INCOSE Healthcare Working Group

4th Annual Systems Engineering in Healthcare Conference

# Cybersecurity Recommended Practices for Medical Systems

## Based on International Standards

MDISS

MEDICAL DEVICE INNOVATION, SAFETY & SECURITY CONSORTIUM

Eric C. Cosman
Principal Consultant
OIT Concepts, LLC
eric.cosman@oitconcepts.com

# Topics for Today

- Background
- Project Overview
- The 624433 Standards
- Current Status
- Next Steps

# Topics for Today

- **Background**
- Project Overview
- The 624433 Standards
- Current Status
- Next Steps

# The Proposal…

"Exploit the parallels between industrial control and medical systems cybersecurity to develop a set of recommended practices (RP's), based on established international standards."

# Solution Characteristics

- Requirements engineering
- Security for reliability and integrity
- Multi-discipline
- Testing and evaluation
- Certification and compliance
- Life cycle focus

***A Systems Engineering approach required***

# Topics for Today

- Background
- **Project Overview**
- The 624433 Standards
- Current Status
- Next Steps

# The Premise…

- Industrial control and medical device systems share many common characteristics, including:
- High risk – proper operation and system integrity are paramount.
- Both include devices and components from multiple suppliers.
- Connectivity has increased without adequate consideration of security.
- Role-based human interfaces to monitor operation.

# Starting Point…

- "Review, revise and complete an existing draft of a cybersecurity recommended practice document for the client's membership."
- Original draft document based on WIB Report M2784-X10
  - Requirements "interpreted" in the medical device context
- Final version based on IEC 62443-2-4 international standard
  - Part of the ISA/IEC 62443 series

# Approach

- Breakdown previous draft
  - List categories
  - Requirements and comments by category
- Compare to organization of 62443-2-4
- Map categories and requirements
- Establish document structure
- Interpret requirements

# Topics for Today

- Background
- Project Overview
- **The 624433 Standards**
- Current Status
- Next Steps

# Principal Authoring Committee

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

- 700+ members, representing companies across many sectors, including:
  - Chemical Processing
  - Food, Beverage and Pharmaceuticals
  - Manufacturing
  - Petroleum Refining
  - Water

# In Collaboration With…

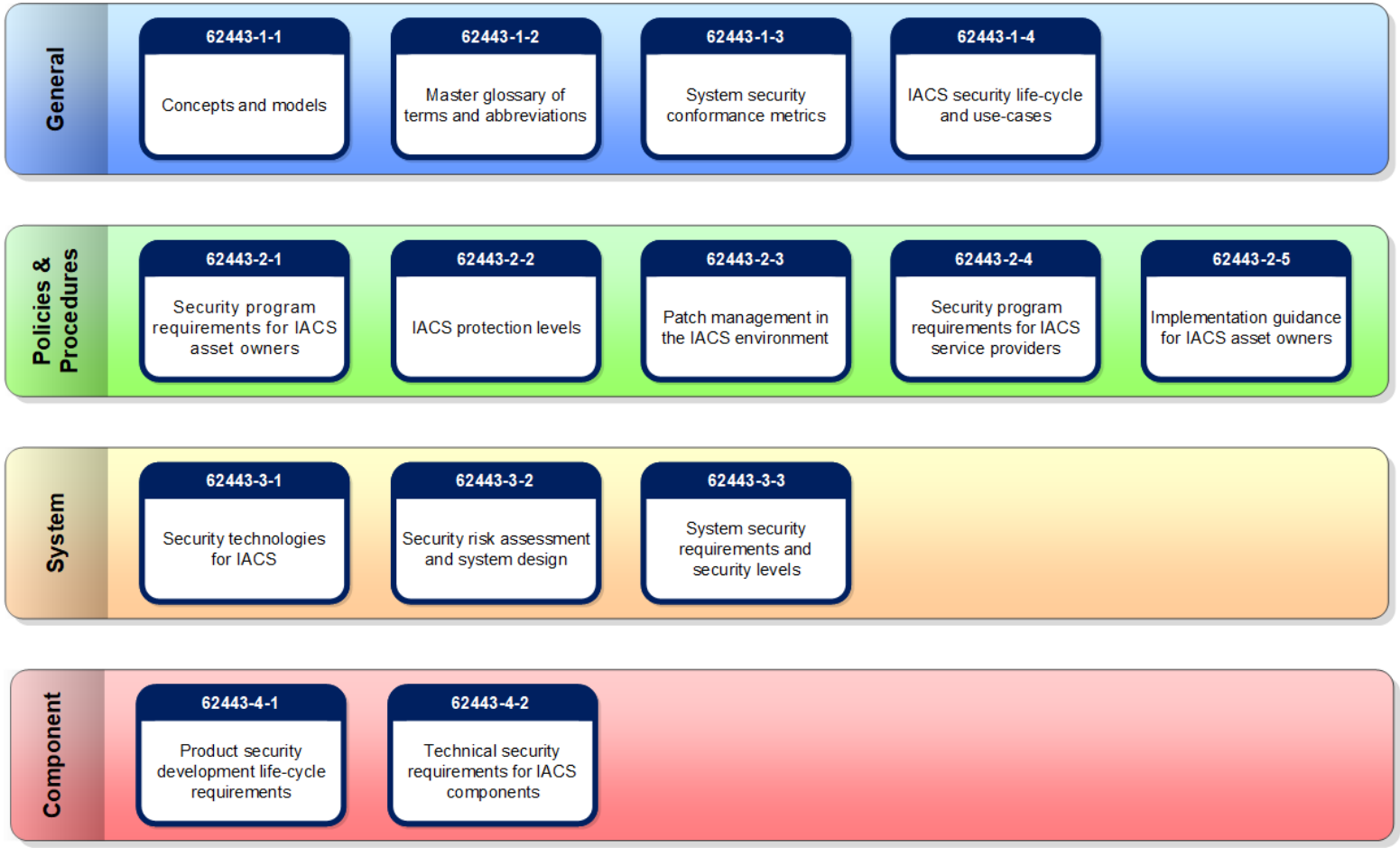
IEC Technical Committee 65, working group 10:

