Setting the Standard for Automation™

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709
PHONE (919) 549-8411
FAX (919) 549-8288
E-MAIL info@isa.org
www.isa.org

NIST Cybersecurity Framework

ISA99 Response to Request for Information

Date:	April 5, 2013
Organization:	International Society of Automation (ISA) / The Automation Federation
Committee:	ISA99, Industrial Automation and Control Systems Security
Type:	International industry standards development organization
Sector Scope:	All industrial sectors and critical infrastructure
Technical Scope:	Industrial automation and control systems

On behalf of the ISA99 Committee on Industrial and Automation Control Systems (IACS) Security, we are pleased to submit this response to the Request for Information on the subject Framework for Reducing Cyber Risks to Critical Infrastructure. In providing the requested information, we have focused on describing the ongoing, ANSI-accredited ISA99 program that has drawn industrial cybersecurity experts from across the globe to develop a comprehensive series of consensus industry standards.

Respectfully,

Eric C. Cosman
James D. Gilsinn

ISA99 Co-Chairs

Table of Contents

1 About ISA

The International Society of Automation, ISA, is a global, nonprofit technical association of more than 30,000 automation professionals engaged in the design, development, production, and application of devices and systems that sense, measure, and control industrial processes and manufacturing operations.

ISA provides education and training, professional certification, conferences and workshops, standards, and publications including textbooks, a magazine, and a peer-reviewed technical journal. ISA has local member sections in 28 countries and 19 different technical divisions and interest groups. Based in Research Triangle Park, North Carolina, ISA is the founding member of the Automation Federation, an umbrella nonprofit with 15 organizational members representing more than 400,000 individual practitioners, unifying the profession and serving as the voice of automation.

ISA is best known for developing consensus industry standards that meet American National Standards Institute (ANSI) requirements for openness and due process. Through ISA's ANSI accreditation, many original ISA Standards have been adopted to become widely used international standards through the International Electrotechnical Commission (IEC) in vital areas including industrial cybersecurity, enterprise-control system integration, batch process control, and process safety.

ISA is leading an international program called ISA99 to develop a comprehensive set of cybersecurity standards for industrial automation and control systems (IACS) and critical infrastructure that are being adopted as the IEC 62443 series of standards. Unlike programs targeted at specific industries, the ISA99 initiative is applicable to all key industry sectors and critical infrastructure in recognition of the interrelated nature of industrial computer networks in which cyber vulnerabilities exploited in one sector can impact multiple sectors and infrastructure.

2 The need for standards specific to Industrial Automation and Control Systems

2.1 Overview

Industrial automation and control systems designs increasingly use commercial-off-the-shelf (COTS) technology (for example, network protocols and operating systems) that are inexpensive, efficient, and highly automated, and that can be interconnected in heterogeneous environments. These systems are also increasingly interconnected with non-IACS networks for business reasons. These devices, open networking technologies, and increased connectivity present greater opportunities for cyber attacks against control system hardware and software. These multiple weaknesses can lead to serious or even catastrophic health, safety and environmental (HSE), financial and/or reputational consequences in deployed control systems.

The private sector across the industrial automation landscape (including vendors, integrators, asset owners, ISA and the Automation Federation) is greatly concerned about these weaknesses and vulnerabilities and has been working collectively to provide defensible solutions appropriate to both existing and newly built critical infrastructure. For more than a decade, the ISA99 committee has drawn together leading industrial cybersecurity experts to work within the parameters of a largely volunteer structure to develop the comprehensive strategic architecture of the ISA-62443 series of standards, which have now been recognized by industry worldwide through simultaneous adoption by the International Electrotechnical Commission (IEC).

Organizations choosing to deploy general purpose information technology (IT) cybersecurity solutions to address IACS security may unknowingly expose their systems to significant cyber vulnerabilities arising from a lack of understanding of the highly interrelated and complex nature of IACS networks. While some business IT applications and security solutions can be applied in certain IACS operations, they must be applied in an informed and intelligent way to avoid potentially serious inadvertent consequences. This statement is not simply conjecture, but an established conclusion from, for example, NIST Special Publication 800-82 (June 2011) as well as active research into recommended IACS security practices and associated standards by both government and private industry.

2.2 Component Types

Industrial automation and control systems are generally composed of two types of components:

- Information processing elements (e.g., Human-Machine Interfaces (HMI's) and Historians) that are based on commodity operating systems such as Windows®. To a large degree, traditional Information Technology (IT) cybersecurity approaches, with appropriate care, can be used to secure these components. Applying these approaches to a deployed system is expensive, however, as it requires substantial retesting and modifications of operational procedures.
- Field measurement and control devices that generally use real time operating systems. The communication at this level is usually implemented using industrial application protocols. Modern versions of these are based on industry standards such as Ethernet and TCP/IP. Securing these field devices requires a major modification of traditional IT cybersecurity policies, technologies, and testing, and in many areas entirely new approaches are necessary. Integration of cybersecurity capabilities has begun for the latest generation of field devices, but devices deployed in the field have a lifecycle measured in decades rather than years. Moreover, many industrial protocols have not yet specified security mechanisms.

