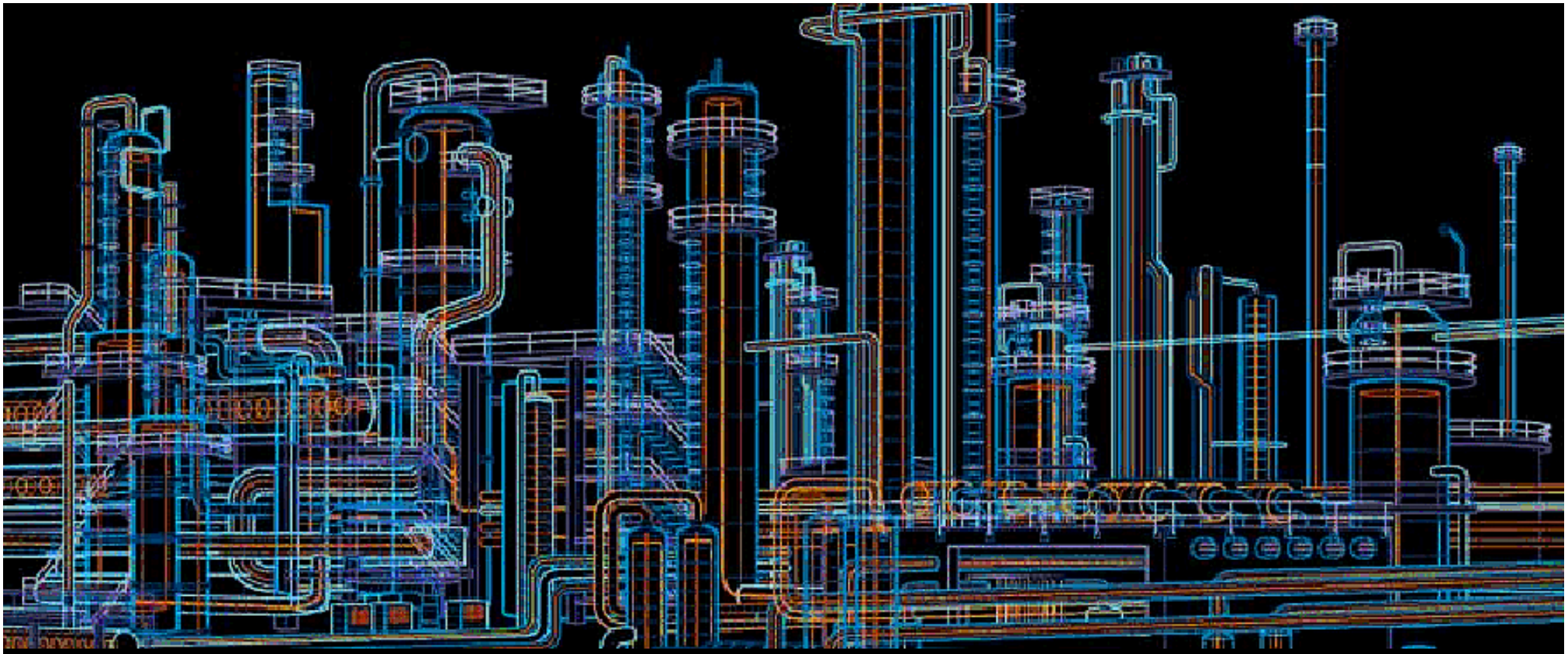


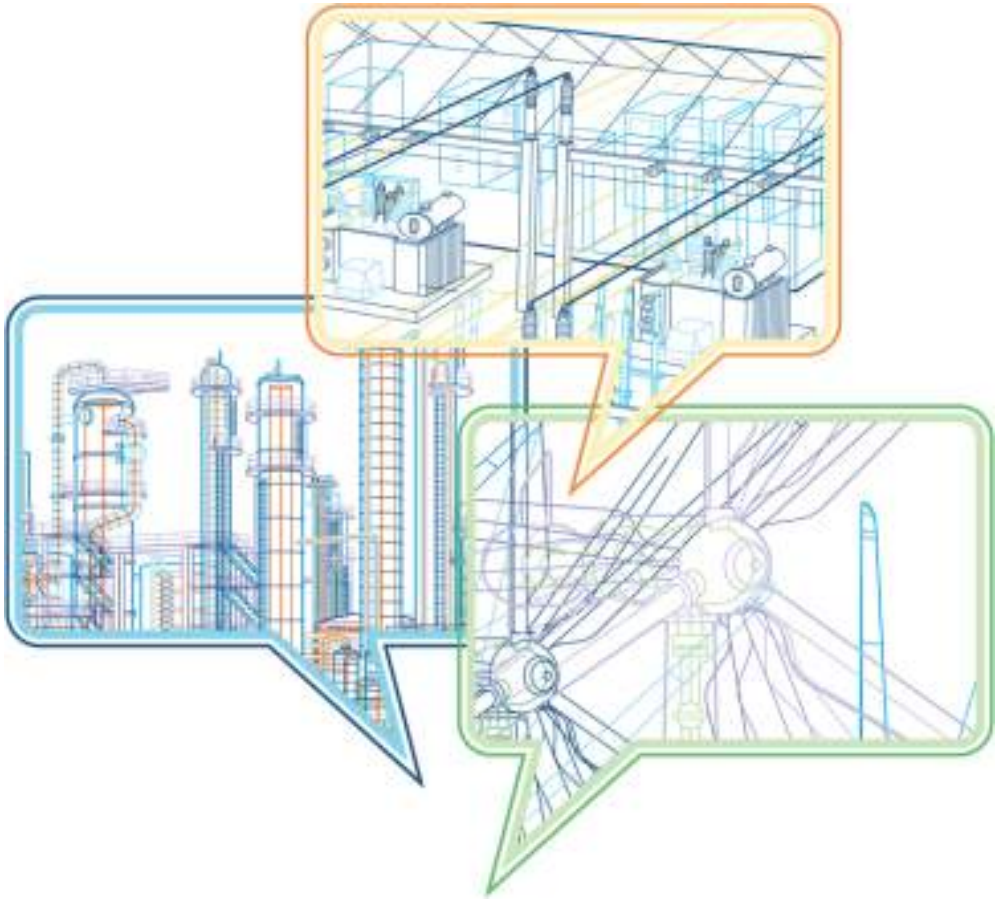
Markus Braendle, Division Cyber Security Manager, Power Systems

Cyber security

Effectively and efficiently tackling the challenges ahead

Automation & Power World 2011
April 18-21, 2011 in Orlando, Florida

Automation & Power World 2011
April 18-21, 2011 in Orlando, Florida



- Save the date for this "must attend" event!
- April 18-21, 2011
- Orlando World Center Marriott, Florida
- Over 400 hours of educational training
  - Business forum
  - Customer case studies
  - Hands-on training
  - Panel discussions
  - Technical workshops
- Earn PDHs and CEUs
- Technology & Solution Center
  - Over 70,000 sq. ft. of exhibits
- Network with your peers
- www.abb.com/a&pworld

ABB Automation & Power World
At-a-glance

400+

Educational workshops
Automation & Power World offers over 400 hours of educational workshops specifically designed to make engineers, maintenance and management more valuable to their companies.

70K

Technology & Solution Center
Over 1 ½ acres (70,000 ft²) of with nearly100 tons of electrical gear and 100's of experts ready to answer any of your questions and share the future of Automation & Power Solutions.

