NEXDEFENSE
SECURITY FROM THE INSIDE OUT

Security Standards Overview

Name: Graham Speake
Position: Vice President and Chief Product Architect
Company: NexDefense

2014 YOKOGAWA USERS CONFERENCE AND EXHIBITION
Harness the Future of Innovation

Bio

- BSc Electrical and Electronics Engineer
- 20 years experience in computer security
- 14 Years experience in automation security
- Worked as an independent consultant on financial security
- Member of ISA, ISCI, ISC^2
- Worked for Ford Motor Company, ICS, ATOS-Origin, BP and Yokogawa
- Vice President and Chief Product Architect at NexDefense

Background

And History

Language difficulties

I am not in the office at the moment. Send any work to be translated

Early days ....

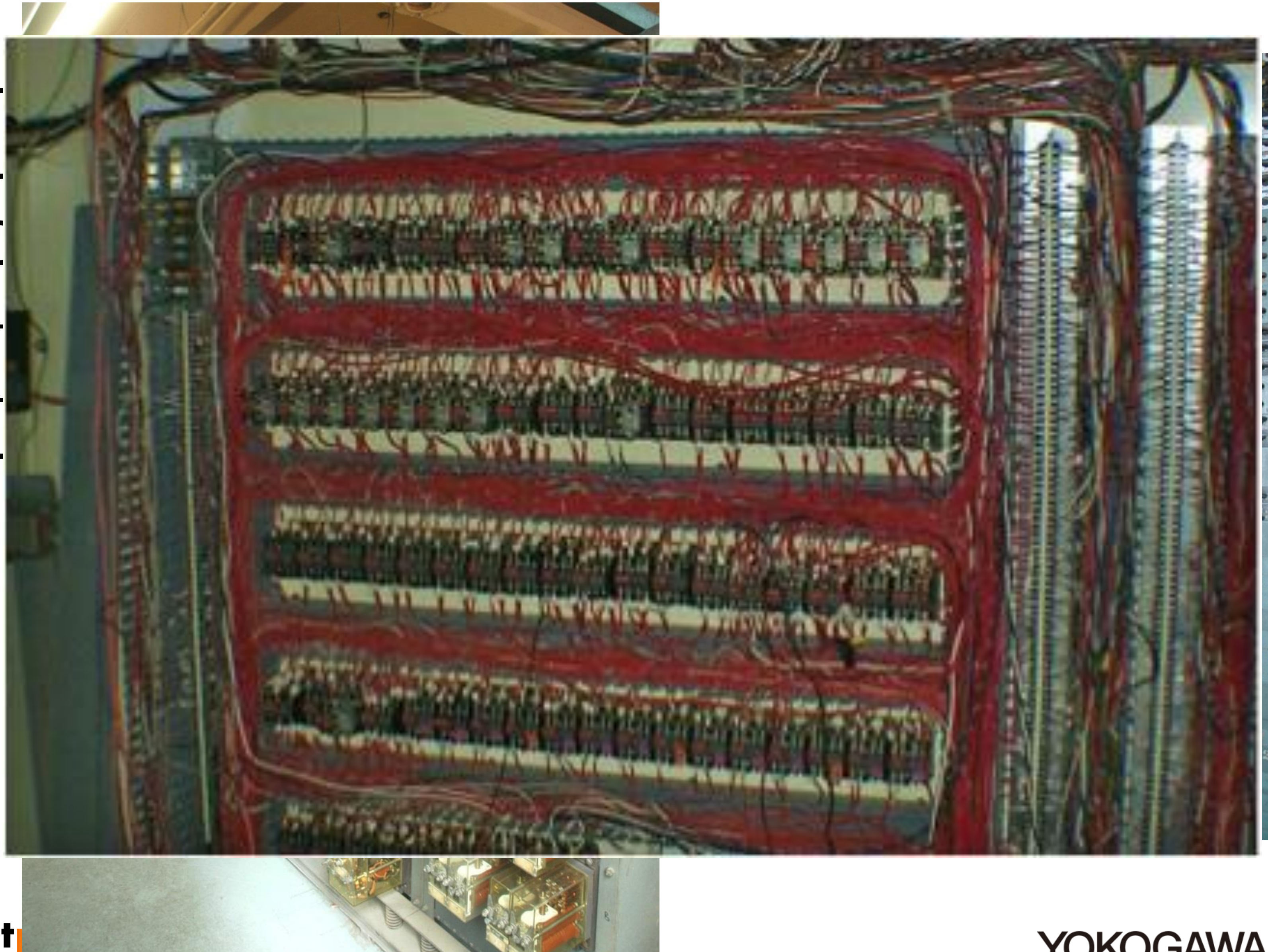
- Man has always invented machinery to ease the burden
- IBM minicomputers used in 1960s
- First industrial control computer
  - Texaco Port Arthur (Ramo-Wooldridge)
- First DCS : 1975
  - Yokogawa Centum
  - Honeywell TDC 2000

Hardwired systems

- Processes originally controlled by hardwired systems
- Completely stand-alone
- Relay-based
  - Really hard to hack into

Relay systems

- L
- L
- C
  -
  -
- T



Early computerization

- 70s and 80s show an explosion in systems
- PLCs, multiple DCS manufacturers
- End users rushed in to deploy
  - Configuration and modification simplification
  - Enhanced control functions
- Vendors came (and went)

Vendors

- Metso
- Bailey Controls
- Taylor Instrument
- Foxboro
- Varian Data Machines
- Valmet
- Bristol
- Fisher and Porter
- Midac
- DEC

DCS evolution

- Major evolution of DCS during 1980s
  – More powerful operator stations (HMIs)
  – Fully distributed control
  – Proprietary hardware and software
  – Little / no standardization
    - Between vendors
    - Within a company (vendor or end user)
  – Growth in oil and gas exploration

Rise of the DCS

- New DCS models and upgrades proliferate
  - I/O boards
  - Number of different devices
  - Control software increases in sophistication
  - Security?

Proprietary systems

- Proliferation of systems
  - Many disparate vendors
  - Multiple vendor mergers and acquisitions
    - Well known names of 70s and 80s disappear
    - Users think about standardization
  - Custom made hardware and software
- Rise of Microsoft and IBM PCs in IT world

Vendor Systems Development

- Often non-computer orientated design team
  - Systems designed by engineers
- Computer Science seen as an corporate IT function
  - Based on mainframes / minicomputers
  - Punched cards
  - 8" floppy disks
- DEC PDP-11 often used
  - Used and taught in engineering degrees

Rise of Personal Computing

- Personal computers proliferate in 1980s and 1990s
  - Atari
  - Sinclair
  - BBC (Acorn)
- Cost of computers came down
  - (but why do they always seem to be the same?)
- Networking became the norm (but not standardized)
  - Token ring

Internet and TCP/IP

- Growth of TCP/IP in late 80s
- Internet starting becoming popular
  - CompuServe
  - AOL
  - BBS
- Microsoft Windows gained popularity
  - Added games!

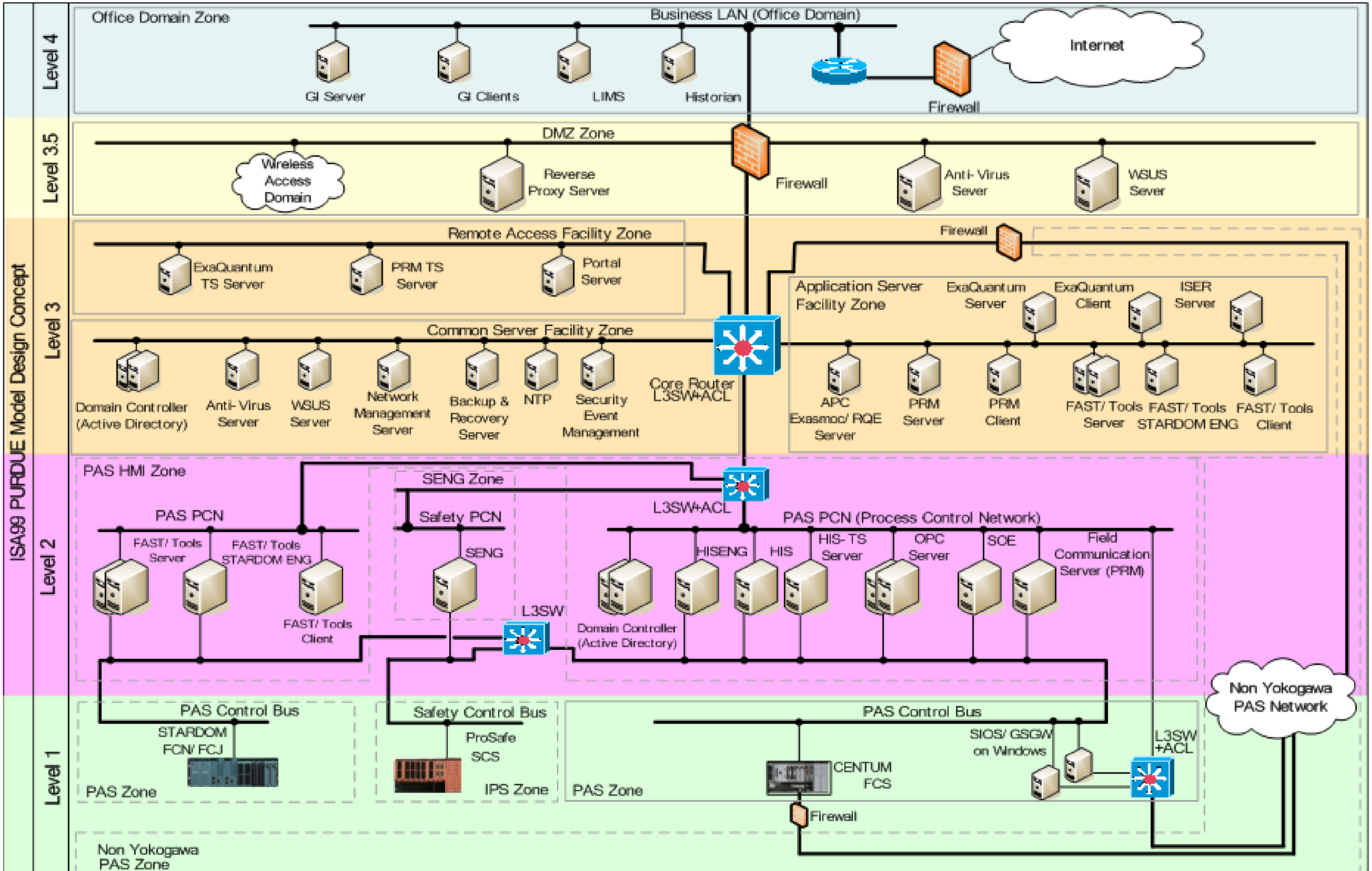
Rise of Microsoft

- Microsoft Windows NT
  - Stable (ish) platform
  - Used extensively in IT
  - Large pool of expertise
- OPC (1996)
  - Object Linking and Embedding for Process Control
  - Now Open Platform Communication Foundation
  - Communication of real-time plant data between different vendors

Cost equation

- HMIs can cost $50000
- PC can cost $2000
  - Do more
  - Better display
  - Easily extensible
  - Buy from multiple sources
- End users
  - Question cost
  - Standardization
- Vendors pushed towards Windows

Typical deployment



Where we are today

2001

- 9/11 changed the thought process
- Companies looked at security
- Industrial security woefully lacking
- Control systems compromised

Accidental incidents

- PLCs crashed by IT security audit
- Duplicate IP address prevents machine startup
- IP address change shuts down chemical plant
- Accidental programming of a remote PLC
- AV software prevents boiler safety shutdown
- Multiple USB infections

Malware infections

- Sasser infects chemical plant
- Blaster infects chemical plant
- Slammer infects power company control centre
- Nachi and Sasser infect baggage handling systems
- Sobig virus shuts down train signalling system
- Slammer infects nuclear power plant
- Virus shuts down flight planning computer

Internal hackers

- Disgruntled employee changes PLC passwords to obscenity
- Maroochy Shire Sewage Spill
- White hat takeover of DCS consoles
- Venezuela Oil striking PLC hacker sabotage

External hackers

- APT at
- Stuxne
- Shamo
  - Up t
- Zombi

Advances since 2001

- Slow progress
  - Vendors, asset owners, consultants
- Public – private initiatives
  - Lots of paper
  - Roadmaps
- Standards coming out
  - ISA 99 / ISA 62443 / IEC 62443
- Certifications
  - Process / systems / people

Reasons for inaction – I've got a firewall!

