Jim Gilsinn

National Institute of Standards & Technology (NIST)
Engineering Laboratory

Kevin P. Staggs, CISSP

Engineering Fellow
Advanced Technology Labs,
Honeywell Automation and Control

Mike Ahmadi

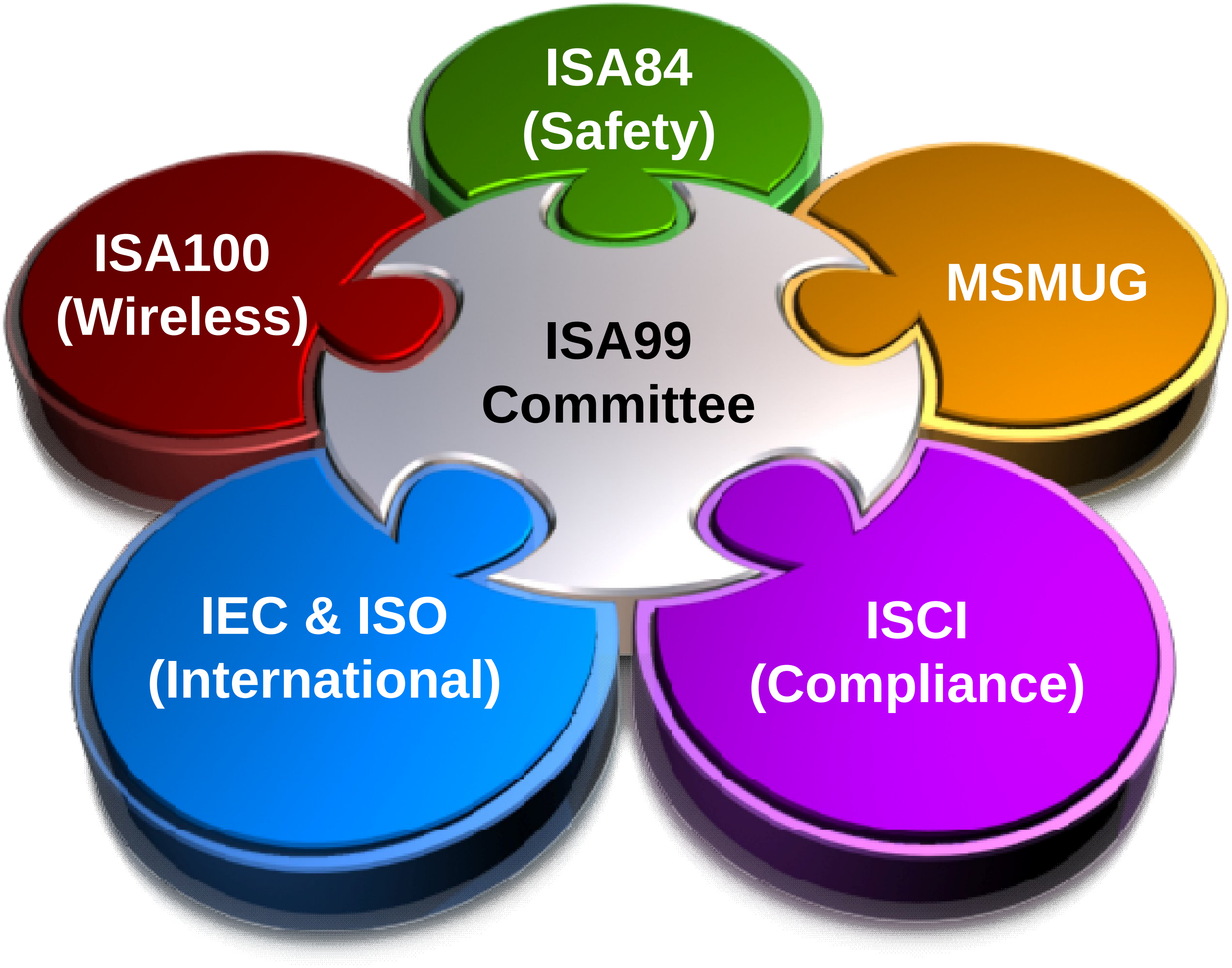
GraniteKey LLC
Vice President - Operations

ISA99 Committee

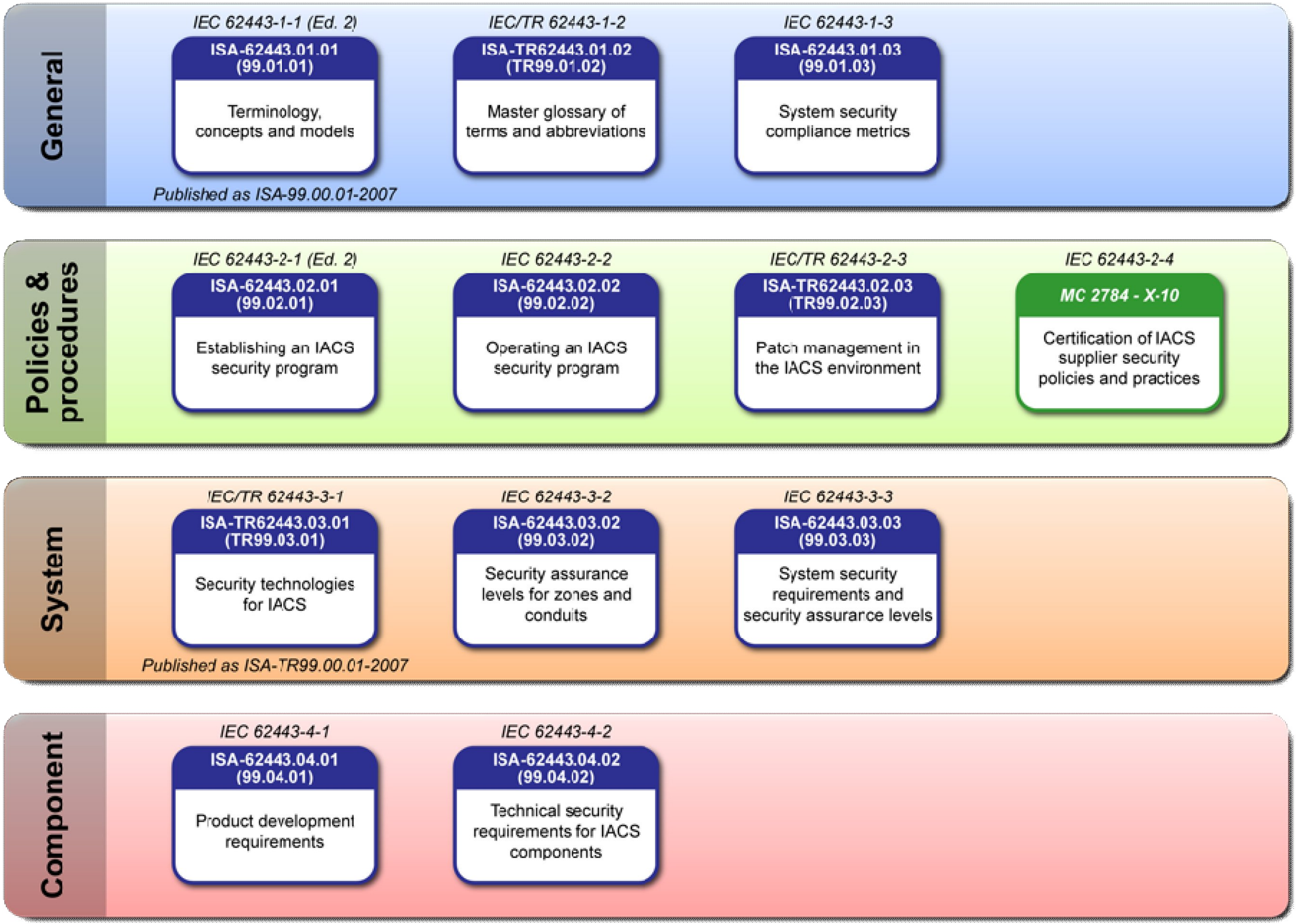
- Addresses Industrial Automation and Control Systems Security
- Compromise could result in:
  - Endangerment of public or employee safety
  - Loss of public confidence
  - Violation of regulatory requirements
  - Loss of proprietary or confidential information
  - Economic loss
  - Impact on entity, local, state, or national security

- Over 500 members
- Sectors include:
  - Chemical Processing
  - Petroleum Refining
  - Food and Beverage
  - Power
  - Pharmaceuticals
  - Discrete Part Manufacturing
  - Process Automation Suppliers
  - IT Suppliers
  - Government Labs
  - Consultants

