KENEXIS

ISA/IEC 62443: Intro & How To

Jim Gilsinn

Jim Gilsinn

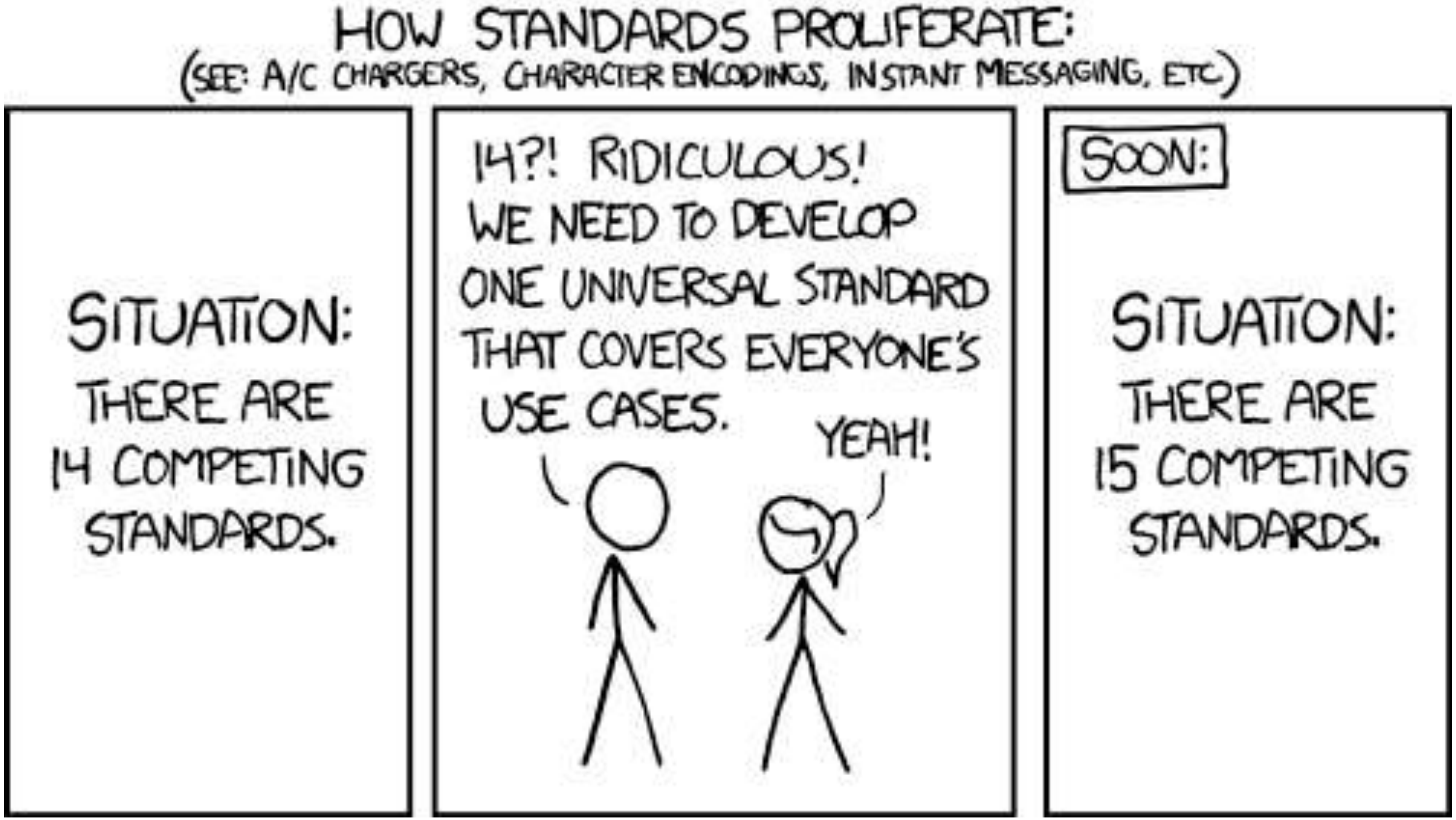
- Principal Consultant, Kenexis
- Previously, Engineering Lab @ NIST
- ISA99 Committee, Co-Chair
    - ISA99, Working Group 2, Co-Chair
    - ISA99, General Editor
- MSEE, Controls

CISSP Certified Information Systems Security Professional

CEH Certified Ethical Hacker

ISA ISA/IEC 62443 Cybersecurity Expert

To Many Standards!