- "To prepare international standards for systems and elements used for industrial-process measurement and control concerning continuous and batch processes."

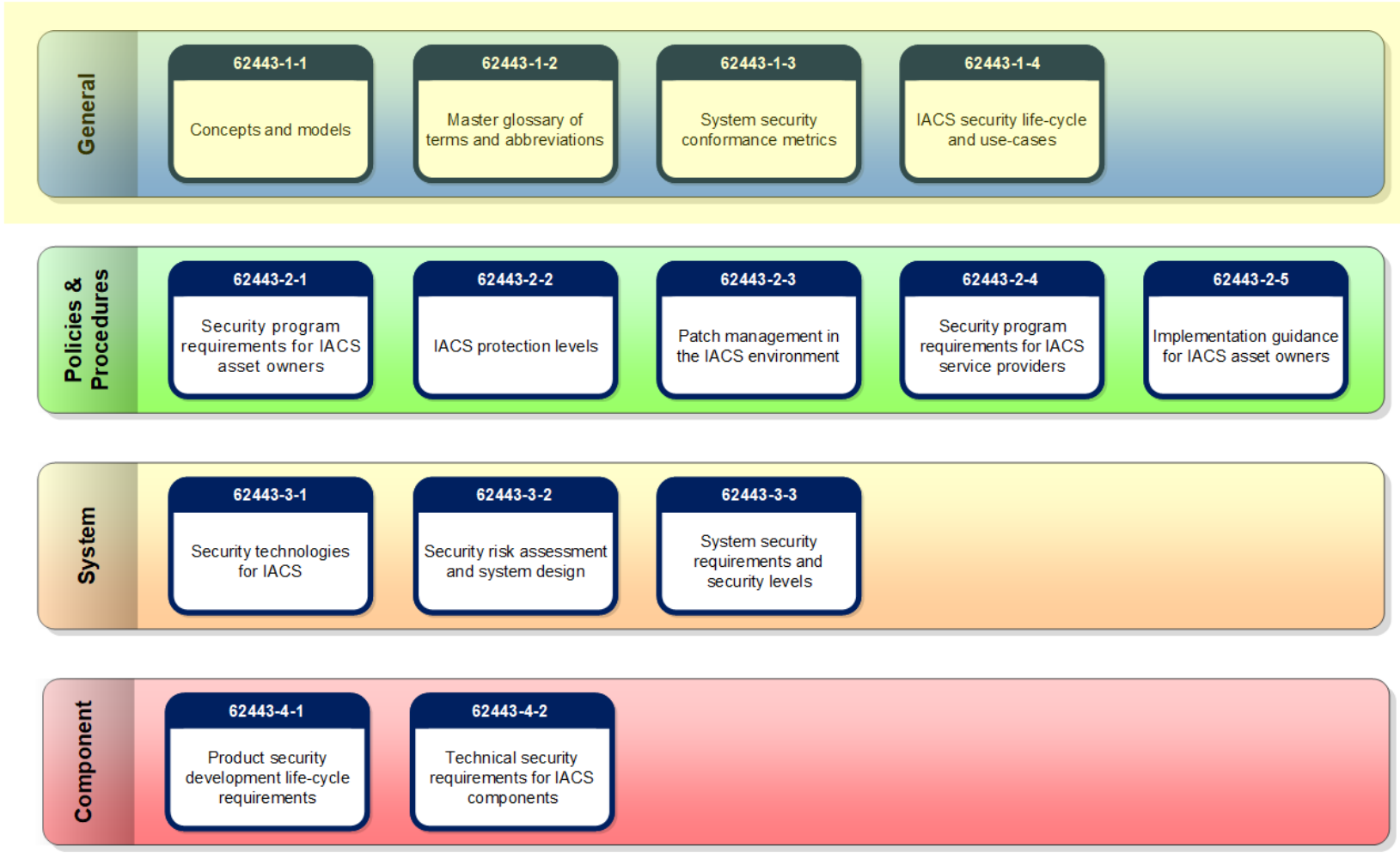
# Scope Based on Consequence

- "… systems whose compromise could result in any or all of the following situations:
  - endangerment of public or employee safety
  - environmental protection
  - loss of public confidence
  - violation of regulatory requirements
  - loss of proprietary or confidential information
  - economic loss
  - impact on entity, local, state, or national security"

