Journal of Loss Prevention in the Process Industries 26 (2013) 982–993

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

Identification and application of security measures for petrochemical industrial control systems

H.M. Leith*, John W. Piper [1]

AcuTech Consulting Group, 1919 Gallows Road, Suite 900, Vienna, VA 22182, USA[1]

ARTICLE INFO

Article history:
Received 2 April 2013
Accepted 7 October 2013

Keywords:
Industrial control systems
Security controls
Cyber risk assessment
Security threats
Configuration management

ABSTRACT

The financial success of the chemical and petrochemical industry will increasingly depend upon the security of process control systems. This paper presents recommendations and insights gleaned from over 100 security risk assessment (SRA) and process control analyses, using requirements baselines extracted from the National Institute of Standards and Technology (NIST) special publication 800-53 (and Appendix A), the *Recommended Security Controls for Federal Information Systems and Organizations*, in conjunction with NIST special publication 800-82, *Guide to Industrial Control Systems(ICS) Security*, to provide the bridge in application of 800-53 controls to IC/SCADA.

The paper identifies how current and projected malevolent threats posed by insiders, outsiders, collusion, and system-induced threats can erode system performance in terms of shut downs, sabotage, production disruption, and contamination. The issue is not whether there are clear and present cyber threats, nor whether there are business prudent practices that can be implemented to counter those threats; but rather that there is such a diverse compendium, at times conflicting and often technically obtuse guidance, that clarity is needed to narrow the focus of this guidance to assist those responsible for implementing effective process control security.

The paper focuses on application of business-prudent controls and discusses how disparities in implementation of controls can exacerbate system vulnerabilities. Topics include issues of processes control system management, systems documentation, use of contractors and remote contractor access, system authorities that exceed user needs, misalignment of staff perception of information asset values, exposures related to use of USB ports, lack of encryption, and background surety gaps for individuals and contractor companies with access to process control systems.

The paper examines the dynamics of communicating information from process control systems to business IT systems and the pressure from business operations to capture process data and make it available in near real-time through administrative networks. Such pressures may influence systems administrators to overlook or ignore firewall and systems engineering architecture, increasing potentials for two-way interface between business and process control that significantly increases exploit exposures. Despite the availability of excellent guidelines for physical and technical security of IT related assets, these practices are too often unheeded in favor of expediency or expanded access. The paper includes a discussion of Risk Management Framework models that should be considered to enhance the correspondences and relationships between multiple organizational domains, thereby promoting more effective cyber security for current and future process control systems.

The paper summarizes the process for establishing security for industrial control systems (ICS), and addresses cyber security baseline requirements and expectations, within a risk management framework that provides a decision basis, threat dynamics, common vulnerabilities, and prudent mitigation measures. Much of this summary has been derived from The Information Technology Laboratory at the National Institute of Standards and Technology (NIST) *Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems* and *NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security*. NIST has also published *Applying NIST SP 800-53 to Industrial Control Systems* which demonstrates the relationship of 800-53 to ICS security and the application of more than 20 control families and over 625 control elements to ICS security. Although originally designed for Federal systems,

* Corresponding author. Tel.: +1 703 676 3180.
E-mail addresses: hleith@aol.com, hleith@acutech-consulting.com (H.M. Leith), jpiper@acutech-consulting.com (J.W. Piper).
[1] http://www.acutech-consulting.com.

0950-4230/$ – see front matter
http://dx.doi.org/10.1016/j.jlp.2013.10.009

portions of these publications also provide a solid foundation for critical commercial and industrial information control systems in terms of addressing the basic questions that companies in the process industry should consider when selecting security controls, including:

- What controls are actually needed to protect process systems, while supporting operations and safeguarding critical assets?
- Can the selected controls suggested for Federal systems effectively be implemented for systems in the process industry?
- Once selected and implemented, will these controls really be effective in protecting the processes?

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* helps answer questions to strengthen commercial processes information security programs. The security controls articulated in NIST SP 800-53 provide guidance and recommend practices applicable to security systems in process industries, to provide a foundation for understanding the fundamental concepts of security controls. The introductory material presents the concept of security controls and their use within well-defined information security programs. Some of the issues discussed include the structural components of controls, how the controls are organized into families, and the use of controls to support information security programs. The guide outlines the essential steps that should be followed to determine needed controls, to assure the effectiveness of controls, and to maintain the effectiveness of installed controls.

The appendices in NIST SP 800-53 provide additional resources including general references, definitions, explanation of acronyms, a breakdown of security controls for graduated levels of security requirements, a catalog of security controls, and information relating security controls to other standards and control sets. The controls are organized into classes of operational, management, and technical controls, and then into families within each class. To maintain parity and applicability with advances in technology, NIST also plans to review and to update the controls in the catalog as technology changes and new safeguards and new information security countermeasures are identified. NIST SP 800-53 and related documents are available at http://csrc.nist.gov/publications/nistpubs/index.html. The extensive reference list in SP 800-53 includes standards, guidelines, and recommendations that process industry companies can use as the foundation for comprehensive security planning and lifecycle management processes. Additionally, a significant effort of broad commercial and government cooperation, the Consensus Audit Guideline (CAG) provides a 20-element cyber security controls roster supporting a common commercial framework for cyber security, correlating to the NIST 800-53 Control Library.

1. Industrial control system security in the process industry

Industrial control systems (ICS), include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) and Human–Machine Interface (HMI) commonly found in the chemical and petrochemical industry process control sectors. These control systems are vital to the operation of critical infrastructures that are increasingly highly interconnected and mutually dependent systems. Historically, ICS had little resemblance to traditional information technology (IT) systems in that ICS were "isolated systems" running proprietary control protocols using specialized hardware and software. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions. ICS managers are increasingly adopting IT solutions to promote corporate business systems connectivity and remote access capabilities. ICS are being designed and implemented using industry standard computers, operating systems (OS) and network protocols; hence they increasingly resemble traditional IT systems. This integration supports new IT capabilities, but reduces the isolation of ICS from the outside world, creating a greater need for ICS security. While security solutions have been designed to deal with security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new security solutions are needed that must be specifically tailored to the ICS environment.

The term "security" is considered herein to mean the prevention of illegal or unwanted access, intentional or unintentional interference with the proper and intended operation, or inappropriate access to industrial automation and control systems. The focus includes operating systems, data processing and control systems, associated networks, software applications, and other programmable configurable components; where "security controls" are the management, operational, and technical safeguards that protect the confidentiality, integrity, and availability of an information system and its information. In this context, organizations face critical decisions in selecting and implementing the right controls and in making the controls an effective part of their integrated information security programs.

2. Nature of ICS assets and issues with IT systems

Although some characteristics between IT and ICS are similar, it is important to note that ICS also have characteristics that differ significantly from traditional information processing systems. Many of these differences stem from the fact that logic executing in ICS often has a direct effect on the physical world. ICS have unique performance and reliability requirements and often use operating systems and applications that may be considered "unconventional" to IT personnel unfamiliar with ICS functionality. Some of these differing characteristics can pose significant risks to health and safety, serious damage to the environment, as well as serious financial consequences, production losses, national economic impact, and compromise of proprietary information. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of critical ICS control systems.