

System Specification Based Network Modeling For

This book constitutes the refereed proceedings of the 9th International Conference on Information Security and Cryptology, ICISC 2006, held in Busan, Korea in November/December 2006. The 26 revised full papers cover such topics as hash functions, block and stream ciphers, network security and access control, mobile communications security, forensics, copyright protection, biometrics, public key cryptosystems, and digital signatures.

This volume contains technical papers and panel position papers selected from the proceedings of the International Symposium on Information Systems and Technologies for Network Society, held together with the IPSJ (information processing society of Japan) National Convention, in September 1997. Papers were submitted from all over the world, especially from Japan, Korea and China. Since these countries are believed to form one of the major computer manufacturing centers in the world, a panel on “Computer Science Education for the 21st Century” was set up. A special session on the Japanese project on Software Engineering invited representative researchers from the project, which is supported by the Ministry of Education, Japan.

In areas such as military, security, aerospace, and disaster management, the need for performance optimization and interoperability among heterogeneous systems is increasingly important. Model-driven engineering, a paradigm in which the model becomes the actual software, offers a promising approach toward systems of systems (SoS) engineering. However, model-driven engineering has largely been unachieved in complex dynamical systems and netcentric SoS, partly because modeling and simulation (M&S) frameworks are stove-piped and not designed for SoS composability. Addressing this gap, Netcentric System of Systems Engineering with DEVS Unified Process presents a methodology for realizing the model-driven engineering vision and netcentric SoS using DEVS Unified Process (DUNIP). The authors draw on their experience with Discrete Event Systems Specification (DEVS) formalism, System Entity Structure (SES) theory, and applying model-driven engineering in the context of a netcentric SoS. They describe formal model-driven engineering methods for netcentric M&S using standards-based approaches to develop and test complex dynamic models with DUNIP. The book is organized into five sections: Section I introduces undergraduate students and novices to the world of DEVS. It covers systems and SoS M&S as well as DEVS formalism, software, modeling language, and DUNIP. It also assesses DUNIP with the requirements of the Department of Defense’s (DoD) Open Unified Technical Framework (OpenUTF) for netcentric Test and Evaluation (T&E). Section II delves into M&S-based systems engineering for graduate students, advanced practitioners, and industry professionals. It provides methodologies to apply M&S principles to SoS design and reviews the development of executable architectures based on a framework such as the Department of Defense Architecture Framework (DoDAF). It also describes an approach for building netcentric knowledge-based contingency-driven systems. Section III guides graduate students, advanced DEVS users, and industry professionals who are interested in building DEVS virtual machines and netcentric SoS. It discusses modeling standardization, the deployment of models and simulators in a netcentric environment, event-driven architectures, and more. Section IV explores real-world case studies that realize many of the concepts defined in the previous chapters. Section V outlines the next steps and looks at how the modeling of netcentric complex adaptive systems can be attempted using DEVS concepts. It touches on the boundaries of DEVS formalism and the future work needed to utilize advanced concepts like weak and strong emergence, self-organization, scale-free systems, run-time modularity, and event interoperability. This groundbreaking work details how DUNIP offers a well-structured,

platform-independent methodology for the modeling and simulation of netcentric system of systems.

Modern society depends critically on computers that control and manage the systems on which we depend in many aspects of our daily lives. While this provides conveniences of a level unimaginable just a few years ago, it also leaves us vulnerable to attacks on the computers managing these systems. In recent times the explosion in cyber attacks, including viruses, worms, and intrusions, has turned this vulnerability into a clear and visible threat. Due to the escalating number and increased sophistication of cyber attacks, it has become important to develop a broad range of techniques, which can ensure that the information infrastructure continues to operate smoothly, even in the presence of dire and continuous threats. This book brings together the latest techniques for managing cyber threats, developed by some of the world's leading experts in the area. The book includes broad surveys on a number of topics, as well as specific techniques. It provides an excellent reference point for researchers and practitioners in the government, academic, and industrial communities who want to understand the issues and challenges in this area of growing worldwide importance.

