Industrial Network Security Securing Critical Infrastructure Networks For Smart Grid Scada And Other Industrial Control Systems | 97486f76cc94a955b93fa571580ee442

ECCWS 2017 16th European Conference on Cyber Warfare and SecurityCyber Security of Industrial Control Systems in the Future Internet EnvironmentHandbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's Smart Grids and Their Communication SystemsAdvanced Information Networking and ApplicationsCybersecurity of Industrial SystemsSecurity Solutions and Applied Cryptography in Smart Grid CommunicationsIndustrial CybersecuritySecuring Critical Infrastructures and Critical Control Systems: Approaches for Threat ProtectionIndustrial Network SecuritySmart Grid SecurityNew Dimensions of Information WarfareCyber Security and Threats: Concepts, Methodologies, Tools, and ApplicationsSecurity and Quality in Cyber-Physical Systems EngineeringCybernetics and Algorithms in Intelligent SystemsCritical Infrastructure Protection XIRecent Developments on Industrial Control Systems ResilienceIndustrial Network SecurityIndustrial Network SecurityCyber-security of SCADA and Other Industrial Control SystemsInformation Systems Security and PrivacyCyber Security for Cyber Physical SystemsGuide to Vulnerability Analysis for Computer Networks and SystemsRecent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS)Diagnosability, Security and Safety of Hybrid Dynamic and Cyber-Physical SystemsStrategic Innovative Marketing and Tourism3D Imaging Technologies—Multidimensional Signal Processing and Deep LearningSecure Control of Networked Control Systems and Its ApplicationsPower Systems ResilienceIntrusion Detection in Wireless Ad-Hoc NetworksApplied Cyber Security and the Smart GridCyber Defence in the Age of AI, Smart Societies and Augmented HumanitySecuring the Internet of Things: Concepts, Methodologies, Tools, and ApplicationsResilient Control Architectures and Power SystemsSecuring India in the Cyber EraCritical Infrastructure Protection IXProgress in Artificial IntelligenceCybersecurity and Human Rights in the Age of CyberveillanceComputer SecurityAdvances in Cybersecurity Management

ECCWS 2017 16th European Conference on Cyber Warfare and Security This book covers a very broad range of topics in marketing, communication, and tourism, focusing especially on new perspectives and technologies that promise to influence the future direction of marketing research and practice in a digital and innovational era. Among the areas covered are product and brand management, strategic marketing, B2B marketing and sales management, international marketing, business communication and advertising, digital and social marketing, tourism and hospitality marketing and management, destination branding and cultural management, and event marketing. The book comprises the proceedings of the International Conference on Strategic Innovative Marketing and Tourism (ICSIMAT) 2018, where researchers, academics, and government and industry practitioners from around the world came together to discuss best practices, the latest research, new paradigms, and advances in theory. It will be of interest to a wide audience, including members of the academic community, MSc and PhD students, and marketing and tourism professionals.

Cyber Security of Industrial Control Systems in the Future Internet Environment The Smart Grid security ecosystem is complex and multi-disciplinary, and relatively under-researched compared to the traditional information and network security disciplines. While the Smart Grid has provided increased efficiencies in monitoring power usage, directing power supplies to serve peak power needs and improving efficiency of power delivery, the Smart Grid has also opened the way for information security breaches and other types of security breaches. Potential threats range from meter manipulation to directed, high-impact attacks on critical infrastructure that could bring down regional or national power grids. It is essential that security measures are put in place to ensure that the Smart Grid does not succumb to these threats and to safeguard this critical infrastructure at all times. Dr. Florian Skopik is one of the leading researchers in Smart Grid security, having organized and led research consortia and panel discussions in this field. Smart Grid Security will provide the first truly holistic view of leading edge Smart Grid security research. This book does not focus on vendor-specific solutions, instead providing a complete presentation of forward-looking research in all areas of Smart Grid security. The book will enable practitioners to learn about upcoming trends, scientists to share new directions in research, and government and industry decision-makers to prepare for major strategic decisions regarding implementation of Smart Grid technology. Presents the most current and leading edge research on Smart Grid security from a holistic standpoint, featuring a panel of top experts in the field. Includes coverage of risk management, operational security, and secure development of the Smart Grid. Covers key technical topics, including threat types and attack vectors, threat case studies, smart metering, smart home, e- mobility, smart buildings, DERs, demand response management, distribution grid operators, transmission grid operators, virtual power plants, resilient architectures, communications protocols and encryption, as well as physical security.

Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's This book shows some secure control methods of networked control systems related to linear control system, nonlinear control system, multi-agent system and its applications in power systems. The proposed secure control methods provide some useful results about modeling of network attacks, resilient analysis and synthesis methods, active defense control method. The contents of this book are lists as followings. (1) Modeling of DoS attacks, deception attacks and replay attacks; (2)Secure control methods are proposed by combing delay system method, switched system method and event-based control method. (3) Active control methods are proposed by using model-predictive control and redundant control. (4) The proposed control methods are applied to the security problem of power system. The methods of this book include DoS attacks modeling such as, periodic jamming attack model,model-based average dwell time model, deception attack modeling and relay attack modeling; piece-wise Lyapunov-Krasoviskii functional

method, stochastic control method; the results including resilient conditions of networked control system and related resilient control design method with linear matrix inequalities(LMIs). From this book, readers can learn about the general network attack modeling methods, resilient analysis and synthesis methods, active control methods from viewpoint of redundancy control, and secure conditions of power systems. Some fundamental knowledge prepared to read this book includes delay system theory, event triggered mechanism, T-S fuzzy system theory and frequency/voltage control of power system.

Smart Grids and Their Communication Systems This book constitutes the refereed proceedings of the 20th EPIA Conference on Artificial Intelligence, EPIA 2021, held virtually in September 2021. The 62 full papers and 6 short papers presented were carefully reviewed and selected from a total of 108 submissions. The papers are organized in the following topical sections: artificial intelligence and IoT in agriculture; artificial intelligence and law; artificial intelligence in medicine; artificial intelligence in power and energy systems; artificial intelligence in transportation systems; artificial life and evolutionary algorithms; ambient intelligence and affective environments; general AI; intelligent robotics; knowledge discovery and business intelligence; multi-agent systems: theory and applications; and text mining and applications.

Advanced Information Networking and Applications This book revises the strategic objectives of Information Warfare, interpreting them according to the modern canons of information age, focusing on the fabric of society, the economy, and critical Infrastructures. The authors build plausible detailed real-world scenarios for each entity, showing the related possible threats from the Information Warfare point of view. In addition, the authors dive into the description of the still open problems, especially when it comes to critical infrastructures, and the countermeasures that can be implemented, possibly inspiring further research in the domain. This book intends to provide a conceptual framework and a methodological guide, enriched with vivid and compelling use cases for the readers (e.g. technologists, academicians, military, government) interested in what Information Warfare really means, when its lenses are applied to current technology. Without sacrificing accuracy, rigor and, most importantly, the big picture of Information Warfare, this book dives into several relevant and up-to-date critical domains. The authors illustrate how finance (an always green target of Information Warfare) is intertwined with Social Media, and how an opponent could exploit these latter ones to reach its objectives. Also, how cryptocurrencies are going to reshape the economy, and the risks involved by this paradigm shift. Even more compelling is how the very fabric of society is going to be reshaped by technology, for instance how our democratic elections are exposed to risks that are even greater than what appears in the current public discussions. Not to mention how our Critical Infrastructure is becoming exposed to a series of novel threats, ranging from state-supported malware to drones. A detailed discussion of possible countermeasures and what the open issues are for each of the highlighted threats complete this book. This book targets a widespread audience that includes researchers and advanced level students studying and working in computer science with a focus on security. Military officers, government officials and professionals working in this field will also find this book useful as a reference.

Cybersecurity of Industrial Systems Master the fundamentals of resilient power grid control applications with this up-to-date resource from four industry leaders Resilient Control Architectures and Power Systems delivers a unique perspective on the singular challenges presented by increasing automation in society. In particular, the book focuses on the difficulties presented by the increased automation of the power grid. The authors provide a simulation of this real-life system, offering an accurate and comprehensive picture of a how a power control system works and, even more importantly, how it can fail. The editors invite various experts in the field to describe how and why power systems fail due to cyber security threats, human error, and complex interdependencies. They also discuss promising new concepts researchers are exploring that promise to make these control systems much more resilient to threats of all kinds. Finally, resilience fundamentals and applications are also investigated to allow the reader to apply measures that ensure adequate operation in complex control systems. Among a variety of other foundational and advanced topics, you'll learn about: The fundamentals of power grid infrastructure, including grid architecture, control system architecture, and communication architecture The disciplinary fundamentals of control theory, human-system interfaces, and cyber security The fundamentals of resilience, including the basis of resilience, its definition, and benchmarks, as well as cross-architecture metrics and considerations The application of resilience concepts, including cyber security challenges, control challenges, and human challenges A discussion of research challenges facing professionals in this field today Perfect for research students and practitioners in fields concerned with increasing power grid automation, Resilient Control Architectures and Power Systems also has a place on the bookshelves of members of the Control Systems Society, the Systems, Man and Cybernetics Society, the Computer Society, the Power and Energy Society, and similar organizations.

