ISA-99 – Industrial Automation & Control Systems Security

Jim Gilsinn

National Institute of Standards & Technology (NIST)
Engineering Laboratory

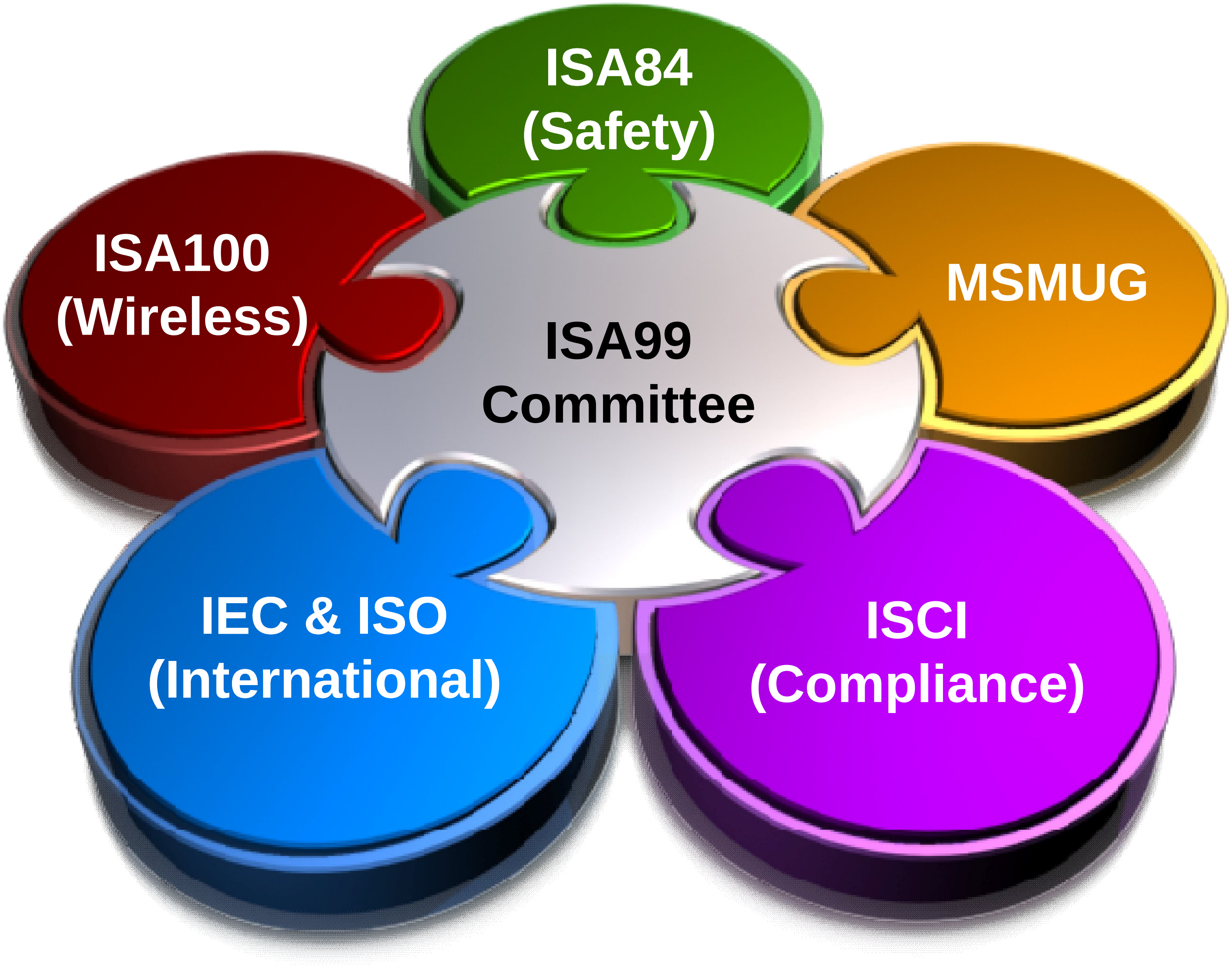
#GridInterop

ISA99 Committee

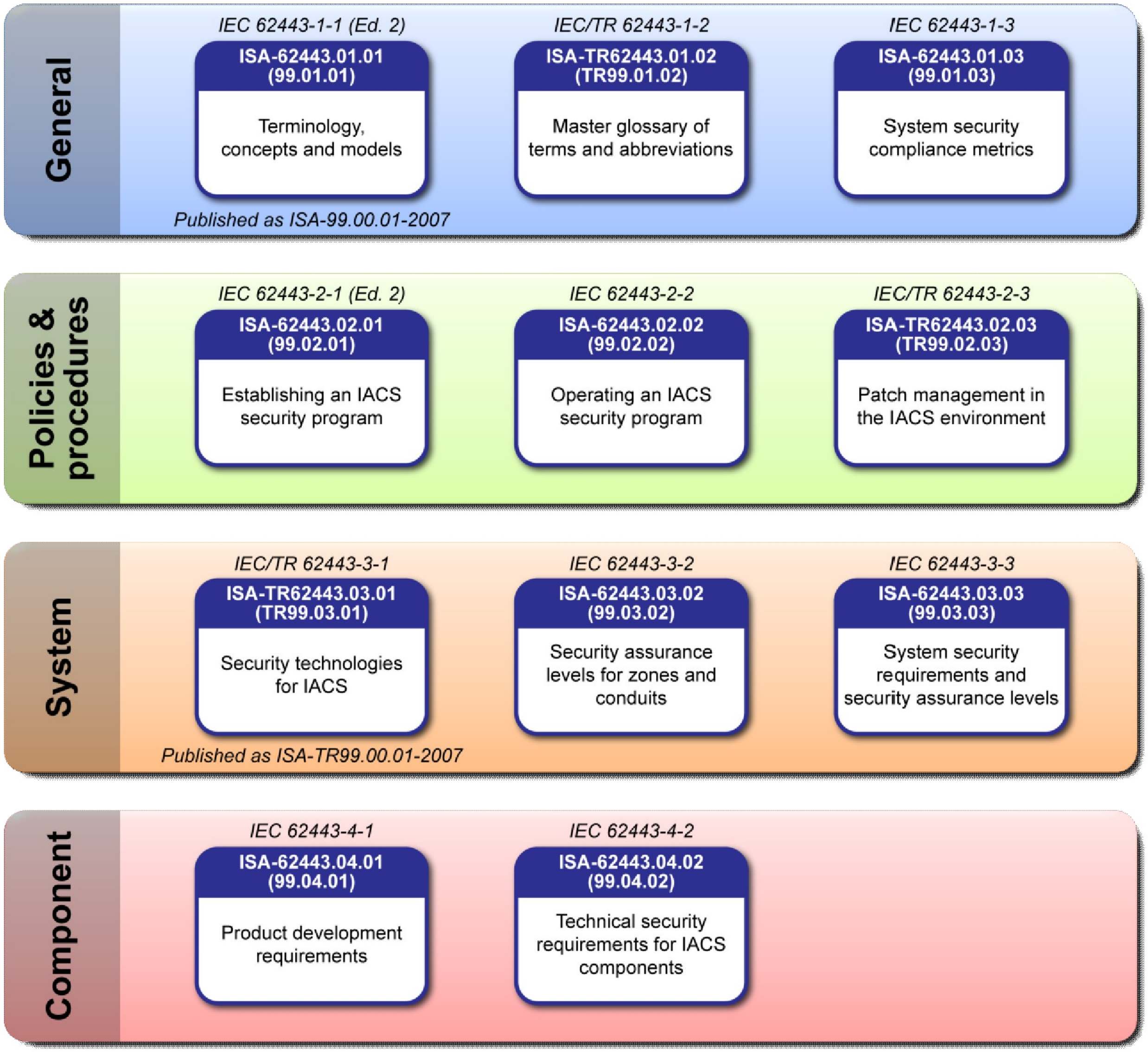
- Addresses Industrial Automation and Control Systems
- Compromise could result in:
  - Endangerment of public or employee safety
  - Loss of public confidence
  - Violation of regulatory requirements
  - Loss of proprietary or confidential information
  - Economic loss
  - Impact on entity, local, state,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