4,000

Connect with peers
With over 4,000 of your peers in attendance, this is a powerful opportunity to network and learn from the industry. In addition, over 45 customers will be sharing their own case studies.

Educational workshops developed for all audiences
Just a few examples

Roles

- **Engineering**
- **Management**
- **Maintenance**

Company types

- **Industrials**
- **EPCs**
- **Utilities**
- **OEMs**

- The coming wave of process safety system migration
- Implementing an alarm management strategy for a 100,000 I/O system - Case study
- Replacement and retrofit of large motors: Challenges and solutions
- Dynamic studies for large scale renewable energy integration at a Texas CREZ - Case study
- Secure commissioning of your process plant - Case study
- New arc flash mitigation technologies and techniques for a safer working environment
- Robotics 101
- A better approach to non-revenue water loss
- Electric vehicles: Are they real this time?
- Why is SIL more important than architecture?

Past attendees input

"I am impressed with the different parts of the program, the workshops and also the exhibit set-up... there is a lot of information to pick up."
Duane Souers, Georgia Pacific

"It's a great opportunity to get a lot of exposure to people and products in one week."
Pardeep Gill, Alcoa

"It is well worth the time given the opportunities to: learn from industry experts, network with peers in the same industry, learn about emerging technologies, and build excellent supplier relationships."
Sanjin Osmancevic, National Grid

Cyber security
Effectively and efficiently tackling the challenges ahead

- Speaker name: Markus Braendle
- Speaker title: Division Cyber Security Manager, Power Systems
- Company name: ABB, Inc

- Speaker name: Jim Crowley
- Speaker title: North American Sales Director, Energy Management
- Company name: Industrial Defender

Cyber Security @ Automation and Power World
April 18-21, 2011 – Orlando, Florida

Cyber Security: Technologies and Solutions

Tuesday, April 19, 2011

Session 1 – 9:30 a.m.	WSE-109-1	NERC-CIP, ISA 99 and other cyber security standards: What's new and how do they affect you
Session 2 – 11:00 a.m.	WSE-111-1	Secure your process plant operation
Session 3 – 1:30 p.m.	WSE-107-1	Cyber security: Buying a pig in a poke? How to get the security you need
Session 4 – 3:00 p.m.	WSE-110-1	Proper monitoring and configuration: Getting the most out of your cyber security investments
Session 5 – 4:30 p.m.	WSE-112-1	Security features, capabilities and support of your 800xA system

Wednesday, April 20, 2011

Session 6 – 8:00 a.m.	WPS-107-1	Cyber security in your Relion®-based protection and control solutions
Session 7 – 9:30 a.m.	CSE-102-1	Secure commissioning of your process plant: Case study
Session 8 – 11:00 a.m.	WTP-121-1	Addressing today's compliance challenges with automated solutions
Session 9 – 1:30 p.m.	CSE-101-1	Leveraging the ABB - Industrial Defender partnership to secure your control system: Case study
Session 10 – 3:00 p.m.	WSE-106-1	Cyber security in the system life cycle: ABB's commitment
Session 11 – 4:30 p.m.	PSE-108-1	Cyber security: The present state and where the future will lead

Thursday, April 21, 2011

Session 12 – 8:00 a.m.	WSE-103-1	Cyber security 101: What you need to know about current threats, solutions, standards and more
Session 13 – 9:30 a.m.	WSE-105-1	Cyber security for smart grid

Featured speakers

- Tim Roxey, NERC
- Eric Cosman, Dow Chemicals
- Brian Ahern, Industrial Defender
- Tyler Williams, Wurldtech

Agenda

Main drivers

Discussion of risk

Challenges

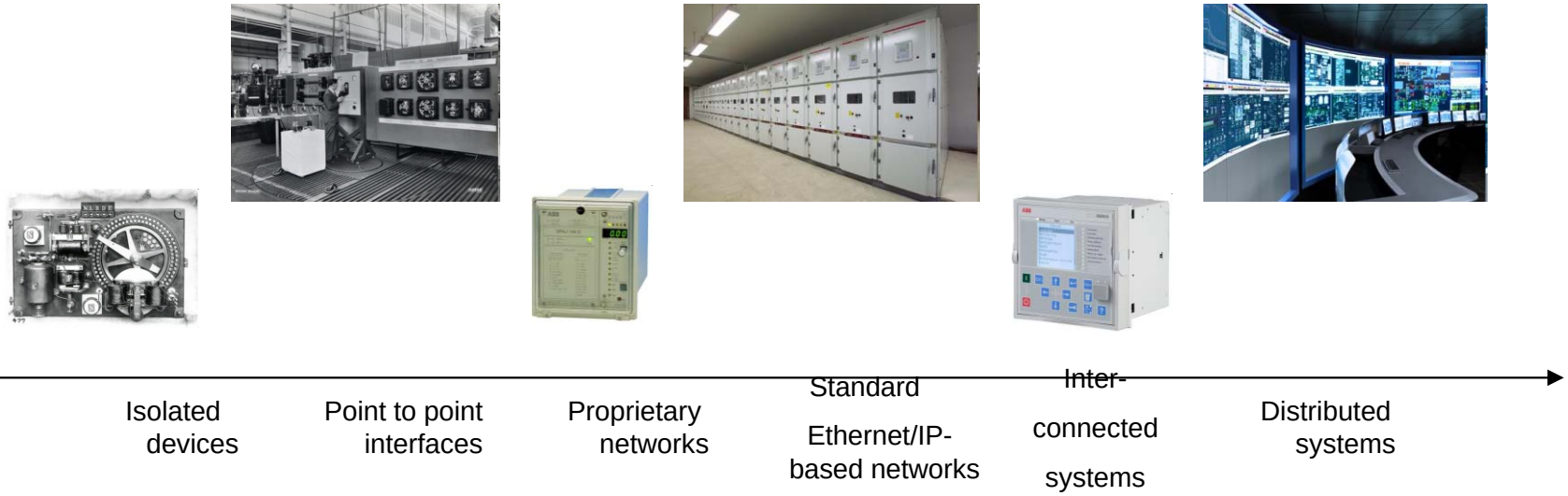
Solution approaches

Conclusions

Demand & drivers for cyber security

Why is it an issue?

Main drivers
Discussion of risk
Challenges
Solution approaches
Conclusions



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

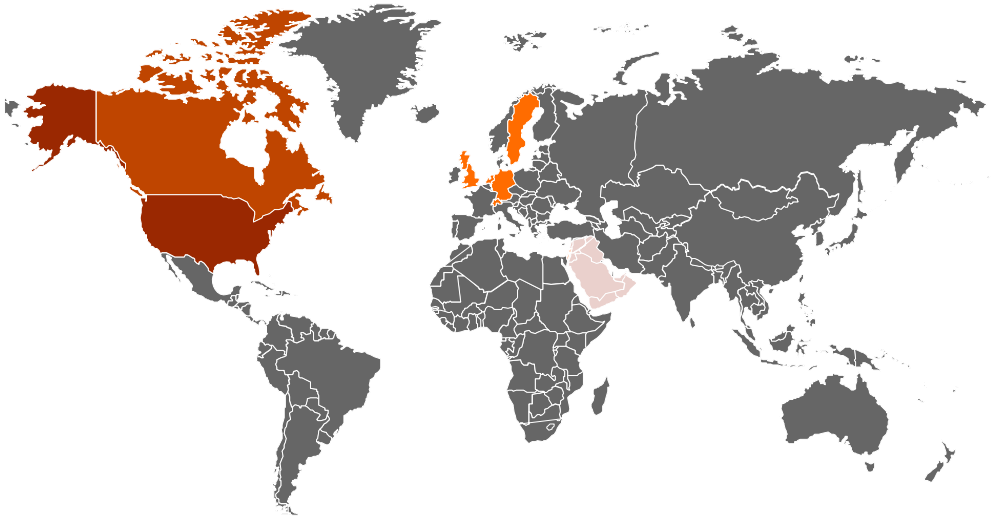
Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions



