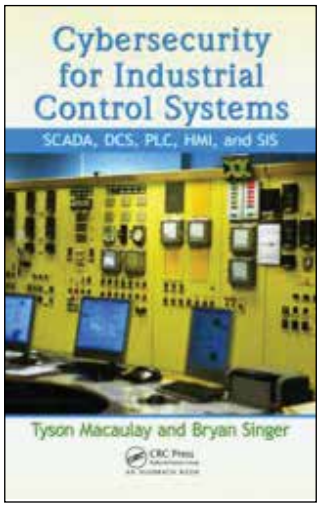
Reviewed by A. Krista Kivisild, CISA, CA, who has had a diverse career in audit, working in government, private companies and public organizations. Kivisild has experience in IT audit, governance, compliance/regulatory auditing, value for money auditing and operational auditing. She has served as a volunteer instructor, training not-for-profit boards on board governance concepts, with the Alberta (Canada) Government Board Development Program and has served as the membership director and CISA director for the ISACA Winnipeg (Manitoba, Canada) Chapter.

Cybersecurity for Industrial Control Systems

In June 2010, a computer worm known as Stuxnet, designed to attack industrial programmable logic controllers (PLCs) in target areas, such as nuclear power plants in Iran,[1] was discovered. While certainly not the first (nor the last) piece of malware targeting industrial control systems (ICSs), it helped bring this type of industrial espionage into the limelight, as it appeared to involve matters of national security, bringing the activity of planting a virus from the fictional world of James Bond to the real world of national secret service agencies. Suddenly, mundane control systems became provocative.



By Tyson Macaulay and Bryan Singer

ICSs have been around for decades with the job of controlling, monitoring and managing large production systems, often in critical infrastructure industries, such as electric power generators, transportation systems, dams, chemical facilities, petrochemical operations and pipelines. ICSs include process control systems (PCSs), distributed control systems (DCSs), and supervisory control and data acquisition (SCADA). While not traditionally lively, the field of ICS has been rapidly expanding with security solutions in response to the increasing threats. Despite this expansion, there is still a small amount of management-level guidance to develop business cases for risk managers to use to perform assessments. There is also a lack of guidance for use by auditors to evaluate the adequacy and balance of controls relative to risk.[2] In short, the purpose of the book *Cybersecurity for Industrial Control Systems* by Tyson Macaulay and Bryan Singer is to address the imbalance between the available technical information on ICS security and related management-level guidance.

The authors do a good job of providing a thorough introduction into ICSs, explaining all of the technical details and information so that even novice information systems (IS) security professionals or auditors can get their bearings and begin to have a solid understanding of the business and the environment in which ICS operates. While ICS and related subjects can be technical, this book presents them with enough detail and in a straightforward enough manner so that the information is clear. From here, the authors provide ample information to ensure that even an experienced security professional is fully briefed on the threats, vulnerabilities, risk assessment techniques and what is coming next in the field. From this vantage point, the book serves as a good reference book to gain a valuable breadth of knowledge of areas falling within the field of ICS.

The book is well documented throughout and includes references to various regulations governing the field of ICS, including those from the US National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and the UK National Security Advice Centre. It also discusses the impact of various regulatory commissions across different countries, as these bodies set standards for process controls, establish security standards for industry and, thus, have an impact on ICS security. The book also compares ICS security to regular IT security and highlights any differences and similarities.

Although the book is well documented and provides great detail, there is some truth in the saying that it is not possible to be all things to all people. The authors identify their target audience as IT or ICS security novices, IT or ICS security practitioners, experienced IT security gurus, auditors of IT systems, forensic practitioners, accident investigators, and ICS engineers. This target audience contains quite a wide range of readers with differing needs. While there is sufficient detail from a security, audit or investigative point of view, those who are engineers or are involved with forensics may require more

detailed information than this book provides. For most users, the detailed explanations, supporting figures and tables, and detailed references at the end of each chapter provide the answers to their questions.

ICSs are not new, but more and more they are being exposed to new threats as they become Internet-facing and their critical services are exposed to attack. *Cybersecurity for Industrial Control Systems* provides readers with a solid foundation to understand what the different control systems are, what the threats and vulnerabilities are, what the current and new risk assessment techniques are in the field of ICS risk management, and where ICS security is headed in the future.

EDITOR'S NOTE

Cybersecurity for Industrial Control Systems is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

ENDNOTE

[1] Gross, Michael Joseph; "A Declaration of Cyber-War," *Vanity Fair*, April 2011, *www.vanityfair.com/culture/features/2011/04/stuxnet-201104*

[2] Macaulay, Tyson; Bryan Singer; *Cybersecurity for Industrial Control Systems SCADA, DCS, PLC, HMI, and SIS*, CRC Press, USA, 2012