NATO Advanced Institute Ottawa, Ontario/ Canada, July 26 - August 6, 1982

The Third International Conference on Network Security and Applications (CNSA-2010) focused on all technical and practical aspects of security and its applications for wired and wireless networks. The goal of this conference is to bring together researchers and practitioners from academia and industry to focus on understanding modern security threats and countermeasures, and establishing new collaborations in these areas. Authors are invited to contribute to the conference by submitting articles that illustrate research results, projects, survey work and industrial experiences describing significant advances in the areas of security and its applications, including: • Network and Wireless Network Security • Mobile, Ad Hoc and Sensor Network Security • Peer-to-Peer Network Security • Database and System Security • Intrusion Detection and Prevention • Internet Security, and Applications Security and Network Management • E-mail Security, Spam, Phishing, E-mail Fraud • Virus, Worms, Trojans Protection • Security Threats and Countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc.) • Ubiquitous Computing Security • Web 2. 0 Security • Cryptographic Protocols • Performance Evaluations of Protocols and Security Application There were 182 submissions to the conference and the Program Committee selected 63 papers for publication. The book is organized as a collection of papers from the First International Workshop on Trust Management in P2P Systems (IWTMP2PS 2010), the First International Workshop on Database Management Systems (DMS- 2010), and the First International Workshop on Mobile, Wireless and Networks Security (MWNS-2010).

Real-Time Simulation Technologies: Principles, Methodologies, and Applications is an edited compilation of work that explores fundamental concepts and basic techniques of real-time simulation for complex and diverse systems across a broad spectrum. Useful for both new entrants and experienced experts in the field, this book integrates coverage of detailed theory, acclaimed methodological approaches, entrenched technologies, and high-value applications of real-time simulation—all from the unique perspectives of renowned international contributors. Because it offers an accurate and otherwise unattainable assessment of how a system will behave over a particular time frame, real-time simulation is increasingly critical to the optimization of dynamic processes and adaptive systems in a variety of enterprises. These range in scope from the maintenance of the national power grid, to space exploration, to the development of virtual reality programs and cyber-physical systems. This book outlines how, for these and other undertakings, engineers must assimilate real-time data with computational tools for rapid decision making under uncertainty. Clarifying the central concepts behind real-time simulation tools and techniques, this one-of-a-kind resource: Discusses the state of the art, important challenges, and high-impact developments in simulation

technologies Provides a basis for the study of real-time simulation as a fundamental and foundational technology Helps readers develop and refine principles that are applicable across a wide variety of application domains As science moves toward more advanced technologies, unconventional design approaches, and unproven regions of the design space, simulation tools are increasingly critical to successful design and operation of technical systems in a growing number of application domains. This must-have resource presents detailed coverage of real-time simulation for system design, parallel and distributed simulations, industry tools, and a large set of applications.

This book introduces the state-of-the-art in research in parallel and distributed embedded systems, which have been enabled by developments in silicon technology, micro-electro-mechanical systems (MEMS), wireless communications, computer networking, and digital electronics. These systems have diverse applications in domains including military and defense, medical, automotive, and unmanned autonomous vehicles. The emphasis of the book is on the modeling and optimization of emerging parallel and distributed embedded systems in relation to the three key design metrics of performance, power and dependability. Key features: Includes an embedded wireless sensor networks case study to help illustrate the modeling and optimization of distributed embedded systems. Provides an analysis of multi-core/many-core based embedded systems to explain the modeling and optimization of parallel embedded systems. Features an application metrics estimation model; Markov modeling for fault tolerance and analysis; and queueing theoretic modeling for performance evaluation.

Discusses optimization approaches for distributed wireless sensor networks; high-performance and energy-efficient techniques at the architecture, middleware and software levels for parallel multicore-based embedded systems; and dynamic optimization methodologies. Highlights research challenges and future research directions. The book is primarily aimed at researchers in embedded systems; however, it will also serve as an invaluable reference to senior undergraduate and graduate students with an interest in embedded systems research. Security and privacy protection within computer networks can be a challenge. By examining the current problems and challenges this domain is facing, more efficient strategies can be established to safeguard personal information against invasive pressures. Security and Privacy in Smart Sensor Networks is a critical scholarly resource that examines recent developments and emerging trends in smart sensor security and privacy by providing new models, practical solutions, and technological advances related to security. Featuring coverage on a broad range of topics such as cloud security, encryption, and intrusion detection systems, this book is geared towards academicians, engineers, IT specialists, researchers, and students seeking current research on authentication and intrusion detection.

