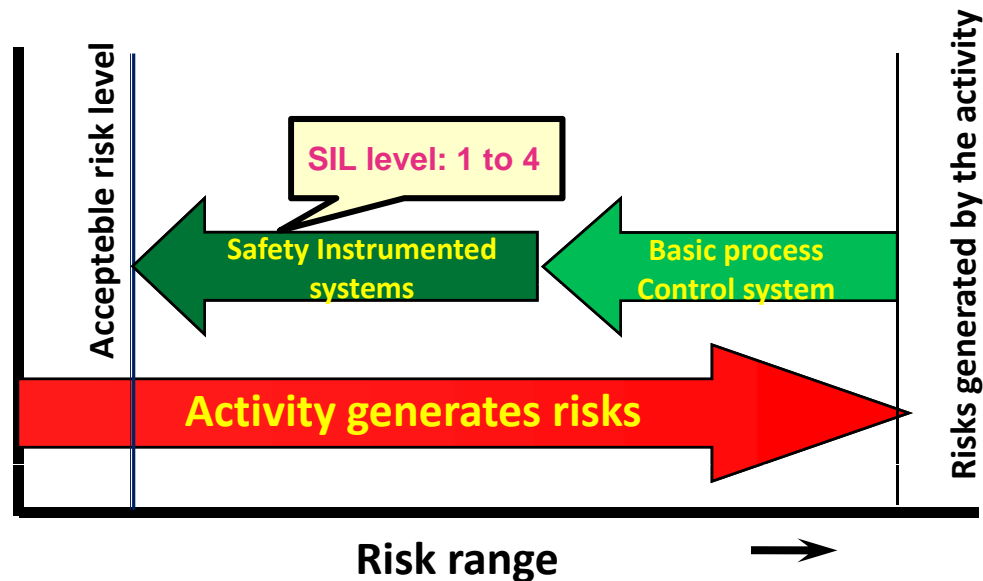
General	 <p>IEC 62443-1-1 (Ed 2) Terminology, concepts and models ISA 62443.01.01</p>	<p>IEC/TR 62443-1-2 Master glossary of terms and abbreviations ISA 62443.01.02</p>	<p>IEC 62443-1-3 System security compliance metrics ISA 62443.01.03</p>	
Asset owner	 <p>IEC 62443-2-1 (Ed 2) Establishing an IACS security program ISA 62443.02.01</p>	<p>IEC 62443-2-2 Operating an IACS security program ISA 62443.02.02</p>	<p>IEC/TR 62443-2-3 Patch management in the IACS environment ISA 62443.02.03</p>	 <p>IEC/TR 62443-2-4 Certification of IACS supplier security policies and practices Développé par WIB</p>
System integrator	 <p>IEC/TR 62443-3-1 Security technologies for IACS ISA 62443.03.01</p>	<p>IEC 62443-3-2 Security assurance levels for zones and conduits ISA 62443.03.02</p>	 <p>IEC 62443-3-3 System security requirements and security assurance levels ISA 62443.03.03</p>	
Component provider	<p>IEC 62443-4-1 Product development requirements ISA 62443.04.01</p>	<p>IEC 62443-4-2 Technical security requirements for IACS components ISA 62443.04.02</p>		



General philosophy (1)

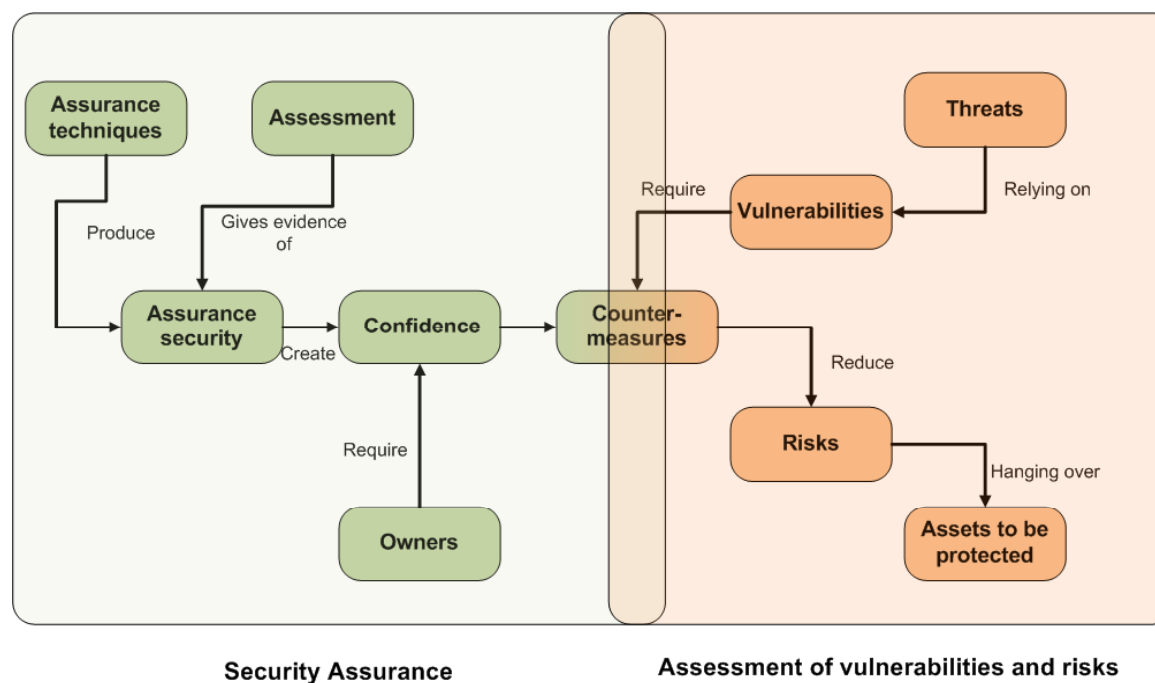


- **Similar to the IEC 61508 / 61511 (functional safety) :**
 - Any industrial activity generates risks due to various threats and vulnerabilities
 - These risks are or are not acceptable
 - If they are not acceptable, they have to be reduced by countermeasures
 - As regards functional safety, these countermeasures may reside in the implementation of Safety Instrumented Systems (SIS) characterized by their Safety Integrity level (SIS), ranging from 1 to 4



General philosophy (2)

- In cyber-security, counter-measures (technical & procedural) permit the level of risk resulting from a risk analysis and the security assurance resulting from a system assessment to converge to an acceptable SAL (Security Assurance Level)