Security Solutions and Applied Cryptography in Smart Grid Communications

Industrial Cybersecurity The information infrastructure---comprising computers, embedded devices, networks and software systems---is vital to day-to-day operations in every sector: information and telecommunications, banking and finance, energy, chemicals and hazardous materials, agriculture, food, water, public health, emergency services, transportation, postal and shipping, government and defense. Global business and industry, governments, indeed society itself, cannot function effectively if major components of the critical information infrastructure are degraded, disabled or destroyed. Critical Infrastructure Protection 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 various critical infrastructure sectors. Areas of coverage include: Themes and Issues, Control Systems Security, Cyber-Physical Systems Security,

Infrastructure Security, Infrastructure Modeling and Simulation, Risk and Impact Assessment. This book is the ninth 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 nineteen edited papers from the Ninth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, held at SRI International, Arlington, Virginia, USA in the spring of 2015. Critical Infrastructure Protection IX 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. Mason Rice is an Assistant Professor of Computer Science at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection 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.

Industrial Network Security Cyber-physical systems (CPS) are characterized as a combination of physical (physical plant, process, network) and cyber (software, algorithm, computation) components whose operations are monitored, controlled, coordinated, and integrated by a computing and communicating core. The interaction between both physical and cyber components requires tools allowing analyzing and modeling both the discrete and continuous dynamics. Therefore, many CPS can be modeled as hybrid dynamic systems in order to take into account both discrete and continuous behaviors as well as the interactions between them. Guaranteeing the security and safety of CPS is a challenging task because of the inherent interconnected and heterogeneous combination of behaviors (cyber/physical, discrete/continuous) in these systems. This book presents recent and advanced approaches and tech-niques that address the complex problem of analyzing the diagnosability property of cyber physical systems and ensuring their security and safety against faults and attacks. The CPS are modeled as hybrid dynamic systems using different model-based and data-driven approaches in different application domains (electric transmission networks, wireless communication networks, intrusions in industrial control systems, intrusions in production systems, wind farms etc.). These approaches handle the problem of ensuring the security of CPS in presence of attacks and verifying their diagnosability in presence of different kinds of uncertainty (uncertainty related to the event occurrences, to their order of occurrence, to their value etc.).

Smart Grid Security This book presents intuitive explanations of the principles and applications of power system resiliency, as well as a number of straightforward and practical methods for the impact analysis of risk events on power system operations. It also describes the challenges of modelling, distribution networks, optimal scheduling, multi-stage planning, deliberate attacks, cyber-physical systems and SCADA-based smart grids, and how to overcome these challenges. Further, it highlights the resiliency issues using various methods, including strengthening the system against high impact events with low frequency and the fast recovery of the system properties. A large number of specialists have collaborated to provide innovative solutions and research in power systems resiliency. They discuss the fundamentals and contemporary materials of power systems resiliency, theoretical and practical issues, as well as current issues and methods for controlling the risk attacks and other threats to AC power systems. The book includes theoretical research, significant results, case studies, and practical implementation processes to offer insights into electric power and engineering and energy systems. Showing how systems should respond in case of malicious attacks, and helping readers to decide on the best approaches, this book is essential reading for electrical engineers, researchers and specialists. The book is also useful as a reference for undergraduate and graduate students studying the resiliency and reliability of power systems.

New Dimensions of Information Warfare This book constitutes the revised selected papers of the 5th International Conference on Information Systems Security and Privacy, ICISSP 2019, held in Prague, Czech Republic, in February 2019. The 19 full papers presented were carefully reviewed and selected from a total of 100 submissions. The papers presented in this volume address various topical research, including new approaches for attack modelling andprevention, incident management and response, and user authentication andaccess control, as well as business and human-oriented aspects such as data pro-tection and privacy, and security awareness.

Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications 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.

Security and Quality in Cyber-Physical Systems Engineering The ubiquity of modern technologies has allowed for increased connectivity between people and devices across the globe. This

connected infrastructure of networks creates numerous opportunities for applications and uses. As the applications of the internet of things continue to progress so do the security concerns for this technology. The study of threat prevention in the internet of things is necessary as security breaches in this field can ruin industries and lives. Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications is a vital reference source that examines recent developments and emerging trends in security and privacy for the internet of things through new models, practical solutions, and technological advancements related to security. Highlighting a range of topics such as cloud security, threat detection, and open source software, this multi-volume book is ideally designed for engineers, IT consultants, ICT procurement managers, network system integrators, infrastructure service providers, researchers, academics, and professionals interested in current research on security practices pertaining to the internet of things.

Cybernetics and Algorithms in Intelligent Systems Security, privacy, and trust in the Internet of Things (IoT) and CPS (Cyber-Physical Systems) are different from conventional security as concerns revolve around the collection and aggregation of data or transmission of data over the network. Analysis of cyber-attack vectors and the provision of appropriate mitigation techniques are essential research areas for these systems. Adoption of best practices and maintaining a balance between ease of use and security are, again, crucial for the effective performance of these systems. Recent Advances in Security, Privacy and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS) discusses and presents techniques and methodologies, as well as a wide range of examples and illustrations, to effectively show the principles, algorithms, challenges, and applications of security, privacy, and trust for IoT and CPS. Book features: Introduces new directions for research, development, and engineering security, privacy, and trust of IoT and CPS Includes a wealth of examples and illustrations to effectively demonstrate the principles, algorithms, challenges, and applications Covers most of the important security aspects and current trends not present in other reference books This book will also serve as an excellent reference in security, privacy, and trust of IoT and CPS for professionals in this fast-evolving and critical field. The chapters present high-quality contributions from researchers, academics, and practitioners from various national and international organizations and universities.

Critical Infrastructure Protection XI This book explores various challenging problems and applications areas of wireless sensor networks (WSNs), and identifies the current issues and future research challenges. Discussing the latest developments and advances, it covers all aspects of in WSNs, from architecture to protocols design, and from algorithm development to synchronization issues. As such the book is an essential reference resource for undergraduate and postgraduate students as well as scholars and academics working in the field.

Recent Developments on Industrial Control Systems Resilience This proceedings book covers the theory, design and applications of computer networks, distributed computing and information systems. Today’s networks are evolving rapidly, and there are several developing areas and applications. These include heterogeneous networking supported by recent technological advances in power wireless communications, along with silicon integration of various functionalities such as sensing, communications, intelligence and actuations, which is emerging as a critically important disruptive computer class based on a new platform, networking structure and interface that enables novel, low-cost and high-volume applications. However, implemeting these applications has sometimes been difficult due to interconnection problems. As such, different networks need to collaborate, and wired and next-generation wireless systems need to be integrated in order to develop high-performance computing solutions to address the problems arising from these networks’ complexities. This ebook presents the latest research findings, as well as theoretical and practical perspectives on the innovative methods and development techniques related to the emerging areas of information networking and applications

Industrial Network 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.

Industrial Network Security This book explores the geopolitics of the global cyber space to analyse India's cyber security landscape. As conflicts go more online, nation-states are manipulating the cyber space to exploit each other's dependence on information, communication and digital technologies. All the major powers have dedicated cyber units to breach computer networks, harvest sensitive data and proprietary information, and disrupt critical national infrastructure operations. This volume reviews threats to Indian computer networks, analyses the country's policy responses to these threats, and suggests comprehensive measures to build resilience in the system. India constitutes the second largest internet user base in the world, and this expansion of the user base also saw an accompanying rise in cyber crimes. The book discusses how the country can protect this user base, the data-dependent critical infrastructure, build resilient digital payment systems, and answer the challenges of the dark net. It also explores India's cyber diplomacy, as an emerging economy with a large IT industry and a well-established technological base. Topical and lucid, this book as part of The Gateway House Guide to India in the 2020s series, will be of interest to scholars and researchers of cyber security, digital diplomacy, foreign policy, international relations, geopolitics, strategic affairs, defence studies, South Asian politics and international politics.

