Cyber Security Assessment Of Industrial Control Systems
7b609e7a558c1022770def817fcbff5e

Protecting Industrial Control Systems from Electronic Threats
Cybersecurity of Industrial Systems
Cyber-Physical Systems: Industry 4.0 Challenges
Industrial Internet
Cyber-security of SCADA and Other Industrial Control Systems
Physical Security in the Process Industry
Trusted Computing and Information Security
Information Security Applications
Industrial Cybersecurity
A Guide to Innovative Public-Private Partnerships
Critical Infrastructure Risk Assessment
Department of Homeland Security Appropriations for 2014
Cybersecurity for Industrial Control Systems
Security of Industrial Control Systems and Cyber Physical Systems
Resilience of Cyber-Physical Systems
Hacking Exposed Industrial Control Systems: ICS and SCADA Security
Secrets & Solutions
Industrial Network Security
Industrial Cybersecurity
Hands-On Industrial Internet of Things
CYBER SECURITY ANALYSIS USING POLICIES & PROCEDURES
Industrial Network Security
Intelligent Computing and Internet of Things

Get up and running with industrial cybersecurity monitoring with this hands-on book, and explore ICS cybersecurity monitoring tasks, activities, tools, and best practices Key Features Architect, design, and build ICS networks with security in mind Perform a variety of security assessments, checks, and verifications Ensure that your security processes are effective, complete, and relevant Book Description With Industrial Control Systems (ICS) expanding into traditional IT space and even into the cloud, the attack surface of ICS environments has increased significantly, making it crucial to recognize your ICS vulnerabilities and implement advanced techniques for monitoring and defending against rapidly evolving cyber threats to critical infrastructure. This second edition covers the updated Industrial Demilitarized Zone (IDMZ) architecture and shows you how to implement, verify, and monitor a holistic security program for your ICS environment. You'll begin by learning how to design security-oriented architecture that allows you to implement the tools, techniques, and activities covered in this book effectively and easily. You'll get to grips with the monitoring, tracking, and trending (visualizing) and procedures of ICS cybersecurity risks as well as understand the overall security program and posture/hygiene of the ICS environment. The book then introduces you to threat hunting principles, tools, and techniques to help you identify malicious activity successfully. Finally, you'll work with incident response and incident recovery tools and techniques in an ICS environment. By the end of this book, you'll have gained a solid understanding of industrial cybersecurity monitoring, assessments, incident response activities, as well as threat hunting. What you will learn Monitor the ICS security posture actively as well as passively Respond to incidents in a controlled and standard way Understand what incident response activities are required in your ICS environment Perform threat-hunting exercises using the Elasticsearch, Logstash, and Kibana (ELK) stack Assess the overall effectiveness of your ICS cybersecurity program Discover tools, techniques, methodologies, and activities to perform risk assessments for your ICS environment Who this book is for If you are an ICS security professional or anyone curious about ICS cybersecurity for extending, improving, monitoring, and validating your ICS cybersecurity posture, then this book is for you. IT/OT professionals interested in entering the ICS cybersecurity monitoring domain or searching for additional learning material for different industry-leading cybersecurity certifications will also find this book useful.
This book deals with the state-of-the-art of physical security knowledge and research in the chemical and process industries. Legislation differences between Europe and the USA are investigated, followed by an overview of the how, what and why of contemporary security risk assessment in this particular industrial sector. Innovative solutions such as attractiveness calculations and the use of game theory, advancing the present science of adversarial risk analysis, are discussed. The book further stands up for developing and employing dynamic security risk assessments, for instance based on Bayesian networks, and using OR methods to truly move security forward in the chemical and process industries.

This book constitutes the proceedings of the 21st International Conference on Information Security, ISC 2018, held in Guildford, UK, in September 2018. The 26 full papers presented in this volume were carefully reviewed and selected from 59 submissions. The book also includes one invited talk in full-paper length. The papers were organized in topical sections named: software security; symmetric ciphers and cryptanalysis; data privacy and anonymization; outsourcing and assisted computing; advanced encryption; privacy-preserving applications; advanced signatures; and network security.