# The ISA-62443/IEC 62443 series



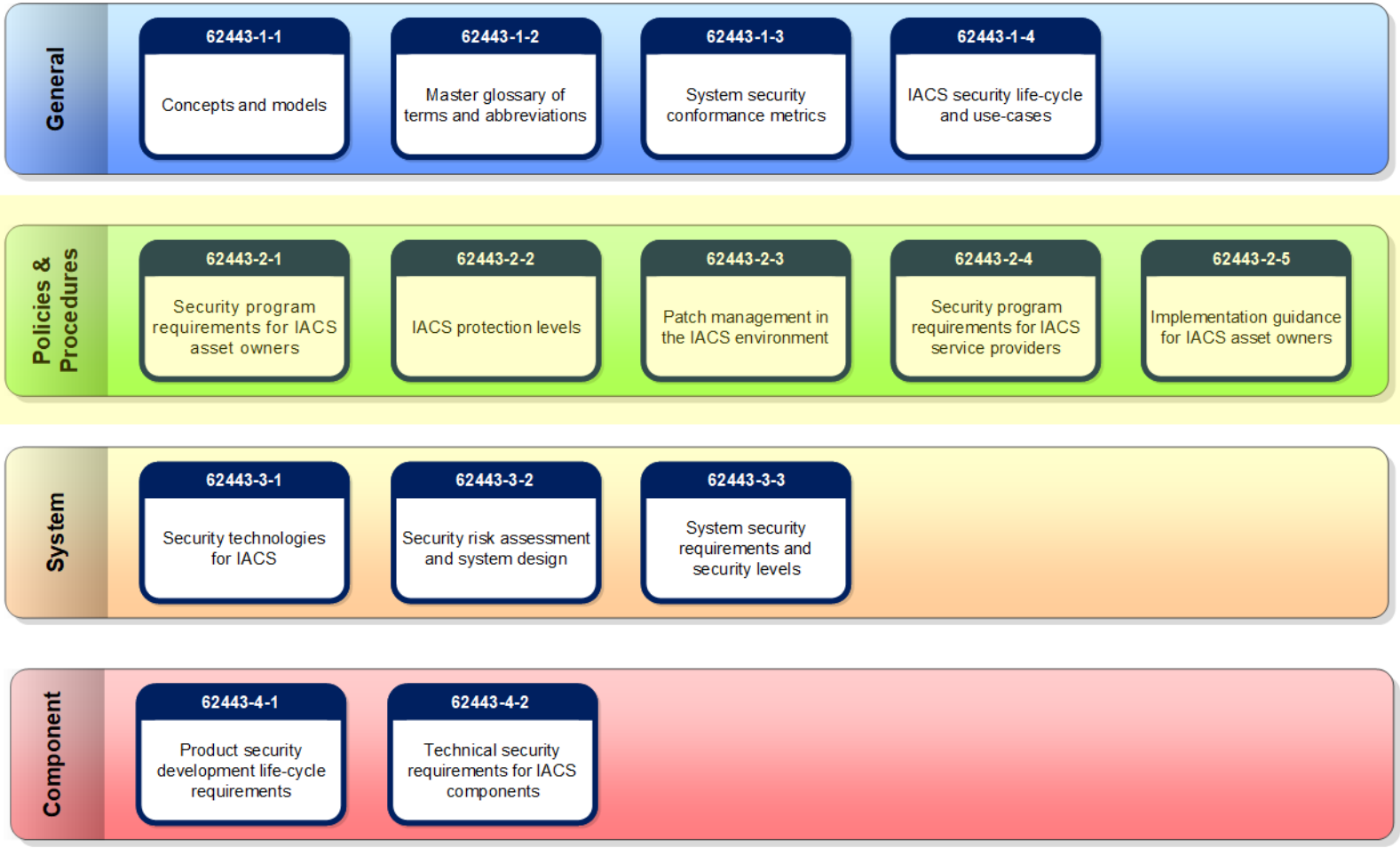
# The ISA-62443/IEC 62443 series




Target Audience

General (all roles)

