Cyber Security tutorial

Cigre Study Committee D2 Meeting 2015
Lima, Perú – October 12th-16th, 2015

Fernadez German (Spain), Dennis Holstein (USA), Robert Evans (Australia), Jens Zerbst (Sweden)

Presented by: Lhoussain Lhassani (Stedin – The Netherlands)

Agenda

- ***Cyber security***
  - ***Vulnerabilities***
  - ***Threats***
  - ***Likelihood***
  - ***Impact***
  - ***Countermeasure***
  - ***Standards, Best Practices, Guidelines***
  - ***Cigré's role***

What is Cyber Security?

"Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."

European Commission: „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Brussels, 2013

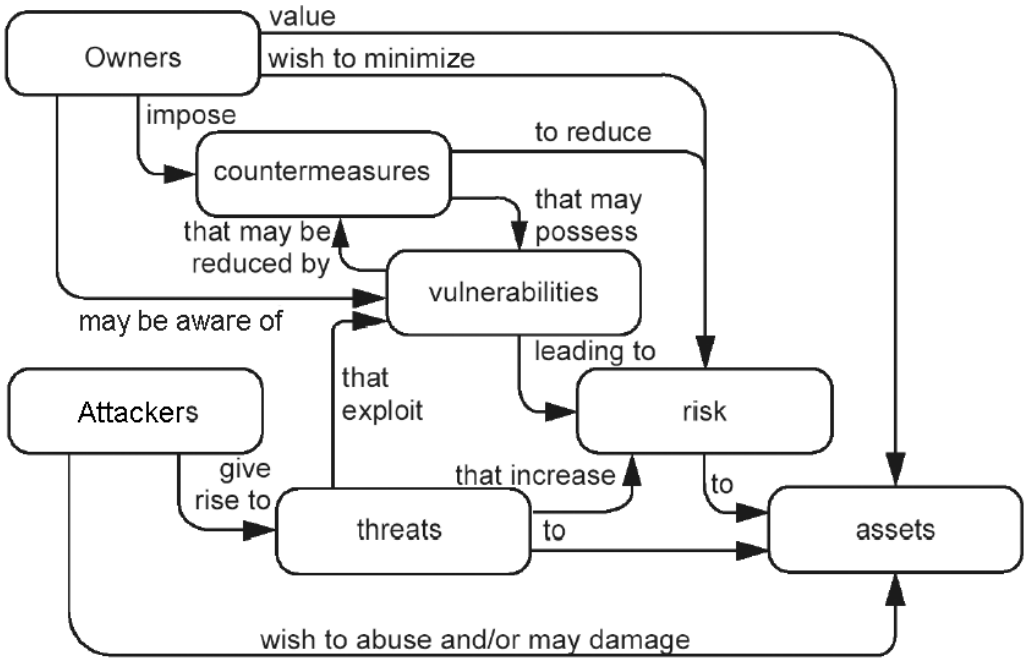
"Cybersecurity is primarily about people, processes and technologies working together "to encompas the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

"Cyberspace policy review: Assuring a Trusted and Resilient Information and Communications Infrastructure", http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Risks

"Risk in the computer security context is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

It is measured in terms of a combination of the likelihood of an event and the severity of its consequences"



Source: Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17
Security concepts and relationship (adapted from ISO 13335-1 2004)

Changes in a Energy Power Utility (EPU) infrastructure towards Smart Grids

- ***Introduction and expansion of a communication network for the current and upcoming electricity network***
- ***Introduction of new technology and connectivity approach***
- ***Long term usage of legacy assets in the domains operation, bulk generation, transmission and distribution***
- ***Introduction of intelligent control and connectivity between different domains; e.g. customer, markets, service provider, operation, bulk generation, transmission and distribution***
- ***In some parts usage of large scale homogeneous technical environmental***

Vulnerability vectors of an EPU infrastructure

- ***Introduction of connectivity, e.g. remote services, business integration, un-trusted partners***
- ***Usage of commercial off-the-shelf (COTS) system as the base for I&C systems***
- ***Wide scale usage of legacy systems***
- ***Immature and vulnerable system designs***
- ***Increased number of end user devices, e.g. maintenance notebooks.***
- ***Increasing technical complexity (e.g. protocols)***
- ***“Security by obscurity" security culture background***
- ***Lacking physical access restriction***

Comparison IT - ICS

SECURITY TOPIC	INFORMATION TECHNOLOGY	ICS SYSTEMS
Anti-virus & Mobile Code	*Common & widely used*	*Uncommon and can be difficult to deploy*
Support Technology Lifetime	*3-5 years*	*Up to 20 years*
Outsourcing	*Common/widely used*	*Rarely used (vendor only)*
Application of Patches	*Regular/scheduled*	*Slow (vendor specific)*
Change Management	*Regular/scheduled*	*Legacy based – unsuitable for modern security*
Time Critical Content	*Delays are usually accepted*	*Critical due to safety*
Availability	*Delays are usually accepted*	*24 x 7 x 365 x forever*
Security Awareness	*Good in private and public sector*	*Generally poor*
Security Testing/Audit	*Scheduled and mandated*	*Occasional testing for outages / audit*
Physical Security	*Secure*	*Remote and unmanned*

Source: Department of Homeland Security

Top 10 Vulnerabilities of ICS (1)

1. ***Inadequate policies, procedures, and security culture.***
2. ***Inadequately designed control system networks that lack sufficient defence-in-depth mechanisms.***
3. ***Remote access to the control system without appropriate access control.***
4. ***System administration mechanisms and software used in control systems are not adequately scrutinized or maintained.***
5. ***Use of inadequately secured WiFi wireless communication for control.***

