The Connection Algorithm Take Risks Defy The Status Quo And Live Your Passions

Occupational Safety and Hygiene II contains selected papers from the International Symposium on Occupational Safety and Hygiene (SHO2014, Guimar Portugal, 13-14 February 2014), which was organized by the Portuguese Society for Occupational Safety and Hygiene (SPOSHO). The contributions focus on selected topics, which include (but is not limited t

Risk measures play a vital role in many subfields of economics and finance. It has been proposed that risk measures could be analysed in relation to the performance of variables extracted from empirical real-world data. For example, risk measures may help inform effective monetary and fiscal policies and, therefore, the further development of pricing models for financial assets such as equities, bonds, currencies, and derivative securities.A Special Issue of “Risk Measures with Applications in Finance and Economics” will be devoted to advancements in the mathematical and statistical development of risk measures with applications in finance and economics. This Special Issue will bring together the theory, practice and real-world applications of risk measures. This book is a collection of papers published in the Special Issue of “Risk Measures with Applications in Finance and Economics” for Sustainability in 2018.

Safety, Reliability and Risk Analysis. Theory, Methods and Applications contains the papers presented at the joint ESREL (European Safety and Reliability) and SRA-Europe (Society for Risk Analysis Europe) Conference (Valencia, Spain, 22-25 September 2008). The book covers a wide range of topics, including: Accident and Incident Investigation; Crisi

During the last decade there have been increasing societal concerns over sustainable developments focusing on the conservation of the environment, the welfare and safety of the individual and at the same time the optimal allocation of available natural and financial resources. As a consequence the methods of risk and reliability analysis are becomi

Risk, Reliability and Safety contains papers describing innovations in theory and practice contributed to the scientific programme of the European Safety and Reliability conference (ESREL 2016), held at the University of Strathclyde in Glasgow, Scotland (25—29 September 2016). Authors include scientists, academics, practitioners, regulators and other key individuals with expertise and experience relevant to specific areas. Papers include domain specific applications as well as general modelling methods. Papers cover evaluation of contemporary solutions, exploration of future challenges, and exposition of concepts, methods and processes. Topics include human factors, occupational health and safety, dynamic and systems reliability modelling, maintenance optimisation, uncertainty analysis, resilience assessment, risk and crisis management.

This book collects the papers presented at the 7th International Conference on Risk Analysis and Crisis Response (RACR-2019) held in Athens, Greece, on October 15-19, 2019. The overall theme of the seventh international conference on risk analysis and crisis response is Risk Analysis Based on Data and Crisis Response Beyond Knowledge, highlighting science and technology to improve risk analysis capabilities and to optimize crisis response strategy. This book contains primarily research articles of risk issues. Underlying topics include natural hazards and major (chemical) accidents prevention, disaster risk reduction and society resilience, information and communication technologies safety and cybersecurity, modern trends in crisis management, energy and resources security, critical infrastructure, nanotechnology safety and others. All topics include aspects of multidisciplinarity and complexity of safety in education and research. The book should be valuable to professors, engineers, officials, businessmen and graduate students in risk analysis and risk management.

Managing risk is essential for every organization. However, significant opportunities may be lost by concentrating on the negative aspects of risk without bearing in mind the positive attributes. The objective of Project Risk Management: Managing Software Development Risk is to provide a distinct approach to a broad range of risks and rewards associated with the design, development, implementation and deployment of software systems. The traditional perspective of software development risk is to view risk as a negative characteristic associated with the impact of potential threats. The perspective of this book is to explore a more discerning view of software development risks, including the positive aspects of risk associated with potential beneficial opportunities. A balanced approach requires that software project managers approach negative risks with a view to reduce the likelihood and impact on a software project, and approach positive risks with a view to increase the likelihood of exploiting opportunities. Project Risk Management: Managing Software Development Risk explores software development risk both from a technological and business perspective. Issues regarding strategies for software development are discussed and topics including risks related to technical performance, outsourcing, cybersecurity, scheduling, quality, costs, opportunities and competition are presented. Bringing together concepts across the broad spectrum of software engineering with a project management perspective, this volume represents both a professional and scholarly perspective on the topic.

