Tutorial Industrial Information System Security Part 2

Eventually, you will enormously discover a other experience and finishing by spending more cash. nevertheless when? do you admit that you require to get those every needs taking into account having significantly cash? Why dont you attempt to acquire something basic in the beginning? Thats something that will lead you to understand even more not far off from the globe, experience, some places, similar to history, amusement, and a lot more?

It is your entirely own mature to proceed reviewing habit. in the midst of guides you could enjoy now is **Tutorial Industrial Information System Security Part 2** below.

GB, GB/T, GBT - Product Catalog. Translated English of Chinese Standard (All national standards GB, GB/T, GBT, GBZ) - https://www.chinesestandard.net 2018-01-01
This document provides the comprehensive list of Chinese National Standards - Category: GB; GB/T, GBT.

Cybersecurity Program Development for Business - Chris Moschovitis 2018-04-06
"This is the book executives have been waiting for. It is clear: With deep expertise but in nontechnical language, it describes what cybersecurity risks are and the decisions executives need to make to address them. It is crisp: Quick and to the point, it doesn't waste words and won't waste your time. It is candid: There is no sure cybersecurity defense, and Chris Moschovitis doesn't pretend there is; instead, he tells you how to understand your company's risk and make smart business decisions about what you can mitigate and what you cannot. It is also, in all likelihood, the only book ever written (or ever to be written) about cybersecurity defense that is fun to read." —Thomas A. Stewart, Executive Director, National Center for the Middle Market and Co-Author of Woo, Wow, and Win: Service Design, Strategy, and the Art of Customer Delight Get answers to all your cybersecurity questions In 2016, we reached a tipping point—a moment where the global and local implications of cybersecurity became undeniable. Despite the seriousness of the topic, the term "cybersecurity" still exasperates many people. They feel terrorized and overwhelmed. The majority of business people have very little understanding of cybersecurity, how to manage it, and what's really at risk. This essential guide, with its dozens of examples and case studies, breaks down every element of the development and management of a cybersecurity program for the executive. From understanding the need, to core risk management principles, to threats, tools, roles and responsibilities, this book walks the reader through each step of developing and implementing a cybersecurity program. Read cover-to-cover, it’s a thorough overview, but it can also function as a useful reference book as individual questions and difficulties arise. Unlike other cybersecurity books, the text is not bogged down with industry jargon Speaks specifically to the executive who is not familiar with the development or implementation of cybersecurity programs Shows you how to make pragmatic, rational, and informed decisions for your organization Written by a top-flight technologist with decades of experience and a track record of success If you’re a business manager or executive who needs

to make sense of cybersecurity, this book demystifies it for you.

CISSP: Certified Information Systems Security Professional Study Guide - James Michael Stewart 2012-07-10

Fully updated Sybex Study Guide for the industry-leading security certification: CISSP Security professionals consider the Certified Information Systems Security Professional (CISSP) to be the most desired certification to achieve. More than 200,000 have taken the exam, and there are more than 70,000 CISSPs worldwide. This highly respected guide is updated to cover changes made to the CISSP Body of Knowledge in 2012. It also provides additional advice on how to pass each section of the exam. With expanded coverage of key areas, it also includes a full-length, 250-question practice exam. Fully updated for the 2012 CISSP Body of Knowledge, the industry-leading standard for IT professionals Thoroughly covers exam topics, including access control, application development security, business continuity and disaster recovery planning, cryptography, operations security, and physical (environmental) security Examines information security governance and risk management, legal regulations, investigations and compliance, and telecommunications and network security Features expanded coverage of biometrics, auditing and accountability, software security testing, and many more key topics CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition prepares you with both the knowledge and the confidence to pass the CISSP exam.

Information Technology Risk Management in Enterprise Environments - Jake Kouns 2011-10-04

Discusses all types of corporate risks and practical means of defending against them. Security is currently identified as a critical area of Information Technology management by a majority of government, commercial, and industrial organizations. Offers an effective risk management program, which is the most critical function of an information security program.

Medical Device Cybersecurity for Engineers and Manufacturers - Axel Wirth 2020-08-31

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.

Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection - Laing, Christopher 2012-12-31

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.