ISA99 Connecting with Others



ISA-99 & IEC 62443 Series



General	*IEC 62443-1-1 (Ed. 2)* ISA-62443.01.01 (99.01.01) Terminology, concepts and models	*IEC/TR 62443-1-2* ISA-TR62443.01.02 (TR99.01.02) Master glossary of terms and abbreviations	*IEC 62443-1-3* ISA-62443.01.03 (99.01.03) System security compliance metrics	
Policies & procedures	*IEC 62443-2-1 (Ed. 2)* ISA-62443.02.01 (99.02.01) Establishing an IACS security program	*IEC 62443-2-2* ISA-62443.02.02 (99.02.02) Operating an IACS security program	*IEC/TR 62443-2-3* ISA-TR62443.02.03 (TR99.02.03) Patch management in the IACS environment	*IEC 62443-2-4* *MC 2784 - X-10* Certification of IACS supplier security policies and practices
System	*IEC/TR 62443-3-1* ISA-TR62443.03.01 (TR99.03.01) Security technologies for IACS	*IEC 62443-3-2* ISA-62443.03.02 (99.03.02) Security assurance levels for zones and conduits	*IEC 62443-3-3* ISA-62443.03.03 (99.03.03) System security requirements and security assurance levels	
Component	*IEC 62443-4-1* ISA-62443.04.01 (99.04.01) Product development requirements	*IEC 62443-4-2* ISA-62443.04.02 (99.04.02) Technical security requirements for IACS components		

Published as ISA-99.00.01-2007

Published as ISA-TR99.00.01-2007

Current as of December 2011

Foundational Requirements & SALS

- Foundational Requirements
  - Identification & Authentication Control
  - Use Control
  - Data Integrity
  - Data Confidentiality
  - Restricted Data Flow
  - Timely Response to Events
  - Resource Availability

- Types of Security Assurance Levels
  - Target SALs
  - Achieved SALs
  - Capability SALs

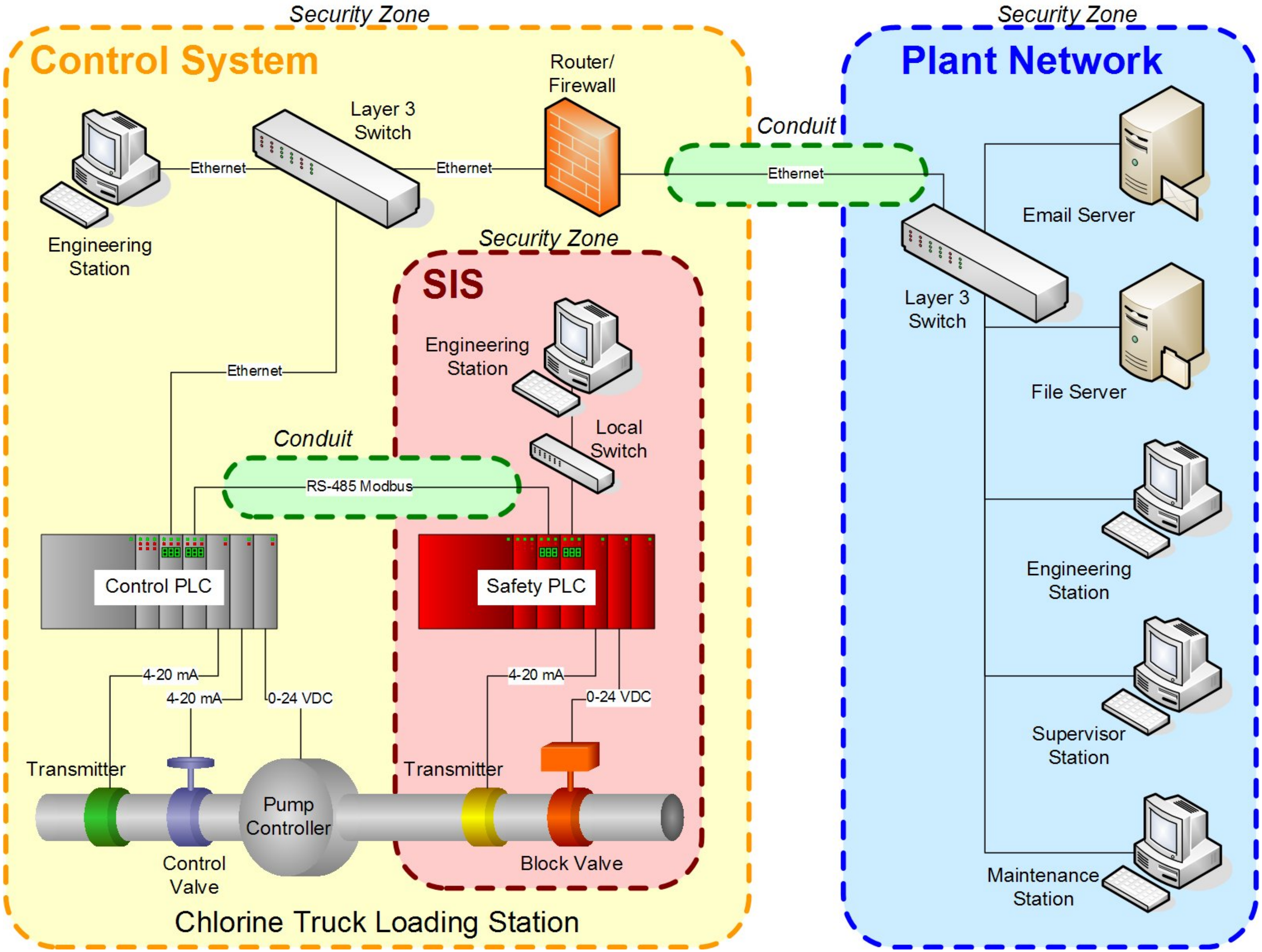
Level Definitions – Protection Against ...

- 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

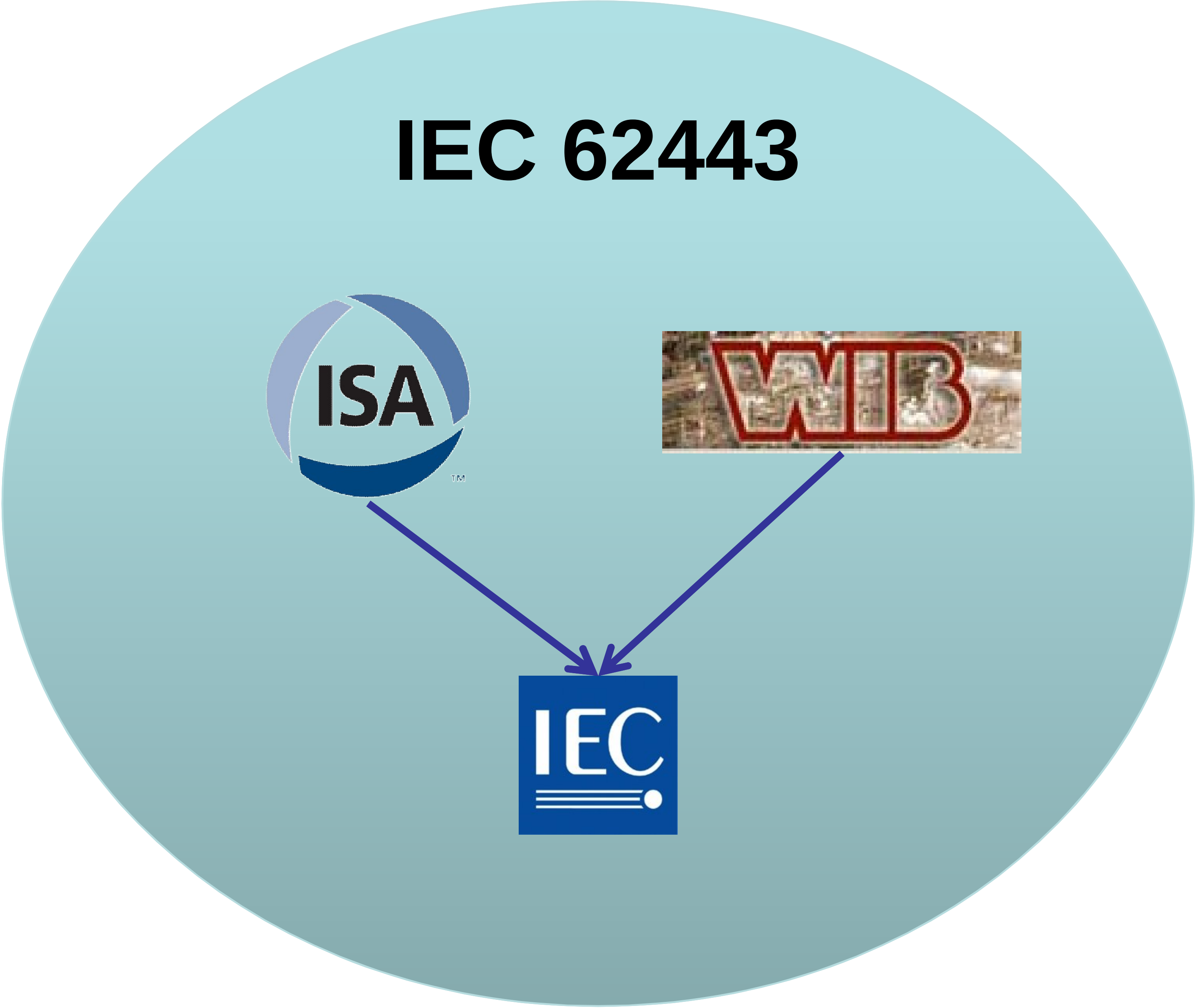
Simplified Asset Owner Use Case

- Establishes and operates a security program based upon -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