Internet provided us unlimited options by enabling us with constant & dynamic information that changes every single minute through sharing of information across the globe many organizations rely on information coming & going out from their network Security of the information shared on the global. Networks give birth to the need of the cyber security. Cyber security means the security of the information residing in your cyberspace from unwanted & unauthorized persons. Through different-different policies & procedures we can prevent our information from both locally & globally active invaders (Hackers). Cyber security is a proactive step to prevent data assets. The policies & procedures, helps us to assess off activeness & ineffectiveness of the security maintained so far by the organizations. Policies & procedures ensures that a standalone PC & a networked PC can be provided in a very off active manner. This Thesis describes the methodologies & techniques involved in policies & procedures along with its benefits & precision. The main objective of the proposed work is to lay down a secure & authentic network so that no intruder can gain unauthorized access. The proposed technique concentrates and supports to the basic security principle like authorization, integrity, dynamization and confidentiality during analysis and implementation of the whole process. The level of security & its implementation requires skills & proper monitoring of the system as a whole. Thesis aims at creating a security mesh to explain the importance of computer security to different organizations.

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

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.

This book provides an overview of state-of-the-art research on “Systems and Optimization Aspects of Smart Grid Challenges.” The authors have compiled and integrated different aspects of applied systems optimization research to smart grids, and also describe some of its critical challenges and requirements. The promise of a smarter electricity grid could significantly change how consumers use and pay for their electrical power, and could fundamentally reshape the current Industry. Gaining increasing interest and acceptance, Smart Grid technologies combine power generation and delivery systems with advanced communication systems to help save energy, reduce energy costs and improve reliability. Taken together, these technologies support new approaches for load balancing and power distribution, allowing optimal runtime power routing and cost management. Such unprecedented capabilities, however, also present a set of new problems and challenges at the technical and regulatory levels that must be addressed by Industry and the Research Community.

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

This book enables organizations in both the private and public sectors to develop and execute efficient and effective business partnerships. Detailed requirements and market potentials are developed which would help entice the private sector to use its own resources to develop products and services without delay and at minimal cost to taxpayers. This is a 'must read' for anyone interested in doing business with the government as well as government leaders who are being forced to trim budgets and show genuine value in their agencies.

This book constitutes the refereed proceedings of the Chinese Conference on Trusted Computing and Information Security, CTCIS 2019, held in Shanghai, China, in October 2019. The 22 revised full papers presented were carefully reviewed and selected from 247 submissions. The papers are centered around cryptography, systems security, trusted computing, information security, network security, information hiding.

This six volume set LNCS 11063 – 11068 constitutes the thoroughly refereed conference proceedings of the 4th International Conference on Cloud Computing and Security, ICCCS 2018, held in Haikou, China, in June 2018. The 386 full papers of these six volumes were carefully reviewed and selected from 1743 submissions. The papers cover ideas and achievements in the theory and practice of all areas of inventive systems which includes control, artificial intelligence, automation systems, computing systems, electrical and informative systems. The six volumes are arranged according to the
subject areas as follows: cloud computing, cloud security, encryption, information hiding, IoT security, multimedia forensics

This part of GB/T 30976 specifies the objectives, assessment contents and implementation process of the information security assessment of industrial control systems (SCADA, DCS, PLC, PCS, etc.). This part applies to system designers, equipment manufacturers, system integrators, engineering companies, users, asset owners, and assessment and certification agencies to perform assessment against the information security of the industrial control systems.

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

Physical Security in the Process Industry: Theory with Applications deals with physical security in the field of critical infrastructures where hazardous materials are a factor, along with the state-of-the-art thinking and modeling methods for enhancing physical security. The book offers approaches based on scientific insights, mainly addressing terrorist attacks. Moreover, the use of innovative techniques is explained, including Bayesian networks, game-theory and petri-networks. Dealing with economic parameters and constraints and calculating the costs and benefits of security measures are also included. The book will be of interest to security (and safety) scientists, security managers and the public at large. Discusses how to achieve inherent physical security using a scientific approach Explores how to take adequate add-on physical security measures Covers risk assessment tools and applications for practical use in the industry Demonstrates how to optimize security decisions using security models and approaches Considers economic aspects of security decisions

This book explains the key feature to develop a complex and stable network that helps to gather the data to optimize the asset performance and maximize the production in the Industries leveraging on the cloud infrastructure and services. By the end, you can design the Industrial IoT network and the architecture for processing its data in the cloud.