Reason 2 – I've got a Windows firewall!

Reasons for inaction

- Asset owners
  - Skills not available
  - Cost of deployment (and opex)
  - Not a target
  - No management buy-in
  - Shareholders
  - Not regulated
- Vendors
  - Skills not available
  - No management buy-in
  - Not seen as saleable

Consultants

Certifications

- Wurldtech
  - WIB certification scheme
  - Now becoming 62443-2-4
  - Processes and systems
  - Mainly vendors
  - Take-up very slow
- Wurldtech
  - Achilles

Threats

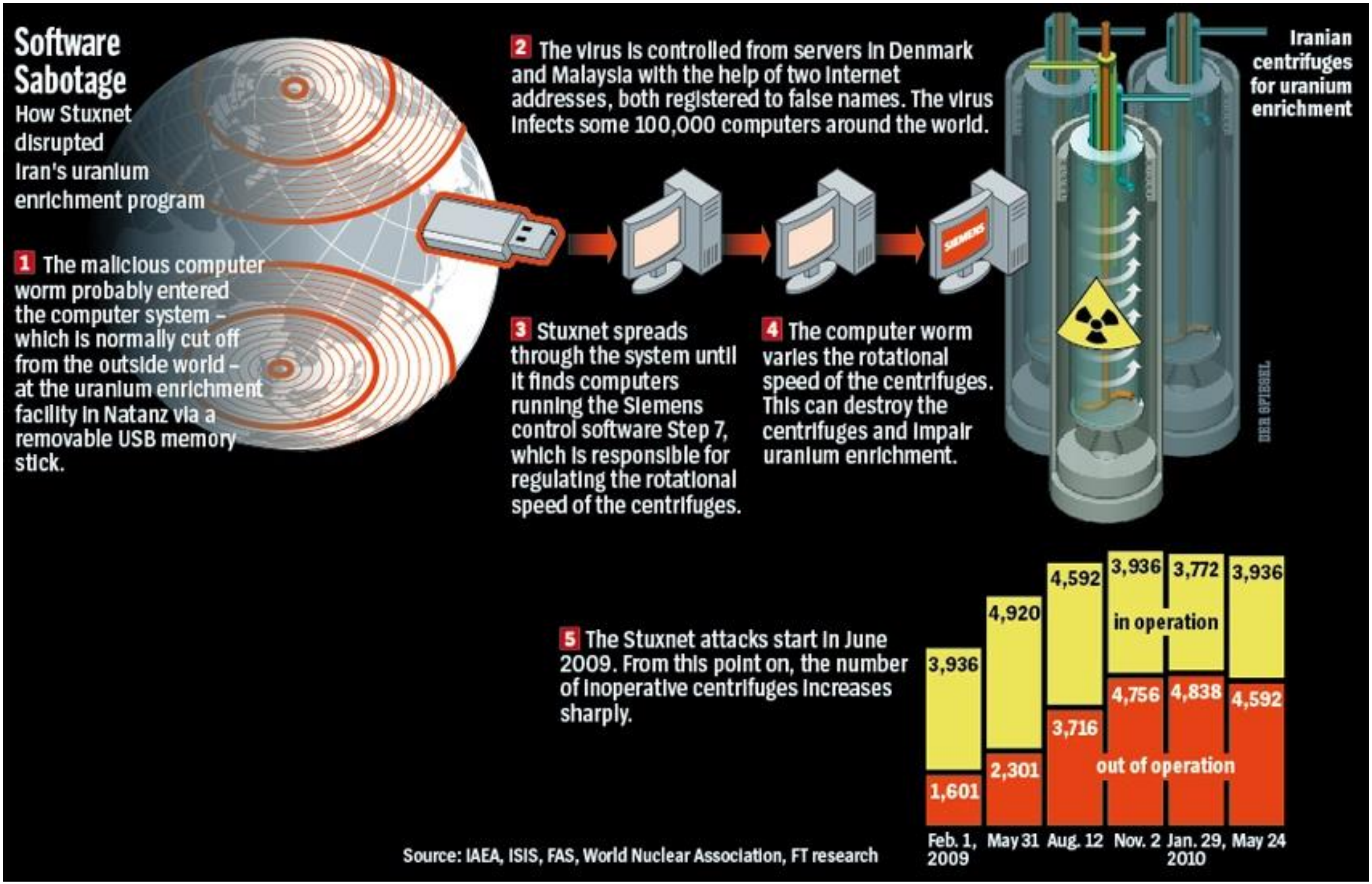
Cybersecurity threat history (2010 – today)

- Stuxnet
- Duqu
- Nitro
- Night Dragon
- Shamoon
- Anonymous
- Dragonfly / Energetic Bear

Stuxnet (2010)

- Stuxnet
  - Very targeted attack
  - Air gapped system
  - Not a game changer

Stuxnet


Software Sabotage
How Stuxnet disrupted Iran's uranium enrichment program
1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.
2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.
3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.
4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.
Iranian centrifuges for uranium enrichment
SIEMENS
5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.
3,936
1,601
4,920
2,301
4,592
3,716
3,936
4,756
3,772
4,838
3,936
4,592
in operation
out of operation
Feb. 1, 2009
May 31
Aug. 12
Nov. 2
Jan. 29, 2010
May 24
Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

Duqu (2011)

- Based on Stuxnet code
- No ICS specific attacks
- Stolen digital certificate to aid installation
- Information gathering

Source : http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf

Nitro (2011)

- NGOs -> motor industry -> chemicals
- 30 chemical companies infected
- Phishing and spear-phishing attacks
- Poison-ivy RAT
- Target : intellectual property

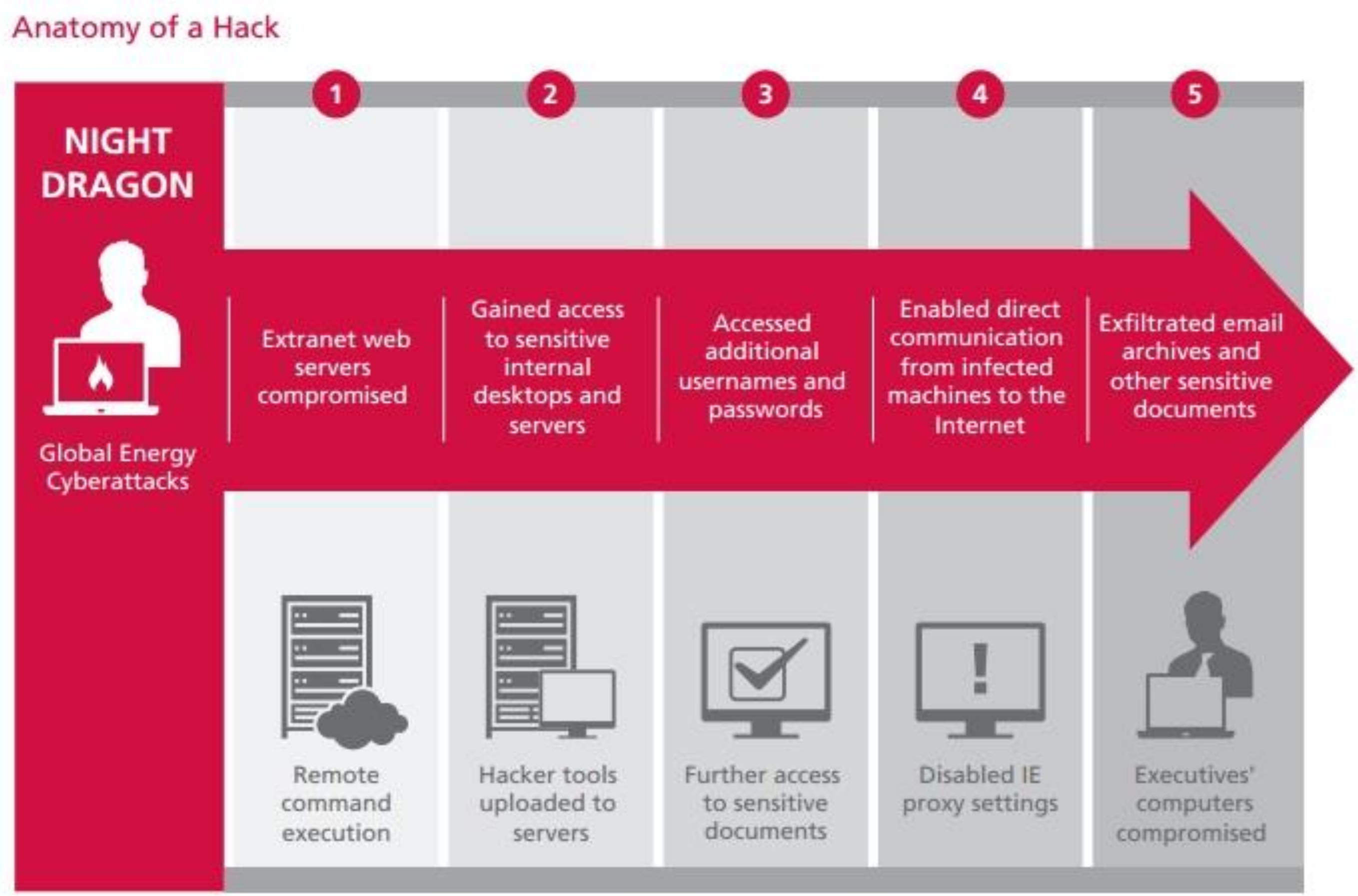
Source :
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

Night Dragon (2009 - 2011)

- Targeted many oil and gas companies
- Primary purpose data extraction
- Attacker IP addresses resolve to China

Night Dragon (2009 - 2011)

Source: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf



Shamoon (2012)

- Infected ~30000 Saudi Aramco computers
- Self-replicating worm
- Destructive - wiped the hard drives
- Purpose – stop the flow of oil
- Spread to RasGas and others

Anonymous (ongoing)

- Hacktivist group
- OpPetrol

Heartbleed (2014)

- SSL/TSL bug
- Code used in critical infrastructure components
- Discovered by Codenomicon

Dragonfly / Energetic Bear (2014

- Dragonfly Group (Symantec) / Energetic Bear (Crowdstrike)
  - Active since 2011
  - Appears to be Russian origin
  - HAVEX RAT and SYSMain RAT
  - Initial targets:
    - US / Canada defense and aviation
  - Lately
    - European energy firms

Dragonfly modus operandi

- Initially spear phishing executives
- Watering hole attacks
  - Mainly ICS vendors
- Infected software packages
  - VPN into PLC equipment
    - 250 downloads
  - PLC manufacturer
    - Software available 6 weeks
  - Alternative energy manufacturer
    - Software available for 10 days

Source: https://scadahacker.com/files/havex/Symantec%20-%20Security%20Response%20-%20Dragonfly%20v1.0.pdf

Fertger (Peacepipe)

- Actively scanning for OPC
- No active component (yet)

```
Programm was started at 14:46:11
***********************************************************
***************
14:46:11.0081: Start finging of LAN hosts...
14:46:11.0081: Was found 2 hosts in LAN:
                         01) [\\<hostname>]
                         02) [\\<hostname>]
***********************************************************
***************
14:46:11.0081: Start finging of OPC Servers...
14:46:17.0133: Thread 01 return error code: 0x800706ba
14:46:17.0133: Was found 2 OPC Servers.
          1) [\\<hostname>\ArduinoSerialOPCDAServer.1]
               CLSID:                {F57384B1-95E2-4591-
876C-C608F439FEEA}
               UserType:             OPC Server for Arduino
               VerIndProgID:
ArduinoSerialOPCDAServer.TISMInternalOPCDataItemServer
               OPC version support: +++
          2) [\\<hostname>\Matrikon.OPC.Simulation.1]
               CLSID:                {F8582CF2-88FB-11D0-
B850-00C0F0104305}
               UserType:             MatrikonOPC Server for
Simulation and Testing
               VerIndProgID:         Matrikon.OPC.Simulation
               OPC version support: +++
***********************************************************
***************
14:46:17.0133: Start finging of OPC Tags...
14:46:17.0133: Thread 01 running...
14:46:17.0133: Thread 02 running...
14:46:17.0133: Thread 01 finished.
14:46:17.0398: Thread 02 finished.
     1)[\\<hostname>\Matrikon Inc (780) 448-1010
http://www.matrikonopc.com]
     Saved in 'OPCServer01.txt'
```