- Two interconnected processes : information security assurance and threat-risk assessment

Major differences

- **Functional safety** deals with **accidental** failures, changes, destructions...which can be assessed in terms of probabilities.
 - **Cyber-security** deals with **intentional** security events : illegal or unwanted penetrations or interferences which are not probabilistic events.
 - Cyber-security can have a diversity of origins and consequences
- ➔ The IEC 62443 challenge is to introduce rationality in a non rational sphere

Key point :

- Functional safety failures may result from internal causes as well as from external ones
- Cyber-security events only result from unwanted penetrations

Key principle : Defense in depth

- Attacks come from outside. But a perimeter defense is not sufficient.
- Several barriers must be establish in order to reduce the probability of attacker success the deeper into the ICS they go
- **Defense in depth** : provision of multiple security protections, especially in layers, with the intent to delay if not prevent an attack
- A flaw in one layer can be mitigated by capabilities in other layers
- System security becomes a set of layers within the overall network security

Defense in depth implementation : Security zones



- Defense in depth implementation leads to divide the system into **security zones**, according to their functionality/criticality and to their physical location
- **Security zones : grouping of logical or physical assets that share common security requirements**
- The **security policy of a zone** is enforced by a combination of mechanisms both at the zone edge and within the zone. Zones can be hierarchical in the sense that they can be comprised of a collection of subzones.



