Introduction

NOTE The format of this document follows the ISO/IEC requirements discussed in ISO/IEC Directives, Part 2. [9] This document specifies the format of the document as well as the use of terms like "shall", "should", and "may". The directives requirements specified in Clause 4 use the conventions discussed in Appendix H of the Directives document.

Overview

Cyber security is an increasingly important topic in modern organizations. Many organizations involved in information technology (IT) and business have been concerned with cyber security for many years and have well-established Cyber Security Management Systems (CSMS) in place as defined by International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 17799 [14] and ISO/IEC 27001 [15]. These management systems give an organization a well-established method for protecting its assets from cyber attacks.

Industrial Automation and Control System (IACS) organizations have begun using commercial-off-the-shelf (COTS) technology developed for business systems in their everyday processes, which has provided an increased opportunity for cyber attack against the IACS equipment. For many reasons these systems are not usually as robust, in the IACS environment, as are systems designed specifically as IACS at dealing with cyber attack for many reasons. This weakness may lead to health, safety and environmental (HSE) consequences.

Organizations may try to use the pre-existing IT and business cyber security solutions to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, they need to be applied in the correct way to eliminate inadvertent consequences.

A cyber security management system for IACS

Management systems typically provide guidance on what should be included in a management system, but do not provide guidance on how to go about developing the management system. ANSI/ISA–99.02.01–2009 addresses the "what" aspect of a CSMS for IACS and also provides guidance on how to go about developing the CSMS for IACS.

A common engineering approach when faced with a challenging problem is to break the problem into smaller pieces and address each piece in a disciplined manner. This approach is a sound one for addressing cyber security risks with IACS. However, a frequent mistake made in addressing cyber security is to deal with cyber security one system at a time. Cyber security is a much larger challenge that must address the entire set of IACS as well as the policies, procedures, practices and personnel that surround and utilize those IACS. Implementing such a wide-ranging management system may require a cultural change within an organization.

Addressing cyber security on an organization-wide basis can seem like a daunting task. Unfortunately, there is no simple cookbook for security. There is good reason for this. 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. All situations will be different. In some situations the risk may be related to HSE factors rather than purely economic impact. The risk may have an unrecoverable consequence rather than a temporary financial setback. Therefore, a cookbook set of mandatory security practices will either be overly restrictive and likely quite costly to follow, or be insufficient to address the risk.

Relationship with ISO/IEC 17799 and ISO/IEC 27001

ISO/IEC 17799 [14] and ISO/IEC 27001 [15] are excellent standards that describe a cyber security management system for business/information technology systems. Much of the content in these standards is applicable to IACS as well. ANSI/ISA–99.02.01–2009 emphasizes the need for consistency between the practices to manage IACS cyber security with the practices to manage business/information technology systems cyber security. Economies will be realized by making these programs consistent. Users of this ISA document are encouraged to read ISO/IEC 17799 and 27001 for additional supporting information. ANSI/ISA–99.02.01–2009 builds on the guidance in these standards. It addresses some of the important differences between IACS and general business/information technology systems. It introduces the important concept that cyber security risks with IACS may have HSE implications and must be integrated with other existing risk management practices addressing these risks.

Document outline

This standard is structured to follow the ISO/IEC and ISA guidelines for standards development as closely as possible, per the following:.

- Clause 1 describes the scope of this standard.
- Clause 2 lists a number of normative references for this standard.
- Clause 3 defines a list of terms and abbreviations needed for this standard. This list is in addition to the list of terms defined in ANSI/ISA–99.01.01–2007. [1]
- Clause 4 defines the elements of a cyber security management system for industrial automation and control systems. Clause 4 is normative.
- Annex A provides guidance on how to develop the elements of the cyber security management system for IACS.
- Annex B describes an example process that an organization could use to develop the elements of the cyber security management system for IACS.
- The bibliography lists references to other sources used in the development of this standard or with some relevance to the material presented here.