Cybersecurity for Industrial Control Systems

SCADA, DCS, PLC, HMI, and SIS

Tyson Macaulay and Bryan Singer

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Cybersecurity for Industrial Control Systems

SCADA, DCS, PLC, HMI, and SIS

Tyson Macaulay and Bryan Singer

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **Informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
Version Date: 20111027

International Standard Book Number: 978-1-4398-0196-3 (Hardback)

Library of Congress Cataloging-in-Publication Data

Macaulay, Tyson.
Cybersecurity for Industrial Control Systems : SCADA, DCS, PLC, HMI, and SIS / Tyson Macaulay, Bryan Singer.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-4398-0196-3 (hardcover : alk. paper)
1. Process control--Security measures. 2. Automatic machinery--Security measures. 3. Computer security. I. Singer, Bryan. II. Title.

TS156.8.M328 2012
658.4'78--dc23 2011036559

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Cybersecurity for Industrial Control Systems

SCADA, DCS, PLC, HMI, and SIS

Authors

Tyson Macaulay is the security liaison officer (SLO) for Bell Canada. In this role, he is responsible for technical and operational risk management solutions for Bell's largest enterprise clients.

Macaulay leads security initiatives addressing large, complex, technology solutions including physical and logical (IT) assets, and regulatory/legal compliance requirements. He supports engagements involving multinational companies and international governments. Macaulay also supports the development of engineering and security standards through the Professional Engineers of Ontario and the International Standards Organization (ISO) SC 27 Committee.

Macaulay's leadership encompasses a broad range of industry sectors from the defense industry to high-tech start-ups. His expertise includes operational risk management programs, technical services, and incident management processes. He has successfully served as prime architect for large-scale security implementations in both public and private sector institutions, working on projects from conception through development to implementation. Macaulay is a respected thought leader with publications dating from 1993. His work has covered authorship of peer-reviewed white papers, IT security governance programs, technical and integration services, and incident management processes. Further information on Macaulay's publications and practice areas can be found online at: www.tysonmacaulay.com.

Previously, Macaulay served as director of risk management for a U.S. defense contractor in Ottawa, Electronic Warfare Associates (EWA; 2001–2005), and founded General Network Services (GNS; 1996–2001). Macaulay's career began as a research consultant for the Federal Department of Communications (DoC) on information networks, where he helped develop the first generation of Internet services for the DoC in the 1990s.

Bryan L. Singer, CISM, CISSP, CAP, is principal consultant for Kenexis Consulting Corporation. Singer has more than 15 years experience in information technology security, including 7 years specializing in industrial automation and control systems security, critical infrastructure protection, and counterterrorism. His background focuses on software development, network design, information security, and industrial security. Industry experience includes health care, telecommunications, water/wastewater, automotive, food and beverage, pharmaceuticals, fossil and hydropower generation, oil and gas, and several others. He has specialized in process intelligence and manufacturing disciplines such as historians, industrial networking, power and energy management (PEMS), manufacturing enterprise systems (MES), laboratory information management systems (LIMS), enterprise resource planning (ERP), condition-based monitoring (CBM), and others.

Singer began his professional career with the U.S. Army as an intelligence analyst. After the military, he worked in various critical infrastructure fields in software development and systems design, including security. Singer has worked for great companies such as EnteGreat, Rockwell Automation, FluidIQs, and Wurldtech before joining Kenexis Consulting and cofounding Kenexis Security in 2008. At Kenexis, he is responsible for development, deployment, and management of industrial network design and security services from both a safety and a system architecture perspective.

Singer is also the cochairman of ISA-99 Security Standard, a former board member of the Department of Homeland Security's Process Control Systems Forum, member of Idaho National Labs recommended practices commission, U.S. technical expert to IEC, North American Electronics Reliability Corporation (NERC) drafting team member for NERC CIP, and other industry roles.