Managerial Guide for Handling Cyber-terrorism and Information Warfare - Lech Janczewski 2005-01-01

"This book presents IT managers with what cyberterrorism and information warfare is and how to handle the problems associated with them"--Provided by publisher.

Official (ISC)2 Guide to the CISSP CBK - Steven Hernandez CISSP 2009-12-22

With each new advance in connectivity and convenience comes a new wave of threats to privacy and security capable of destroying a company's reputation, violating a consumer's privacy, compromising intellectual property, and in some cases endangering personal safety. This is why it is essential for information security professionals to stay up to da

Information Systems Security - Vinod Ganapathy 2018-12-10

This book constitutes the refereed proceedings of the 14th International Conference on Information Systems Security, ICISS 2018, held in Bangalore, India, in December 2018.The 23 revised full papers presented in this book together with 1 invited paper and 3 keynote abstracts were carefully reviewed and selected from 51 submissions. The papers are organized in the following topical sections: security for ubiquitous computing; modelling and anaylsis of attacks; smartphone security; cryptography and theory; enterprise and cloud security; machine learning and security; privacy; and client security and authentication.

Effective Cybersecurity - William Stallings 2018-07-20

The Practical, Comprehensive Guide to Applying Cybersecurity Best Practices and Standards in Real Environments In Effective Cybersecurity, William Stallings introduces the technology, operational procedures, and management practices needed for successful cybersecurity. Stallings makes extensive use of standards and best practices documents that are often used to guide or mandate cybersecurity implementation. Going beyond these, he offers in-depth tutorials on the “how” of implementation, integrated into a unified framework and realistic plan of action. Each chapter contains a clear technical overview, as well as a detailed discussion of action items and appropriate policies. Stallings offers many pedagogical features designed to help readers master the material: clear learning objectives, keyword lists, review questions, and QR codes linking to relevant standards documents and web resources. Effective Cybersecurity aligns with the comprehensive Information Security Forum document “The Standard of Good Practice for Information Security,” extending ISF’s work with extensive insights from ISO, NIST, COBIT, other official standards and guidelines, and modern professional, academic, and industry literature. • Understand the cybersecurity discipline and the role of standards and best practices • Define security governance, assess risks, and manage strategy and tactics • Safeguard information and privacy, and ensure GDPR compliance • Harden systems across the system development life cycle (SDLC) • Protect servers, virtualized systems, and storage • Secure networks and electronic communications, from email to VoIP • Apply the most appropriate methods for user authentication • Mitigate security risks in supply chains and cloud environments This knowledge is indispensable to every cybersecurity professional. Stallings presents it systematically and coherently, making it practical and actionable.

Industrial Communication Technology Handbook - Richard Zurawski 2017-12-19

Featuring contributions from major technology vendors, industry consortia, and government and private research establishments, the Industrial Communication Technology Handbook, Second Edition provides comprehensive and authoritative coverage of wire- and

wireless-based specialized communication networks used in plant and factory automation, automotive applications, avionics, building automation, energy and power systems, train applications, and more. New to the Second Edition: 46 brand-new chapters and 21 substantially revised chapters Inclusion of the latest, most significant developments in specialized communication technologies and systems Addition of new application domains for specialized networks The Industrial Communication Technology Handbook, Second Edition supplies readers with a thorough understanding of the application-specific requirements for communication services and their supporting technologies. It is useful to a broad spectrum of professionals involved in the conception, design, development, standardization, and use of specialized communication networks as well as academic institutions engaged in engineering education and vocational training.

Security for Service Oriented Architectures - Walter Williams 2014-04-24

Although integrating security into the design of applications has proven to deliver resilient products, there are few books available that provide guidance on how to incorporate security into the design of an application. Filling this need, Security for Service Oriented Architectures examines both application and security architectures and illustrates the relationship between the two. Supplying authoritative guidance on how to design distributed and resilient applications, the book provides an overview of the various standards that service oriented and distributed applications leverage, including SOAP, HTML 5, SAML, XML Encryption, XML Signature, WS-Security, and WS-SecureConversation. It examines emerging issues of privacy and discusses how to design applications within a secure context to facilitate the understanding of these technologies you need to make intelligent decisions regarding their design. This complete guide to security for web services and SOA considers the malicious user story of the abuses and attacks against applications as examples of how design flaws and oversights have subverted the goals of providing resilient business functionality. It reviews recent research on access control for simple and conversation-based web services, advanced digital identity management techniques, and access control for web-based workflows. Filled with illustrative examples and analyses of critical issues, this book provides both security and software architects with a bridge between software and service-oriented architectures and security architectures, with the goal of providing a means to develop software architectures that leverage security architectures. It is also a reliable source of reference on Web services standards. Coverage includes the four types of architectures, implementing and securing SOA, Web 2.0, other SOA platforms, auditing SOAs, and defending and detecting attacks.