Connecting with Others



ISA-99 Work Products



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
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	

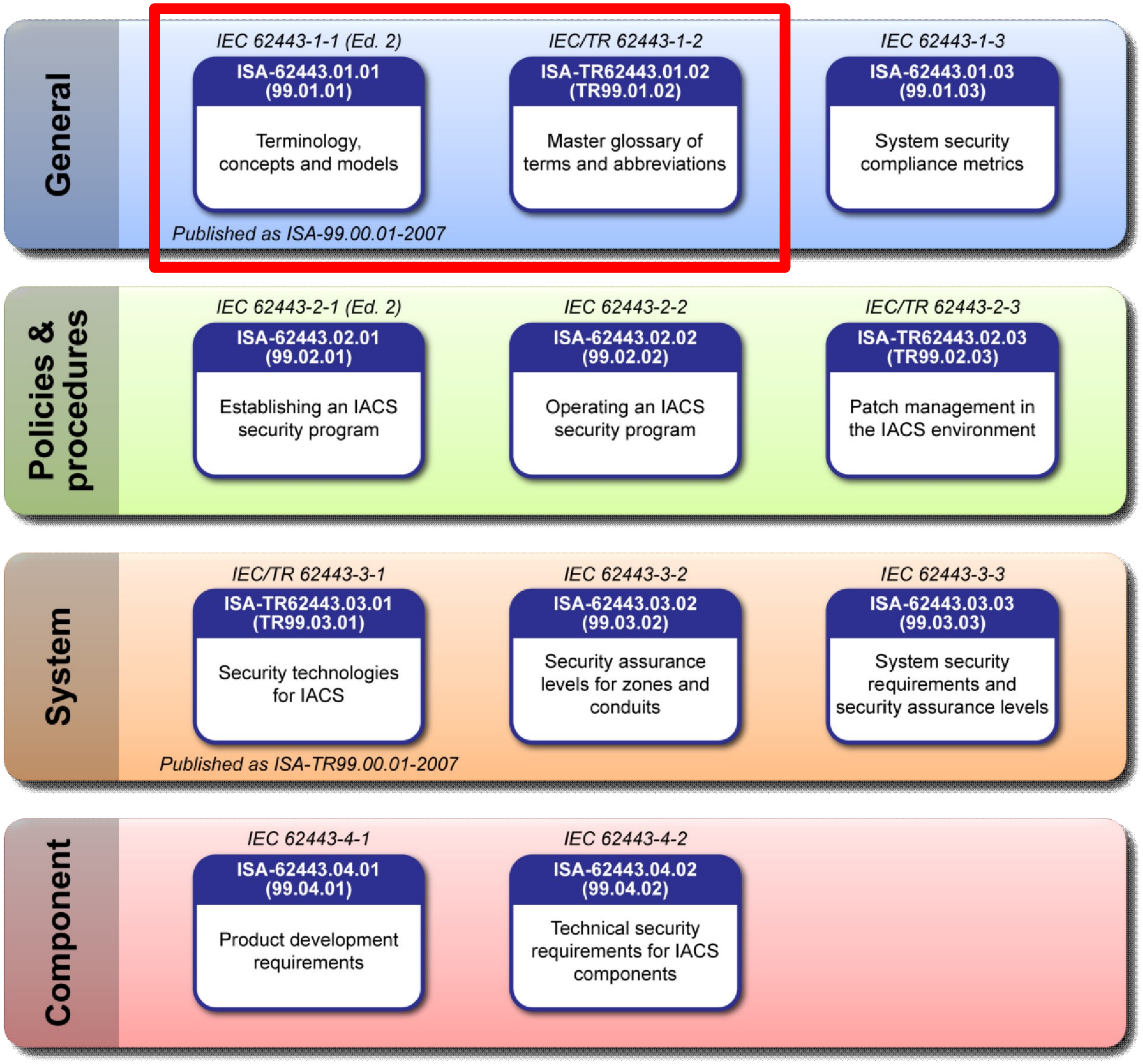
Published as ISA-99.00.01-2007

Published as ISA-TR99.00.01-2007

- 4 Main Series
  - General
  - Policies & Procedures
  - System
  - Component
- IEC 62443 Series Matches

