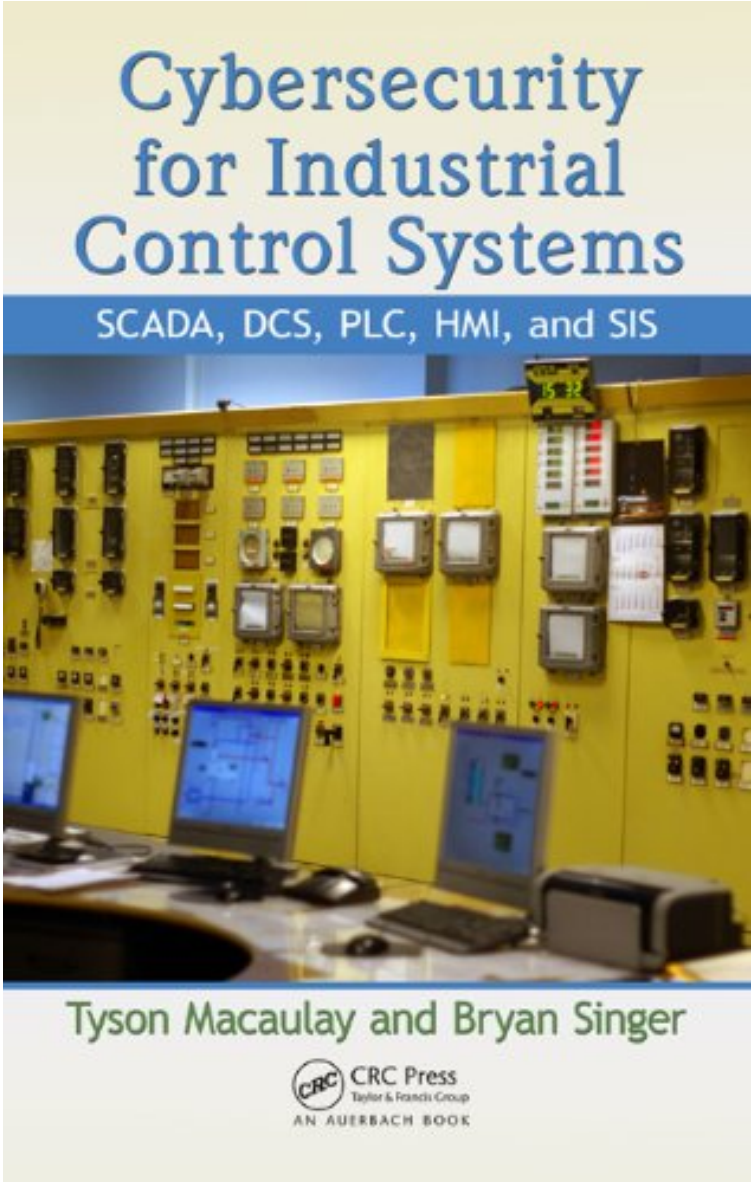
Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS

Tyson Macaulay, Bryan L. Singer



#1316663 in eBooks 2012-01-24 2012-01-24File Name: B0071ART60 | File size: 53.Mb

Tyson Macaulay, Bryan L. Singer : Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS before purchasing it in order to gage whether or not it would be worth my time, and all praised Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS:

9 of 9 people found the following review helpful. Best ICS Security Book To Date By FarBy Dale PetersonI had high

hopes for this book since Bryan Singer is very experienced in ICS, ICS security and IT security --- and Bryan and co-author Tyson McCauley did not disappoint. To date this is clearly the best book on ICS Security by far. (Note - Langner's book Robust Control System Networks: How to Achieve Reliable Control After Stuxnet is a 5-star, must read, but it intentionally talks engineering not security)The two best things about this book are:1. They got the facts right about both ICS and IT security. This is not as easy as it sounds as most books have failed or been simplistic in one area or another.2. They provided the background information for a beginner to understand, but followed that up with significant technical detail and examples. It's a good book for a beginner or intermediate in either area, and even those with years of experience in both areas will learn something. For me the best new info was the Overall Equipment Effectiveness (OEE) and Security OEE as a future risk assessment technique in Chapter 4.Chapter 1 provides a good background on ICS for the IT security audience. Again, sounds straightforward, but a lot of the ICS security books today read like the authors have not spent much hands on time with a SCADA or DCS. Excellent material for the IT security professional or anyone else new to ICS. They started to lose me on the Taxonomy of Convergence in that chapter, but I'm interested to hear what others thought of that sub-section.Chapter 2 covers threats to ICS, and there is great information here such as:- "given today's network threat environment, ICS security impacts are first and foremost likely to occur as a result of unintended effects of outsider attacks"- "ICS is most likely to suffer as a matter of the lucky hit or collateral damage, as opposed to direct attack"- "indirect threat of impacts associated with the probing, scanning and attacking inadvertently impacts the fragile ICS devices"- "Differentiating between phishers, spammers, foreign intelligence, and organized crime is not very productive if they are all using the same attack vectors"I could go on and on as I highlighted sentences throughout the chapter and was muttering yes as I read.Chapter 3: ICS Vulnerabilities introduces the readers to classes of ICS impacts such as Loss of Control and Denial of View. This has been talked about at S4 and other conferences by Zach Tudor, Bryan and others, but it has not yet been adopted by those entering the ICS security world. Chapter 3 will likely be the most beneficial to the largest number of readers.Chapter 4 covers ICS Risk Assessment Techniques. Those new to ICS security will benefit from the first half of the chapter covering the most popular current techniques. The old hands are likely to learn more in the second half of the chapter where the authors cover possible future techniques.Chapter 5: What Is Next In ICS Security focuses primarily on IPv6. It's material readers won't find elsewhere, but it seems a bit out of the flow of the book. My guess is IPv6 is something one or both of the authors feel passionate about and wanted to add it in. There's nothing wrong with a bit of a self-reward as writing a book is a very difficult.So why not a 5-star review? McCauley and Singer actually predict the reason in Chapter 1. They write "We intend to satisfy a wide range of readers in this book; this is where we become most ambitious". They are writing for the IT security professional who doesn't know ICS and for the ICS engineer who doesn't know security. Inevitably there are chunks of information that are simplistic for either audience, and this comes at the expense of an even more in depth discussion. It's an understandable decision to take this approach since it increases the potential readership size.This is clearly the book to get or give if you want to read about ICS security today.2 of 2 people found the following review helpful. Pretty darn comprehensive for a BeginnerBy Steven D. AlexanderFirst of all, this is not an technical "how to" manual. It is an overview of the emerging world of cybersecurity. This industry is still in its preteen stage. This book looks at and explains different approaches to securing Process Control Networks and gives you information about who is leading this and what it available. It is a very good reference book and can guide you to making the right decisions based on your individual needs. But be warned, the concepts and explanations therein are pretty "technical" and the author does not go get into much definition. Which is not the purpose of this book. It is definitely written for those already mature in this field. Which I am not but it broadens my understanding helps me to "catch up".3 of 3 people found the following review helpful. Cybersecurity for ICSBy MoonDoggyThis book has been an excellent read. It has an abundance of engineering detail and builds on the NIST 800-82 and NERC guidelines. I have recommended this book to my fellow security engineers and have shared it with folks at CSSP INL.