Example of SALs



A Truly Collaborative Effort



IEC 62443

The WIB – A Collection of End Users

- The Werkgroep Instrument Beoorderling (WIB), or the international instrument users association
- Comprised of over 50 end-users from various industrial sectors located around the world
- Collaborate to solve various manufacturing challenges
- History
  - Founded In 1962 (The Netherlands)
  - 75+ Global End-user Members
  - Plant Security Sub-working Group led by Shell cyber security team

GDF SUEZ

AkzoNobel
Tomorrow's Answers Today

TOTAL

bp

ارامكو السعودية
Saudi Aramco

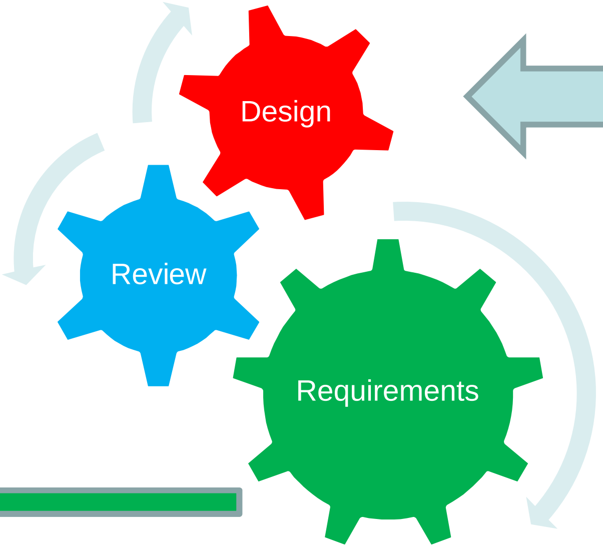
ExxonMobil

DOW

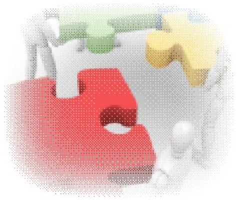
The WIB Storyline: From Concept To Standard

NERC/CIP, CFATS, DHS Procurement Language, ISA-99, NIST 800-53, ISO 2700x, NISTIR 7628 etc, etc, etc.

Select the low hanging fruit



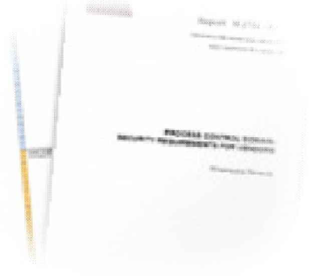
First industry driven standard



Grid-Interop

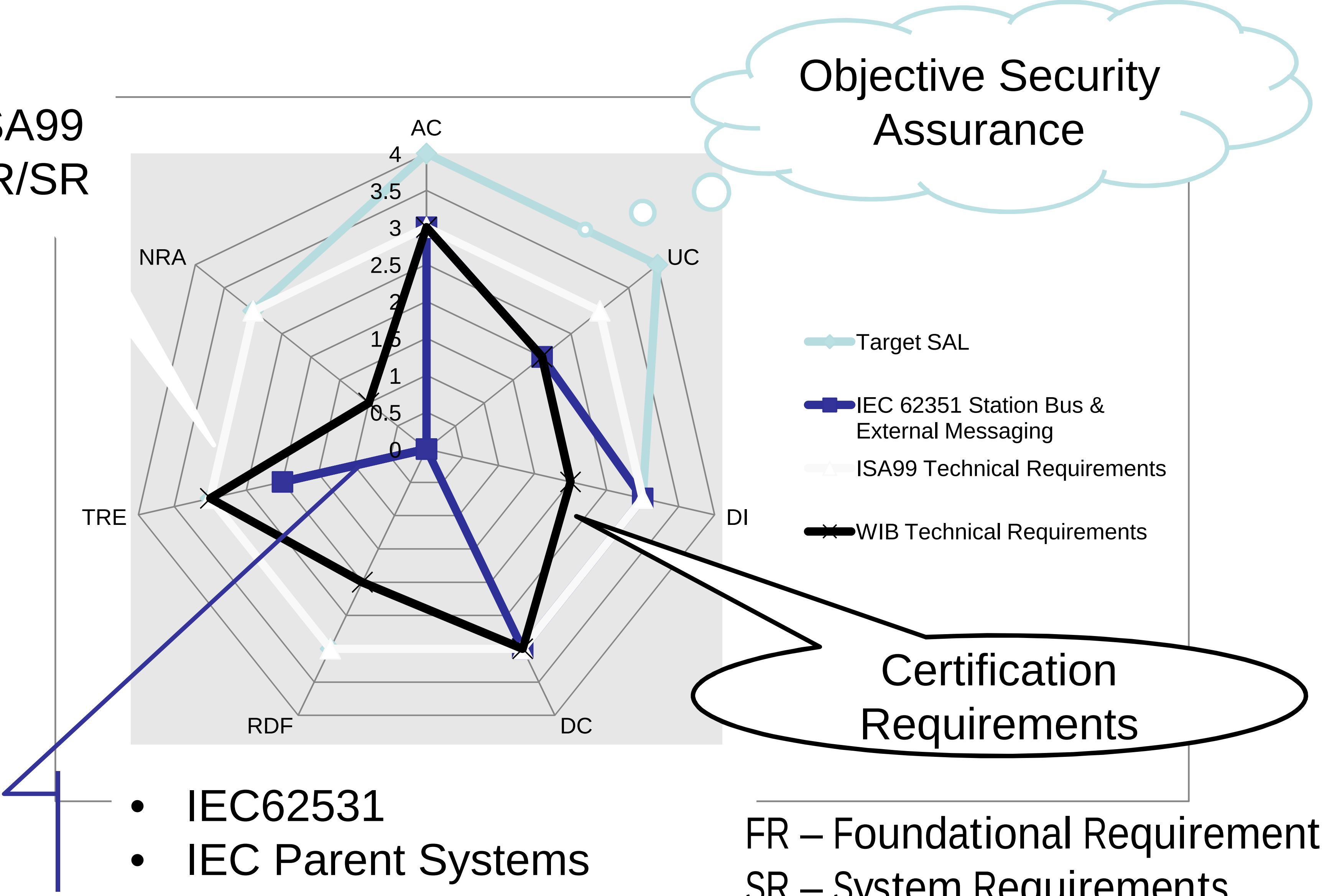
The WIB Security Requirements

- The WIB Plant Security Working Group (PSWG) announced version 2 of the security requirements for Vendor’s in November 2010
  - 2 versions with 4 revisions
  - 50+ stakeholders: vendors, end-users, consultants, subject matter experts
  - Over 1000 comments/change requests
  - Aligned To IEC framework for future adoption (IEC 62443-2-4 approval pending)