Source: http://www.fireeye.com/blog/technical/targeted-attack/2014/07/havex-its-down-with-opc.html

Mitigation strategies

- Defense in depth
- Network and control system knowledge

- Don't just rely on one very strong protection measure.
  - No single security measure is perfect – any small vulnerability could render a single protection measure ineffective
  - Good security fra
  - Also this provides

Kee

Oute

Murc

Portc

Drav

Moat

Rewind to the 1980's

- Industry-wide focus on Safety due to some significant events
- Safety Instrumented Systems (SIS) technology changing from electrical relays to programmable electronic systems (PES)
- Limited skillset in asset owner organizations to assess SIS safety integrity
- Solution:
  - IEC 61508/61511 international standards
  - Independent 3rd party safety integrity assessment

Fast Forward to Today

- Industry-wide focus on Security due to many significant events
- Industrial Automation and Control Systems (IACS) technology changing from vendor proprietary to IP networking and COTS hardware/OS
- Limited skillset in asset owner organizations to assess IACS cybersecurity capabilities
- Solution:
  - ISA/IEC 62443 international standards
  - Independent 3rd party security assessment - ISASecure®

Overview of ISA/IEC standards

Overview

- The Situation
- Chlorine Truck Loading Use Case
- Design & Risk Management Process
- Systems vs. Zones & Conduits
- Design Considerations
- Security Level Vector Discussion

The Situation

- The Problem
  - With so many standards out there, how do you pick the best one?
  - Once you've picked a set of standards, how do you apply them?
- Security Standards
  - ISA/IEC 62443 (13)
  - ISO/IEC 2700x (10+)
  - NIST FIPS and SP800 (7+)
  - NERC CIP (8)
  - Smart Grid (?)

IT Standards

Sector-Specific Standards

- And that's just the security standards, then take into account the functional standards
  - Wireless = ISA 100.11a, WirelessHART, Zigbee, WiFi, Bluetooth…
  - Safety = ISA 84, IEC 61508/61511, DO-254, OSHA…
  - Management = ISO 9000, 14000, 31000, 50001, Six-Sigma…
  - And plenty of others…

ISA/IEC 62443 Series (Proposed)

General

- **ISA-62443-1-1** — Terminology, concepts and models
- **ISA-TR62443-1-2** — Master glossary of terms and abbreviations
- **ISA-62443-1-3** — System security compliance metrics
- **ISA-TR62443-1-4** — IACS security lifecycle and use-case

Published as ISA-99.00.01-2007

Policies & procedures

- **ISA-62443-2-1** — Requirements for an IACS security management system
- **ISA-TR62443-2-2** — Implementation guidance for an IACS security management system
- **ISA-TR62443-2-3** — Patch management in the IACS environment
- **ISA-62443-2-4** — Installation and maintenance requirements for IACS suppliers

Published as ISA-99.02.01-2009

System

- **ISA-TR62443-3-1** — Security technologies for IACS
- **ISA-62443-3-2** — Security levels for zones and conduits
- **ISA-62443-3-3** — System security requirements and security levels

Published as ISA-TR99.00.01-2007

Component

- **ISA-62443-4-1** — Product development requirements
- **ISA-62443-4-2** — Technical security requirements for IACS components

Security Standards

- Security standards generally tell you what has to be done or specified, but don't tell you how to go about doing it
  - Functional specifications
  - Security controls/countermeasures
- Some standards show a generic process, but leave it up to the reader to apply it in their case
- A few use-cases exist, but many times these are:
  - Sector-specific
  - Only apply in certain cases
  - Limited in scope
- Very few end-users discuss the details of their processes
  - Restrict information from potential attackers
- Almost no vendors or system integrators discuss the details of their processes
  - Restrict information from potential competitors

Chlorine Truck Loading Use Case

- Setting the Stage
  - ISA99 is trying to use a single use-case throughout the entire series to show how each part of the standard fits into the process
  - While the chlorine truck loading example is related to the chemical industry, the concepts presented could relate to any industry
  - The example allows for somewhat more realistic discussions of risk than in an IT-focused, DHS-focused, or purely hypothetical example
- Use case in early development and idea phase
  - Will take quite a long time to complete entire use-case
  - Different parts of use-case will probably emerge at different times

Chlorine Truck Loading Use Case:The Narrative

- Pharmaceutical Company XYZCorp
  - Wants to start producing new product (FixItAll)
  - No room for new production plant at existing facilities
  - Chemical process requires relatively small amounts of chlorine
  - Existing facility produces chlorine in large enough quantities
- XYZCorp considers their options
  - Conducts business assessment of building new facility
    - Existing facilities all near space capacity
    - New facility has good access to roads
    - Land is suitable and available
    - Existing chlorine production facility over 50 miles away
  - Considers options for transporting chlorine
    - Pipeline
    - Rail
    - Truck

Chlorine Truck Loading Use-Case: The Plan

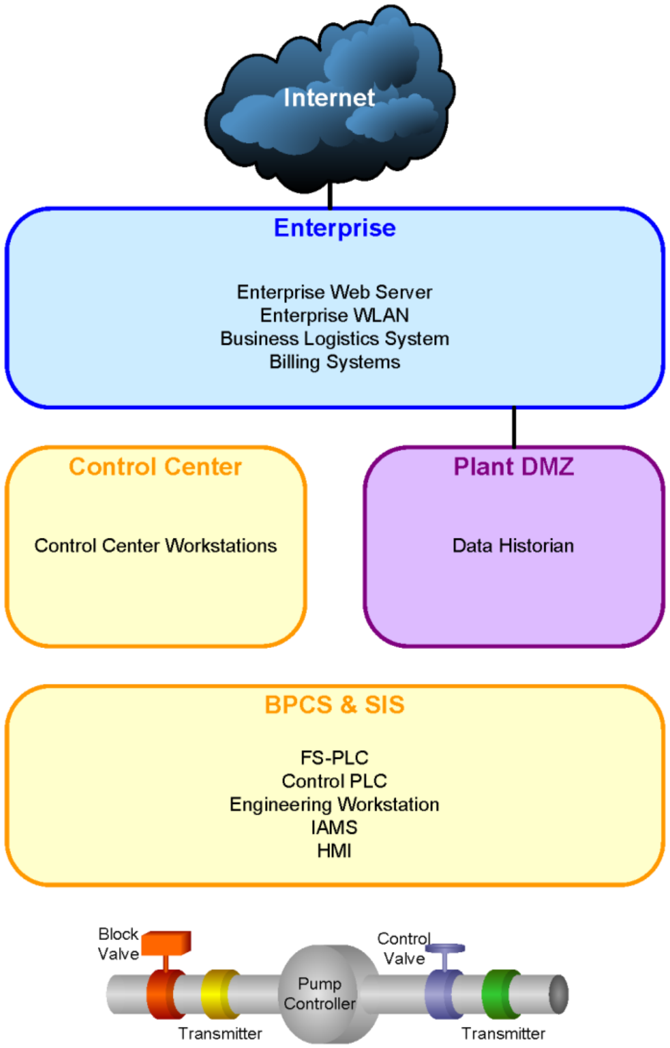
- Build truck loading/unloading facilities
  - Loading @ existing facility, unloading @ new facility
  - Unmanned except during loading/unloading operations
  - Hazardous chemical requires special handling & safety
- Generations of equipment
  - Existing facility uses legacy equipment (brown-field)
  - New facility designed with current technology (green-field)
- Facility monitoring & control
  - Unmanned – centralized monitoring @ control center
  - Manned & operational – local control with both local & centralized monitoring
- Attached to business systems
  - Billing & logistics
  - Inventory tracking

Use Case: Design Considerations

- Systems needed
  - Safety Instrumented System (SIS)
  - Basic Process Control System (BPCS)
  - Control center
  - Plant DMZ
  - Enterprise systems
- Level of SIS integration with BPCS?
  - Air-gapped
  - Interfaced
  - Integrated

Initial Design Process: Identify the Control Assets

- Process Equipment
  - Pump Controller
  - Transmitters
  - Block and Control Valves
- BPCS & SIS
  - Functional Safety-PLC
  - Control PLC
  - Engineering Workstation(s)
  - Instrument Asset Management System
  - Human-Machine Interface(s)
- Control Center
  - Control Center Workstations
- Plant DMZ
  - Data Historian
- Enterprise
  - Enterprise Web Server
  - Enterprise WLAN
  - Business Logistics System
  - Billing System



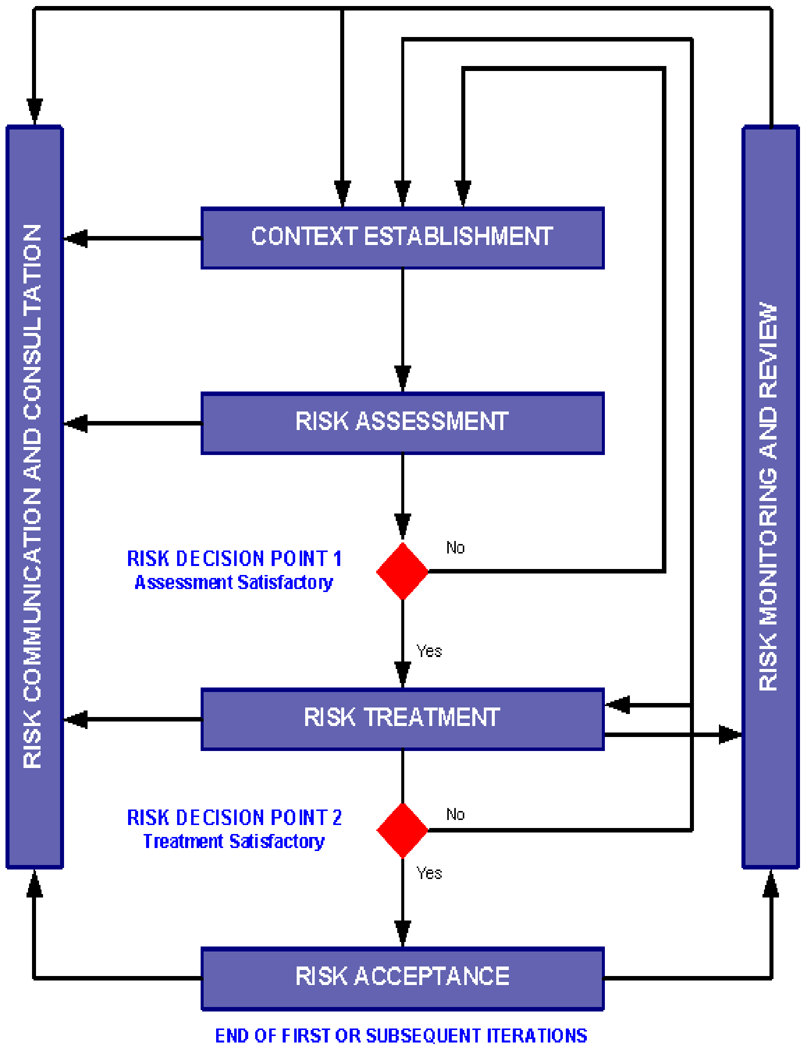
Now What???

