6 Example Scada Pro

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.

The fourth edition of the Official (ISC)2® Guide to the SSCP CBK® is a comprehensive resource providing an in-depth look at the seven domains of the SSCP Common Body of Knowledge (CBK). This latest edition provides an updated, detailed guide that is considered one of the best tools for candidates striving to become an SSCP. The book offers step-by-step guidance through each of SSCP's domains, including best practices and techniques used by the world's most experienced practitioners. Endorsed by (ISC)² and compiled and reviewed by SSCPs and subject matter experts, this book brings together a global, thorough perspective to not only prepare for the SSCP exam, but it also provides a reference that will serve you well into your career.

These proceedings of the SAI Intelligent Systems Conference 2016 (IntelliSys 2016) offer a remarkable collection of chapters on a wide range of topics in intelligent systems, artificial intelligence and their applications to the real world. Authors hailing from 56 countries on 5 continents submitted 404 papers to the conference, attesting to the global importance of the conference's themes. After being reviewed, 222 papers were accepted for presentation, and 168 were ultimately selected for these proceedings. Each has been reviewed on the basis of its originality, novelty and rigorousness. The papers not only present state-of-the-art methods and valuable experience from researchers in the related research areas; they also outline the field's future development.

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.

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

Handbook of Information and Communication SecuritySpringer Science & Business Media

The fourth volume in the established Energy from the Desert series examines and evaluates the potential and feasibility of Very Large Scale Photovoltaic Power Generation (VLS-PV) systems, which have capacities ranging from several megawatts to gigawatts, and to develop practical project proposals toward implementing the VLS-PV systems in the future. It comprehensively analyses all major issues involved in such large scale applications, based on the latest scientific and technological developments by means of close international co-operation with experts from different countries. From the perspective of the global energy situation, global warming, and other environmental issues, it is apparent that VLS-PV systems can: contribute substantially to global energy needs become economically and technologically feasible soon contribute significantly to global environmental protection contribute significantly to socio-economic development This book recognises that very large scale solar electricity generation provides economic, social and environmental benefits, security of electricity supply and fair access to affordable and sustainable energy solutions and that VLS-PV systems must be one of the promising options for large-scale deployment of PV systems and renewable energy technologies.

Blackhatonomics explains the basic economic truths of the underworld of hacking, and why people around the world devote tremendous resources to developing and implementing malware. The book provides an economic view of the evolving business of cybercrime, showing the methods and motivations behind organized cybercrime attacks, and the changing tendencies towards cyber-warfare. Written by an exceptional author team of Will Gragido, Daniel J Molina, John Pirc and Nick Selby, Blackhatonomics takes practical academic principles and backs them up with use cases and extensive interviews, placing you right into the mindset of the cyber criminal. Historical perspectives of the development of malware as it evolved into a viable economic endeavour Country specific cyber-crime analysis of the United States, China, and Russia, as well as an analysis of the impact of Globalization on cyber-crime Presents the behind the scenes methods used to successfully execute financially motivated attacks in a globalized cybercrime economy Provides unique insights, analysis, and useful tools for justifying corporate information security budgets Provides multiple points of view, from pure research, to corporate, to academic, to law enforcement Includes real world cybercrime case studies and profiles of high-profile cybercriminals

Cyber warfare has become more pervasive and more complex in recent years. It is difficult to regulate, as it holds an ambiguous position within the laws of war. This book investigates the legal and ethical ramifications of cyber war, considering which sets of laws apply to it, and how it fits into traditional ideas of armed conflict.

At its core, information security deals with the secure and accurate transfer of information. While information security has long been important, it was, perhaps, brought more clearly into mainstream focus with the so-called "Y2K" issue. Te Y2K scare was the fear that c- puter networks and the systems that are controlled or operated by sofware would fail with the turn of the millennium, since their clocks could lose synchronization by not recognizing a number (instruction) with three zeros. A positive outcome of this scare was the creation of several Computer Emergency Response Teams (CERTs) around the world that now work - operatively to exchange expertise and information, and to coordinate in case major problems should arise in the modern IT environment. Te terrorist attacks of 11 September 2001 raised security concerns to a new level. Te - ternational community responded on at least two fronts; one front being the transfer of reliable information via secure networks and the other being the collection of information about - tential terrorists. As a sign of this new emphasis on security, since 2001, all major academic publishers have started technical journals focused on security, and every major communi- tions conference (for example, Globecom and ICC) has organized workshops and sessions on security issues. In addition, the IEEE has created a technical committee on Communication and Information Security. Te ?rst editor was intimately involved with security for the Athens Olympic Games of 2004.