Fundamentals of Information Security - Sanil Nadkarni 2021-01-06

An Ultimate Guide to Building a Successful Career in Information Security KEY FEATURES ¥Understand the basics and essence of Information Security. ¥Understand why Information Security is important. ¥Get tips on how to make a career in Information Security. ¥Explore various domains within Information Security. ¥Understand different ways to find a job in this field. DESCRIPTIONÊÊ The book starts by introducing the fundamentals of Information Security. You will deep dive into the concepts and domains within Information Security and will explore the different roles in Cybersecurity industry. The book includes a roadmap for a technical and non-technical student who want to make a career in Information Security. You will also understand the requirement, skill and competency required for each role. The book will help you sharpen your soft skills required in the Information Security domain. The book will help you with ways and means to apply for jobs and will share

tips and tricks to crack the interview.ÊÊ This is a practical guide will help you build a successful career in Information Security. WHAT YOU WILL LEARNÊ ¥Understand how to build and expand your brand in this field. ¥Explore several domains in Information Security. ¥Review the list of top Information Security certifications. ¥Understand different job roles in Information Security. ¥Get tips and tricks that will help you ace your job interview. WHO THIS BOOK IS FORÊ Ê The book is for anyone who wants to make a career in Information Security. Students, aspirants and freshers can benefit a lot from this book. TABLE OF CONTENTS 1. Introduction to Information Security 2. Domains in Information Security 3. Information Security for non-technical professionals 4. Information Security for technical professionals 5.Ê Skills required for a cybersecurity professional 6. How to find a job 7. Personal Branding

Building an Effective Security Program for Distributed Energy Resources and Systems - Mariana Hentea 2021-04-06 Building an Effective Security Program for Distributed Energy Resources and Systems Build a critical and effective security program for DERs Building an Effective Security Program for Distributed Energy Resources and Systems requires a unified approach to establishing a critical security program for DER systems and Smart Grid applications. The methodology provided integrates systems security engineering principles, techniques, standards, and best practices. This publication introduces engineers on the design, implementation, and maintenance of a security program for distributed energy resources (DERs), smart grid, and industrial control systems. It provides security professionals with understanding the specific requirements of industrial control systems and real-time constrained applications for power systems. This book: Describes the cybersecurity needs for DERs and power grid as critical infrastructure Introduces the information security principles to assess and manage the security and privacy risks of the emerging Smart Grid technologies Outlines the functions of the security program as well as the scope and differences between traditional IT system security requirements and those required for industrial control systems such as SCADA systems Offers a full array of resources— cybersecurity concepts, frameworks, and emerging trends Security Professionals and Engineers can use Building an Effective Security Program for Distributed Energy Resources and Systems as a reliable resource that is dedicated to the essential topic of security for distributed energy resources and power grids. They will find standards, guidelines, and recommendations from standards organizations, such as ISO, IEC, NIST, IEEE, ENISA, ISA, ISACA, and ISF, conveniently included for reference within chapters.

Document Retrieval Index - 1976

Software Engineering and Computer Systems, Part II - Jasni Mohamad Zain 2011-06-28

This Three-Volume-Set constitutes the refereed proceedings of the Second International Conference on Software Engineering and Computer Systems, ICSECS 2011, held in Kuantan, Malaysia, in June 2011. The 190 revised full papers presented together with invited papers in the three volumes were carefully reviewed and selected from numerous submissions. The papers are organized in topical sections on software engineering; network; bioinformatics and e-health; biometrics technologies; Web engineering; neural network; parallel and distributed e-learning; ontology; image processing; information and data management; engineering; software security; graphics and multimedia; databases; algorithms; signal processing; software design/testing; e- technology; ad hoc networks; social networks; software process modeling; miscellaneous topics in software engineering and computer systems.