Source: NERC Top 10 Vulnerabilities of Control Systems

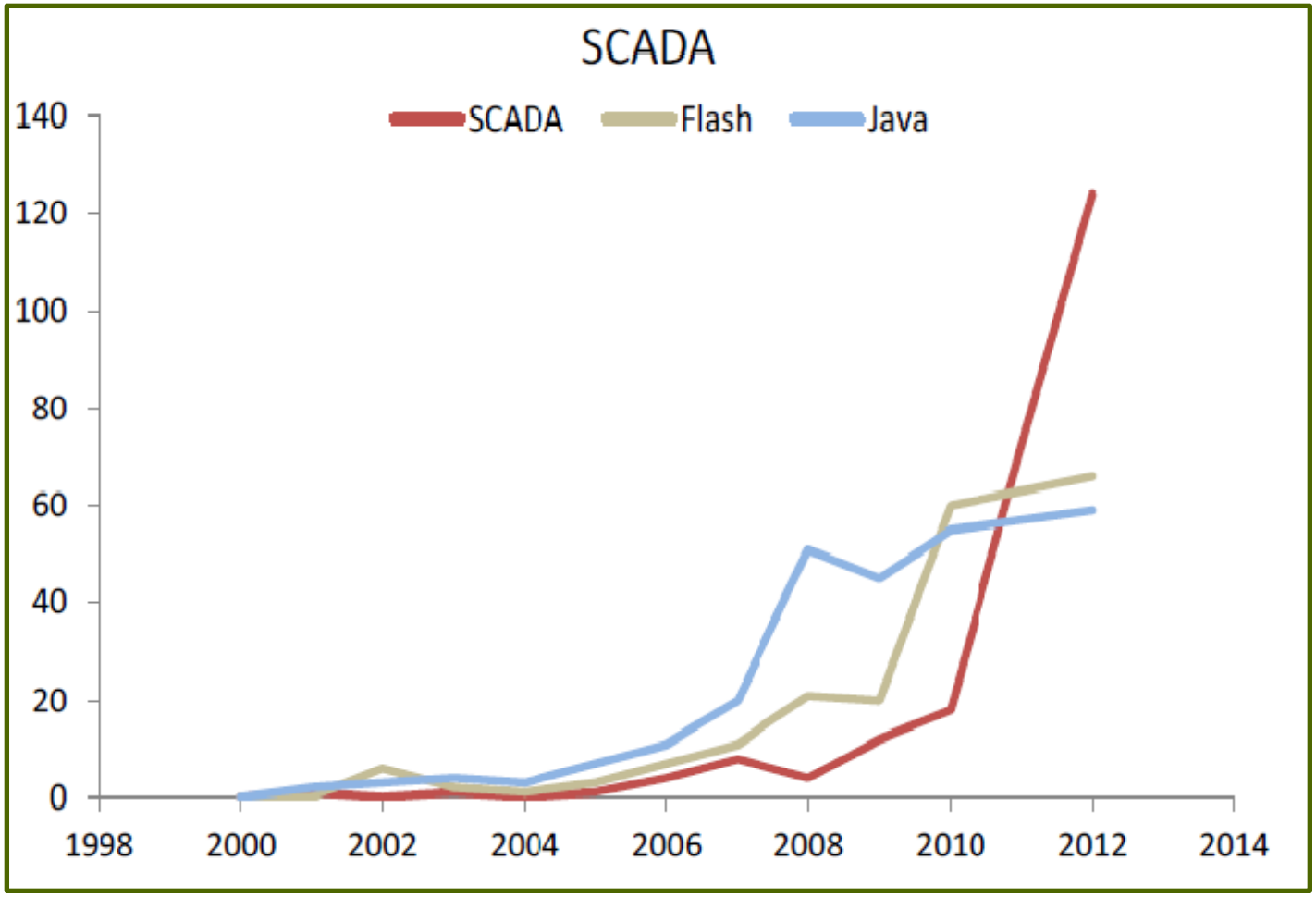
Top 10 Vulnerabilities of ICS (2)

6. ***Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes.***
7. ***Insufficient application of tools to detect and report on anomalous or inappropriate activity.***
8. ***Unauthorized or inappropriate applications or devices on control system networks.***
9. ***Control systems command and control data not authenticated.***
10. ***Inadequately managed, designed, or implemented critical support infrastructure.***

Source: NERC Top 10 Vulnerabilities of Control Systems

ICS/SCADA vulnerability disclosures

ICS/SCADA vulnerability disclosures increased more than 600% since 2010 and almost doubled from 72 in 2011 to 124 in 2012. These 124 vulnerabilities affect the products of 49 vendors; the top 20 are listed in Table 3.



Source: NSS Labs, Inc. "VULNERABILITY THREAT TRENDS" by Stefan Frei, Ph.D.

