Iec 62443 2 4 Cyber Security Capabilities

This book constitutes the refereed proceedings of the Third International Conference on Reliability, Safety, and Security of Railway Systems, RSSRail 2019, held in Lille, France in June 2019. The 18 full papers presented in this book were carefully reviewed and selected from 38 submissions. They cover a range of topics including railways system and infrastructure advance modelling; scheduling and track planning; safety process and validation; modelling; formal verification; and security.

Biomedical Informatics is now indispensible in modern healthcare, and the field covers a very broad spectrum of research and application outcomes, ranging from cell to population, and including a number of technologies such as imaging, sensors, and biomedical equipment, as well as management and organizational subjects. This book presents 65 full papers and two keynote speeches from the 2017 edition of the International Conference on Informatics, Management, and Technology in Healthcare (ICIMTH 2017), held in Athens, Greece in July 2017. The papers are grouped in three chapters, and cover a wide range of topics, reflecting the current scope of Biomedical Informatics. In essence, Biomedical Informatics empowers the transformation of healthcare, and the book will be of interest to researchers, providers and healthcare practitioners alike.

This book constitutes the proceedings of the 13th IFIP TC 8 International Conference on Computer Information Systems and Industrial Management, CISIM 2014, held in Ho Chi Minh City, Vietnam, in November 2014. The 60 paper presented in this volume were carefully reviewed and selected from 98 submissions. They are organized in topical sections named: algorithms; biometrics and biometrics applications; data analysis and information retrieval; industrial management and other applications; modelling and optimization; networking; pattern recognition and image processing; and various aspects of computer security.

This book constitutes the revised selected papers from the 14th International Conference on Risks and Security of Internet and Systems, CRiSIS 2019, held in Hammamet, Tunisia, in October 2019. The 20 full papers and 4 short papers presented in this volume were carefully reviewed and selected from 64 submissions. They cover diverse research themes that range from classic topics, such as risk analysis and management; access control and permission; secure embedded systems; network and cloud security; information security policy; data protection and machine learning for security; distributed detection system and blockchain.

Advanced Manufacturing and Automation V contains the proceedings of the 5th International Workshop of Advanced Manufacturing and Automation (IWAMA 2015). This meeting continues the success of this important international workshop series and disseminates the works of academic and industrial experts, from around the world, in the areas of advanced manufacturing and automation. The disciplines of manufacturing and automation have attained paramount importance and are vital factors for the maintenance and improvement of the economy of a nation and the quality of life. Manufacturing and automation are advancing at a rapid pace and new technologies are constantly emerging in the fields. The challenges faced by today□s engineers are forcing them to keep on top of the emerging trends through continuous research and development. The papers comprising these proceedings cover various topics including: Robotics and automation; Computational intelligence; Design and optimization; Product life-cycle management; Integration of CAD/CAPP/CAM/CIMS; Advanced manufacturing systems; Manufacturing operations management; Knowledge-based manufacturing; Manufacturing quality control and management; Sustainable production; Diagnosis and prognosis of machines; Lean and agile manufacturing; Virtual and grid manufacturing; Resource and asset management; Logistics and supply chain management; RFID applications; Predictive maintenance; Reliability and maintainability in manufacturing; Project management; Renewable energy development; Environment protection; Intelligent detection.

Concerning application layer DDoS attacks, Bureau 121, camfecting, cyber attack threat trends, ECHELON, Fifth Dimension Operations, Intervasion of the UK, Military-digital complex, PLA Unit 61398, Stuxnet, and more

Explores how the automotive industry can address the increased risks of cyberattacks and incorporate security into the software development lifecycle While increased connectivity and advanced software-based automotive systems provide tremendous benefits and improved user experiences, they also make the modern vehicle highly susceptible to cybersecurity attacks. In response, the automotive industry is investing heavily in establishing cybersecurity engineering processes. Written by a seasoned automotive expert with abundant international industry expertise, Building Secure Cars: Assuring the Software Development Lifecycle introduces readers to various types of cybersecurity activities, measures, and solutions that can be applied at each stage in the typical automotive development process. This book aims to assist auto industry insiders build more secure cars by incorporating key security measures into their software development lifecycle. Readers will learn to better understand common problems and pitfalls in the development process that lead to security vulnerabilities. To overcome such challenges, this book details how to apply and optimize various automated solutions, which allow software development and test teams to identify and fix vulnerabilities in their products quickly and efficiently. This book balances technical solutions with automotive technologies, making implementation practical. Building Secure Cars is: □ One of the first books to explain how the automotive industry can address the increased risks of cyberattacks, and how to incorporate security into the software development lifecycle □ An optimal resource to help improve software security with relevant organizational workflows and technical solutions □ A complete guide that covers introductory information to more advanced and practical topics □ Written by an established professional working at the heart of the automotive industry □ Fully illustrated with tables and visuals, plus real-life problems and suggested solutions to enhance the learning experience This book is written for software development process owners, security policy owners, software developers and engineers, and cybersecurity teams in the automotive industry. All readers will be empowered to improve their organizations security postures by understanding and applying the practical technologies and solutions inside.