Even though some of the technologies used in IACS are similar to those used in traditional IT applications, significant differences in characteristics occur due to the fact that logic executing in an IACS environment has a direct affect on the physical world. The approach used to define IACS cybersecurity requirements thus needs to be based on a combination of functional requirements and risk assessment, often requiring an awareness of operational issues as well.

In most cases, a focus on information protection alone is ineffective when considering IACS security. Control systems rarely store or use Personally Identifiable Information. Direct access to the Internet from a control network is often discouraged or prohibited and E-mail usage is also often restricted or even unsupported. Thus, many of the toughest problems facing traditional IT security can often be effectively mitigated by blocking these types of vulnerable applications and protocols, particularly in those parts of a control system deemed 'critical'.

2.3 Security Objectives

A critical requirement of IACS security measures is that they must not have the potential to cause impacts to essential services and functions, including emergency procedures. In contrast, IT security measures as often deployed do have this potential. IACS security goals focus on control system availability, plant safety, plant protection, plant operations (even in a degraded mode) and time-critical system response. General IT security goals often do not place the same emphasis on these factors, typically being more concerned with protecting information than physical assets. This difference in emphasis is often referred to as CIA (confidentiality, integrity, and availability) vs. IAC (integrity, availability, confidentiality).

Understanding this fundamental difference in goals between IACS security and IT security is essential to understanding the need for IACS-specific security standards. This is not simply a matter of semantics, but rather these different goals need to be clearly recognized and stated as security objectives regardless of the degree of plant integration intended and/or achieved. A key step in risk assessment, as required by ISA-62443-1-1, Terminology, Concepts and Models, and ISA-62443-2-1, IACS Security Management System – Requirements, is the identification of which services and functions are truly essential for operations (in some facilities, for example, engineering support may be determined to be a non-essential service or function). In some cases, it may be acceptable for a security action to cause temporary loss of a non-essential service or function, unlike an essential service or function that must not be adversely affected. Additionally, timing is critical for certain control and safety functions. Latency introduced by some IT security solutions, for example, can cause unexpected and adverse control system impacts due to timing delays

2.4 IACS security and Existing Standards

As IACS security requirements are codified, there are a number of common constraints that must be met. Earlier sections have already alluded to a number of them. The result should provide a flexible framework that facilitates addressing current and future vulnerabilities in IACS and applying necessary mitigations in a systematic, defensible manner. It is important to understand that the intention of the ISA-62443 series is to build extensions to enterprise security that adapt the requirements for business IT systems and combines them with the unique requirements for strong availability needed by IACS.

As documented in ISA-62443, an essential function is a "function or capability that is required to maintain health, safety, the environment and availability for the equipment under control." As noted earlier, security measures must not adversely affect essential functions of a high availability IACS unless supported by a risk assessment.

NOTE: In support of this vital point, ISA-62443-2-1 provides guidance on the documentation associated with the risk assessment required to support instances where security measures may affect essential functions.

Based on a risk analysis, some facilities may determine that certain types of security measures may halt continuous operations, but must not result in loss of protection that could result in health, safety and environmental (HSE) consequences. Some specific constraints could include:

- Accounts used for essential functions must not be locked out, even temporarily.
- Verifying and recording operator actions to enforce non-repudiation must not add significant delay to system response time.
- For mission critical control systems with inherently high availability requirements, the failure of the certificate authority or other key management mechanisms must not interrupt essential functions.
- Identification and authentication must not prevent the initiation of safety systems. Similarly for authorization enforcement.
- Incorrectly time-stamped audit records must not adversely affect essential functions.
- Essential functions of an IACS must be maintained if zone boundary protection goes into fail-close and/or island mode.
- A denial of service (DoS) event on the control system or safety system network must not prevent the safety system from actuating as designed.

An IACS rarely operates in isolation from the rest of the enterprise, and thus some essential security functions can be expected to be handled by an external resource. Examples of this might be the maintenance of firewalls and intrusion detection systems by corporate organizations. In addition, in some high resource availability applications, compensating countermeasures external to the control system (such as additional physical security measures and/or enhanced personnel background checks) will be needed. In some cases, a legacy control system that cannot be adequately secured with technology might be made more dependent upon compensating countermeasures such as physical access control and 24/7 staffing and supervision. Sensitivity to lockout or loss of control due to security measures is increased, not decreased, for mission critical control systems. Consequently, a risk assessment which includes noting local operational constraints might result in local relaxation of security controls to enable better availability in combination with enhanced surrounding countermeasures.