Contents

1

INTRODUCTION

This book is either ambitious, brave, or reckless approaching a topic as rapidly evolving as industrial control system (ICS) security. From the advent of ICS-targeted malicious software such as Stuxnet to the advanced persistent threats posed by organized crime and state-sponsored entities, ICS is in the crosshairs and practices and controls considered safe today may be obsolete tomorrow. Possibly more so than in more traditional IT security, because of the differences inherent in ICS.

We are taking a chance by addressing highly technical topic—the security of industrial automation and process control, also known as ICS security—from both technical and management perspectives, and at times from a more philosophical perspective. The reason for this approach is that a substantial amount of ad hoc and anecdotal technical material and analysis already exist, and this material would benefit from a broader treatment that includes business-level topics such as business case development and compliance and, ultimately, more effective enterprise risk management.

On the face of it, securing communications and operations in industrial automation and process control offers unique challenges in that not only do we deal with the traditional data and communications security requirements found on any given IT network, but we also must deal with the reality of the physics of a process in which motion is controlled and manipulated through data-dependent systems and computers—physical changes that can impact a system in myriad ways. These include costly production stoppages, maintenance failures and repairs, and even hazardous releases and dangerous failures.

In some cases, the published standards and recognized and generally accepted approaches for ICS security and traditional IT security can appear so similar as to be superfluous; however, they are developed to serve substantially different objectives. It is these few substantially different objectives that inspire this book, in which we intend

to discuss ICS security requirements coupled with operational and management solutions.

The overall objective of this book is to improve industrial and enterprise risk management in this age of Internet protocol (IP) convergence, recognizing that industrial systems require the balancing of many engineering and business requirements more tightly than is often the case in a data-centric IT system.

Where This Book Starts and Stops

The mark of a mature technical discipline is when discussion around operational details and nuances is balanced by discussion of management strategies and tactics: how to get the best results from the technology at the granular, device level, and how to coordinate and consolidate entire systems into an efficient whole. Evidence of a mature practice manifests when even the most complex technical and engineering subjects can be expressed in a meaningful way at any level of an organization so that risk impacts and mitigations can be clearly communicated at all levels.

Evidence of an immature discipline is readily apparent in inconsistent practices, dependence on "experts and qualitative measures" and a solid dose of faith in what the experts provide in order to gain a comfort factor of risk reduction to business operations.

The domain of ICS has been expanding rapidly with security solutions and solutions vendors relative to the evidence of threats specifically against process control assets. However, compared to the related field of IT security, there is still a relatively small amount of management-level guidance available for the operational managers developing business cases, risk managers performing assessments, or auditors seeking context against which to evaluate the adequacy and balance of controls and safeguards relative to risks. This book is intended in part to address the imbalance between technical details and information about ICS security and management-level guidance specific to process control security.

By management-level guidance we mean information that can be consumed by those trying to balance the business requirements of risk reduction, production, and operational budgets into an effective blended strategy: how much risk can you treat versus how much risk can you transfer versus risk you can accept. This balance between treatment, transfer, and acceptance is fundamental to overall

risk management and does not require deep technical knowledge. Technical knowledge and information is an important input to this process, and as such we refer the reader to the many technical publications related to ICS security—from vendor white papers to National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) standards.

This book is not about process control security architectures. Where it is useful to reference or provide security architectures we will do so, but we will reference prior work in this area such as that from NIST 800-53 revision 2, "Recommended Security Controls for Federal Information System," and 800-82, "Guide to Industrial Control System (ICS) Security," ISA-99 Industrial Automation and Control Systems Security Standard, and the UK National Security Advice Centre.[1]

