Critical Infrastructure And Scada Systems Security Scada

SCADA system security is a significant United States national security issue based on the systems' vulnerabilities and the cyber threats that seek to exploit them. Within the last fifteen years as SCADA systems have collectively transitioned to Transmission Control Protocol/Internet Protocol (TCP/IP) networks, analysts and policy-makers have expressed increased concern over the general security and protection of SCADA systems, which are responsible for monitoring and controlling our nation's critical infrastructure. SCADA systems are susceptible based on their ease of entry and their attractiveness as a target. In addition, there a number of cyber threats such as hackers and malware, insiders, terrorist organizations and state actors that are dangerous based on their intent and capabilities. U.S. government engagement with private sector owners and operators of critical infrastructures is essential for mitigating the abundant threats that characterize cyber-terrorism.

Critical Infrastructure Protection II describes original research results and innovative applications in the interdisciplinary field of critical infrastructure protection. Also, it highlights the importance of weaving science, technology and policy in crafting sophisticated solutions that will help secure information, computer and network assets in the various critical infrastructure sectors. This book is the second volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.10 on Critical Infrastructure Protection, an international community of scientists, engineers, practitioners and policy makers dedicated to advancing research, development and implementation efforts focused on infrastructure protection. The book contains a selection of twenty edited papers from the Second Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection held at George Mason University, Arlington, Virginia, USA in the spring of 2008.

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.

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.

The information infrastructure – comprising computers, embedded devices, networks and software systems – is vital to operations in every sector: information technology, telecommunications, energy, banking and finance, transportation systems, chemicals, agriculture and food, defense industrial base, public health and health care, national monuments and icons, drinking water and water treatment systems, commercial facilities, dams, emergency services, commercial nuclear reactors, materials and waste, postal and shipping, and government facilities. Global business and industry, governments, indeed society itself, cannot function if major components of the critical information infrastructure are degraded, disabled or destroyed. This book, Critical Infrastructure Protection IV, is the fourth volume in the annual series produced by IFIP Working Group 11.10 on Critical Infrastructure Protection, an active international community of scientists, engineers, practitioners and policy makers dedicated to advancing research, development and implementation efforts related to critical infrastructure protection. The book presents original research results and innovative applications in the area of infrastructure protection. Also, it highlights the importance of weaving science, technology and policy in crafting sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors. This volume contains seventeen edited papers from the Fourth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection held at the National Defense University, Washington, DC, March 15–17, 2010. The papers were refereed by members of IFIP Working Group 11.10 and other internationally-recognized experts in critical infrastructure protection.

The information infrastructure – comprising computers, embedded devices, networks and software systems – is vital to operations in every sector: chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems. Global business and industry, governments, indeed society itself, cannot function if major components of the critical information infrastructure are degraded, disabled or destroyed. Critical Infrastructure Protection XIV describes original research results and innovative applications in the interdisciplinary field of critical infrastructure protection. Also, it highlights the importance of weaving science, technology and policy in crafting sophisticated, yet practical, solutions that will help secure information, computer and network assets in the critical infrastructure sectors.
various critical infrastructure sectors. Areas of coverage include: Aviation Infrastructure Security; Vehicle Infrastructure Security; Telecommunications Systems Security; Industrial Control Systems Security; Cyber-Physical Systems Security; and Infrastructure Modeling and Simulation. This book is the fourteenth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.10 on Critical Infrastructure Protection, an international community of scientists, engineers, practitioners and policy makers dedicated to advancing research, development and implementation efforts focused on infrastructure protection. The book contains a selection of sixteen edited papers from the Fourteenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, held at SRI International, Arlington, Virginia, USA in the spring of 2020. Critical Infrastructure Protection XIV is an important resource for researchers, faculty members and graduate students, as well as for policy makers, practitioners and other individuals with interests in homeland security.

The increased use of technology is necessary in order for industrial control systems to maintain and monitor industrial, infrastructural, or environmental processes. The need to secure and identify threats to the system is equally critical. Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection provides a full and detailed understanding of the vulnerabilities and security threats that exist within an industrial control system. This collection of research defines and analyzes the technical, procedural, and managerial responses to securing these systems.

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.