Comparison of Security Assurance

ISA99
FR/SR



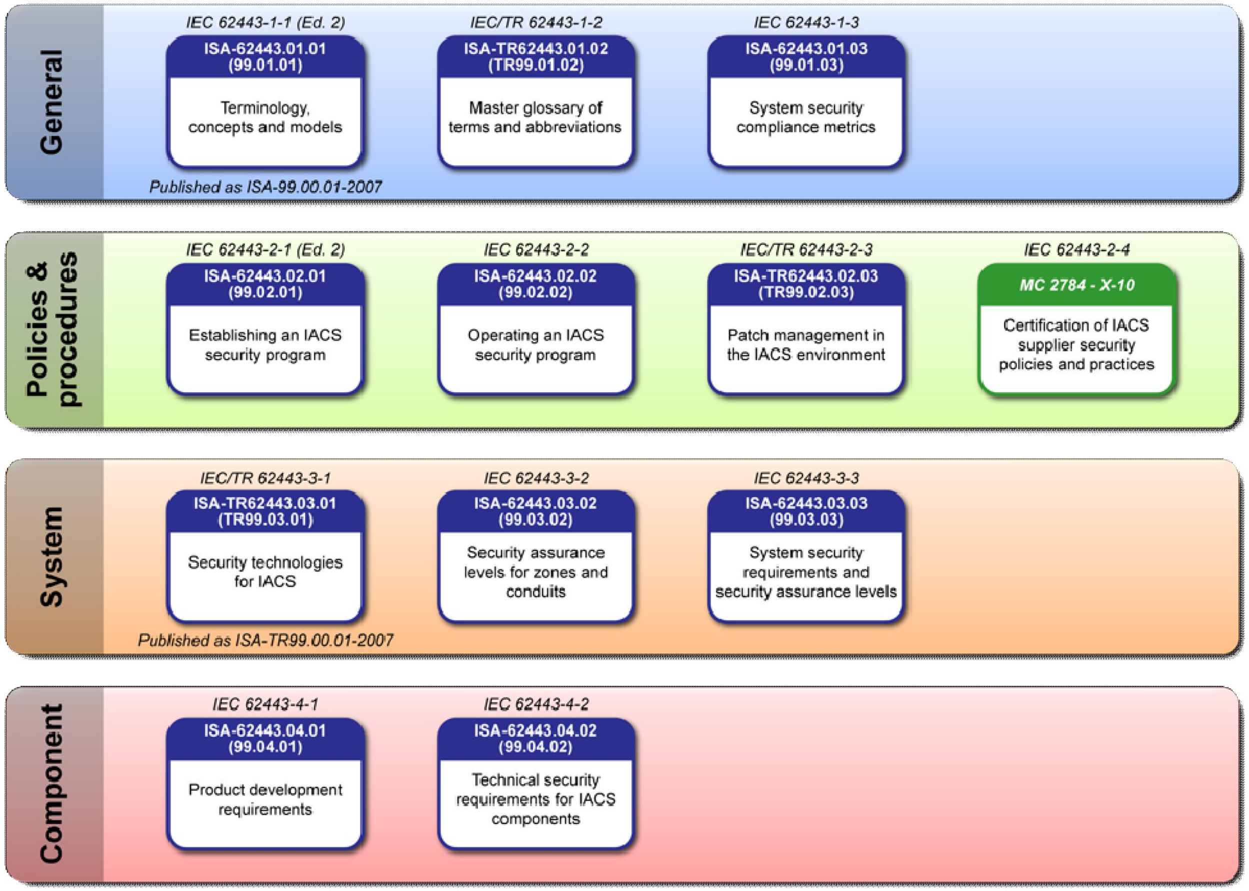
Objective Security Assurance

Certification Requirements

- IEC62531
- IEC Parent Systems

FR – Foundational Requirements
SR – System Requirements

Alignment with ISA99 & NISTIR 7628



General

IEC 62443-1-1 (Ed. 2) — ISA-62443.01.01 (99.01.01) — Terminology, concepts and models

IEC/TR 62443-1-2 — ISA-TR62443.01.02 (TR99.01.02) — Master glossary of terms and abbreviations

IEC 62443-1-3 — ISA-62443.01.03 (99.01.03) — System security compliance metrics

Published as ISA-99.00.01-2007

Policies & procedures

IEC 62443-2-1 (Ed. 2) — ISA-62443.02.01 (99.02.01) — Establishing an IACS security program

IEC 62443-2-2 — ISA-62443.02.02 (99.02.02) — Operating an IACS security program

IEC/TR 62443-2-3 — ISA-TR62443.02.03 (TR99.02.03) — Patch management in the IACS environment

IEC 62443-2-4 — MC 2784 - X-10 — Certification of IACS supplier security policies and practices

System

IEC/TR 62443-3-1 — ISA-TR62443.03.01 (TR99.03.01) — Security technologies for IACS

IEC 62443-3-2 — ISA-62443.03.02 (99.03.02) — Security assurance levels for zones and conduits

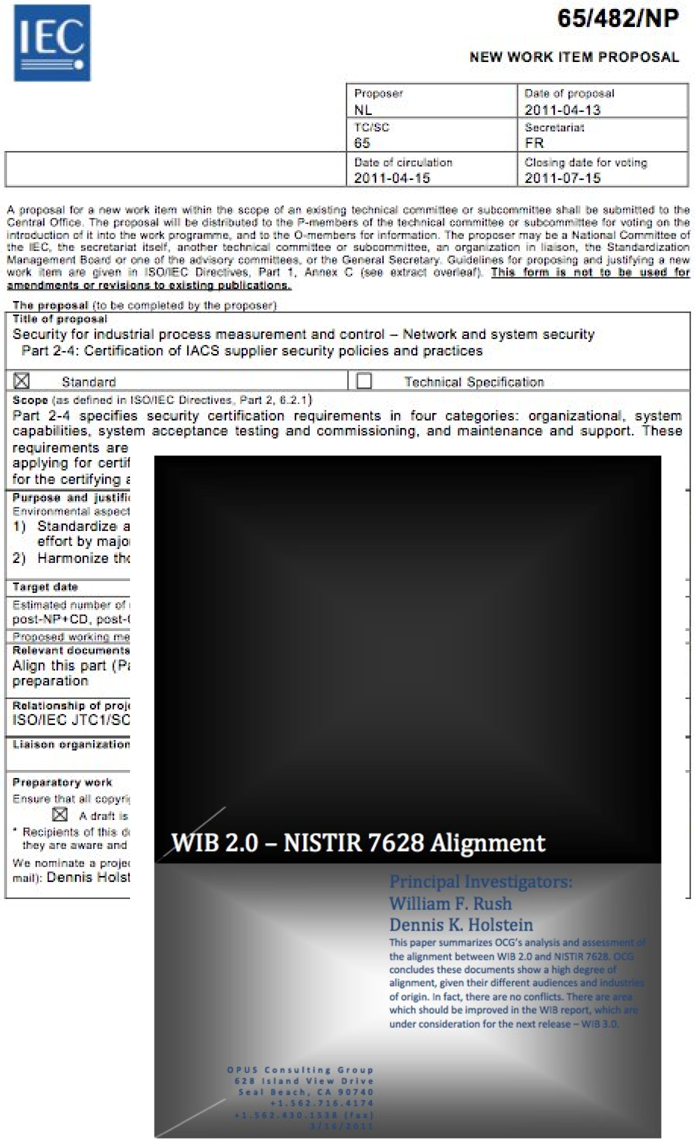
IEC 62443-3-3 — ISA-62443.03.03 (99.03.03) — System security requirements and security assurance levels

Published as ISA-TR99.00.01-2007

Component

IEC 62443-4-1 — ISA-62443.04.01 (99.04.01) — Product development requirements

IEC 62443-4-2 — ISA-62443.04.02 (99.04.02) — Technical security requirements for IACS components



IEC

65/482/NP

NEW WORK ITEM PROPOSAL

	Proposer NL	Date of proposal 2011-04-13
	TC/SC 65	Secretariat FR
	Date of circulation 2011-04-15	Closing date for voting 2011-07-15

A proposal for a new work item within the scope of an existing technical committee or subcommittee shall be submitted to the Central Office. The proposal will be distributed to the P-members of the technical committee or subcommittee for voting on the introduction of it into the work programme, and to the O-members for information. The proposer may be a National Committee of the IEC, the secretariat itself, another technical committee or subcommittee, an organization in liaison, the Standardization Management Board or one of the advisory committees, or the General Secretary. Guidelines for proposing and justifying a new work item are given in ISO/IEC Directives, Part 1, Annex C (see extract overleaf). **This form is not to be used for amendments or revisions to existing publications.**

The proposal (to be completed by the proposer)

Title of proposal
Security for industrial process measurement and control – Network and system security
Part 2-4: Certification of IACS supplier security policies and practices

☒ Standard □ Technical Specification

Scope (as defined in ISO/IEC Directives, Part 2, 6.2.1)
Part 2-4 specifies security certification requirements in four categories: organizational, system capabilities, system acceptance testing and commissioning, and maintenance and support. These requirements are
applying for certif
for the certifying a

Purpose and justific
Environmental aspect
1) Standardize a
effort by majo
2) Harmonize the

Target date

Estimated number of
post-NP+CD, post-C

Proposed working me

Relevant documents
Align this part (Pa
preparation

Relationship of proj
ISO/IEC JTC1/SC

Liaison organization

Preparatory work
Ensure that all copyri
☒ A draft is
* Recipients of this d
they are aware and

We nominate a proje
mail): Dennis Holst

WIB 2.0 – NISTIR 7628 Alignment

Principal Investigators:
William F. Rush
Dennis K. Holstein

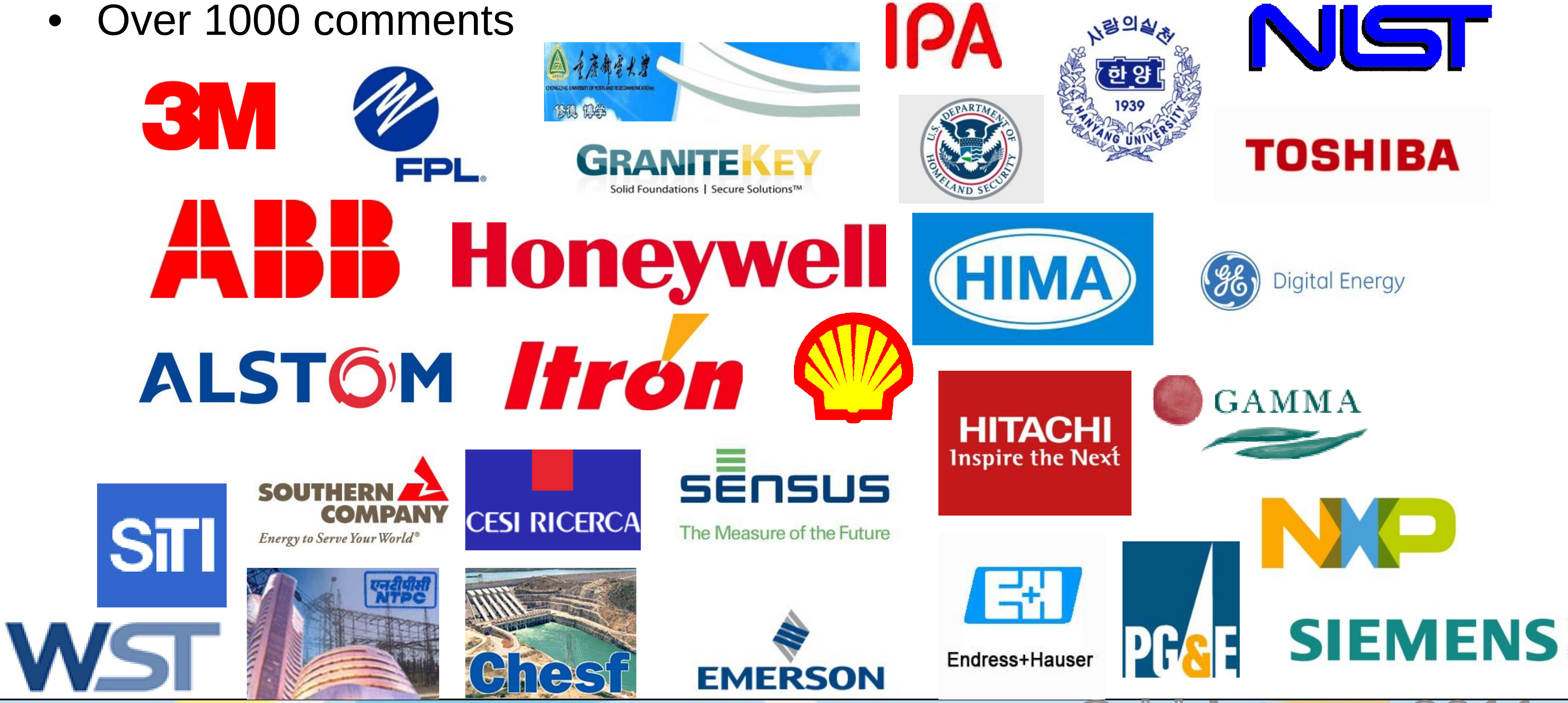
This paper summarizes OCG's analysis and assessment of the alignment between WIB 2.0 and NISTIR 7628. OCG concludes these documents show a high degree of alignment, given their different audiences and industries of origin. In fact, there are no conflicts. There are area which should be improved in the WIB report, which are under consideration for the next release – WIB 3.0.