Current as of December 2011

ISA-99 Work Products

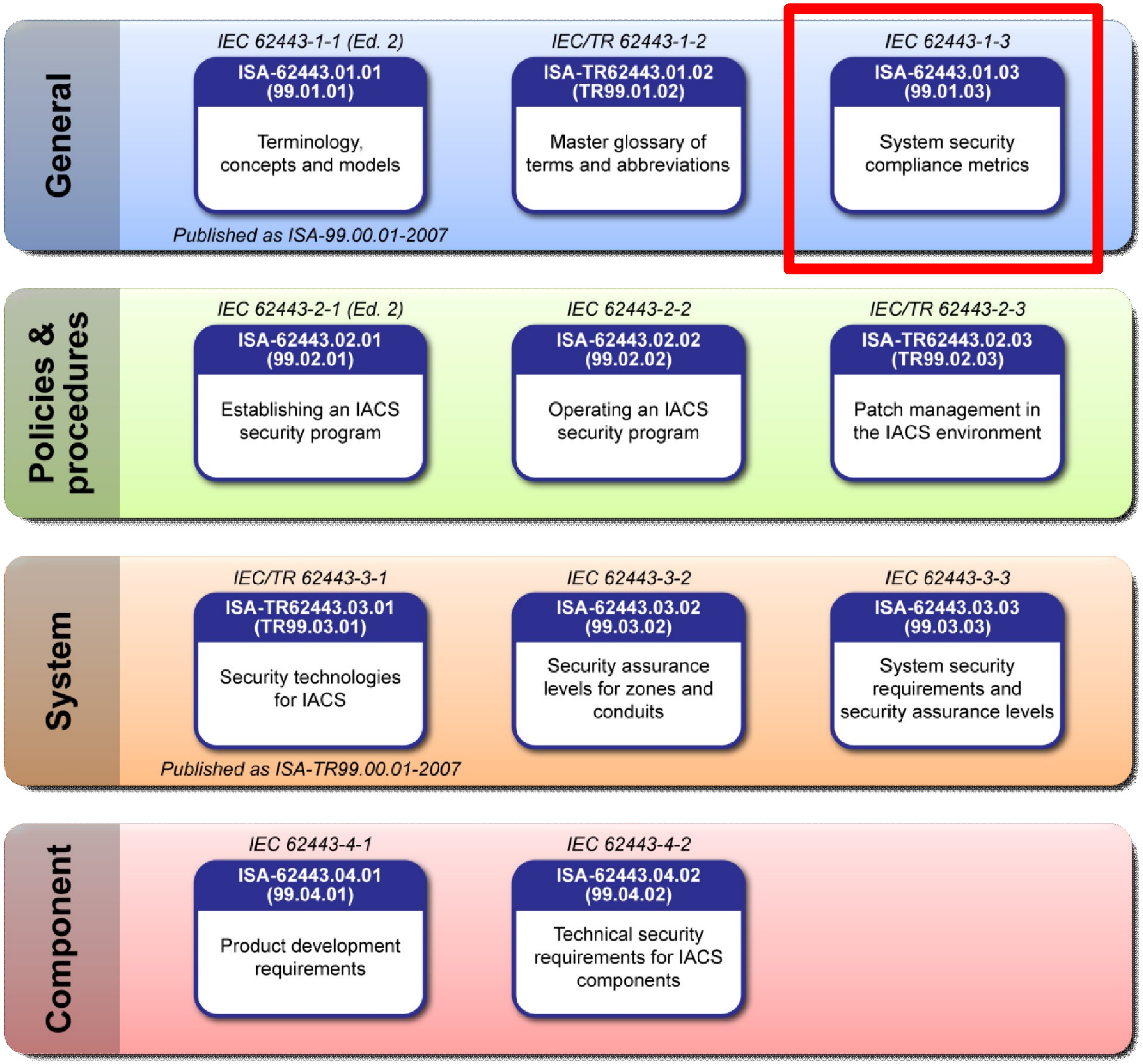


General	*IEC 62443-1-1 (Ed. 2)* **ISA-62443.01.01 (99.01.01)** Terminology, concepts and models	*IEC/TR 62443-1-2* **ISA-TR62443.01.02 (TR99.01.02)** Master glossary of terms and abbreviations	*IEC 62443-1-3* **ISA-62443.01.03 (99.01.03)** System security compliance metrics
	Published as ISA-99.00.01-2007		
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
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	

- Terminology, concepts and models
  - Foundational Material
  - Consistent Terminology