This six-volume set presents cutting-edge advances and applications of expert systems. Because expert systems combine the expertise of engineers, computer scientists, and computer programmers, each group will benefit from buying this important reference work. An "expert system" is a knowledge-based computer system that emulates the decision-making ability of a human expert. The primary role of the expert system is to perform appropriate functions under the close supervision of the human, whose work is supported by that expert system. In the reverse, this same expert system can monitor and double check the human in the performance of a task. Human-computer interaction in our highly complex world requires the development of a wide array of expert systems. Key Features * Expert systems techniques and applications are presented for a diverse array of topics including: * Experimental design and decision support * The integration of machine learning with knowledge acquisition for the design of expert systems * Process planning in design and manufacturing systems and process control applications * Knowledge discovery in large-scale knowledge bases * Robotic systems * Geographic information systems * Image analysis, recognition and interpretation * Cellular automata methods for pattern recognition * Real-time fault tolerant control systems * CAD-based vision systems in pattern matching processes * Financial systems * Agricultural applications * Medical diagnosis

Requirements engineering is the process by which the requirements for software systems are gathered, analyzed, documented, and managed throughout their complete lifecycle. Traditionally it has been concerned with technical goals for, functions of, and constraints on software systems. Aurum and Wohlin, however, argue that it is no longer appropriate for software systems professionals to focus only on functional and non-functional aspects of the intended system and to somehow assume that organizational context and needs are outside their remit. Instead, they call for a broader perspective in order to gain a better understanding of the interdependencies between enterprise stakeholders, processes, and software systems, which would in turn give rise to more appropriate techniques and higher-quality systems. Following an introductory chapter that provides an exploration of key issues in requirements engineering, the book is organized in three parts. Part 1 presents surveys of state-of-the-art requirements engineering process research along with critical assessments of existing models, frameworks and techniques. Part 2 addresses key areas in requirements engineering, such as market-driven requirements engineering, goal modeling, requirements ambiguity, and others. Part 3 concludes the book with articles that present empirical evidence and experiences from practices in industrial projects. Its broader perspective gives this book its distinct appeal and makes it of interest to both researchers and practitioners, not only in software engineering but also in other disciplines such as business process engineering and management science.

Body area networks (BANs) are networks of wireless sensors and medical devices embedded in clothing, worn on or implanted in the body, and have the potential to revolutionize healthcare by enabling pervasive healthcare. However, due to their critical applications affecting human health, challenges arise when designing them to ensure they are safe for the user, sustainable without requiring frequent battery replacements and secure from interference and malicious attacks. This book lays the foundations of how BANs can be redesigned from a cyber-physical systems perspective (CPS) to overcome these issues. Introducing cutting-edge theoretical and practical techniques and taking into account the unique environment-coupled characteristics of BANs, the book examines how we can re-imagine the design of safe, secure and sustainable BANs. It features real-world case studies, suggestions for further investigation and project ideas, making it invaluable for anyone involved in pervasive and mobile healthcare, telemedicine, medical apps and other cyber-physical systems.

This practical new resource gives you a comprehensive understanding of the design and deployment of transmission networks for wireless applications. From principles and design, to equipment procurement, project management, testing, and operation, it's a practical, hands-on engineering guide with numerous real-life examples of turn-key operations in the wireless networking industry. This book, written for both technical and non-technical professionals, helps you deal with the costs and difficulties involved in setting up the local access with technologies that are still in the evolutionary stage. Issues involved in the deployment of various transmission technologies, and their impact on the overall wireless network topology are discussed. Strategy and approach to transmission network planning, design and deployment are explored. The book offers practical guidelines and advice derived from the author's own experience on projects worldwide. You gain a solid grounding in third generation wireless networks with increased capacity requirements, while learning all about packet data architecture, and how it will impact future transmission network design and deployment.

Supervisory Control and Data Acquisition (SCADA) systems are deeply ingrained in the fabric of critical infrastructure sectors. These computerized real-time process control systems, over geographically dispersed continuous distribution operations, are increasingly subject to serious damage and disruption by cyber means due to their standardization and connectivity to other networks. However, SCADA systems generally have little protection from the escalating cyber threats. To achieve defense-in-depth for SCADA systems by means of intrusion detection and resilient control, this dissertation strives for a robust stochastic signal and system approach without being overly-pessimistic. Its