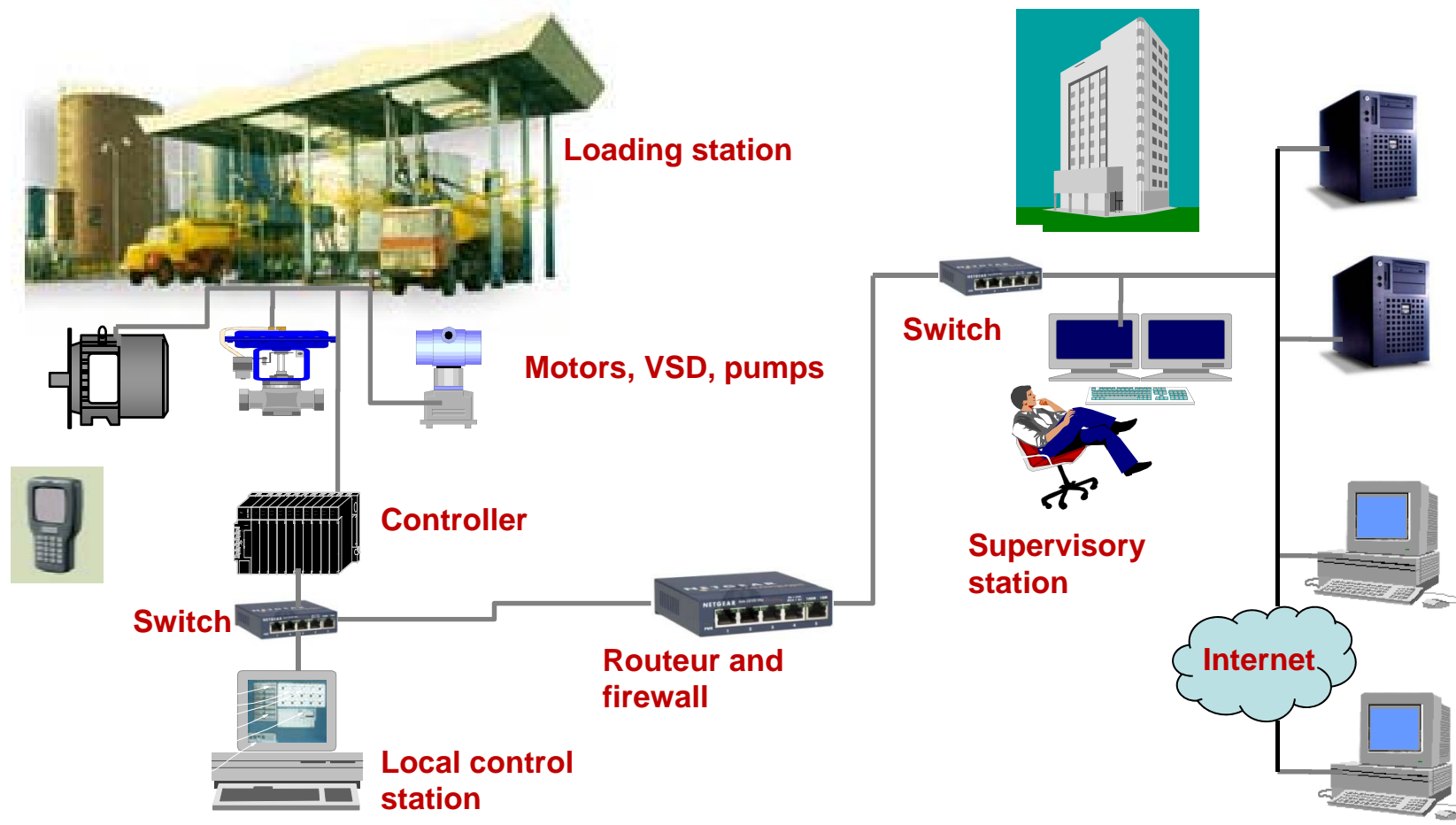
Connecting the zones : conduits



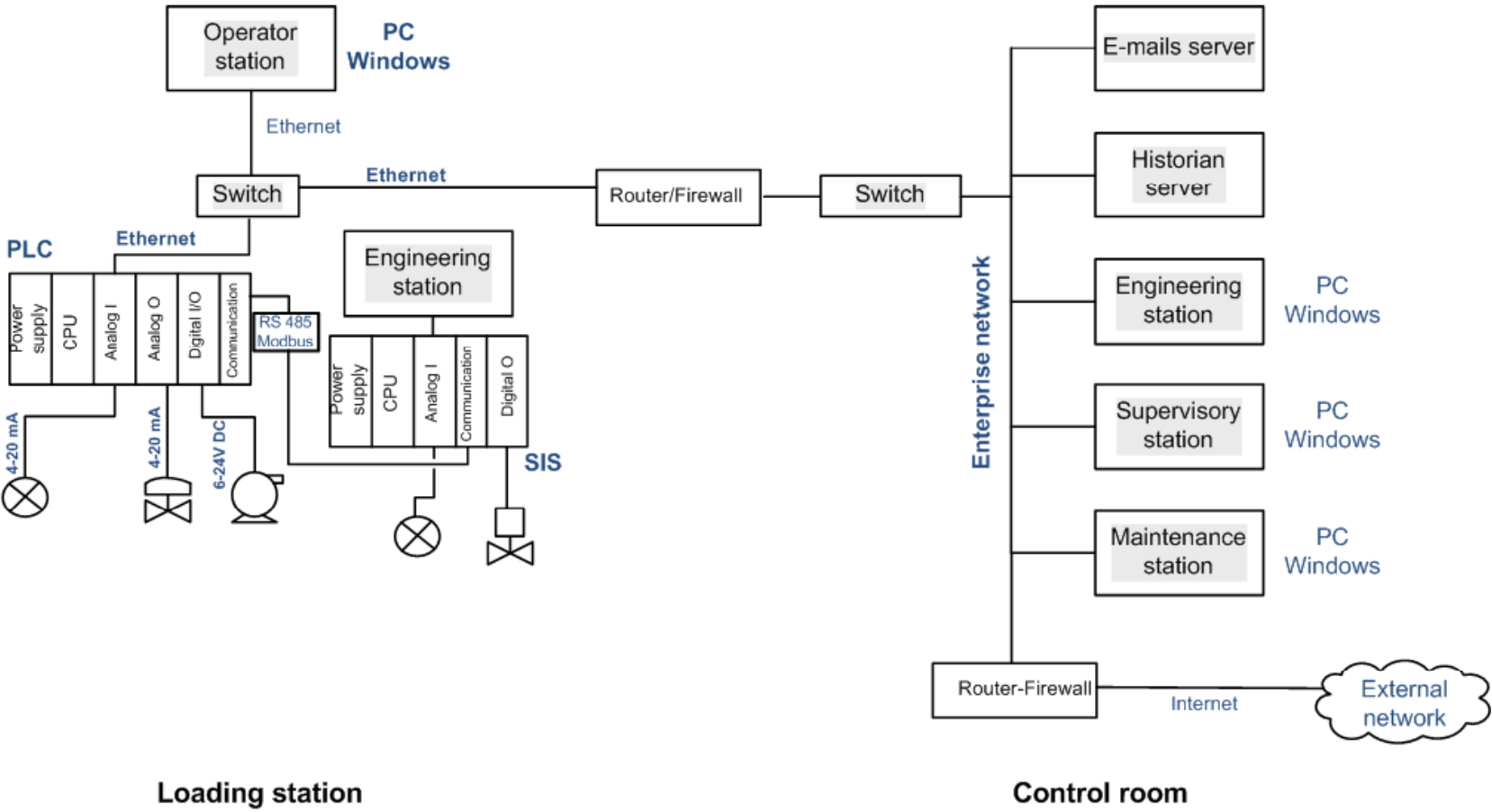
- A zone is never isolated : connections between the zones are called **conduits**
- Conduit : **logical grouping of communication assets that protects the security of the channels it contains**
- Note: Analogy to the way that a physical conduit protects cables from physical damage
- **The security policy of a conduit aims to :**
 - Control access to zones
 - Resist Denial of service attacks
 - Protect the integrity and confidentiality of network traffic



Basic example : a chlorine truck loading station



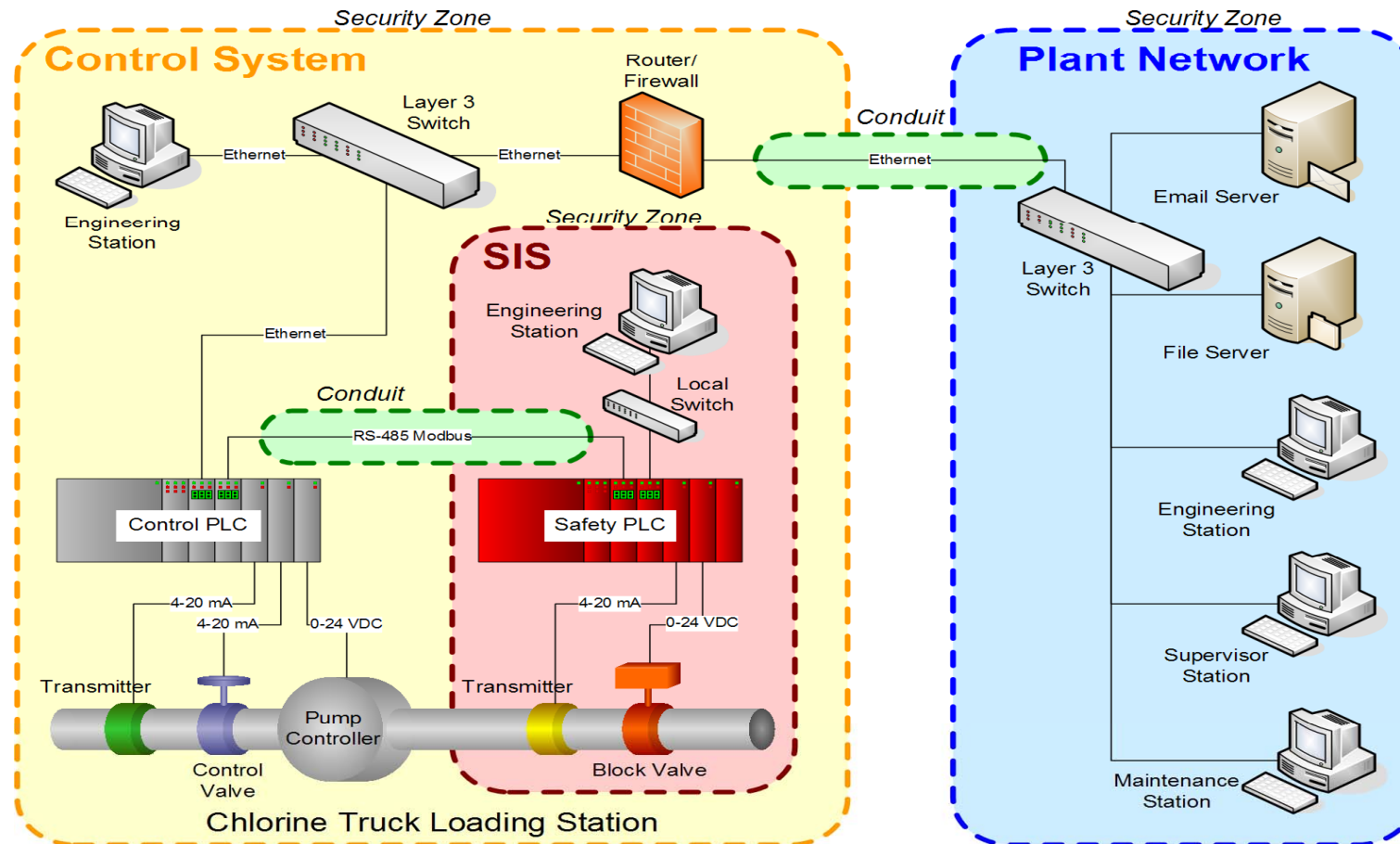
Functional architecture



Loading station

Control room

Décomposition en zones et conduits



Establishing an IACS security program

Risk analysis



- Aims to identify and classify risks for each zone, based on threats, vulnerabilities and consequences
- Permits to assign to each security zone a Security Assurance Level *target*, ranging from 1 to 4 (1 to 5 in nuclear industry)

