Cybersecurity For Industrial Control Systems Scada Dcs Plc Hmi And Sis Author Tyson Macaulay Jan 2012

When somebody should go to the books stores, search introduction by shop, shelf by shelf, it is in point of fact problematic. This is why we allow the book compilations in this website. It will completely ease you to look guide **cybersecurity for industrial control systems scada dcs plc hmi and sis author tyson macaulay jan 2012** as you such as.

By searching the title, publisher, or authors of guide you in point of fact want, you can discover them rapidly. In the house, workplace, or perhaps in your method can be every best area within net connections. If you point to download and install the cybersecurity for industrial control systems scada dcs plc hmi and sis author tyson macaulay jan 2012, it is definitely easy then, in the past currently we extend the connect to purchase and create bargains to download and install cybersecurity for industrial control systems scada dcs plc hmi and sis author tyson macaulay jan 2012 so simple!

Practical SCADA for Industry - David Bailey 2003-06-23
A SCADA system gathers information, such as where a leak on a pipeline has occurred, transfers the information back to a central site, alerting the home station that the leak has occurred, carrying out necessary analysis and control, such as determining if the leak is critical, and displaying the information in a logical and organized fashion. SCADA systems can be relatively simple, such as one that monitors environmental conditions of a small office building, or incredibly complex, such as a system that monitors all the activity in a nuclear power plant or the activity of a municipal water system. An engineer's introduction to Supervisory Control and Data Acquisition (SCADA) systems and their application in monitoring and controlling equipment and industrial plant Essential reading for data acquisition and control professionals in plant engineering, manufacturing, telecommunications, water and waste control, energy, oil and gas refining and transportation Provides the knowledge to analyse, specify and debug SCADA systems, covering the fundamentals of hardware, software and the communications systems that connect SCADA operator stations
Cybersecurity of Industrial Systems - Jean-Marie Flaus 2019-07-30
How to manage the cybersecurity of industrial systems is a crucial question. To implement relevant solutions, the industrial manager must have a clear understanding of IT systems, of communication networks and of control-command systems. They must also have some knowledge of the methods used by attackers, of the standards and regulations involved and of the available security solutions. Cybersecurity of Industrial Systems presents these different subjects in order to give an in-depth overview and to help the reader manage the cybersecurity of their installation. The book addresses these issues for both classic SCADA architecture systems and Industrial Internet of Things (IIoT) systems.
Handbook of Big Data Privacy - Kim-Kwang Raymond Choo 2020-03-18
This handbook provides comprehensive knowledge and includes an overview of the current state-of-the-art of Big Data Privacy, with chapters written by international world leaders from academia and industry working in this field. The first part of this book offers a review of security challenges in critical infrastructure and offers methods that utilize acritical intelligence (AI) techniques to overcome those issues. It then focuses on big data security and privacy issues in relation to developments in the Industry 4.0. Internet of Things (IoT) devices are becoming a major source of security and privacy concern in big data platforms. Multiple solutions that leverage machine learning for addressing security and privacy issues in IoT environments are also discussed this handbook. The second part of this handbook is focused on privacy and security issues in different layers of big data systems. It discusses about methods for evaluating security and privacy of big data systems on network, application and physical layers. This handbook elaborates on existing methods to use data analytic and AI techniques at different layers of big data platforms to identify privacy and security attacks. The final part of this handbook is focused on analyzing cyber threats applicable to the big data environments. It offers an in-depth review of attacks applicable to big data platforms in smart grids, smart farming, FinTech, and health sectors. Multiple solutions are presented to detect, prevent and analyze cyber-attacks and assess the impact of malicious payloads to those environments. This handbook provides information for security and privacy experts in most areas of big data including; FinTech, Industry 4.0, Internet of Things, Smart Grids, Smart Farming and more. Experts working in big data, privacy, security, forensics, malware analysis, machine learning and data analysts will find this handbook useful as a reference. Researchers and advanced-level computer science students focused on computer systems, Internet of Things, Smart Grid, Smart Farming, Industry 4.0 and network analysts will also find this handbook useful as a reference.
Critical Infrastructure Risk Assessment - Ernie Hayden, MIPM, CISSP, CEH, GICSP(Gold), PSP 2020-08-25
As a manager or engineer have you ever been assigned a task to perform a risk assessment of one of your facilities or plant systems? What if you are an insurance inspector or corporate auditor? Do you know how to prepare yourself for the inspection, decided what to look for, and how to write your report? This is a handbook for junior and senior personnel alike on what constitutes critical infrastructure and risk and offers guides to the risk assessor on preparation, performance, and documentation of a risk assessment of a complex facility. This is a definite “must read” for consultants, plant managers, corporate risk managers, junior and senior engineers, and university students before they jump into their first technical assignment.
Industrial Cybersecurity - Pascal Ackerman 2017-10-18
Your one-step guide to understanding industrial cyber security, its control systems, and its operations. About This Book Learn about endpoint protection such as anti-malware implementation, updating, monitoring, and sanitizing user workloads and mobile devices Filled with practical examples to help you secure critical infrastructure systems efficiently A step-by-step guide that will teach you the techniques and methodologies of building robust infrastructure systems Who This Book Is For If you are a security professional and want to ensure a robust environment for critical infrastructure systems, this book is for you. IT professionals interested in getting into the cyber security domain or who are looking at gaining industrial cyber security certifications will also find this book useful. What You Will Learn Understand industrial cybersecurity, its control systems and operations Design security-oriented architectures, network segmentation, and security support services Configure event monitoring systems, anti-malware applications, and endpoint security Gain knowledge of ICS risks, threat detection, and access management Learn about patch management and life cycle management Secure your industrial control systems from design through retirement In Detail With industries expanding, cyber attacks have increased significantly. Understanding your control system's vulnerabilities and learning techniques to defend critical infrastructure systems from cyber threats is increasingly important. With the help of real-world use cases, this book will teach you the methodologies and security measures necessary to protect critical infrastructure systems and will get you up to speed with identifying unique challenges.Industrial cybersecurity begins by introducing Industrial Control System (ICS) technology, including ICS architectures, communication media, and protocols. This is followed by a presentation on ICS (in) security. After presenting an ICS-related attack scenario, securing of the ICS is discussed, including topics such as network segmentation, defense-in-depth strategies, and protective solutions. Along with practical examples for protecting industrial control systems, this book details security assessments, risk management, and security program development. It also covers essential cybersecurity aspects, such as threat detection and access management. Topics related to endpoint hardening such as monitoring, updating, and anti-malware implementations are also discussed. Style and approach A step-by-step guide to implement Industrial Cyber Security effectively.
Information and Communication Technology for Intelligent Systems - Tomonobu Senjyu 2020-10-29
This book gathers papers addressing state-of-the-art research in all areas