Current as of December 2011

ISA-99 Work Products

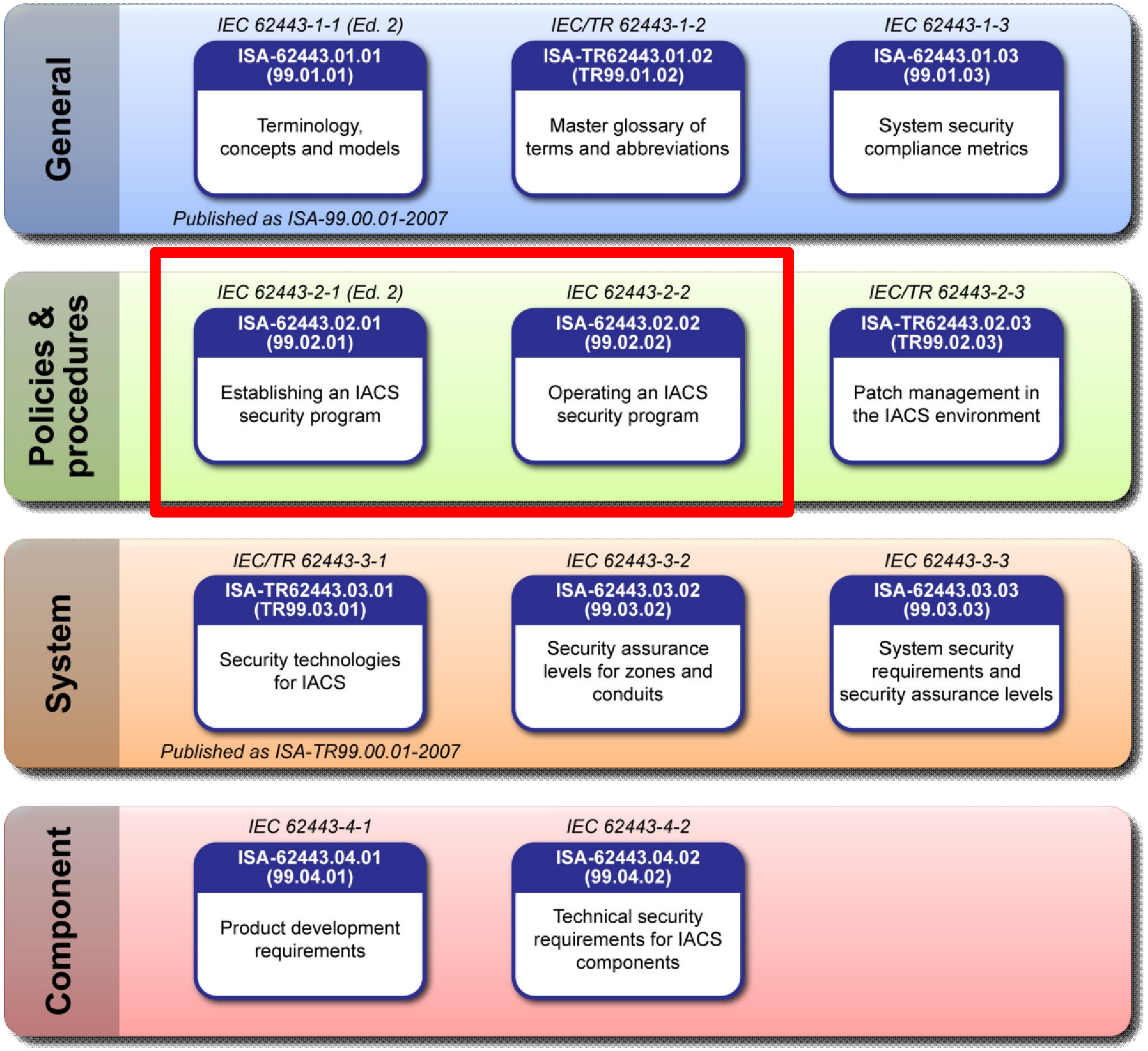


General	IEC 62443-1-1 (Ed. 2) ISA-62443.01.01 (99.01.01) Terminology, concepts and models	IEC/TR 62443-1-2 ISA-TR62443.01.02 (TR99.01.02) Master glossary of terms and abbreviations	IEC 62443-1-3 ISA-62443.01.03 (99.01.03) System security compliance metrics	Published as ISA-99.00.01-2007
Policies & procedures	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	
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		

Current as of December 2011

- Security Compliance Metrics
  - Consistent
  - Usable
  - Quantitative
  - Non-trivial
  - Measure Achieved SALs

ISA-99 Work Products



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
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	

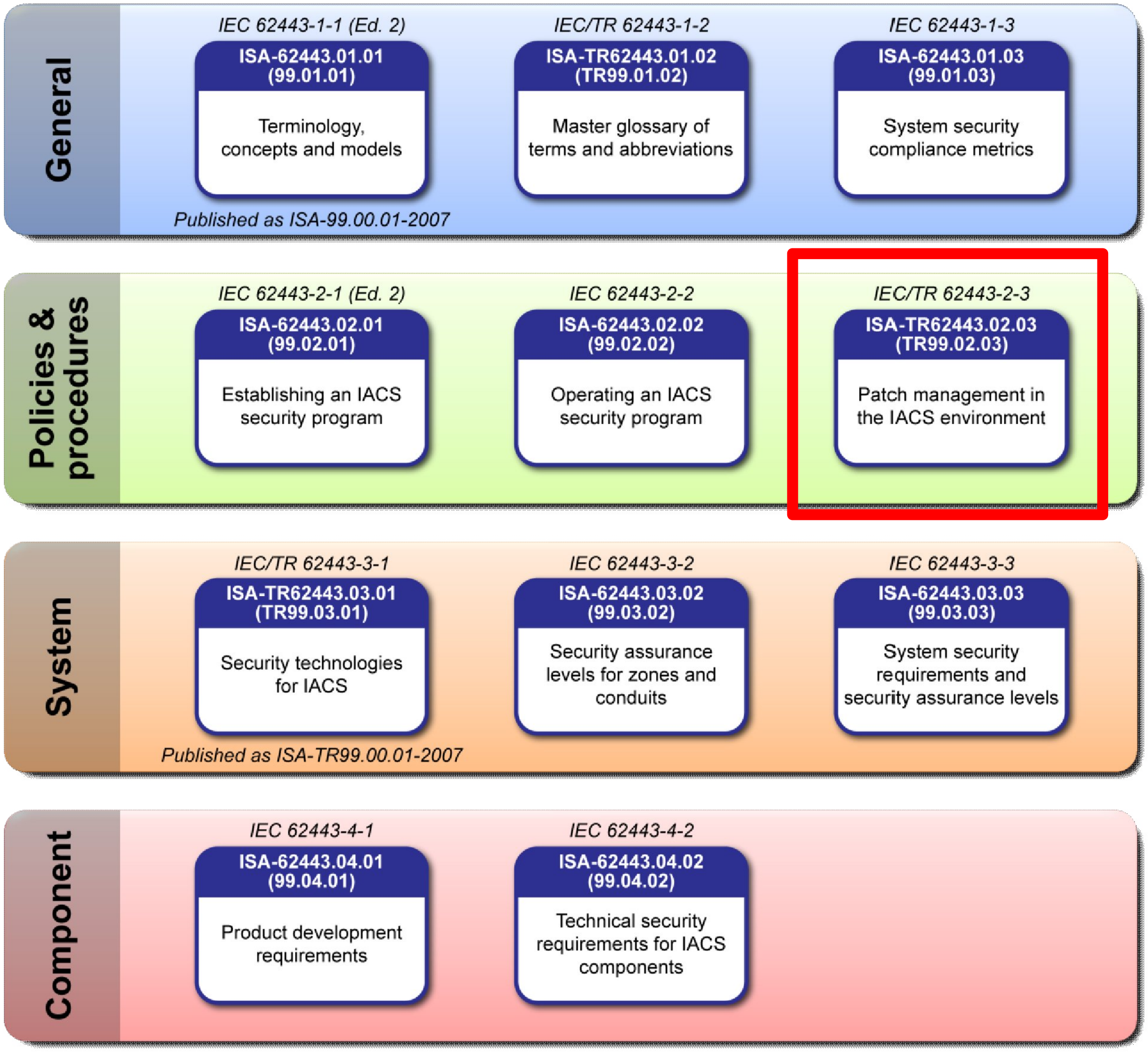
Published as ISA-99.00.01-2007

Published as ISA-TR99.00.01-2007

- Establishing & Operating a Security Program
  - Asset Owner Focused
  - Non-Technical
  - Based upon ISO/IEC 27002
  - IACS-Specific Requirements & Guidance

Current as of December 2011

ISA-99 Work Products



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
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	