This book constitutes the thoroughly refereed papers of the workshops held at the 8th International Conference on New Trends in Model and Data Engineering, MEDI 2018, in Marrakesh, Morocco, in October 2018. The 19 full and the one short workshop papers were carefully reviewed and selected from 50 submissions. The papers are organized according to the 4 workshops: International Workshop on Modeling, Verification and Testing of Dependable Critical Systems, DETECT 2018, Model and Data Engineering for Social Good Workshop, MEDI4SG 2018, Second International Workshop on Cybersecurity and Functional Safety in Cyber-Physical Systems, IWCFS 2018, International Workshop on Formal Model for Mastering Multifaceted Systems, REMEDY 2018.

Critical Information Infrastructures Security
A Guide to Detection and Prevention
Computer Information Systems and Industrial Management
Principles, Modelling and Applications of QRA Studies
Exploring And Implementing Agile Cybersecurity Frameworks and Strategies for Your Organization
□□□ 01□□/2018 □382□
Computer Security
Hearing Before the Committee on Energy and Natural Resources, United States Senate, One Hundred Eleventh Congress, First Session, to Examine the Progress on Smart Grid Initiatives Authorized in the Energy Independence and Security Act of 2007, and Funded in the Stimulus Bill, and to Learn of Opportunities and Impediments to Timely Installation of Smart Grid Technologies, March 3, 2009
From Risk Modelling to Threat Counteraction
ECCWS 2020 20th European Conference on Cyber Warfare and Security
The Specification PEARL Approach
Resilience of Cyber-Physical Systems
Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification

This book introduces the concept of holistic design and development of cyber physical systems to achieve their safe and secure operation. It shows that by following the standards for embedded system's safety and using appropriate hardware and software components inherently safe system's architectures can be devised and certified. While the standards already enable testing and certification of inherently safe and sound hardware, this is still not the case with software. The book demonstrates that Specification PEARL(SPEARL) addresses this issue and proposes appropriate solutions from the viewpoints of software engineering as well as concrete program components. By doing so it reduces the complexity of cyber physical systems design in an innovative way. Three ultimate goals are being followed in the course of defining this new PEARL standard, namely: 1. simplicity over complexity, 2. inherent real-time ability, and 3. conformity to safety integrity and security capability levels.

Cybersecurity for medical devices is no longer optional. We must not allow sensationalism or headlines to drive the discussion… Nevertheless, we must proceed with urgency. In the end, this is about preventing patient harm and preserving patient trust. A comprehensive guide to medical device secure lifecycle management, this is a book for engineers, managers, and regulatory specialists. Readers gain insight into the security aspects of every phase of the product lifecycle, including concept, design, implementation, supply chain, manufacturing, postmarket surveillance, maintenance, updates, and end of life. Learn how to mitigate or completely avoid common cybersecurity vulnerabilities introduced during development and production. Grow your awareness of cybersecurity development topics ranging from high-level concepts to practical solutions and tools. Get insight into emerging regulatory and customer expectations. Uncover how to minimize schedule impacts and accelerate time-to-market while still accomplishing the main goal: reducing patient and business exposure to cybersecurity risks. Medical Device Cybersecurity for Engineers and Manufacturers is designed to help all stakeholders lead the charge to a better medical device security posture and improve the resilience of our medical device ecosystem.