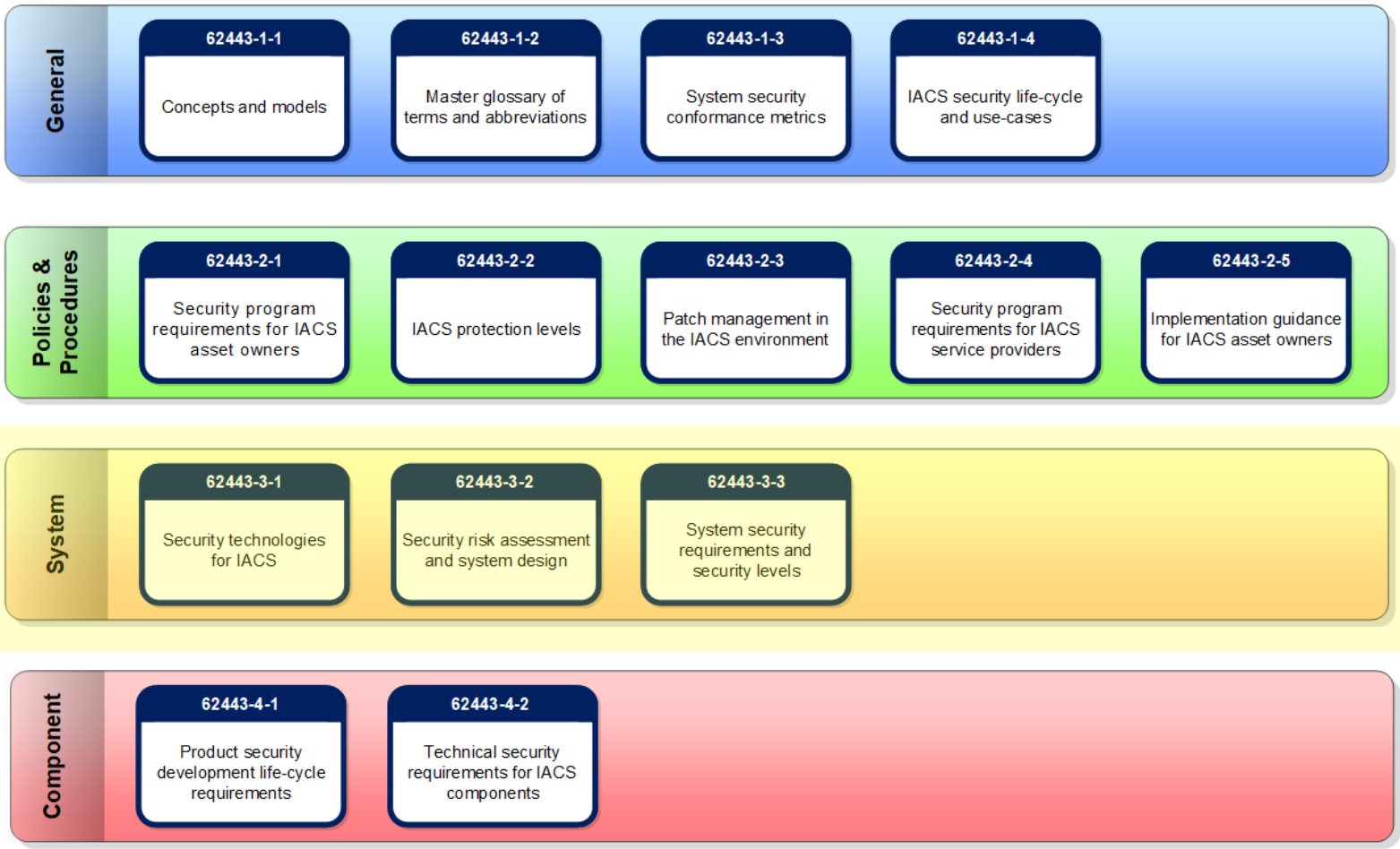
# The ISA-62443/IEC 62443 series




Target Audience

Asset Owner

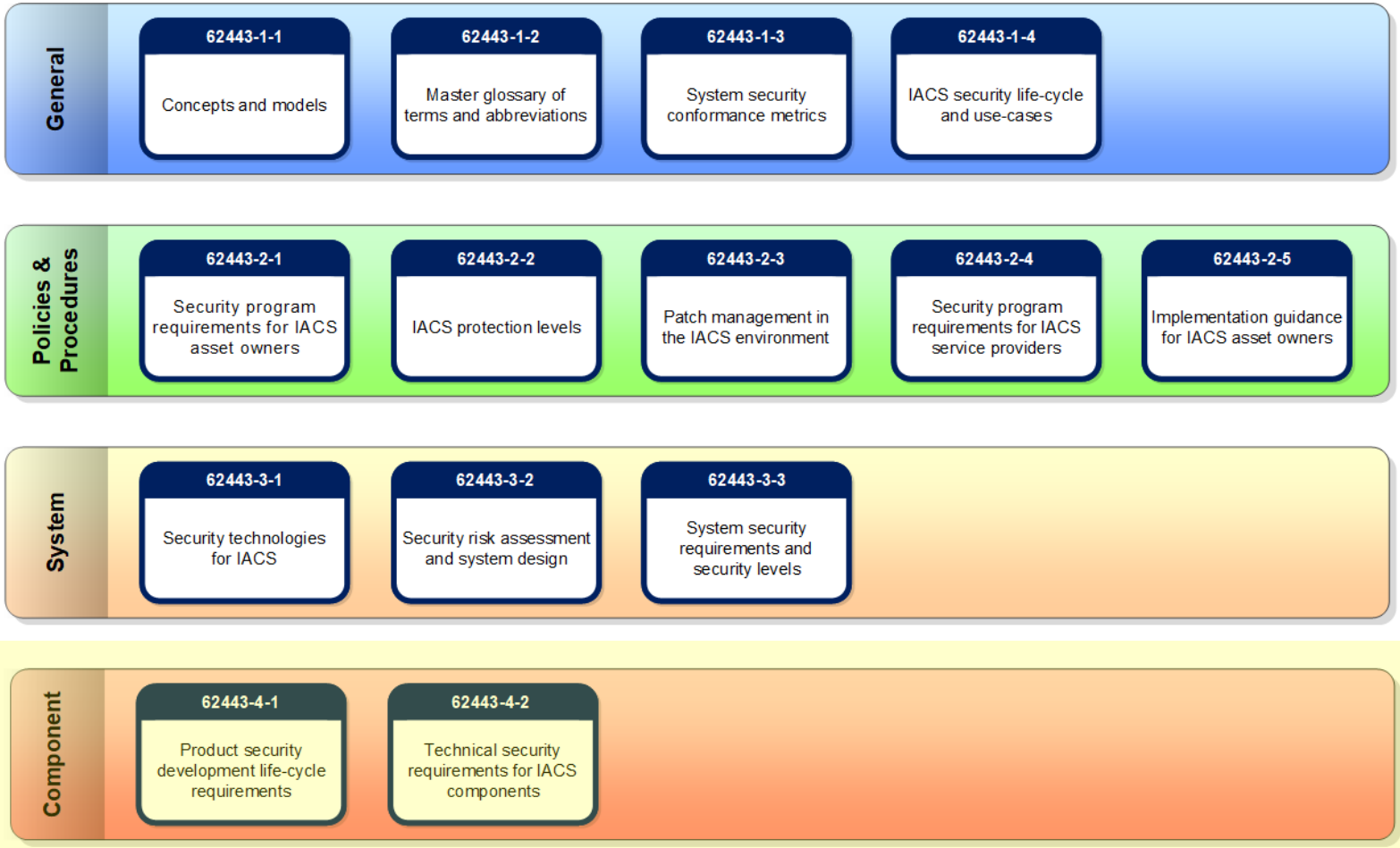
# The ISA-62443/IEC 62443 series




Target Audience

Suppliers & Systems Integrators