of information and communication technologies and their applications in intelligent computing, cloud storage, data mining and software analysis. It presents the outcomes of the Fourth International Conference on Information and Communication Technology for Intelligent Systems, which was held in Ahmedabad, India. Divided into two volumes, the book discusses the fundamentals of various data analysis techniques and algorithms, making it a valuable resource for researchers and practitioners alike.

Critical Infrastructure - Tyson Macaulay 2016-04-19

Critical Infrastructure (CI) is fundamental to the functioning of a modern economy, and consequently, maintaining CI security is paramount. However, despite all the security technology available for threats and risks to CI, this crucial area often generates more fear than rational discussion. Apprehension unfortunately prompts many involved in CI policy to default to old-fashioned intuition rather than depend on modern concrete risk assessment as the basis for vital security decisions. Going beyond definitions, Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies looks at the iron triangle within CI: power, telecom, and finance. It introduces the concept of CI as an industrial and enterprise risk conductor, highlighting the reality that a CI failure can propagate a crisis with far-reaching repercussions. Focuses on Canada and the US Equally for a Useful Cross-Border Security Analysis With $2.5 trillion at stake in United States' CI alone, supreme standards and metrics are mandatory for solid protection of such a sophisticated and complex area. This powerful volume is dedicated to moving CI security into the 21st century, illustrating the danger in basing critical CI policy decisions on the existing legacy frames of reference. It represents one of the first complete departures from policy, planning, and response strategies based on intuition and anecdotal evidence.

Nist Sp 800-82 Rev 2 - Guide to Industrial Control Systems (Ics) Security - National Institute National Institute of Standards 2015-05-29

NIST SP 800-82 Rev 2 Printed in COLOR ePub version also available for use on Kindle, iPad, Android tablet, and iPhone. If you like this book, please leave positive review. This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. Why buy a book you can download for free? First you gotta find it and make sure it''s the latest version (not always easy). Then you gotta print it using a network printer you share with 100 other people - and its outta paper - and the toner is low (take out the toner cartridge, shake it, then put it back). If it''s just 10 pages, no problem, but if it''s a 250-page book, you will need to punch 3 holes in all those pages and put it in a 3-ring binder. Takes at least an hour. An engineer that''s paid $75 an hour has to do this himself (who has assistant''s anymore?). If you are paid more than $10 an hour and use an ink jet printer, buying this book will save you money. It''s much more cost-effective to just order the latest version from Amazon.com This book is published by 4th Watch Books and includes copyright material. We publish compact, tightly-bound, full-size books (8 × by 11 inches), with glossy covers. 4th Watch Books is a Service Disabled Veteran-Owned Small Business (SDVOSB), and is not affiliated with the National Institute of Standards and Technology. For more titles published by 4th Watch Books, please visit: cybah.webplus.net A full copy of all the pertinent cybersecurity standards is available on DVD-ROM in the CyberSecurity Standards Library disc which is available at Amazon.com. NIST SP 500-299 NIST Cloud Computing Security Reference Architecture NIST SP 500-291 NIST Cloud Computing Standards Roadmap Version 2 NIST SP 500-293 US Government Cloud Computing Technology Roadmap Volume 1 & 2 NIST SP 500-293 US Government Cloud Computing Technology Roadmap Volume 3 DRAFT NIST SP 1800-8 Securing Wireless Infusion Pumps NISTIR 7497 Security Architecture Design Process for Health Information Exchanges (HIEs) NIST SP 800-66 Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule NIST SP 1800-1 Securing Electronic Health Records on Mobile Devices NIST SP 800-177 Trustworthy Email NIST SP 800-184 Guide for Cybersecurity Event Recovery NIST SP 800-190 Application Container Security Guide NIST SP 800-193 Platform Firmware Resiliency Guidelines NIST SP 1800-1 Securing Electronic Health Records on Mobile Devices NIST SP 1800-2 Identity and Access Management for Electric Utilities NIST SP 1800-5 IT Asset Management: Financial Services NIST SP 1800-6 Domain Name Systems-Based Electronic Mail Security NIST SP 1800-7 Situational Awareness for Electric Utilities NIST SP 500-288 Specification for WS-Biometric Devices (WS-BD) NIST SP 500-304 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information NIST SP 800-32 Public Key Technology and the Federal PKI Infrastructure NIST SP 800-63-3 Digital Identity Guidelines