OPUS Consulting Group
628 Island View Drive
Seal Beach, CA 90740
+1.562.716.4174
+1.562.430.1538 (fax)
3/16/2011

Grid-Interop™

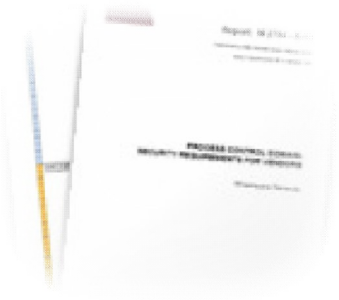
Enormous Outpouring of Participation In IEC Project

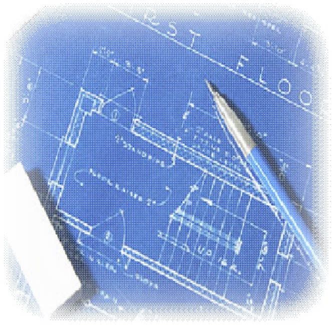
- Over 50 participating organizations from public, private, and academic sectors
- Participation from major countries (including US, China, Japan, Holland, France, Switzerland, Germany, Brazil…and many more)
- Over 1000 comments


IPA
사랑의실천 한양 1939 HANYANG UNIVERSITY
NIST
3M
FPL
重庆邮电大学 CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS 修德 博学
U.S. DEPARTMENT OF HOMELAND SECURITY
TOSHIBA
GRANITEKEY Solid Foundations | Secure Solutions™
ABB
Honeywell
HIMA
GE Digital Energy
ALSTOM
Itron
HITACHI Inspire the Next
GAMMA
SOUTHERN COMPANY Energy to Serve Your World®
CESI RICERCA
SENSUS The Measure of the Future
SiTI
NXP
एनटीपीसी NTPC
Chesf
EMERSON
Endress+Hauser
PG&E
SIEMENS
WST

From Requirements To Vendor Certification

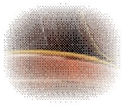
- Build on WIB 2.0
- Blessed by PSWG

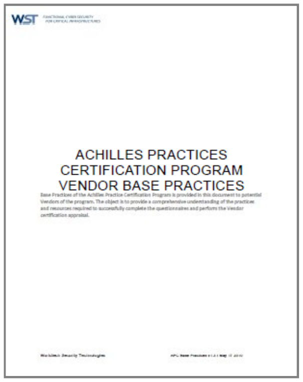

PROCESS CONTROL DOMAIN SECURITY REQUIREMENTS FOR VENDORS



- Scalable certification program
- Internationally accepted frameworks
- Formal, testable criteria

- Over a year of pilot programs
- Multiple vendors
- Various industry sectors




WST FUNCTIONAL CYBER SECURITY FOR CRITICAL INFRASTRUCTURES

ACHILLES PRACTICES
CERTIFICATION PROGRAM
VENDOR BASE PRACTICES

Base Practices of the Achilles Practice Certification Program is provided in this document to potential Vendors of the program. The object is to provide a comprehensive understanding of the practices and resources required to successfully complete the questionnaires and perform the Vendor certification appraisal.

Wurldtech Security Technologies APC Base Practices v1.1 | May 17 2010

- WIB accredited November 2010
- 1st certified vendor January 2011

Asset Owner Procurement needs

- Certifies that suppliers & vendors comply with -2-4 (WIB and APC)
- 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

ISA Security Compliance Institute (ISCI)

- Who We Are
  - Consortium of Asset Owners, Suppliers, and Industry Organizations formed in 2007 under the ISA Automation Standards Compliance Institute (ASCI)
- Mission
  - Establish a set of well-engineered specifications and processes for the testing and certification of critical control systems products
  - Decrease the time, cost, and risk of developing, acquiring, and deploying control systems by establishing a collaborative industry-based program among asset owners, suppliers, and other stakeholders

ISASecure™ Designation

- Trademarked designation that provides instant recognition of product security characteristics and capabilities
- Independent industry stamp of approval
- Similar to ‘Safety Integrity Level’ Certification (ISO/IEC 61508)

ANSI/ACLASS Accredited Conformance Scheme

- All ISASecure certifications accredited as an ISO/IEC Guide 65 conformance scheme by ANSI/ACLASS. This includes both ISO/IEC 17025 and ISO/IEC 17011. http://www.ansi.org/isasecure
  - Provides recognition for ISASecure certification
  - Independent CB accreditation by ANSI/ACLASS
  - ISASecure can scale on a global basis
  - Ensures certification process is open, fair, credible, and robust

ISASecure™ Programs

- Development Process Certifications
  - Software Development Security Assurance (SDSA)
- Product Certifications
  - Embedded Device Security Assurance (EDSA)
- System Certifications
  - System Security Assurance (SSA)

ISASecure™ Development Process Certification

- Software Development Security Assurance (SDSA)
  - Ensures the manufacturer of an industrial automation product follows a robust, secure software development process
  - The vendor’s software development and maintenance processes are audited per the ISASecure SDSA specification