This book introduces readers to cybersecurity and its impact on the realization of the Industry 4.0 vision. It covers the technological foundations of cybersecurity within the scope of the Industry 4.0 landscape and details the existing cybersecurity threats faced by Industry 4.0, as well as state-of-the-art solutions with regard to both academic research and practical implementations. Industry 4.0 and its associated technologies, such as the Industrial Internet of Things and cloud-based design and manufacturing systems are examined, along with their disruptive innovations. Further, the book analyzes how these phenomena capitalize on the economies of scale provided by the Internet. The book offers a valuable resource for practicing engineers and decision makers in industry, as well as researchers in the design and manufacturing communities and all those interested in Industry 4.0 and cybersecurity.
This book provides a brief and general introduction to cybersecurity and cyber-risk assessment. Not limited to a specific approach or technique, its focus is highly pragmatic and is based on established international standards (including ISO 31000) as well as industrial best practices. It explains how cyber-risk assessment should be conducted, which techniques should be used when, what the typical challenges and problems are, and how they should be addressed. The content is divided into three parts. First, part I provides a conceptual introduction to the topic of risk management in general and to cybersecurity and cyber-risk management in particular. Next, part II presents the main stages of cyber-risk assessment from context establishment to risk treatment and acceptance, each illustrated by a running example. Finally, part III details four important challenges and how to reasonably deal with them in practice: risk measurement, risk scales, uncertainty, and low-frequency risks with high consequence. The target audience is mainly practitioners and students who are interested in the fundamentals and basic principles and techniques of security risk assessment, as well as lecturers seeking teaching material. The book provides an overview of the cyber-risk assessment process, the tasks involved, and how to complete them in practice.

As industrial control systems (ICS), including SCADA, DCS, and other process control networks, become Internet-facing, they expose crucial services to attack. Threats like Duqu, a sophisticated worm found in the wild that appeared to share portions of its code with the Stuxnet worm, emerge with increasing frequency. Explaining how to develop and implement an effective cybersecurity program for ICS, Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS provides you with the tools to ensure network security without sacrificing the efficiency and functionality of ICS. Highlighting the key issues that need to be addressed, the book begins with a thorough introduction to ICS. It discusses business, cost, competitive, and regulatory drivers and the conflicting priorities of convergence. Next, it explains why security requirements differ from IT to ICS. It differentiates when standard IT security solutions can be used and where SCADA-specific practices are required. The book examines the plethora of potential threats to ICS, including hi-jacking malware, botnets, spam engines, and porn dialers. It outlines the range of vulnerabilities inherent in the ICS quest for efficiency and functionality that necessitates risk behavior such as remote access and control of critical equipment. Reviewing risk assessment techniques and the evolving risk assessment process, the text concludes by examining what is on the horizon for ICS security, including IPv6, ICSv6 test lab designs, and IPv6 and ICS sensors.

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.

This book constitutes the thoroughly refereed proceedings of the 15th International Workshop on Information Security Applications, WISA 2014, held on Jeju Island, Korea, in August 2014. The 30 revised full papers presented in this volume were carefully reviewed and selected from 69 submissions. The papers are organized in topical sections such as malware detection; mobile security; vulnerability analysis; applied cryptography; network security; cryptography; hardware security; and critical infrastructure security and policy.

This book discusses the birth and background of the Industrial Internet, clarifying its definition and structure, and reviewing the related development trends in China and around the globe, mainly in terms of policies, networks, platforms, security, application and standards. Lastly, it provides insights into the integration of the Industrial Internet with a series of next-gen information technologies, such as time sensitive networking, 5G, edge computing, blockchain...
and artificial intelligence. Intended for researchers and industrial practitioners who have been following the evolution of and trends in the Industrial Internet, the book is also a valuable reference resource for practitioners, scholars, and technical and engineering managers at various levels and in various fields.

This book offers the first benchmarking study of China’s response to the problems of security in cyber space. There are several useful descriptive books on cyber security policy in China published between 2010 and 2016. As a result, we know quite well the system for managing cyber security in China, and the history of policy responses. What we don’t know so well, and where this book is useful, is how capable China has become in this domain relative to the rest of the world. This book is a health check, a report card, on China’s cyber security system in the face of escalating threats from criminal gangs and hostile states. The book also offers an assessment of the effectiveness of China’s efforts. It lays out the major gaps and shortcomings in China’s cyber security policy. It is the first book to base itself around an assessment of China’s cyber industrial complex, concluding that China does not yet have one. As Xi Jinping said in July 2016, the country’s core technologies are dominated by foreigners.

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.

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.

Cyber Security Management: A Governance, Risk and Compliance Framework by Peter Trim and Yang-Im Lee has been written for a wide audience. Derived from research, it places security management in a holistic context and outlines how the strategic marketing approach can be used to underpin cyber security in partnership arrangements. The book is unique because it integrates material that is of a highly specialized nature but which can be interpreted by those with a non-specialist background in the area. Indeed, those with a limited knowledge of cyber security will be able to develop a comprehensive understanding of the subject and will be guided into devising and implementing relevant policy, systems and procedures that make the organization better able to withstand the increasingly sophisticated forms of cyber attack. The book includes a sequence-of-events model; an organizational governance framework; a business continuity management planning framework; a multi-cultural communication model; a cyber security management model and strategic management framework; an integrated governance mechanism; an integrated resilience management model; an integrated management model and system; a communication risk management strategy; and recommendations for counteracting a range of cyber threats.