Additionally, IACS security clearly is consistent with the business IT security concept of "least privilege". The capability to enforce the concept of least privilege is thus a fundamental requirement of IACS security, with granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability should be available when required, unless it has a detrimental impact on safety.

Finally, some characteristics of IACS – the deterministic nature, the limited number of users, and the usually dedicated purpose of the system – make the use of certain security measures potentially more feasible and affordable in IACS environments than they are in business IT environments. Specifically, security measures applying anomaly detection and the whitelisting concept can be more appropriate in an IACS environment.

3 About the ISA 99 Committee

The purpose of the ISA99 committee is to develop and establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure industrial automation and control systems and security practices and assessing electronic security performance. Collectively this information is being delivered as the ISA-62443 series of documents. Guidance is directed towards those responsible for designing, implementing, or managing industrial automation and control systems as defined in the committee scope. This guidance also applies to users, system integrators, security practitioners, and control systems manufacturers and vendors.

More detailed and current information about the committee and its activities is available on a Wiki site maintained for this purpose:

http://isa99.isa.org

3.1 Committee Scope

The scope of the committee includes industrial automation and control systems whose compromise could result in any or all of the following situations:

- endangerment of public or employee safety
- damage to the environment
- loss of public confidence
- violation of regulatory requirements
- loss of proprietary or confidential information
- economic loss
- impact on national security

The concept of IACS cybersecurity is applied by ISA99 in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. Industrial automation and control systems include, but are not limited to:

- hardware and software systems such as Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Supervisory Control and Data Acquisition Systems (SCADA)[1], networked electronic sensing, and monitoring and diagnostic systems
- associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Physical security is an important component in the overall integrity of any control system environment, but is not addressed in detail in the ISA-62443 series of documents.

3.2 Processes

All activities of the ISA99 committee are conducted within the context of an ANSI-approved consensus standards development process. General procedures and rules have been established by the ISA Standards and Practices board. In addition, the committee has defined more specific and detailed governance processes and procedures that assist in guiding committee activities.

3.1 Representation and Participation

The ISA99 committee membership list is reviewed regularly in order to analyze demographic data. The most recent information shows a total committee membership of **569** individuals, representing well over **150** companies and organizations. Although most members are from North America, the committee includes participants from every geographic region. Committee co-chairs are accountable for maintaining the appropriate balance between various stakeholder groups such as asset owners, suppliers and system integrators. The two largest constituencies are "user" (asset owner) and "producer" (supplier), each with approximately 30% of the total members.

[1] Although the term "SCADA" is commonly used to refer to all types of control systems, the ISA99 committee makes a distinction between the types listed.

3.2 Structure

The comprehensive approach of the ISA99 committee is reflected in its working group (WG) structure, shown in Table 1, with each WG focusing on specific aspects of IACS security.

Table 1 – ISA99 Work Groups

Name	Topic	Description
WG 1	Security technologies	Provides general guidance on the applicability of specific technology in the IACS environment
WG 2	Security Program Definition and Operation	Responsible for developing ISA-62443-2-1, Requirements for an IACS Security Management System, including alignment with ISO 27001
WG 3	Terminology, Concepts and Models	Responsible for developing ISA-62443-1-1, Terminology, Concepts and Models. This standard establishes the basis for the 62443 series.
WG 4	Technical Requirements	Responsible for several standards and reports in the ISA-62443 series that defined specific technical requirements for IACS security.
WG 5	Committee Leadership	Includes leaders of each active work group. Purpose is directing committee activities in support of the co-chairs.
WG 6	Patch Management	Provides guidance in the area of patch management in the form of technical report ISA-TR62443-2-3.
WG 7	Safety and Security	Establishes and maintains liaison relationships required for addressing issues at the intersection of IACS security and process safety.
WG 8	Communications and Outreach	Primarily responsible for developing and delivering materials needed to educate and share news about committee activities.
WG 9	Wireless and Security	Establishes and maintains liaison relationships required for addressing issues at the intersection of IACS security and wireless communications.
WG 11	IACS Security for the Nuclear Sector	Provides specific guidance on matters related to cybersecurity in the nuclear sector.

4 About the ISA-62443 Series of Industry Standards

The ISA-62443 series of standards is organized into four categories, as depicted in Figure 1. These categories are:

- *General Concepts* – these documents are overarching in nature and apply to the entire series of standards and technical reports.
- *Policy and Procedure* – these documents address the organizational aspects of policies and procedures for cybersecurity.
- *System* – these documents address the system-level technical aspects of cybersecurity, including system design principles and system capabilities
- *Component* – these documents address the component-level technical aspects of cybersecurity, including development processes and component capabilities.