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Interrelated IACS Cyber Security Standards

ISA

ISA-62443

NIST

Cybersecurity Framework
SP800-53, SP800-82

IEC ISO

ISO/IEC 2700x
IEC 62443

Center for Internet Security®

20 Critical Security Controls

How Do You Pick The Right Standard?

- Regulation
  - Regulated industries may have compliance requirements
  - NERC CIP, NRC/NEI, API, CFATS
- Industry Guidance
  - Some industries have preferred sets of requirements
  - Chemical, Transportation, Oil & Gas
- Corporate Preference/Culture
  - Who owns cyber security for production?

ISA99 & ISA/IEC-62443 Basics

ISA99 Committee

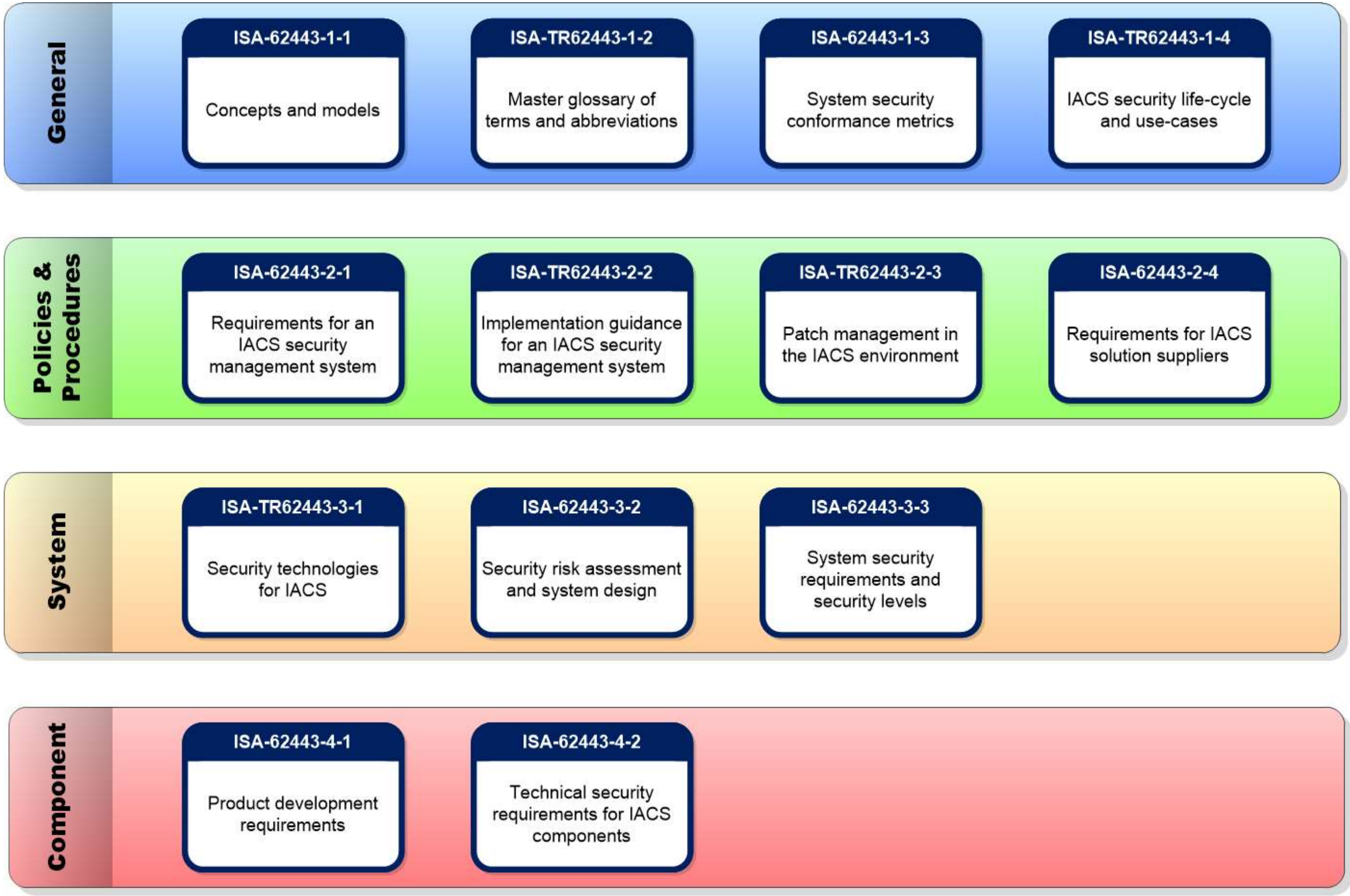
The International Society of Automation (ISA) Committee on Security for Industrial Automation & Control Systems (ISA99)