Cyber Security Management: A Governance, Risk and Compliance Framework simplifies complex material and provides a multi-disciplinary perspective and an explanation and interpretation of how managers can manage cyber threats in a pro-active manner and work towards counteracting cyber threats.
both now and in the future.

The three-volume set CCIS 923, CCIS 924, and CCIS 925 constitutes the thoroughly refereed proceedings of the First International Conference on Intelligent Manufacturing and Internet of Things, and of the 5th International Conference on Intelligent Computing for Sustainable Energy and Environment, ICSEE 2018, held in Chongqing, China, in September 2018. The 135 revised full papers presented were carefully reviewed and selected from over 385 submissions. The papers of this volume are organized in topical sections on: digital manufacturing; industrial product design; logistics, production and operation management; manufacturing material; manufacturing optimization; manufacturing process; mechanical transmission system; robotics.

The two-volume set, LNCS 11098 and LNCS 11099 constitutes the refereed proceedings of the 23nd European Symposium on Research in Computer Security, ESORICS 2018, held in Barcelona, Spain, in September 2018. The 56 revised full papers presented were carefully reviewed and selected from 283 submissions. The papers address issues such as software security, blockchain and machine learning, hardware security, attacks, malware and vulnerabilities, protocol security, privacy, CPS and IoT security, mobile security, database and web security, cloud security, applied crypto, multi-party computation, SDN security.

As a manager or engineer have you ever been assigned a task to perform a risk assessment of one of your facilities or plant systems? What if you are an insurance inspector or corporate auditor? Do you know how to prepare yourself for the inspection, decided what to look for, and how to write your report? This is a handbook for junior and senior personnel alike on what constitutes critical infrastructure and risk and offers guides to the risk assessor on preparation, performance, and documentation of a risk assessment of a complex facility. This is a definite “must read” for consultants, plant managers, corporate risk managers, junior and senior engineers, and university students before they jump into their first technical assignment.

This book constitutes the refereed proceedings of the First Conference on Cybersecurity of Industrial Control Systems, CyberICS 2015, and the First Workshop on the Security of Cyber Physical Systems, WOS-CPS 2015, held in Vienna, Austria, in September 2015 in conjunction with ESORICS 2015, the 20th annual European Symposium on Research in Computer Security. The 6 revised full papers and 2 short papers of CyberICS 2015 presented together with 3 revised full papers of WOS-CPS 2015 were carefully reviewed and selected from 28 initial submissions. CyberICS 2015 focuses on topics covering ICSs, including cyber protection and cyber defense of SCADA systems, plant control systems, engineering workstations, substation equipment, programmable logic controllers, PLCs, and other industrial control system. WOS-CPS 2015 deals with the Security of Cyber Physical Systems, that exist everywhere around us, and range in size, complexity and criticality, from embedded systems used in smart vehicles, to SCADA systems in smart grids to control systems in water distribution systems, to smart transportation systems etc.

This book is an important outcome of the Fifth World Internet Conference. It provides a comprehensive review of China’s Internet development, especially the new practice and achievement in 2018. And it offers a systematic account of China’s experience in Internet development and governance. This year, the book improves China’s Internet Development Index System, optimizes the algorithm model, and enhances data collection, to assess and reflect Internet development more comprehensively, objectively and scientifically.
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.

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

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.

This book presents new findings in industrial cyber-physical system design and control for various domains, as well as their social and economic impacts on society. Industry 4.0 requires new approaches in the context of secure connections, control, and maintenance of cyber-physical systems as well as enhancing their interaction with humans. The book focuses on open issues of cyber-physical system control and its usage, discussing implemented breakthrough systems, models, programs, and methods that could be used in industrial processes for the control, condition assessment, diagnostics, prognostication, and proactive maintenance of cyber-physical systems. Further, it addresses the topic of ensuring the cybersecurity of industrial cyber-physical systems and proposes new, reliable solutions. The authors also examine the impact of university courses on the performance of industrial complexes, and the organization of education for the development of cyber-physical systems. The book is intended for practitioners, enterprise
representatives, scientists, students, and Ph.D. and master’s students conducting research in the area of cyber-physical system development and implementation in various domains.

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.

Copyright code: 7b609e7a558c1022770def817fcbff5e