Design Process

- Now that the business case and some initial design ideas have been put down, where do you go from here?
  A. Design the control system without worrying about the security?
  B. Design everything so secure that it becomes unusable?
  C. Throw in firewalls everywhere?
  D. Conduct a detailed risk assessment at the device level?
  E. Conduct a multi-stage risk assessment starting with the top level and working down to the low level as the design progresses?
- Generally, the ISA99 approach begins with E

Modified ISO/IEC 27005 Risk Management Process

- ISA99, Working Group 2 working on modified ISO/IEC 27005 risk management process
  - Uses basic shell from 27005
  - Modifies it for multi-stage risk assessment process
  - Discusses “jump-in” point
  - Relates risk management process to overall cyber security management system design process
    - Business planning
    - Change management
    - Decommissioning



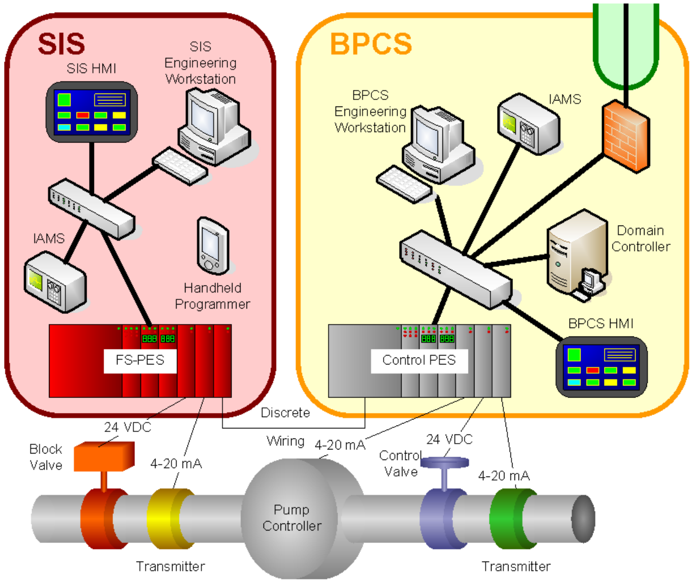
Systems vs. Zones & Conduits

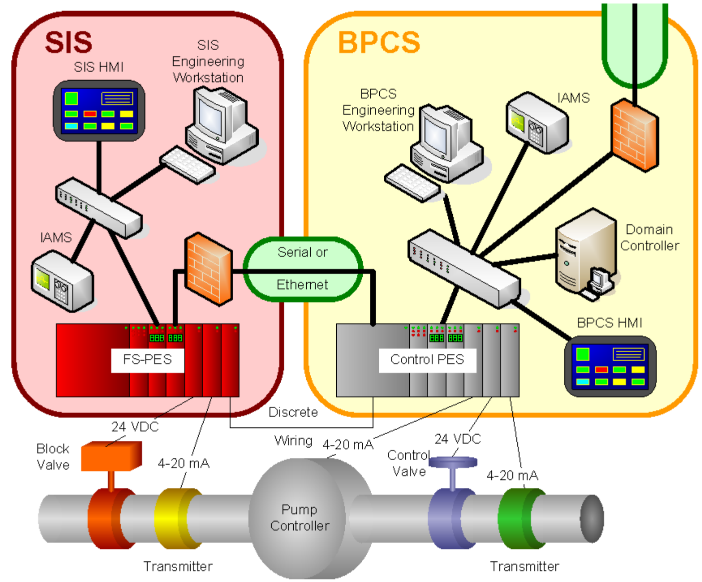
- Systems ≠ Zones
  - Conducting a system breakdown may give some indication of future zones, but there is no direct one-to-one correlation between the two
  - Systems = Collections of equipment/assets that logically function together to perform at least one task
  - Zones = Collections of equipment/assets that logically have similar security requirements
- System breakdown helps to identify different sets of equipment during the risk assessment phase
- Zones are created after the risk assessment phase based on the particular security requirements for that set of equipment/assets
- Conduits are a special kind of zone containing a communication channel

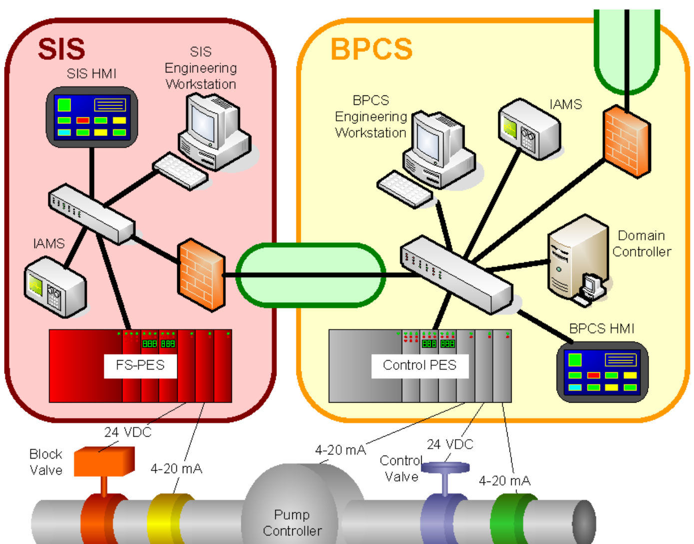
Security Levels

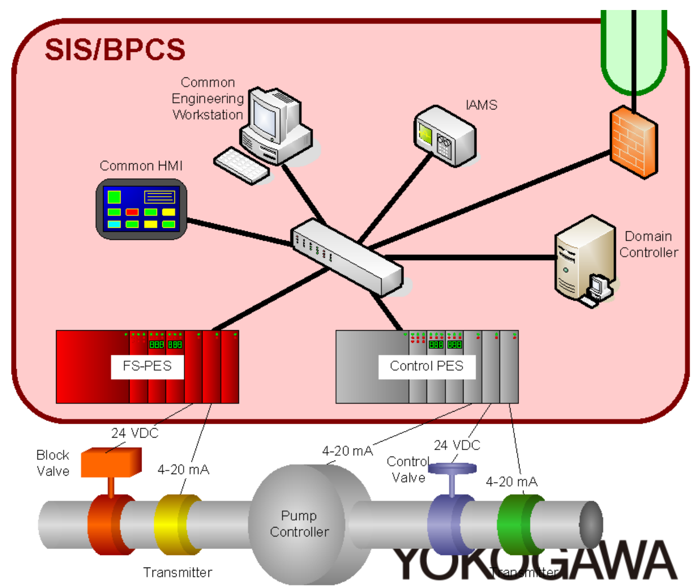
- LEVEL 1
  - Casual & Coincidental
  - Violation
- LEVEL 2
  - Simple Means
  - Low Resources
  - Generic Skills
  - Low Motivation
- LEVEL 3
  - Sophisticated Means
  - Moderate Resources
  - System-Specific Skills
  - Moderate Motivation
- LEVEL 4
  - Sophisticated Means
  - Extended Resources
  - System-Specific Skills
  - High Motivation

Design Considerations: SIS Air-Gapped vs. Interfaced vs. Integrated



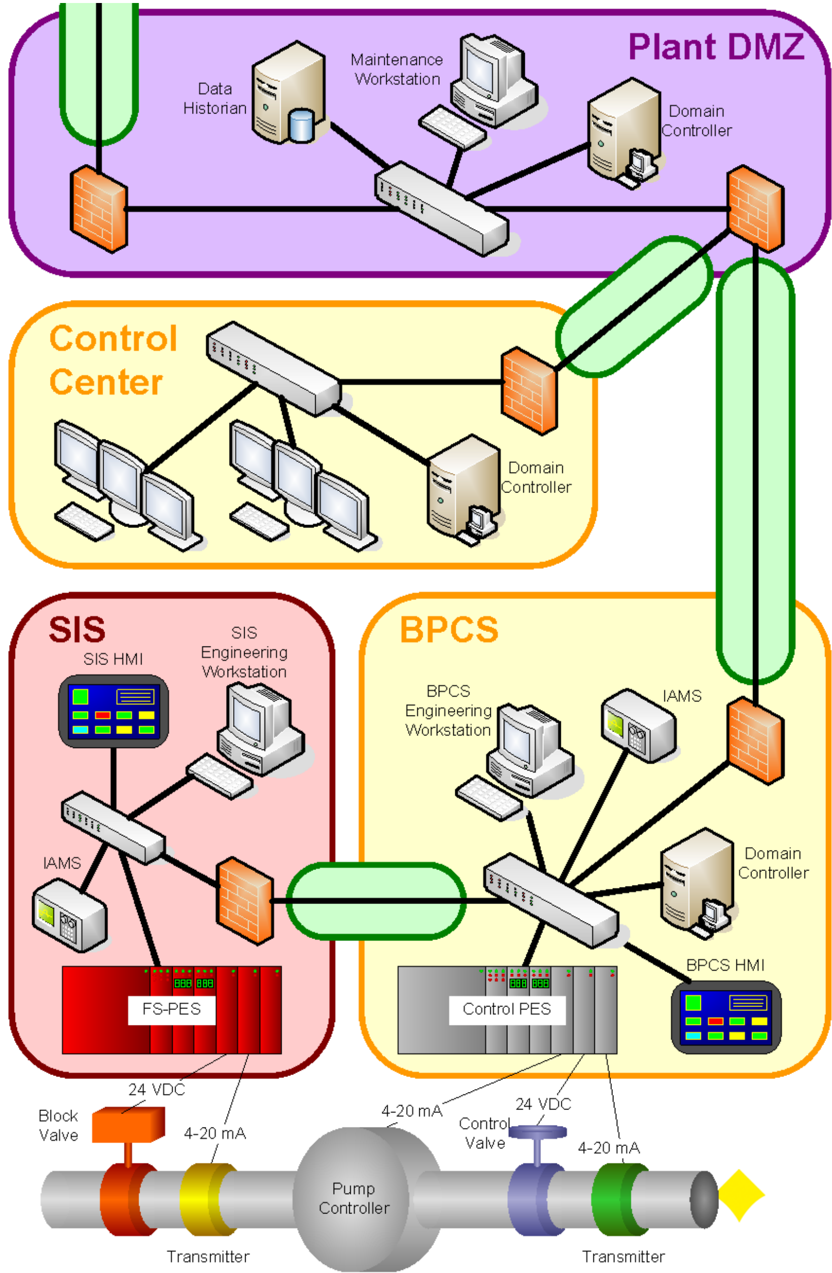






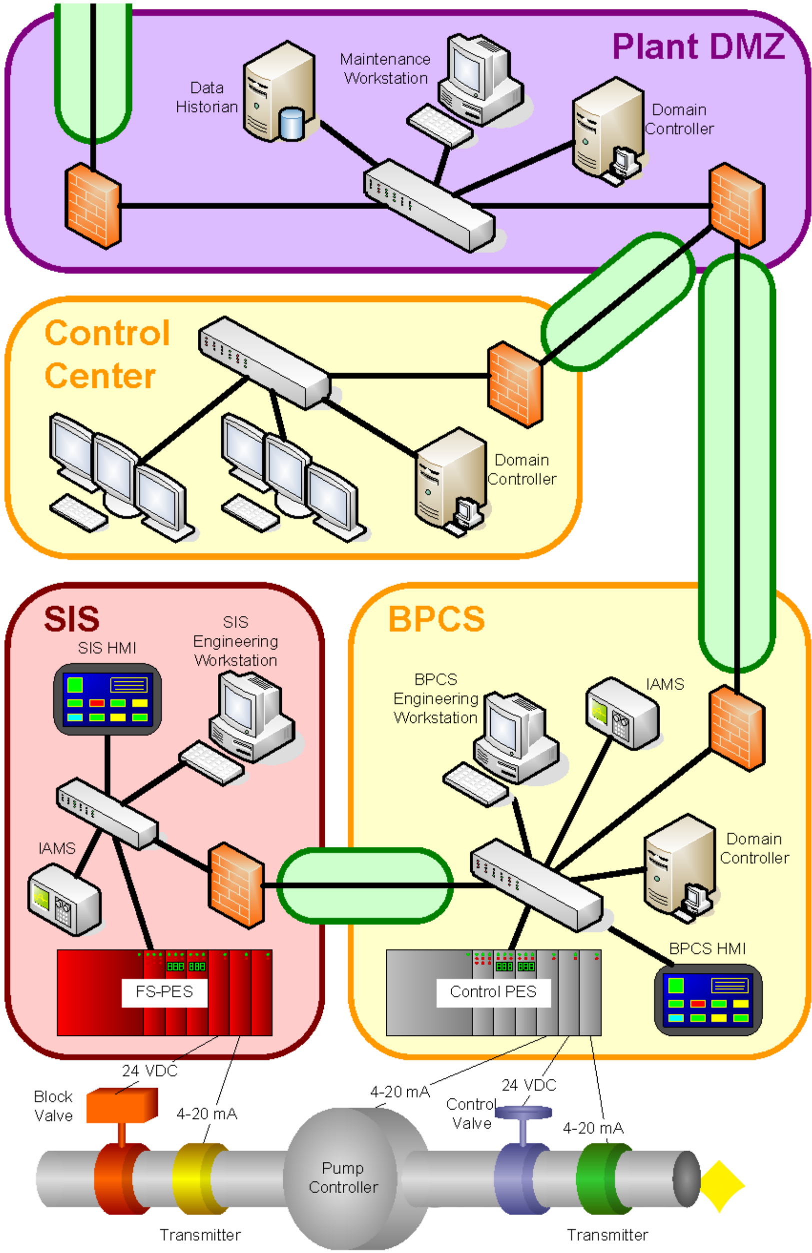
Security Level Vector Discussion

- Industrial Security Isn't Always About Death & Dismemberment
  - Some security concepts don't fit into that model
- Use the Foundational Requirements to Engineer the System Security
  - Identification & Authentication Control
  - Use Control
  - System Integrity
  - Data Confidentiality
  - Restricted Data Flow
  - Timely Response to Events
  - Resource Availability