This book is not an attempt to catalog known vulnerabilities or specific attacks and malware, such as Stuxnet, associated with process control systems. Such an attempt would be futile because such a list would be obsolete long before this book got off the editor's desk and into print. For information about some of the latest process control vulnerabilities, the reader is directed to sources such as the Computer Emergency Response Team[2] or the Process Control System Forum.[3] While these subjects are referenced, there are plenty of resources available that will discuss technical vulnerabilities. Rather, this text deals with the processes and disciplines required to proactively seek, understand, and address such vulnerabilities, and also with looking at the industrial processes in a new way: understanding how unintentional and intentional actions can result in systemic faults and failures that could impact safe and reliable operations in today's modern industrial processes. It is in these areas of failure analysis that we often find opportunities for failures on a day-to-day basis that go largely unnoticed. Until something anomalous occurs. Understanding these possible failure modes and process hazards is the first step in designing a more robust system that resists faults and helps ensure continued operation of mission-critical systems.

Our Audience

We intend to satisfy a wide range of readers in this book; this is where we become most ambitious.

For the IT or ICS security novice there will be plenty of useful background data about the world of ICS and, more importantly, context. Context about the various forms of process control, how they relate to each other, and how they relate to IT systems that might be covered by the same job description, if not residing on the same networks!

For the people dealing with ICS and security on a day-in day-out basis, this book will provide a broad framework for understanding and addressing both technical and business requirements. This book will provide some granular detail but is not intended as a how-to model for hardening process control systems in a step-by-step manner. It will, however, provide many useful insights and guidance on how to assess and manage threats and risks facing ICS, and how to communicate the business case rationale to obtain the resources to address these threats and risks. The material covered in this book is not specific to any particular industry or ICS; it has been specifically authored to help practitioners from any industrial sector, whether they are supporting a legacy system with proprietary protocols and networks migrating to IP, or the latest IPv6 technologies (see Chapter 5 for more on this topic specifically).

The rise of Ethernet usage on the shop floor and the continued need for information visibility throughout the entire enterprise drive ever-increasing convergence between the IT networks and ICS networks. For the experienced IT security guru, this book will provide a good introduction to "the other IT": industrial control systems, often known by related terms such as supervisory control and data acquisition (SCADA) and distributed control systems (DCS), to name a couple.

This soup of acronyms can create a confusing picture and barriers to understanding. ICS, SCADA, DCS, and so forth, are ubiquitous terms that must be understood by IT types. Each term has a different implication for technical architecture, usage, and potential threats, risks, and hazards.

Previously, these industrial environments were disconnected and "closed" due to communications incompatibility with Ethernet and other common local area network (LAN) protocols and the ICS protocols such as Modbus, Profibus, ControlNet, DeviceNet, and more. Today, these protocols are often entirely converged with IT systems on Ethernet and IP networks combining the infrastructures and allowing seamless integration across various layer 1 physical media types (copper, fiber, wireless) and communications protocols.

For auditors of IT systems, this book will be a source of baseline data about controls and safeguards that might be found in the ICS environments as they migrate from analogue to digital and especially IP-based networks.

Forensics practitioners and accident investigators may find utility in this book due to the observations and recommendations made related to safety systems versus ICS, and the manner in which threats and risks might be assessed and ultimately prioritized. We would not presume to indicate any fault or blame associated with threat and risk management methodologies different from those in this book; however, the information, methodologies, controls, and safeguards mentioned in this book should be at least partially represented in most comprehensive ICS security practices.

ICS engineers may find valuable information about how to relate IT security issues to a more familiar view of generally accepted ICS best practices and disciplines such as process safety, efficiency, quality management, and performance management. This book will also assist ICS engineers in the determination of process hazards, mitigation of safety risks, and implementation of engineered safeguards to avoid dangerous failures or impacts to production and supply chain operations.