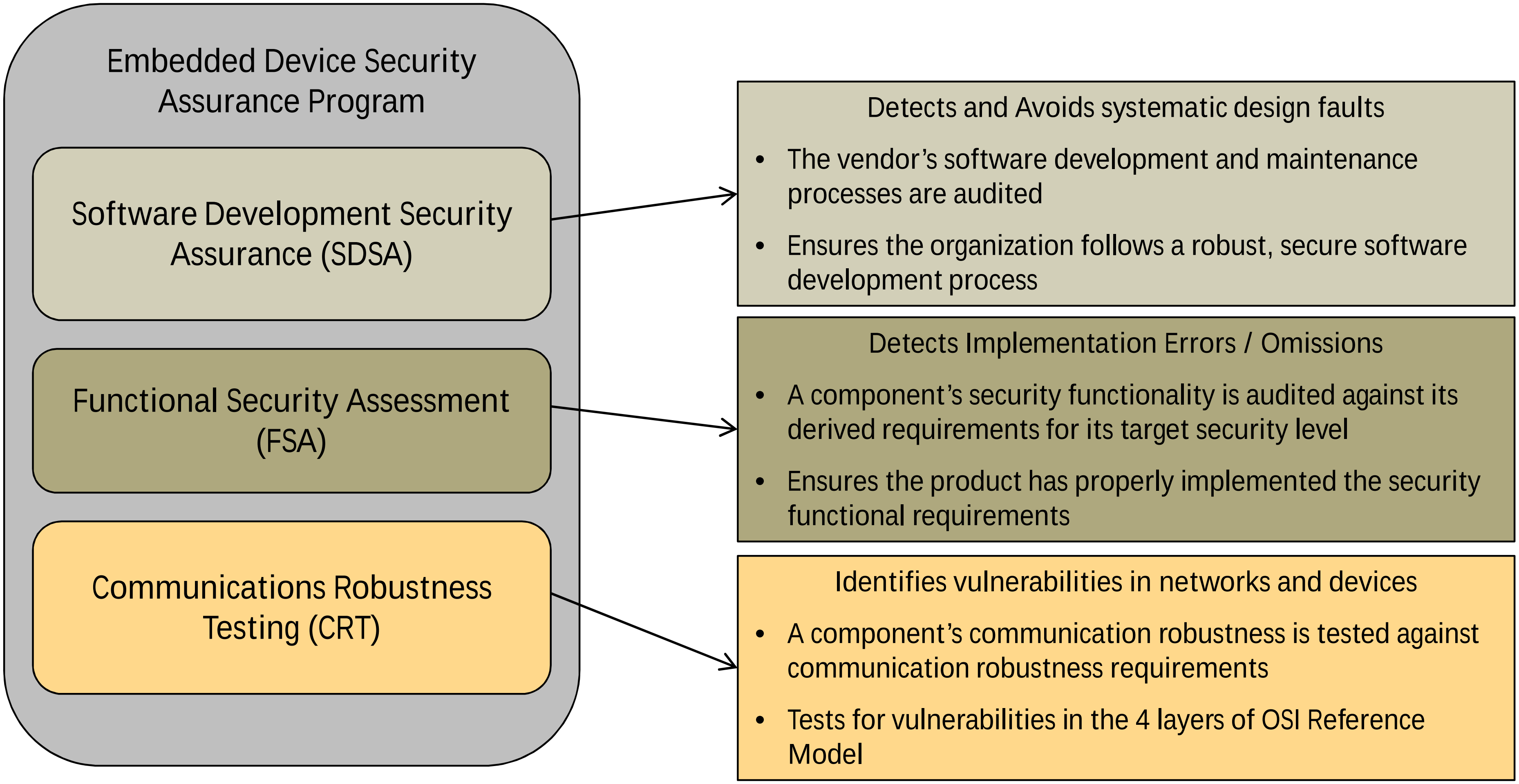
SDSA Phases

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

Grid-Interop

ISASecure™Device Security Assurance Program

ISASecure



Embedded Device Security Assurance Program

Software Development Security Assurance (SDSA)

Functional Security Assessment (FSA)

Communications Robustness Testing (CRT)

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

Detects Implementation Errors / Omissions

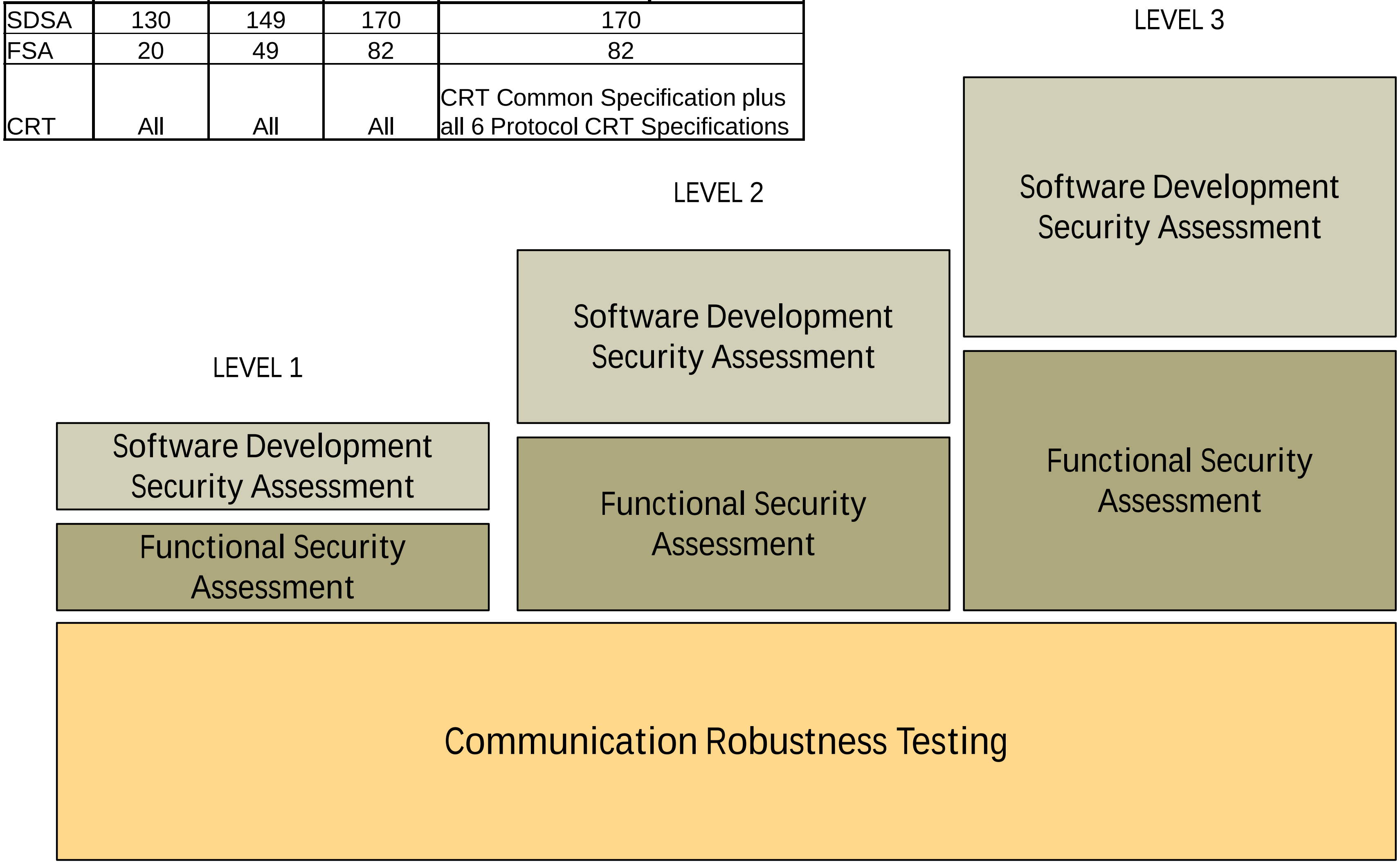
- A component's security functionality is audited against its derived requirements for its target security level
- Ensures the product has properly implemented the security functional requirements

Identifies vulnerabilities in networks and devices

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

ISASecure Levels

	Requirements Necessary to Achieve Certification Levels			
	Level 1	Level 2	Level 3	Total Count in Specification
SDSA	130	149	170	170
FSA	20	49	82	82
CRT	All	All	All	CRT Common Specification plus all 6 Protocol CRT Specifications



LEVEL 1

Software Development Security Assessment

Functional Security Assessment

LEVEL 2

Software Development Security Assessment

Functional Security Assessment

LEVEL 3

Software Development Security Assessment

Functional Security Assessment

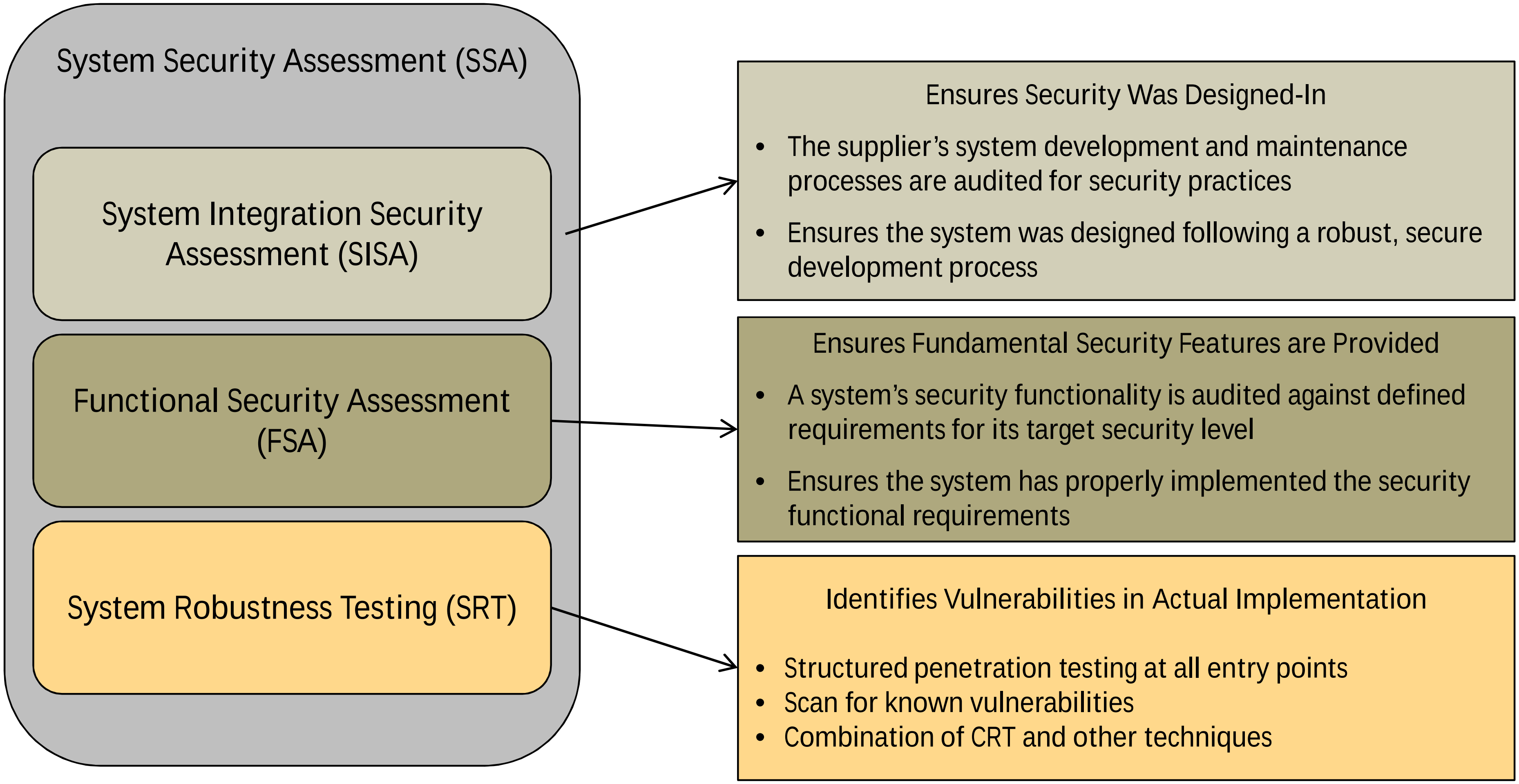
Communication Robustness Testing

EDSA Scope

- Devices 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™System Security Assurance (SSA)