As industrial control systems (ICS), including SCADA, DCS, and other process control networks, become Internet-facing, they expose crucial services to attack. Threats like Duqu, a sophisticated worm found in the wild that appeared to share portions of its code with the Stuxnet worm, emerge with increasing frequency. Explaining how to develop and implement an effective cybersecurity program for ICS, Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS provides you with the tools to ensure network security without sacrificing the efficiency and functionality of ICS.Highlighting the key issues that need to be addressed, the book begins with a thorough introduction to ICS. It discusses business, cost, competitive, and regulatory drivers and the conflicting priorities of convergence. Next, it explains why security requirements differ from IT to ICS. It differentiates when standard IT security solutions can be used and where SCADA-specific practices are required.The book examines the plethora of potential threats to ICS, including hi-jacking malware, botnets, spam engines, and porn dialers. It outlines the range of vulnerabilities inherent in the ICS quest for efficiency and functionality that necessitates risk behavior such as remote access and control of critical equipment. Reviewing risk assessment techniques and the evolving risk assessment process, the text concludes by examining what is on the horizon for ICS security, including IPv6, ICSv6 test lab

designs, and IPv6 and ICS sensors.

I had high hopes for this book since Bryan Singer is very experienced in ICS, ICS security, and IT security ? and Bryan and co-author Tyson McCauley did not disappoint. To date this is clearly the best book on ICS Security by far. The two best things about this book are: 1) They got the facts right about both ICS and IT security. This is not as easy as it sounds as most books have failed or been simplistic in one area or another. 2) They provided the background information for a beginner to understand, but followed that up with significant technical detail and examples. Itrsquo;s a good book for a beginner or intermediate in either area, and even those with years of experience in both areas will learn something. For me the best new info was the Overall Equipment Effectiveness (OEE) and Security OEE as a future risk assessment technique in Chapter 4. hellip; I could go on and on as I highlighted sentences throughout the chapter and was muttering yes as I read. hellip; This is clearly the book to get or give if you want to read about ICS security today.?Dale G Peterson, writing on www.digitalbond.com(For the full review, visit: http://www.digitalbond.com/2012/03/27/4-star-review-for-mccauleysinger-book-cybersecurity-for-ics/#more-11213) I had high hopes for this book since Bryan Singer is very experienced in ICS, ICS security, and IT security -- and Bryan and co-author Tyson McCauley did not disappoint. To date this is clearly the best book on ICS Security by far. The two best things about this book are: 1) They got the facts right about both ICS and IT security. This is not as easy as it sounds as most books have failed or been simplistic in one area or another. 2) They provided the background information for a beginner to understand, but followed that up with significant technical detail and examples. It's a good book for a beginner or intermediate in either area, and even those with years of experience in both areas will learn something. For me the best new info was the Overall Equipment Effectiveness (OEE) and Security OEE as a future risk assessment technique in Chapter 4. ! I could go on and on as I highlighted sentences throughout the chapter and was muttering yes as I read. ! This is clearly the book to get or give if you want to read about ICS security today. -- Dale G Peterson, writing on www.digitalbond.com (For the full review, visit: http://www.digitalbond.com/2012/03/27/4-star-review-for-mccauleysinger-book-cybersecurity-for-ics/#more-11213)About the AuthorTyson Macaulay is the security liaison officer (SLO) for Bell Canada. In this role, he is responsible for technical and operational risk management solutions for Bellrsquo;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 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 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; 2001ndash;2005), and founded General Network Services (GNS; 1996ndash;2001). Macaulay 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 Securityrsquo;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.