The cost and frequency of cybersecurity incidents are on the rise, is your enterprise keeping pace? The numbers of threats, risk scenarios and vulnerabilities have grown exponentially. Cybersecurity has evolved as a new field of interest, gaining political and societal attention. Given this magnitude, the future tasks and responsibilities associated with cybersecurity will be essential to organizational survival and profitability. This publication applies the COBIT 5 framework and its component publications to transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on business and society are illustrated and put in context. This section shows the rise in cost and frequency of security incidents, including APT attacks and other threats with a critical impact and high intensity. Second, the transformation addresses security governance, security management and security assurance. In accordance with the lens concept within COBIT 5, these sections cover all elements of the systemic transformation and cybersecurity improvements.

This volume constitutes the proceedings of the Second International Conference on Reliability, Safety and Security of Railway Systems, RRSRail 2017, held in Pistoia, Italy, in November 2017. The 16 papers presented in this volume were carefully reviewed and selected from 34 submissions. They are organized in topical sections named: communication challenges in railway systems; formal modeling and verification for safety; light rail and urban transit; and engineering techniques and standards. The book also contains one keynote talk in full-paper length.

BOW-TIE INDUSTRIAL RISK MANAGEMENT ACROSS SECTORS Explore an approachable but rigorous treatment of systematic barrier-based approaches to risk management and failure analysis In Bow-Tie Industrial Risk Management Across Sectors: A Barrier-Based Approach, accomplished researcher and author Luca Fiorentini delivers a practical guide to risk management tools, with a particular emphasis on a systematic barrier-based approach called "bow-tie." The book includes discussions of two barrier-based methods, Bow-Tie and Layers of Protection Analysis (LOPA), for risk assessment, and one barrier-based method for incident analysis, Barrier Failure Analysis (BFA). The author also describes a traditional method–Root Cause Analysis–and three quantitative methods–FMEA/FMECA, Fault Tree (FTA), and Event Tree (ETA) with a discussion about their link with barriers. Written from the ground up to be in full compliance with recent ISO 31000 standards on enterprise risk management, and containing several case studies and examples from a variety of industries, Bow-Tie Industrial Risk Management Across Sectors also contains discussions of international standards dealing with common risks faced by organizations, including occupational health and safety, industrial safety, functional safety, environmental, quality, business continuity, asset integrity, and information security. Readers will also benefit from the inclusion of: A thorough introduction to the Bow-Tie method, including its practical application in risk management workflow from ISO 31000, the history of Bow-Tie, related methods, and the application of Bow-Tie in qualitative and quantitative ways An exploration of Barrier Failure Analysis, including events, timelines, barriers, causation paths, and multi-level causes A practical discussion of how to build a Barrier Failure Analysis, including fact finding, event chaining, identifying barriers, assessing barrier states, causation analysis, and recommendations A concise treatment of Bow-Tie construction workflow, including a step-by-step guide Perfect for engineers and other professionals working in risk management, Bow-Tie Industrial Risk Management Across Sectors: A Barrier-Based Approach will also earn a place in the libraries of advanced undergraduate and graduate students studying risk management and seeking a one-stop reference on the "bow-tie" approach and barrier-based methods.

?????????? Qi???????? ??Qi?? ???(Apple)??????????(Wireless Power Consortium, WPC)????Qi??IHS????2014???????????????5,500????2016?????2.05????????30%~40%?????????????ABI Research?????2020??Qi???????7.13?? ????????????? ?????????????????(?1)??MicroUSB?Type-C??????????DC?? ?????????? ????????1986??http://www.mem.com.tw ??? ??? (??)

This is the first textbook to address quantified risk assessment (QRA) as specifically applied to offshore installations and operations. As the second part of the two-volume updated and expanded fourth edition, it adds a new focus on the recent development of Normally Unattended Installations (NUIs), which are essentially autonomous installations that combine digitalization, big data, drones and machine learning, and can be supported by W2W (walk-to-work) vessels. These minimalistic installations with no helideck and very limited safety systems will require a new approach to risk assessment and emergency planning, especially during manned periods involving W2W vessels. Separate chapters analyse the main hazards for offshore structures: fire, explosion, collision, and falling objects, as well as structural and marine hazards. The book explores possible simplifications of risk assessment for traditional manned installations. Risk mitigation and control are also discussed, as well as how the results of quantitative risk assessment studies should be presented. In closing, the book provides an updated approach to environmental risk assessment. The book offers a comprehensive reference guide for academics and students of marine/offshore risk assessment and management. It will also be of interest to professionals in the industry, as well as contractors, suppliers, consultants and regulatory authorities.