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

Canada – similar to USA

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

Middle East – security demand still low to medium but increasing

Drivers for Cyber Security
By industry and applications

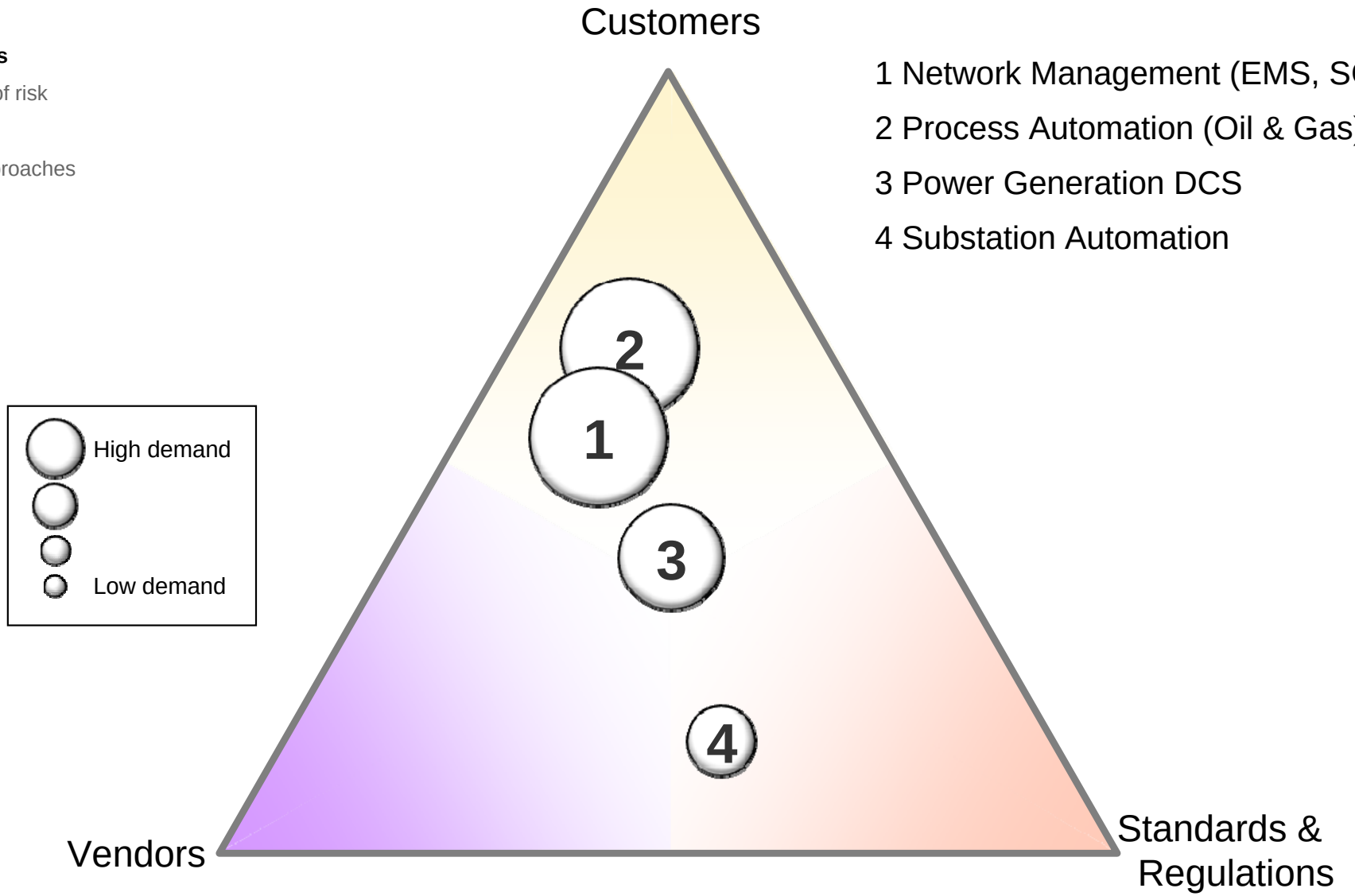
Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions



1 Network Management (EMS, SCADA)

2 Process Automation (Oil & Gas)

3 Power Generation DCS

4 Substation Automation

Drivers for Cyber Security
What about smart grid?

APW Session
WSE-105-1

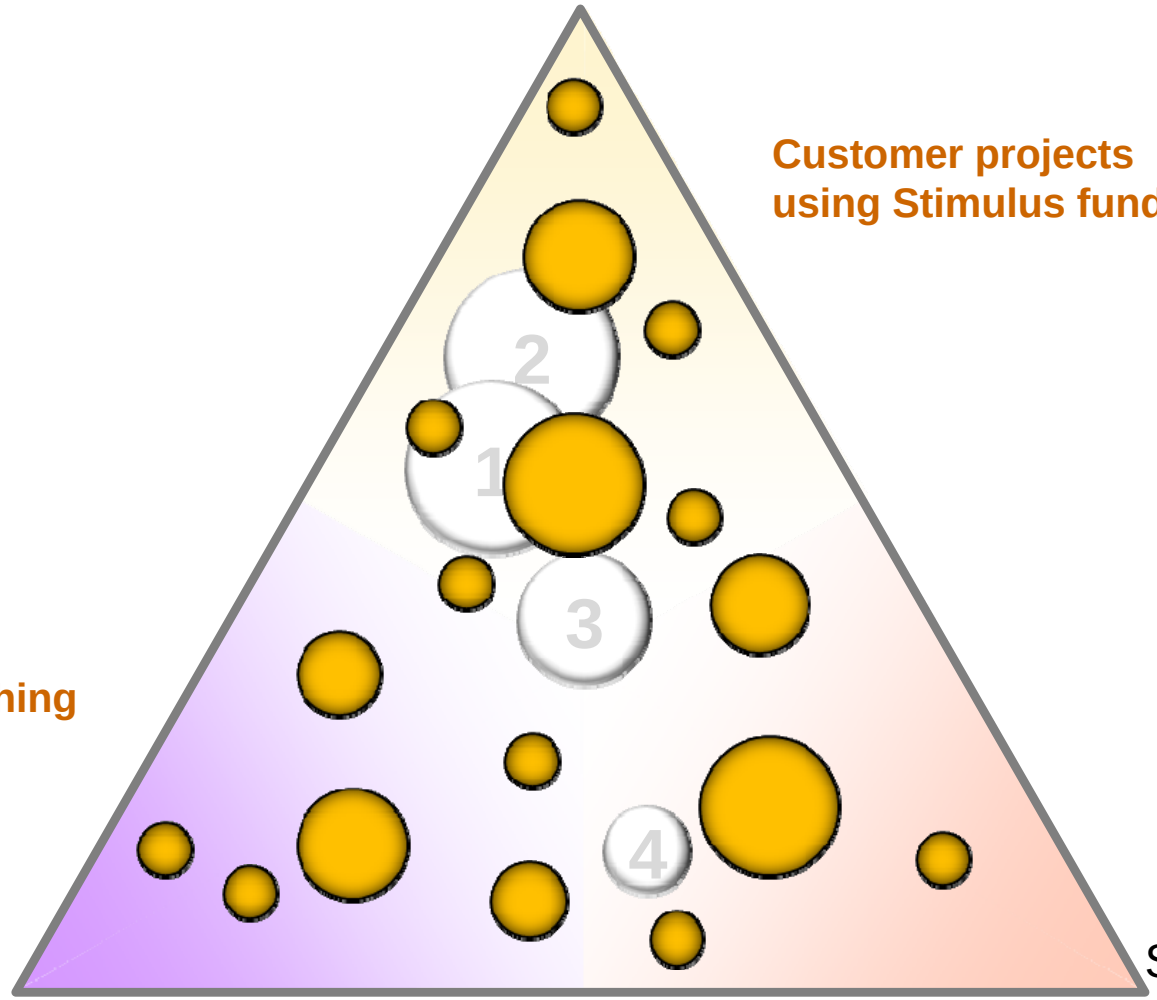
Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions



