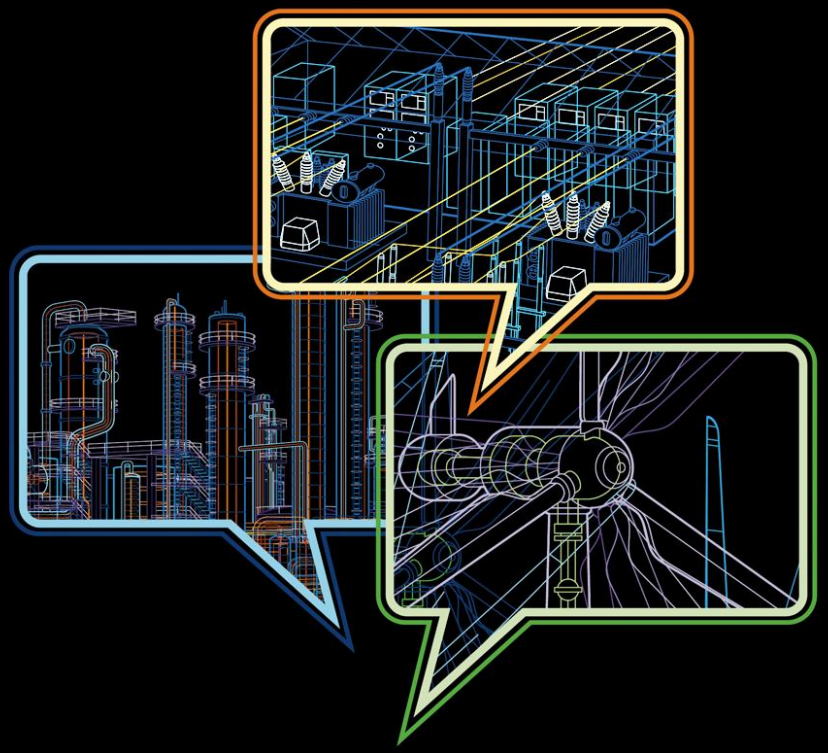


ABB Automation & Power World: April 18-21, 2011

WSE-103-1

Cyber security 101: What you need to know about current threats, solutions, standards and more

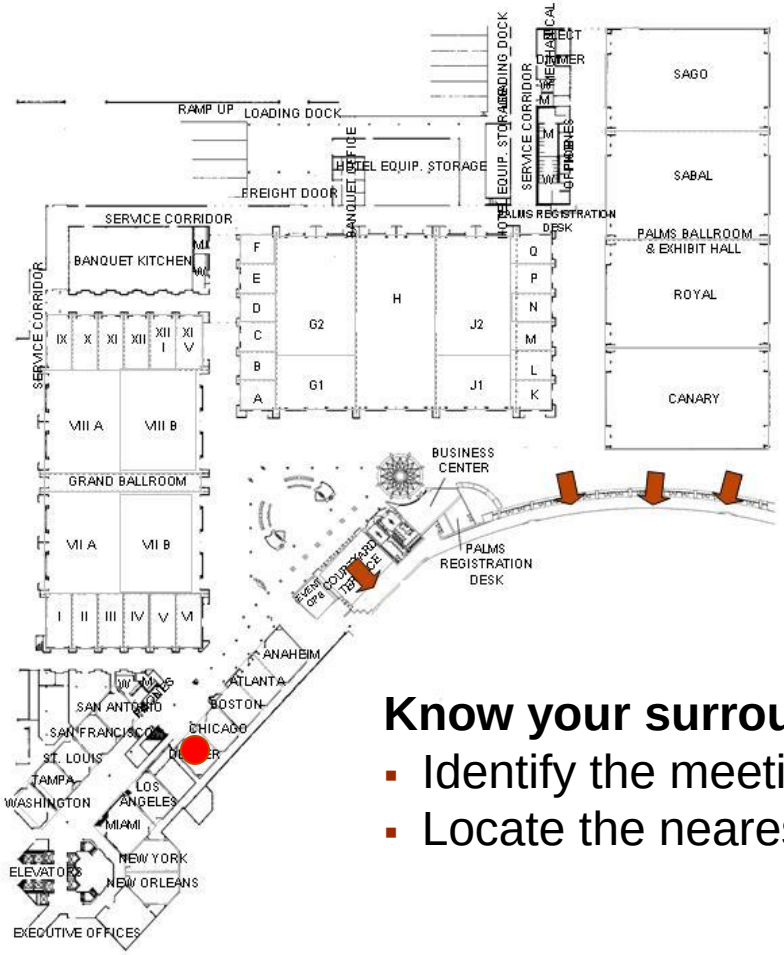
WSE-103-1
Cyber security 101: What you need to know about current threats, solutions, standards and more