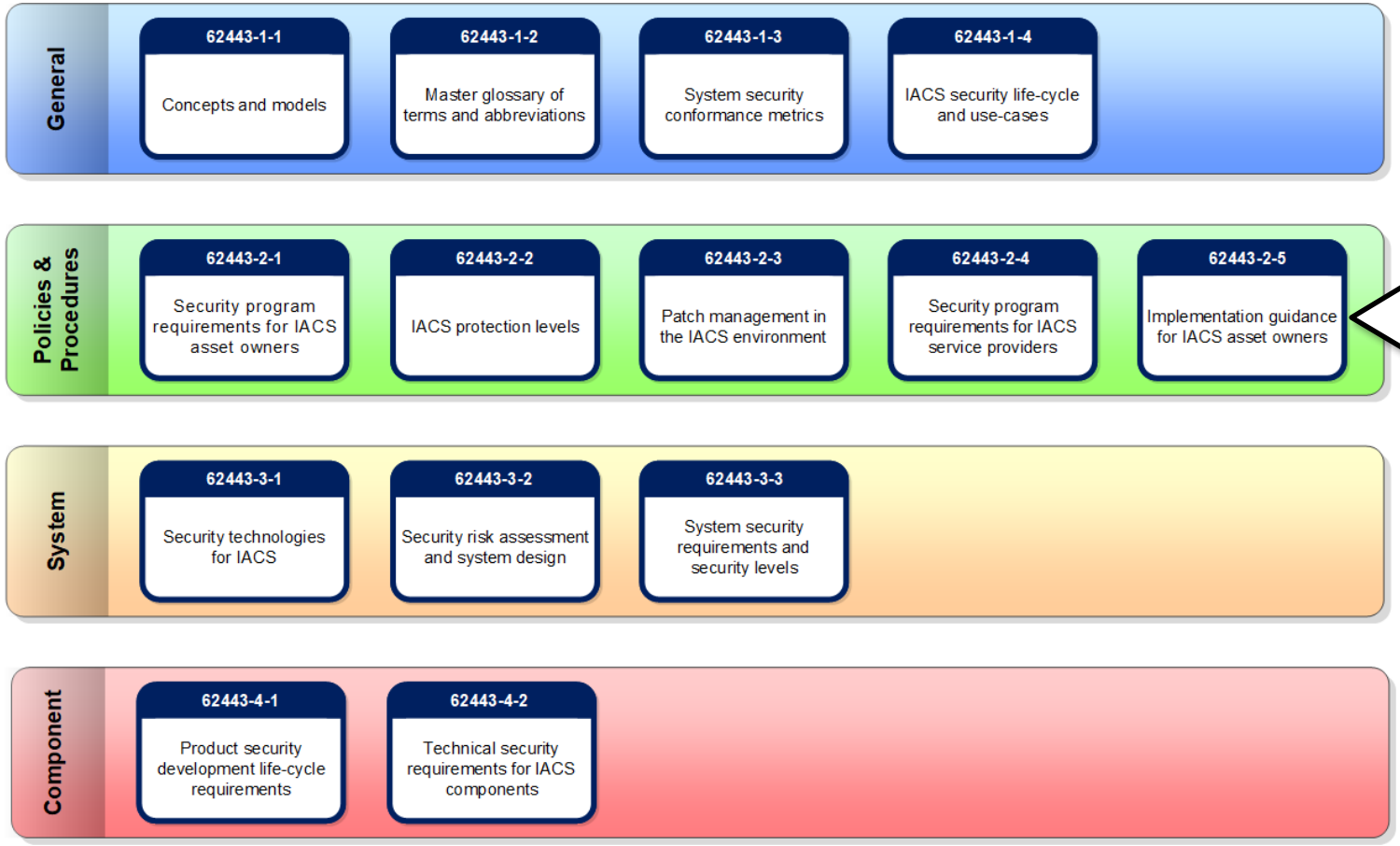
# The ISA-62443/IEC 62443 series




Target Audience

Product and System Suppliers

# The ISA-62443/IEC 62443 series




First MDISS Recommended Practice (RP):

- Define requirements for:
  - ✓ Manufacturer
  - ✓ System Integrator
  - ✓ Health Care Provider
  - ✓ Service Provider

# Topics for Today

- Background
- Project Overview
- The 624433 Standards
- **Current Status**
- Next Steps