main elements are (1) two SCADA-specific comprehensive taxonomies with one on cyber attacks and the other on intrusion detection system to layout the lay of the land and shed light to the workspace, (2) one overall framework/architecture for intrusion detection and resilient control -- Xware (3) its measurement fusion assurance component -- Trust counter, (4) one signal-based early-detection and resilient estimation scheme with proved theoretical performance bounds, for SCADA systems in general. Especially the said Robust General Likelihood Ratio Test (RGLRT) is generic enough and has been applied to linear dynamical systems in general and beyond. (5) The application of RGLRT in network traffic anomaly detection. (6) The application of RGLRT to anomaly detection for SCADA systems in smart grids through model construction and identification for both clean renewable energy supply and variable consumer demand. First, in order to understand the potential danger and to protect SCADA systems, we highlight their difference from standard Information Technology (IT) systems and present a set of security property goals. Furthermore, we systematically identify and classify likely cyber attacks including cyber-induced cyber-physical attacks on SCADA systems according the SCADA's hierarchy. Determined by the impact on control performance of SCADA systems, we use the attack categorization criteria to stress commonalities and important features of such attacks that define unique challenges posed to securing SCADA systems versus traditional IT systems. Second, in order to address the big challenge of how to modify conventional IT intrusion detection techniques to suit the needs of SCADA, we explain the nuance associated with the task of SCADA-specific intrusion detection and frame it in the domain interest of control's researchers to illuminate problem space. We present a taxonomy and a set of metrics for SCADA-specific intrusion detection techniques through heightening their possible use in SCADA systems. In particular, we enumerate a list of Intrusion Detection Systems (IDS) that are proposed to undertake this endeavor. Drawing upon the discussion, we identify the deficits and voids in current research. Based upon this taxonomy and analysis on which SCADA-specific IDS strategies are most likely to succeed, we offer recommendations and future research venues in part through presenting a prototype of such efforts towards this goal. Third, we present the overall architecture for instruction detection and resilient control Xware. It is comprised of two strong footings -- Normalcy Checking, a control theoretic, domain knowledge specific, specification-based payload inspection system and a high-speed, real-time, behavioral-based Network Intrusion Detection System (NIDS). Xware integrates a Trust Counter to verify the truthfulness of sensor measurements. It also provides exfiltration of confidential information from within the intranet. Moreover, Xware hardens SCADA system with compensation schemes when intrusion evades NIDS or unexpected fault occurs to guarantee its performance. It puts things in perceptive and highlights the overall systematic and holistic approach. Fourth, we propose the Trust Counter to deal the case when the possible manifestation of those potential disruption from cyber attacks can affect the Kalman filter, the primary recursive estimation method used in the control engineering field. Whereas, to improve such estimation, data fusion may take place at a central location to fuse and process multiple sensor measurements delivered over the network. In an uncertain networked control system where the nodes and links are subject to attacks, false or compromised or missing individual readings can produce skewed results. To assure the validity of data fusion, we propose a centralized trust rating system. It evaluates the trustworthiness of each sensor reading on top of the fusion mechanism. The ratings are represented by Beta distribution, the conjugate prior of the binomial distribution and its posterior. Then an illustrative example demonstrates its efficiency. Fifth, RGLRT is an earlier anomaly detection and resilient estimation scheme for the cyber-physical systems, networked control systems to be specific, in an uncertain network environment. It robustly identifies and detects outliers among real-time multidimensional measurements of dynamical systems by using an online window-limited sequential Robust Generalized Likelihood Ratio (RGLR) test without any prior knowledge of the occurrence time and distribution of the outliers. The robust sequential testing and quick