Customer projects using Stimulus funding

Vendors pushing technology

NIST CSCTG

IEEE, AMI SEC, NERC CIP

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

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

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	Roadmap 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

APW Session
WSE-109-1

		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?

Risk

Who are the attackers?

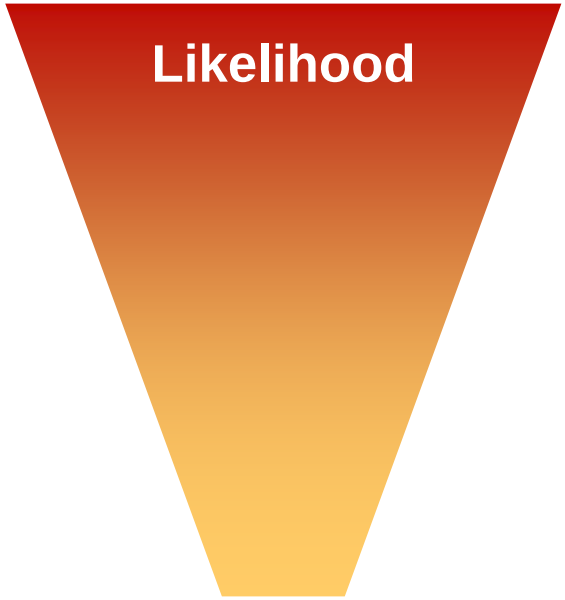
Accidents / mistakes

Rogue insider

Malware

Thieves / extortionists

Enemies / terrorists



Bottom line is

- Likelihood is unknown
- Consequences are potentially huge

How big is the risk?

Stephen Cummings, director of the British government's Centre for the Protection of National Infrastructure,

"Cyberterrorism is a myth"

CNN INTERNATIONAL .com/US

September 27, 2007 -- Updated 1317 GMT (2117 HKT)

Mouse click could plunge city into darkness, experts say

Denial — Panic

Reality

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

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)

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

- Cyber attack can be much more sophisticated
- Substation could be used as entry point into system
- 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

APW Session
WSE-103-1

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

APW Session
WSE-111-1

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

Work in teams
ABB - Industrial Defender partnership

APW Session
CSE-101-1

Why Industrial Defender?

- Global leader for industrial control systems cyber security
- Unmatched cyber security portfolio providing true defense-in-depth solutions

Benefits for end-users

- Combined know-how
- Tested and verified solutions
- Alignment of technologies
- Unified support

More efficient and effective solutions through tight integration

Industrial Defender Solutions

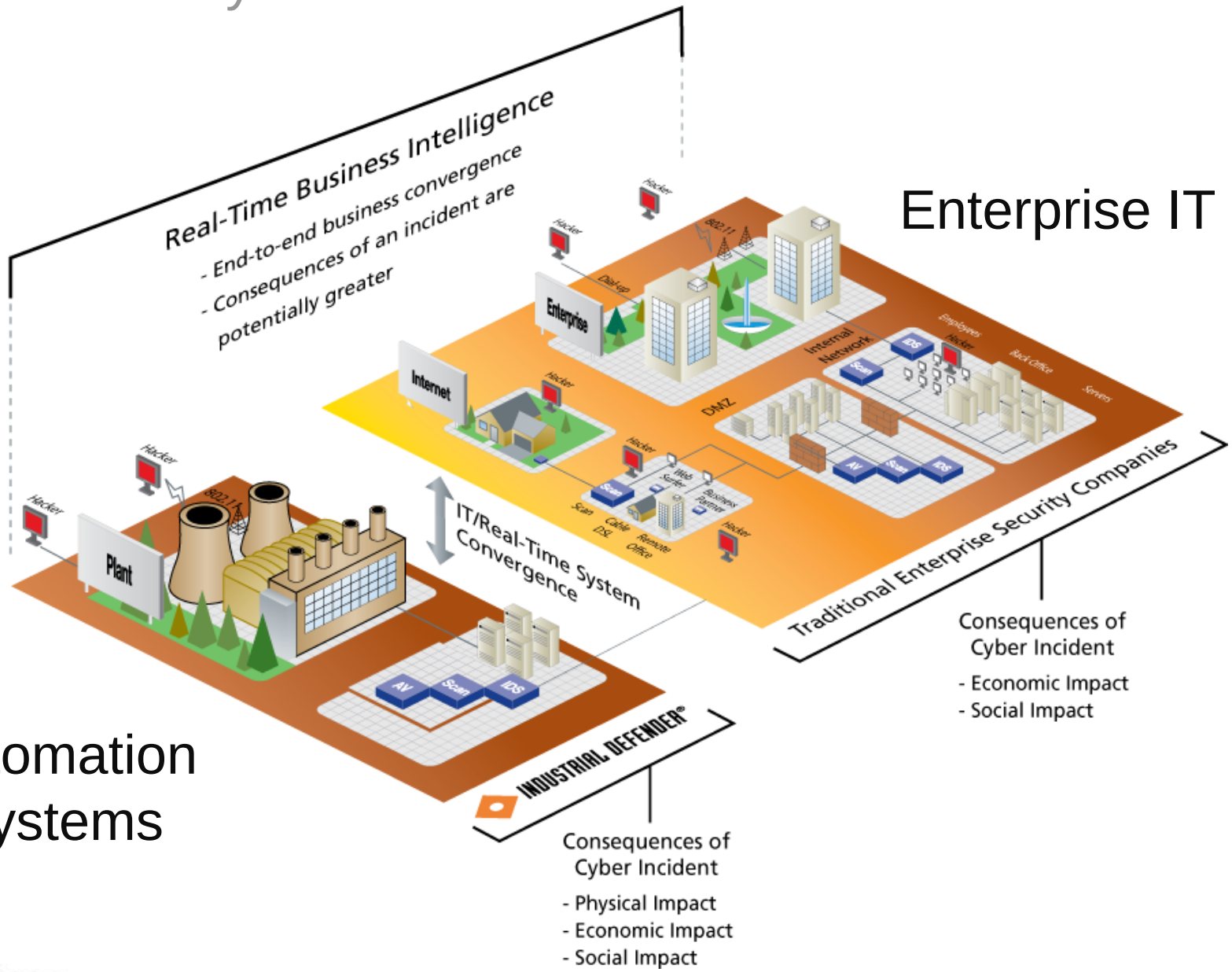
About Industrial Defender

- Exclusive focus on providing an integrated set of products and services for Automation Systems Security Management and Compliance
- Unify two challenging domains
  - Automation Systems
  - Cyber Security
- Headquartered in Boston, MA area
- 8 year focus on Automation System Security Management
- 350 customers worldwide; 10,000 product deployments; 21 countries