This book constitutes the refereed post-conference proceedings of the 5th International Workshop on Security of Industrial Control Systems and Cyber-Physical Systems, CyberICPS 2019, the Third International Workshop on Security and Privacy Requirements Engineering, SECPRE 2019, the First International Workshop on Security, Privacy, Organizations, and Systems Engineering, SPOSE 2019, and the Second International Workshop on Attacks and Defenses for Internet-of-Things, ADIoT 2019, held in Luxembourg City, Luxembourg, in September 2019, in conjunction with the 24th European Symposium on Research in Computer Security, ESORICS 2019. The CyberICPS Workshop received 13 submissions from which 5 full papers 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 9 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 and to GDPR compliance. The SPOSE Workshop received 7 submissions from which 3 full papers and 1 demo paper were accepted for publication. They demonstrate the possible spectrum for fruitful research at the intersection of security, privacy, organizational science, and systems engineering. From the ADIoT Workshop 5 full papers and 2 short papers out of 16 submissions are included. The papers focus on IoT attacks and defenses and discuss either practical or theoretical solutions to identify IoT vulnerabilities and IoT security mechanisms.

Cyber Security Practitioner's Guide
Bow-Tie Industrial Risk Management Across Sectors
US National Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Developments
Computer Safety, Reliability, and Security
Nuclear Power Plants
Second International Conference, RSSRail 2017, Pistoia, Italy, November 14-16, 2017, Proceedings
Smart Grid Security
13th IFIP TC 8 International Conference, CISIM 2014, Ho Chi Minh City, Vietnam, November 5-7, 2014, Proceedings
A practitioner's guide to securing connected industries
Smart Cities, Green Technologies, and Intelligent Transport Systems
Protecting Our National and Economic Security : Joint Hearing Before the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs, United States Senate, One Hundred Thirteenth Congress, First Session, March 7, 2013
Practice and Theory
MEDI 2018 International Workshops, DETECT, MEDI4SG, IWCFS, REMEDY, Marrakesh, Morocco, October 24–26, 2018, Proceedings

Cybersecurity refers to the measures taken to keep electronic information private and safe from damage or theft. It is also used to make sure these devices and data are not misused. Cybersecurity applies to both software and hardware, as well as information on the Internet, and can be used to protect everything from personal information to complex government systems. Cyber security is a distributed problem partly because of the distributed nature of the underlying infrastructure and partly because industries, government and individuals all come at it with different perspectives. Under these circumstances regulation is best attempted from the bottom up, and legalisation, especially in the area of criminal law, should be sharply focused. There is the need for distributed approaches instead of the more traditional single, concentrated approach. Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, and data from attack, damage, and unauthorized access. Cybersecurity training teaches professionals to spot vulnerabilities, fend off attacks, and immediately respond to emergencies. The spread of modern information technologies has brought about considerable changes in the global environment, ranging from the speed of economic transactions to the nature of social interactions to the management of military operations in both peacetime and war. The development of information technology makes it possible for adversaries to attack each other in new ways and with new forms of damage, and may create new targets for attack. This book fully introduces the theory and practice of cyber security. Comprehensive in scope, it covers applied and practical elements, theory, and the reasons for the design of applications and security techniques. It treats both the management and engineering issues of computer security.

Skillfully navigate through the complex realm of implementing scalable, trustworthy industrial systems and architectures in a hyper-connected business world. Key Features Gain practical insight into security concepts in the Industrial Internet of Things (IIoT) architecture Demystify complex topics such as cryptography and blockchain Comprehensive references to industry standards and security frameworks when developing IIoT blueprints Book Description Securing connected industries and autonomous systems is a top concern for the Industrial Internet of Things (IIoT) community. Unlike cybersecurity, cyber-physical security is an intricate discipline that directly ties to system reliability as well as human and environmental safety. Practical Industrial Internet of Things Security enables you to develop a comprehensive understanding of the entire spectrum of securing connected industries, from the edge to the cloud. This book establishes the foundational concepts and tenets of IIoT security by presenting real-world case studies, threat models, and reference architectures. You ' ll work with practical tools to design risk-based security controls for industrial use cases and gain practical know-how on the multi-layered defense techniques including Identity and Access Management (IAM), endpoint security, and communication infrastructure. Stakeholders, including developers, architects, and business leaders, can gain practical insights in securing IIoT lifecycle processes, standardization, governance and assess the applicability of emerging technologies, such as blockchain, Artificial Intelligence, and Machine Learning, to design and implement resilient connected systems and harness significant industrial opportunities. What you will learn Understand the crucial concepts of a multi-layered IIoT security framework Gain insight on securing identity, access, and configuration management for large-scale IIoT deployments Secure your machine-to-machine (M2M) and machine-to-cloud (M2C) connectivity Build a concrete security program for your IIoT deployment Explore techniques from case studies on industrial IoT threat modeling and mitigation approaches Learn risk management and mitigation planning Who this book is for Practical Industrial Internet of Things Security is for the IIoT community, which includes IIoT researchers, security professionals, architects, developers, and business stakeholders. Anyone who needs to have a comprehensive understanding of the unique safety and security challenges of connected industries and practical methodologies to secure industrial assets will find this book immensely helpful. This book is uniquely designed to benefit professionals from both IT and industrial operations backgrounds.

