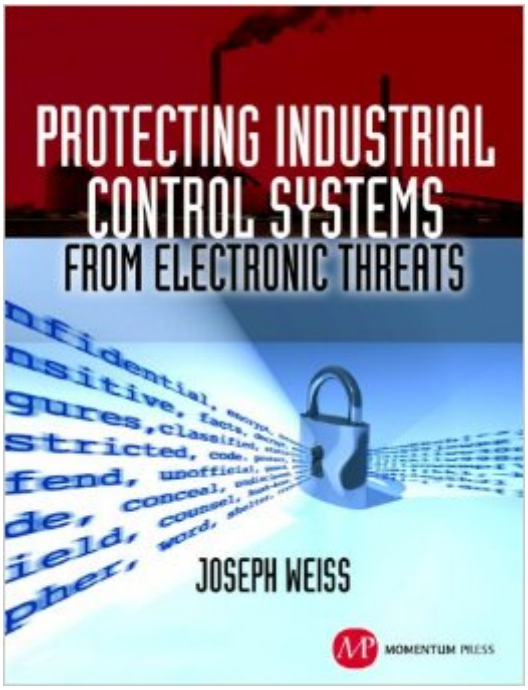
Protecting Industrial Control Systems From Electronic Threats



Synopsis

Aimed at both the novice and expert in IT security and industrial control systems (ICS), this book will help readers gain a better understanding of protecting ICSs from electronic threats. Cyber security is getting much more attention and 'SCADA security' (Supervisory Control and Data Acquisition) is a particularly important part of this field, as are Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs)-and all the other, field controllers, sensors, and drives, emission controls, and that make up the 'intelligence' of modern industrial buildings and facilities. This book will help the reader better understand what is industrial control system cyber security, why is it different than IT security, what has really happened to date, and what needs to be done. Loads of practical advice is offered on everything from clarity on current cyber-security systems and how they can be integrated into general IT systems, to how to conduct risk assessments and how to obtain certifications, to future trends in legislative and regulatory issues affecting industrial security.

Book Information

Hardcover: 310 pages

Publisher: Momentum Press (May 15, 2010)

Language: English

ISBN-10: 1606501976

ISBN-13: 978-1606501979

Product Dimensions: 9.3 x 7.3 x 0.9 inches

Shipping Weight: 1.7 pounds (View shipping rates and policies)

Average Customer Review: 4.2 out of 5 starsÂ Â See all reviewsÂ (8 customer reviews)

Best Sellers Rank: #400,095 in Books (See Top 100 in Books) #19 inÂ Books > Computers & Technology > Hardware & DIY > Microprocessors & System Design > Control Systems #97 inÂ Books > Engineering & Transportation > Engineering > Industrial, Manufacturing & Operational Systems > Industrial Technology #223 inÂ Books > Engineering & Transportation > Engineering > Industrial, Manufacturing & Operational Systems > Manufacturing

Customer Reviews

I approached this review as someone very familiar with many aspects of energy regulation and having broad knowledge of IT security having recently passed my CISSP exam. I am not an Industrial Control Engineer, but am very concerned about cyber threats to our energy, water, chemcial and transportation infrastructure. That is where this book comes in handy. I rated this book

4 stars, because it provides a good grounding of the technical and policy issues and obstacles that have to be addressed to protect infrastructure. Note, this review is my personal opinion and does not reflect the views or opinions of my employer.The 166 pages of this text really amount to a crash course on industrial control systems and document why many typical IT security measures may fail to prevent cyber attacks. In fact the author goes to great lengths to explain how such out of the box security fixes may do more harm than good and bring the underlying hardware and software to a screeching halt. The real impacts of that happening could translate to blackouts and brownouts, pipeline explosions and a host of other inconveniences depending on the kind of system one is dealing with.Joe Weiss leads the reader slowly through the technical issues of industrial control systems and provides numerous examples of how cyber threats have plagued various industries. These summaries are detailed and valuable. I found myself thinking about what administrative and logical controls to apply.This book is ideal for any IT Security professional or regulators who have to grapple with protecting electric, natural gas, oil, water, chemical and transportation infrastructure from cyber attacks. Some of the materials are very technical and policy makers and regulators may find these distracting.