Everyone expects the products and services they use to be secure, but 'building security in' at the earliest stages of a system's design also means designing for use as well. Software that is unusable to end-users and unwieldy to developers and administrators may be insecure as errors and violations may expose exploitable vulnerabilities. This book shows how practitioners and researchers can build both security and usability into the design of systems. It introduces the IRIS framework and the open source CAIRIS platform that can guide the specification of secure and usable software. It also illustrates how IRIS and CAIRIS can complement techniques from User Experience, Security Engineering and Innovation & Entrepreneurship in ways that allow security to be addressed at different stages of the software lifecycle without disruption. Real-world examples are provided of the techniques and processes illustrated in this book, making this text a resource for practitioners, researchers, educators, and students.

Learn the code cracker's malicious mindset, so you can find worn-size holes in the software you are designing, testing, and building. Fuzzing for Software Security Testing and Quality Assurance takes a weapon from the black-hat arsenal to give you a powerful new tool to build secure, high-quality software. This practical resource helps you add extra protection without adding expense or time to already tight schedules and budgets. The book shows you how to make fuzzing a standard practice that integrates seamlessly with all development activities. This comprehensive reference goes through each phase of software development and points out where testing and auditing can tighten security. It surveys all popular commercial fuzzing tools and explains how to select the right one for a software development project. The book also identifies those cases where commercial tools fall short and when there is a need for building your own fuzzing tools.

"This 4th volume in the established Energy From The Desert series examines and evaluates the potential and feasibility of Very Large Scale Photovoltaic Power Generation (VLS-PV) systems, which have capacities ranging from several megawatts to gigawatts, and to develop practical project proposals toward implementing the VLS-PV systems in the future. Comprehensively analysing all major issues involved in such large scale applications, based on the latest scientific and technological developments and by means of close international co-operation with experts from different countries. From the perspective of the global energy situation, global warming, and other environmental issues, it is apparent that VLS-PV systems can: contribute substantially to global energy needs; become economically and technologically feasible soon; contribute significantly to the global environment protection; contribute significantly to socio-economic development. Energy policies around the world are gradually changing direction to focus less on nuclear energy with the expectation to turn to denuclearization entirely with the negative impacts of nuclear energy, while in parallel the importance of and expectations for renewable energy technologies are increasing drastically as possible energy infrastructure, as well as environmental friendly technology. This book recognises that very large scale solar electricity generation provides economic, social and environmental benefits, security of electricity supply and fair access to affordable and sustainable energy solutions and that VLS-PV systems must be one of the promising options for large-scale deployment of PV systems and renewable energy technologies"--

The nexus between water and energy raises a set of public policy questions that go far beyond water and energy. Economic vitality and management of scarce and precious resources are at stake. This book contributes to the body of knowledge and understanding regarding water, energy, and the links between the two in the American West and beyond. The research and analyses presented by the authors shed new light on the choices that must be made in order to avoid unnecessary harm in the development and management of water and energy systems to meet public needs in an ever changing environmental and economic climate. Indeed, the book shows, thoughtfully designed new technologies and approaches can help restore damaged environments and provide a range of benefits. The focus is the American West, but many of the lessons are global in their applicability. After a broad, stage-setting introductory section, the volume looks first at the use of water for energy production and then follows with chapters on the role of energy in water projects. The final section looks at the way forward, providing cases and recommendations for better, more efficient linkages in the water–energy nexus. Students and researchers in economics, public policy, environmental studies and law along with planners and policymakers will find this accessible and very current volume invaluable.

Real-world configurations and supporting materials enable you to deploy Nagios and integrate other tools on a step-by-step basis Simplifies deployment and installation by providing examples of real-world monitoring situations and explains how to configure, architect, and deploy EM solutions to address these situations Shows how to create your own Nagios plug-ins, to monitor devices for which Nagios doesn’t provide plug-ins

Bestselling author Ron Krutz once again demonstrates hisability to make difficult security topics approachable with thisfirst in-depth look at SCADA (Supervisory Control And DataAcquisition) systems Krutz discusses the harsh reality that natural gas pipelines,nuclear plants, water systems, oil refineries, and other industrialfacilities are vulnerable to a terrorist or disgruntled employeecausing lethal accidents and millions of dollars of damage-and whatcan be done to prevent this from happening Examines SCADA system threats and vulnerabilities, theemergence of protocol standards, and how security controls can beapplied to ensure the safety and security of our nationalinfrastructure assets