Evolutionary computing paradigms offer robust and powerful adaptive search mechanisms for system design. This book’s thirteen chapters cover a wide area of topics in evolutionary computing and applications, including an introduction to evolutionary computing in system design; evolutionary neuro-fuzzy systems; and evolution of fuzzy controllers. The book will be useful to researchers in intelligent systems with interest in evolutionary computing, as well as application engineers and system designers.

This book provides insight on how disaster risk management can increase the resilience of society to various natural hazards. The multi-dimensionality of resilience and the various different perspectives in regards to disaster risk reduction are taken explicitly into account by providing studies and approaches on different scales and ranging from natural science based methods to social science frameworks. For all chapters, special emphasis is placed on implementation aspects and specifically in regards to the targets and priorities for action laid out in the Sendai Framework for Disaster Risk Reduction. The chapters provide also a starting point for interested readers on specific issues of resilience and therefore include extensive reference material and important future directions for research.

This two volume set (LNCS 8025-8026) constitutes the refereed proceedings of the Fourth International Conference on Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management, formerly International Conference on Digital Human Modeling, DHM 2013, held as part of the 15th International Conference on Human-Computer Interaction, HCII 2013, held in Las Vegas, USA in July 2013, jointly with 12 other thematically similar conferences. The total of 1666 papers and 303 posters presented at the HCII 2013 conferences was carefully reviewed and selected from 5210 submissions. These papers address the latest research and development efforts and highlight the human aspects of design and use of computing systems. The papers accepted for presentation thoroughly cover the entire field of Human-Computer Interaction, addressing major advances in knowledge and effective use of computers in a variety of application areas. This two-volume set contains 91 papers. The papers in this volume focus on the following topics: driving and aviation safety, human factors and digital human modeling in healthcare, and safety of the human environment.

This is the joint refereed proceedings of the 9th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2006 and the 10th International Workshop on

Randomization and Computation, RANDOM 2006. The book presents 44 carefully reviewed and revised full papers. Among the topics covered are design and analysis of approximation algorithms, hardness of approximation problems, small spaces and data streaming algorithms, embeddings and metric space methods, and more.

The refereed post-proceedings of the First International Symposium on Combinatorics, Algorithms, Probabilistic and Experimental Methodologies are presented in this volume. The symposium provided an interdisciplinary forum for researchers to share their discoveries and approaches. The 46 full papers address large data processing problems using different methodologies from major disciplines such as computer science, combinatorics, and statistics.

This book constitutes the refereed conference proceedings of the 4th Annual Privacy Forum, APF 2016, held in Frankfurt/Main, Germany, in September 2016. The 12 revised full papers presented in this volume were carefully reviewed and selected from 32 submissions. The papers are organized in three sessions: eIDAS and data protection regulation; IoT and public clouds; and privacy policies and privacy risk presentation.

Since the first edition of this book published, Bayesian networks have become even more important for applications in a vast array of fields. This second edition includes new material on influence diagrams, learning from data, value of information, cybersecurity, debunking bad statistics, and much more. Focusing on practical real-world problem-solving and model building, as opposed to algorithms and theory, it explains how to incorporate knowledge with data to develop and use (Bayesian) causal models of risk that provide more powerful insights and better decision making than is possible from purely data-driven solutions. Features Provides all tools necessary to build and run realistic Bayesian network models Supplies extensive example models based on real risk assessment problems in a wide range of application domains provided; for example, finance, safety, systems reliability, law, forensics, cybersecurity and more Introduces all necessary mathematics, probability, and statistics as needed Establishes the basics of probability, risk, and building and using Bayesian network models, before going into the detailed applications A dedicated website contains exercises and worked solutions for all chapters along with numerous other resources. The AgenaRisk software contains a model library with executable versions of all of the models in the book. Lecture slides are freely available to accredited academic teachers adopting the book on their course.