This book constitutes the refereed proceedings of five workshops co-located with SAFECOMP 2018, the 37th International Conference on Computer Safety, Reliability, and Security, held in V ä ster å s, Sweden, in September 2018. The 28 revised full papers and 21 short papers presented together with 5 introductory papers to each workshop were carefully reviewed and selected from 73 submissions. This year's workshops are: ASSURE 2018 – Assurance Cases for Software-Intensive Systems; DECSoS 2018 – ERCIM/EWICS/ARTEMIS Dependable Smart Embedded and Cyber-Physical Systems and Systems-of-Systems; SASSUR 2018 – Next Generation of System Assurance Approaches for Safety-Critical Systems; STRIVE 2018 – Safety, securiTy, and pRivacy In automotiVe systEms; and WAISE 2018 – Artificial Intelligence Safety Engineering.

In an era of unprecedented volatile political and economic environments across the world, computer-based cyber security systems face ever growing challenges. While the internet has created a global platform for the exchange of ideas, goods and services, it has also created boundless opportunities for cyber crime. The debate over how to plan for the cyber security of the future has focused the minds of developers and scientists alike. This book aims to provide a reference on current and emerging issues on systems security from the lens of autonomy, artificial intelligence and ethics as the race to fight and prevent cyber crime becomes increasingly pressing.

This book offers a systematic explanation of cybersecurity protection of electricity supply facilities, including discussion of related costs, relevant standards, and recent solutions. The author explains the current state of cybersecurity in the electricity market, and cybersecurity standards that apply in that sector. He then offers a systematic approach to cybersecurity management, including new methods of cybersecurity assessment, cost evaluation and comprehensive defence. This monograph is suitable for practitioners, professionals, and researchers engaged in critical infrastructure protection.

This book is a compilation of selected papers from the fifth International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection of Nuclear Power Plant, held in November 2020 in Beijing, China. The purpose of this symposium is to discuss Inspection, test, certification and research for the software and hardware of Instrument and Control (I&C) systems in nuclear power plants (NPP), such as sensors, actuators and control system. It aims to provide a platform of technical exchange and experience sharing for those broad masses of experts and scholars and nuclear power practitioners, and for the combination of production, teaching and research in universities and enterprises to promote the safe development of nuclear power plant. Readers will find a wealth of valuable insights into achieving safer and more efficient instrumentation and control systems.

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.

The Handbook of RAMS in Railway Systems: Theory and Practice addresses the complexity in today's railway systems, which use computers and electromechanical components to increase efficiency while ensuring a high level of safety. RAM (Reliability, Availability, Maintainability) addresses the specifications and standards that manufacturers and operators have to meet. Modeling, implementation, and assessment of RAM and safety requires the integration of railway engineering systems; mathematical and statistical methods; standards compliance; and financial/economic factors. This Handbook brings together a group of experts to present RAM and safety in a modern, comprehensive manner.