Trojans, Worms, and Spyware provides practical, easy to understand, and readily usable advice to help organizations to improve their security and reduce the possible risks of malicious code attacks. Despite the global downturn, information systems security remains one of the more in-demand professions in the world today. With the widespread use of the Internet as a business tool, more emphasis is being placed on information security than ever before. To successfully deal with this increase in dependence and the ever growing threat of virus and worm attacks, Information security and information assurance (IA) professionals need a jargon-free book that addresses the practical aspects of meeting new security requirements. This book provides a comprehensive list of threats, an explanation of what they are and how they wreak havoc with systems, as well as a set of rules-to-live-by along with a system to develop procedures and implement security training. It is a daunting task to combat the new generation of computer security threats – new and advanced variants of Trojans, as well as spyware (both hardware and software) and “bombs – and Trojans, Worms, and Spyware will be a handy must-have reference for the computer security professional to battle and prevent financial and operational harm from system attacks. *Provides step-by-step instructions to follow in the event of an attack *Case studies illustrate the "do's," "don'ts," and lessons learned from infamous attacks *Illustrates to managers and their staffs the importance of having protocols and a response plan in place

This book advises the federal government on a national infrastructure research agenda. It takes the position that the traditional disciplinary and institutional divisions among infrastructure modes and professions are largely historical artifacts that impose barriers to the development of new technology and encourages the government to embrace a more interdisciplinary approach. In order to be practical, the study focuses on infrastructure technologies that can be incorporated into or overlay current systems, allow for alternative future alternative future urban development, and are likely to have value cutting across the distinct functional modes of infrastructure. Finally, the report is organized according to seven broad cross-cutting areas that should promote interdisciplinary approaches to infrastructure problems: systems life-cycle management, analysis and decision tools, information management, condition assessment and monitoring technology, the science of materials performance and deterioration, construction equipment and procedures, and technology management.

Government and companies have already invested hundreds of millions of dollars in the convergence of physical and logical security solutions, but there are no books on the topic. This book begins with an overall explanation of information security, physical security, and why approaching these two different types of security in one way (called convergence) is so critical in today’s changing security landscape. It then details enterprise security management as it relates to incident detection and incident management. This is followed by detailed examples of implementation, taking the reader through cases addressing various physical security technologies such as: video surveillance, HVAC, RFID, access controls, biometrics, and more. This topic is picking up momentum every day with every new computer exploit, announcement of a malicious insider, or issues related to terrorists, organized crime, and nation-state threats The author has over a decade of real-world security and management expertise developed in some of the most sensitive and mission-critical environments in the world Enterprise Security Management (ESM) is deployed in tens of thousands of organizations worldwide

This book constitutes the thoroughly refereed post-proceedings of the 5th International Workshop on Critical Information Infrastructure Security, CRITIS 2010, held in Athens, Greece in September 2010. The 12 revised full papers and two poster papers presented went through two rounds of reviewing and improvement and were selected from 30 submissions. The papers included address various techniques to realize the security of systems, communications, and data.

This book focuses on emerging issues following the integration of artificial intelligence systems in our daily lives. It focuses on the cognitive, visual, social and analytical aspects of computing and intelligent technologies, highlighting ways to improve technology acceptance, effectiveness, and efficiency. Topics such as responsibility, integration and training are discussed throughout. The book also reports on the latest advances in systems engineering, with a focus on societal challenges and next-generation systems and applications for meeting them. It also discusses applications in smart grids and infrastructures, systems engineering education as well as defense and aerospace. The book is based on both the AHFE 2018 International Conference on Human Factors in Artificial Intelligence and Social Computing, Software and Systems Engineering, The Human Side of Service Engineering and Human Factors in Energy, July 21–25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA.

The Wiley Handbook of Science and Technology for Homeland Security is an essential and timely collection of resources designed to support the effective communication of homeland security research across all disciplines and institutional boundaries. Truly a unique work this 4 volume set focuses on the science behind safety, security, and recovery from both man-made and natural disasters has a broad scope and international focus. The Handbook: Educates researchers in the critical needs of the homeland security and intelligence communities and the potential contributions of their own disciplines Emphasizes the role of fundamental science in creating novel technological solutions Details the international dimensions of homeland security and counterterrorism research Provides guidance on technology diffusion from the laboratory to the field Supports cross-disciplinary dialogue in this field between operational, R&D and consumer communities

Electrical Engineering Reference Manual is the most comprehensive reference available for the electrical and computer engineering PE exam.

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 readers with an overview to the design of multiapplication smart card environments including the selection of a platform, the creation of applications and the logistics of initial deployment.