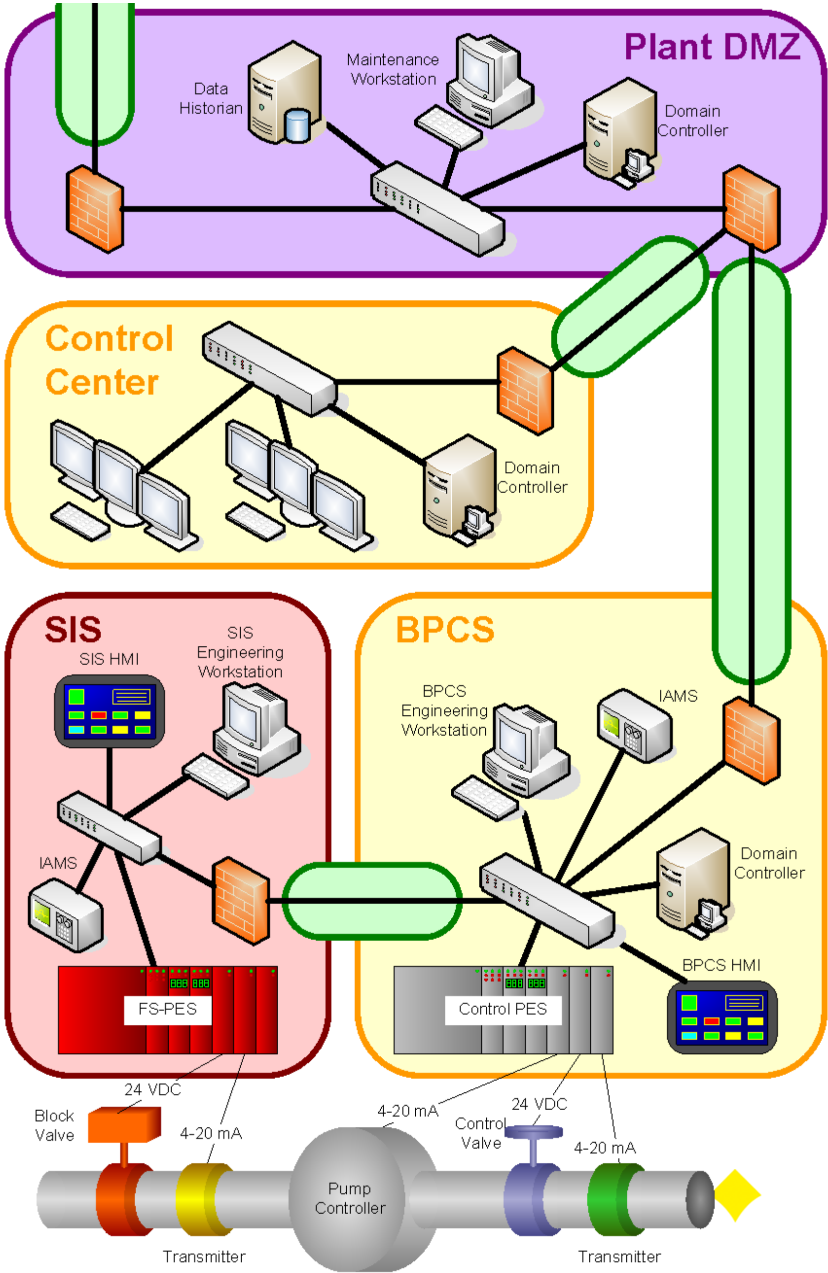
Security Level Vector Discussion

- How will the switches affect the security of the BPCS & SIS?
  - High availability is fairly common
  - Uncommon for switches to have good access control (natively)
  - Confidentiality depends, is SNMP enabled AND secured?
  - If switch fails completely, what happens to system integrity? What about intermittent failures, or bad ports? What are the safety implications?

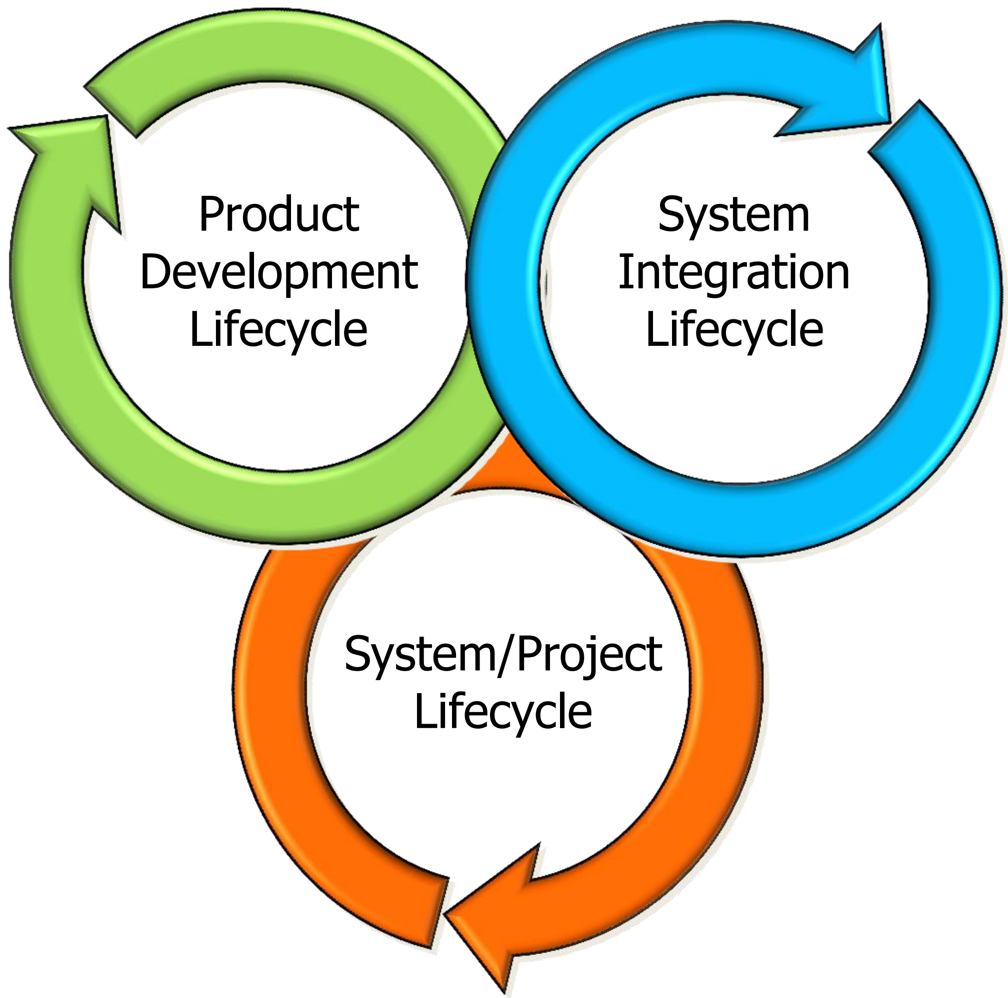


Security Level Vector Discussion

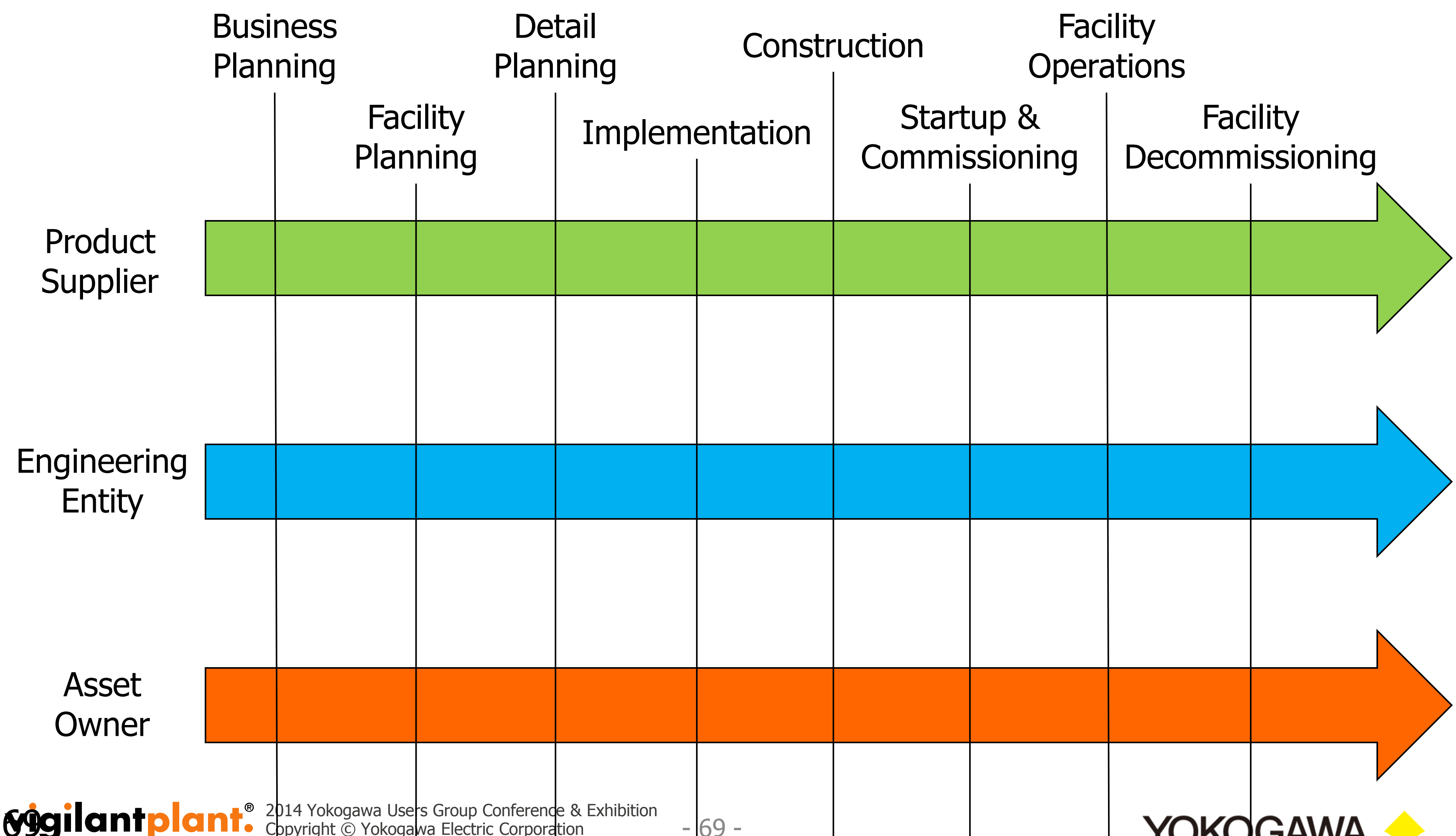
- Now, what about other components?
- How do each of the component capabilities roll into a system capability?
  - Mathematical/Additive?
  - Qualitative assessment of capabilities?
- How do capabilities relate to achieved security levels?