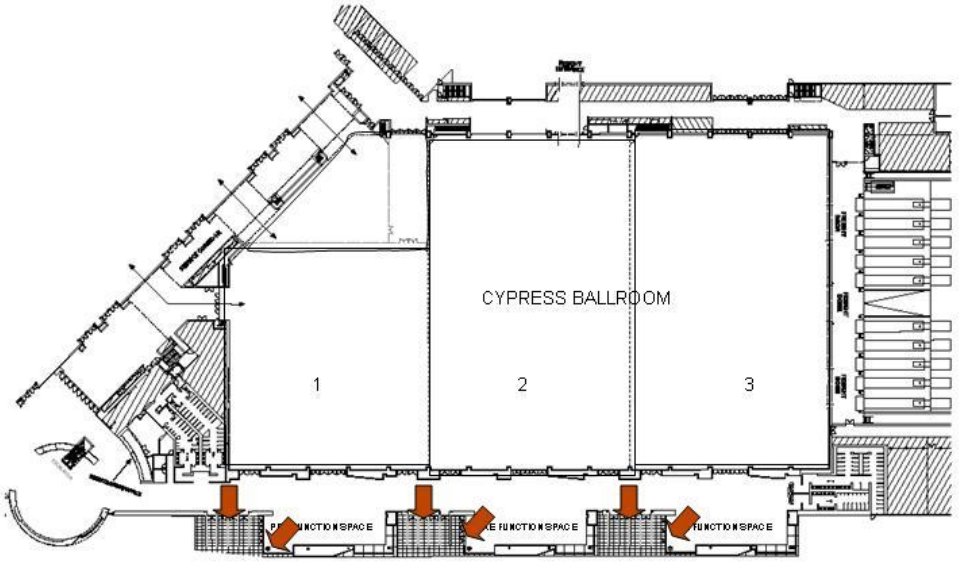
- Speaker name: Bart de Wijs
- Speaker title: Head of Cyber Security PS/PP
- Company name: ABB
- Location: The Netherlands

Your safety is important to us
Please be aware of these emergency procedures

- In the event of an emergency please dial ext. 55555 from any house phone. Do not dial 9-1-1.
- In the event of an alarm, please proceed carefully to the nearest exit. Emergency exits are clearly marked throughout the hotel and convention center.
- Use the stairwells to evacuate the building and do not attempt to use the elevators.
- Hotel associates will be located throughout the public space to assist in directing guests toward the closest exit.
- Any guest requiring assistance during an evacuation should dial “0” from any house phone and notify the operator of their location.
- Do not re-enter the building until advised by hotel personnel or an “all clear” announcement is made.

Your safety is important to us
Convention Center exits in case of an emergency





Know your surroundings:

- Identify the meeting room your workshop is being held in
- Locate the nearest exit

Demand & drivers for cyber security

What is Cyber Security?

The goals of Cyber Security are

- **Availability** – avoid denial of service
- **Integrity** – avoid unauthorized modification
- **Confidentiality** – avoid disclosure
- **Authentication** – avoid spoofing / forgery
- **Authorization** – avoid unauthorized usage
- **Auditability** – avoid hiding of attacks
- **Non-repudiation** – avoid denial of responsibility

Cyber Security has

- **functional aspects** (e.g. user authentication, firewall, anti-virus)
- **quality aspects** (e.g. defense in depth, testing)

Why is cyber security relevant to control systems?

Cyber Security for industrial control systems
Actual incidents

Chasing the Night Dragon in Big-Energy IT

By Richard Adhikari
TechNewsWorld
02/14/11 6:00 AM PT

Print Version
E-Mail Article
Reprints

For years, hackers have been having their way with the IT networks of major oil, energy and petrochemical companies, according to security vendor McAfee. The firm has described the attacks as unsophisticated and sloppy, and it says most seem to originate in China. Others, however, question whether such attacks are still going on and whether they can accurately be traced to any geographic location.

Stuxnet virus targets and spread revealed

By Jonathan Fildes
Technology reporter, BBC News

A powerful internet worm repeatedly targeted five industrial facilities in Iran over 10 months, ongoing analysis by security researchers shows.

Stuxnet, which came to light in 2010, was the first-known virus specifically designed to target real-world infrastructure, such as power stations.

Security firm Symantec has now revealed how waves of new variants were launched at Iranian industrial facilities.

Stuxnet may have been designed to target Iran's nuclear programme

THE WALL STREET JOURNAL.
WSJ.com

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

CIA: Hackers demanding cash disrupted power

Electrical utilities in multiple overseas cities affected
By Ted Bridis
The Associated Press
updated 6:06 p.m. ET, Fri., Jan. 18, 2008

WASHINGTON - Hackers literally turned out the lights in multiple cities after breaking into electrical utilities and demanding extortion payments before disrupting the power, a senior CIA analyst told utility engineers at a trade conference.