Presents a unified mathematical framework for a wide range of problems in estimation and control.

"This book brings together scholars with significantly different backgrounds who share interests in the interplay between trust and technology, presenting novel theoretical perspectives on the topics of trust and technology, as well as some empirical investigations into the trust-building, trust-repairing, and trust-destroying practices in the context of technology"--Provided by publisher.

The TransNav 2011 Symposium held at the Gdynia Maritime University, Poland in June 2011 has brought together a wide range of participants from all over the world. The program has offered a variety of contributions, allowing to look at many aspects of the navigational safety from various different points of view. Topics presented and discussed at the Symposium were: navigation, safety at sea, sea transportation, education of navigators and simulator-based training, sea traffic engineering, ship's manoeuvrability, integrated systems, electronic charts systems, satellite, radio-navigation and anti-collision systems and many others. This book is part of a series of six volumes and provides an overview of Methods and Algorithms in Navigation and is addressed to scientists and professionals involved in research and development of navigation, safety of navigation and sea transportation.

With artificial intelligence on the rise, the way we run our organisations will change—and drastically. But what exactly will that future look like? And who will take the leading role: machines or people? In this compelling new book, leading management guru David De Cremer identifies the key areas where algorithms will collide with human skills, and assesses the likely outcomes. Will your next boss be a robot? Can an AI boss display the human qualities that define a good leader: compassion, empathy, imagination, ethics, and strategic awareness? Drawing on his own research findings, and those from thought leaders around the world, the author presents fascinating insights into the challenges that an automated work environment poses for organisations of the future. Leadership by Algorithm offers some startling conclusions that make clear the true nature of the power struggle between man and machine. It also identifies the leadership qualities needed to deal with this struggle most effectively.

In recent years, ELM has emerged as a revolutionary technique of computational intelligence, and has attracted considerable attentions. An extreme learning machine (ELM) is a single layer feed-forward neural network alike learning system, whose connections from the input layer to the hidden layer are randomly generated, while the connections from the hidden layer to the output layer are learned through linear learning methods. The outstanding merits of extreme learning machine (ELM) are its fast learning speed, trivial human intervene and high scalability. This book contains some selected papers from the International Conference on Extreme Learning Machine 2013, which was held in Beijing China, October 15-17, 2013. This conference aims to bring together the researchers and practitioners of extreme learning machine from a variety of fields including artificial intelligence, biomedical engineering and bioinformatics, system modelling and control, and signal and image processing, to promote research and discussions of “learning without iterative tuning". This book covers algorithms and applications of ELM. It gives readers a glance of the newest developments of ELM.

Conducted properly, information security risk assessments provide managers with the feedback needed to manage risk through the understanding of threats to corporate assets, determination of current control vulnerabilities, and appropriate safeguards selection. Performed incorrectly, they can provide the false sense of security that allows potential threats to develop into disastrous losses of proprietary information, capital, and corporate value. Picking up where its bestselling predecessors left off, The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, Third Edition gives you detailed instruction on how to conduct a security risk assessment effectively and efficiently, supplying wide-ranging coverage that includes security risk analysis, mitigation, and risk assessment reporting. The third edition has expanded coverage of essential topics, such as threat analysis, data gathering, risk analysis, and risk assessment methods, and added coverage of new topics essential for current assessment projects (e.g., cloud security, supply chain management, and security risk assessment methods). This handbook walks you through the process of conducting an effective security assessment, and it provides the tools, methods, and up-to-date understanding you need to select the security measures best suited to your organization. Trusted to assess security for small companies, leading organizations, and government agencies, including the CIA, NSA, and NATO, Douglas J. Landoll unveils the little-known tips, tricks, and techniques used by savvy security professionals in the field. It includes features on how to Better negotiate the

scope and rigor of security assessments Effectively interface with security assessment teams Gain an improved understanding of final report recommendations Deliver insightful comments on draft reports This edition includes detailed guidance on gathering data and analyzes over 200 administrative, technical, and physical controls using the RIIOT data gathering method; introduces the RIIOT FRAME (risk assessment method), including hundreds of tables, over 70 new diagrams and figures, and over 80 exercises; and provides a detailed analysis of many of the popular security risk assessment methods in use today. The companion website (infosecurityrisk.com) provides downloads for checklists, spreadsheets, figures, and tools.