Security Lifecycles



Security Lifecycle



ISCI

Internationally Accredited Conformance Scheme

ISASecure certification programs are accredited as an ISO/IEC Guide 65 conformance scheme and ISO/IEC 17025 lab operations by ANSI/ACLASS.

- Provides global recognition for ISASecure certification
- Independent CB accreditation by ANSI/ACLASS and other global Accreditation Bodies such as JAB or UKAS
- ISASecure can scale on a global basis
- Ensures certification process is open, fair, credible, and robust.
- MOU's with AB's for ISASecure

ANSI Accredited Program PRODUCT CERTIFICATION

ANSI-ASQ National Accreditation Board

PROD JAB

Global Acceptance of ISASecure

- One set of certification criteria
- One certification test/assessment
- One globally recognized mark

Economically efficient for both suppliers and asset owners

Supporters-ISCI Member Companies

ISCI membership is open to all organizations

- Strategic membership
- Technical membership
- Government membership
- Associate membership
- Informational membership

Member organizations

- Chevron
- Aramco Services
- CSSC
- Codenomicon
- exida
- ExxonMobil
- Honeywell
- IT Promotion Agency, Japan
- Schneider Electric (Invensys)
- RTP Corp.
- Yokogawa
- ISA99 Committee Liaison

Global Adoption Expands to Japan

Japan Information-technology Promotion Agency and Control System Security Center

- IPA Translated ISASecure specifications to Japanese
- CSSC set up a test lab in Tagajo-city near Sendai Japan - Control System Security Center Certification Laboratory (CSSC-CL)
- CSSC-CL was accredited by JAB (Japan Accreditation Board) to ISASecure in Q1 2014
- CSSC and CSSC-CL are promoting ISASecure as part of the Japanese critical infrastructure security scheme.
- CSSC-CL certified two EDSA devices in Q2 2014

Japan CSSC Supporters

CSSC Associate Member Companies

1. Advanced Institute of Science and Technology
2. ALAXALA Networks Corporation
3. Azbil Corporation
4. Fuji Electric Co., Ltd.
5. Fujitsu Limited
6. Hitachi, Ltd.
7. Information Technology Promotion Agency
8. Japan Quality Assurance Organization
9. LAC Co., Ltd.
10. McAfee Co., Ltd.
11. Meidensha Corporation
12. Mitsubishi Electric Corporation
13. Mitsubishi Heavy Industries Ltd.
14. Mitsubishi Research Institute Inc.
15. Mori Building Co., Ltd.
16. NEC Corporation
17. NRI Secure Technologies Ltd.
18. NTT Communications Corporation
19. OMRON Corporation
20. The University of Electro-Communications
21. Tohoku Information Systems Company, Incorporated
22. Toshiba Corporation
23. Toyota Info. Technology Center Co., Ltd.
24. Trend Micro Incorporated
25. Yokogawa Electric Corporation

CSSC Supporter Companies

1. Ixia Communications K.K.
2. Japan Nuclear Security System Co., Ltd
3. OTSL Inc.
4. Rock international
5. The Japan Gas Association(JGA)
6. TOYO Corporation

Three ISASecure® certifications available

1. **Embedded Device Security Assurance (EDSA)** IEC-62443-4-2

   Certified Device ISASecure

2. **System Security Assurance (SSA)** IEC-62443-3-3

   Certified System ISASecure

3. **Security Development Lifecycle Assurance (SDLA)** IEC-62443-4-1

   "An ISASecure Certified Development Organization"

ISASecure™

Embedded Device Security Assurance (EDSA)

EDSA Overview

- Certification that the supplier's product is robust against network attacks and is free from known security vulnerabilities
- Meets requirements of ISA/IEC-62443-4-2 for embedded devices (will be re-aligned with 4-2 when formally approved by IEC)
- Currently available – 7 devices certified with more devices under assessment

What is an Embedded Device?

Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process, examples:

- Programmable Logic Controller (PLC)
- Distributed Control System (DCS) controller
- Safety Logic Solver
- Programmable Automation Controller (PAC)
- Intelligent Electronic Device (IED)
- Digital Protective Relay
- Smart Motor Starter/Controller
- SCADA Controller
- Remote Terminal Unit (RTU)
- Turbine controller
- Vibration monitoring controller
- Compressor controller

ISASecure EDSA Certification Program

ISASecure

Embedded Device Security Assurance (EDSA)

Software Development Security Assessment (SDSA)

Detects and Avoids systematic design faults

- The vendor’s software development and maintenance processes are audited
- Ensures the organization follows a robust, secure software development process

Functional Security Assessment (FSA)

Detects Implementation Errors / Omissions

- A component’s security functionality is audited against its derived requirements for its target security level
- Ensures the product has properly implemented the security functional requirements

Communications Robustness Testing (CRT)

Identifies vulnerabilities in networks and devices

- A component’s communication robustness is tested against communication robustness requirements
- Tests for vulnerabilities in the 4 lower layers of OSI Reference Model

ISASecure™

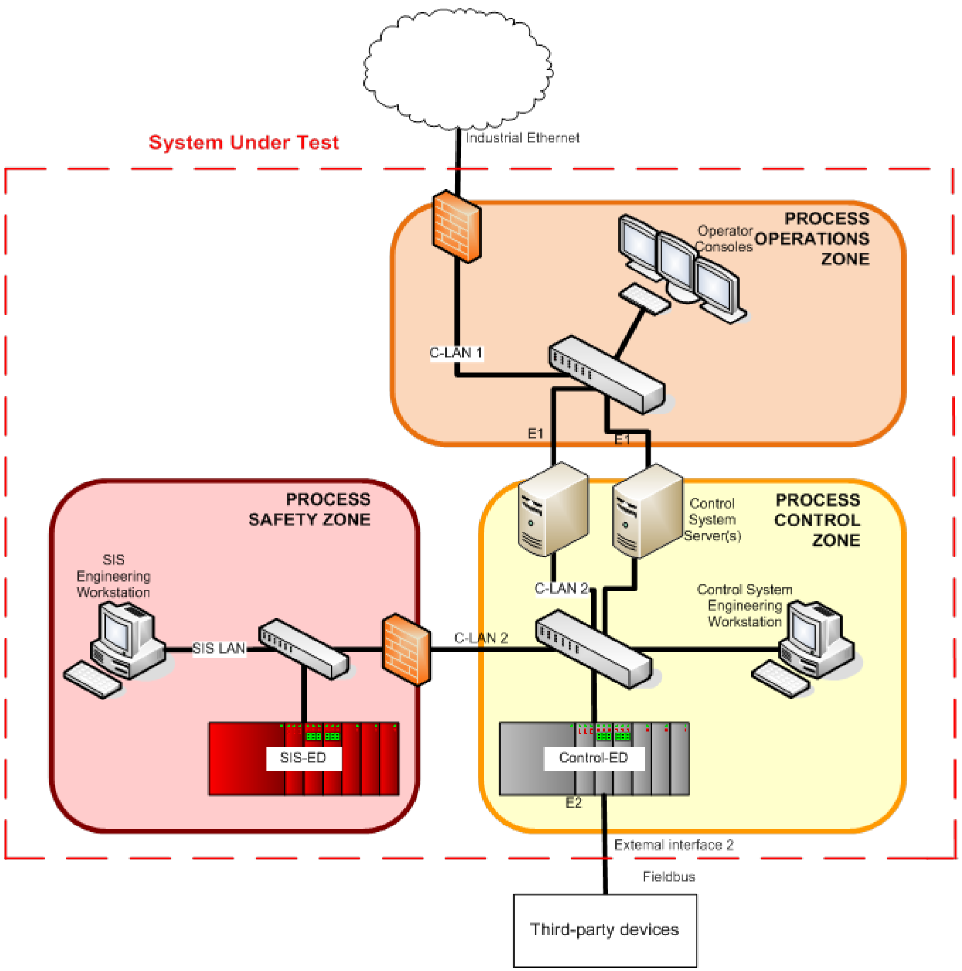
System Security Assurance (SSA)

SSA Overview

- Certification that the supplier's product is robust against network attacks and is free from known security vulnerabilities
- Meets requirements of ISA/IEC-62443-3-3 (SSA was re-aligned with 3-3 by ISCI in 2013 when it was approved by IEC)
- Available as of Q1 2014

What is a “System” ?

- Industrial Control System (ICS) or SCADA system
- Available from a single supplier
- Supported by a single supplier
- Components are integrated into a single system
- May consist of multiple Security Zones
- Can be identified by a product name and version
- Off the shelf; not site or project engineered yet



ISASecure SSA Certification Program

ISASecure

System Security Assessment (SSA)

Security Development Lifecycle Assessment (SDLA)

Ensures Security Was Designed-In

- The supplier's system development and maintenance processes are audited for security practices
- Ensures the system was designed following a robust, secure development process

Functional Security Assessment (FSA)

Ensures Fundamental Security Features are Provided

- A system's security functionality is audited against defined requirements for its target security level
- Ensures the system has properly implemented the security functional requirements

System Robustness Testing (SRT) and Vulnerability Identification Testing (VIT)

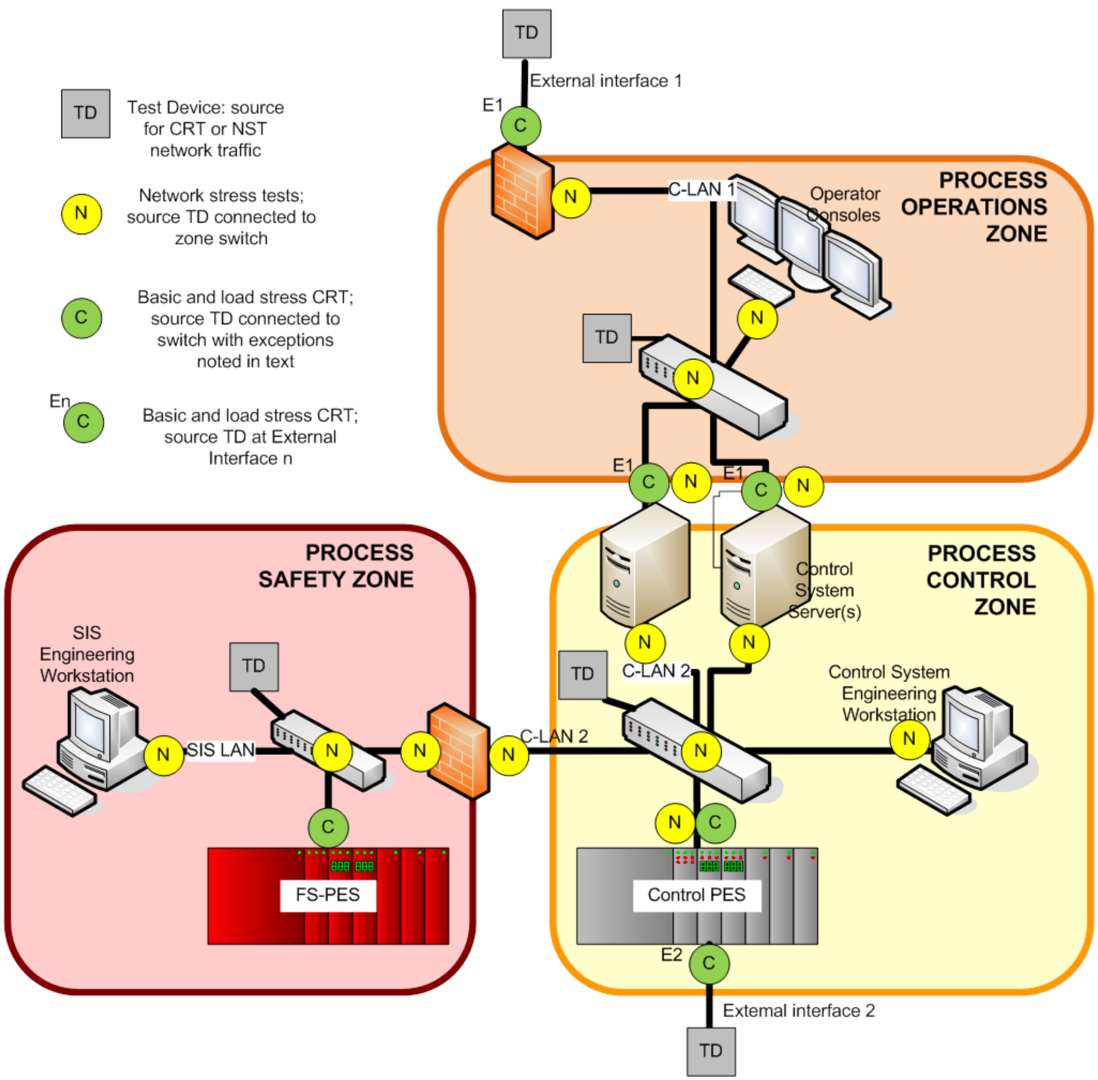
Identifies Vulnerabilities in Actual Implementation