Cyber Security for Power Systems
US government

May 29, 2009

REMARKS BY THE PRESIDENT
ON SECURING OUR NATION'S CYBER INFRASTRUCTURE

" … *In short, America's economic prosperity in the 21st century will depend on cybersecurity.*

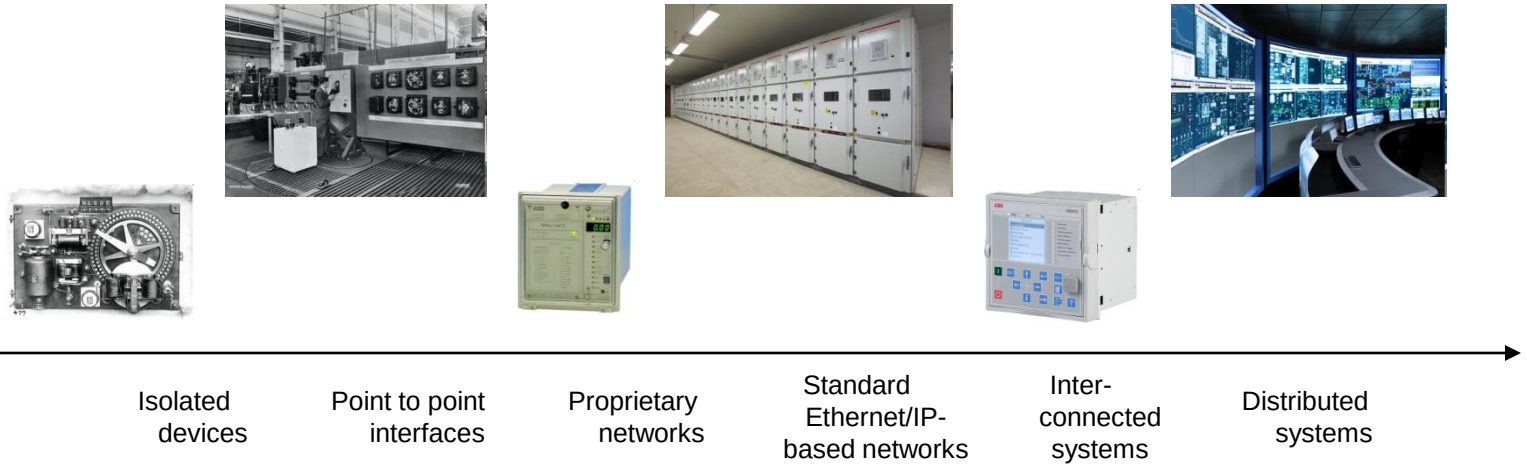
And this is also a matter of public safety and national security. We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control. Yet we know that cyber intruders have probed our electrical grid and that in other countries cyber attacks have plunged entire cities into darkness. …"

"But we do say -- even if an award scored 'A' grades on all aspects but doesn't address cyber -- we reserve right to not go forward with that grant."

Hank Kenchington, Energy Department's Office of Electric Delivery and Energy Reliability

…as the United States deploys new Smart Grid technology, the Federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks.

Why has Cyber Security become an issue?

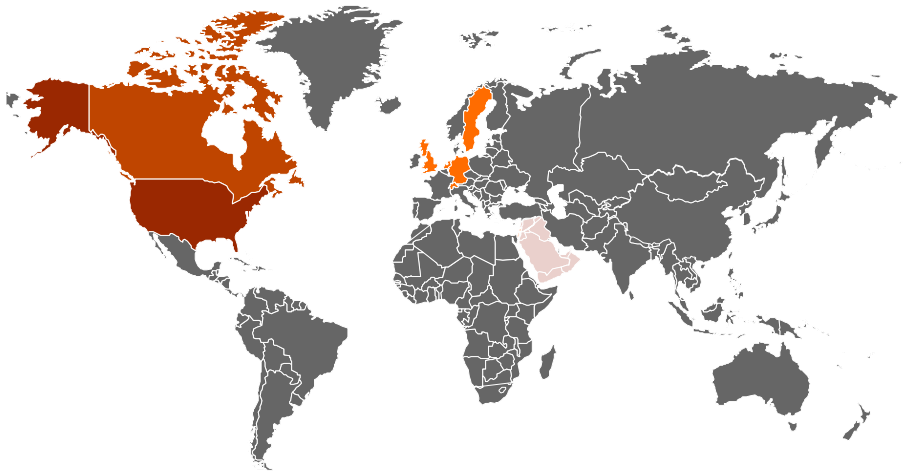


Modern automation, protection and control systems:

- **Leverage standard IT components (e.g. MS Windows, Internet Explorer)**
- **Use IP based communication protocols (“Internet technology”)**
- **Are connected to external networks**
- **Use mobile devices and storage media**