- 500+ members
- Representing companies across all sectors, including:
  - Chemical Processing
  - Petroleum Refining
  - Food and Beverage
  - Energy
  - Pharmaceuticals
  - Water
  - Manufacturing

ISA99 & ISA/IEC 62443

- ISA/IEC 62443 is a series of standards being developed by two groups:
  - ISA99 → ANSI/ISA-62443
  - IEC TC65/WG10 → IEC 62443
- In consultation with:
  - ISO/IEC JTC1/SC27 → ISO/IEC 2700x

ISA/IEC 62443 Series



General

ISA-62443-1-1
Concepts and models

ISA-TR62443-1-2
Master glossary of terms and abbreviations

ISA-62443-1-3
System security conformance metrics

ISA-TR62443-1-4
IACS security life-cycle and use-cases

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
Requirements for IACS solution suppliers

System

ISA-TR62443-3-1
Security technologies for IACS

ISA-62443-3-2
Security risk assessment and system design

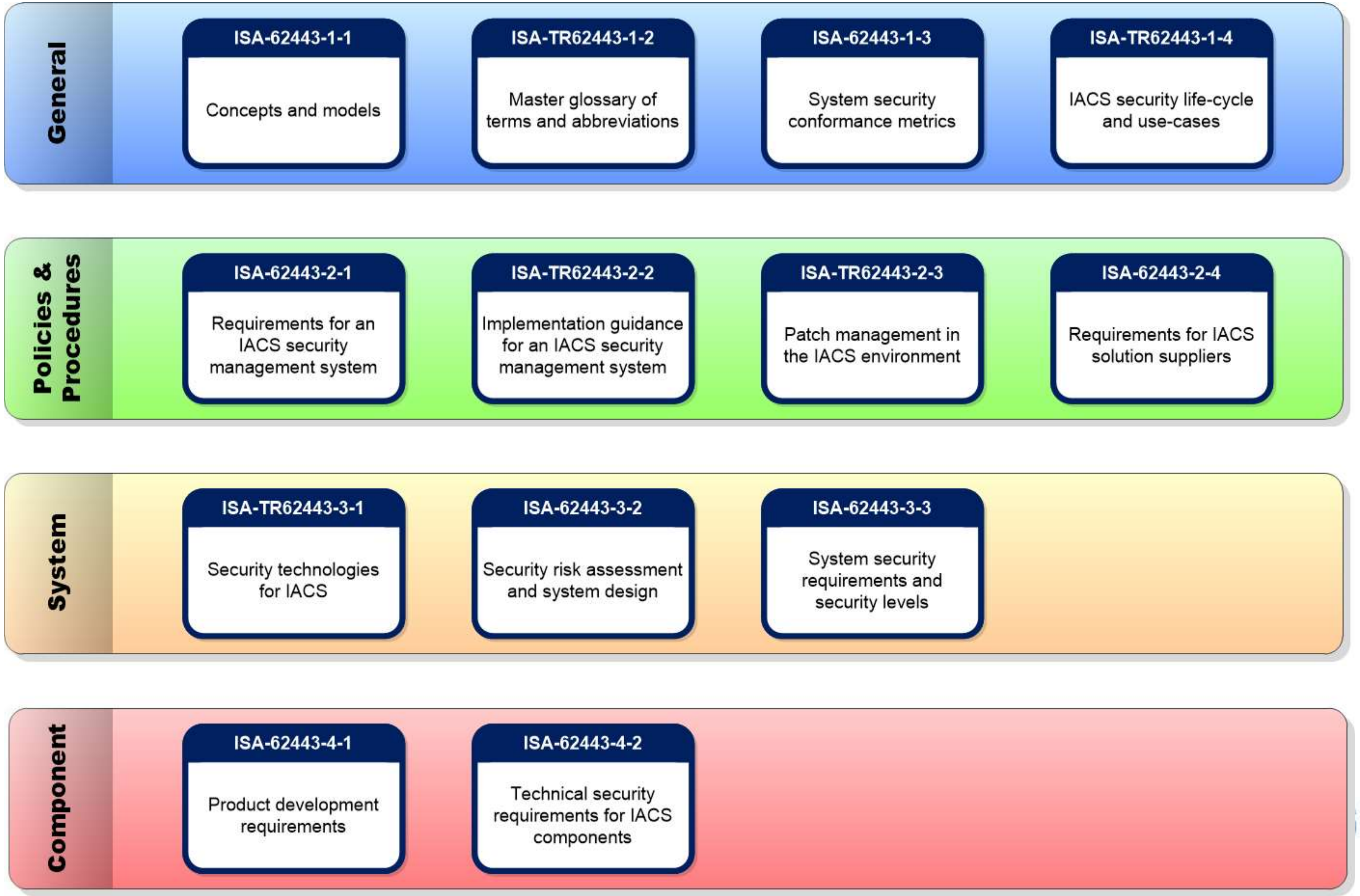
ISA-62443-3-3
System security requirements and security levels