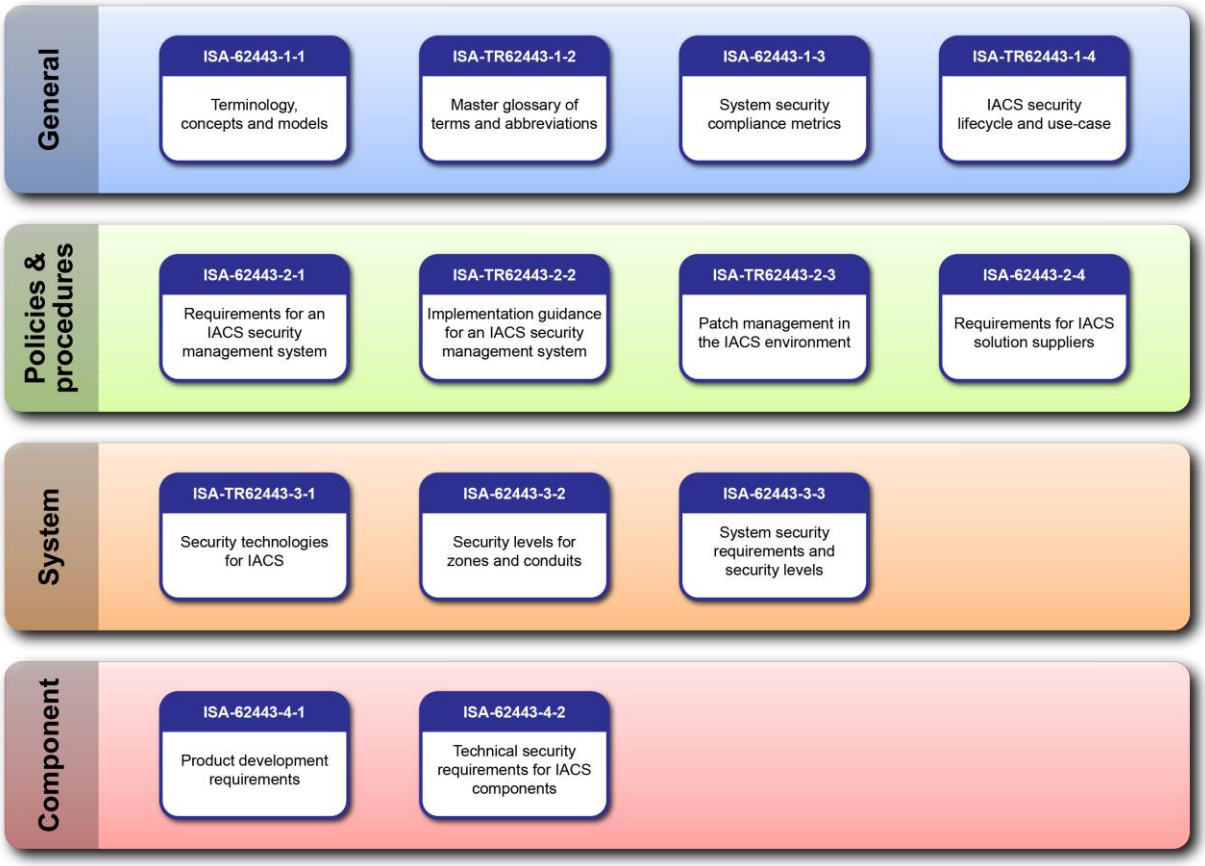

Figure 1 – ISA-62443 Series of Standards and Technical Reports

4.1 Status of Standards

The current status of each of the listed ISA-62443 documents is summarized in the following table.

Table 2 – ISA 62443 Series of Standards and Technical Reports – Development Status

ISA Reference	IEC Reference	Title	Status
ISA-62443-1-1	IEC/TS 62443-1-1	Terminology, concepts and models	Published, Under Revision
ISA-TR62443-1-2	IEC/TR 62443-1-2	Master glossary of terms and abbreviations	Under Development
ISA-62443-1-3	IEC 62443-1-3	System security compliance metrics	Under Development
ISA-62443-1-4	IEC/TR 62443-1-4	IACS security life cycle and use case	Proposed
ISA-62443-2-1	IEC 62443-2-1	IACS security management system – Requirements	Published, Under Revision
ISA-62443-2-2	IEC 62443-2-2	IACS security management system - Implementation guidance	Proposed
ISA-TR62443-2-3	IEC/TR 62443-2-3	Patch management in the IACS environment	Under Development
ISA-62443-2-4	IEC 62443-2-4	Requirements for IACS solution suppliers	Under Development
ISA-TR62443-3-1	IEC/TR 62443-3-1	Security technologies for IACS	Published
ISA-62443-3-2	IEC 62443-3-2	Security assurance levels for zones and conduits	Under Development
ISA-62443-3-3	IEC 62443-3-3	System security requirements and security assurance levels	Approved
ISA-62443-4-1	IEC 62443-4-1	Product Development Requirements	Under Development
ISA-62443-4-2	IEC 62443-4-2	Technical security requirements for IACS components	Under Development

For those documents under development or revision, working drafts are available for public review and comment on the committee Wiki at http://isa99.isa.org.