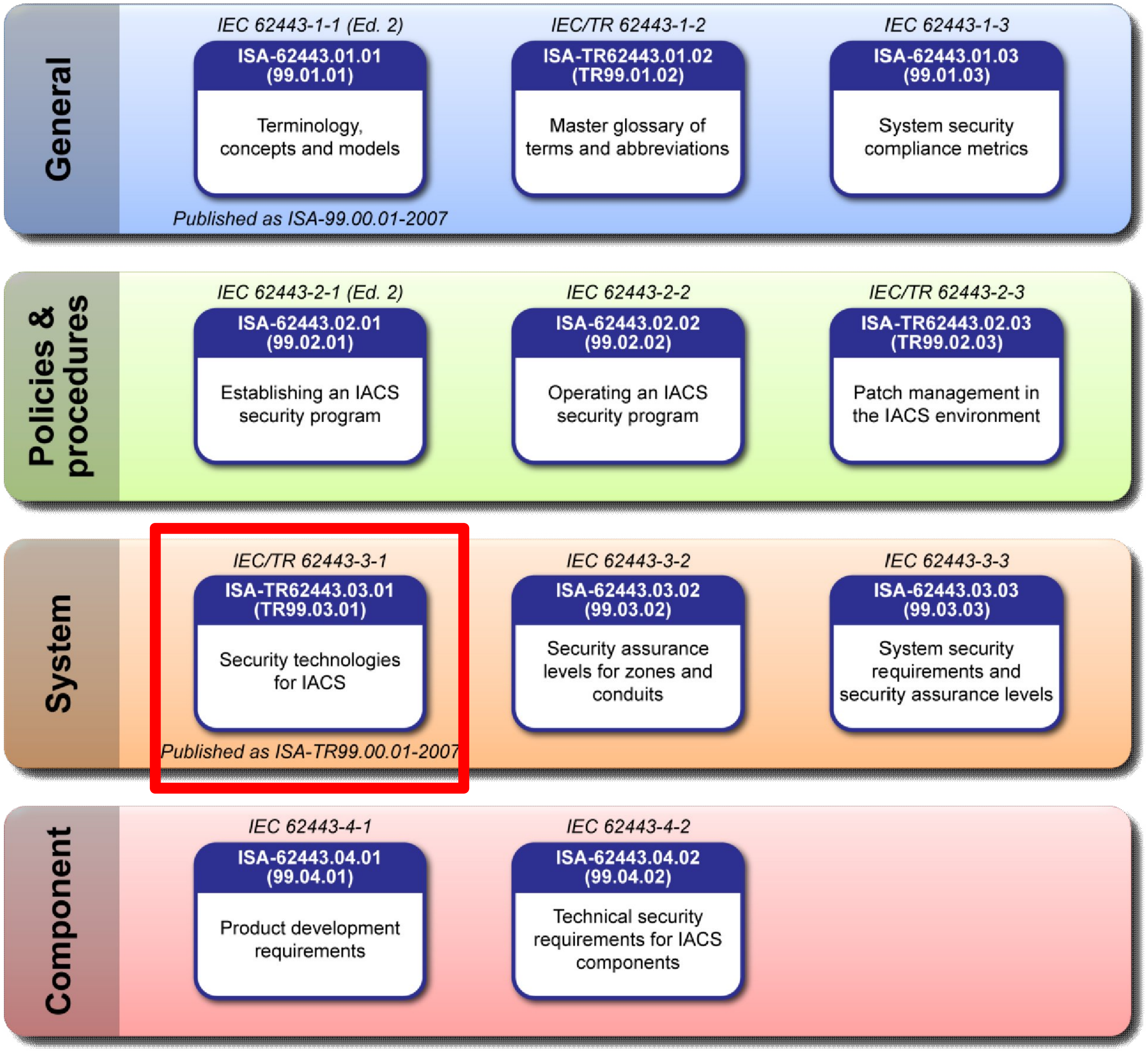
Published as ISA-99.00.01-2007

Published as ISA-TR99.00.01-2007

- Patch Management
  - Applying Well-Established Practices to IACS
  - XML Schema for Patch Descriptions

Current as of December 2011

ISA-99 Work Products



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

System

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

Published as ISA-TR99.00.01-2007

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

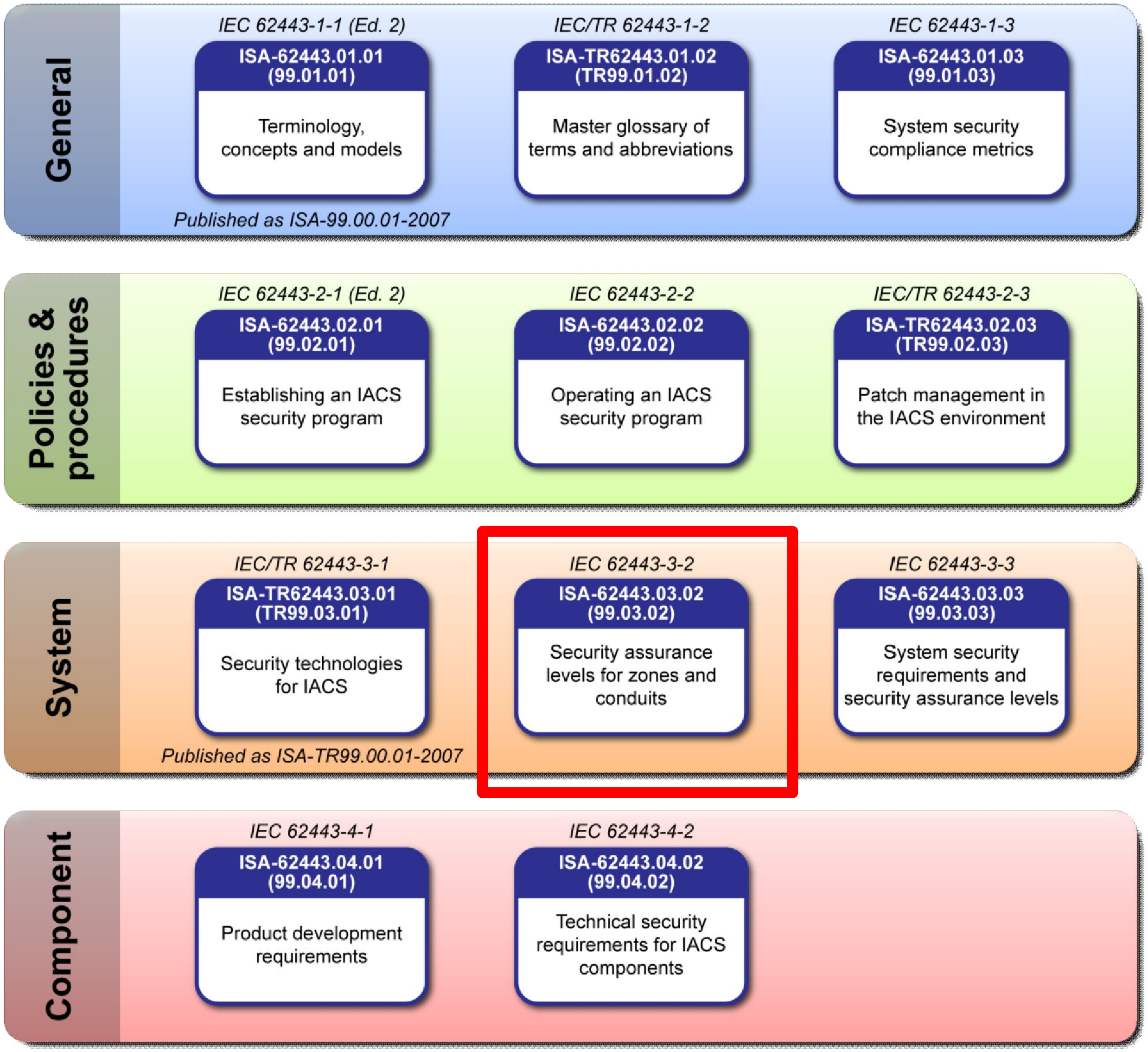
IEC 62443-4-1
ISA-62443.04.01 (99.04.01)
Product development requirements