detection scheme achieves the optimal stopping time with low rates in both false alarm and misdetection. We propose a set of qualitative and quantitative metric to measure its optimality in the context of cyber-physical systems. Further, this resilient and flexible estimation scheme robustly rectifies and cleans data upon both isolated and patchy outliers while maintain the optimality of the Kalman Filter under the nominal condition. Its approximated optimality of the robustification performance is shown through stochastic approximation. Sixth, we give a network anomaly detection scheme as one of the applications of RGLRT. The time series model of Autoregressive Integrated Moving Average (ARIMA) progress, finds its wide usage including network security applications. Model building and anomaly detection based on such models are often a first and important step towards monitoring unexpected problems and assuring the soundness and security of those systems being studied. The time variability by the coefficients in those dynamic regression models is particularly relevant and possibly indicative. To address this issue, a corresponding framework and a novel anomaly detection approach based on the Kalman filter for identifying those dynamic models including their parameters and a General Likelihood Ratio (GLR) test for detecting suspicious changes in the parameters and therefore the models is proposed. The idea is shown through experiments and show its promising potential in terms of accuracy and robustness. Seventh, we apply RGLRT to anomaly detection for SCADA systems in smart grids. While the utilization of clean energy resources including wind and solar power sets to grow from filling the gap of peak hours to taking a larger share in the upcoming smart grid and efficient infrastructure, the price-incentivized electricity consumption shall alleviate peak hours and reduce power outages. Both benign faults and malicious attacks threat the reliability and availability of the new grid. We address these duo problems from the angle of one fundamental technique used. The ARIMA time series models play roles at both ends in this new ecosystem: namely, predicting the variable clean energy resource on the supply side and forecasting the flexible load demand on the consume side. Model construction and anomaly detection based on such models are often a first and important step towards monitoring unexpected problems and assuring the soundness and security of those systems being studied. The time variability of the coefficients in those dynamic regression models is particularly relevant and possibly indicative. Thus a corresponding framework and a novel anomaly detection approach is introduced. It's based on a robustified Kalman Filter for identifying those dynamic models including their parameters and a RGLRT for detecting suspicious changes in the parameters and therefore the models. Currently, the effectiveness and robustness of this method is shown through simulation.

Teachers use e-learning systems to develop course notes and web-based activities to communicate with learners on one side and monitor and classify their progress on the other. Learners use it for learning, communication, and collaboration. Adaptive e-learning systems often employ learner models, and the behavior of an adaptive system varies depending on the data from the learner model and the learner's profile. Without knowing anything about the learner who uses the system, a system would behave in exactly the same way for all learners. Bayesian Networks for Managing Learner Models in Adaptive Hypermedia Systems: Emerging Research and Opportunities is a collection of research on the use of Bayesian networks and methods as a probabilistic formalism for the management of the learner model in adaptive hypermedia. It specifically discusses comparative studies, transformation rules, and case diagrams that support all phases of the learner model and the use of Bayesian networks and multi-entity Bayesian networks to manage dynamic aspects of this model. While highlighting topics such as developing the learner model, learning management systems,

and modeling techniques, this book is ideally designed for instructional designers, course administrators, educators, researchers, and professionals.

A smartphone is a portable device that combines mobile telephone and computing functions into one unit. It is a cellular telephone with an integrated computer and other features not originally associated with telephones such as an operating system, web browsing, multimedia functionality, the ability to run software applications, along with core phone functions such as voice calls and text messaging. Smartphones typically contain a number of metal–oxide–semiconductor (MOS) integrated circuit (IC) chips, include various sensors that can be leveraged by pre-included and third-party software (such as a magnetometer, proximity sensors, barometer, gyroscope, accelerometer and more), and support wireless communications protocols (such as Bluetooth, Wi-Fi, or satellite navigation). The best phones offer you everything you want from a mobile device. They deliver great cameras, the performance you need to multitask and enough battery life. The existing brands for Smartphones nowadays are: Samsung, Xiaomi, iPhone, Nokia, Huawei, Google Pixel, HTC, Asus, LG, Alcatel, Infinix, Panasonic, BlackBerry, Tecno, TCL, Oppo, Realme, Gionee, ZTE, Sony, Vivo, Lava, Lenovo, Microsoft, and Motorola. The most popular brands of smartphones are: Samsung, Apple, Huawei, Xiaomi, Oppo, Vivo, Realme, Sony. Choosing a smartphone for yourself not easy task. Factors that affect your choices of Smart phone are: price range, features, the operating system you prefer, the important specs for you. To help you to pick the best smartphone for you, I provide here briefer review for the specifications of different types of smartphones along with some helpful customer reviews in order to see ow the customers evaluate the product. This report consists of the following sections: 1. Price comparison of different budget smartphone models. 2. The differences between 2G, 3G, 4G LTE, 5G networks and WIFI. 3. The differences between NFC and Bluetooth. 4. The differences Android and iOS. 5. How to choose a smartphone by brand, carrier, or features. 6. How to keep your phone from overheating. 7. Security issues according to Check Point. 8. Samsung. 9. Xiaomi Redmi. 10. Xiaomi Poco. 11. Apple. 12. Nokia. 13. Huawei. 14. Google Pixel. 15. Microsoft. 16. Realme. 17. Sony. 18. Others mobile brands: HTC, Asus, LG, Alcatel, Infinix, Panasonic, BlackBerry, Tecno, TCL, Gionee, ZTE, Oppo, Vivo, Lava, Lenovo, Motorola, Meizu, Honor, OnePlus. 19. References. The aim of this book is to provide the latest research findings, innovative research results, methods and development techniques from both theoretical and practical perspectives related to intelligent social networks and collaborative systems, intelligent networking systems, mobile collaborative systems, secure intelligent cloud systems, etc., and to reveal synergies among various paradigms in the multi-disciplinary field of intelligent collaborative systems. It presents the Proceedings of the 9th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2017), held on August 24–26, 2017 in Toronto, Canada. With the rapid evolution of the Internet, we are currently experiencing a