Two recent trends have raised concerns about the security and stability of Supervisory Control and Data Acquisition (SCADA) systems. The first is a move to define standard interfaces and communications protocols in support of cross-vendor compatibility and modularity. The second is a move to connect nodes in a SCADA system to open networks such as the Internet. Recent failures of critical infrastructure SCADA systems highlight these concerns. To ensure continued operations in times of crisis, SCADA systems, particularly those operating in our critical infrastructure, must be secured. Developing an abstract generic framework for defining and understanding SCADA systems is a necessary first step. A framework can provide the tools to understand the system's functions and capabilities, and how components in the system relate and interface with each other. This thesis examines and describes SCADA systems, their components, and commonly used communications protocols. It presents a matrix approach to describing and defining the features, functions and capabilities of a SCADA system. Two small SCADA systems, using industry standard components and simulating real world applications, were designed and constructed for this thesis to provide context for applying the matrix approach. This book constitutes the refereed proceedings of the 29th IFIP TC 11 International Information Security and Privacy Conference, SEC 2014, held in Marrakech, Morocco, in June 2014. The 27 revised full papers and 14 short papers presented were carefully reviewed and selected from 151 submissions. The papers are organized in topical sections on intrusion detection, data security, mobile security, privacy, metrics and risk assessment, information flow control, identity management, identifiability and decision making, malicious behavior and fraud and organizational security.

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.

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.

This book constitutes revised selected papers from the 6th International Workshop on Critical Information Infrastructure Security, CRITIS 2011, held in Lucerne, Switzerland, in September 2011. The 16 full papers and 6 short papers presented in this volume were carefully reviewed and selected from 38 submissions. They deal with all areas of critical infrastructure protection research.

Bestselling author Ron Krutz once again demonstrates his ability to make difficult security topics approachable with this first in-depth look at SCADA (Supervisory Control And Data Acquisition) systems Krutz discusses the harsh reality that natural gas pipelines, nuclear plants, water systems, oil refineries, and other industrial facilities are vulnerable to a terrorist or disgruntled employee causing lethal accidents and millions of dollars of damage-and what can be done to prevent this from happening Examines SCADA systems threats and vulnerabilities, the emergence of protocol standards, and how security controls can be applied to ensure the safety and security of our national infrastructure assets.

The information infrastructure--comprising computers, embedded devices, networks, and software systems--is vital to operations in every sector. Global business and industry, governments, and society itself, cannot function effectively if major components of the critical information infrastructure are degraded, disabled or destroyed. This book contains a selection of 27 edited papers from the First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection.

Critical infrastructure facilities allow the United States and other nations to run smoothly every day. Many critical infrastructure facilities that use Supervisory Control and Data Acquisition (SCADA) systems are susceptible to a cyber-attack. Among the plethora of facilities that use SCADA systems are: electric grids, nuclear power plants, water treatment facilities, transportation, etc. These Industrial Control Systems (ICS) then commonly feed into response and management systems mandated by the Department of Homeland Security for protecting United States assets and people and responding to natural and manmade events. Enhancing the US national SCADA/ICS protection is becoming more and more important as the interconnectivity of the national and the world is expanding with the Internet of Things (IoT) and Industrial Internet of Things (IIoT) with the known risks and threats continuing to rise. Creating and providing in-depth Cyber Security and Cyber Hygiene recommendations will allow privately owned Critical Infrastructure (CI) facilities using SCADA/ICS the tools to prevent cyber-attacks from occurring. Finding ways to further the Cybersecurity of SCADA and ICS systems will benefit the public and the owners of the systems, as more and more attacks continue to occur via the profoundly interconnected nature of today’s internet. New solutions are very promising such as enhancing major public-private partnerships like the FBI InfraGard and potentially new national bodies like the Department of Energy’s Office of Cybersecurity and Emergency Response or other specialized agencies. Private-sector and government professional organizations and conferences focused on SCADA and ICS are also leading the nation and world in being better prepared and learning from the attacks or mishaps that have impacted others. Turning security recommendations of SCADA/ICS provided by the National Institute of Standards and Technology (NIST) into requirements will better prepare the workers of CI facilities for cyber-attacks. Turning the recommendations into requirements will also strengthen the government contracts that are meant to perform security audits on the CI facilities.