4.2 General Concepts

General Concept is a term applied to subjects that are important to the understanding of the material in the ISA-62443 series, but are fairly common in the general area of cybersecurity. Each of these concepts is provided as informative content in the first standard in the series, ISA-624431-1-1, and may be referenced in subsequent standards in the series. At this time, the following general concepts have been identified by the ISA99 committee:

- Security Context
- Security Objectives
- Threat-Risk Assessment
- Security Levels
- Security Lifecycle
- Security Program Maturity
- Security Policies
- Defense in Depth
- Security Zones and Conduits
- Role Based Access Control

4.3 Foundational Requirements

In addition to the general concepts, the first standard in the series, ISA-62443-1-1, defines a set of foundational requirements which serve as a common frame of reference in the remaining documents in the series. These foundational requirements are:

- Identification and Authentication Control
- Use Control
- System Integrity
- Data Confidentiality
- Restricted Data Flow
- Timely Response to Events
- Resource Availability

These foundational requirements are used to semi-formally describe the security levels as well as to structure the technical requirements on the system and component levels.

5 Relationship to International Standards

The ISA99 committee has both formal and information liaisons with key national and international groups. ISA99 uses these relationships to communicate with other groups where there is some joint interest in industrial automation and control systems security.

The largest and most wide reaching international committee liaison that ISA99 maintains is with IEC TC65/WG10, Security for Industrial Process Measurement and Control. ISA99 is responsible for generating 12 of the 13 documents currently planned for the ISA/IEC 62443 series. The documents are generated in ISA99 and subsequently voted on and published by both ISA and IEC with minimal differences. The lone standard that IEC TC65/WG10 is directly responsible for generating is IEC-62443-2-4 (Requirements for IACS Solution Suppliers), which will be incorporated into the ISA-62443 series as a U.S. national modification to the IEC version.

ISA99 also maintains a formal liaison agreement with ISO/IEC JTC1/SC27, Working Groups 1 and 3 to develop a security program for IACS. The security program document will not only be published by ISA and IEC, but will also become a formal modification to the ISO/IEC 27001/2 standards used heavily by the IT industry.

ISA99 has established joint working groups with other key ISA committees, including ISA84, *Electrical/Electronic/Programmable Electronic Systems (E/E/PES) for Use in Process Safety Applications*; ISA100, *Wireless Systems for Automation*, and ISA67, *Nuclear Power Plant Standards*.

ISA99 also maintains informal relationships through member joint participation and sharing of documents with groups like the American Chemistry Council, DHS ICSJWG, LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity), the ISA Security Compliance Institute, and others.

These agreements are intended to ensure that there will be a single definitive set of international standards for IACS cybersecurity, the ISA/IEC 62443 series. This goal is in direct response to requests from numerous multi-national companies, including both asset owners and system suppliers.

6 Response to RFI Questions

This section presents ISA99's responses to the specific questions posed in the Request for Information (RFI). Language from the RFI is shown in **bold**, followed by the committee response. Since the ISA99 committee is not representing any particular end user or industry, our responses to the questions below are directed more at addressing the underlying problems that are highlighted by the questions. This is accomplished by providing at least one reference to the ISA99 work to show that the topic has an appropriate section or sections within the scope of the ISA-62443 documents.

6.1 Current Risk-Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

1. **What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?**

   As discussed in section 2 of this response, one of the greatest challenges in improving cybersecurity practices for Industrial Automation and Control Systems is that many of the practices and techniques used for general purpose IT systems are not be applicable for industrial use. The primary reason is that the security objectives for the IT sector are confidentiality, integrity, and availability, in that order, whereas the security objectives for the IACS sector are integrity, availability and confidentiality. Stated another way, the IT sector is responsible for protection of information, whereas the IACS sector is responsible for protection of the physical world. This is the primary reason the ISA99 committee was formed to develop standards and practices that are specific to Industrial Automation and Control Systems.

2. **What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?**

   The ISA99 committee has taken a cross-sector approach to the development of Industrial Automation and Control Systems standards and practices from the beginning. The committee has a large, diverse and international membership that represents many sectors. The committee has also been heavily influenced by cross-sector efforts such as the DHS Catalog of Control Systems Security: Recommendations for Standards Developers, the DHS Cross-sector Roadmap for Cybersecurity of Control Systems, NIST 800-53 Recommended Security Control for Federal Information Systems and Organizations, and NIST 800-82 Guide to Industrial Control Systems (ICS) Security.

