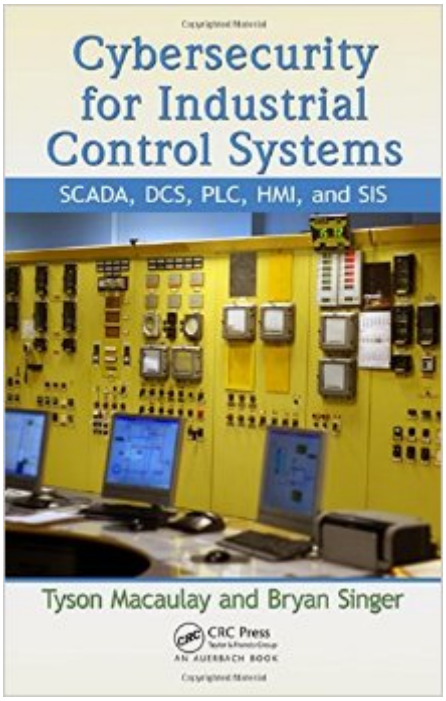
Cybersecurity For Industrial Control Systems: SCADA, DCS, PLC, HMI, And SIS



Synopsis

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.

Book Information

Hardcover: 203 pages

Publisher: Auerbach Publications; 1 edition (December 13, 2011)

Language: English

ISBN-10: 1439801967

ISBN-13: 978-1439801963

Product Dimensions: 9.3 x 6.4 x 0.7 inches

Shipping Weight: 1.1 pounds (View shipping rates and policies)

Average Customer Review: 4.4 out of 5 starsÂ Â See all reviewsÂ (8 customer reviews)

Best Sellers Rank: #601,878 in Books (See Top 100 in Books) #29 inÂ Books > Computers & Technology > Digital Audio, Video & Photography > Speech & Audio Processing #31 inÂ Books > Computers & Technology > Hardware & DIY > Microprocessors & System Design > Control Systems #142 inÂ Books > Computers & Technology > Certification > CompTIA

Customer Reviews

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. (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.

Dmca