Get complete coverage of all six CCFP exam domains developed by the International Information Systems Security Certification Consortium (ISC)2. Written by a leading computer security expert, this authoritative guide fully addresses cyber forensics techniques, standards, technologies, and legal and ethical principles. You'll find learning objectives at the beginning of each chapter, exam tips, practice exam questions, and in-depth explanations. Designed to help you pass the exam with ease, this definitive volume also serves as an essential on-the-job reference. COVERS ALL SIX EXAM DOMAINS: Legal and ethical principles Investigations Forensic science Digital forensics Application forensics Hybrid and emerging technologies ELECTRONIC CONTENT INCLUDES: 250 practice exam questions Test engine that provides full-length practice exams and customized quizzes by chapter or by exam domain

Broadband is one of the most transformative technologies of the 21st century, yet our understanding of its regional impacts remains somewhat rudimentary. Not only are issues of broadband pricing and speed relevant in this context, but the overall quality of service for broadband can often dictate its impacts on regional development. This book illuminates the regional impacts of this pervasive and important technology. The principle aim of this book is to deepen our understanding of broadband and its connections to regional development. First, it uses a geospatial lens to explore how the relationship between broadband and regional development influences access to technology platforms, dictates provision patterns, and facilitates the shrinkage of space and time in non-uniform and sometimes unexpected ways. Second, it book provides a comprehensive guide that details the strengths and weaknesses of publically available broadband data and their associated uncertainties, allowing regional development professionals and researchers to make more informed decisions regarding data use, analytical models and policy recommendations. Finally, this book is the first to detail the growing importance of broadband to digital innovation and entrepreneurship in regions. This book will be of interest to regional development professionals and researchers in economics, public policy, geography, regional science and planning.

Transmission Pipeline Calculations and Simulations Manual is a valuable time- and money-saving tool to quickly pinpoint the essential formulae, equations, and calculations needed for transmission pipeline routing and construction decisions. The manual’s three-part treatment starts with gas and petroleum data tables, followed by self-contained chapters concerning applications. Case studies at the end of each chapter provide practical experience for problem solving. Topics in this book include pressure and temperature profile of natural gas pipelines, how to size pipelines for specified flow rate and pressure limitations, and calculating the locations and HP of compressor stations and pumping stations on long distance pipelines. Case studies are based on the author's personal field experiences Component to system level coverage Save time and money designing pipe routes well Design and verify piping systems before going to the field Increase design accuracy and systems effectiveness

SCADA systems are at the heart of the modern industrial enterprise. In a market that is crowded with high-level monographs and reference guides, more practical information for professional engineers is required. This book gives them the knowledge to design their next SCADA system more effectively.

"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.

This book constitutes the proceedings of the 10th International Symposium on Cyberspace Safety and Security, CSS 2018, held in Amalfi, Italy, in October 2018. The 25 full papers presented in this volume were carefully reviewed and selected from 79 submissions. The papers focus on cybersecurity; cryptography, data security, and biometric techniques; and social security, ontologies, and smart applications.

Here's the ideal tool if you're looking for a flexible, straightforward analysis system for your everyday design and operations decisions. This new third edition includes sections on stations, geographical information systems, "absolute" versus "relative" risks, and the latest regulatory developments. From design to day-to-day operations and maintenance, this unique volume covers every facet of pipeline risk management, arguably the most important, definitely the most hotly debated, aspect of pipelining today. Now expanded and updated, this widely accepted standard reference guides you in managing the risks involved in pipeline operations. You'll also find ways to create a resource allocation model by linking risk with cost and customize the risk assessment technique to your specific requirements. The clear step-by-step instructions and more than 50 examples make it easy. This edition has been expanded to include offshore pipelines and distribution system pipelines as well as cross-country liquid and gas transmission pipelines. The only comprehensive manual for pipeline risk management Updated material on stations, geographical information systems, "absolute" versus "relative" risks, and the latest regulatory developments Set the standards for global pipeline risk management

The availability and security of many services we rely upon including water treatment, electricity, healthcare, transportation, and financial transactions are routinely put at risk by cyber threats. The Handbook of SCADA/Control Systems Security is a fundamental outline of security concepts, methodologies, and relevant information pertaining to the

This comprehensive resource explains the development of UAVs, drone threats, counter-UAV systems, and strategies to handle UAVs, focusing on the practical aspects of counter-unmanned aerial vehicle (UAV) systems and technologies.Theory, technical and operational practice with insights from industry and policing are covered, and the full rogue drone threat landscape and counter-drone technologies and systems is explored. The book provides insight into counter-drone strategy, developing effective counter-drone strategies and measures, as well as counter-drone programs and the regulatory frameworks governing the use of drones. It includes analysis of future drone and counter-drone challenges and highlights ongoing research and innovation activities and an examination of future drone technologies. Written by authors who have extensive academic, research, innovation, technical, industry and police operational investigative expertise at international level, this book is useful for the aviation sector, law enforcement and academia.

This book discusses water resources management in Romania from a hydrological perspective, presenting the latest research developments and state-of-the-art knowledge that can be applied to efficiently solve a variety of problems in integrated water resources management. It focuses on a wide range of water resources issues – from hydrology and water quantity, quality and supply to flood protection, hydrological hazards and ecosystems, and includes case studies from various watersheds in Romania. As such, the book appeals to researchers, practitioners and graduates as well as to anybody interested in water resources management.