shift from the traditional sharing of information and applications as the main purpose of the Web to an emergent paradigm that puts people at the very centre of networks and exploits the value of people's connections, relations and collaborations. Social networks are also playing a major role in the dynamics and structure of intelligent Web-based networking and collaborative systems. Virtual campuses, virtual communities and organizations effectively leverage intelligent networking and collaborative systems by tapping into a broad range of formal and informal electronic relations, such as business-to-business, peer-to-peer and many types of online collaborative learning interactions, including the emerging e-learning systems. This has resulted in entangled systems that need to be managed efficiently and autonomously. In addition, the latest and powerful technologies based on Grid and wireless infrastructure as well as Cloud computing are now greatly enhancing collaborative and networking applications, but are also facing new issues and challenges. The principal objective of the research and development community is to stimulate research that leads to the creation of responsive environments for networking and, in the longer-term, the development of adaptive, secure, mobile, and intuitive intelligent systems for collaborative work and learning.

The two-volume set, LNCS 10492 and LNCS 10493 constitutes the refereed proceedings of the 22nd European Symposium on Research in Computer Security, ESORICS 2017, held in Oslo, Norway, in September 2017. The 54 revised full papers presented were carefully reviewed and selected from 338 submissions. The papers address issues such as data protection; security protocols; systems; web and network security; privacy; threat modeling and detection; information flow; and security in emerging applications such as cryptocurrencies, the Internet of Things and automotive. This book constitutes the refereed proceedings of the First International Workshop on Self-Organizing Systems, IWSOS 2006. The book offers 16 revised full papers and 6 revised short papers together with 2 invited talks and 3 poster papers. The papers are organized in topical sections on dynamics of structured and unstructured overlays, self-organization in peer-to-peer networks, self-organization in wireless environments, self-organization in distributed and grid computing, self-managing and autonomic computing, and more.

For more than 20 years, Network World has been the premier provider of information, intelligence and insight for network and IT executives responsible for the digital nervous systems of large organizations. Readers are responsible for designing, implementing and managing the voice, data and video systems their companies use to support everything from business critical applications to employee collaboration and electronic commerce.

Poor performance is one of the main quality-related shortcomings that cause software projects to fail. Thus, the need to address performance concerns early during the software development process is fully acknowledged, and there is a growing interest in the research and software industry communities towards techniques, methods and tools that permit to

manage system performance concerns as an integral part of software engineering. Model-based software performance analysis introduces performance concerns in the scope of software modeling, thus allowing the developer to carry on performance analysis throughout the software lifecycle. With this book, Cortellessa, Di Marco and Inverardi provide the cross-knowledge that allows developers to tackle software performance issues from the very early phases of software development. They explain the basic concepts of performance analysis and describe the most representative methodologies used to annotate and transform software models into performance models. To this end, they go all the way from performance primers through software and performance modeling notations to the latest transformation-based methodologies. As a result, their book is a self-contained reference text on software performance engineering, from which different target groups will benefit: professional software engineers and graduate students in software engineering will learn both basic concepts of performance modeling and new methodologies; while performance specialists will find out how to investigate software performance model building.

Database Management Systems: Understanding and Applying Database Technology focuses on the processes, methodologies, techniques, and approaches involved in database management systems (DBMSs). The book first takes a look at ANSI database standards and DBMS applications and components. Discussion focus on application components and DBMS components, implementing the dynamic relationship application, problems and benefits of dynamic relationship DBMSs, nature of a dynamic relationship application, ANSI/NDL, and DBMS standards. The manuscript then ponders on logical database, interrogation, and physical database. Topics include choosing the right interrogation language, procedure-oriented language, system control capabilities, DBMSs and language orientation, logical database components, and data definition language. The publication examines system control, including system control components, audit trails, reorganization, concurrent operations, multiple database processing, security and privacy, system control static and dynamic differences, and installation and maintenance. The text is a valuable source of information for computer engineers and researchers interested in exploring the applications of database technology.