3. **Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?**

ISA-62443-2-1, *Requirements for an IACS Security management system*, includes a security management system based on the analysis of risk, the establishment of security policy, organization and awareness, the selection of security countermeasures, and their implementation.

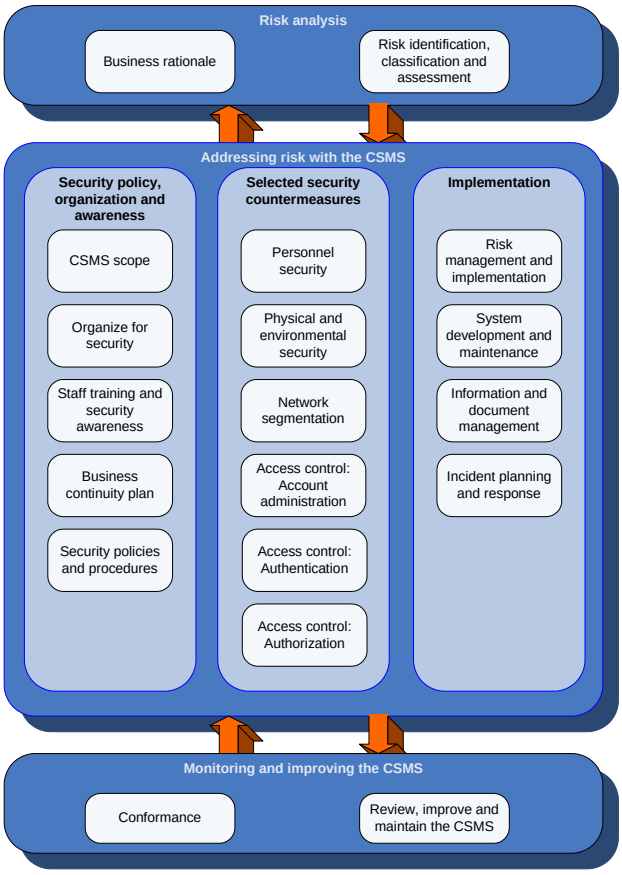

Figure 2 – Graphical view of elements of a cyber security management system

4. **Where do organizations locate their cybersecurity risk management program/office?**

ISA-62443-2-1, *Requirements for an IACS security management system*, describes the characteristics and requirements for a security program, but it allows individual organizations flexibility in how to implement it. This is important because many organizations already have well established security programs for Industrial Automation and Control Systems.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

ISA-62443-2-1, *Requirements for an IACS Security Management System*, includes the identification, classification, and assessment of risk. It includes the systematic identification, prioritization and analysis of threats, vulnerabilities and consequences. Specific requirements include:

- Select a risk assessment methodology
- Provide risk assessment background information
- Conduct a high-level risk assessment
- Identify industrial automation and control systems
- Develop simple network diagrams
- Prioritize systems

ISA-62443-3-2, *Security Levels for Zones and Conduits*, is currently in development. It includes a method for segmenting control systems into *Security Zones*, with communications *Conduits* between them, and assigning *Security Level* requirements for each Zone and Conduit using a risk-based methodology. Security Zones are a more comprehensive method for achieving network segmentation, separation between IT and IACS, and separation between control systems and safety instrumented systems.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

ISA-62443-2-1, *Requirements for an IACS security management system*, facilitates the integration of cybersecurity risk assessment into an organizations' existing risk management system for industrial or manufacturing operations. This allows health, safety, environmental, security and other risks to be assessed at the same time in a comprehensive manner.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

ISA-62443-1-3, *System security compliance metrics*, currently under development, includes a framework for metrics development and use, and recommended metrics for the entire cybersecurity lifecycle.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

Not applicable to this RFI submittal.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

Not applicable to this RFI submittal.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

The ISA-62443-1-3 work product was created to address this specific question. While the choice of specific goals may vary by situation, it is important that there be a well defined set of metrics identified for use with other standards in the ISA-62443 series.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

Not applicable to this RFI submittal.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Because many US-based organizations operate internationally, it is vital that the Cybersecurity Framework point to international standards wherever possible to facilitate the cost effective implementation of cybersecurity for Industrial Automation and Control Systems. The ISA-62443 series of standards is being simultaneously submitted to the International Electrotechnical Commission (IEC) for international review, comment and approval.

The ISA Security Compliance Institute (www.ISASecure.org) is an organization that develops cybersecurity conformance assessment programs based on the ISA-62443 series of standards and practices. See the separate RFI submittal for the ISA Security Compliance Institute for more details.

6.2 Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?