Modern control systems are specialized IT Systems

Drivers for Cyber Security
The global picture



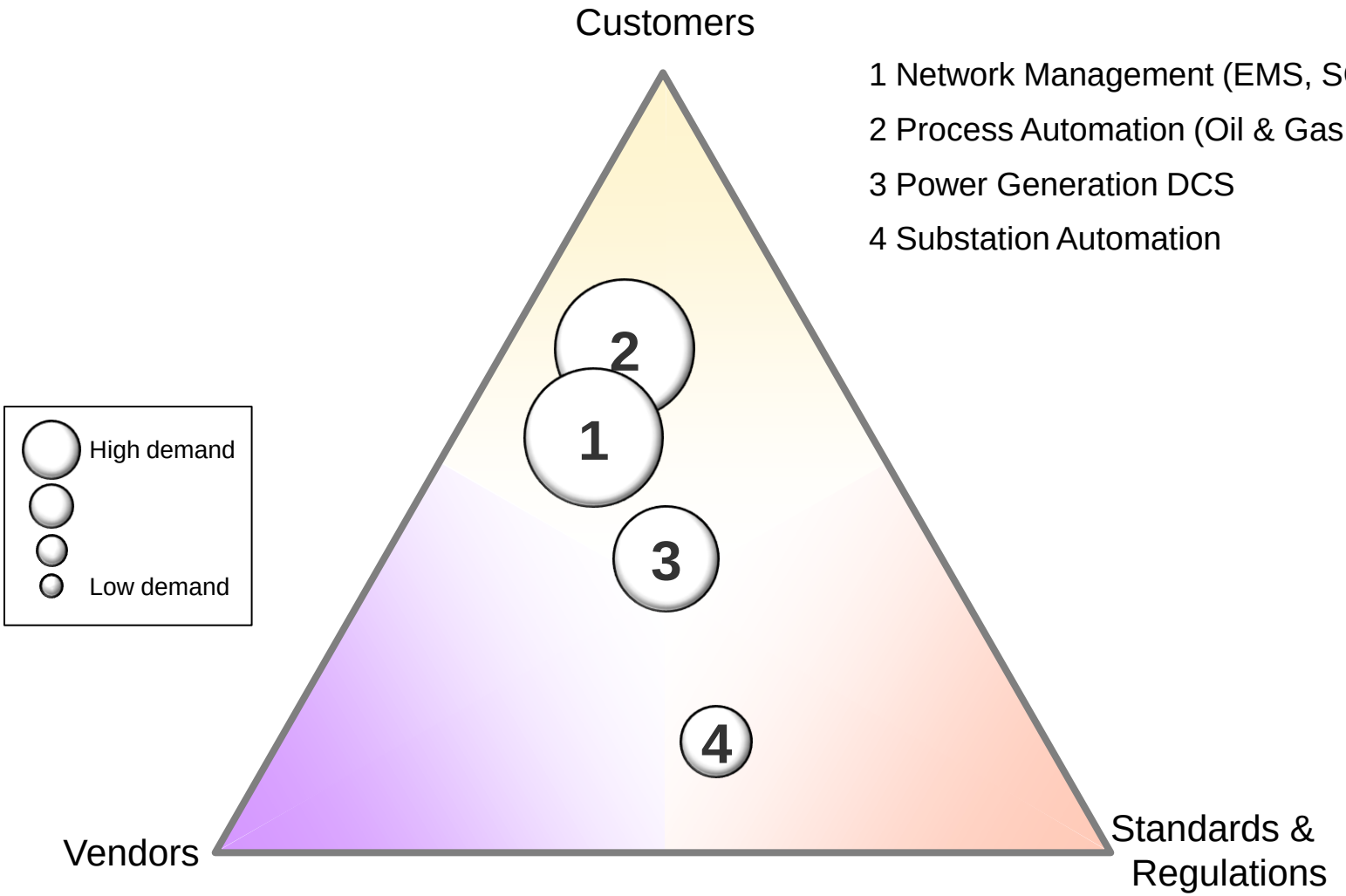
USA – biggest security demand, mainly driven by regulation and Smart Grid initiatives