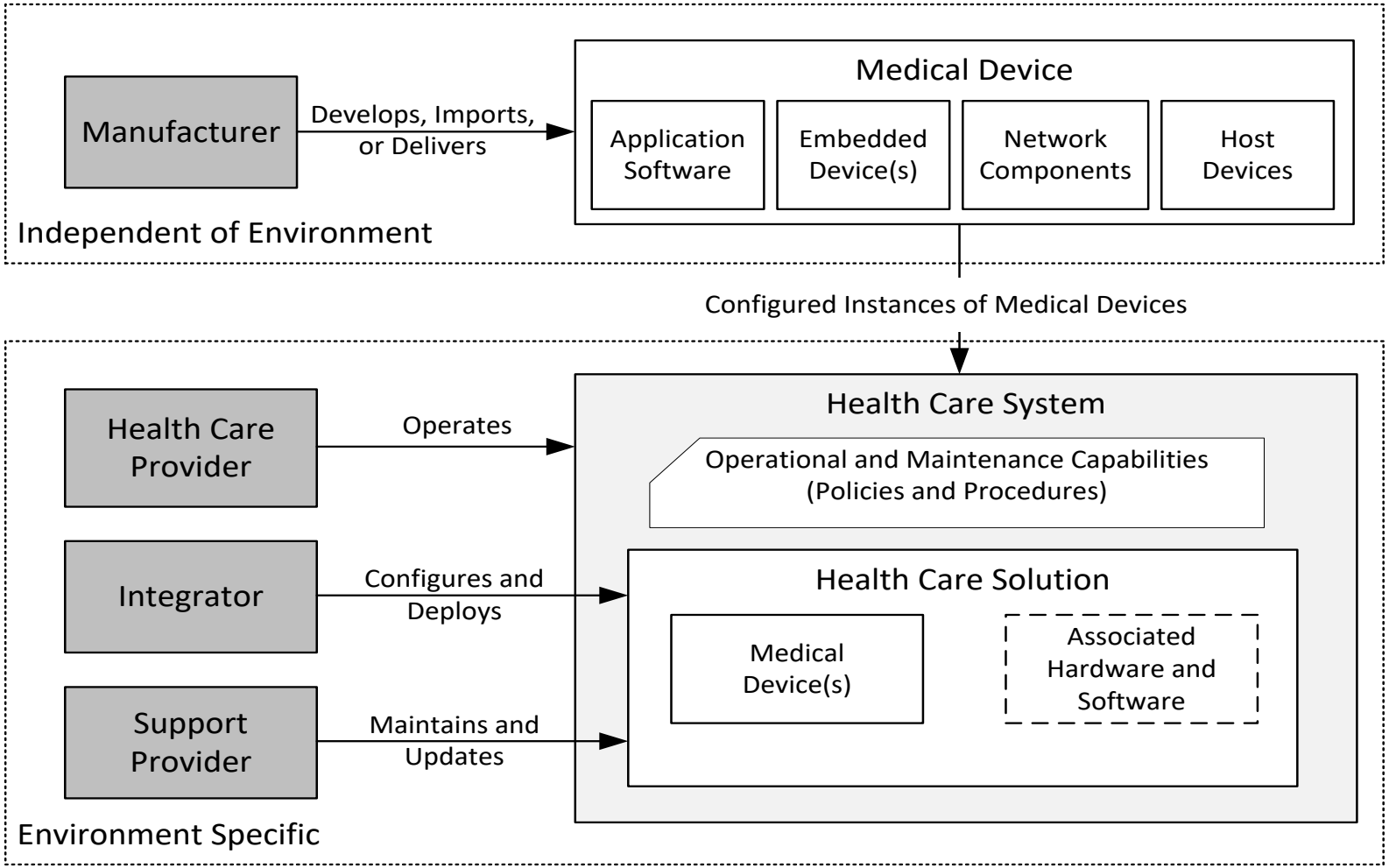
# Functional and Process Context

- Establish Role Descriptions
  - Basis for implications
- Define the Process Context
- Requirement Interpretation
  - Implications