Component

ISA-62443-4-1
Product development requirements

ISA-62443-4-2
Technical security requirements for IACS components

Roles



General/Everyone	General	ISA-62443-1-1 Concepts and models	ISA-TR62443-1-2 Master glossary of terms and abbreviations	ISA-62443-1-3 System security conformance metrics	ISA-TR62443-1-4 IACS security life-cycle and use-cases
Asset Owners	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 Requirements for IACS solution suppliers
System Integrators	System	ISA-TR62443-3-1 Security technologies for IACS	ISA-62443-3-2 Security risk assessment and system design	ISA-62443-3-3 System security requirements and security levels	
Vendors	Component	ISA-62443-4-1 Product development requirements	ISA-62443-4-2 Technical security requirements for IACS components		

How Do We Use ISA/IEC 62443?

Creating a Security Program

- As a consultant, how do we help our customers create a security program?
- No one standard has everything
- Don’t try to be an expert in everything
  - Pick one and become an expert
  - Pick one or two others and become knowledgeable
  - Get exposed to the others
  - Pick individuals to gain knowledge on different ones
  - Many of them have similar requirements
- Customers generally have one in mind
  - As part of RFP, customers generally indicate which one they want to use as their base

Creating a Security Program (cont’d)

- Try to avoid one-off solutions
  - Start with a main standard
  - Integrate good parts of other standards
  - Create a repeatable process
- But, don’t create a cookie-cutter solution
  - Customers all have different needs and priorities
  - Security program will need to be tailored
- Include a checklist, but don’t focus on it
  - Everyone talks about not using a checklist approach
  - Customers want a simple assessment tool to evaluate whether they met their design goals
  - Checklists provide “add-on value” for customers

Creating a Security Program (cont’d)

- Avoid approaching this from a purely security point of view
  - If security is seen as insurance, it will be difficult to justify
  - Risk management or incident response is a good tact
  - System reliability and production uptime are also another tact
- A viable security program is difficult to design without an assessment
  - A security program shouldn’t exist in a vacuum
  - Understand what you have and how you work

Assess Current State

Identify the SUC

- Clear definition of scope
- Identify organizations as well

Conduct High-Level Risk Assessment

- Reuse existing information
- General risk assessment categories
- Not comprehensive

Define Zones & Conduits

- Network segmentation
- Logical/physical breakdown
- Consider safety, wireless, temporary, vendors/contractors

Conduct Detailed Risk Assessment

- Identification & classification
- Asset inventory
- Network diagrams
- Data captures
- Infrastructure configs/rules
- Identify existing vulnerabilities
- Define potential consequences
- Determine potential threats

Design The Solution

Define Targets

- Don’t overcomplicate
- Utilize similar target levels

Evaluate Countermeasures

- Evaluate data from detailed risk assessment
- Compare to “industry” recommendations
- Understand OT is different

Design & Integrate

- Design solutions
- Pick equipment
- Integrate in test environment, if possible

Reevaluate Countermeasures

- Redo detailed risk-assessment analysis

Questions?

- Contact Information
  - Jim Gilsinn
  - jim.gilsinn@kenexis.com
  - https://www.kenexis.com
  - +1-614-323-2254
  - @JimGilsinn

- ISA99 Information
  - http://isa99.isa.org

Security Is Not About Compliance!