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

- Security Technologies
  - Guidance on Applying Existing Tools, Technology and Controls to IACS

Current as of December 2011

ISA-99 Work Products



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

System

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

Published as ISA-TR99.00.01-2007

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

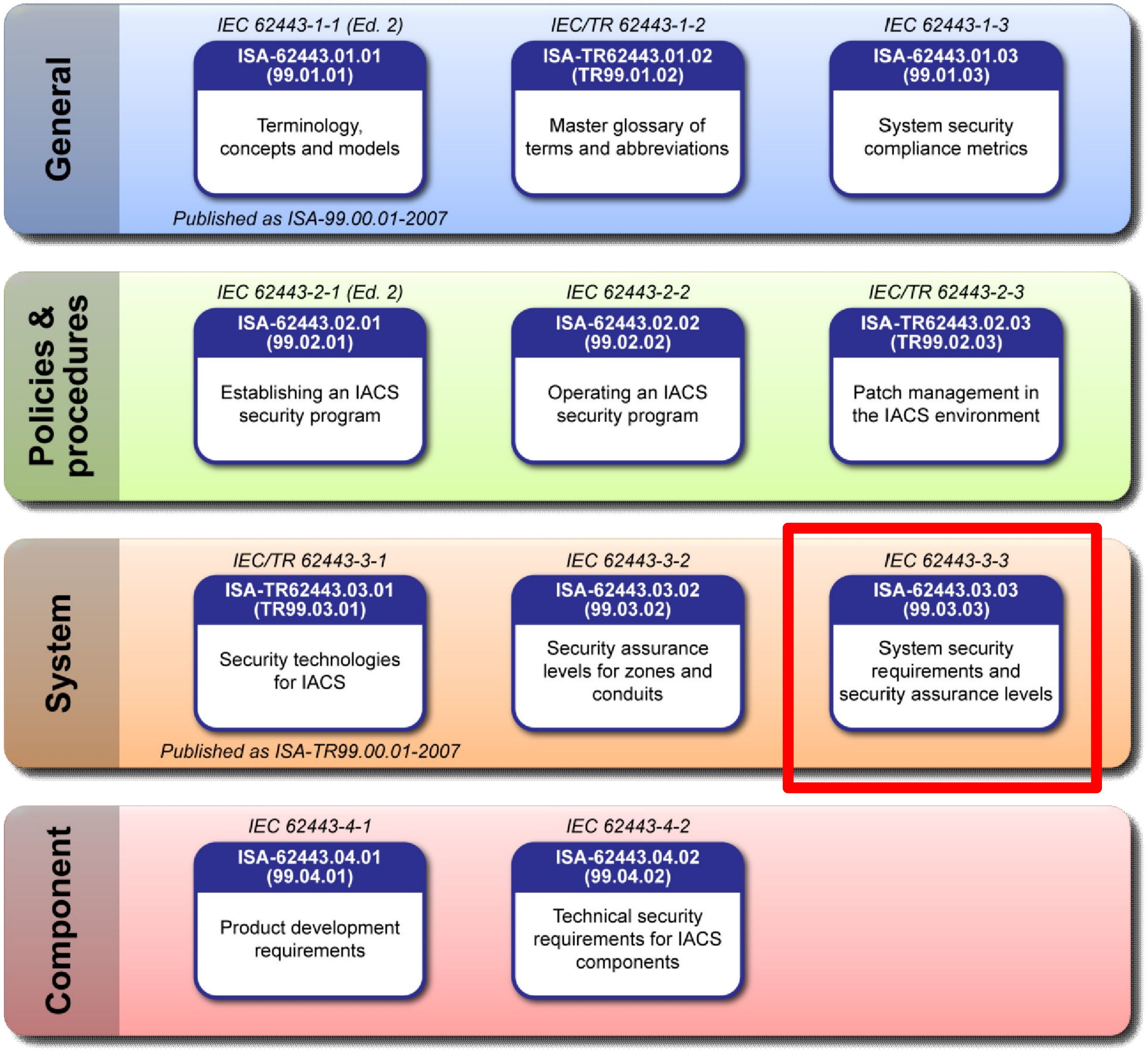
IEC 62443-4-1
ISA-62443.04.01 (99.04.01)
Product development requirements

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

Current as of December 2011

- Zones & Conduits
  - Defining Logical Architecture Breakdown
  - Determine Target SALs