Practical Industrial Internet of Things Security - Sravani Bhattacharjee 2018-07-30

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.

Formal Methods and Software Engineering - Michael Butler 2007-10-27

This book constitutes the refereed proceedings of the 9th International Conference on Formal Engineering Methods, ICFEM 2007, held in Boca Raton, Florida, USA, November 14-15, 2007. The 19 revised full papers together with two invited talks presented were carefully reviewed and selected from 38 submissions. The papers address all current issues in formal methods and their applications in software engineering. The papers are organized in topical sections.

JT; JT/T; JTT - Product Catalog. Translated English of Chinese Standard. (JT; JT/T; JTT) - https://www.chinesestandard.net 2018-01-01

This document provides the comprehensive list of Chinese Industry Standards - Category: JT; JT/T; JTT.

The Information Systems Security Officer's Guide - Gerald L. Kovacich 2003-08-05

Clearly addresses the growing need to protect information and information systems in the global marketplace.

GB, GB/T, GBT Chinese Standard(English-translated version) - Catalog002 - CODEOFCHINA - Dr. Meng Yongye 2018-05-04

All English-translated Chinese codes are available at: www.codeofchina.com

Commerce, Justice, Science, and Related Agencies Appropriations for 2011, Part 2, 111-2 Hearings - 2010

Official (ISC)2 Guide to the CISSP CBK - Adam Gordon 2015-04-08
As a result of a rigorous, methodical process that (ISC) follows to routinely update its credential exams, it has announced that enhancements will be made to both the Certified Information Systems Security Professional (CISSP) credential, beginning April 15, 2015. (ISC) conducts this process on a regular basis to ensure that the examinations and

Security and Privacy Trends in the Industrial Internet of Things - Cristina Alcaraz 2019-05-13
This book, written by leaders in the protection field of critical infrastructures, provides an extended overview of the technological and operative advantages together with the security problems and challenges of the new paradigm of the Internet of Things in today's industry, also known as the Industry Internet of Things (IIoT). The incorporation of the new embedded technologies and the interconnected networking advances in the automation and monitoring processes, certainly multiplies the functional complexities of the underlying control system, whilst increasing security and privacy risks. The critical nature of the application context and its relevance for the well-being of citizens and their economy, attracts the attention of multiple, advanced attackers, with stealthy abilities to evade security policies, ex-filter information or exploit vulnerabilities. Some real-life events and registers in CERTs have already clearly demonstrated how the control industry can become vulnerable to multiple types of advanced threats whose focus consists in hitting the safety and security of the control processes. This book, therefore, comprises a detailed spectrum of research papers with highly analytical content and actuation procedures to cover the relevant security and privacy issues such as data protection, awareness, response and resilience, all of them working at optimal times. Readers will be able to comprehend the construction problems of the fourth industrial revolution and are introduced to effective, lightweight protection solutions which can be integrated as part of the new IIoT-based monitoring ecosystem.

Computational Science and Its Applications - ICCSA 2006 - Osvaldo Gervasi 2006-05-11
The five-volume set LNCS 3980-3984 constitutes the refereed proceedings of the International Conference on Computational Science and Its Applications, ICCSA 2006. The volumes present a total of 664 papers organized according to the five major conference themes: computational methods, algorithms and applications high performance technical computing and networks advanced and emerging applications geometric modelling, graphics and visualization information systems and information technologies. This is Part IV.

Index of Administrative Publications - United States. Department of the Army 1978

GB/T-2016, GB-2016 -- Chinese National Standard PDF-English, Catalog (year 2016) - https://www.chinesestandard.net 2020-06-06
This document provides the comprehensive list of Chinese National Standards - Category: GB, GB/T Series of year 2016.

Readings & Cases in Information Security: Law & Ethics - Michael E. Whitman 2010-06-23
Readings and Cases in Information Security: Law and Ethics provides a depth of content and analytical viewpoint not found in many other books. Designed for use with any Cengage Learning security text, this resource offers readers a real-life view of information security management, including the ethical and legal issues associated with various on-the-job experiences. Included are a wide selection of foundational readings and scenarios from a variety of experts to give the reader the most realistic perspective of a career in information security. Important Notice:

Media content referenced within the product description or the product text may not be available in the ebook version.