Embedded systems are informally defined as a collection of programmable parts surrounded by ASICs and other standard components, that interact continuously with an environment through sensors and actuators. The programmable parts include micro-controllers and Digital Signal Processors (DSPs). Embedded systems are often used in life-critical situations, where reliability and safety are more important criteria than performance. Today, embedded systems are designed with an ad hoc approach that is heavily based on earlier experience with similar products and on manual design. Use of higher-level languages such as C helps structure the design somewhat, but with increasing complexity it is not sufficient. Formal verification and automatic synthesis of implementations are the surest ways to guarantee safety. Thus, the POLIS system which is a co-design environment for embedded systems is based on a formal model of computation. POLIS was initiated in 1988 as a research project at the University of California at Berkeley and, over the years, grew into a full design methodology with a software system supporting it. Hardware-Software Co-Design of Embedded Systems: The POLIS Approach is intended to give a complete overview of the POLIS system including its formal and algorithmic aspects. Hardware-Software Co-Design of Embedded Systems: The POLIS Approach will be of interest to embedded system designers (automotive electronics, consumer electronics and telecommunications),

micro-controller designers, CAD developers and students.

Modeling and Simulation of Computer Networks and Systems: Methodologies and Applications introduces you to a broad array of modeling and simulation issues related to computer networks and systems. It focuses on the theories, tools, applications and uses of modeling and simulation in order to effectively optimize networks. It describes methodologies for modeling and simulation of new generations of wireless and mobiles networks and cloud and grid computing systems. Drawing upon years of practical experience and using numerous examples and illustrative applications recognized experts in both academia and industry, discuss: Important and emerging topics in computer networks and systems including but not limited to; modeling, simulation, analysis and security of wireless and mobiles networks especially as they relate to next generation wireless networks Methodologies, strategies and tools, and strategies needed to build computer networks and systems modeling and simulation from the bottom up Different network performance metrics including, mobility, congestion, quality of service, security and more... *Modeling and Simulation of Computer Networks and Systems* is a must have resource for network architects, engineers and researchers who want to gain insight into optimizing network performance through the use of modeling and simulation. Discusses important and emerging topics in computer networks and Systems including but not limited to; modeling, simulation, analysis and security of wireless and mobiles networks especially as they relate to next generation wireless networks Provides the necessary methodologies, strategies and tools needed to build computer networks and systems modeling and simulation from the bottom up Includes comprehensive review and evaluation of simulation tools and methodologies and different network performance metrics including mobility, congestion, quality of service, security and more

This book constitutes the proceedings of the 12th IFIP TC 8 International Conference, CISIM 2013, held in Cracow, Poland, in September 2013. The 44 papers presented in this volume were carefully reviewed and selected from over 60 submissions. They are organized in topical sections on biometric and biomedical applications; pattern recognition and image processing; various aspects of computer security, networking, algorithms, and industrial applications. The book also contains full papers of a keynote speech and the invited talk.

This book constitutes the refereed proceedings of the 15th International Conference on Practical Applications of Scalable Multi-Agent Systems, PAAMS 2017, held in Porto, Portugal, in June 2017. The 11 revised full papers, 11 short papers, and 17 Demo papers were carefully reviewed and selected from 63 submissions. The papers report on the application and validation of agent-based models, methods, and technologies in a number of key application areas, including day life and real world, energy and networks, human and trust, markets and bids, models and tools, negotiation and conversation, scalability and resources.

This book constitutes the refereed proceedings of the 14th International Conference on Secure IT Systems, NordSec 2009, held in Oslo, Norway, October 14-16, 2009. The 20 revised full papers and 8 short papers presented were carefully reviewed and selected from 52 submissions. Under the theme Identity and Privacy in the Internet Age, this year's conference explored policies, strategies and technologies for protecting identities and the growing flow of personal information passing through the Internet and mobile networks under an increasingly serious threat picture. Among the contemporary security issues discussed were Security Services Modeling, Petri Nets, Attack Graphs, Electronic Voting Schemes, Anonymous Payment Schemes, Mobile ID-Protocols, SIM Cards, Network Embedded Systems, Trust, Wireless Sensor Networks, Privacy, Privacy Disclosure Regulations, Financial Cryptography, PIN Verification, Temporal Access Control, Random Number Generators, and some more.