Cyber-security of SCADA and Other Industrial Control Systems 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.

Information Systems Security and Privacy Presenting cutting-edge research, Intrusion Detection in Wireless Ad-Hoc Networks explores the security aspects of the basic categories of wireless ad-hoc networks and related application areas. Focusing on intrusion detection systems (IDSs), it explains how to establish security solutions for the range of wireless networks, including mobile ad-hoc networks, hybrid wireless networks, and sensor networks. This edited volume reviews and analyzes state-of-the-art IDSs for various wireless ad-hoc networks. It includes case studies on honesty-based intrusion detection systems, cluster oriented-based intrusion detection systems, and trust-based intrusion detection systems. Addresses architecture and organization issues Examines the different types of routing attacks for WANs Explains how to ensure Quality of Service in secure routing Considers honesty and trust-based IDS solutions Explores emerging trends in WAN security Describes the blackhole attack detection technique Surveying existing trust-based solutions, the book explores the potential of the CORIDS algorithm to provide trust-based solutions for secure mobile applications. Touching on more advanced topics, including security for smart power grids, securing cloud services, and energy-efficient IDSs, this book provides you with the tools to design and build secure next-generation wireless networking environments.

Cyber Security for Cyber Physical Systems Nowadays one only needs to read the newspaper headlines to appreciate the importance of Industrial Network Security. Almost daily an article comes out describing the threat to our critical infrastructure, from spies in our electrical grid to the looming threat of cyberwar. Whether we talk about process control systems that run chemical plants and refineries, supervisory control and data acquisition (SCADA) systems for utilities, or factory automation systems for discrete manufacturing, the backbone of our nationA's critical infrastructure consists of these industrial networks and is dependent on their continued operation. This easy-to-read book introduces managers, engineers, technicians, and operators on how to keep our industrial networks secure amid rising threats from hackers, disgruntled employees, and even cyberterrorists.

Guide to Vulnerability Analysis for Computer Networks and Systems This book concentrates on a wide range of advances related to IT cybersecurity management. The topics covered in this book include, among others, management techniques in security, IT risk management, the impact of technologies and techniques on security management, regulatory techniques and issues, surveillance technologies, security policies, security for protocol management, location management, GOS management, resource management, channel management, and mobility management. The authors also discuss digital contents copyright protection, system security management, network security management, security management in network equipment, storage area networks (SAN) management, information security management, government security policy, web penetration testing, security operations, and vulnerabilities management. The authors introduce the concepts, techniques, methods, approaches and trends needed by cybersecurity management specialists and educators for keeping current their cybersecurity management knowledge. Further, they provide a glimpse of future directions where cybersecurity management techniques, policies, applications, and theories are headed. The book is a rich collection of carefully selected and reviewed manuscripts written by diverse cybersecurity management experts in the listed fields and edited by prominent cybersecurity management

researchers and specialists. Provides a professional development resource for educators and practitioners on the state-of-the-art cybersecurity management materials; Contributes towards the enhancement of the community outreach and engagement component of cybersecurity management; Introduces various techniques, methods, and approaches adopted by cybersecurity management experts.

Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS) 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.

Diagnosability, Security and Safety of Hybrid Dynamic and Cyber-Physical Systems This book is a pioneering yet primary general reference resource on cyber physical systems and their security concerns. Providing a fundamental theoretical background, and a clear and comprehensive overview of security issues in the domain of cyber physical systems, it is useful for students in the fields of information technology, computer science, or computer engineering where this topic is a substantial emerging area of study.

Strategic Innovative Marketing and Tourism This book provides profound insights into industrial control system resilience, exploring fundamental and advanced topics and including practical examples and scenarios to support the theoretical approaches. It examines issues related to the safe operation of control systems, risk analysis and assessment, use of attack graphs to evaluate the resiliency of control systems, preventive maintenance, and malware detection and analysis. The book also discusses sensor networks and Internet of Things devices. Moreover, it covers timely responses to malicious attacks and hazardous situations, helping readers select the best approaches to handle such unwanted situations. The book is essential reading for engineers, researchers, and specialists addressing security and safety issues related to the implementation of modern industrial control systems. It is also a valuable resource for students interested in this area.