Pentesting Industrial Control Systems - Paul Smith 2021-12-09

Learn how to defend your ICS in practice, from lab setup and intel gathering to working with SCADA Key FeaturesBecome well-versed with offensive ways of defending your industrial control systemsLearn about industrial network protocols, threat hunting, Active Directory compromises, SQL injection, and much moreBuild offensive and defensive skills to combat industrial cyber threatsBook Description The industrial cybersecurity domain has grown significantly in recent years. To completely secure critical infrastructure, red teams must be employed to continuously test and exploit the security integrity of a company's people, processes, and products. This is a unique pentesting book, which takes a different approach by helping you gain hands-on experience with equipment that you'll come across in the field. This will enable you to understand how industrial equipment interacts and operates within an operational environment. You'll start by getting to grips with the basics of industrial processes, and then see how to create and break the process, along with gathering open-source intel to create a threat landscape for your potential customer. As you advance, you'll find out how to install and utilize offensive techniques used by professional hackers. Throughout the book, you'll explore industrial equipment, port and service discovery, pivoting, and much more, before finally launching attacks against systems in an industrial network. By the end of this penetration testing book, you'll not only understand how to analyze and navigate the intricacies of an industrial control system (ICS), but you'll also have developed essential offensive and defensive skills to proactively protect industrial networks from modern cyberattacks. What you will learnSet up a starter-kit ICS lab with both physical and virtual equipmentPerform open source intel-gathering pre-engagement to help map your attack landscapeGet to grips with the Standard Operating Procedures (SOPs) for penetration testing on industrial equipmentUnderstand the principles of traffic spanning and the importance of listening to customer networksGain fundamental knowledge of ICS communicationConnect physical operational technology to engineering workstations and supervisory control and data acquisition (SCADA) softwareGet hands-on with directory scanning tools to map web-based SCADA solutionsWho this book is for If you are an ethical hacker, penetration tester, automation engineer, or IT security professional looking to maintain and secure industrial networks from adversaries, this book is for you. A basic understanding of cybersecurity and recent cyber events will help you get the most out of this book.

Protecting Industrial Control Systems from Electronic Threats - Joseph Weiss 2010

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.

Cybersecurity for Industrial Control Systems - Tyson Macaulay 2016

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 im.

Cyber Security - K S Manoj 2020-09-05

Written in an easy to understand style, this book provides a

comprehensive overview of the physical-cyber security of Industrial Control Systems benefitting the computer science and automation engineers, students and industrial cyber security agencies in obtaining essential understanding of the ICS cyber security from concepts to realization. The Book -> Covers ICS networks, including zone-based architecture and its deployment for product delivery and other Industrial services. -> Discusses SCADA networking with required cryptography and secure industrial communications. -> Furnishes information about industrial cyber security standards presently used. -> Explores defence-in-depth strategy of ICS from conceptualisation to materialisation. -> Provides many real-world documented examples of attacks against industrial control systems and mitigation techniques. -> Is a suitable material for Computer Science and Automation engineering students to learn the fundamentals of industrial cyber security.

Cybersecurity for Industrial Control Systems - Tyson Macaulay 2012-02-02

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.

Critical Information Infrastructures Security - Grigore Havarneanu 2017-11-21

This book constitutes the post-conference proceedings of the 11th International Conference on Critical Information Infrastructures Security, CRITIS 2016, held in Paris, France, in October 2016. The 22 full papers and 8 short papers presented were carefully reviewed and selected from 58 submissions. They present the most recent innovations, trends, results, experiences and concerns in selected perspectives of critical information infrastructure protection covering the range from small-scale cyber-physical systems security via information infrastructures and their interaction with national and international infrastructures.