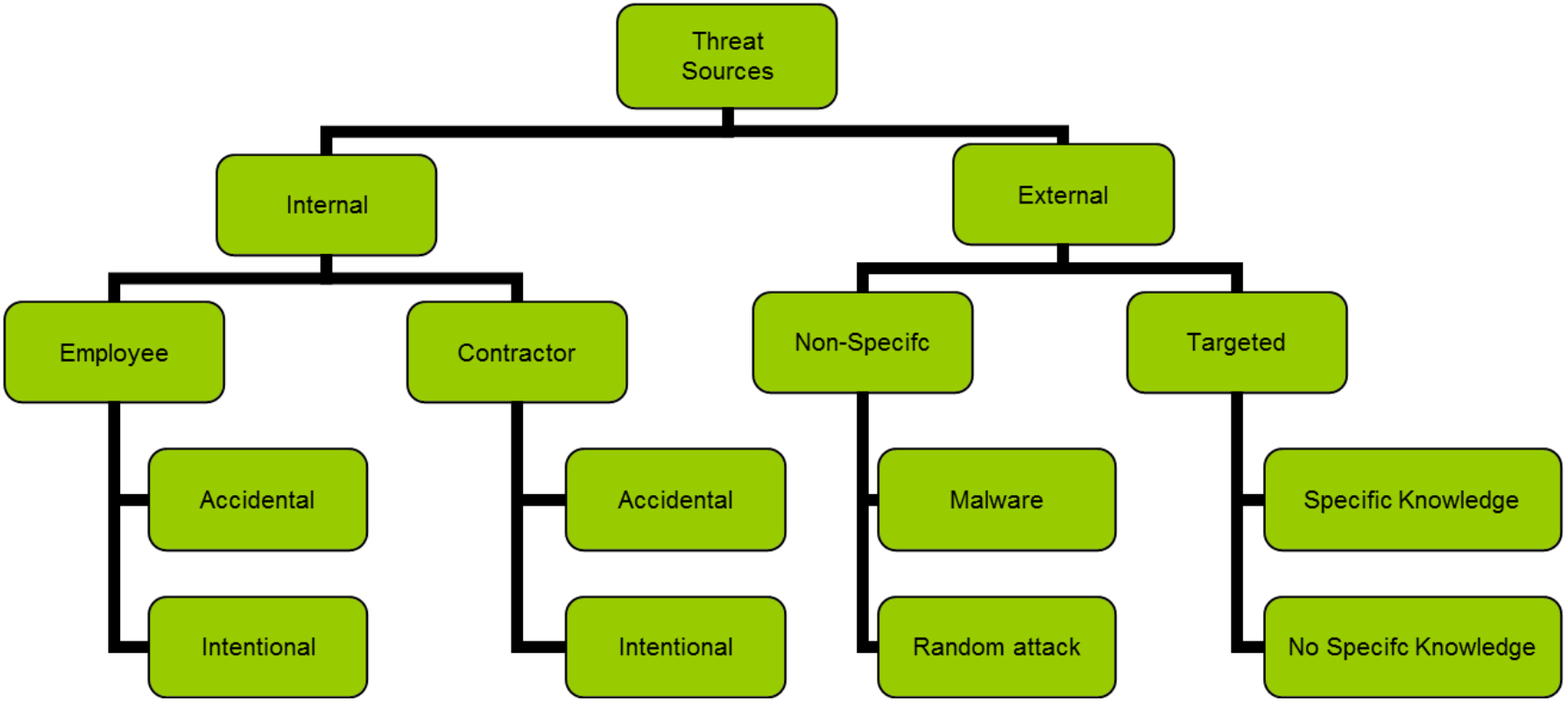
ICS/SCADA vulnerability disclosures

ICS/SCADA vulnerability disclosures increased more than 600% since 2010 and almost doubled from 72 in 2011 to 124 in 2012. These 124 vulnerabilities affect the products of 49 vendors. The top 20 are listed in the table below:

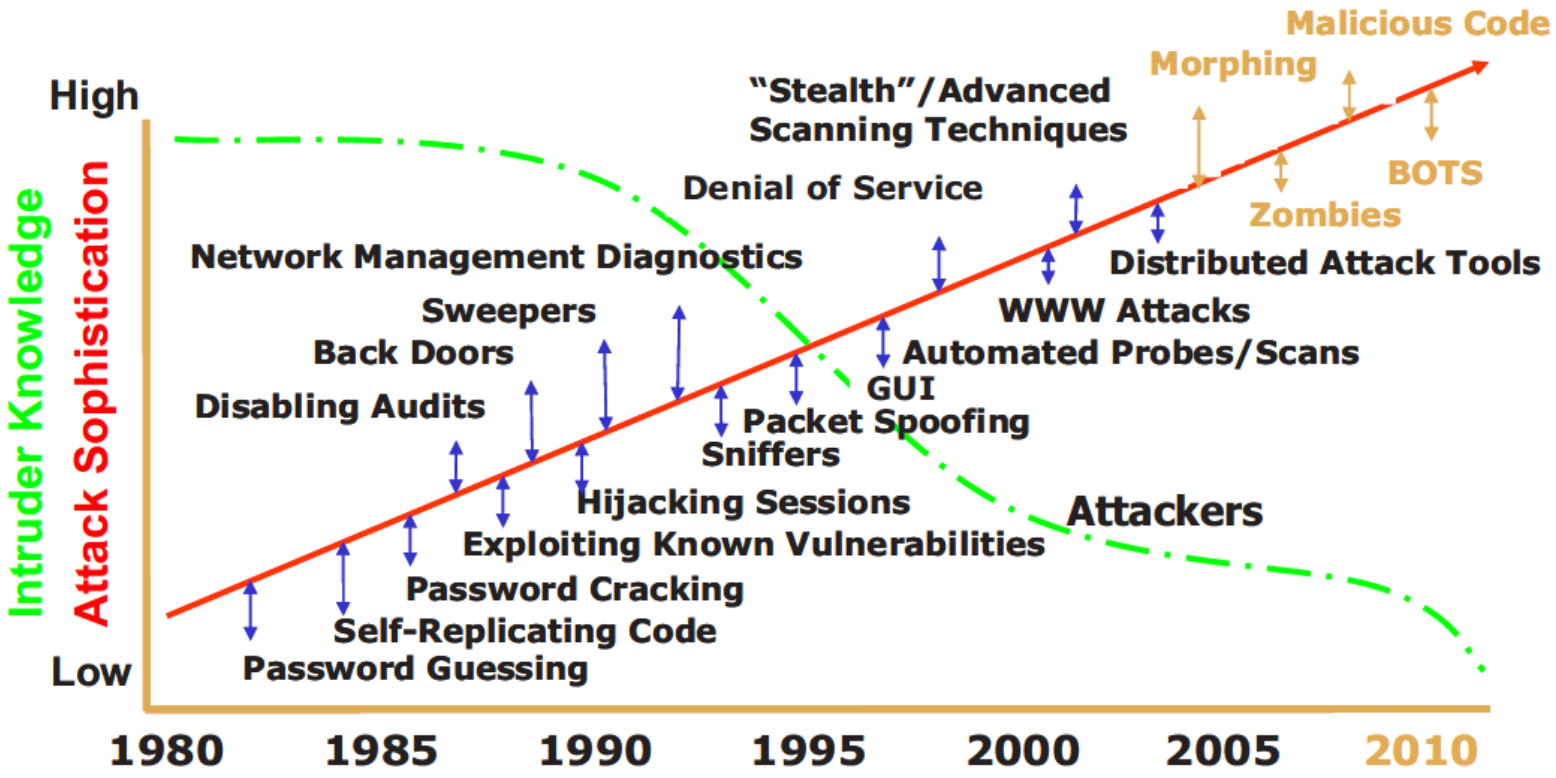
#	Vendor	CVEs	#	Vendor	CVEs
1	Siemens	31	11	Cogentdatahub	6
2	Advantech	24	12	Cisco	6
3	Invensys	16	13	Ecava	6
4	GE	12	14	Indusoft	6
5	Rockwell Automation	11	15	Intellicom	6
6	Wellintech	11	16	Koyo	5
7	Sielcosistemi	10	17	Iconics	5
8	7t	10	18	Progea	5
9	Windriver	7	19	Measuresoft	5
10	Schneider-Electric	6	20	Areva	5

Source: NSS Labs, Inc. “VULNERABILITY THREAT TRENDS” by Stefan Frei, Ph.D.