CISSP Training Guide - Roberta Bragg 2002

The CISSP (Certified Information Systems Security Professionals) exam is a six-hour, monitored paper-based exam covering 10 domains of information system security knowledge, each representing a specific area of expertise. This book maps the exam objectives and offers numerous features such as exam tips, case studies, and practice exams.

Critical Information Infrastructures Security - Bernhard Hämmerli 2013-10-18

This book constitutes the thoroughly refereed post-proceedings of the 7th International Workshop on Critical Information Infrastructures Security, CRITIS 2012, held in Lillehammer, Norway, in September 2012. The 23 revised full papers were thoroughly reviewed and selected from 67 submissions. The papers are structured in the following topical sections: intrusion management; smart metering and grid, analysis and modeling; SCADA; cyber issues; CI analysis; CIP sectors; CI assessment; and threat modeling.

The IT Service Part 2 – The Handbook - Pierre Bernard 2012-06-06

Since the early 2000s numerous external scenarios and drivers have added significant pressures upon the IT organisations. Among many, these include: Regulatory compliance: data privacy requirements and corporate scandals have focused a requirement for transparency – with high impact on IT organisations Economic pressures: require IT organisations to more closely align with business imperatives. The outcome has been an explosion of ‘standards’ and ‘frameworks’ each designed to support the IT organisation as it demonstrates to the world that they are the’ rock’ of an organisation: strong, reliable, effective and efficient. Most of these standards and frameworks have great elements but no organisation can adopt them all – and many were created without sufficient considerations for interoperability. The IT Service (in 2 parts) looks at the key and very simple goals of an IT organisation and clearly and succinctly presents to the reader the best ‘rock solid’ elements in the Industry. It then shows how all the key elements can easily ‘crystallise’ together –with great templates and check-lists. In Part 1 (another book) the reader is presented with the simple objectives that the IT department really must address. In Part 2 (this book) the reader gains expert advice on how the components of IT Service are ‘crystallised’ in a real environment. There’s a delightfully simple set of steps: OVERVIEW OF THE SERVICE DESIGN PACKAGE THE SERVICE STRATEGY ASPECTS Of SERVICE DESIGN OUTPUTS OF THE SERVICE DESIGN PHASE OUTPUTS OF THE SERVICE TRANSITION PHASE OUTPUTS OF THE SERVICE OPERATION PHASE Within these the Author gives a very simple set of templates (or tells you where they are to be found), practical guidance and very simple checklists. It’s up the reader how far you develop each stage: a lot depends on the nature of your business of course. The joy of this approach is that the reader knows that all basic components are identified -- and that more extensive resources are referred to if the reader wishes to extend.

GB/T-2012, GB-2012 -- Chinese National Standard PDF-English, Catalog (year 2012) - https://www.chinesestandard.net 2020-06-06

This document provides the comprehensive list of Chinese National Standards - Category: GB, GB/T Series of year 2012.

Military Publications - United States. Department of the Army 1978

Cybersecurity in the Electricity Sector - Rafał Leszczyna 2019-08-30

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.

Information Systems for Business and Beyond - David T. Bourgeois 2014

"Information Systems for Business and Beyond introduces the concept of information systems, their use in business, and the larger impact they are having on our world."--BC Campus website.

Computational Intelligence in Security for Information Systems - Álvaro Herrero 2011-05-30

This book constitutes the refereed proceedings of the 4th International Conference on Computational Intelligence in Security for Information Systems, CISIS 2011, held in Torremolinos-Málaga, in June 2011 as a satellite event of IWANN 2011, the International Work-Conference on Artificial and Natural Neural Networks. The 38 revised full papers presented were carefully reviewed and selected from a total of 70 submissions. The papers are organized in topical sections on machine learning and intelligence, network security, cryptography, securing software, and applications of intelligent methods for security.

Scientific and Technical Aerospace Reports - 1991-07

Recent Developments on Industrial Control Systems Resilience - Emil Pricop 2019-10-05

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.

GB/T; GBT - Product Catalog. Translated English of Chinese Standard. (GB/T; GBT) - https://www.chinesestandard.net 2018-01-01

This document provides the comprehensive list of Chinese National Standards - Category: GB/T; GBT.

Critical Infrastructure Protection - Javier Lopez 2012-03-15

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