The approach used to address IACS cybersecurity is dependent on factors including the regulatory climate, the level of standardization of solutions, the relationship with the system supplier(s) and the level of technical expertise available. It is the objective of the ISA99 committee to produce a set of consensus-based standards that can be applied in virtually any sector, with the details tailored to meet the needs of the specific situation. This can be done by the asset owner, the solution provider or an independent engineering company.

2. Which of these approaches apply across sectors?

See the response to the previous question.

3. Which organizations use these approaches?

The approach taken for a particular situation or by a particular organization can be influenced by the size and complexity of systems and the level of technical expertise available. The large number of companies represented by the members of the ISA99 committee is a clear indicator that there is strong support for robust, multi-industry international standards.

4. What, if any, are the limitations of using such approaches?

An overly simplistic approach to protecting complex systems leads to a situation where protection is inadequate. Conversely, a complex response to what is inherently a simpler situation can lead to excessive costs of ownership and operation. In either case there will be certain "minimum acceptable" requirements, such as basic protection against malicious software, network segmentation, and the like. These are generally articulated in the form of industry standards such as those that make up the ISA-62443 series.

5. What, if any, modifications could make these approaches more useful?

Standards are more useful if they are comprehensive in scope and available sooner. To that end the most immediate opportunity is to sponsor and support the involvement of more industry experts in their development, and to provide the necessary administrative support to accelerate the development process.

Also, in securing industrial control systems the sometimes complex and arcane security related topics and recommendations must be expressed in terms and within a framework that can be understood and managed by operations and control engineers who are not security experts. Their expertise and major driver is to operate the process under control in the safest, most efficient and profitable manner possible. Moreover, their "language" is that of operations, and not security.

6. How do these approaches take into account sector-specific needs?

ISA formed the ISA99 committee to address the need for cybersecurity standards for industrial automation and control systems regardless of the sector (or country) in which they are employed. The committee has benefited from long term support from many large, multinational companies throughout the process industries. It clearly makes considerably more business sense to have comprehensive, sector-independent standards than to attack the problem on a sector-by-sector basis.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

See above response to question 6. The essential elements of effective standards can be largely sector independent. The nature of how such standards are applied and the specific metrics or performance levels applied can and should be variable by sector, depending on the nature of the processes, materials used, and importance to the critical infrastructure.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

Sector-specific agencies and coordinating councils can promote the use of standards and encourage their members to adopt generally acceptable practices consistent with those standards. They can also sponsor and support standards development by sharing their experience and expertise.

9. What other outreach efforts would be helpful?

Improvements are always desirable in the degree of outreach and collaboration across sectors and across borders. The ISA99 committee has established liaison relationships in vital areas such as process safety and nuclear plant cybersecurity.

6.3 Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

Describing and promoting such practices is an essential theme of the entire ISA-62443 series of standards. Such practices must fully address not only security technology, but also the people and process elements of the subject. As described in ISA-62443-1-1, *Terminology, Concepts and Models*:

"To establish a mature and robust IACS cybersecurity program requires that attention and resources are devoted to the principles of "people", "processes", and "technology". This concept has also been referred to as the people-process-technology triad or triangle. The people-process-technology concept has been applied to business processes moreover than just cybersecurity. The basic premise is that people, processes, and technology all have roles in the cybersecurity of IACS."

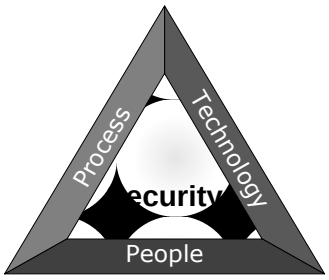

Figure 4 – Security Aspects Triad

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- **Separation of business from operational systems**
- **Use of encryption and key management**
- **Identification and authorization of users accessing systems**
- **Asset identification and management**
- **Monitoring and incident detection tools and capabilities**
- **Incident handling policies and procedures**
- **Mission/system resiliency practices**
- **Security engineering practices**
- **Privacy and civil liberties protection**

1. **Are these practices widely used throughout critical infrastructure and industry?**

   While it not our place as a standards committee to comment on what practices are widely used, we can state that the ISA-62443 series of standards addresses all of these practices (and more), with the exception of privacy and civil liberties protection. These latter items are not typically emphasized in protecting industrial systems since these systems usually do not contain a great deal of personal information.

   The ISA-62443 Policy and Procedure documents define when and how these and other practices should be applied. The System documents and Component documents address the technologies and how they should be applied.

2. **How do these practices relate to existing international standards and practices?**

   The ISA99 committee has made great efforts to bring together numerous standards and recommendations that exist and then to create a comprehensive set of documents that is consistent and broadly applicable to all IACS scenarios. The members of the ISA99 committee have worked closely with or are members of other key ISA, IEC and NIST teams. The bibliography sections of the documents include many references to existing documents as proof of the inclusive nature of the ISA99 initiative. See section 5 above.