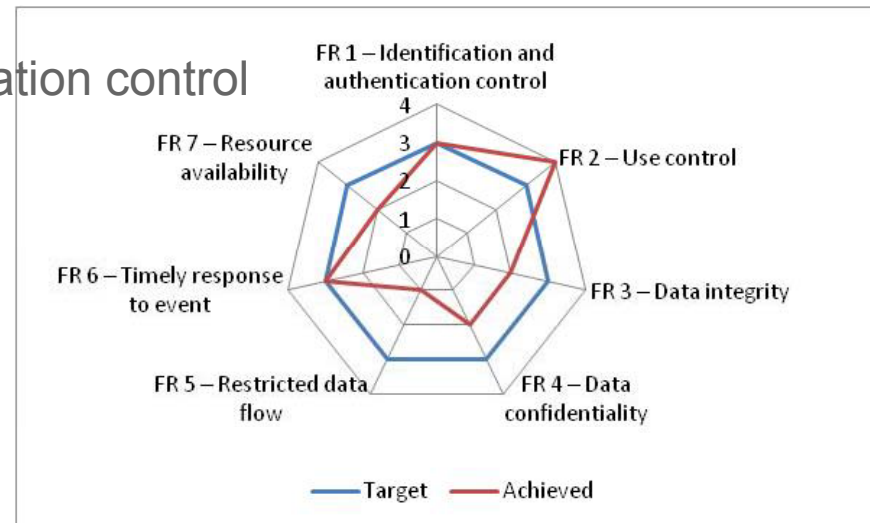
Risk level and corresponding SAL		Criticality of consequences			
		No impact	Minor	Major	Very severe
Probability	High	Medium risk SAL 2	High risk SAL 3	Very high risk SAL 4	Very high risk SAL 4
	Medium	Medium risk SAL 2	High risk SAL 3	Very high risk SAL 4	Very high risk SAL 4
	Low	Low risk SAL 1	Medium risk SAL 2	Medium risk SAL 2	High risk SAL 3
	Very low	Low risk SAL 1	Low risk SAL 1	Medium risk SAL 2	High risk SAL 3

Security Assurance Levels



- Security Assurance Levels (SALs) *achieved* are assessed for each security zone using the 7 functional requirements set forth by IEC 62443 :

- FR 1 – Identification and authentication control
- FR 2 – Use control
- FR 3 – Data integrity
- FR 4 – Data confidentiality
- FR 5 – Restricted data flow
- FR 6 – Timely response to event
- FR 7 – Resource availability



- SALs achieved can be expressed as a vector such as :

$$S_{Control\ zone}^{achieved} = \{3, 3, 4, 2, 3, 3, 3\}$$

- If a SAL= achieved < SALs target, countermeasures are requested

Short glance at some usual counter-measures

- In case of discrepancy between SALs target et SALs achieved, counter-measures are requested :