Reality of the Automation Systems Environment…

- Always-On Mentality (system reboots not a way of life)
- Legacy Infrastructure (low bandwidth, slower processors)
- Unique Industrial Endpoint Infrastructure (more than just clients, servers, networking devices)
- Applications lag most recent versions of O/S and Patches
- Industrial Protocols (DNP3, Modbus, IEC61850, etc)
- Application anomaly monitoring in addition to O/S anomaly monitoring

Assuring Security, Availability & Compliance of Automation Systems



Managing Control Systems Networked Devices

Automation Systems Security Management

- Network and event management
- Break / Fix (Incident response)
- Change management
- Software / patch management
- Cyber security vulnerability assessment
- Auditing and compliance

Device Interfaces and Communications

- Event / log collection
- IDS / IPS
- Configuration and patch data collection
- Remote access controls

Automation Systems Devices

Servers: PCS, SCADA, …

Work stations

Firewalls

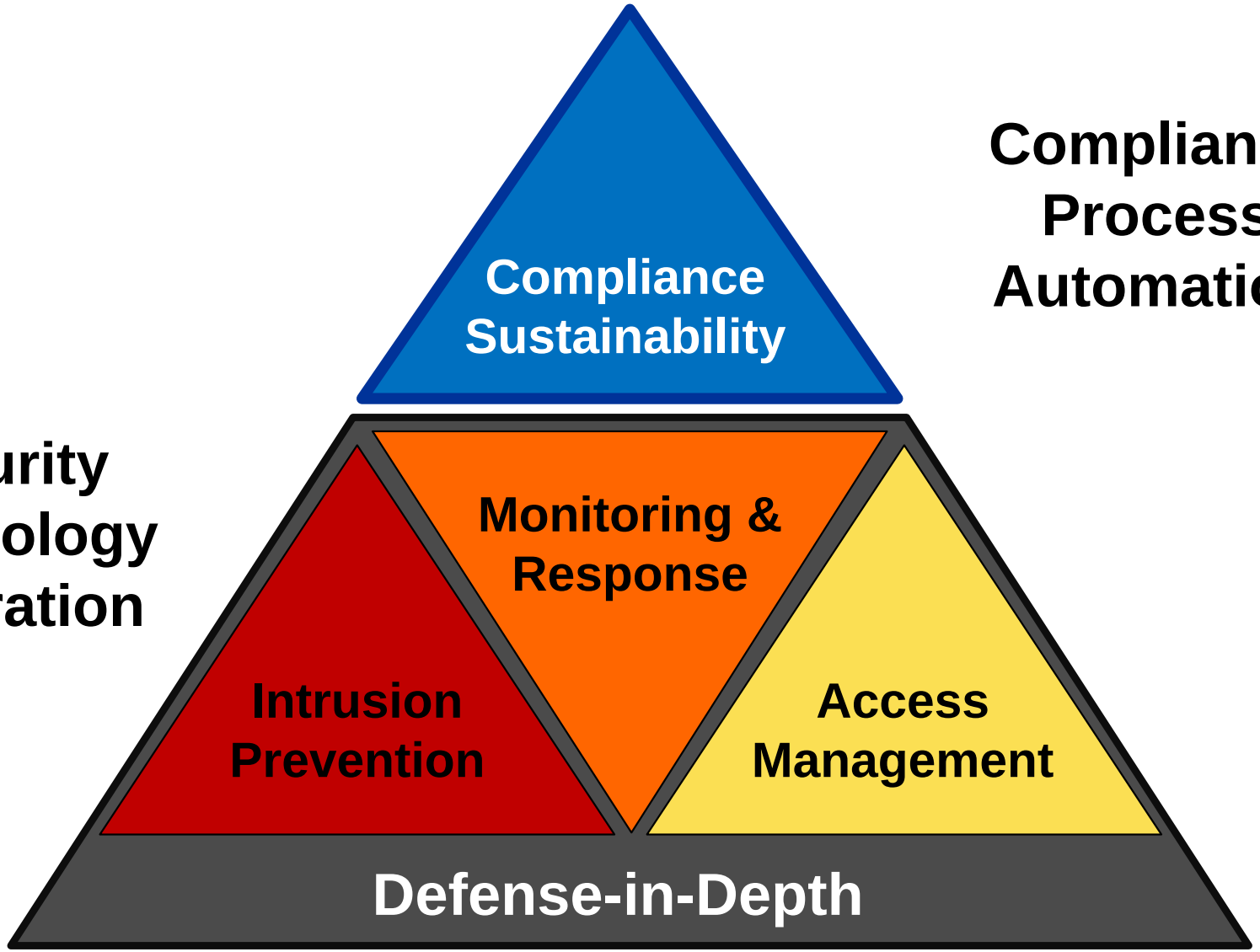
HMI Stations

Hardened networking devices

IEDs, Sensors, Controllers

INDUSTRIAL DEFENDER®

Solution: Integrated Automation System Security Management



Compliance Process Automation

Security Technology Integration

Sample Solution Approaches

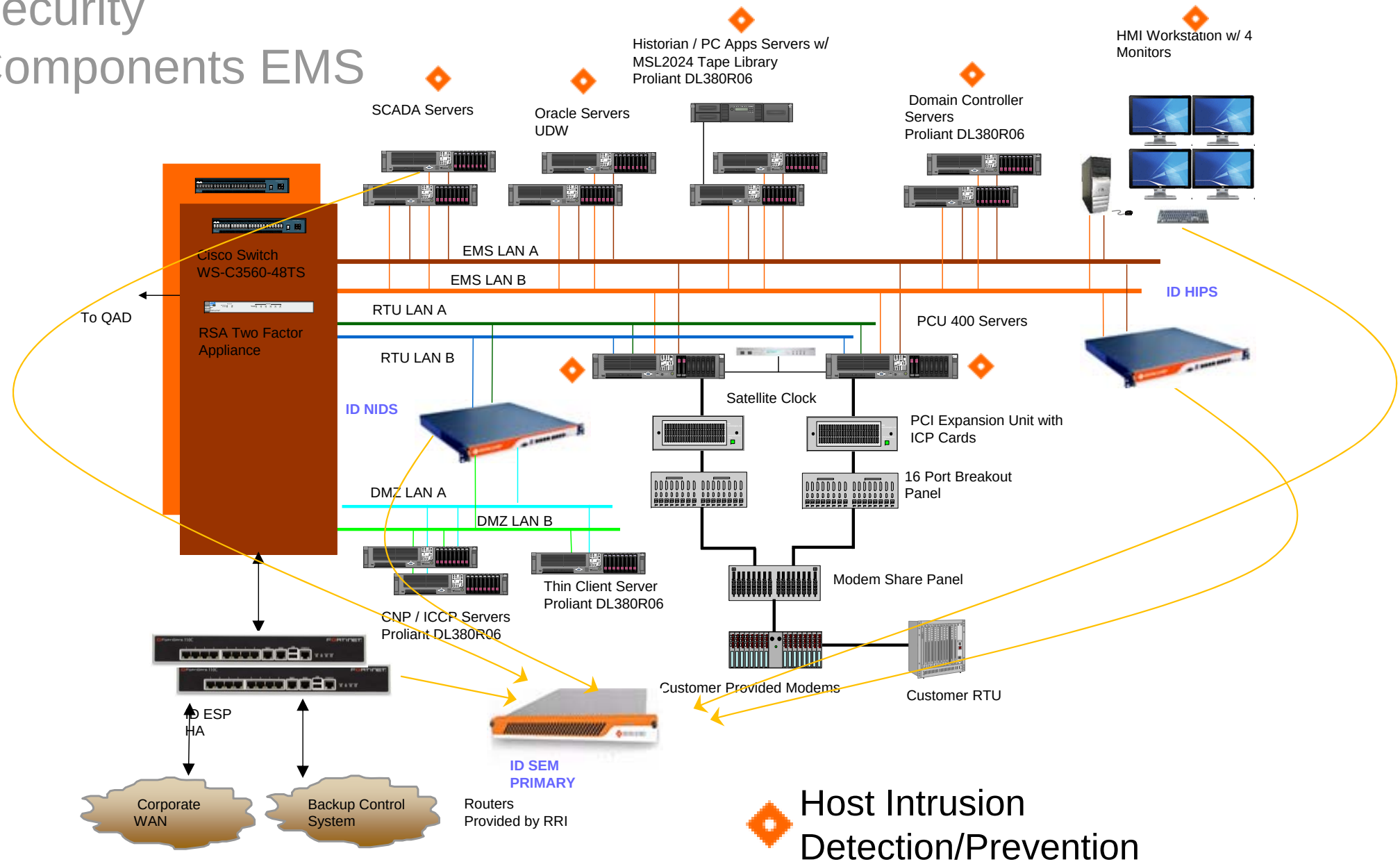
- Example 1 – Securing Energy Management System
  - Monitor networked servers, workstations and other end points
  - Deploy host intrusion prevention system
  - Provide security operator console for monitoring and alerting
- Example 2 – Multi Plant NERC Compliance Reporting
  - Collect required data from Servers, HMI stations, PLC's, routers, etc.
  - Deploy security operator console for alerting and data collection
  - Normalize data in data collection repository with pre-built reports to reduce manual collection of data and auditing