- Structured penetration testing at all entry points
- Scan for known vulnerabilities (VIT)
- Combination of CRT and other techniques

SSA System Robustness Test

- Asset Discovery Scan
  - scan to discover the components on the network
- Communications Robustness Test
  - verify that essential functions continue to operate under high network load and malformed packets
- Network Stress Test
  - verify that essential functions continue to operate under high network load
- Vulnerability Identification Test
  - scan all components for the presence of known vulnerabilities (using Nessus)
  - based on National Vulnerability Database

SSA System Robustness Test



ISASecure™

Security Development Lifecycle Assurance (SDLA)

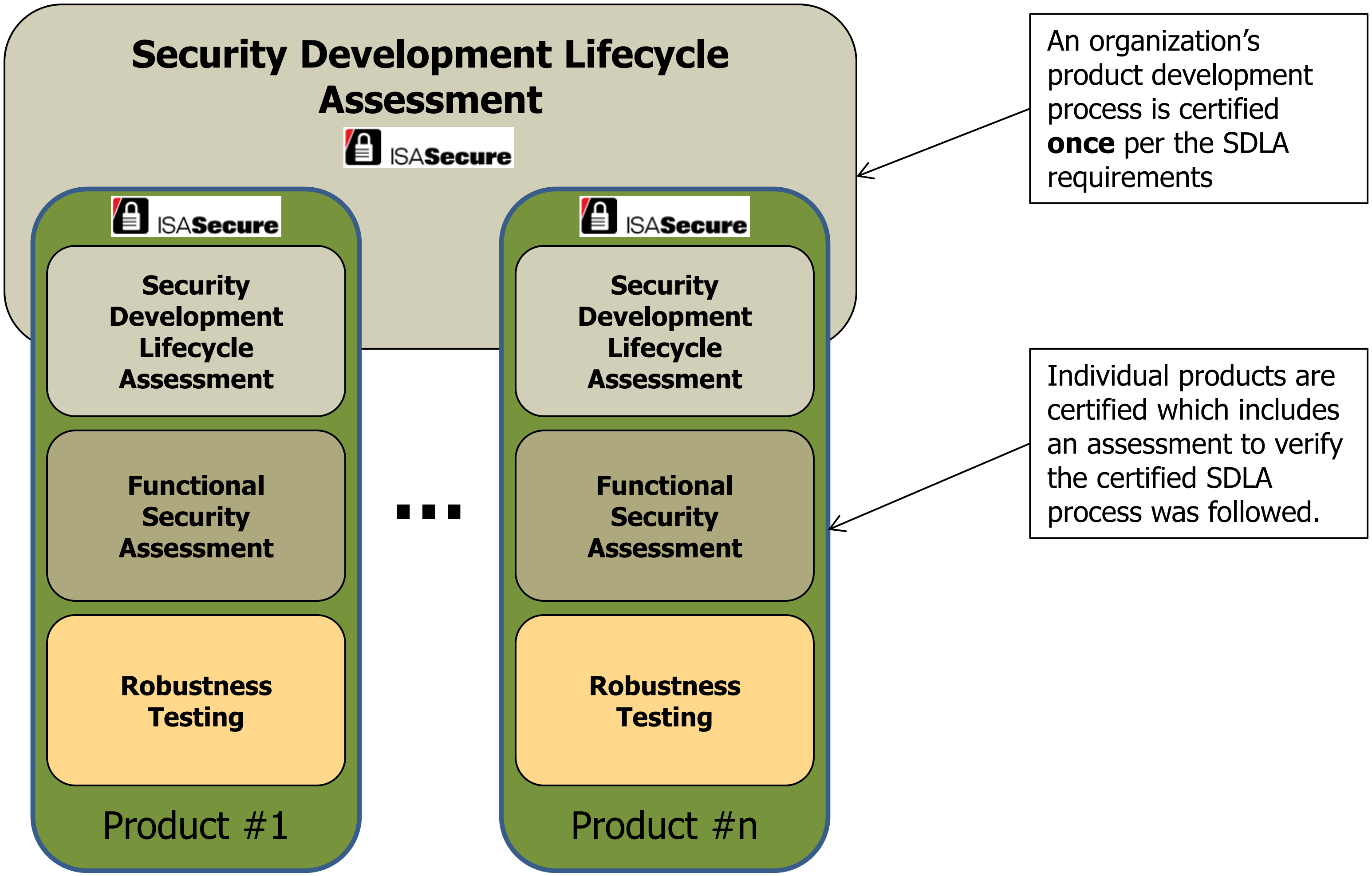
SDLA Overview

- Certification that the supplier's product development work process includes security considerations throughout the lifecycle.
  (Organization process certification)
- Meets requirements of ISA/IEC-62443-4-1
  (will be re-aligned with 4-1 when it is formally approved by IEC)
- Based on several industry-recognized security development lifecycle processes
- Launched May 2014

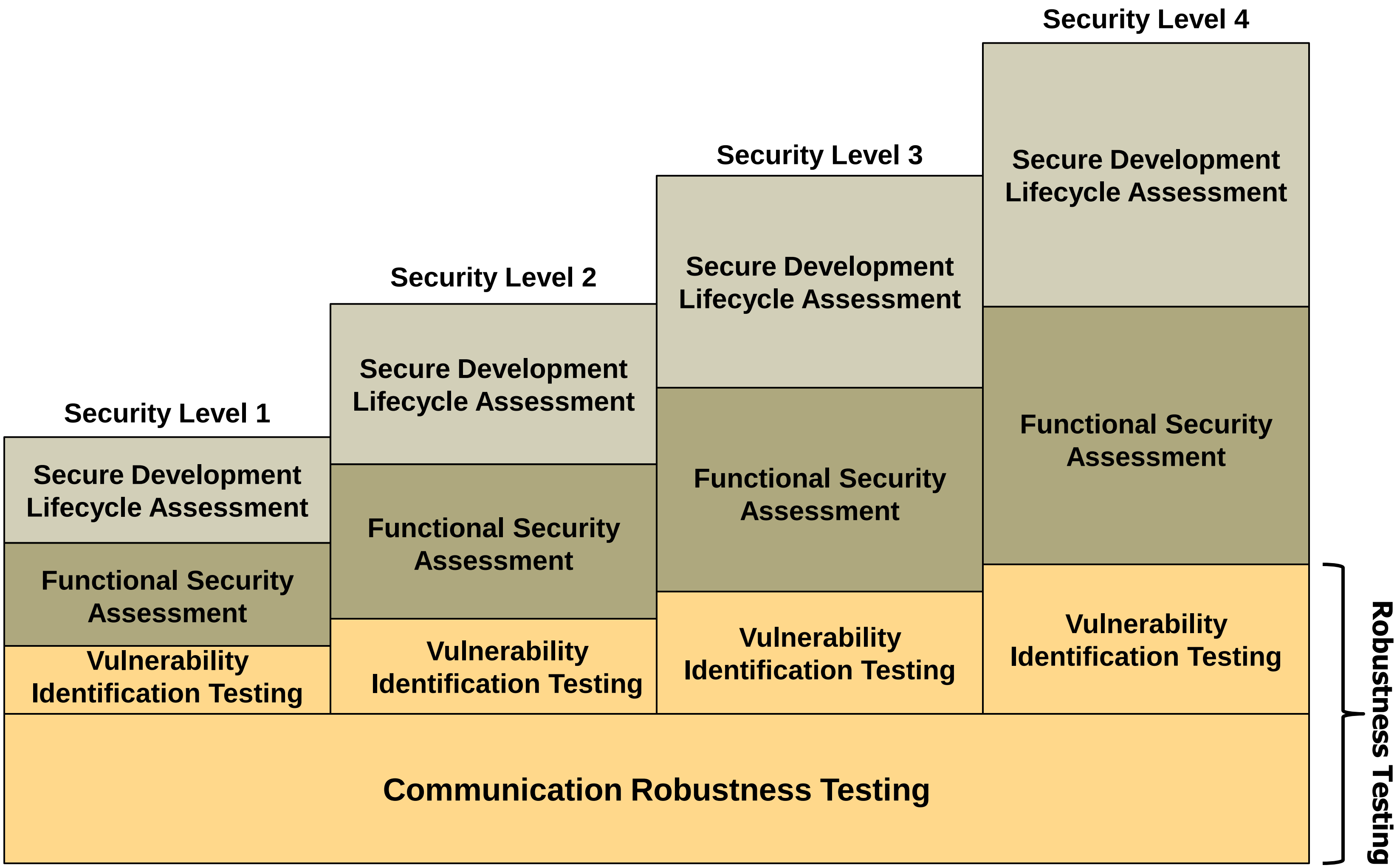
SDLA Phases

1. Security Management Process
2. Security Requirements Specification
3. Security Architecture Design
4. Security Risk Assessment (Threat Model)
5. Detailed Software Design
6. Document Security Guidelines
7. Module Implementation & Verification
8. Security Integration Testing
9. Security Process Verification
10. Security Response Planning
11. Security Validation Testing
12. Security Response Execution

Multiple Product Certification



Security Levels



Test Tools Available for Use in ISASecure

Communication Robustness Test tools

1. Codenomicon – Defensics X
2. FFR – Raven
3. Wurldtech – Achilles

Vulnerability Scanning Tools

1. Tenable - Nessus

Simplified Asset Owner Use Case

- Establishes and operates a security program based upon 62443-2-1 & -2-2
- Maintains a patch management system using -2-3
- Certifies that suppliers & vendors comply with -2-4
- Measures achieved security using metrics from -1-3
  - Uses zone & conduit model to design their systems based upon -3-2
  - Builds and/or procures systems that comply with technical requirements in -3-3
  - Builds and/or procures components that comply with:
    - Product development lifecycle in -4-1
    - Technical requirements in -4-2

In Summary

- ISA/IEC-62443 standards set the requirements for Industrial Automation and Control Systems
- ISASecure certifies that suppliers and products meet the ISA/IEC-62443 standards
- Asset Owners have confidence that the IACS products they purchase are robust against network attacks and are free from known security vulnerabilities