Robust Control System Networks - Ralph Langner 2011-09-15

From the researcher who was one of the first to identify and analyze the infamous industrial control system malware "Stuxnet," comes a book that takes a new, radical approach to making Industrial control systems safe from such cyber attacks: design the controls systems themselves to be "robust." Other security experts advocate risk management, implementing more firewalls and carefully managing passwords and access. Not so this book: those measures, while necessary, can still be circumvented. Instead, this book shows in clear, concise detail how a system that has been set up with an eye toward quality design in the first place is much more likely to remain secure and less vulnerable to hacking, sabotage or malicious control. It blends several well-established concepts and methods from control theory, systems theory, cybernetics and quality engineering to create the ideal protected system. The book's maxim is taken from the famous quality engineer William Edwards Deming, "If I had to reduce my message to management to just a few words, I'd say it all has to do with reducing variation." Highlights include: - An overview of the problem of "cyber fragility" in industrial control systems - How to make an industrial control system "robust," including principal design objectives and overall strategic planning - Why using the methods of quality engineering like the Taguchi method, SOP and UML will help to design more "armored" industrial control systems.

Proceedings of the 12th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2020) - Ajith Abraham 2021-04-15

This book highlights the recent research on soft computing and pattern recognition and their various practical applications. It presents 62 selected papers from the 12th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2020) and 35 papers from the 16th International Conference on Information Assurance and Security (IAS 2020), which was held online, from December 15 to 18, 2020. A premier conference in the field of artificial intelligence, SoCPaR-IAS 2020 brought together researchers, engineers and practitioners whose work involves intelligent systems, network security and their applications in industry. Including contributions by authors from 40 countries, the book offers a valuable reference guide for all researchers, students and practitioners in the fields of Computer Science and Engineering.

Information Security Management Handbook, Sixth Edition - Richard O'Hanley 2013-08-29

Updated annually, the Information Security Management Handbook, Sixth Edition, Volume 7 is the most comprehensive and up-to-date reference available on information security and assurance. Bringing together the knowledge, skills, techniques, and tools required of IT security professionals, it facilitates the up-to-date understanding required to stay one step ahead of evolving threats, standards, and regulations. Reporting on the latest developments in information security and recent changes to the (ISC)2® CISSP Common Body of Knowledge (CBK®), this volume features 27 new chapters on topics such as BYOD, IT consumerization, smart grids, security, and privacy. Covers the fundamental knowledge, skills, techniques, and tools required by IT security professionals Updates its bestselling predecessors with new developments in information security and the (ISC)2® CISSP® CBK® Provides valuable insights from leaders in the field on the theory and practice of computer security technology Facilitates the comprehensive and up-to-date understanding you need to stay fully informed The ubiquitous nature of computers and networks will always provide the opportunity and means to do harm. This edition updates its popular predecessors with the information you need to address the vulnerabilities created by recent innovations such as cloud computing, mobile banking, digital wallets, and near-field communications. This handbook is also available on CD.

Digital Transformation in Semiconductor Manufacturing - Sophia Keil 2020-01-01

This open access book reports on cutting-edge electrical engineering and microelectronics solutions to foster and support digitalization in the semiconductor industry. Based on the outcomes of the European project iDev40, which were presented at the two first conference editions of the European Advances in Digital Transformation Conference (EADCT 2018 and EADTC 2019), the book covers different, multidisciplinary aspects related to digital transformation, including technological and industrial developments, as well as human factors research and applications. Topics include modeling and simulation methods in semiconductor operations, supply chain management issues, employee training methods and workplaces optimization, as well as smart software and hardware solutions for semiconductor manufacturing. By highlighting industrially relevant developments and discussing open issues related to digital transformation, the book offers a timely, practice-oriented guide to graduate students, researchers and professionals interested in the digital transformation of manufacturing domains and work environments.

Industrial Cybersecurity - Pascal Ackerman 2021-10-07

Get up and running with industrial cybersecurity monitoring with this hands-on book, and explore ICS cybersecurity monitoring tasks, activities, tools, and best practices Key FeaturesArchitect, design, and build ICS networks with security in mindPerform a variety of security assessments, checks, and verificationsEnsure that your security processes are effective, complete, and relevantBook Description With Industrial Control Systems (ICS) expanding into traditional IT space and even into the cloud, the attack surface of ICS environments has increased significantly, making it crucial to recognize your ICS vulnerabilities and implement advanced techniques for monitoring and defending against rapidly evolving cyber threats to critical infrastructure. This second edition covers the updated Industrial Demilitarized Zone (IDMZ) architecture and shows you how to implement, verify, and monitor a holistic security program for your ICS environment. You'll begin by learning how to design security-oriented architecture that allows you to implement the tools, techniques, and activities covered in this book effectively and easily. You'll get to grips with the monitoring, tracking, and trending (visualizing) and procedures of ICS cybersecurity risks as well as understand the overall security program and posture/hygiene of the ICS environment. The book then

introduces you to threat hunting principles, tools, and techniques to help you identify malicious activity successfully. Finally, you'll work with incident response and incident recovery tools and techniques in an ICS environment. By the end of this book, you'll have gained a solid understanding of industrial cybersecurity monitoring, assessments, incident response activities, as well as threat hunting. What you will learnMonitor the ICS security posture actively as well as passivelyRespond to incidents in a controlled and standard wayUnderstand what incident response activities are required in your ICS environmentPerform threat-hunting exercises using the Elasticsearch, Logstash, and Kibana (ELK) stackAssess the overall effectiveness of your ICS cybersecurity programDiscover tools, techniques, methodologies, and activities to perform risk assessments for your ICS environmentWho this book is for If you are an ICS security professional or anyone curious about ICS cybersecurity for extending, improving, monitoring, and validating your ICS cybersecurity posture, then this book is for you. IT/OT professionals interested in entering the ICS cybersecurity monitoring domain or searching for additional learning material for different industry-leading cybersecurity certifications will also find this book useful.

Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology - Nicholas Michael Sambaluk 2019-08-08

This reference work examines how sophisticated cyber-attacks and innovative use of social media have changed conflict in the digital realm, while new military technologies such as drones and robotic weaponry continue to have an impact on modern warfare. • Provides fascinating information about cyber weapons that effectively strike through cyberspace to weaken and even cripple its target • Demonstrates how social media is employed in conflicts in innovative ways, including communication, propaganda, and psychological warfare • Explores potential technology avenues related to ensuring the continued military advantages of the United States • Identifies and describes nuclear, precision, and other technological capabilities that have historically been the preserve of superpowers but have been newly acquired by various states

Critical Infrastructure Protection - Javier Lopez 2012-03-30

The present volume aims to provide an overview of the current understanding of the so-called Critical Infrastructure (CI), and particularly the Critical Information Infrastructure (CII), which not only forms one of the constituent sectors of the overall CI, but also is unique in providing an element of interconnection between sectors as well as often also intra-sectoral control mechanisms. The 14 papers of this book present a collection of pieces of scientific work in the areas of critical infrastructure protection. In combining elementary concepts and models with policy-related issues on one hand and placing an emphasis on the timely area of control systems, the book aims to highlight some of the key issues facing the research community.

Prevention of Accidents at Work - Ales Bernatik 2017-09-25

Prevention of Accidents at Work collects papers presented at the 9th International Conference on the Prevention of Accidents at Work (WOS 2017) held in Prague, Czech Republic, on October 3-6, 2017, organized by the VSB-Technical University of Ostrava. The conference on current issues within occupational safety is organized under the umbrella of Workingonsafety.net (WOS.net). WOS.net is an international network of decision-makers, researchers and professionals responsible for the prevention of accidents and trauma at work. The network aims to bring accident prevention experts together in order to facilitate the exchange of experience, new findings and best practices between different countries and sectors. WOS.net is supported by the European Agency for Safety and Health at Work (EU-OSHA). The overall theme is safety management complexity in a changing society, with the motto: Do we need a holistic approach? Underlying topics include: Foundations of safety science: theories, principles, methods and tools; Research to practice: achievements, lessons learned and challenges; Risk management and safety culture: case studies, best practices and further needs; Safety regulation: reasonable practicable approach; Education and training: prerequisite for safety; Complexity and safety: multidisciplinarity and inter-stakeholder views. Prevention of Accidents at Work should be valuable to researchers, policy makers, safety professionals, labor inspectors, labor administrators and other experts in the prevention of occupational accidents.

Software Engineering Perspectives and Application in Intelligent Systems - Radek Silhavy 2016-04-26

The volume Software Engineering Perspectives and Application in Intelligent Systems presents new approaches and methods to real-world problems, and in particular, exploratory research that describes novel approaches in the field of Software Engineering. Particular emphasis is laid on modern trends in selected fields of interest. New algorithms or methods in a variety of fields are also presented. The 5th Computer Science On-line Conference (CSOC 2016) is intended to provide an international forum for discussions on the latest research results in all areas related to Computer Science. The addressed topics are the theoretical aspects and applications of Computer Science, Artificial Intelligences, Cybernetics, Automation Control Theory and Software Engineering.

Security in Cyber-Physical Systems - Ali Ismail Awad 2021-03-05

This book is a relevant reference for any readers interested in the security aspects of Cyber-Physical Systems and particularly useful for those looking to keep informed on the latest advances in this dynamic area. Cyber-Physical Systems (CPSs) are characterized by the intrinsic combination of software and physical components. Inherent elements often include wired or wireless data communication, sensor devices, real-time operation and automated control of physical elements. Typical examples of associated application areas include industrial control systems, smart grids, autonomous vehicles and avionics, medial monitoring and robotics. The incarnation of the CPSs can therefore range from considering individual Internet-of-Things devices through to large-scale infrastructures. Presented across ten chapters authored by international researchers in the field from both academia and industry, this book offers a series of high-quality contributions that collectively address and analyze the state of the art in the security of Cyber-Physical Systems and related technologies. The chapters themselves include an effective mix of theory and applied content, supporting an understanding of the underlying security issues in the CPSs domain, alongside related coverage of the technological advances and solutions proposed to address them. The chapters comprising the later portion of the book are specifically focused upon a series of case examples, evidencing how the protection concepts can translate into practical application.