Flood Risk and Social Justice provides an overview of flood risk mitigation practices, covering issues that range from the social and ethical, to the scientific and practical.

This book provides readers with up-to-date research of emerging cyber threats and defensive mechanisms, which are timely and essential. It covers cyber threat intelligence concepts against a range of threat actors and threat tools (i.e. ransomware) in cutting-edge technologies, i.e., Internet of Things (IoT), Cloud computing and mobile devices. This book also provides the technical information on cyber-threat detection methods required for the researcher and digital forensics experts, in order to build intelligent automated systems to fight against advanced cybercrimes. The ever increasing number of cyber-attacks requires the cyber security and forensic specialists to detect, analyze and defend against the cyber threats in almost real-time, and with such a large number of attacks is not possible without deeply perusing the attack features and taking corresponding intelligent defensive actions – this in essence defines cyber threat intelligence notion. However, such intelligence would not be possible without the aid of artificial intelligence, machine learning and advanced data mining techniques to collect, analyze, and interpret cyber-attack campaigns which is covered in this book. This book will focus on cutting-edge research from both academia and industry, with a particular emphasis on providing wider knowledge of the field, novelty of approaches, combination of tools and so forth to perceive reason, learn and act on a wide range of data collected from different cyber security and forensics solutions. This book introduces the notion of cyber threat intelligence and analytics and presents different attempts in utilizing machine learning and data mining techniques to create threat feeds for a range of consumers. Moreover, this book sheds light on existing and emerging trends in the field which could pave the way for future works. The inter-disciplinary nature of this book, makes it suitable for a wide range of audiences with backgrounds in artificial intelligence, cyber security, forensics, big data and data mining, distributed systems and computer networks. This would include industry professionals, advanced-level students and researchers that work within these related fields.

This book presents intellectual, innovative, information technologies (I3-technologies) based on logical and probabilistic (LP) risk models. The technologies presented here consider such models for structurally complex systems and processes with logical links and with random events in economics and technology. The volume describes the following components of risk management technologies: LP-calculus; classes of LP-models of risk and efficiency; procedures for different classes; special software for different classes; examples of applications; methods for the estimation of probabilities of events based on expert information. Also described are a variety of training courses in these topics. The classes of risk models treated here are: LP-modeling, LP-classification, LP-efficiency, and LP-forecasting. Particular attention is paid to LP-models of risk of failure to resolve difficult economic and technical problems. Amongst the discussed procedures of I3-technologies are the construction of LP-models, LP-identification of risk models; LP-risk analysis, LP-management and LP-forecasting of risk. The book further considers LP-models of risk of invalidity of systems and processes in accordance with the requirements of ISO 9001-2008, LP-models of bank operational risks in accordance with the requirements of Basel-2, complex risk LP-models for preventing ammunition depot explosions, enterprise electric power supply systems, debugging tests of technical systems, etc. The book also considers LP-models of credit risks, securities portfolios, operational risks in banking, conteraction of bribes and corruption, etc. A number of applications is given to show the effectiveness of risk management technologies. In addition, topics of lectures and practical computer exercises intended for a two-semester course “Risk management technologies” are suggested.