Industrial control systems (ICS) execute large-scale manufacturing and commodity product delivery processes. They run electronic power grids, nuclear power plants, water and sewage treatment plants, transportation signaling, and numerous other recognizably critical infrastructures. Joe Weiss walks the layman effortlessly through the world of ICS cyber-components: distributed control systems, programmable logic controllers, intelligent electronic devices, remote terminal units, and supervisory control and data acquisition (DCS, PLC, IED, RTU, and SCADA). Along the way, he points out the cybersecurity vulnerabilities inherent in the design and operation of these systems. With examples that can be directly traced to headline news, he describes how easy it is to disrupt these systems with simple cybersecurity hacks.Though it may seem odd to the reader that such obviously critical systems are so easily disrupted, the way that Weiss explains the evolution of ICS and the myths that surround attempts at ICS technical security evaluation, his story line makes sense. For example, a typical software program lives 3-5 years before a major architectural change. A typical industrial control system lives 15-20. That means that the technology components in an ICS are likely to be at least 10 years old, very outdated by technology standards, and correspondingly vulnerable to today’s sophisticated cyber-attacks. In addition, cybersecurity threats to ICS are not the same as cybersecurity threats to mainstream information technology. An ICS is typically much more sensitive to very small changes in electronic components. Hence, technology

controls that are often proscribed for mainstream information assurance, like scanning and patching, can actually harm these systems more than they help them.

I had the honor of speaking with Joe Weiss yesterday in connection with a project on which I'm working. I had, coincidentally, just come across his book (Protecting ICSs) earlier in the day after searching for top-rated books on the subject, and it took only a few minutes listening to him for me to order the book and have it shipped overnight.When I mentioned his reviews, he sounded genuinely surprised, and clearly hadn't checked his book on . When I told him that there were six very good reviews and one poor review, he guessed immediately who wrote the poor one; I didn't ask, but there is clearly some sort of personal matter between Joe and Dale that might have clouded Dale's judgment.Now that I've read a substantial portion of the book, I can confirm that Dale has some sort of personal axe to grind with Joe, and his criticisms are more indicative of his own bias than the quality of the work. I want to get on to my own assessment, but a couple of examples should convince a rational reader of Dale's inaccuracy.First, his comment about the book needing "a quality editor" is simply BS: I've read hundreds of technical works on a wide range of topics, and this one is as clearly and logically written as any of them -- and the writing is much better, from the point of view of diction, usage, grammar, and other technical aspects of writing, than most. I'm a writer and a publisher, and I know whereof I speak.Second, he quotes a paragraph from Chapter 1 in which Joe says that 9/11 "shifted the onus [of cyber security for ICS] from the end user to the government," and complains that he "wanted to understand why [Joe] thinks this was unfortunate" -- clearly implying that Joe failed to make it clear.

Malware and Threats in Windows, Linux, and Mac Memory Threats of the Galaxy (Star Wars Roleplaying Game) Magickal Protection: Defend Against Curses, Gossip, Bullies, Thieves, Demonic Forces, Violence, Threats and Psychic Attack Saving the World from Asteroids and Planning for Coronal Mass Ejection threats.: What isn't being done to protect us from impacts and the power grids from ... (Collected Works: John A. McCormick Book 3) Power Electronic Converters Modeling and Control: with Case Studies (Advanced Textbooks in Control and Signal Processing) Cyber-security of SCADA and Other Industrial Control Systems (Advances in Information Security) Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions Industrial Automated Systems: Instrumentation and Motion Control Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS Hacking SCADA/Industrial Control Systems: The Pentest Guide Tuning of Industrial Control Systems