   As a result, the ISA-62443 standards are gaining increased attention internationally, and across many sectors. For example, ISA-62443-2-1, *IACS Security Management System – Requirements,* is currently being revised to address comments from the international community and to improve its alignment with the ISO 27000 series of standards for information security.

   More information on the relationships between the ISA-62443 standards and other international standards is given in section 5 of this document.

3. **Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?**

   Because of the ever-changing nature of threats and technology and the uniqueness of each situation, our committee does not prescribe a list of measures for all situations. The ISA-62443 series includes a risk-based methodology for selecting the practices that are most appropriate to mitigate risk for a given situation.

ISA-62443-1-1 Clause 9.1 states:

> *"The objective is to identify the security needs and important characteristics of the environment at a level of detail necessary to address the security issues with a common understanding of the framework and vocabulary."*

4. Are some of these practices not applicable for business or mission needs within particular sectors?

The position of the ISA99 committee is that providing a straightforward list of practices is the correct approach to security – always keeping in mind that the overriding goal is to achieve an appropriate security program for a given situation. This includes the need to provide a life cycle which may change what is needed over time.

ISA-62443-2-1 Clause 0.2 states:

> *"There is not a one-size-fits-all set of security practices. Absolute security may be achievable, but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is really a balance of risk versus cost."*

5. Which of these practices pose the most significant implementation challenge?

Again it is difficult to be specific without details on the IACS system. Any measure that removes or limits an operator's view of the process will be difficult to implement. Practices like individual passwords or system patching are considerably more difficult to apply on an IACS.

To use patching as an example, on a business system patches are pushed down from a central system once the patches are released from the vendor and some general testing is completed. For an IACS, in contrast, it is often necessary to perform extra testing and wait for the system to not be in use, and then apply the patch by hand to ensure that the system is ready to use after the patch is applied.

6. How are standards or guidelines used by organizations in the implementation of these practices?

The ISA-62443 series is designed to be the most comprehensive set of standards that will, in conjunction with any regulation-specific documents, provide organizations the guidance needed to develop and maintain an appropriate security program for their operations.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

ISA-62443-2-2, *IACS Security Management System - Implementation Guidance*, will cover implementation guidance for an IACS security management program. Also, ISA-TR62443-1-4, *IACS Security Life Cycle and Use Case*, is specifically intended to define the common life cycle that is used throughout the ISA-62443 series.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

ISA-62443-2-1, *IACS Security Management System – Requirements*, deals specifically with this need in Clause 4.4.3. The rationale for that clause states:

> *"Review and monitoring are required for the CSMS to remain effective, since the CSMS must respond to changes in internal and external threats, vulnerabilities and consequences, as well as changes in risk tolerance, legal requirements and evolving technical and non-technical approaches to risk mitigation."*

And as noted, ISA-62443-2-2 is designed to cover the implementation guidance for a complete program.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

ISA-62443-2-1, *IACS Security Management System – Requirements*, and ISA-62443-2-2, *IACS Security Management System - Implementation Guidance*, cover the topics of Human Resources Security. While these documents address topics like roles and responsibilities for all involved, they do not cover privacy and civil liberties. In general, an IACS does not contain information related to personnel privacy and civil liberty. One exception might be a system used in the medical space. This is an area that needs to be discussed and possibly included in future editions of those standards, with the understanding that a global document cannot provide specific details on such widely defined concepts.

10. What are the international implications of this framework on your global business or in policymaking in other countries?

The ISA-62443 documents are developed using input, references and industrial cybersecurity experts from across the globe. Reflecting this international collaboration, the numbering system for the ISA-62443 series is based on IEC document numbering. It is the ISA99 committee's firm direction to create documents that are published by the IEC as soon as possible after completing the ISA standards process.

11. How should any risks to privacy and civil liberties be managed?

The concepts and definitions of privacy and civil liberties are very dependent on country and cultural background. Since the ISA99 committee is developing a global set of standards, these topics can only be addressed from a very high level. As stated in the response to question 9 (above), these topics need to be addressed in ISA-62443-2-2.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

The ISA-62443 series assumes continual assessment and response to new and changing risks, so this list will always be subject to revision. The practices that form the basis of effective IACS security include what the standards describe as "Fundamental Concepts." These include (but are not limited to):

- Separation of functions using the concept of zones and conduits. A specific and critical example of this is the distinction between basic control and safety functions.
- Assignment of security levels based on a defined set of criteria.
- Maintaining overall system integrity (including but not limited to data integrity).
- Providing high availability for continuous operation.
- Accommodating the implications of the long service life of IACS systems.