"This book argues that while algorithms and artificial intelligence offer many benefits to society, those benefits may be at the cost of civil rights and legal remedies in the legal system"--

More than a century and half ago, William Froude and his son Robert [1,2] conducted the first scientifically designed towing tank experiments using scaled ship models traveling in calm water or waves. Since then, advances in mathematics and technology have led to the development of various methods for the assessment of the dynamic behavior of ships. Yet, as we enter the 2nd decade of the 21st century the advent of goal-based regulations and the emergence of safe and sustainable shipping standards still confront our ability to understand the fundamentals and assure absolute ship safety in design and operations. To instigate renewed interest in the well-rehearsed subject of ship dynamics this Special Issue presents a collection of 12 high-quality research contributions with a focus on the prediction and analysis of the dynamic behavior of ships in a stochastic environment. The papers presented are co-authored by leading subject matter experts from Europe, the Far East, and the USA. These papers will be of interest to academics, practitioners, and regulators involved in the progression of ship science, technical services, and safety standards.

This book proposes a uniform logic and probabilistic (LP) approach to risk estimation and analysis in engineering and economics. It covers the methodological and theoretical basis of risk management at the design, test, and operation stages of economic, banking, and engineering systems with groups of incompatible events (GIE). This edition includes new chapters providing a detailed treatment of scenario logic and probabilistic models for revealing bribes. It also contains clear definitions and notations, revised sections and chapters, an extended list of references, and a new subject index, as well as more than a hundred illustrations and tables which motivate the presentation.

This two-volume set LNCS 11581 and 11582 constitutes the thoroughly refereed proceedings of the 10th International Conference on Digital Human Modeling and Applications in

Health, Safety, Ergonomics and Risk Management, DHM 2019, which was held as part of the 21st HCI International Conference, HCII 2019, in Orlando, FL, USA, in July 2019. The total of 1275 papers and 209 posters included in the 35 HCII 2019 proceedings volumes were carefully reviewed and selected from 5029 submissions. DHM 2019 includes a total of 77 papers; they were organized in topical sections named: Part I, Human Body and Motion: Anthropometry and computer aided ergonomics; motion prediction and motion capture; work modelling and industrial applications; risk assessment and safety. Part II, Healthcare Applications: Models in healthcare; quality of life technologies; health dialogues; health games and social communities.

This book presents the revised version of seven tutorials given at the NETWORKING 2002 Conference in Pisa, Italy in May 2002. The lecturers present a coherent view of the core issues in the following areas: - peer-to-peer computing and communications - mobile computing middleware - network security in the multicast framework - categorizing computing assets according to communication patterns - remarks on ad-hoc networking - communication through virtual technologies - optical networks.

This book gathers the Proceedings of the 8th International Conference on Robot Intelligence Technology and Applications (RITA 2020). The areas covered include: Instrumentation and Control, Automation, Autonomous Systems, Biomechatronics and Rehabilitation Engineering, Intelligent Systems, Machine Learning, Mobile Robotics, Social Robotics and Humanoid Robotics, Sensors and Actuators, and Machine Vision, as well as Signal and Image Processing. As a valuable asset, the book offers researchers and practitioners a timely overview of the latest advances in robot intelligence technology and its applications.

The first edition, published November 2016, was targeted at the directors and senior managers of SMEs and larger organisations that have not yet paid sufficient attention to cybersecurity and possibly did not appreciate the scale or severity of permanent risk to their businesses. The book was an important wake-up call and primer and proved a significant success, including wide global reach and diverse additional use of the chapter content through media outlets. The new edition, targeted at a similar readership, will provide more detailed information about the cybersecurity environment and specific threats. It will offer advice on the resources available to build defences and the selection of tools and managed services to achieve enhanced security at acceptable cost. A content sharing partnership has been agreed with major technology provider Alien Vault and the 2017 edition will be a larger book of approximately 250 pages.

??This book combines game theory and complex networks to examine intentional technological risk through modeling. As information security risks are in constant evolution, the methodologies and tools to manage them must evolve to an ever-changing environment. A formal global methodology is explained in this book, which is able to analyze risks in cyber security based on complex network models and ideas extracted from the Nash equilibrium. A risk management methodology for IT critical infrastructures is introduced which provides guidance and analysis on decision making models and real situations. This model manages the risk of succumbing to a digital attack and assesses an attack from the following three variables: income obtained, expense needed to carry out an attack, and the potential consequences for an attack. Graduate students and researchers interested in cyber security, complex network applications and intentional risk will find this book useful as it is filled with a number of models, methodologies and innovative examples. ?