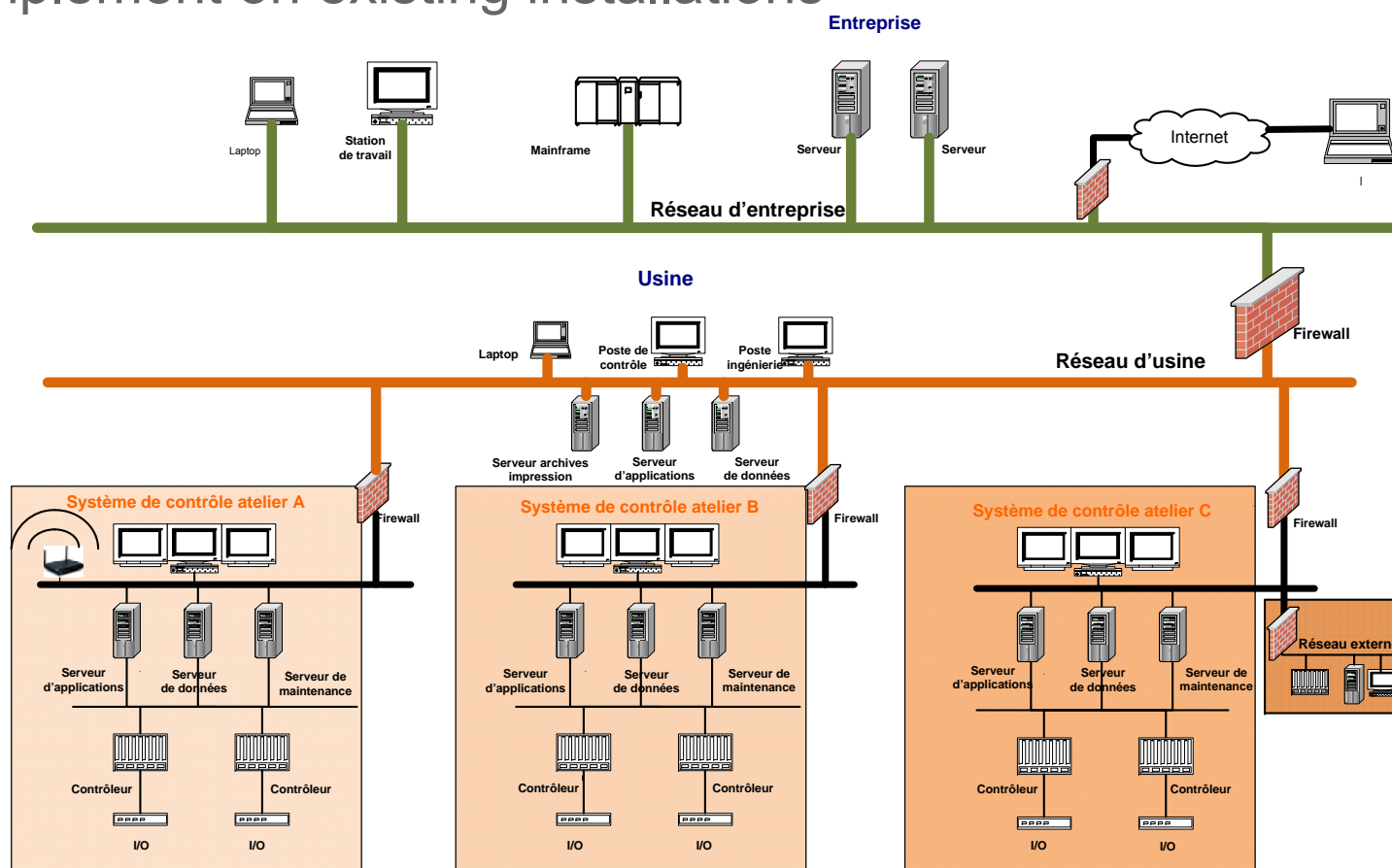
Security management Technical measures

- Antivirus, antispymware
- Firewalls, traffic analyzers
- Encryption, Virtual Private networks
- Passwords, Authentication systems
- Access control, Intrusion detection/prevention
- Network segmentation, etc.
- Rights management
- Patch management (system & applications)
- Security incidents management
- Training, etc

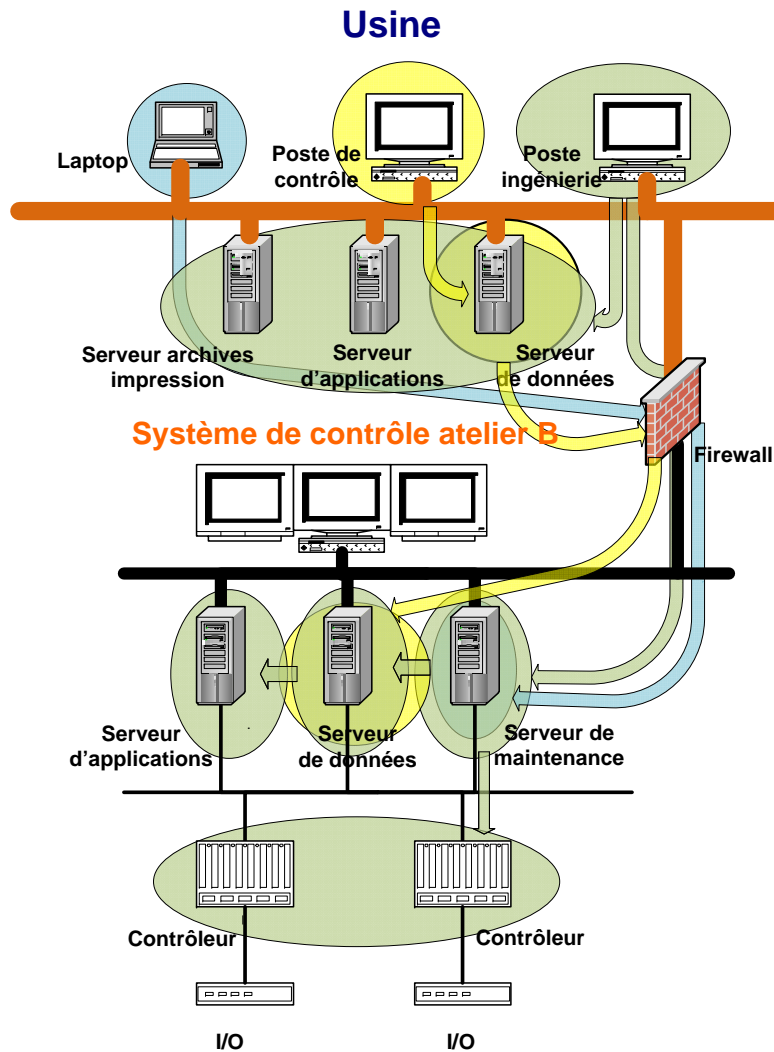
➔ Possibly, the system architecture will have to revisited

Architecture segmentation(1)

- Physical segmentation: the most secure but difficult to implement on existing installations

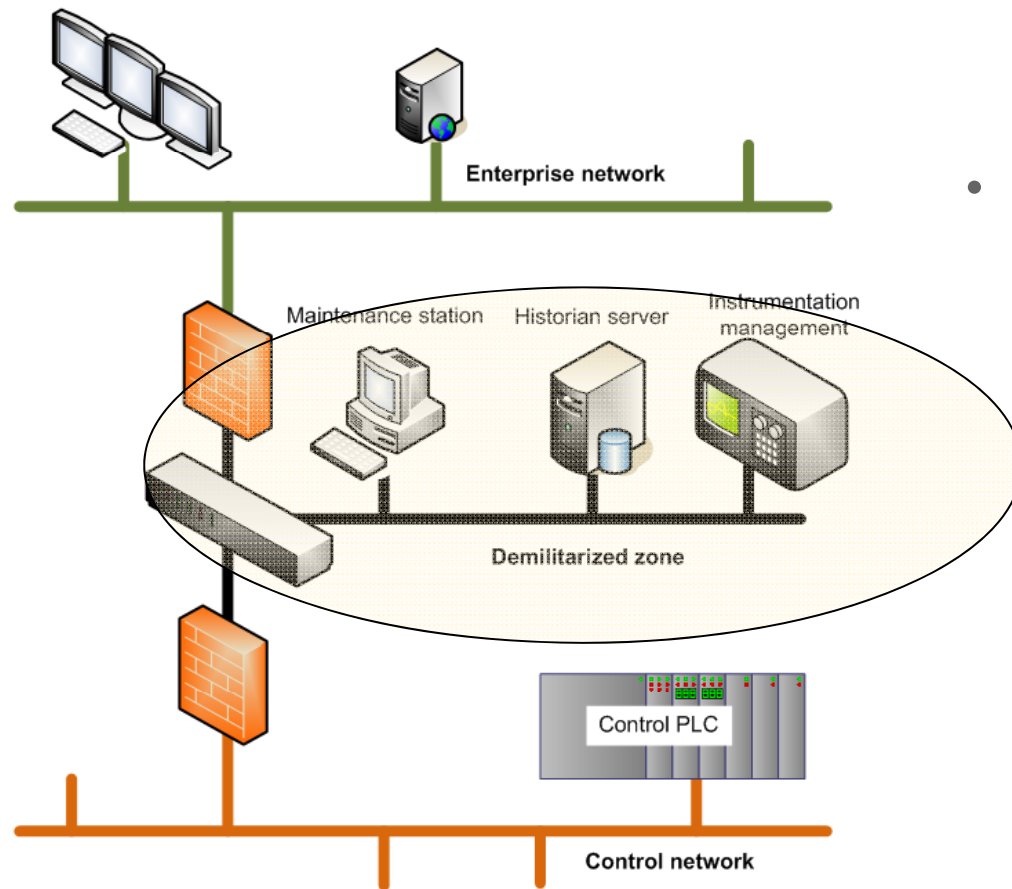


Architecture segmentation (2)