The Cybersecurity Partnership Between the Private Sector and Our Government
Certified Arborist Exam
Managing Critical Infrastructure
CYBERWARFARE SOURCEBOOK
A Barrier-Based Approach
Industrial Control Systems Security and Resiliency
Cybersecurity in the Electricity Sector
SAFECOMP 2018 Workshops, ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, V ä ster å s, Sweden, September 18, 2018, Proceedings
Cybersecurity of Industrial Systems
Arborist Certification
Offshore Risk Assessment Vol. 2
Practical Industrial Internet of Things Security
Federal Register

A practical book that will help you defend against malicious activities DESCRIPTION Modern Cybersecurity practices will take you on a journey through the realm of Cybersecurity. The book will have you observe and participate in the complete takeover of the network of Company-X, a widget making company that is about to release a revolutionary new widget that has the competition fearful and envious. The book will guide you through the process of the attack on Company-X's environment, shows how an attacker could use information and tools to infiltrate the companies network, exfiltrate sensitive data and then leave the company in disarray by leaving behind a little surprise for any users to find the next time they open their computer. After we see how an attacker pulls off their malicious goals, the next part of the book will have your pick, design, and implement a security program that best reflects your specific situation and requirements. Along the way, we will look at a variety of methodologies, concepts, and tools that are typically used during the activities that are involved with the design, implementation, and improvement of one's cybersecurity posture. After having implemented a fitting cybersecurity program and kickstarted the improvement of our cybersecurity posture improvement activities we then go and look at all activities, requirements, tools, and methodologies behind keeping an eye on the state of our cybersecurity posture with active and passive cybersecurity monitoring tools and activities as well as the use of threat hunting exercises to find malicious activity in our environment that typically stays under the radar of standard detection methods like firewall, IDS' and endpoint protection solutions. By the time you reach the end of this book, you will have a firm grasp on what it will take to get a healthy cybersecurity posture set up and maintained for your environment. KEY FEATURES - Learn how attackers infiltrate a network, exfiltrate sensitive data and destroy any evidence on their way out - Learn how to choose, design and implement a cybersecurity program that best fits your needs - Learn how to improve a cybersecurity program and accompanying cybersecurity posture by checks, balances and cyclic improvement activities - Learn to verify, monitor and validate the cybersecurity program by active and passive cybersecurity monitoring activities - Learn to detect malicious activities in your environment by implementing Threat Hunting exercises WHAT WILL YOU LEARN - Explore the different methodologies, techniques, tools, and activities an attacker uses to breach a modern company's cybersecurity defenses - Learn how to design a cybersecurity program that best fits your unique environment - Monitor and improve one's cybersecurity posture by using active and passive security monitoring tools and activities. - Build a Security Incident and Event Monitoring (SIEM) environment to monitor risk and incident development and handling. - Use the SIEM and other resources to perform threat hunting exercises to find hidden mayhem WHO THIS BOOK IS FOR This book is a must-read to everyone involved with establishing, maintaining, and improving their Cybersecurity program and accompanying cybersecurity posture. TABLE OF CONTENTS 1. What's at stake 2. Define scope 3.Adhere to a security standard 4. Defining the policies 5. Conducting a gap analysis 6. Interpreting the analysis results 7. Prioritizing remediation 8. Getting to a comfortable level 9. Conducting a penetration test. 10. Passive security monitoring. 11. Active security monitoring. 12. Threat hunting. 13. Continuous battle 14. Time to reflect

This book constitutes revised selected papers from the 13th International Conference on Critical Information Infrastructures Security, CRITIS 2018, held in Kaunas, Lithuania, in September 2018.The 16 full papers and 3 short papers presented were carefully reviewed and selected from 61 submissions. They are grouped in the following topical sections: advanced analysis of critical energy systems, strengthening urban resilience, securing internet of things and industrial control systems, need and tool sets for industrial control system security, and advancements in governance and resilience of critical infrastructures.

These proceedings represent the work of contributors to the 19th European Conference on Cyber Warfare and Security (ECCWS 2020), supported by University of Chester, UK on 25-26 June 2020. The Conference Co-chairs are Dr Thaddeus Eze and Dr Lee Speakman, both from University of Chester and the Programme Chair is Dr Cyril Onwubiko from IEEE and Director, Cyber Security Intelligence at Research Series Limited. ECCWS is a well-established event on the academic research calendar and now in its 19th year the key aim remains the opportunity for participants to share ideas and meet. The conference was due to be held at University of Chester, UK, but due to the global Covid-19 pandemic it was moved online to be held as a virtual event. The scope of papers will ensure an interesting conference. The subjects covered illustrate the wide range of topics that fall into this important and ever-growing area of research.