This volume of Advances in Intelligent and Soft Computing contains accepted papers presented at SOCO 2011 held in the beautiful and historic city of Salamanca, Spain, April 2011. This volume presents the papers accepted for the 2011 edition, both for the main event and the Special Sessions. SOCO 2011 Special Sessions are a very useful tool in order to complement the regular program with new or emerging topics of particular interest to the participating community. Four special sessions were organized related to relevant topics as: Optimization and Control in Industry, Speech Processing and Soft Computing, Systems, Man & Cybernetics and Soft Computing for Medical Applications. Supervisory Control and Data Acquisition (SCADA) systems are used in almost all industrial processes including use in the nation's critical infrastructure. The electric, water, and gas industries are merely a few that rely heavily on the use of SCADA systems in order to provide reliable service to the public. Any disruption in these systems would lead to major issues in day to day life and could produce a hazardous environment until the services are restored. SCADA equipment was first implemented decades ago, and in some cases the equipment deployed at that time is still in use today. As network technology emerged and advanced over the last several years, SCADA systems were adapted in order to provide network access and control from remote locations. This led to vulnerabilities in limiting access to the system and provided a means for hackers, hactavist, and nation-
states to gain control of critical infrastructure SCADA systems in order to cause both physical and economical damage. New technologies and research areas have emerged in an effort to thwart these possible intrusions and attacks. However, there is a need to have adequate means of testing new security devices since it would be impractical to test on a functioning SCADA system. This leads to the development of simulations and testbeds that can provide a low-cost, easily configurable means of testing new cyber security devices. A water treatment and distribution simulation was developed in order to provide this means of testing. The simulation encompasses two components. The first is a software simulation that provides virtualized components typically found in water systems such as pumps, valves, and water tanks. The second is a hardware component that provides an interface from the software to actual SCADA equipment such as remote terminal units and human machine interfaces. The simulation was tested with a prototype cyber security device to ensure functionality. Attacks were carried out on the SCADA system with and without the security device in place. The simulation allowed for both a virtualized and physical response to the attacks. The simulation provided a robust, cost-effective testbed for verifying the functionality of the security device.

Keywords: SCADA, National Critical Infrastructure, Attack/Defense Analysis, Risk Assessment SCADA system security was reviewed for a combined-cycle natural gas-fired and geothermal power generation station. An attack/defense scenario of the risks, threats, vulnerabilities, impacts, and required countermeasures was performed. The Ryan - Nichols risk equation was used to measure risks. Risk and attack lethality were directly related. Taxonomy of threats to SCADA systems was created based on the approximated lethality for power generation plants. Policy recommendations were made to DHS to help improve the security of the power generation plants that control the nation's critical infrastructures. Several factors determined the effectiveness of policies once they were implemented. The U.S. government was stepping up and introducing legislation in the Senate to improve the security of the nation's critical infrastructures. The key findings in this research paper indicated that there was a lack of enforcement of the existing policies and not a large push to fix existing vulnerabilities. The calculation of risk and the taxonomy of threat lethality showed the need to improve current SCADA security because of the dire consequences to the U.S. critical infrastructure and population. The conclusion of the research was that to minimize and mitigate large-scale cyber-attacks, countermeasures need to be implemented, flaws in software and hardware need to be fixed, negligence needs to be prevented, and defense tactics need to be put in place.

In our hyper-connected digital world, cybercrime prevails as a major threat to online security and safety. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. The Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance combines the most recent developments in data protection and information communication technology (ICT) law with research surrounding current criminal behaviors in the digital sphere. Bridgeing research and practical application, this comprehensive reference source is ideally designed for use by investigators, computer forensics practitioners, and experts in ICT law, as well as academicians in the fields of information security and criminal science.

Electrical energy usage is increasing every year due to population growth and new forms of consumption. As such, it is increasingly imperative to research methods of energy control and safe use. Security Solutions and Applied Cryptography in Smart Grid Communications is a pivotal reference source for the latest research on the development of smart grid technology and best practices of utilization. Featuring extensive coverage across a range of relevant perspectives and topics, such as threat detection, authentication, and intrusion detection, this book is ideally designed for academicians, researchers, engineers and students seeking current research on ways in which to implement smart grid platforms all over the globe.

In Nuclear Infrastructure Protection and Homeland Security, authors Frank R. Spellman and Melissa L. Stoudt present all the information needed for nuclear infrastructure employers and employees to handle security threats they must be prepared to meet. This book constitutes the thoroughly refereed post-conference proceedings of the Third International Workshop on Critical Information Infrastructures Security, CRITIS 2008, held in Rome, Italy, in October 2008. The 39 revised full papers presented were carefully reviewed and selected from a total of 70 submissions. All the contributions highlight the current development in the field of Critical (Information) Infrastructures and their Protection. Specifically they emphasized that the efforts dedicated to this topic are beginning to provide some concrete results. Some papers illustrated interesting and innovative solutions devoted to understanding, analyzing and modeling a scenario composed by several heterogeneous and interdependent infrastructures. Furthermore, issues concerning crisis management scenarios for interdependent infrastructures have been illustrated. Encouraging preliminary results have been presented about the development of new technological solutions addressing self-healing capabilities of infrastructures, that is regarded as one of the most promising research topics to improve the infrastructures' resilience.