Security and Quality in Cyber-Physical Systems Engineering - Stefan Biffl 2019-11-09

This book examines the requirements, risks, and solutions to improve the security and quality of complex cyber-physical systems (C-CPS), such as production systems, power plants, and airplanes, in order to ascertain whether it is possible to protect engineering organizations against cyber threats and to ensure engineering project quality. The book consists of three parts that logically build upon each other. Part I "Product Engineering of Complex Cyber-Physical Systems" discusses the structure and behavior of engineering organizations producing complex cyber-physical systems, providing insights into processes and engineering activities, and highlighting the requirements and border conditions for secure and high-quality engineering. Part II "Engineering Quality Improvement" addresses quality improvements with a focus on engineering data generation, exchange, aggregation, and use within an engineering organization, and the need for proper data modeling and engineering-result validation. Lastly, Part III "Engineering Security Improvement" considers security aspects concerning C-CPS engineering, including engineering organizations' security assessments and engineering data management, security concepts and technologies that may be leveraged to mitigate the manipulation of engineering data, as well as design and run-time aspects of secure complex cyber-physical systems. The book is intended for several target groups: it enables computer scientists to identify research issues related to the development of new methods, architectures, and technologies for improving quality and security in multi-disciplinary engineering, pushing forward the current state of the art. It also allows researchers involved in the engineering of C-CPS to gain a better understanding of the challenges and requirements of multi-disciplinary engineering that will guide them in their future research and development activities. Lastly, it offers practicing engineers and managers with engineering backgrounds insights into the benefits and limitations of applicable methods, architectures, and technologies for selected use cases.

Managing the Complexity of Critical Infrastructures - Roberto Setola 2017-02-10

This book is open access under a CC BY 4.0 license. This book summarizes work being pursued in the context of the CIPRNet (Critical Infrastructure Preparedness and Resilience Research Network) research project, co-funded by the European Union under the Seventh Framework Programme (FP7). The project is intended to provide concrete and on-going support to the Critical Infrastructure Protection (CIP) research communities, enhancing their preparedness for CI-related emergencies,

while also providing expertise and technologies for other stakeholders to promote their understanding and mitigation of the consequences of CI disruptions, leading to enhanced resilience. The book collects the tutorial material developed by the authors for several courses on the modelling, simulation and analysis of CIs, representing extensive and integrated CIP expertise. It will help CI stakeholders, CI operators and civil protection authorities understand the complex system of CIs, and help them adapt to these changes and threats in order to be as prepared as possible for mitigating emergencies and crises affecting or arising from CIs.

Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures - Department of Department of Defense 2017-02-28

The scope of the ACI TTP includes all DoD ICS. DoD ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations, such as skid-mounted programmable logic controllers (PLC) are typical configurations found throughout the DoD. ICS are often used in the DoD to manage sectors of critical infrastructure such as electricity, water, wastewater, oil and natural gas, and transportation. Why buy a book you can download for free? First you gotta find a good clean (legible) copy and make sure it's the latest version (not always easy). Some documents found on the web are missing some pages or the image quality is so poor, they are difficult to read. We look over each document carefully and replace poor quality images by going back to the original source document. We proof each document to make sure it's all there - including all changes. If you find a good copy, you could print it using a network printer you share with 100 other people (typically its either out of paper or toner). If it's just a 10-page document, no problem, but if it's 250-pages, you will need to punch 3 holes in all those pages and put it in a 3-ring binder. Takes at least an hour. It's much more cost-effective to just order the latest version from Amazon.com This book is published by 4th Watch Books and includes copyright material. We publish compact, tightly-bound, full-size books (8 x 11 inches), with glossy covers. 4th Watch Books is a Service Disabled Veteran-Owned Small Business (SDVOSB). If you like the service we provide, please leave positive review on Amazon.com. A full copy of all the pertinent cybersecurity standards is available on DVD-ROM in the CyberSecurity Standards Library disc which is available at Amazon.com. For more titles published by 4th Watch Books, please visit: cybah.webplus.net UFC 4-010-06 Cybersecurity of Facility-Related Control Systems UFC 4-021-02 Electronic Security Systems by Department of Defense FC 4-141-05N Navy and Marine Corps Industrial Control Systems Monitoring Stations UFC 4-010-01 DoD Minimum Antiterrorism Standards for Buildings UFC 4-020-01 DoD Security Engineering Facilities Planning Manual UFC 3-430-08N Central Heating Plant UFC 3-410-01 Heating, Ventilating, and Air Conditioning Systems UFC 3-810-01N Navy and Marine Corps Environmental Engineering for Facility Construction UFC 3-730-01 Programming Cost Estimates for Military Construction UFC 1-200-02 High-Performance and Sustainable Building Requirements UFC 3-301-01 Structural Engineering UFC 3-430-02FA Central Steam Boiler Plants UFC 3-430-11 Boiler Control Systems

SCADA Security - What's broken and how to fix it - Andrew Ginter 2019-03

Modern attacks routinely breach SCADA networks that are defended to IT standards. This is unacceptable. Defense in depth has failed us. In ""SCADA Security"" Ginter describes this failure and describes an alternative. Strong SCADA security is possible, practical, and cheaper than failed, IT-centric, defense-in-depth. While nothing can be completely secure, we decide how high to set the bar for our attackers. For important SCADA systems, effective attacks should always be ruinously expensive and difficult. We can and should defend our SCADA systems so thoroughly that even our most resourceful enemies tear their hair out and curse the names of our SCADA systems' designers.