The landscape of court technology has changed rapidly. As digital tools help facilitate the business and administrative process, multiple entry points for data breaches have also significantly increased in the judicial branch at all levels. Cybersecurity & the Courthouse: Safeguarding the Judicial Process explores the issues surrounding cybersecurity for the court and court systems. This unique resource provides the insight to: Increase your awareness of the issues around cybersecurity Properly defend client and case information Understand the steps needed to mitigate and control the risk of and fallout from a data breach Identify possible pathways to address strengths and weaknesses in individual proceedings as they are presented to the courts Learn how to address the risk of a significant data breach Key Highlights Include: Comprehensive guidance to legal professionals on the growing concerns of cybersecurity within the courts Vital information needed to mitigate and control the risk of and the fallout of a data breach Addresses the issues of data security, and the necessary steps to protect the integrity of the judicial process Provides a roadmap and the steps necessary to protect data in legal cases before the court

This book addresses the latest approaches to holistic Cyber-Physical System (CPS) resilience in real-world industrial applications. Ensuring the resilience of CPSs requires cross-discipline analysis and involves many challenges and open issues, including how to address evolving cyber-security threats. The book describes emerging paradigms and techniques from two main viewpoints: CPSs' exposure to new threats, and CPSs' potential to counteract them. Further, the chapters address topics ranging from risk modeling to threat management and mitigation. The book offers a clearly structured, highly accessible resource for a diverse readership, including graduate students, researchers and industry practitioners who are interested in evaluating and ensuring the resilience of CPSs in both the development and assessment stages. Foreword by Prof. Shiyan Hu, Chair of Cyber-Physical Systems at Linnaeus University, Sweden.

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

The Smart Grid has the potential to revolutionize electricity delivery systems, and the security of its infrastructure is a vital concern not only for cyber-security practitioners, engineers, policy makers, and utility executives, but also for the media and consumers. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid explores the important techniques, challenges, and forces that will shape how we achieve a secure twenty-first century electric grid. Includes a Foreword by Michael Assante, President and CEO, National Board of Information Security Examiners Following an overview of the components of the Smart Grid, the book delves into the evolution of security standards and regulations and examines ways in which the Smart Grid might be regulated. The authors discuss the technical details about how metering technology is being implemented and the likely threats and vulnerabilities that utilities will face. They address the home area network (HAN) and examine distribution and transmission—the foundation for the delivery of electricity, along with distributed generation, micro-grids, and operations. The book explores future concepts—such as energy storage and the use of plug-in electric vehicles (PEVs)—in addition to the concomitant risk for fraud and manipulation with stored energy. Consumer-related issues are discussed as they pertain to emerging ways of receiving and generating energy. The book examines dysfunctions ranging from inadvertent outages to cyber-attack and presents recommendations on how to respond to these incidents. It concludes with speculation of future cyber-security challenges and discusses new ways that the grid can be defended, such as better key management and protection. Written in a style rigorous enough for the practitioner yet accessible to a broad audience, this comprehensive volume covers a topic that is becoming more critical to industry and consumers everywhere.

Papers presented at the 7th in a series of interdisciplinary conferences on safety and security engineering are contained in this book. The papers include the work of engineers, scientists, field researchers, managers and other specialists involved in one or more of the theoretical and practical aspects of safety and security. Safety and Security Engineering, due to its special nature, is an interdisciplinary area of research and application that brings together in a systematic way, many disciplines of engineering, from the traditional to the most technologically advanced. This volume covers topics such as crisis management, security engineering, natural and man-made disasters and emergencies, risk management, and control, protection and mitigation issues. Specific themes include: Risk analysis, assessment and management; System safety engineering; Incident monitoring; Information and communication security; Disaster management; Emergency response; Critical infrastructure protection; Counter terrorism issues; Human factors; Transportation safety and security; Modelling and experiments; Security surveillance systems; Cyber security / E security; Loss prevention; BIM in Safety and Security.