Around the world, SCADA (supervisory control and data acquisition) systems and other real-time process control networks run mission-critical infrastructure—everything from the power grid to water treatment, chemical manufacturing to transportation. These networks are at increasing risk due to the move from proprietary systems to more standard platforms and protocols and the interconnection to other networks. Because there has been limited attention paid to security, these systems are seen as largely unsecured and very vulnerable to attack. This book addresses currently undocumented security issues affecting SCADA systems and overall critical infrastructure protection. The respective co-authors are among the leading experts in the world capable of addressing these related-but-independent concerns of SCADA security. Headline-making threats and countermeasures like malware, sidejacking, biometric applications, emergency communications, security awareness planning, personnel & workplace preparedness and bomb threat planning will be addressed in detail in this one of a kind book-of-books dealing with the threats to critical infrastructure protection. They collectively have over a century of
expertise in their respective fields of infrastructure protection. Included among the contributing authors are Paul Henry, VP of Technology Evangelism, Secure Computing, Chet Hosmer, CEO and Chief Scientist at Weststone Technologies, Phil Drake, Telecommunications Director, The Charlotte Observer, Patrice Bourgeois, Tenable Network Security, Sean Lowther, President, Stealth Awareness and Jim Windle, Bomb Squad Commander, CMPD. * Internationally known experts provide a detailed discussion of the complexities of SCADA security and its impact on critical infrastructure * Highly technical chapters on the latest vulnerabilities to SCADA and critical infrastructure and countermeasures * Bonus chapters on security awareness training, bomb threat planning, emergency communications, employee safety and much more * Companion Website featuring video interviews with subject matter experts offer a "sit-down" with the leaders in the field

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.

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 supervisory control and data acquisition (SCADA) systems and technology that quietly operate in the background of critical utility and industrial facilities worldwide. Divided into five sections, the book examines topics comprising functions within and throughout industrial control systems (ICS) environments. Topics include: Emerging trends and threat factors that plague the ICS security community Risk methodologies and principles that can be applied to safeguard and secure an automated operation Methods for determining events leading to a cyber incident, and methods for restoring and mitigating issues—including the importance of critical communications The necessity and reasoning behind implementing a governance or compliance program A strategic roadmap for the development of a secured SCADA/control systems environment, with examples Relevant issues concerning the maintenance, patching, and physical localities of ICS equipment How to conduct training exercises for SCADA/control systems The final chapters outline the data relied upon for accurate processing, discusses emerging issues with data overload, and provides insight into the possible future direction of ISC security. The book supplies crucial information for securing industrial automation/process control systems as part of a critical infrastructure protection program. The content has global applications for securing essential governmental and economic systems that have evolved into present-day security nightmares. The authors present a "best practices" approach to securing business management environments at the strategic, tactical, and operational levels.

Since the initial inception of this book, there have been significant strides to safeguard the operations of our world's infrastructures. In recent years, there has also been a shift to more fluid postures associated with resilience and the establishment of redundant infrastructure. In keeping with the fast-changing nature of this field, Critical Infrastructure: Homeland Security and Emergency Preparedness, Third Edition has been revised and updated to reflect this shift in focus and to incorporate the latest developments. The book begins with the historical background of critical infrastructure and why it is important to society. It then explores the current trend in understanding the infrastructure's sensitivity to impacts that flow through its networked environment. Embracing an "all-hazards approach" to homeland security, critical infrastructure protection and assurance, and emergency management, the authors examine: The National Response Framework (NRF) and how it can be applied globally The relationships between the public and private sectors, and the growing concept of public-private partnerships The shift from the need-to-know paradigm to one based on information sharing, and the nature of necessary controls as this shift continues The need for organizations to adopt resilient planning, implementation, and decision-making processes in order to respond to changes within the threat environment What, where, why, and how risk assessments are to be performed, and why they are needed The impact of new regulation, individually applied self-regulation, industry and government regulation, and law enforcement. In the final chapters, the book discusses current information sharing and analysis centers (ISACs), distributed control systems, and supervisory control and data acquisition (SCADA) systems and their challenges. It concludes by exploring current challenges associated with establishing a trusted network across various sectors—demonstrating how models of information can be categorized and communicated within trusted communities to better assure the public-private relationship.

Version 1.0. This guidebook provides information for enhancing the security of Supervisory Control and Data Acquisition Systems (SCADA) and Industrial Control Systems (ICS). The information is a comprehensive overview of industrial control system security, including administrative controls, architecture design, and security technology. This is a guide for enhancing security, not a how-to manual for building an ICS, and its purpose is to teach ICS managers, administrators, operators, engineers, and other ICS staff what security concerns they should be taking into account. Other related products: National Response Framework, 2008 is available here: https://bookstore.gpo.gov/products/sku/064-000-00444-6 National Strategy for Homeland Security (October 2007) is available here: https://bookstore.gpo.gov/products/sku/041-001-00657-5 New Era of Responsibility: Renewing America's Promise can be found here: https://bookstore.gpo.gov/products/sku/041-001-00660-5

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.