Industrial Network Security - Eric D. Knapp 2014-12-09

As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems—energy production, water, gas, and other vital systems—becomes more important, and heavily mandated. Industrial Network Security, Second Edition arms you with the knowledge you need to understand the vulnerabilities of these distributed supervisory and control systems. The book examines the unique protocols and applications that are the foundation of industrial control systems, and provides clear guidelines for their protection. This how-to guide gives you thorough understanding of the unique challenges facing critical infrastructures, new guidelines and security measures for critical infrastructure protection, knowledge of new and evolving security tools, and pointers on SCADA protocols and security implementation. All-new real-world examples of attacks against control systems, and more diagrams of systems Expanded coverage of protocols such as 61850, Ethernet/IP, CIP, ISA-99, and the evolution to IEC62443 Expanded coverage of Smart Grid security New coverage of signature-based detection, exploit-based vs. vulnerability-based detection, and signature reverse engineering

Securing SCADA Systems - Ronald L. Krutz 2005-11-07

Bestselling author Ron Krutz once again demonstrates hisability to make difficult security topics approachable with thisfirst in-depth look at SCADA (Supervisory Control And DataAcquisition) systems Krutz discusses the harsh reality that natural gas pipelines,nuclear plants, water systems, oil refineries, and other industrialfacilities are vulnerable to a terrorist or disgruntled employeecausing lethal accidents and millions of dollars of damage-and whatcan be done to prevent this from happening Examines SCADA system threats and vulnerabilities, theemergence of protocol standards, and how security controls can beapplied to ensure the safety and security of our nationalinfrastructure assets

Applied Incident Response - Steve Anson 2020-01-29

Incident response is critical for the active defense of any network, and incident responders need up-to-date, immediately applicable techniques with which to engage the adversary. Applied Incident Response details effective ways to respond to advanced attacks against local and remote network resources, providing proven response techniques and a framework through which to apply them. As a starting point for new incident handlers, or as a technical reference for hardened IR veterans, this book details the latest techniques for responding to threats against your network, including: Preparing your environment for effective incident response Leveraging MITRE ATT&CK and threat intelligence for active network defense Local and remote triage of systems using PowerShell, WMIC, and open-source tools Acquiring RAM and disk images locally and remotely Analyzing RAM with Volatility and Rekall Deep-dive forensic analysis of system drives using open-source or commercial tools Leveraging Security Onion and Elastic Stack for network security monitoring Techniques for log analysis and aggregating high-value logs Static and dynamic analysis of malware with YARA rules, FLARE VM, and Cuckoo Sandbox Detecting and responding to lateral movement techniques, including pass-the-hash, pass-the-ticket, Kerberoasting, malicious use of PowerShell, and many more Effective threat hunting techniques Adversary emulation with Atomic Red Team Improving preventive and detective controls

Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions - Clint Bodungen 2016-09-22

Learn to defend crucial ICS/SCADA infrastructure from devastating attacks the tried-and-true Hacking Exposed way This practical guide reveals the powerful weapons and devious methods cyber-terrorists use to compromise the devices, applications, and systems vital to oil and gas pipelines, electrical grids, and nuclear refineries. Written in the battle-tested Hacking Exposed style, the book arms you with the skills and tools necessary to defend against attacks that are debilitating—and potentially deadly. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions explains vulnerabilities and attack vectors specific to ICS/SCADA protocols, applications, hardware, servers, and workstations. You will learn how hackers and malware, such as the infamous Stuxnet worm, can exploit them and disrupt critical processes, compromise safety, and bring production to a halt. The authors fully explain defense strategies and offer ready-to-deploy countermeasures. Each chapter features a real-world case study as well as notes, tips, and cautions. Features examples, code samples, and screenshots of ICS/SCADA-specific attacks Offers step-by-step vulnerability assessment and penetration test instruction Written by a team of ICS/SCADA security experts and edited by Hacking Exposed veteran Joel Scambray

Handbook of SCADA/Control Systems Security - Robert Radvanovsky 2013-02-19

The availability and security of many services we rely upon including water treatment, electricity, healthcare, transportation, and financial transactions are routinely put at risk by cyber threats. The Handbook of SCADA/Control Systems Security is a fundamental outline of security concepts, methodologies, and relevant information pertaining to the

Building Arduino PLCs - Pradeeka Seneviratne 2017-02-07

Learn the fundamentals of PLCs and how to control them using Arduino software to create your first Arduino PLC. You will learn how to draw Ladder Logic diagrams to represent PLC designs for a wide variety of automated applications and to convert the diagrams to Arduino sketches. A comprehensive shopping guide includes the hardware and software

components you need in your tool box. You will learn to use Arduino UNO, Arduino Ethernet shield, and Arduino WiFi shield. Building Arduino PLCs shows you how to build and test a simple Arduino UNO-based 5V DC logic level PLC with Grove Base shield by connecting simple sensors and actuators. You will also learn how to build industry-grade PLCs with the help of ArduiBox. What You'll Learn Build ModBus-enabled PLCs Map Arduino PLCs into the cloud using NearBus cloud connector to control the PLC through the Internet Use do-it-yourself light platforms such as IFTTT Enhance your PLC by adding Relay shields for connecting heavy loads Who This Book Is For Engineers, designers, crafters, and makers. Basic knowledge in electronics and Arduino programming or any other programming language is recommended.