This book provides a scientific modeling approach for conducting metrics-based quantitative risk assessments of cybersecurity vulnerabilities and threats. This book provides a scientific modeling approach for conducting metrics-based quantitative risk assessments of cybersecurity threats. The author builds from a common understanding based on previous class-tested works to introduce the reader to the current and newly innovative approaches to address the maliciously-by-human-created (rather than by-chance-occurring) vulnerability and threat, and related cost-effective management to mitigate such risk. This book is purely statistical data-oriented (not deterministic) and employs computationally intensive techniques, such as Monte Carlo and Discrete Event Simulation. The enriched JAVA ready-to-go applications and solutions to exercises provided by the author at the book’s specifically preserved website will enable readers to utilize the course related problems. • Enables the reader to use the book's website's applications to implement and see results, and use them making ‘budgetary’ sense • Utilizes a data analytical approach and provides clear entry points for readers of varying skill sets and backgrounds • Developed out of necessity from real in-class experience while teaching advanced undergraduate and graduate courses by the author Cyber-Risk Informatics is a resource for undergraduate students, graduate students, and practitioners in the field of Risk Assessment and Management regarding Security and Reliability Modeling. Mehmet Sahinoglu, a Professor (1990) Emeritus (2000), is the founder of the Informatics Institute (2009) and its SACS-accredited (2010) and NSA-certified (2013) flagship Cybersystems and Information Security (CSIS) graduate program (the first such full degree in-class program in Southeastern USA) at AUM, Auburn University’s metropolitan campus in Montgomery, Alabama. He is a fellow member of the SDPS Society, a senior member of the IEEE, and an elected member of ISI. Sahinoglu is the recipient of Microsoft's Trustworthy Computing Curriculum (TCC) award and the author of Trustworthy Computing (Wiley, 2007).

This is the Proceedings of the Eighth International Conference on Management Science and Engineering Management (ICMSEM) held from July 25 to 27, 2014 at Universidade Nova de Lisboa, Lisbon, Portugal and organized by International Society of Management Science and Engineering Management (ISMSEM), Sichuan University (Chengdu, China) and Universidade Nova de Lisboa (Lisbon, Portugal). The goals of the conference are to foster international research collaborations in Management Science and Engineering Management as well as to provide a forum to present current findings. A total number of 138 papers from 14 countries are selected for the proceedings by the conference scientific committee through rigorous referee review. The selected papers in the second volume are focused on Computing and Engineering Management covering

areas of Computing Methodology, Project Management, Industrial Engineering and Information Technology.
Operational Risk Control with Basel II, provides a sound methodology for operational risk control and focuses on management risk and ways to avoid it. The book explains why and how information technology is a major operational risk and shows how to integrate cost control in the operational risk perspective. It aslo details analytical approaches to operational risk control, to help with scorecard developments, explains the distinction between High Frequency Low Risk and Low Frequency High Risk events and provides many case studeies from banking and insurance to demonstrate the attention operational risks deserve. Assists risk professionals in preparing their institution to comply with the New Capital Adequacy Framework issued by the Basel Committee on Banking Supervision, which becomes mandatory from January 1, 2006 Readers benefit from a significantly broader viewpoint on types of operational risks, operational risks controls, and results to be expected from operational risk management - compared to what the reader may gain from books previously published on this same topic
This book constitutes the refereed proceedings of the 9th IFIP/IEEE International Conference on Management of Multimedia and Mobile Networks and Services, MMNS 2006, held in Dublin, Ireland in October 2006 in the course of the 2nd International Week on Management of Networks and Services, Manweek 2006. The 18 revised full papers and six revised short papers presented were carefully reviewed and selected from 71 submissions.