ISASecure



System Security Assessment (SSA)

System Integration Security Assessment (SISA)

Functional Security Assessment (FSA)

System Robustness Testing (SRT)

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

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

Identifies Vulnerabilities in Actual Implementation

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

SSA Scope

- Control system platforms, packaged systems and application specific systems
- Examples:
  - General purpose ICS platforms
  - Boiler control systems
  - Burner management systems
  - Drilling control systems
  - Wellhead control systems
  - Ovens, dryers, heaters
  - Machine control system
  - Batch control systems
  - Turbine control systems

ISASecure™ Benefits

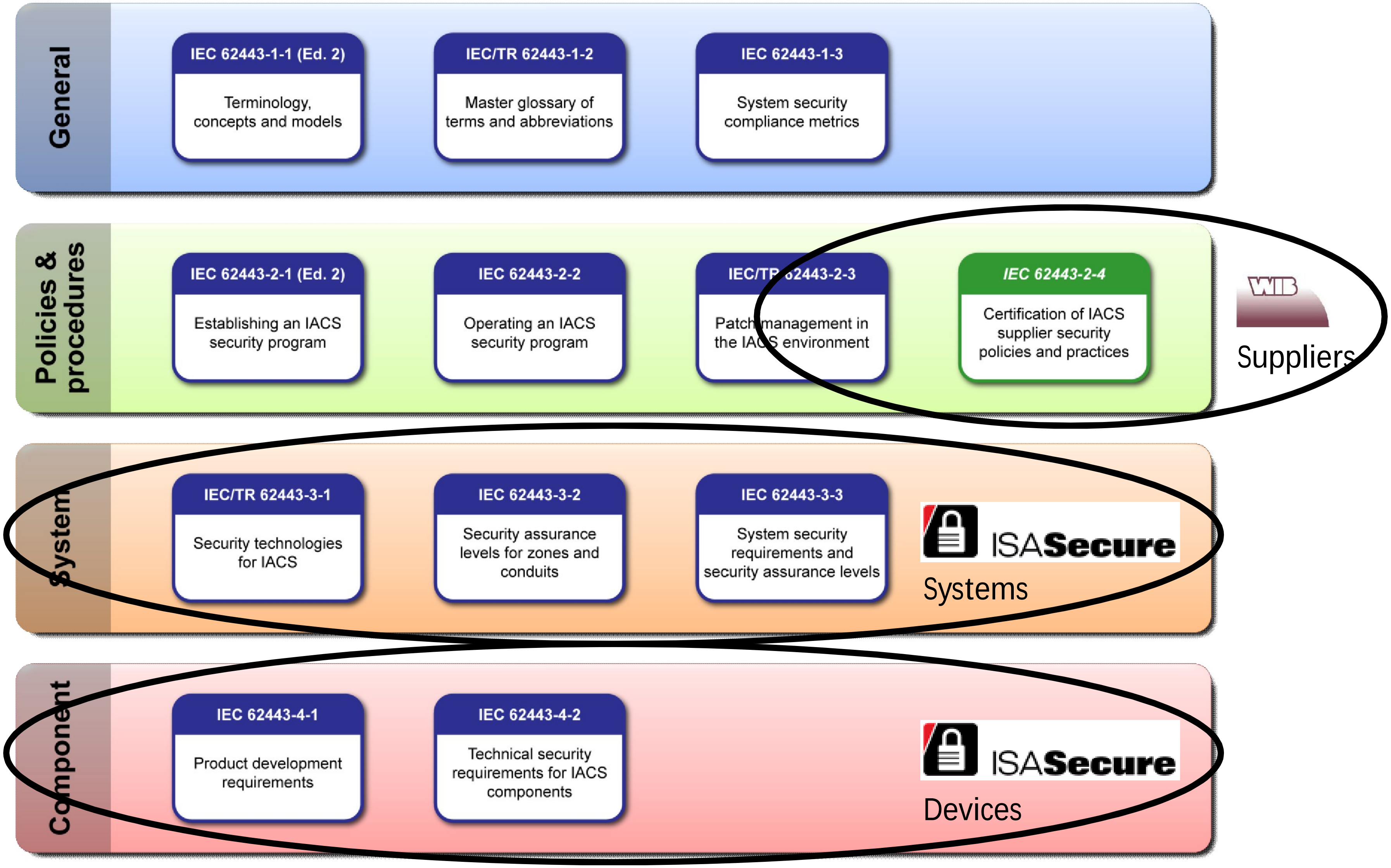
Asset Owner/Operator

- Easy to specify
- Build security requirement into RFP
- Reduced time in FAT/SAT
- Know security level out of the box

Supplier

- Build security
  - Reduced support costs
  - Fewer vulnerabilities in the field
- Evaluated once
- Recognition for effort
- Differentiator

Certification Reference Standards



General

- **IEC 62443-1-1 (Ed. 2)**: Terminology, concepts and models
- **IEC/TR 62443-1-2**: Master glossary of terms and abbreviations
- **IEC 62443-1-3**: System security compliance metrics

Policies & procedures

- **IEC 62443-2-1 (Ed. 2)**: Establishing an IACS security program
- **IEC 62443-2-2**: Operating an IACS security program
- **IEC/TR 62443-2-3**: Patch management in the IACS environment
- ***IEC 62443-2-4***: Certification of IACS supplier security policies and practices

System

- **IEC/TR 62443-3-1**: Security technologies for IACS
- **IEC 62443-3-2**: Security assurance levels for zones and conduits
- **IEC 62443-3-3**: System security requirements and security assurance levels

Component

- **IEC 62443-4-1**: Product development requirements
- **IEC 62443-4-2**: Technical security requirements for IACS components

Scalability: The Certification Levels

Bronze certification: 148 of 272 Requirements

Entry-level certification, awarded for successful completion of all applicable requirements for security policies and practices that that have been implemented and verified through direct measurement or analysis.

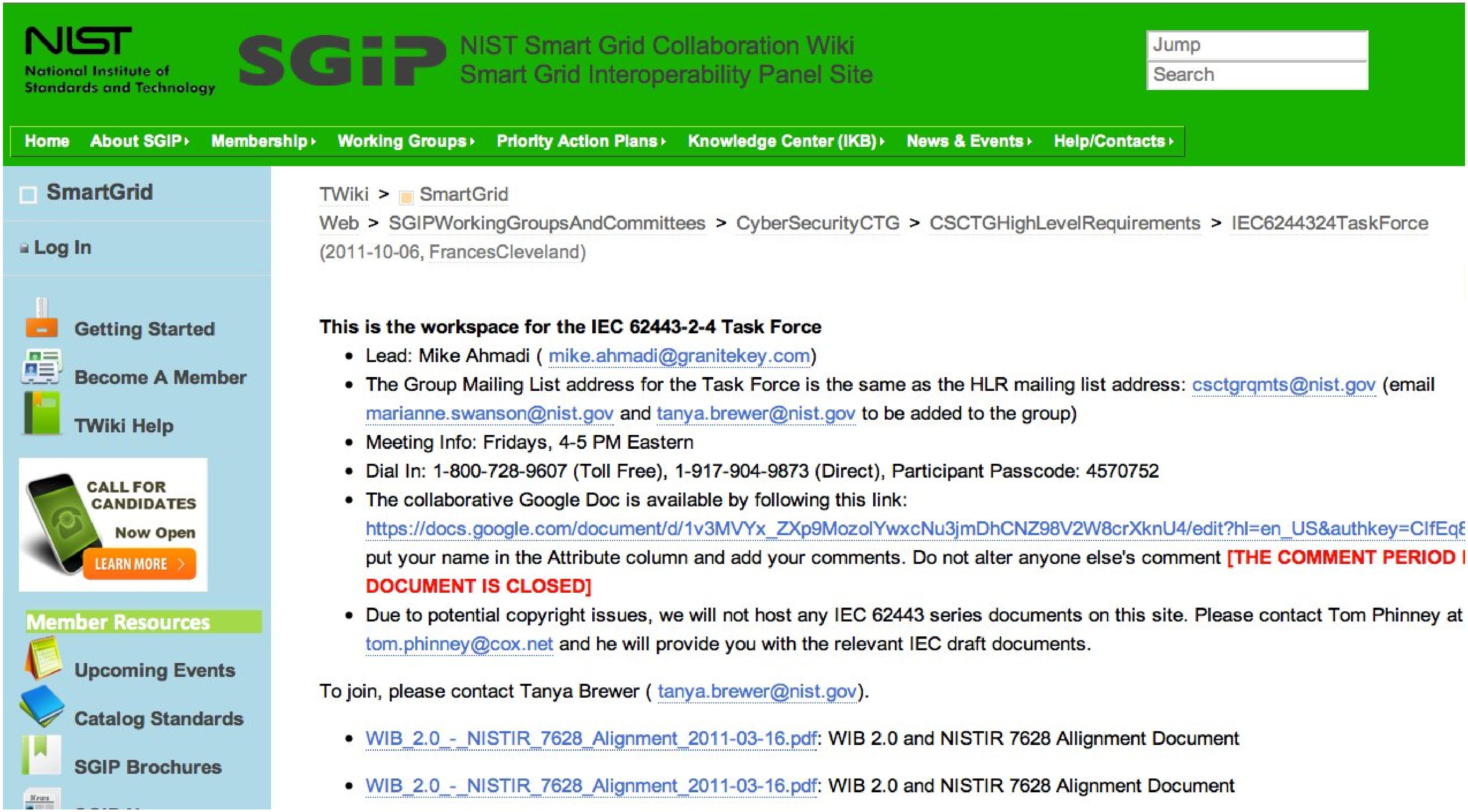
Silver certification: 218 of 272 Requirements