Service Orientation in Holonic and Multi-Agent Manufacturing - Theodor Borangiu 2018-12-12

This book gathers the peer-reviewed papers presented at the 8th edition of the International Workshop “Service Orientation in Holonic and Multi-Agent Manufacturing – SOHOMA’18” held at the University of Bergamo, Italy on June 11–12, 2018. The objective of the SOHOMA annual workshops is to foster innovation in smart and sustainable manufacturing and logistics systems by promoting new concepts, methods and solutions that use service orientation of agent-based control technologies with distributed intelligence. Reflecting the theme of SOHOMA’18: “Digital transformation of manufacturing with agent-based control and service orientation of Internet-scale platforms”, the research included focuses on how the digital transformation, as advocated by the “Industry 4.0”, “Industrial Internet of Things”, “Cyber-Physical Production Systems” and “Cloud Manufacturing” frameworks, improves the efficiency, agility and sustainability of manufacturing processes, products, and services, and how it relates to the interaction between the physical and informational worlds, which is implemented in the virtualization of products, processes and resources managed as services.

Applied Cyber Security and the Smart Grid - Eric D. Knapp 2013-02-26

Many people think of the Smart Grid as a power distribution group built on advanced smart metering—but that’s just one aspect of a much larger and more complex system. The "Smart Grid" requires new technologies throughout energy generation, transmission and distribution, and even the homes and businesses being served by the grid. This also represents new information paths between these new systems and services, all of which represents risk, requiring a more thorough approach to where and how cyber security controls are implemented. This insight provides a detailed architecture of the entire Smart Grid, with recommended cyber security measures for everything from the supply chain to the consumer. Discover the potential of the Smart Grid Learn in depth about its systems See its vulnerabilities and how best to protect it

Cybersecurity for Industrial Control Systems - Tyson Macaulay 2016-04-19

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 im

Cyber-security of SCADA and Other Industrial Control Systems - Edward J. M. Colbert 2016-08-23

This book provides a comprehensive overview of the fundamental security of Industrial Control Systems (ICSs), including Supervisory Control and Data Acquisition (SCADA) systems and touching on cyber-physical systems in general. Careful attention is given to providing the reader with clear and comprehensive background and reference material for each topic pertinent to ICS security. This book offers answers to such questions as: Which specific operating and security issues may lead to a loss of efficiency and operation? What methods can be used to monitor and protect my system? How can I design my system to reduce threats?This book offers chapters on ICS cyber threats, attacks, metrics, risk, situational awareness, intrusion detection, and security testing, providing an advantageous reference set for current system owners who wish to securely configure and operate their ICSs. This book is appropriate for non-specialists as well. Tutorial information is provided in two initial chapters and in the beginnings of other chapters as needed. The book concludes with advanced topics on ICS governance, responses to attacks on ICS, and future security of the Internet of Things.

Cyber-Physical Systems Security - Çetin Kaya Koç 2018-12-06

The chapters in this book present the work of researchers, scientists, engineers, and teachers engaged with developing unified foundations, principles, and technologies for cyber-physical security. They adopt a multidisciplinary approach to solving related problems in next-generation systems, representing views from academia, government bodies, and industrial partners, and their contributions discuss current work on modeling, analyzing, and understanding cyber-physical systems.

Industrial Control Systems Security and Resiliency - Craig Rieger 2020-10-30

This book provides a comprehensive overview of the key concerns as well as research challenges in designing secure and resilient Industrial Control Systems (ICS). It will discuss today's state of the art security architectures and couple it with near and long term research needs that compare to the baseline. It will also establish all discussions to generic reference architecture for ICS that reflects and protects high consequence scenarios. Significant strides have been made in making industrial control systems secure. However, increasing connectivity of ICS systems with commodity IT devices and significant human interaction of ICS systems during its operation regularly introduces newer threats to these systems resulting in ICS security defenses always playing catch-up. There is an emerging consensus that it is very important for ICS missions to survive cyber-attacks as well as failures and continue to maintain a certain level and quality of service. Such resilient ICS design requires one to be proactive in understanding and reasoning about evolving threats to ICS components, their potential effects on the ICS mission’s survivability goals, and identify ways to design secure resilient ICS systems. This book targets primarily educators and researchers working in the area of ICS and Supervisory Control And Data Acquisition (SCADA) systems security and resiliency. Practitioners responsible for security deployment, management and governance in ICS and SCADA systems would also find this book useful. Graduate students will find this book to be a good starting point for research in this area and a reference source.