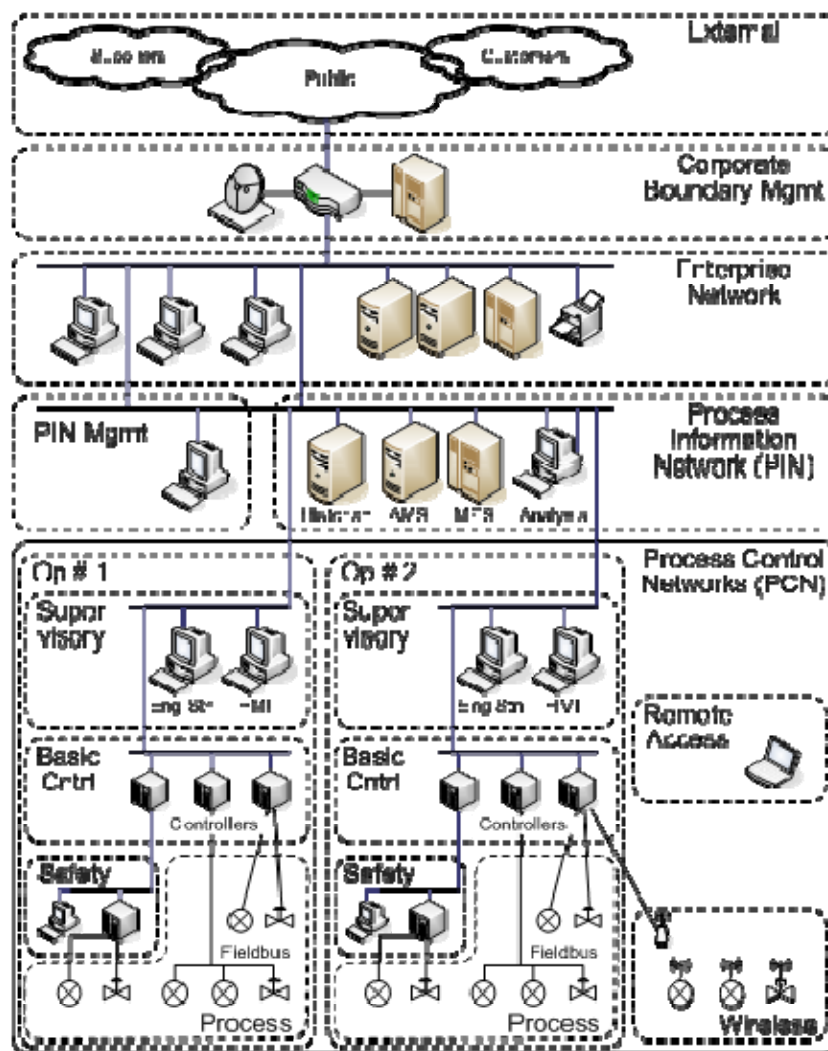
- Virtual segmentation (V-LAN)
 - Division of networks into several interwoven logical sub-networks
 - Based on programming of switches/firewalls

Demilitarized zones



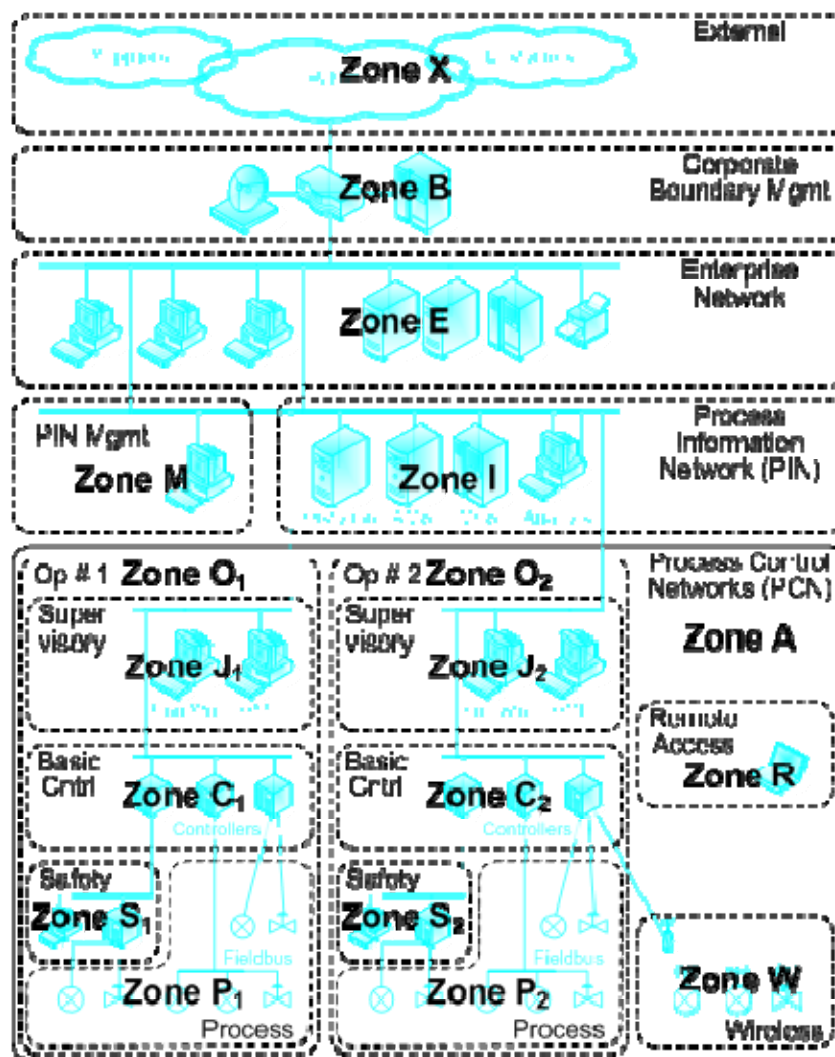
- Perimeter network segment that is logically between internal and external networks
- A demilitarized zone aims to enforce the control network's policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the control network from outside attacks