Awarded for successful completion of all applicable requirements and selected requirement enhancements that have been implemented and verified through direct measurement or analysis.

Gold certification: 272 of 272 Requirements

Awarded for successful completion of all applicable security policies and practices that exist in a vendor’s system. Gold level contains additional performance and industry-specific requirements.

NIST Cyber Security Working Group (CSWG)



TWiki > SmartGrid Web > SGIPWorkingGroupsAndCommittees > CyberSecurityCTG > CSCTGHighLevelRequirements > IEC6244324TaskForce (2011-10-06, FrancesCleveland)

This is the workspace for the IEC 62443-2-4 Task Force

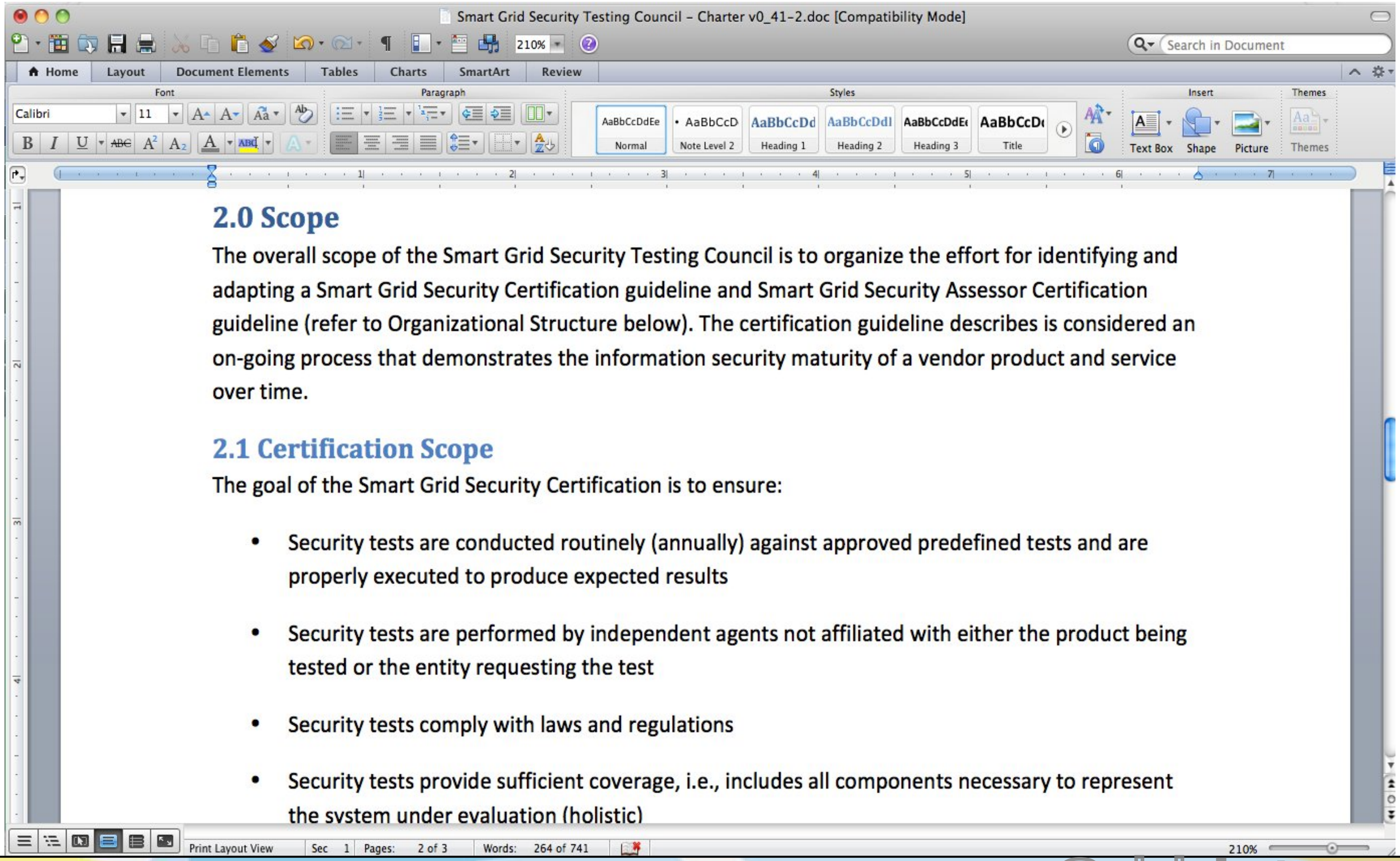
- Lead: Mike Ahmadi (mike.ahmadi@granitekey.com)
- The Group Mailing List address for the Task Force is the same as the HLR mailing list address: csctgrqmts@nist.gov (email marianne.swanson@nist.gov and tanya.brewer@nist.gov to be added to the group)
- Meeting Info: Fridays, 4-5 PM Eastern
- Dial In: 1-800-728-9607 (Toll Free), 1-917-904-9873 (Direct), Participant Passcode: 4570752
- The collaborative Google Doc is available by following this link: https://docs.google.com/document/d/1v3MVYx_ZXp9MozolYwxcNu3jmDhCNZ98V2W8crXknU4/edit?hl=en_US&authkey=CIfEq put your name in the Attribute column and add your comments. Do not alter anyone else's comment **[THE COMMENT PERIOD I DOCUMENT IS CLOSED]**
- Due to potential copyright issues, we will not host any IEC 62443 series documents on this site. Please contact Tom Phinney at tom.phinney@cox.net and he will provide you with the relevant IEC draft documents.

To join, please contact Tanya Brewer (tanya.brewer@nist.gov).

- WIB_2.0_-_NISTIR_7628_Alignment_2011-03-16.pdf: WIB 2.0 and NISTIR 7628 Allignment Document
- WIB_2.0_-_NISTIR_7628_Alignment_2011-03-16.pdf: WIB 2.0 and NISTIR 7628 Alignment Document

UCAIug OpenSG Security Conformity Task Force

- Task force formed under OpenSG to address security conformity
- Could serve as adjudicator for member organizations



2.0 Scope

The overall scope of the Smart Grid Security Testing Council is to organize the effort for identifying and adapting a Smart Grid Security Certification guideline and Smart Grid Security Assessor Certification guideline (refer to Organizational Structure below). The certification guideline describes is considered an on-going process that demonstrates the information security maturity of a vendor product and service over time.

2.1 Certification Scope

The goal of the Smart Grid Security Certification is to ensure:

- Security tests are conducted routinely (annually) against approved predefined tests and are properly executed to produce expected results
- Security tests are performed by independent agents not affiliated with either the product being tested or the entity requesting the test
- Security tests comply with laws and regulations
- Security tests provide sufficient coverage, i.e., includes all components necessary to represent the system under evaluation (holistic)

Applying the IEC 62443 Work Products

- Several organizations using:
  - – Concepts as defined in 62443-1-1
  - – Programs as defined in 62443-2-1
  - – Zone & Conduit model
  - – Vendor Practices Certification in 62443-2-4
- Case studies are becoming available
- Overall, the feedback is quite good!

More Information

- ISA99 Wiki
  - – http://isa99.isa.org
- IEC 62443-2-4 Twiki
  - – http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/IEC6244324TaskForce
- Contacts
  - – Eric Cosman, eric.cosman@gmail.com
  - – Bryan Singer, bryan.singer@kenexis.com
  - – Jim Gilsinn, james.gilsinn@nist.gov
  - – Charley Robinson, crobinson@isa.org
  - – Andre Ristaino, aristaino@isa.org
  - – Mike Ahmadi, mike.ahmadi@granitekey.com