Threat sources



The increasing complexity of threats as attackers proliferate



Source: LIPSON, H.F., Tracking and Tracing Cyber-Attacks: Technical Challanges and Global Policy Issues, Special Report CMS/SEI-2002-SR-009

Example of evolation of Likelihood

- The U.S. Department of Homeland Security is warning that a witches brew of recent events make it increasingly likely that politically or ideologically motivated hackers may launch digital attacks against industrial control systems.
- Potentially aiding would-be attackers are specialized search engines like Shodan and the Every Routable IP Project, which were designed specifically to locate online devices that may be overlooked or ignored by regular search engines. Indeed, according to Wightman, a quick search using Shodan revealed 117 vulnerable devices directly connected to the Internet, although Wightman said he suspected the computer location service could turn up far more with a more targeted search. To complicate matters further, Wightman said tools for automating the exploitation of the backdoor will soon be made available for Metasploit, a penetration testing tool used by hackers and security professionals alike

Source: http://krebsonsecurity.com/tag/every-routable-ip-project

Impact

Examples:

- ***Safety***
- ***Fraud***
- ***Compromised Privacy***
- ***Non-compliance***
- ***Availability, Reliability and Integrity***

Example of impact – A real world scenario

- ***Stuxnet,*** *2010-2014*

Target: Malicious code targeted ICS at an Iranian nuclear plant.

theguardian

Sunday 26 September 2010 20.54

Anti-Iran computer bug had powerful backers

Stuxnet computer code designed to infect industrial plants created by well-funded hackers, says Symantec Corp expert

Sagar Meghani and Nasser Karimi, Associated Press in Washington and Tehran

A powerful computer code attacking industrial facilities around the world, but mainly in Iran, was probably created by experts working for a country or a well-funded private group, according to an analysis by a leading computer security company.

The malicious code, called Stuxnet, was designed to go after several "high-value targets", said Liam O Murchu, manager of security response operations at Symantec Corp. But both O Murchu and US government experts say there is no proof it was developed to target nuclear plants in Iran, despite recent speculation from some researchers.

Creating the malicious code required a team of as many as five to 10 highly educated and well-funded hackers. Government experts and outside analysts say they haven't been able to determine who developed it or why.

The malware has infected as many as 45,000 computer systems around the world. Siemens AG, the company that designed the system targeted by the worm, said it has infected 15 of the industrial control plants it was apparently intended to infiltrate. It is not clear what sites were infected, but they could include water filtration, oil delivery, electrical and nuclear plants.

None of those infections has adversely affected the industrial systems, according to Siemens.

CBSN
CBS News. Always On.

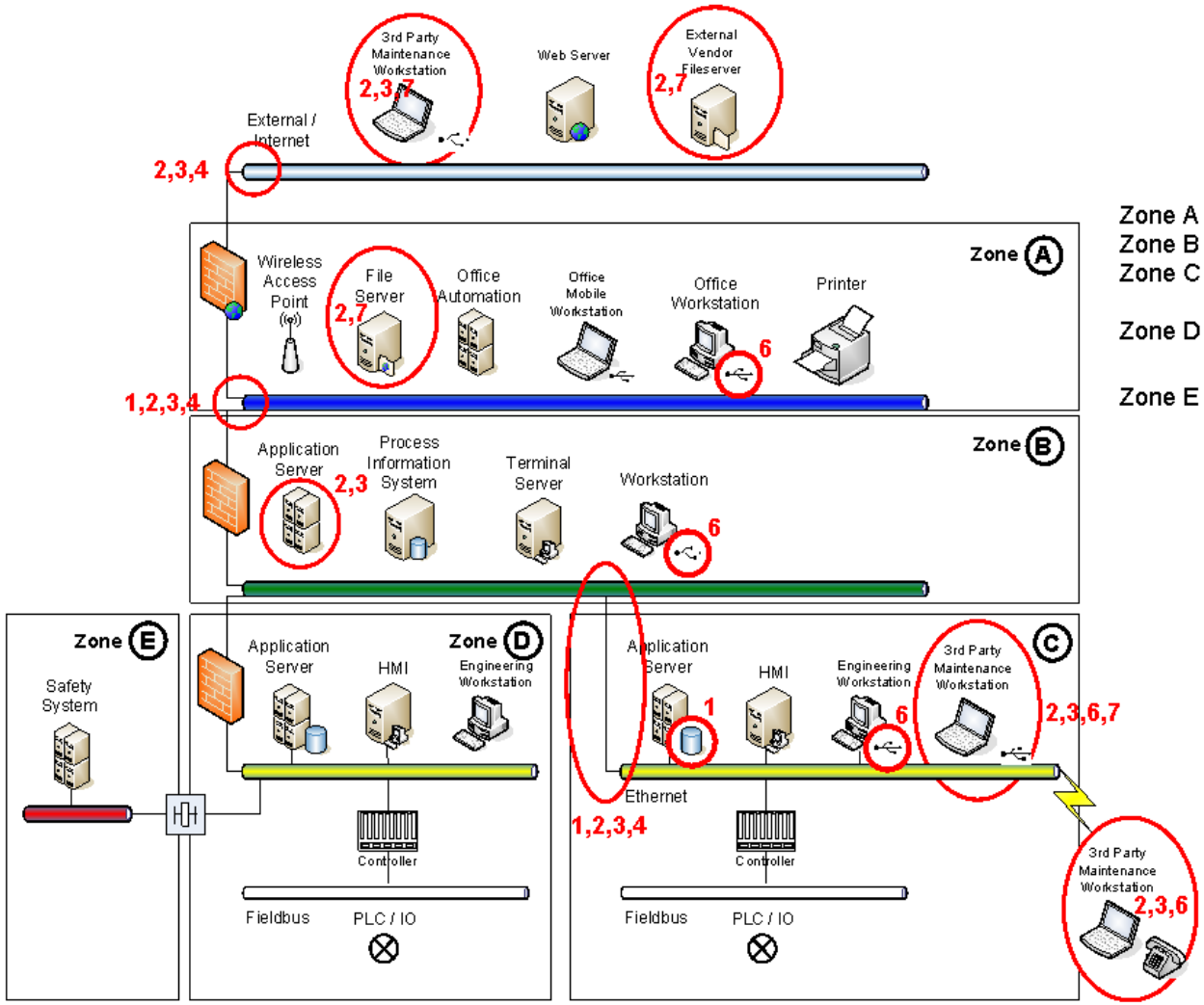
2012 Jun 04

Stuxnet: Computer worm opens new era of warfare

Computer virus's evident success in damaging Iran's nuclear facility has officials asking if our own infrastructure is safe. Steve Kroft reports.