Canada – similar to USA

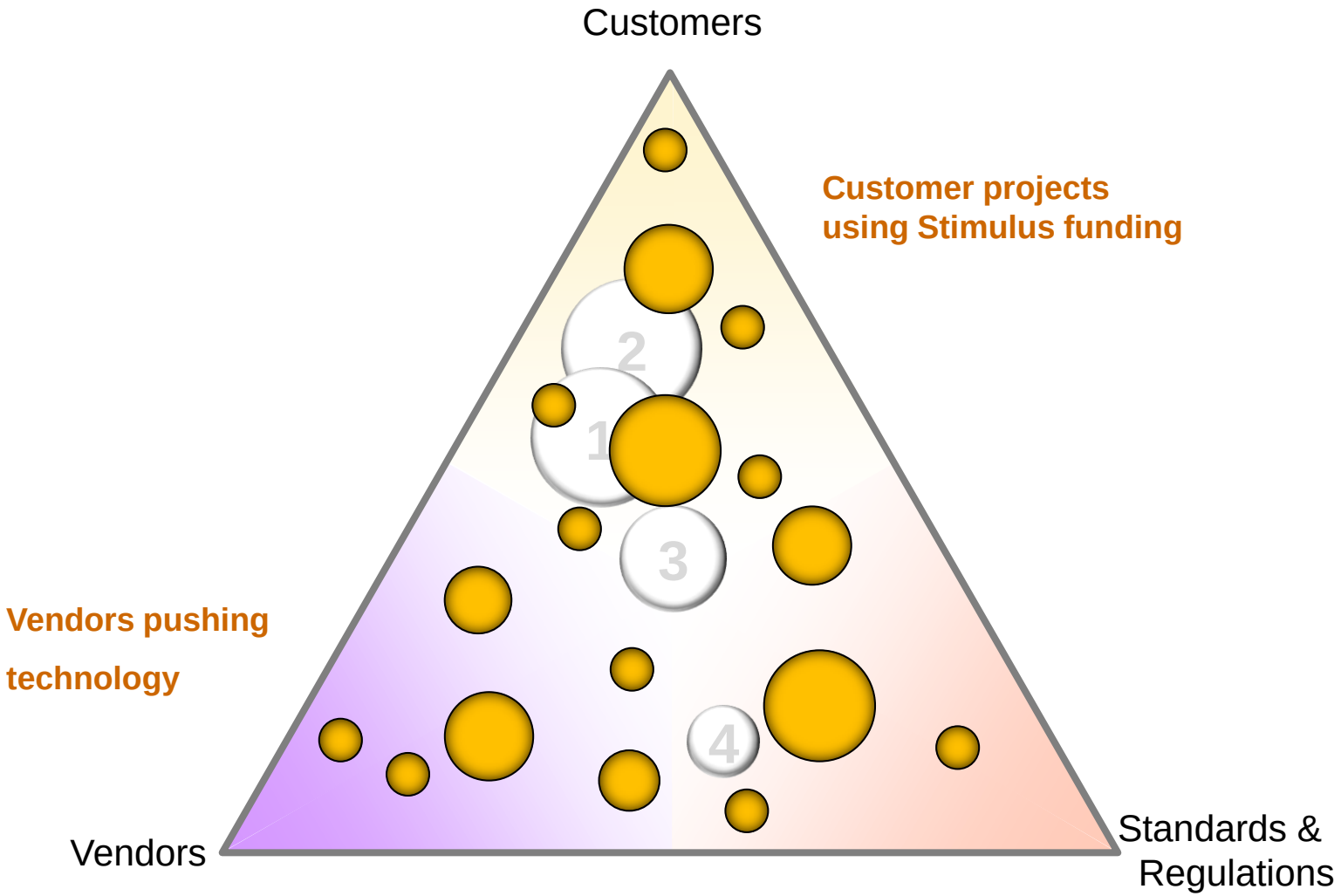
Europe – less security demand, main drivers Netherlands, Germany, Sweden, UK

Middle East – security demand still low to medium but increasing

Drivers for Cyber Security
By industry and applications



Drivers for Cyber Security
What about smart grid?



Drivers for Cyber Security
Standards, regulations, best practices, …

Committee/Document	Title	Comment
AGA / Report 12	AGA Report No. 12, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan, American Gas Association, March 2006	Detailed description see below
American Chemistry Council / Cyber Security Guideline	Guidance for Addressing Cybersecurity in the Chemical Industry, Version 3.0, May 2006	Detailed description see below
API / API 1164	SCADA Security, First Edition API Standard 1164, Pipeline SCADA Security, September 2004	Detailed description see below
API / Security Guideline	API Security Guidelines for the Petroleum Industry, April 2005	Detailed description see below
CIGRE / Security for Information Systems and Intranets in Electric Power Systems	Management of Information Security for an Electric Power Utility - On Security Domains and Use of ISO/IEC17799 Standard	Detailed description see below
CPNI / SCADA Best Practice	A good practice guide: Process Control and SCADA Security	Detailed description see below
CPNI / SCADA Firewalling	Firewall Deployment for SCADA and Process Control Networks	Detailed description see below
DHS / Catalog for Standards Developers	Catalog of Control Systems Security: Recommendations for Standards Developers	Detailed description see below
DoE / DHS Roadmap	DoE / DHS Roadmap to Secure Control Systems in the Energy Sector	Detailed description see below
DoE / ESISAC Risk Management Checklist	Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities	Detailed description see below
DoE / ESISAC VAM	Vulnerability Assessment Methodology	Detailed description see below
DoE / TSWG 21 Steps	21 Steps to Improve Cyber Security for SCADA systems	Detailed description see below