Security Solution Components - EMS

APW Session
WSE-110-1

- **Security Event Manager (SEM)**
  - Management console for logs and alerts
- **Network Intrusion Detection(NIDS)**
  - Signatures for Industrial Protocols such as Modbus, DNP3, Etc.
- **Host Intrusion Prevention Manager (HIPS)**
  - Endpoint protection for servers and workstations for Control Room environments
  - Human Machine Interface Devices (HMI)
  - Whitelisting engine
- **Security Sensors (agents for endpoints)**
  - Programmable Logic Controllers (PLCs)
  - Intelligent Electronic Devices (IEDs)
  - Workstations and servers for control room environments
  - Any SNMP / syslog capable devices within the control room environment

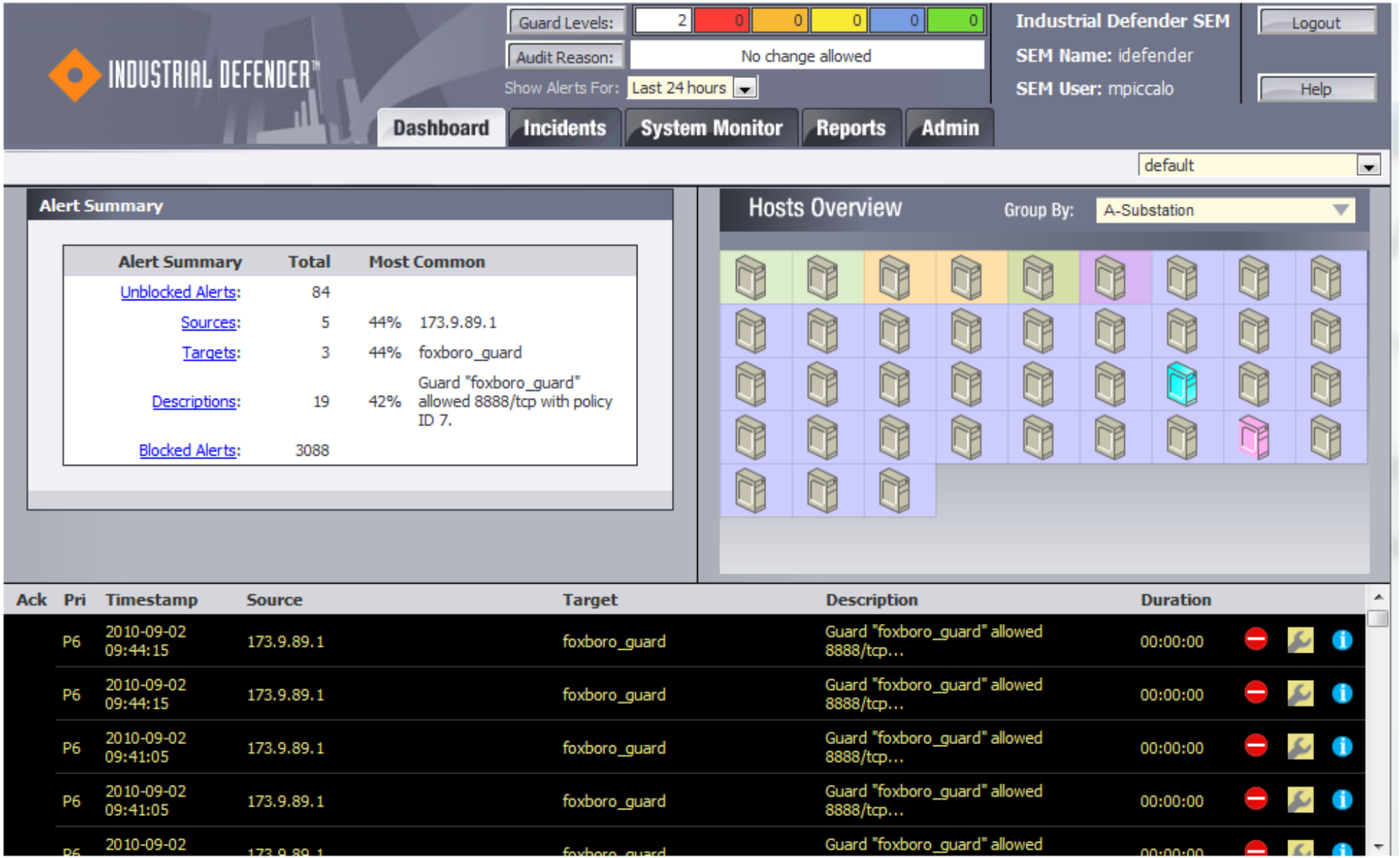
Security Components EMS



Host Intrusion Detection/Prevention

Example Energy Management System

SEM Dashboard Example



Multi Plant Compliance Solution

APW Session
WTP-121-1

Purpose-built compliance solution for Compliance Reporting needs for ***all*** devices within the Electronic Security Perimeter (ESP)

- Enables customers to effectively meet compliance and auditing requirements ***without disruption to system availability***
- ***Automates and streamlines*** process for data collection and archiving across system assets and applications
- Efficiently produces necessary data, reports, and documentation in a secure and consolidated location
- Provides for ***Compliance Sustainability***

Compliance Solution Overview

- Compliance solution ***automatically gathers and archives*** critical system details including:
  - System patch levels
  - Installed software components
  - User accounts with permissions
  - User activities
  - System configurations
  - System activities (performance and security events)
  - Ports and services
  - Security event data (device logs)
  - Much, much more…
- Normalizes system information from diverse endpoints
  - Data is standardized across platforms and presented in a professional looking format
- Supports multiple baseline configurations to include regulatory compliance (NIST SP 800-53, 10 CFR 73.54,NERC CIP, CFATS, ISO27000, etc.), internal compliance, etc.
- Turn-key installation with robust 'out-of-the-box' reporting
  - On-demand, subscription-based, and scheduled reporting
  - HTML, MHTML, PDF, XML, CSV, TIFF, Word, and Excel formats available

Base Compliance Solution Components

Sensors and Collectors

- Sensors collect alert, intrusion, and activity information from devices
- Collectors collect configurations and other information from devices
- Data collected from many devices to include firewalls, switches, routers, NIDS, HMIs, servers, workstations, etc.