Protection of security zones by firewalls



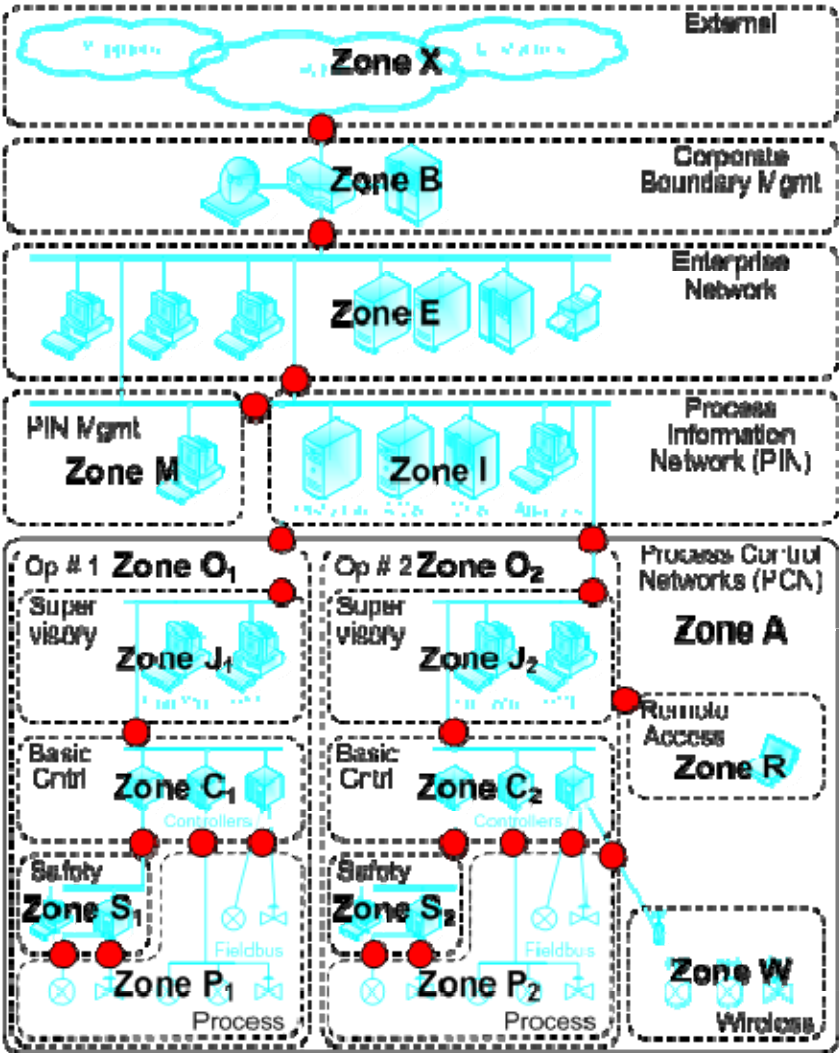
Source : Eric Byres

Specifying the zones



Source : Eric Byres

Defining the conduits

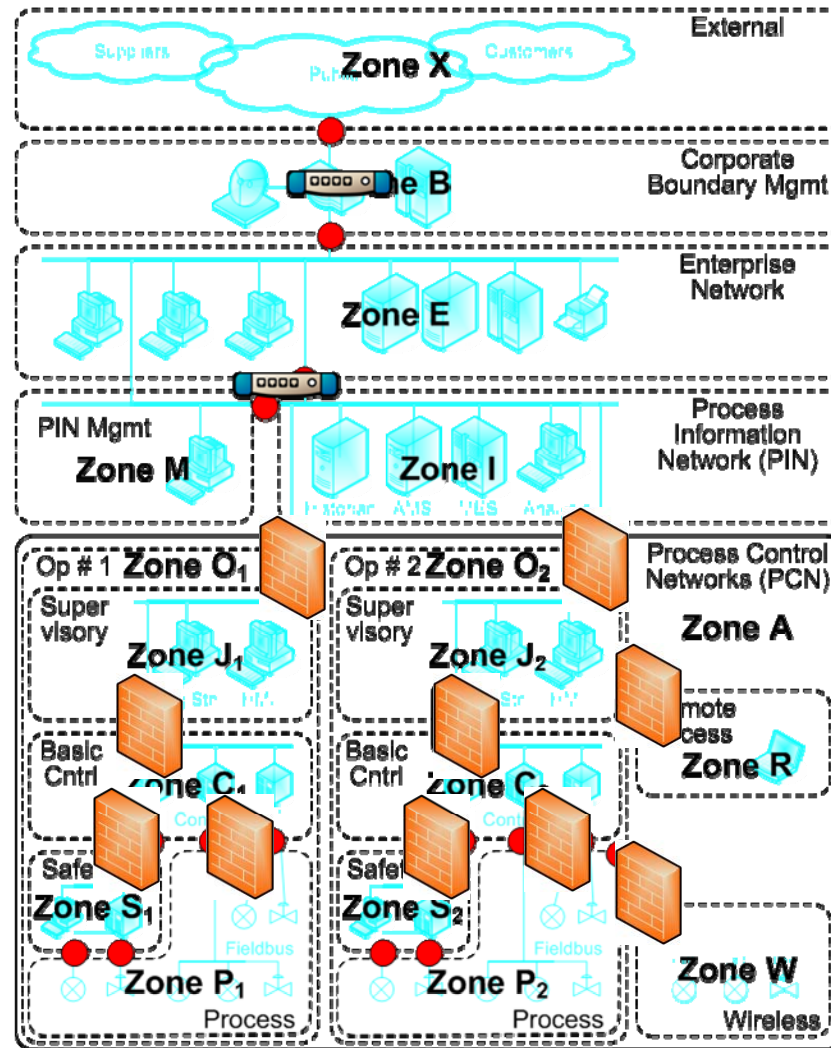


Source : Eric Byres

Protecting the conduits and the zones with firewalls



Firewalls have to be specified and programmed carefully !