In places like the United States, regulators and legislators have shown forbearance when it comes to setting standards for process controls, even around the most sensitive infrastructures. For instance, the Federal Energy Regulatory Commission (FERC)[4] allows the industry-lead North American Electricity Reliability Council (NERC)[5] to establish security standards for the industry, even though the standards were essentially first approved by FERC before being deemed mandatory for NERC members. NERC is actually a North American organization, including energy suppliers in Canada; so the U.S. FERC has pretty much legislated for other countries at the same time. Other jurisdictions like the European Union appear to be headed in a similar direction. At the time of the writing of this book, considerable additional regulatory and legislative efforts are moving forward, including recommended practices and requirements from the Nuclear Regulatory Commission[6] and the Chemical Facility Anti-Terrorism Standards defined in 6 CFR 27, Appendix A.[7] These and similar efforts continue to develop throughout the world's governments as the

need to protect critical infrastructure becomes increasingly clear. This book aspires to contribute to those discussions about ICS security.

What Is an Industrial Control System?

Process control system (PCS), distributed control system (DCS), and supervisory control and data acquisition (SCADA) are names frequently applied to the systems that control, monitor, and manage large production systems. The systems are often in critical infrastructures industries, such as electric power generators, transportation systems, dams, chemical facilities, petrochemical operations, pipelines, and others, giving the security of PCS, DCS, and SCADA systems evaluated importance in the increasingly networked world we live in.

SCADA especially is a term that has fairly recently been deprecated. In 2002 the International Society of Automation (ISA) started work on security standards for what it called industrial automation and control systems (IACS), under the aegis of its 99 standard.

IACS included SCADA services and reflected the wider and broader industrial infrastructures that were based on IP and interfaced with IT systems. IACS was further shortened in 2006 when the Department of Homeland Security (DHS) published *Mitigations for Vulnerabilities Found in Control System (CS) Networks.* Finally, in 2008, the National Institute of Standards and Technology applied the current compromise name, industry control systems (ICS), in its landmark publication of NIST 800-82: *Guide to Industrial Control System Security.*

In this chapter we will distinguish between PCS, DCS, and SCADA systems as a matter of formal detail, but for the most part we intend all three systems when using the term *industrial control systems* (ICS): as a preliminary summary, ICS gathers information from a variety of endpoint devices about the current status of a production process, which may be fully or partially automated. Historians, typical IT systems within process control environments, gather information concerning the production process. PCS, DCS, SCADA, and so forth, read values and interact based upon automated logic alarms and events requiring operators interaction, or report automated system state changes.

A process control system allows operators to make control decisions, which might then be relayed upstream, downstream, or to parallel processes for execution by the same system. These systems could be within the four walls of one building, or could be spread throughout a potentially massive geographical region (in the case for items such as pipelines, power distribution, water and wastewater management.) For example, an ICS might gather information from endpoint devices that allow operators to assess that a leak may have opened in a pipeline. The system aggregates this information at a central site, which (hopefully) contains intelligence and analytics alerting a control station and operators that the leak has occurred. Operators then carry out necessary analysis to determine if and how the leak may impact operations, safety, and regulations (environmental, health, and safety).

ICS displays the information gathered from endpoint devices in a logical and organized fashion, and keeps a history of the parameters received from the endpoint device. If the leak under investigation required that pressure in the pipeline be reduced or even that the pipeline be shut down, then these operational instructions may be issued from the control station through the ICS. Another possibility is that the ICS is intended for monitoring but not active intervention, in which case the operators would dispatch maintenance teams according to the coordinates provided by the process control system.

This example starts to reveal the fact that control systems can be relatively simple or incredibly complex. More often than not, the systems are more complex than is readily apparent on the surface, which in part distinguishes them from IT systems. For instance, where the traditional IT space deals with a fairly limited set of operating systems, communications protocols, and Open System Interconnection (OSI) model layer 1 (physical) and layer 2 (data link) device vendors (as illustrated in Figure 1.3), a typical process environment can represent hundreds of devices from different vendors with different specifications, protocols, and physical deployment requirements.

Systems may be solely intended for the purpose of collecting, displaying, and archiving information from endpoint devices. For instance, urban traffic flow information from various intersections around a large city is used for both day-to-day governance and long-term urban planning. Alternately, ICS in a nuclear power plant or a municipal water system may have the ability to apply either automatic,