(CBS News) The most pernicious computer virus ever known wasn't out to steal your money, identity, or passwords. So what was the intricate Stuxnet virus after? Its target appears to have been the centrifuges in a top secret Iranian nuclear facility. Stuxnet showed, for the first time, that a cyber attack could cause significant physical damage to a facility. Does this mean that future malware, modeled on Stuxnet, could target other critical infrastructure -- such as nuclear power plants or water systems? What kind of risk do we face in this country? Steve Kroft reports.

Simplified example of a plant architecture showing different attack vectors of Stuxnet[1]



Zone A : Office Automation
Zone B : Process planning
Zone C : Process control (Block 1)
(ex: insufficient security controls)
Zone D : Process control (Block 2)
(ex: sufficient security controls)
Zone E : Safety Systems
(Security control of seperation:
e.g. air gap, data diode)

1) Referring to the current publicly available information, no no claim of completeness

Show case: Attack vectors of Stuxnet[1]

1. ***Network propagation: Infecting WinCC machines via a hardcoded password***
2. ***Network propagation: Propagating through network shares***
3. ***Network propagation: Propagating through the MS08-067 Windows Server Service Vulnerability***
4. ***Propagation: Peer-to-peer communication and updates***
5. ***Propagation: Propagating through the MS10-061 Print Spooler Zero-Day Vulnerability[2]***
6. ***Removable drive propagation: LNK Vulnerability (CVE-2010-2568) or AutoRun.Inf***
7. ***Step 7 Project File Infections: S7 files, MCP files or TMP files***

1) Referring to the current publicly available information.
Source: W32.Stuxnet Dossier, 2011, Nicolas Falliere, Liam O Murchu, Eric Chien

Example of impact – a real world scenario

- **Dragonfly /Havex / Energetic Bear campaign,** 2010 to Aug 2014

Target: A campaign against defence, aviation and energy companies

INTERNATIONAL BUSINESS TIMES

State-Sponsored Hacking Group Dragonfly Attacks Thousands of US and EU Energy Firms

By Rahul R, David Gilbert
July 2, 2014 09:41

Energy Companies in America and Europe hacked by Dragonfly
Data from thousands of energy companies in the United States and Europe have been compromised in an on-going cyber espionage campaign being carried out by an Eastern European hacker group called Dragonfly.
According to a report by digital security firm Symantec, companies predominantly belonging to the energy sector were spied upon by Dragonfly during a campaign which Energy supplies could be affected in countries hit by the espionage operation.
The Symantec report provides a list of countries thought to have been the target of Dragonfly's latest cyber espionage campaign. The list includes various electricity generation companies, petroleum suppliers and industrial energy equipment providers across the United States, France, Italy, Germany, Spain, Poland and Turkey.
While a number of other countries are also said to have been hit by Dragonfly's latest digital espionage operations but no UK-based companies are mentioned in the report.

infosecurity
STRATEGY.INSIGHT.TECHNIQUE.

Dragonfly/Havex Targeting Pharmaceutical Sector

29 Sep 2014

The Dragonfly malware previously thought to be focused exclusively on the critical energy and chemical sectors is now thought to be more likely targeting pharmaceutical companies.
In the first of four reports from Belden, focused on executing the malicious code on systems that reflect real-world ICS configurations and observing the Dragonfly's impact, some factors have been uncovered that suggest that a main target for Dragonfly is the intellectual property of pharmaceutical organizations.
Over the past few years, industrial infrastructure has been identified as a key target for hackers and government-sponsored cyber-warfare, attracting some of the most sophisticated cyber-attacks on record, including Stuxnet, Flame and Duqu.
Earlier in the year, security researchers spotted a new attack campaign using infected ICS/SCADA manufacturer websites as part of watering hole attacks to commit commercial espionage and take over industrial control systems—and Dragonfly was shown to be behind it, according to F-Secure. Earlier in the year, the remote access trojan (RAT) was used in the past to target energy firms as part of campaigns by a Russian group dubbed 'Energetic Bear' by Crowdstrike.
Dragonfly, a.k.a. Havex, is significant because it is the first one of the advanced attacks since Stuxnet to have payloads that target specific industrial control system (ICS) components.

Example of impact – a real world scenario

- **Shamoon / Wiper,** August 2012

Target: A Saudi Arabian oil company, Saudi Aramco, has over 30,000 Workstations wiped

The New York Times

In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back

By NICOLE PERLROTH OCT. 23, 2012

The hackers picked the one day of the year they knew they could inflict the most damage on the world's most valuable company, Saudi Aramco.

On Aug. 15, more than 55,000 Saudi Aramco employees stayed home from work to prepare for one of Islam's holiest nights of the year — Lailat al Qadr, or the Night of Power — celebrating the revelation of the Koran to Muhammad.

That morning, at 11:08, a person with privileged access to the Saudi state-owned oil company's computers, unleashed a computer virus to initiate what is regarded as among the most destructive acts of computer sabotage on a company to date. The virus erased data on three-quarters of Aramco's corporate PCs — documents, spreadsheets, e-mails, files — replacing all of it with an image of a burning American flag.

United States intelligence officials say the attack's real perpetrator was Iran, although they offered no specific evidence to support that claim. But the secretary of defense, Leon E. Panetta, in a recent speech warning of the dangers of computer attacks, cited the Aramco sabotage as "a significant escalation of the cyber threat." In the Aramco case, hackers who called themselves the "Cutting Sword of Justice" and claimed to be activists upset about Saudi policies in the Middle East took responsibility.

infosecurity
STRATEGY.INSIGHT.TECHNIQUE.

Saudi Aramco Cyber Attacks a 'wake-up call', Says Former NSA Boss

8 MAY 2014

Former NSA boss Gen. Keith Alexander has claimed that the Shamoon malware attacks on Middle East energy company Saudi Aramco in 2012 were a "wake-up call for everybody" that could have severe repercussions for the safety of critical infrastructure networks.

The longest serving director of the much-maligned US security agency made the remarks in a marathon two-hour interview with *Australian Financial Review*, which has published the 17,500-word transcript.

In response to a question asking whether Stuxnet is a "harbinger of a new age of cyber warfare", he argued that, in fact, the Aramco attack was perhaps more noteworthy.