Third International Conference, RSSRail 2019, Lille, France, June 4–6, 2019, Proceedings
Smart Grid Initiatives and Technologies
Safety and Security Engineering VII
Cybersecurity & the Courthouse: Safeguarding the Judicial Process
Engineering Safe and Secure Cyber-Physical Systems
Modern Cybersecurity Practices
Informatics Empowers Healthcare Transformation
Transforming Cybersecurity: Using COBIT 5
New Trends in Model and Data Engineering
Innovative Technologies for Instrumentation and Control Systems : the Fifth International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection of Nuclear Power Plant (ISNPP)
Medical Device Cybersecurity for Engineers and Manufacturers
9th International Conference, SMARTGREENS 2020, and 6th International Conference, VEHITS 2020, Prague, Czech Republic, May 2-4, 2020, Revised Selected Papers
Risks and Security of Internet and Systems

Cybersecurity in the Electricity SectorManaging Critical InfrastructureSpringer Nature

This book includes extended and revised selected papers from the 9th International Conference on Smart Cities and Green ICT Systems, SMARTGREENS 2020, and the 6th International Conference on Vehicle Technology and Intelligent Transport Systems, VEHITS 2020, held in Prague, Czech Republic, in May 2020. The 30 full papers presented during SMARTGREENS and VEHITS 2020 were carefully reviewed and selected from the 117 submissions. The papers present research on advances and applications in the fiels of smart cities, electric vehicles, sustainable computing and communications, energy aware systems and technologies, intelligent vehicle technologies, intelligent transport systems and infrastructure, connected vehicles.

Learn how to detect and prevent the hacking of medical equipment at hospitals and healthcare facilities. A cyber-physical attack on building equipment pales in comparison to the damage a determined hacker can do if he/she gains access to a medical-grade network as a medical-grade network controls the diagnostic, treatment, and life support equipment on which lives depend. News reports inform us how hackers strike hospitals with ransomware that prevents staff from accessing patient records or scheduling appointments. Unfortunately, medical equipment also can be hacked and shut down remotely as a form of extortion. Criminal hackers will not ask for a $500 payment to unlock an MRI, PET or CT scan, or X-ray machine—they will ask for much more. Litigation is bound to follow and the resulting punitive awards will drive up hospital insurance costs and healthcare costs in general. This will undoubtedly result in increased regulations for hospitals and higher costs for compliance. Unless hospitals and other healthcare facilities take the steps necessary to secure their medical-grade networks, they will be targeted for cyber-physical attack, possibly with life-threatening consequences. Cybersecurity for Hospitals and Healthcare Facilities is a wake-up call explaining what hackers can do, why hackers would target a hospital, the way hackers research a target, ways hackers can gain access to a medical-grade network (cyber-attack vectors), and ways hackers hope to monetize their cyber-attack. By understanding and detecting the threats, you can take action now—before your hospital becomes the next victim. What You Will Learn: Determine how vulnerable hospital and healthcare building equipment is to cyber-physical attack Identify possible ways hackers can hack hospital and healthcare

facility equipment Recognize the cyber-attack vectors—or paths by which a hacker or cracker can gain access to a computer, a medical-grade network server, or expensive medical equipment in order to deliver a payload or malicious outcome Detect and prevent man-in-the-middle or denial-of-service cyber-attacks Find and prevent hacking of the hospital database and hospital web application Who This Book Is For: Hospital administrators, healthcare professionals, hospital & healthcare facility engineers and building managers, hospital & healthcare facility IT professionals, and HIPAA professionals

US National Cyber Security Strategy and Programs Handbook - Strategic Information and Developments

This practice test includes 216 multiple choice test questions about Certified Arborist Exam. The test has been carefully developed to assist you to pass your actual test. It will help you prepare for and pass your exam on the first attempt but it does not include any study guide. The book focuses only on carefully selected practice questions. Two main topics; TREES and OTHER ISSUES are covered in this test. TREES questions focus on; #9642 Tree Biology #9642 Tree Protection #9642 Tree Risk Management #9642 Pruning #9642 Urban Foresty #9642 Diagnosis & Treatment OTHER ISSUES questions focus on; #9642 Soil Management #9642 Safe Work Practices #9642 Identification & Selection #9642 Installation & Establishment

Cyber Security

Building Secure Cars

Digital Transformation, Cyber Security and Resilience of Modern Societies

13th International Conference, CRITIS 2018, Kaunas, Lithuania, September 24-26, 2018, Revised Selected Papers

Advanced Manufacturing and Automation V

Cybersecurity for Hospitals and Healthcare Facilities

Assuring the Automotive Software Development Lifecycle

Theory and Practice

Handbook of RAMS in Railway Systems

An End-to-End View of Security in the New Electrical Grid

14th International Conference, CRISIS 2019, Hammamet, Tunisia, October 29-31, 2019, Proceedings

ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, September 26-27, 2019 Revised Selected Papers