The unfortunate events of September 11, 2001 have caused a renewed effort to protect our Nation's Critical Infrastructures. SCADA systems are relied upon in a large number of the sectors that make up the critical infrastructure, and their importance was reinforced during the massive power outage that occurred in August 2003. Growing reliance upon the Internet has emphasized the vulnerability of SCADA system communications to cyber attack. Only through diligent and continuous vulnerability assessment and certification and accreditation of these
systems will the United States be able to mitigate some of the vulnerabilities of these systems. A case study presented here has validated the need for continued focus in this area. This thesis consolidates some of the research that has already been done in the area of SCADA vulnerability assessment and applies it by developing an initial vulnerability assessment checklist for Department of the Navy systems. This checklist can and should also be used in the certification and accreditation of DoN SCADA systems. A promising technology was also discovered during this research that should be explored further to secure SCADA communications. This will be touched on briefly.

We depend on information and information technology (IT) to make many of our day-to-day tasks easier and more convenient. Computers play key roles in transportation, health care, banking, and energy. Businesses use IT for payroll and accounting, inventory and sales, and research and development. Modern military forces use weapons that are increasingly coordinated through computer-based networks. Cybersecurity is vital to protecting all of these functions. Cyberspace is vulnerable to a broad spectrum of hackers, criminals, terrorists, and state actors. Working in cyberspace, these malevolent actors can steal money, intellectual property, or classified information; impersonate law-abiding parties for their own purposes; damage important data; or deny the availability of normally accessible services. Cybersecurity issues arise because of three factors taken together - the presence of malevolent actors in cyberspace, societal reliance on IT for many important functions, and the presence of vulnerabilities in IT systems. What steps can policy makers take to protect our government, businesses, and the public from those who would take advantage of system vulnerabilities? At the Nexus of Cybersecurity and Public Policy offers a wealth of information on practical measures, technical and nontechnical challenges, and potential policy responses. According to this report, cybersecurity is a never-ending battle; threats will evolve as adversaries adopt new tools and techniques to compromise security. Cybersecurity is therefore an ongoing process that needs to evolve as new threats are identified. At the Nexus of Cybersecurity and Public Policy is a call for action to make cybersecurity a public safety priority. For a number of years, the cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the fundamentals of cybersecurity and the discussion of potential policy responses, this book will be a resource for policy makers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace.

Through the rise of big data and the Internet of things, terrorist organizations have been freed from geographic and logistical confines and now have more power than ever before to strike the average citizen directly at home. This, coupled with the inherently asymmetrical nature of cyberwarfare, which grants great advantage to the attacker, has created an unprecedented national security risk that both governments and their citizens are woefully ill-prepared to face. Examining cyber warfare and terrorism through a critical and academic perspective can lead to a better understanding of its foundations and implications. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications is an essential reference for the latest research on the utilization of online tools by terrorist organizations to communicate with and recruit potential extremists and examines effective countermeasures employed by law enforcement agencies to defend against such threats. Highlighting a range of topics such as cyber threats, digital intelligence, and counterterrorism, this multi-volume book is ideally designed for law enforcement, government officials, lawmakers, security analysts, IT specialists, software developers, intelligence and security practitioners, students, educators, and researchers.

Challenging the supposed notion that corporations can contain a breach before it becomes public knowledge, Managing Cybersecurity Risk, Second Edition explains how organizations can develop and implement a comprehensive enterprise-wide cybersecurity risk management strategy. The authors show how to map out 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 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, sensors, 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

Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat ProtectionApproaches for Threat ProtectionGI Global

Author Robert Lee created this wonderful illustrated guide to SCADA to educate and inform. Supervisory Control And Data Acquisition (SCADA) systems pervade every part of our technological life. They are embedded in hospitals, power grids, and manufacturing plants. Most systems were designed and deployed well before the modern day Internet and the incredible amount of cyber attacks we see in the news daily. SCADA systems are subject to those attacks and most are vulnerable. Understanding this vulnerability and moving the conversation towards protecting the critical infrastructure controlled by SCADA systems is the purpose of SCADA and Me. This easy-to-consume book is a must-have for anyone involved in cyber education.

Copyright: e21588badc1f822a9bfbf6df69b835f8