ISA-99 Work Products



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

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

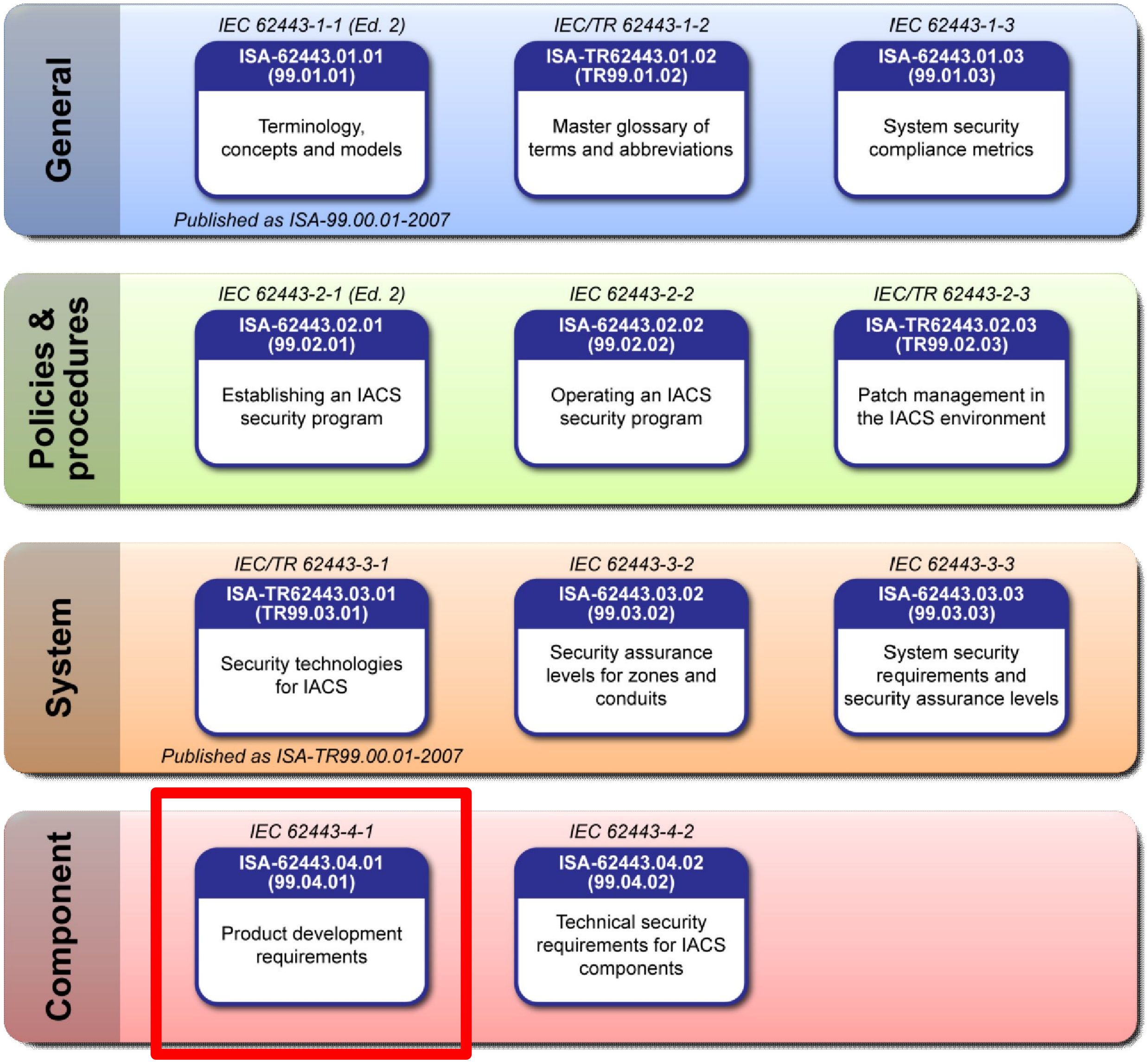
IEC 62443-4-1
ISA-62443.04.01 (99.04.01)
Product development requirements

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

- System-Level Security Requirements
  - Technical Controls
  - IACS-Specific Requirements & Guidance
  - Specifies Capability SALs

Current as of December 2011

ISA-99 Work Products



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
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	

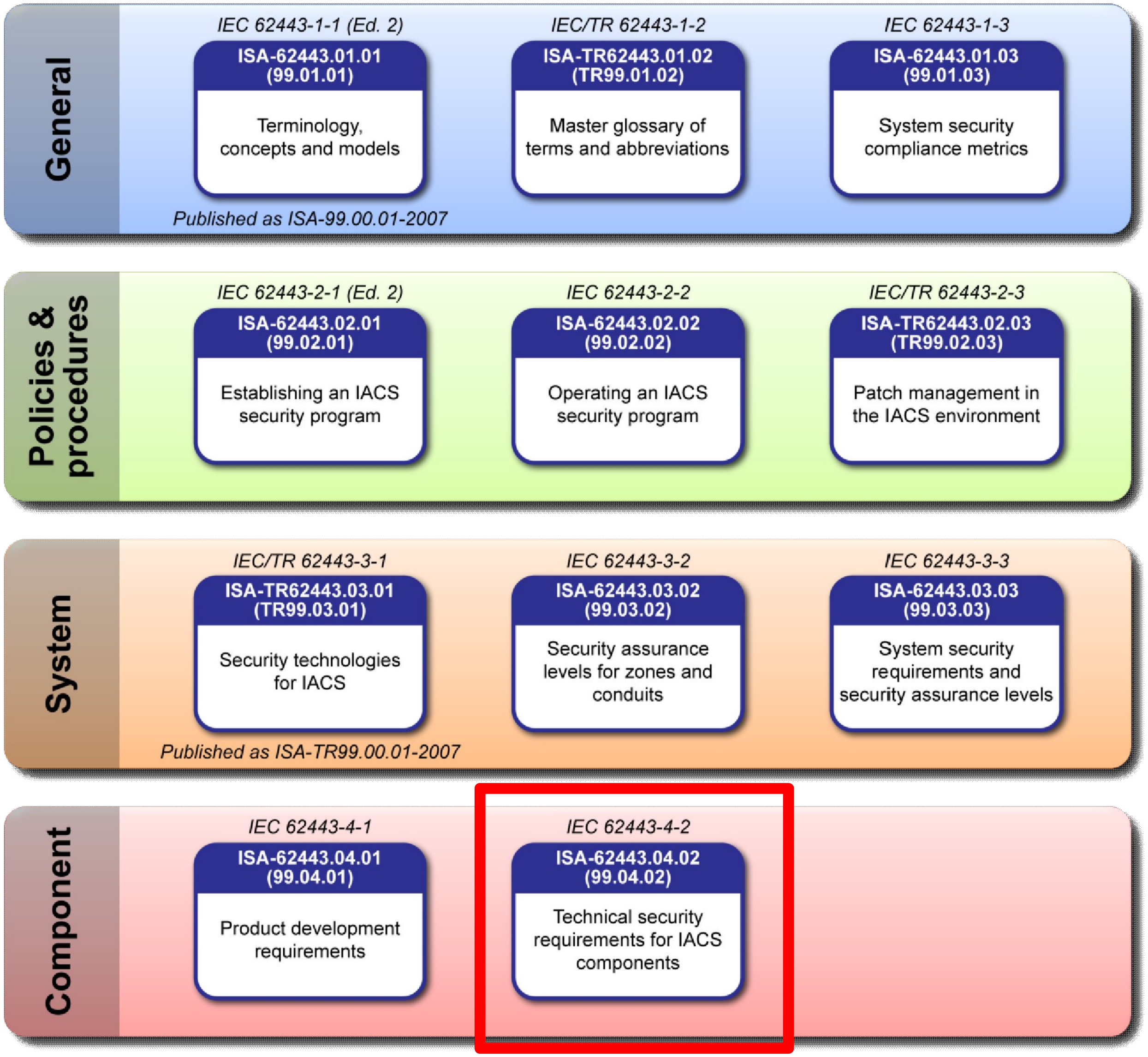
Published as ISA-99.00.01-2007

Published as ISA-TR99.00.01-2007

- Product Development Lifecycle
  - Requirements for Each Development Phase
  - Building Security in From Ground Up