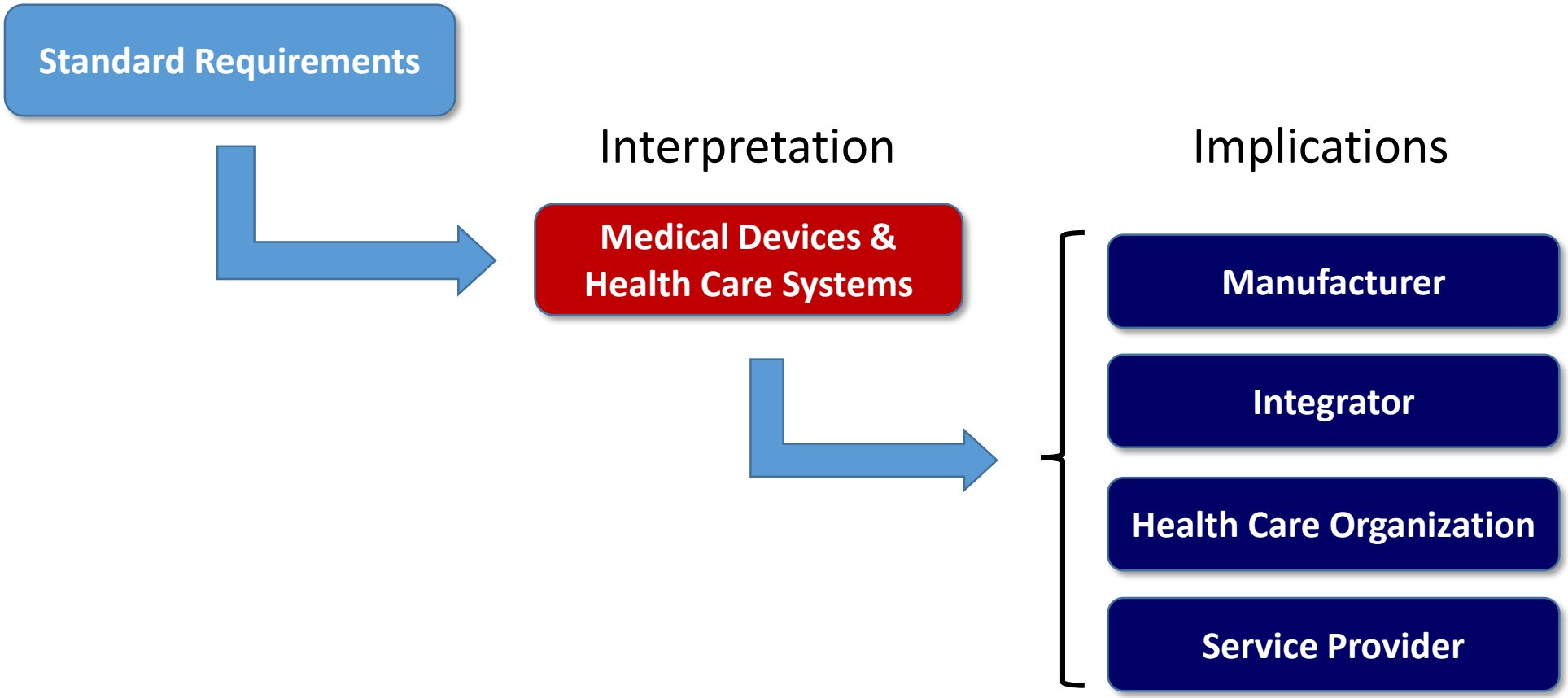
# Principal Roles

- Manufacturer
- Health Care Provider
- Service Provider
  - Integrator
  - Support Provider

# Roles and Processes



# Requirement Interpretation



# Requirement Interpretation Example

### 1.1.1 Training – Security Requirements (SP.01.01)

**Base Requirement or Requirement Enhancement (NN.01.01[-x])**

Original Statement

Interpretation

Implications for the Manufacturer

Implications for the Integrator

Implications for the Health Care Provider

Implications for the Support Provider

# Topics for Today

- Background
- Project Overview
- The 624433 Standards
- Current Status
- **Next Steps**

# Repeating the process…

- Develop additional recommended practices
  - Corresponding to remaining standards in the 62443 series
  - Based on relative priority and degree of completion
- Estimate of effort prorated based on number of normative requirements

# Additional Standards

| 62443 Standard | | Intended Audience | Intent |
|---|---|---|---|
| 62443-3-3 | | All Roles | Interpret the essential system-level requirements and how they relate to specific desired security levels. |
| 62443-4-1 | | Suppliers and Integrators | Provide context-specific guidance on the requirements for product development. |
| 62443-4-2 | | Manufacturers | Provide context-specific guidance on expectations for the security of system components. |
| 62443-3-2 | | Health Care Providers and System Integrators | Describes the activities required to perform security risk assessments on a new or existing system and the design activities required to mitigate the risk to tolerable levels. |
| 62443-2-1 | | Health Care Providers | Provide guidance on what is expected from an effective cybersecurity management system, based on the requirements stated in the first edition (2009) of this standard. |
| 62443-2-3 | | Health Care Providers and Support Providers | Describe the specific needs for effective patch management. |


Eric C. Cosman
Principal Consultant
OIT Concepts, LLC
eric.cosman@oitconcepts.com