Security Event Manager (SEM)

- Single aggregation point for collected data
- Stores collected data, generates real-time alerts with visualization, and forwards data to Compliance Manager

Compliance Manager

- Consolidates events, logs, and configuration information from all systems in a single, secure repository
- Provides tools for risk analysis, compliance assessment, and automated generation of audit reports

Viewing Reports…

INDUSTRIAL DEFENDER®
Compliance Manager

ComplianceAdministrator | Change Password | Log out | Help | About

Member Administration | View Reports | Manage Files | Baselines

Show Available Widgets » Change Tab Settings »

Report Browser

- Asset
  - Asset Inventory
- Configuration
  - Device Details
  - Ports and Services
- NERC CIP
  - NERC-CIP 002
  - NERC-CIP 003
  - NERC-CIP 005
  - NERC-CIP 007
- Perimeter
  - Access Control Device User Acc
  - Access Control Device User Acc
  - Access Control Devices (ACD)
  - Firewall Reports
- Software and Patches
  - Software
  - Software Patches
- Users
  - User Access
  - User Accounts

Report Viewer

View | Subscriptions

Location: Foxboro, unclassified ESP: Foxboro, unclassified View Report

1 of 1 100% Find | Next

Asset Inventory

INDUSTRIAL DEFENDER®

Location: Foxboro, ... [2]
ESP: Foxboro, ... [2]

Created on: 2/7/2011 11:47:43 AM
Created by: CM-DEMO\Administrator

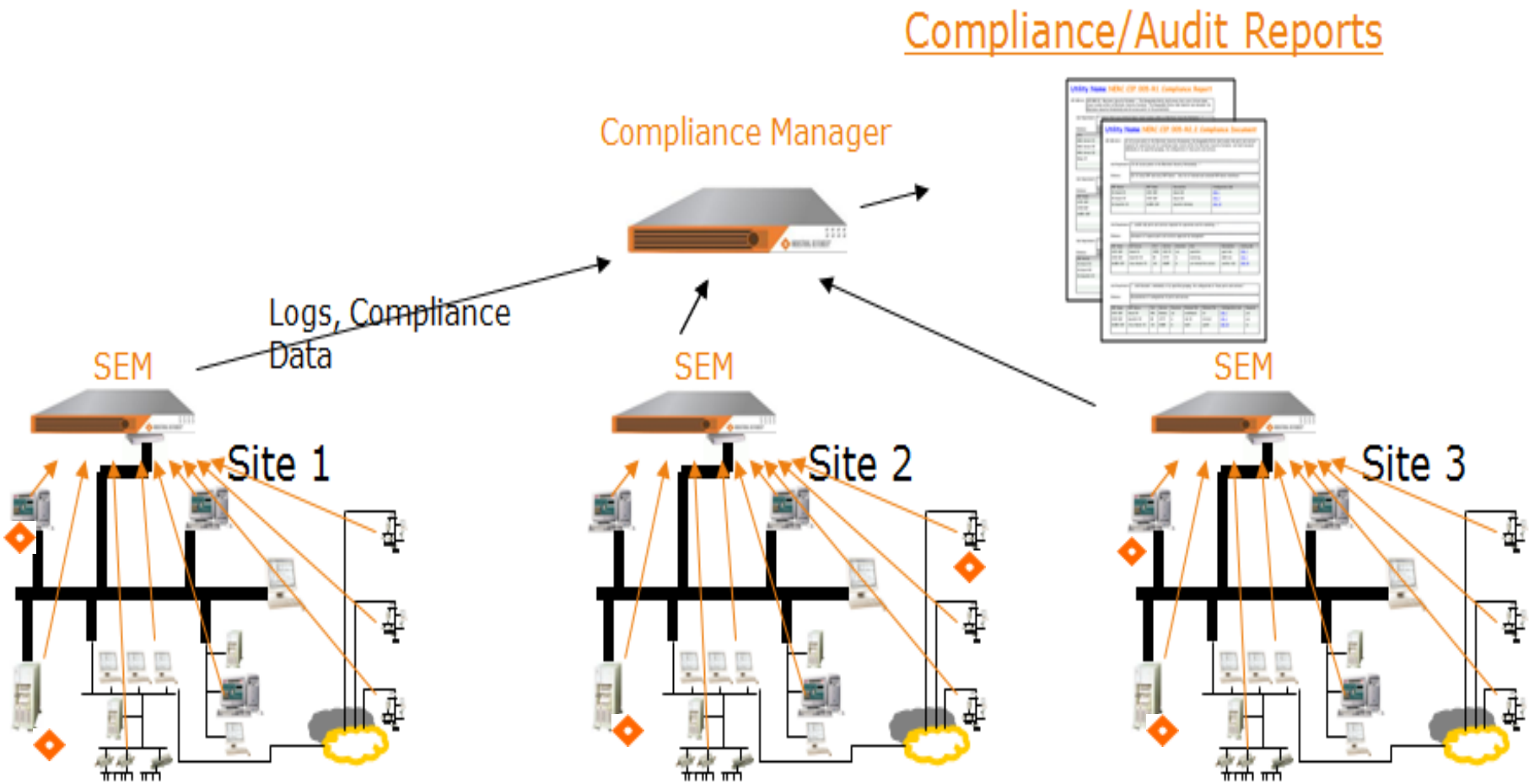
Description

Location	ESP	Device Name	Device Type	Criticality	Description
Foxboro	Foxboro	Commit	Fortigate	ESP	
		execute	Red Hat	Cyber Monitoring	Demo Console
		Laptop	Windows	CCA	Dell Laptop
		WMI-XP-02		CCA	
	unclassified	cm-demo		Cyber Monitoring	Compliance Manager

Compliance & Security Solution Overview

Compliance monitoring and reporting includes SEM, Agents, and Compliance Manager Repository

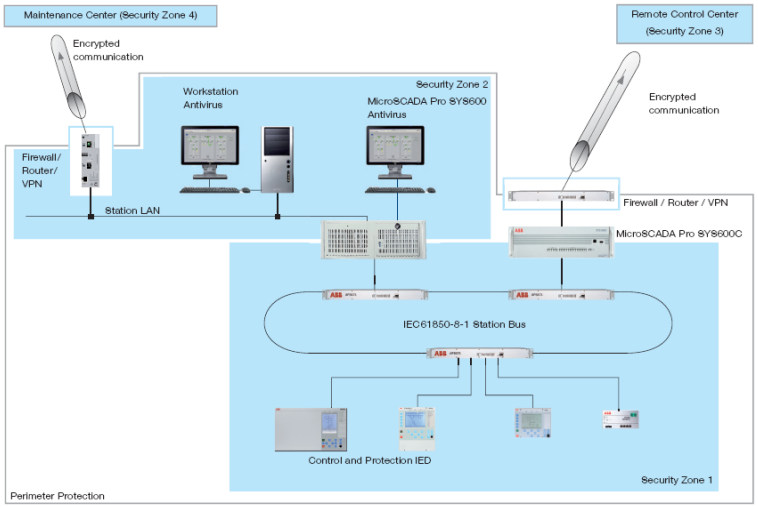
Sample Multi Plant Reporting Configuration