Current as of December 2011

ISA-99 Work Products

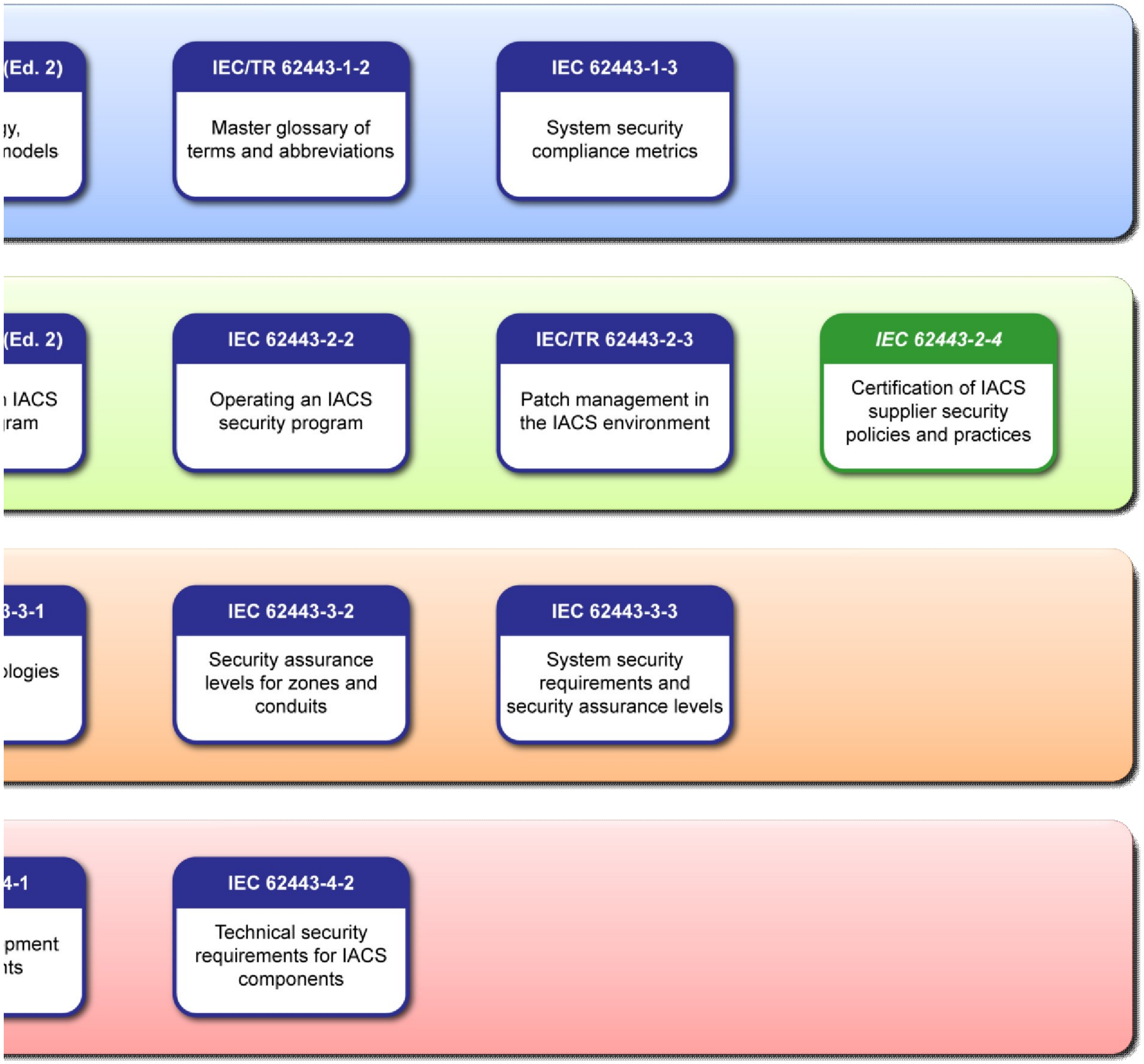


General	*IEC 62443-1-1 (Ed. 2)* **ISA-62443.01.01 (99.01.01)** Terminology, concepts and models *Published as ISA-99.00.01-2007*	*IEC/TR 62443-1-2* **ISA-TR62443.01.02 (TR99.01.02)** Master glossary of terms and abbreviations	*IEC 62443-1-3* **ISA-62443.01.03 (99.01.03)** System security compliance metrics
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
System	*IEC/TR 62443-3-1* **ISA-TR62443.03.01 (TR99.03.01)** Security technologies for IACS *Published as ISA-TR99.00.01-2007*	*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	

- Component-Level Security Requirements
  - Technical Controls
  - Expand System-Level Reqs. For Individual Components
  - IACS-Specific Requirements & Guidance
  - Specifies Capability SALs

Current as of December 2011

IEC 62443 Document Series


(Ed. 2)
y,
nodels
IEC/TR 62443-1-2
Master glossary of terms and abbreviations
IEC 62443-1-3
System security compliance metrics
(Ed. 2)
IACS
ram
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
3-3-1
logies
IEC 62443-3-2
Security assurance levels for zones and conduits
IEC 62443-3-3
System security requirements and security assurance levels
4-1
pment
ts
IEC 62443-4-2
Technical security requirements for IACS components

Current as of December 2011

- IEC 62443-2-4
  - – Additional Document in IEC Series
  - – Outside ISA99 Structure
  - – Vendor Certification Requirements

Additional Technical Working Groups

- WG7 – Security & Safety
- WG8 – Communications & Outreach
- WG9 – Wireless Security
- WG11 – Nuclear Plant Security

Applying the ISA-99 Work Products

- Several organizations using
  - Concepts as defined in ISA-99.01.01
  - Programs as defined in ISA-99.02.01
  - Zone & Conduit model
- Case studies are becoming available
- Overall, the feedback is quite good!

More Information

- ISA99 Wiki
  - http://isa99.isa.org
- Contacts
  - Eric Cosman, eric.cosman@gmail.com
  - Bryan Singer, bryan.singer@kenexis.com
  - Jim Gilsinn, james.gilsinn@nist.gov
- ISA Staff
  - Charley Robinson, crobinson@isa.org