Committee/Document	Title	Comment
DoE / TSWG Securing SCADA and ICS	Securing Your SCADA and Industrial Control Systems	Detailed description see below
IEC 61400-25	Communications for monitoring and control of wind power plants	Detailed description see below
IEC 61784-4	Industrial Communications - Fieldbus Profile - Part 4: Profiles for secure communications in industrial networks	Detailed description see below
IEC 62210	Power system control and associated communications – Data and communication security	Detailed description see below
IEC 62351	Data and communication security	Detailed description see below
IEC 62443	SECURITY FOR INDUSTRIAL PROCESS MEASUREMENT AND CONTROL - Network and system security	Detailed description see below
IEEE 1402	IEEE Guide for Electric Power Substation Physical and Electronic Security	Detailed description see below
IEEE P1686	Draft Standard for Substation IED Cyber Security Standards	Detailed description see below
IEEE P1689	Trial Use Standard for Cyber Security of Serial SCADA Links and IED Remote Access	Detailed description see below
IEEE P 1711	Trial Use Standard for SCADA Serial Link Cryptographic Modules and Protocol	Detailed description see below
ISA -99 series	Security of industrial automation and control systems	Detailed description see below
ISO 13335	Information Technology - Guidelines for the Management of IT-Security	Detailed description see below
ISO 15408	Common Criteria	Detailed description see below
ISO 17799	Code of practice for information security management	precursor of ISO 27000 series and therefore not further considered
ISO 2700x	Information technology – Security techniques – Information security management systems – Requirements	Detailed description see below
NAMUR NA 115	IT-Security for Industrial Automation Systems: Constraints for measures applied in process industries	Detailed description see below
NERC CIP-002-009	Cyber Security Standard	Detailed description see below
NERC DoE / ESISAC Security Guidelines	Security Guidelines for the Electricity Sector	Detailed description see below

Committee/Document	Title	Comment
NIST PP ICC	Protection Profile for Industrial Control Centers	Detailed description see below
NIST SP 800-53	Recommended Security Controls for Federal Information Systems	Base for ISA 99 and therefore not further considered
NIST SP800-82	Guide to Industrial Control Systems (ICS) Security	Detailed description see below
NIST/PCSRF PP Field Devices	Field Device Protection Profile For SCADA Systems in Medium Robustness Environments	Detailed description see below
OLF Guideline No. 104	Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems	Detailed description see below
SEMA	Guide to Increased Security in Process Control Systems for Critical Societal Functions	Detailed description see below
VDEW M-07/2005	Zehn Schritte zur VEDIS-Sicherheit	Detailed description see below
VDI 2182	Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell	Detailed description see below
VGB-R 175	IT Sicherheit für Erzeugungsanlagen	Detailed description see below

…. and many, many more!

Technical vs. non-technical

Generic vs. application specific

End user vs. vendor centric

Drivers for Cyber Security
The most relevant efforts

		Status
NIST SGIP-CSWG	Smart Grid Interoperability Panel – Cyber Security Working Group	On-going
NERC CIP	Cyber Security regulation for North American Power Utilities	Released, On-going
IEC 62351	Data and Communications Security	Partly released, On-going
IEEE PSRC H13	Cyber Security Requirements for Substation Automation, Protection and Control Systems	On-going
IEEE 1686	IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities	Finalized
ISA S99	Industrial Automation and Control System Security	Partly released, On-going
ICSJWG	Industrial Control System Joint Working Group	On-going

What is ***really*** driving Cyber Security?
What is driving the drivers?

Currently many initiatives and activities driven by technology, solutions and FUD*

however

Control System security should be based on an understanding of risk

So, how big is the risk?

*FUD = Fear Uncertainty and Doubt

Risk

Who are the attackers?