3D Imaging Technologies—Multidimensional Signal Processing and Deep Learning Cybersecurity and Human Rights in the Age of Cyberveillance is a collection of articles by distinguished authors from the US and Europe and presents contemporary perspectives on the limits of human rights in the international internet community.

Secure Control of Networked Control Systems and Its Applications This book presents high-quality research in the field of 3D imaging technology. The second edition of International Conference on 3D Imaging Technology (3DDIT-MSP&DL) continues the good traditions already established by the first 3DIT conference (IC3DIT2019) to provide a wide scientific forum for researchers, academia and practitioners to exchange newest ideas and recent achievements in all aspects of image processing and analysis, together with their contemporary applications. The conference proceedings are published in 2 volumes. The main topics of the papers comprise famous trends as: 3D image representation, 3D image technology, 3D images and graphics, and computing and 3D information technology. In these proceedings, special attention is paid at the 3D tensor image representation, the 3D content generation technologies, big data analysis, and also deep learning, artificial intelligence, the 3D image analysis and video understanding, the 3D virtual and augmented reality, and many related areas. The first volume contains papers in 3D image processing, transforms and technologies. The second volume is about computing and information technologies, computer images and graphics and related applications. The two volumes of the book cover a wide area of the aspects of the contemporary multidimensional imaging and the related future trends from data acquisition to real-world applications based on various techniques and theoretical approaches.

Power Systems Resilience The book presents a broad overview of emerging smart grid technologies and communication systems, offering a helpful guide for future research in the field of electrical engineering and communication engineering. It explores recent advances in several computing technologies and their performance evaluation, and addresses a wide range of topics, such as the essentials of smart grids for fifth generation (5G) communication systems. It also elaborates the role of emerging communication systems such as 5G, internet of things (IoT), IEEE 802.15.4 and cognitive radio networks in smart grids. The book includes detailed surveys and case studies on current trends in smart grid systems and communications for smart metering and monitoring, smart grid energy storage systems, modulations and waveforms for 5G networks. As such, it will be of interest to practitioners and researchers in the field of smart grid and communication infrastructures alike.

Intrusion Detection in Wireless Ad-Hoc Networks This book constitutes the thoroughly refereed post-conference proceedings of the Third International Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems, CyberICPS 2017, and the First International Workshop on Security and Privacy Requirements Engineering, SECPRE 2017, held in Oslo,

Norway, in September 2017, in conjunction with the 22nd European Symposium on Research in Computer Security, ESORICS 2017. The CyberICPS Workshop received 32 submissions from which 10 full and 2 short papers were selected for presentation. They cover topics related to threats, vulnerabilities and risks that cyber-physical systems and industrial control systems face; cyber attacks that may be launched against such systems; and ways of detecting and responding to such attacks. From the SECPRE Workshop 5 full papers out of 14 submissions are included. The selected papers deal with aspects of security and privacy requirements assurance and evaluation; and security requirements elicitation and modelling.

Applied Cyber Security and the Smart Grid Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems describes an approach to ensure the security of industrial networks by taking into account the unique network, protocol, and application characteristics of an industrial control system, along with various compliance controls. It offers guidance on deployment and configuration, and it explains why, where, and how security controls should be implemented. Divided into 11 chapters, the book explains the basics of Ethernet and Transmission Control Protocol/Internet Protocol (TCP/IP) networking communications and the SCADA and field bus protocols. It also discusses industrial networks as they relate to “critical infrastructure and cyber security, potential risks and consequences of a cyber attack against an industrial control system, compliance controls in relation to network security practices, industrial network protocols, such as Modbus and DNP3, assessment of vulnerabilities and risk, how to secure enclaves, regulatory compliance standards applicable to industrial network security, and common pitfalls and mistakes, like complacency and deployment errors. This book is a valuable resource for plant operators and information security analysts, as well as compliance officers who want to pass an audit with minimal penalties and/or fines. Covers implementation guidelines for security measures of critical infrastructure Applies the security measures for system-specific compliance Discusses common pitfalls and mistakes and how to avoid them

Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity 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 XI 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 various critical infrastructure sectors. Areas of coverage include: Infrastructure Protection, Infrastructure Modeling and Simulation, Industrial Control System Security, and Internet of Things Security. This book is the eleventh 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 Eleventh Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, held at SRI International, Arlington, Virginia, USA in the spring of 2017. Critical Infrastructure Protection XI 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.

Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications In today’s modernized market, many fields are utilizing internet technologies in their everyday methods of operation. The industrial sector is no different as these technological solutions have provided several benefits including reduction of costs, scalability, and efficiency improvements. Despite this, cyber security remains a crucial risk factor in industrial control systems. The same public and corporate solutions do not apply to this specific district because these security issues are more complex and intensive. Research is needed that explores new risk assessment methods and security mechanisms that professionals can apply to their modern technological procedures. Cyber Security of Industrial Control Systems in the Future Internet Environment is a pivotal reference source that provides vital research on current security risks in critical infrastructure schemes with the implementation of information and communication technologies. While highlighting topics such as intrusion detection systems, forensic challenges, and smart grids, this publication explores specific security solutions within industrial sectors that have begun applying internet technologies to their current methods of operation. This book is ideally designed for researchers, system engineers, managers, networkers, IT professionals, analysts, academicians, and students seeking a better understanding of the key issues within securing industrial control systems that utilize internet technologies.

Resilient Control Architectures and Power Systems This book presents new approaches and methods applied to real-world problems, and in particular, exploratory research relating to novel approaches in the field of cybernetics and automation control theory. Particularly focusing on modern trends in selected fields of interest, it presents new algorithms and methods in intelligent systems in cybernetics. This book constitutes the third volume of the refereed proceedings of the Cybernetics and Algorithms in Intelligent Systems Section of the 7th Computer Science On-line Conference 2018 (CSOC 2018), held online in April 2018.

Securing India in the Cyber Era 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.

Critical Infrastructure Protection IX 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

Progress in Artificial Intelligence This professional guide and reference examines the challenges of assessing security vulnerabilities in computing infrastructure. Various aspects of vulnerability assessment are covered in detail, including recent advancements in reducing the requirement for expert knowledge through novel applications of artificial intelligence. The work also offers a series of case studies on how to develop and perform vulnerability assessment techniques using start-of-the-art intelligent mechanisms. Topics and features: provides tutorial activities and thought-provoking questions in each chapter, together with numerous case studies; introduces the fundamentals of vulnerability assessment, and reviews the state of the art of research in this area; discusses vulnerability assessment frameworks, including frameworks for industrial control and cloud systems; examines a range of applications that make use of artificial intelligence to enhance the vulnerability assessment processes; presents visualisation techniques that can be used to assist the vulnerability assessment process. In addition to serving the needs of security practitioners and researchers, this accessible volume is also ideal for students and instructors seeking a primer on artificial intelligence for vulnerability assessment, or a supplementary text for courses on computer security, networking, and artificial intelligence.

Cybersecurity and Human Rights in the Age of Cyberveillance Cyber security has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new vulnerabilities arise. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications contains a compendium of the latest academic material on new methodologies and applications in the areas of digital security and threats. Including innovative studies on cloud security, online threat protection, and cryptography, this multi-volume book is an ideal source for IT specialists, administrators, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information.

Computer Security 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

Advances in Cybersecurity Management This publication highlights the fast-moving technological advancement and infiltration of Artificial Intelligence into society. Concepts of evolution of society through interconnectivity are explored, together with how the fusion of human and technological interaction leading to Augmented Humanity is fast becoming more than just an endemic phase, but a cultural phase shift to digital societies. It aims to balance both the positive progressive outlooks such developments bring with potential issues that may stem from innovation of this kind, such as the invasive procedures of bio hacking or ethical connotations concerning the usage of digital twins. This publication will also give the reader a good level of understanding on fundamental cyber defence principles, interactions with Critical National Infrastructure (CNI) and the Command, Control, Communications and Intelligence (C3I) decision-making framework. A detailed view of the cyber-attack landscape will be garnered; touching on the tactics, techniques and procedures used, red and blue teaming initiatives, cyber resilience and the protection of larger scale systems. The integration of AI, smart societies, the human-centric approach and Augmented Humanity is discernible in the exponential growth, collection and use of [big] data; concepts woven throughout the diversity of topics covered in this publication; which also discusses the privacy and transparency of data ownership, and the potential dangers of exploitation through social media. As humans are become ever more interconnected, with the prolificacy of smart wearable devices and wearable body area networks, the availability of and abundance of user data and metadata derived from individuals has grown exponentially. The notion of data ownership, privacy and situational awareness are now at the forefront in this new age.