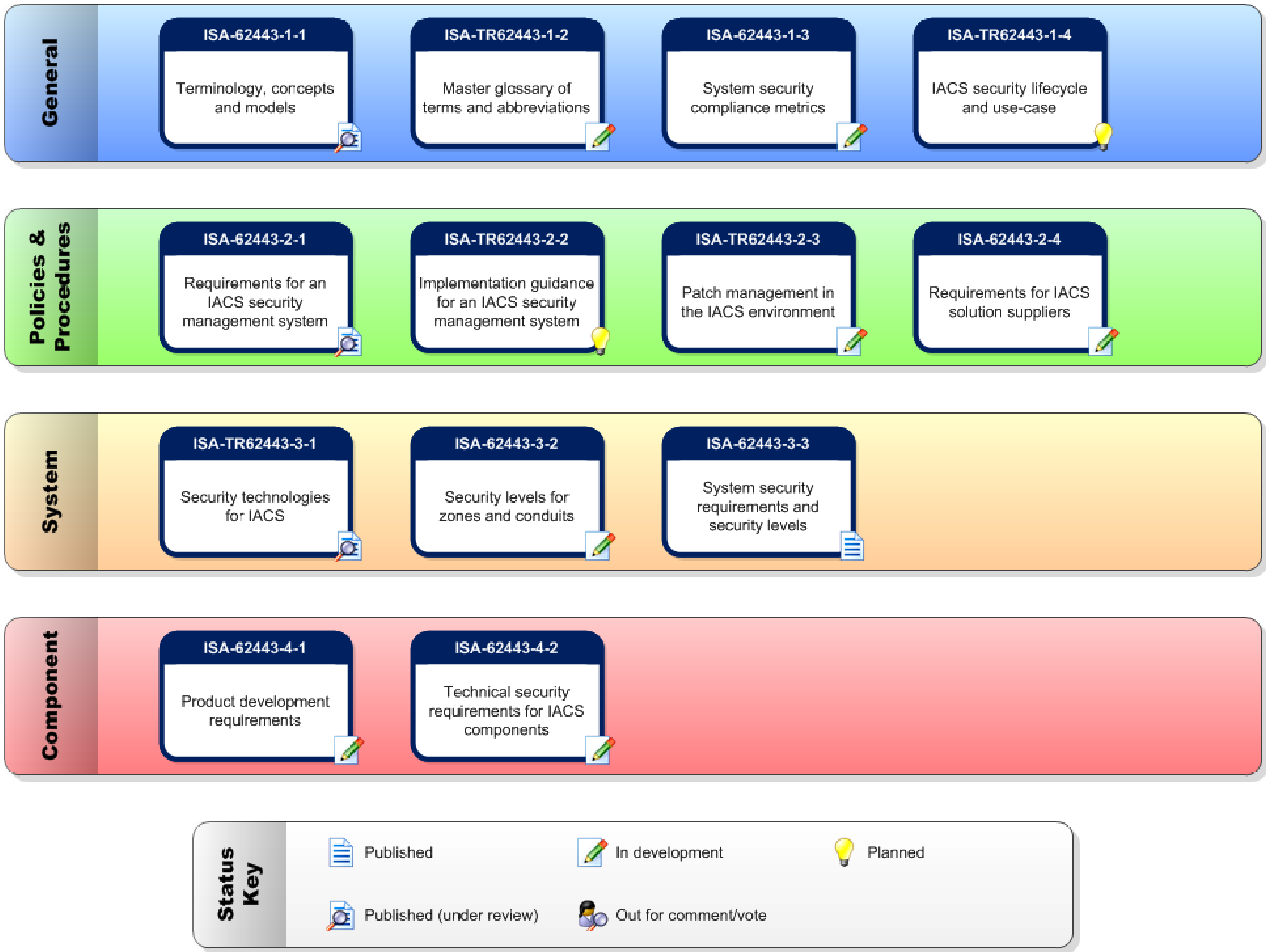
USA Government – Executive Order

- ISA under Automation Federation facilitating NIST effort to develop a cybersecurity framework.
- Draft framework 1.0 completed in 2013. IEC 62443 standards are prominent in the document.
- Cybersecurity Framework 2.0. Plans are underway for a meeting this Fall in Illinois by the White House and NIST

Glossary

Acronym	Description
ACLASS	One of three brands of the ANSI-ASQ National Accreditation Board
ANSI	American National Standards Institute
CSSC	Control System Security Center, Japan-R&D and test lab in Tagajo-city Japan
CSSC-CL	Control System Security Center, Japan – certification lab operation
ISA	International Society of Automation
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IPA	Information-technology Promotion Agency, Japan
ISCI	ISA Security Compliance Institute
JAB	Japan Accreditation Board-Japan based IEC accreditation body (AB)

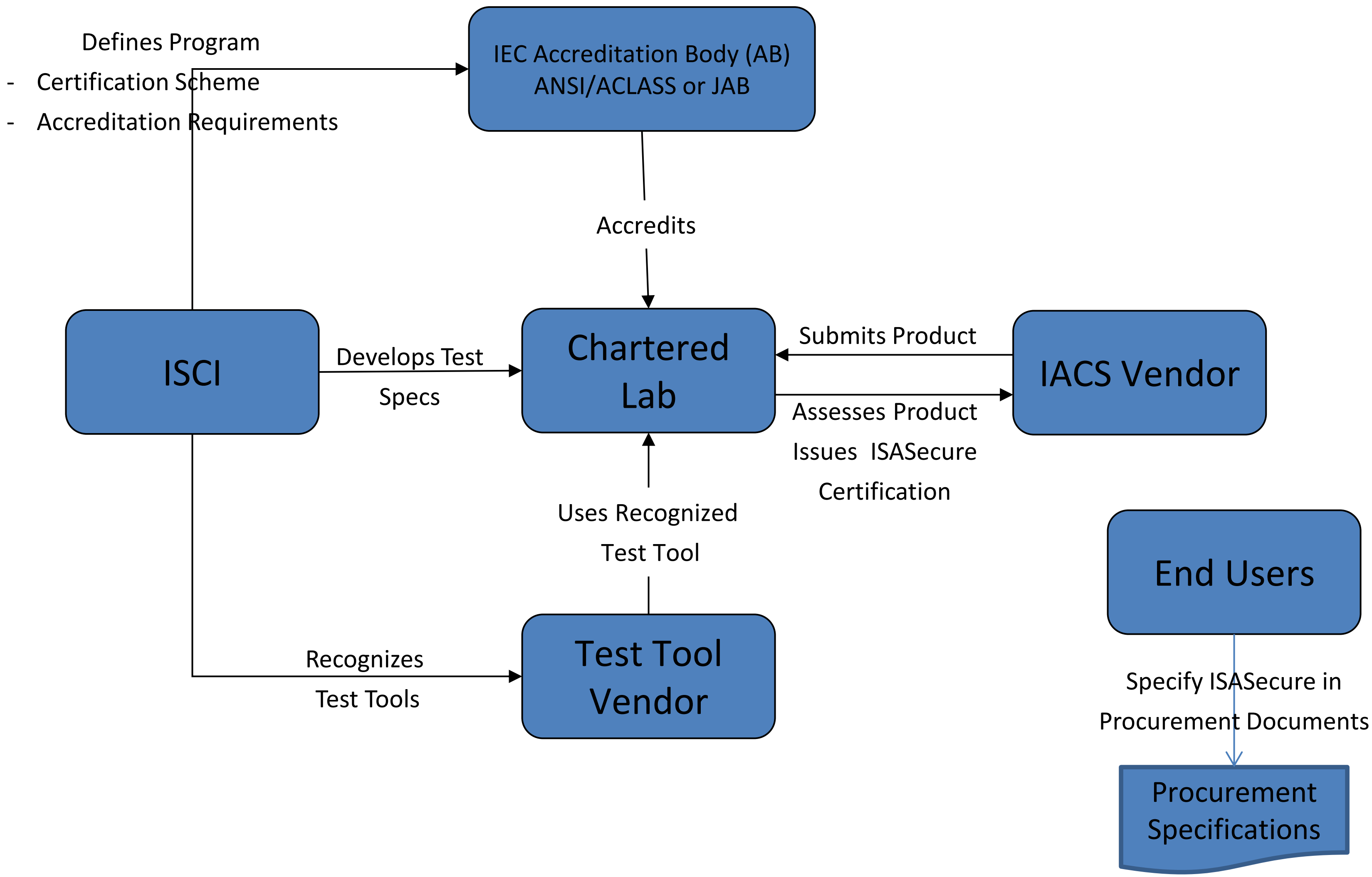
ISA 62443 Status (July 2014)



ISASecure Certified Devices – Q3 2014

Supplier	Type	Model	Version	Level	Test Lab
Honeywell Process Solutions	Safety Manager	HPS 1009077 C001	R145.1	EDSA 2010.1 Level 1	exida
RTP Corporation	Safety manager	RTP 3000	A4.36	EDSA 2010.1 Level 2	exida
Honeywell Process Solutions	DCS Controller	Experion C300	R400	EDSA 2010.1 Level1	exida
Honeywell Process Solutions	Fieldbus Controller	Experion FIM	R400	EDSA 2010.1 Level 1	exida
Yokogawa Electric Corporation	Safety Control System	ProSafe-RS	R3.02.10	EDSA2010.1 Level 1	exida
Yokogawa Electric Corporation	DCS Controller	CENTUM VP	R5.03.00	EDSA 2010.1 Level 1	CSSC-CL
Hitachi, Ltd.	DCS Controller	HISEC 04/R900E	01-08-A1	EDSA 2010.1 Level 1	CSSC-CL

ISASecure Program Structure



CSSC-CL Receives Accreditation from JAB

April 2014 Photo-Mr. Hideaki Kobayashi, Vice-President of CSSC-CL showing Guide 65 and ISO 17025 accreditation certificates from JAB for ISASecure EDSA conformance scheme.

CSSC-CL ISCI Meeting July 2014

July 2014 Photo-Andre Ristaino, ISCI Managing Director with Mr. Hideaki Kobayashi, Vice-President of CSSC-CL and team members during tour and celebration of accreditation by JAB and completion of first two ISASecure EDSA certifications.

Questions?

No bears were hurt in the making of this presentation

Contact details

Graham Speake

Vice President and Chief Product Architect, NexDefense
ICS 410 Course Instructor, The SANS Institute

Email: graham.speake@nexdefense.com
LinkedIn: Graham Speake

Who to contact for ISA99 committee

Eric Cosman

Co-Chairman ISA99 Committee

eric.cosman@gmail.com

Jim Gilsinn

Co-Chairman ISA99 Committee

jimgilsinn@gmail.com

ISASecure certificate - exida

The manufacturer may use the marks:

Certified Device ISASecure

CERTIFIED exida ISASecure LEVEL 1 CAPABLE

Reports:
HPS FIM 1108033 R3 V1R0
CRT Test Report
HPS FIM 1108033 R4 V1R0
Certification Report

Validity:
This Certificate is restricted to the specified version of the referenced Device (including the model number, hardware / firmware / software version) set forth in this Certificate. Furthermore, the unit shall be operated in a network and operational environment meeting the assumptions in the Certification Report.

Revision 1.3 August 21, 2013

ISASecure Chartered Laboratory:
exida
64 North Main St.
Sellersville, PA 18960
License: ISCI-CL0001
ACLASS Cert No: AT-1531

exida Certification Services

Certificate / Certificat
Zertifikat / 合格証

HPS 1108033 C002

exida hereby confirms that the

Experion® Series C FIM

Manufactured by

Honeywell Process Solutions
Phoenix, Arizona
USA

Has been assessed per the relevant requirements of:

ISASecure™ Embedded Device Security Assurance Program
2010.1

And meets the requirements for:

LEVEL 1

Model Number:	*Series C FIM with 9 Port FTE Control Firewall Module and Input Output Termination Assemblies (IOTA)*
Firmware Version:	*R400*

exida Certification

Authorized Representative

Who to Contact to Certify Products

ISASecure EDSA Chartered Lab:

Exida – USA and EU

Mike Medoff
Director of Security Services
Phone: (215) 453-1720
Fax: (215) 257-1657
Email: mmedoff@exida.com
Website: http://www.exida.com

ANSI Accredited Program
PRODUCT CERTIFICATION

ANSI-ASQ National Accreditation Board

ISASecure EDSA Chartered Lab:

CSSC - Japan

Kenzo Yoshimatsu

Phone: +81 (22) 353-6751
Email: kenzo.yoshimatsu@css-center.or.jp
Website: http://www.css-center.or.jp

PROD
JAB

Who to contact for ISCI Membership

Andre Ristaino
Managing Director, ASCI
Phone: 919-990-9222
Fax: 919-549-8288
Email: aristaino@isa.org
Website: http://www.isasecure.org

Section Divider

Thank-You