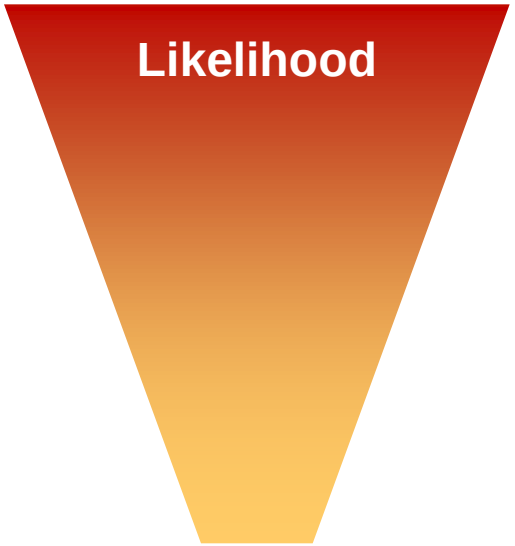
Accidents / mistakes

Rogue insider

Malware

Thieves / extortionists

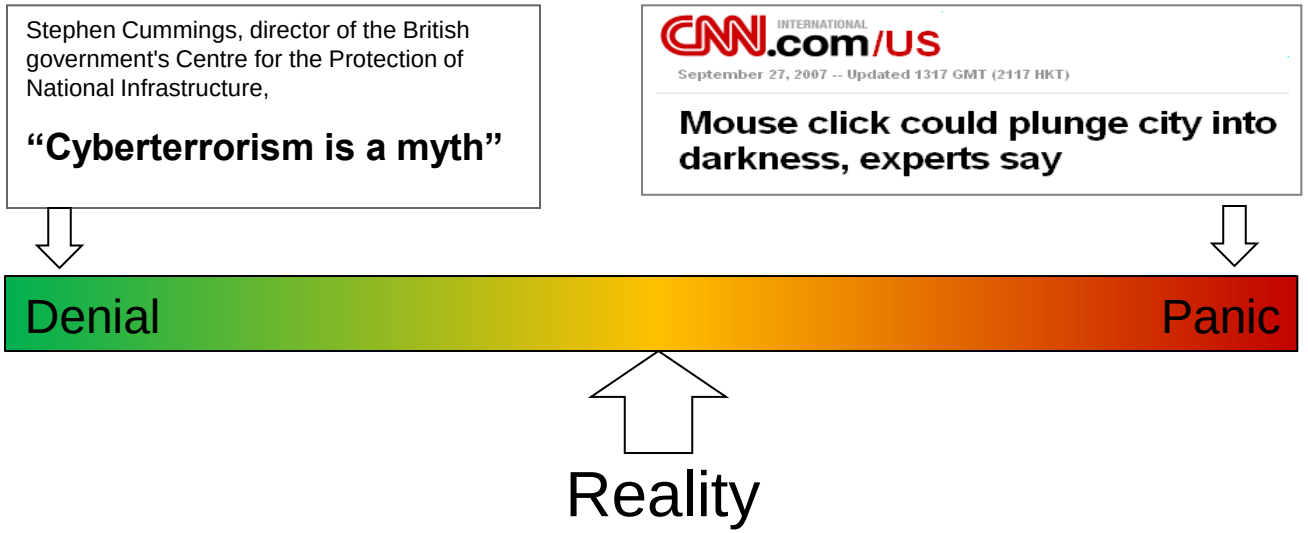
Enemies / terrorists



Bottom line is

- Likelihood is unknown
- Consequences are potentially huge

How big is the risk?



Cyber incidents are real and cyber security for industrial control systems must be taken seriously

but it is a challenge that **can** be met

Challenges

Enterprise IT vs. Control systems
A different set of challenges

	Enterprise IT	Control systems
Primary object under protection	Information	Physical process
Primary risk impact	Information disclosure, financial	Safety, health, environment, financial
Main security objective	Confidentiality	Availability
Security focus	Central Servers (fast CPU, lots of memory, …)	Distributed System (possibly limited resources)
Availability requirements	95 – 99% (accept. downtime/year: 18.25 - 3.65 days)	99.9 – 99.999% (accept. downtime/year: 8.76 hrs – **5.25 minutes**)
Problem response	Reboot, patching/upgrade, isolation	Fault tolerance, online repair

Cyber Security vs. Safety
Similar but different

Cyber Security = Safety

- Both require(d) a culture change
- Both are all about processes
- Both require training
- Both require top management support

Cyber Security ≠ Safety

- Safety is static and predictable (threats don’t change)
- Cyber Security is constantly changing (threats change)
- For Cyber Security the attacker evolves
- Safety solutions can be certified

Main challenges for end users

WHY to protect **WHAT** from **WHOM** and **HOW**

Assessment of existing systems

Making cyber security part of risk management process

Definition of security requirements for vendors & system integrators

Operation and management of security architecture

- Continuous monitoring of the infrastructure
- Regular analysis of log files
- Regular reevaluation of security architecture
- Continuous threat modeling & risk management
- Development of IT-security policies and processes

Training of employees

Evaluation and planning of “new” costs

© ABB Group

Main challenges for end users
Addressing risk

Answer the what *ifs*

- What if I cannot operate this device
- What if someone else can operate this device
- What if this information gets disclosed

- **What if someone opens this breaker**
- **What if it does not open when it should**

Don’t fall for myths

Cyber security is only an issue for TCP/IP based systems

- Serial links are just as vulnerable
- Even isolated systems have entry points
  (e.g. portable media, see the Stuxnet case)

Cyber attacks will not come from within the physical perimeter because a physical attack would be easier

- Cyber attack can be much more sophisticated
- Attack could be used as entry point into other systems
- Cyber attack can be “accidental”

Security of “isolated” systems

- Most systems are NOT really isolated
- Virtual connections always exists (e.g. portable media, laptops)