"The new age was not necessarily Stuxnet. It was what happened to Saudi Aramco in August 2012. That's the wakeup call, I think, for everybody," he told *AFR*.

"DDOS attackers employed a virus that infected the hard drives of over 30,000 computers at Aramco, overwriting and effectively destroying data. A similar attack on our critical infrastructure networks could have grave effects on financial markets, communication networks, and health and safety services to name a few."

Countermeasure, security controls

1. ***Identify all connections to SCADA networks.***
2. ***Disconnect unnecessary connections to the SCADA network***
3. ***Evaluate and strengthen the security of any remaining connections to the SCADA network***
4. ***Harden SCADA networks by removing or disabling unnecessary services.***
5. ***Do not rely on proprietary protocols to protect your system.***
6. ***Implement the security features provided by device and system vendors***
7. ***Establish strong controls over any medium that is used as a backdoor into the SCADA network***

…

10. ***Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security***

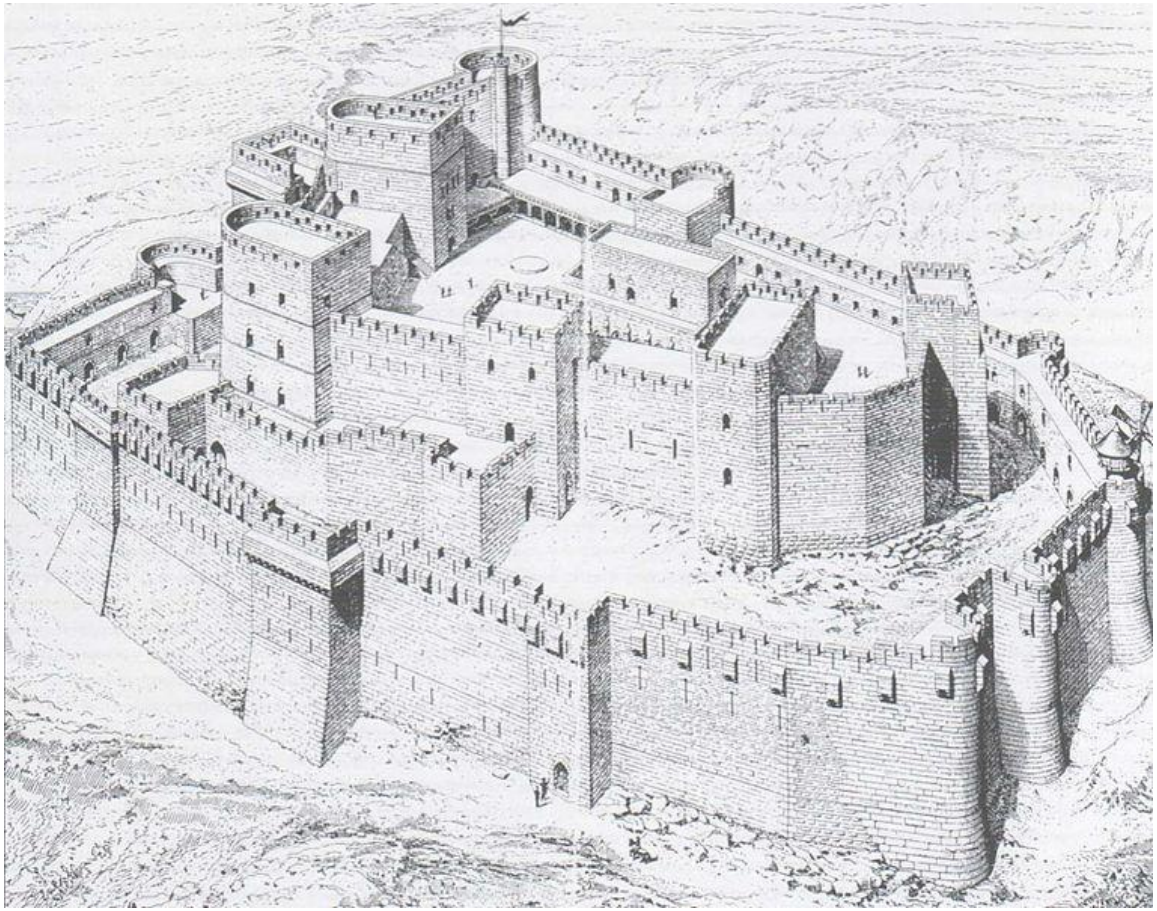
…

12. ***Clearly define cyber security roles, responsibilities, and authorities for managers,***