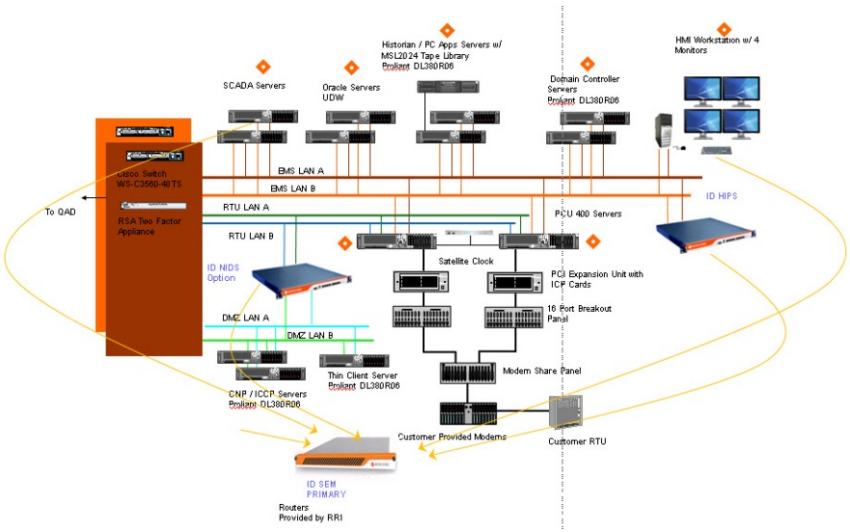


Industrial Defender Solution Summary

- Specialists in control system security and compliance
- Purpose built technology to provide defense in depth with minimal impact on automation systems
- Automated compliance reporting eliminates manual collection of audit data
- Applications for Energy Management, Plant Control Systems as well as many other automation use cases

ABB -Industrial Defender Partnership
Summary





Robust,
security enabled

ABB – products

+

Industrial
Defender

cyber security

solutions

Defense in Depth

Trends & Conclusions

Trends

APW Session
PSE-108-1

	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

Cyber Security @ Automation and Power World
April 18-21, 2011 – Orlando, Florida

Cyber Security: Technologies and Solutions

Tuesday, April 19, 2011

Session 1 – 9:30 a.m.	WSE-109-1	NERC-CIP, ISA 99 and other cyber security standards: What's new and how do they affect you
Session 2 – 11:00 a.m.	WSE-111-1	Secure your process plant operation
Session 3 – 1:30 p.m.	WSE-107-1	Cyber security: Buying a pig in a poke? How to get the security you need
Session 4 – 3:00 p.m.	WSE-110-1	Proper monitoring and configuration: Getting the most out of your cyber security investments
Session 5 – 4:30 p.m.	WSE-112-1	Security features, capabilities and support of your 800xA system

Wednesday, April 20, 2011

Session 6 – 8:00 a.m.	WPS-107-1	Cyber security in your Relion®-based protection and control solutions
Session 7 – 9:30 a.m.	CSE-102-1	Secure commissioning of your process plant: Case study
Session 8 – 11:00 a.m.	WTP-121-1	Addressing today's compliance challenges with automated solutions
Session 9 – 1:30 p.m.	CSE-101-1	Leveraging the ABB - Industrial Defender partnership to secure your control system: Case study
Session 10 – 3:00 p.m.	WSE-106-1	Cyber security in the system life cycle: ABB's commitment
Session 11 – 4:30 p.m.	PSE-108-1	Cyber security: The present state and where the future will lead

Thursday, April 21, 2011

Session 12 – 8:00 a.m.	WSE-103-1	Cyber security 101: What you need to know about current threats, solutions, standards and more
Session 13 – 9:30 a.m.	WSE-105-1	Cyber security for smart grid

Featured speakers

- Tim Roxey, NERC
- Eric Cosman, Dow Chemicals
- Brian Ahern, Industrial Defender
- Tyler Williams, Wurldtech

Automation & Power World 2011
April 18-21, 2011 in Orlando, Florida

Workshop statistics
Over 400 hours of training

- ~45 customer presented case studies
- 87 sessions in the Technology and Solution Center
- 11 hours of panel discussions consisting of customers, industry experts and ABB executives
- Nearly 50 hours of hands on technical training

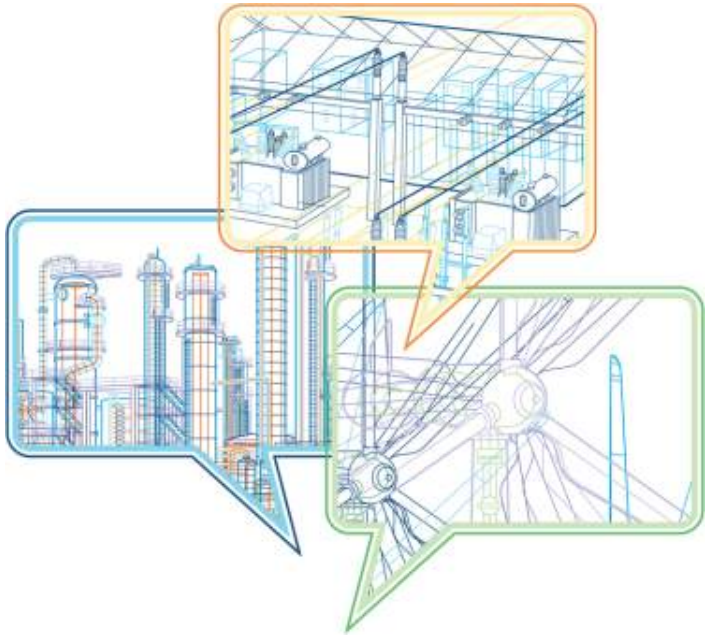
ABB Automation & Power World
Registration options

	Full Conference	Courtesy Registration
Access to ABB product developers and application experts in the 70,000 ft² (over 1.5 acre) Technology & Solution Center	✓	✓
Access to a series of complimentary and educational workshops.	✓	✓
Free Lunch and Tuesday Evening Reception	✓	✓
Access to over 300 additional educational workshops – Including ARC Analysts presentations	✓	
Up to $1,500 off a future ABB purchase*	✓	
Complimentary ARC report valued at $2,500!*	✓	
Evening Events (Monday and Wednesday)	✓	
* See www.abb.com/a&pworld for more details **Cost**	$300 per day or $800 for all three days.	Free!

Top ten reasons to attend

- Become more valuable, choose from over 400 educational workshops and hands-on training sessions
- Connect with thousands of peers and industry experts from 40 countries
- Ask questions of, and give feedback to, ABB product developers and executive management
- Get up to date with new and emerging technologies and industry trends
- Learn how to maximize the value from your existing assets
- Discover how to improve grid reliability, energy efficiency and industrial productivity
- Apply lessons learned from over 45 customer-presented case studies
- Focus on critical non-technical issues facing your company in the business forums
- Succeed professionally by earning CEUs on select workshops and PDHs for every workshop you attend
- See the widest range of technologies from one company at one conference!

Automation & Power World 2011
April 18-21, 2011 in Orlando, Florida



Register today!

www.abb.com/a&pworld

Join the Automation & Power conversation:
Stay in the loop:

Power and productivity
for a better world™

ABB