Solution approaches

Back to the basics

Accept responsibility

Security is about processes

Ignore compliance - at least at first

There is no such thing as 100% security

Security does not come for free

Use a pragmatic approach based on common best practices

Effectively use what is available

Access Control & Least-privileges

Make use of the possibility to have **personal** accounts

Make use of the ability to **change** passwords

Make use of (role based) access control to **limit** access privileges

System hardening

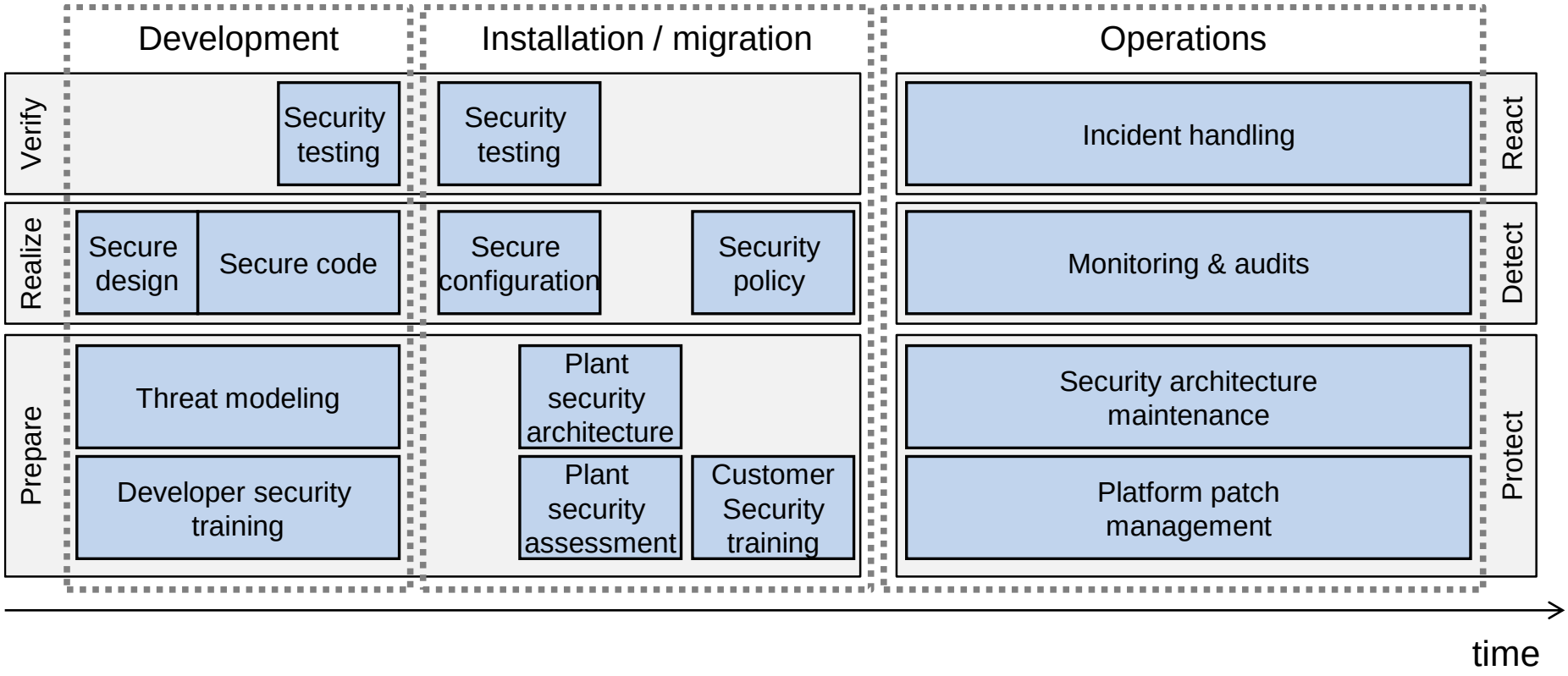
Servers and Workstations

- Removal of unused software
- Disabling unused services
- Removal unused accounts
- Change of default passwords

Network and other Devices

- Disabling unused services
- Removal unused accounts
- Change of default passwords

Cyber Security challenges in the system lifecycle



Trends & Conclusions

Trends

	Today	Trend
Regulation & Government initiatives	NERC CIP regulation for securing Bulk Electric System	Additional security regulations expected for Smart Grid and will cover all voltage level  Government organizations increase attention to securing critical infrastructure
Application focus	DCS, EMS, SCADA	Focus on end-to-end security
Business aspects	Smart Grid stimulus funding tied to sound security approach Avoiding fines associated with non-compliance (end-users)	Reduction of risk (for both end-users and vendors) 

Conclusions

Security is **not just a matter of technology**, it is primarily about people, relationships, organizations and processes working in tandem to prevent an attack

Effective security solutions require a **joint effort** by vendors, integrators, operating system providers and end users.

There is **no single solution** that is effective for all organizations and applications.

Security is a continuous process, not a product or a one-time investment

Security must be addressed with **multiple barriers** and requires both **protection** and **detection** mechanisms

Security is about risk management - perfect security is neither existent nor economically feasible

© ABB Group

Reminders
Automation & Power World 2011

- Please be sure to complete the workshop evaluation
- Professional Development Hours (PDHs) and Continuing Education Credits (CEUs):
  - You will receive a link via e-mail to print certificates for all the workshops you have attended during Automation & Power World 2011.
  - BE SURE YOU HAVE YOUR BADGE SCANNED for each workshop you attend. If you do not have your badge scanned you will not be able to obtain PDHs or CEUs.

Power and productivity
for a better world™