…

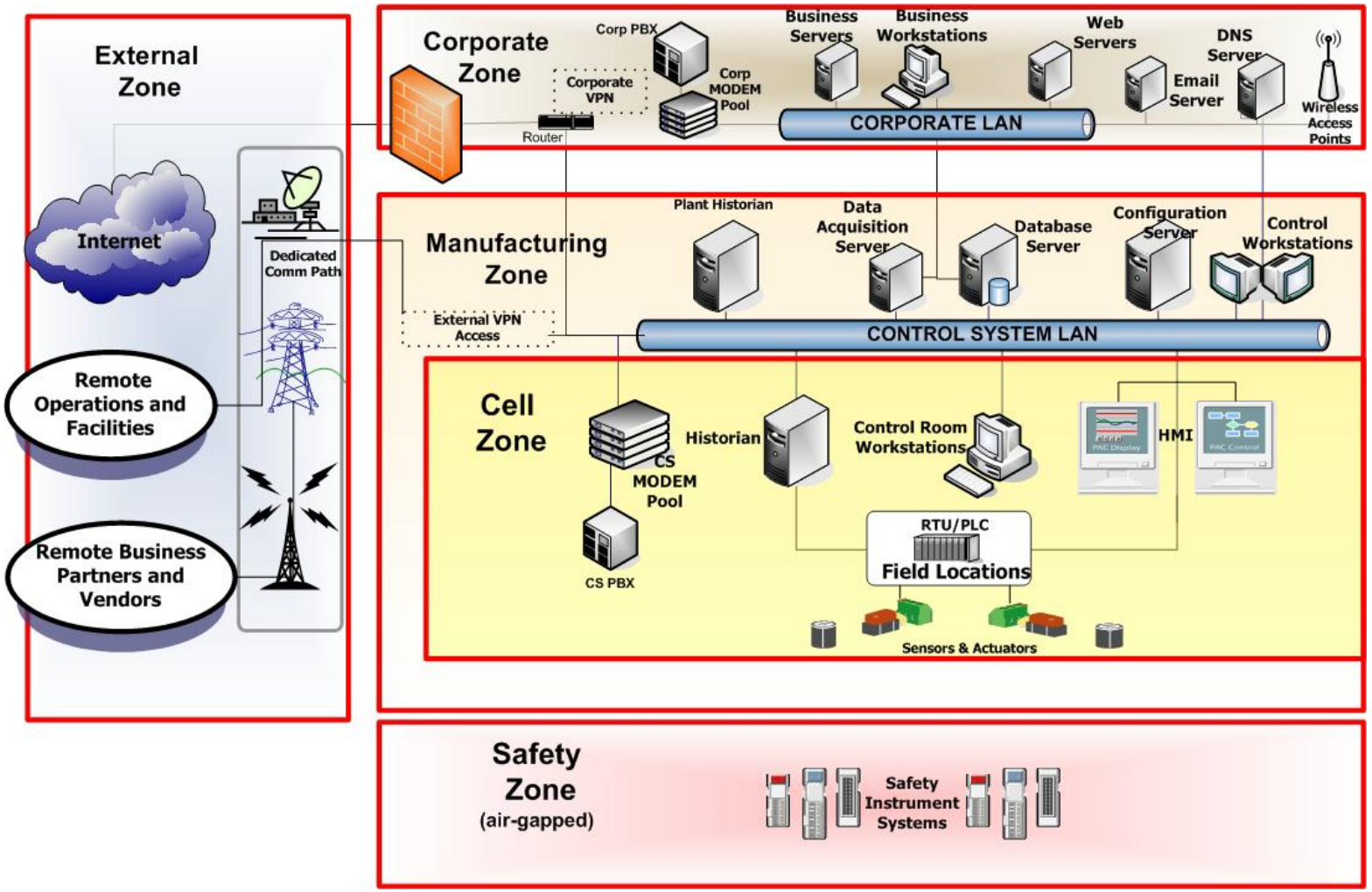
Source: 21 Steps to Improve Cyber Security of SCADA Networks , Department of Energy

Example: Graded Security Approach as an countermeasuer example based on the work of D2.31



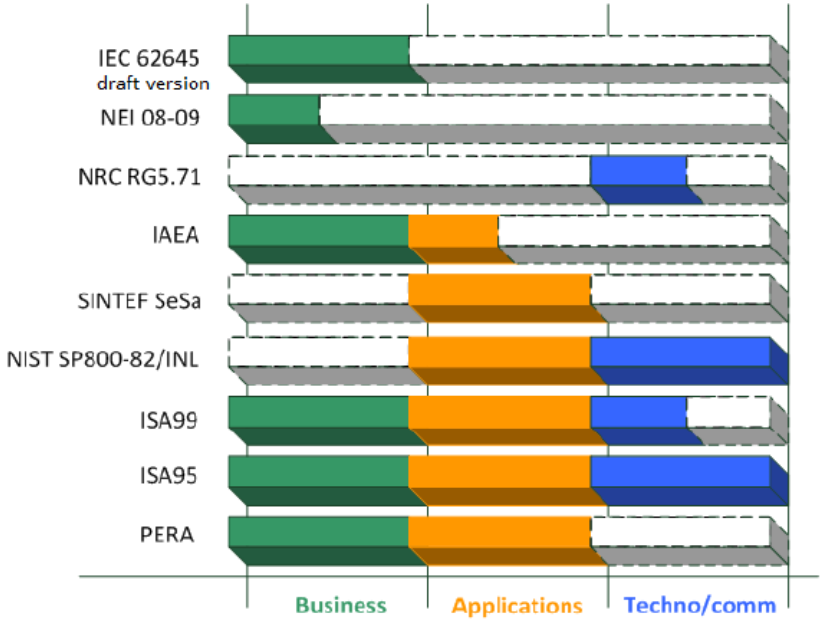
Castle *Krak des Chavaliers* in Syria

Example: Graded security approach in an EPU infrastructure



Source: Homeland security, Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defence-In-Depth Strategies

Graded security approach in Best Practice and Standard



***Business layer** is about business processes, services, functions and events of business units. In the context of a "graded security approach" the business layer is adapted to criteria like safety, operational relevance, impact to production and business processes.*

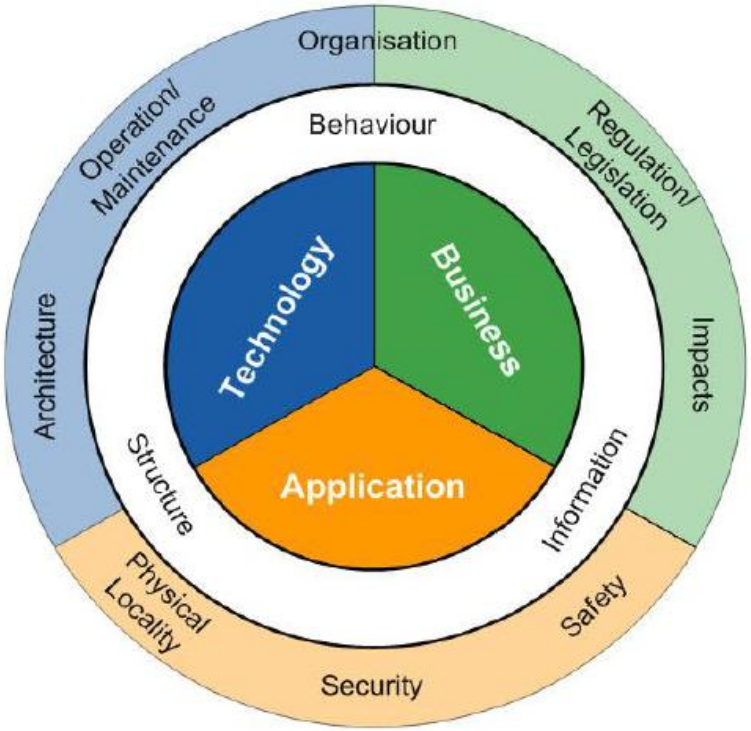
***Application layer** is about software applications that support the components in the business with application services. In the context of a "graded security approach" the application layer is adapted to criteria like application categories, e.g. Data Acquisition Server, Applications server, Historian, Database, HMI, etc.*