Source : Eric Byres

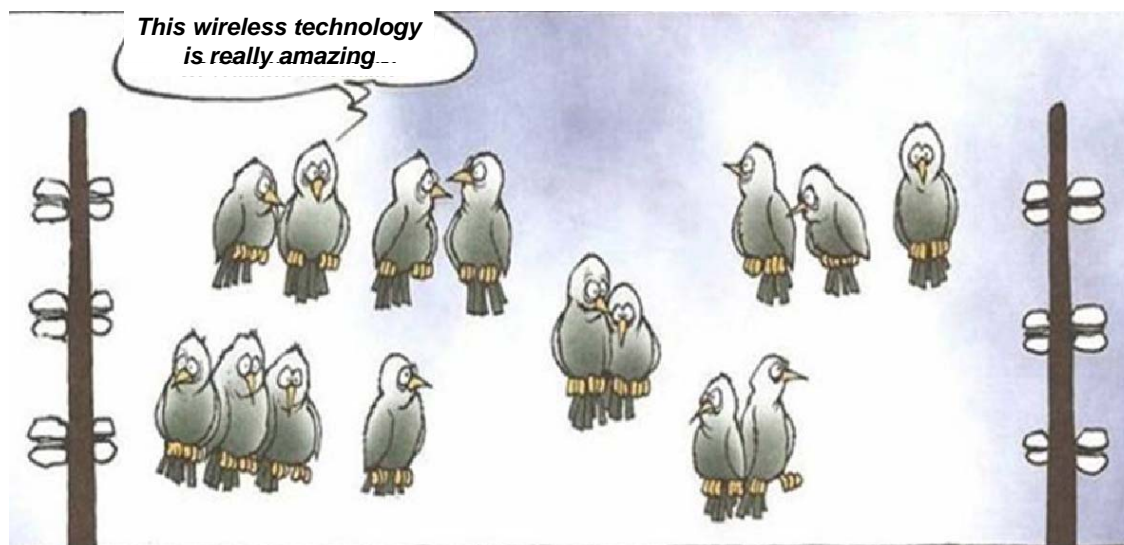
Limiting and monitoring remote accesses

- Prevent access from laptops, unknown IPs
- Avoid to give access rights to sub-contractors
- Limit access right to personnel when traveling
- Record and analyze all intrusion attempts
- Use full-fledged VPN solutions when necessary (remote maintenance), with authentication, encryption, integrity control and security management.



Activating securities on wireless communications

- Radiocommunications may offer a higher security level than wired communications
- Example : Wi-Fi WPA2 (enterprise version)
 - Authentication by Radius or Kerberos servers with asymmetric keys
 - Encryption by block ciphering using AES 128 algorithm or equivalent (Advanced Encryption Standard)



**Security Policy, organization and awareness
are as important as technical measures**

Security policy and procedures (1)

- As important as technical measures
- Less investment intensive but more volatile
- A cyber-security management system requires :
 - Top management support
 - Setting up a team of stakeholders
 - Gathering the various cultures : information systems, automation
 - Sharing experiences and good practices
 - Defining indicators for measuring progress and results
- Develop security procedures
 - Screen personnel initially and on an ongoing basis(insider risk)
 - Protect sensitive assets
 - Physical protection
 - Logical protection (identification, authentication, authorization, registration)

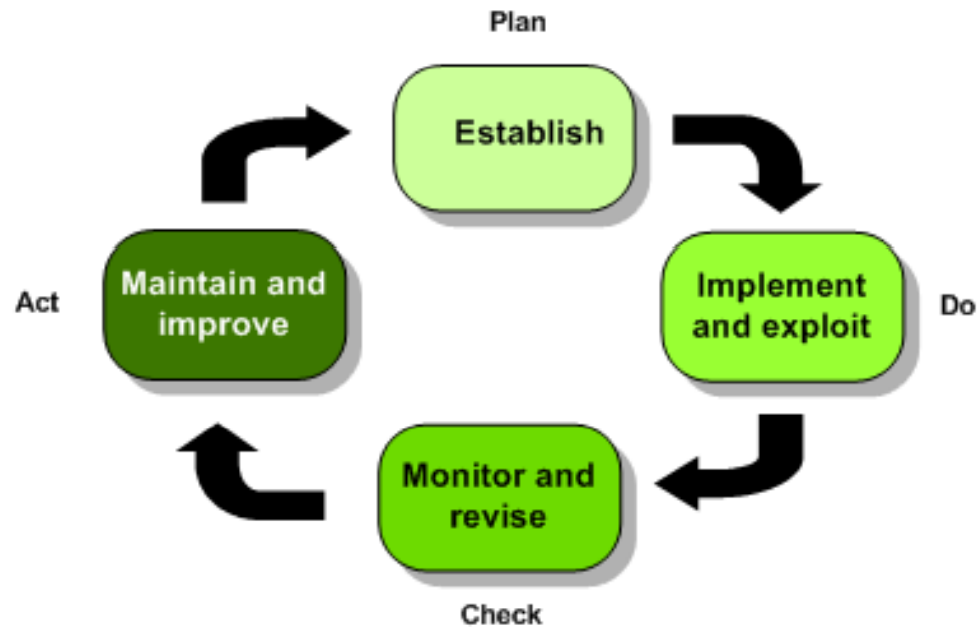
Security policy and procedures (2)

- Develop security procedures (Cont.)
 - Establish procedures for using certain devices
 - CD Roms, USB drives, laptops et PCs, remote connections
 - Carefully manage
 - Firewalls, antivirus, passwords
- Awareness and training
 - All the personnel has to be educated, at the right level, based on well prepared tutorials
- Respond appropriately to any incident
 - Organize safeguards and back-ups
 - Establish a reporting procedure for unusual events
 - Identify priority sectors to be preserve
 - Establish recovery plans

After the counter-measures...



- **Review, improve and maintain**
 - Assign an organization to manage and maintain the CSMS
 - Evaluate the CSMS periodically
 - Identify and implement corrective and preventive actions



Why to invest in cyber-security ?



- The risk does exist
- The risk is increasing
- A Cyber-security Management System will never totally eliminate the risks but it may drastically reduce their probability and their consequences
- Investing in cyber-security is like paying for an insurance; Insurance looks expensive only before the accident.
- Investing in cyber-security relates more to game theory than to conventional investment profitability.
- IEC 62433 (ex ISA-99) aims to reduce the risk to an acceptable level using a rational approach

THANKS FOR YOUR ATTENTION



Jean-Pierre HAUET

jean-pierre.hauet@kbintelligence.com

www.hauet.com