***Technology layer** deals with the hardware and communication infrastructure to support the application layer. In the context of a "graded security approach" the technology layer is adapted to criteria like network categories, e.g. control system LAN*

Evaluation of the graded security approach efficiency

- ***Isolation or network segmentation is an effective mitigation of infection ways between secure zones, see e.g. segment D and E. Important is the efficiency of the implemented security controls establishing the graded security approach, e.g. firewall/traffic control rules to separate zones.***
- ***The application of different security controls in different zones enables an adapted and practical implementation with a sufficient security, see e.g. USB restriction in segment D and E, but not in A and B. In segment A and B, antivirus scanner (and not represented organizational procedures) may be considered sufficient for USB-based attack processes .***
- ***Graded security approach enables the usage of best-of-breed security controls, see e.g. antivirus scanner in segment A and B, but due to system characteristic, or uncompleted implementation not in D and C.***
- ***Infringements of the graded security approach could lead to direct failures of the overall security posture, see e.g. 3rd party maintenance in segment C.***

Classification criteria categories



A reduction of classification criteria to a pure security discussion without taking surrounding elements into consideration could lead to constraints and contradiction of requirements and design principles. Experience has shown that these cause complications, time delay, unnecessary high costs or technical workarounds in the implementation, operation or maintenance phase of digital systems in a "graded security" implementation.

Conclusion: Graded security approach as a countermeasure

- ***Graded security approach is an established and effective protection methodology for an infrastructure of an EPU***
- ***Practical methodologies, guidelines, classification criteria, which reference to standards and best practices, are needed to ease the setup of a Graded security approach and to ensure compliance***
- ***The reduction of a Graded Security approach implementations only to security requirements could lead to constraints (time, quality, cost) and to contradiction of requirements and design principles.***
- ***Definition of a Graded security approach and requirements set for specific areas (e.g. in the smart grid architecture) could simplify and standardize implementation and enable connectivity and integration.***

Standards, Best Practices, Guidelines

- ***Critical Infrastructure Protection (CIP), (NERC, US):***

  A framework to improve physical and cyber security for the bulk power system of North America relating to reliability.

- ***ISA99/IEC-62443 Committee on Industrial Automation and Control Systems Security:***

  The purpose of the ISA99/IEC-62443 committee is to develop and establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure industrial automation and control systems and security practices and assessing electronic security performance.

Standards, Best Practices, Guidelines

- ***Centre for the Protection of National Infrastructure (CPNI) (UK)***

  The United Kingdoms government authority which provides protective security advice to businesses and organisations across the national infrastructure.

- ***The Department of Homeland Security (DHS) (US)***

  The DHS is a cabinet department of the United States federal government, with the primary responsibilities of protecting the United States and its territories (including protectorates) from and responding to terrorist attacks, man-made accidents, and natural disasters.

- ***National Institute of Standards and Technology (NIST) (US)***

  The NIST Special Publications 800 series present documents of general interest to the computer security community.

Examples: Standards, Best Practices, Guidelines

Type	Title	Publisher
Standard	ISA 99 - Work Products and draft versions	ISA
Best Practice	21 Steps to Improve Cyber Security of SCADA Networks	DoE
Assessment	Cyber security for Critical Infrastructure Protection	GAO
Guideline	Guide to Increased Security in Industrial Control Systems	MSB
Guideline	SP800-53 - Recommended Security Controls for Information Systems (incl. ICS)	NIST
Guideline	NISTIR-7628 - Guidelines for Smart Grid Cyber Security - Introduction	NIST
Guideline	D2.22 Cigre Technical Brochure - EPU security guidelines	CIGRE
Standard	ISO/IEC 27019:2013 Information technology Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	ISO

Cigré's role

- ***CIGRÉ Working Group D2.22***
  "Treatment of Information Security for Electric Power Utilities (EPUs)".
- ***CIGRÉ Working Group D2.31***
  "Security architecture principles for digital systems in Electric Power Utilities (EPUs)"
- ***CIGRÉ Working Group D2.38***
  "A framework for EPU operators to manage the response to a cyber-initiated threat to their critical infrastructure"
- **SCD2 Working Group WG D2.01** ***conducted a global survey in 2013 to determine the priority of operational and business information systems issues for EPUs.***

Electra article – Oct. 2014

Invited Papers

STATUS OF CYBERSECURITY

By Jens Zerbst, Liro Rinta-Jouppi, Giovanna Dondossola, Christophe Poirier, Pascal Sitbon, Dennis Holstein, John McDonald, Robert Evans

Thanks to Ludovic PIETRE-CAMBACEDES from EdF

Abstract

Today electricity generation, transmission, and distribution operations are increasingly dependent on digital systems including information systems and communication networks. This evolution introduces new vulnerabilities to the reliability of electricity supply, based on the introduction and exposure of vulnerabilities in digital systems, architectures, and communications. The paper gives an status of Cyber security including a discussion of the current risks and threats landscape EPUs are facing. The paper gives further a status of the current available assistance to EPUs including best practices, standards an practical implementation guidelines.

more automated control and thus making it impossible to operate them without digital systems.

- Smart grids and their numerous new services will rely on distributed automation and new customer participation requirements, and will therefore radically change network accesses, core architectures and the use of digital systems [1].

"This evolution introduces new vulnerabilities to the reliability of electricity supply, based on the introduction and exposure of vulnerabilities in digital systems, architectures, and communications. This situation calls for new security requirements for digital systems and the underlying architecture used in EPUs. Security requirements have to be

Current Working Group D2.40

Proposed 4 working streams:

1. ***Changing threat landscape:*** ***Rising cyber risks for EPUs based on current and next generation vulnerabilities of digital systems and new threats.***
2. ***IT security in cloud computing:*** ***Cloud computing offers new opportunities for EPUs, but at the same time potentially introduces new risks. These risks have to be assessed and mitigated in an effective manner during implementation and operation.***
3. ***IT security in remote services:*** ***In many ways remote services and mobility enable EPUs to drive cost performance, higher availability and open up new business opportunities, but they also introduce new technology and connectivity and with these, new risks which have to be assessed and mitigated.***
4. ***Cyber security regulations:*** ***The infrastructure of EPUs is considered in many countries as critical infrastructure and is subject to regulations. Due to the current threat picture, regulatory requirements are developing. Effective implementation should ensure the necessary compliance and protection level.***