The Joint Advanced Strike Technology (JAST) resulted from the decisions of the Secretary of Defense' Bottom Up Review (BUR). Each

service has a demonstrated need for advanced technology aircraft to meet future contingencies, but it was determined that costs for development and production of these several different aircraft could not be met due to budgetary constraints. The BUR found that there were not enough resources available to support all these programs in future years. The decision was made to continue with the Air Force F-22 fighter aircraft, and the F/A-18E/F aircraft for the Navy, but to cancel the A/F-X and the MRF. The decision on ASTOL was to continue that research, but to secure specific commitment of resources by at least two of the three Services before building a flying prototype. The BUR also confirmed the continuing needs that were to be met by the A/F-X and MRF programs. This led to the establishment of the Joint Advanced Strike Technology Program in July 1993.

This book constitutes the refereed proceedings of the 4th International Workshop, PMBS 2013 in Denver, CO, USA in November 2013. The 14 papers presented in this volume were carefully reviewed and selected from 37 submissions. The selected articles broadly cover topics on massively parallel and high-performance simulations, modeling and simulation, model development and analysis, performance optimization, power estimation and optimization, high performance computing, reliability, performance analysis, and network simulations.

The articles presented in this Special Issue cover different aspects of the urban planning process, such as simulation, optimization or decision-making. The authors highlighted the importance of performing an integrated design of the district, considering different sectors, different energy vectors and different operation modes. In order to better integrate renewable and residual energy sources (R²ES), careful design of systems and storage solutions should be performed. Different storage solutions were tested, ranging from large-scale thermal energy storage to vehicle batteries or the thermal mass of buildings. Van der Heijde et al. (2019) proposed a two-layer design optimization algorithm to design a district heating network with solar thermal collectors, seasonal thermal energy storage and excess heat injection. Pajot et al. (2019) also performed an optimization of the sizing and control of energy systems in a district equipped with heat pumps, with thermal energy storage or thermal mass utilization. A hybrid distribution system, coupling the thermal and electrical networks, was proposed by Widl et al. (2019). Arnaudo et al. (2019) used the vehicle-to-grid (V2G) concept to decrease the overloading of the electrical distribution network during heat pump operation. Finally, Kazmi et al. (2019) proposed an integrated decision-making planning approach for a better integration of R²ES in the distribution network. The complexity of urban planning leads to the development of new tools and methodologies. Until now, operation was poorly integrated in the design phase. New urban building energy modeling tools were proposed by the different authors. These tools are either based on co-simulations or integrated solutions to be able to capture the fine dynamics of a district. The difficulty of generating the input data for the models was also discussed. Regarding the methodology, most articles proposed a two-stage optimization procedure to optimize both the operational and design aspects. Mixed-integer linear programming (MILP) and genetic algorithms were often used to find optimal solutions.

This book constitutes the refereed proceedings of the 5th International Workshop on System Analysis and Modelling, SAM 2006, held in Kaiserslautern, Germany in May/June 2006. The 14 revised full papers cover language profiles, evolution of development

languages, model-driven development, and language implementation.

Im ersten Teil dieser Arbeit wird ein Algorithmus vorgestellt, der spannungsabhängige Einspeisung von Wirk- und Blindleistung in den Lastfluss-Algorithmus integriert. Es wird eine Beschleunigung von bis zu einer Größenordnung gegenüber dem derzeit gängigen Verfahren, und eine verbesserte Robustheit erreicht.

Im zweiten Teil wird ein Phasor-Framework zur dynamischen Simulation von Stromnetzen vorgestellt. Die wesentliche Neuheit ist die Möglichkeit der Integration von Zustandsdiagrammen direkt in die Komponentenmodelle. Damit wird eine wesentlich schnellere Modellentwicklung ermöglicht als mit verfügbaren Tools. Im dritten Teil werden Modelle entwickelt und in das Framework integriert. Der Schwerpunkt liegt auf einem Photovoltaik-Modell welches das dynamische $P(V)$, $Q(V)$ und $P(f)$ Verhalten nach VDE 4105 im Bereich Sekunden bis Minuten abbildet.

Im vierten Teil wird das entwickelte Phasor-Framework verwendet, um das Wiedereinschaltverhalten von Photovoltaikanlagen in einem dieselbetriebenen Inselnetz in der Niederspannung zu untersuchen. Die Untersuchung zeigt, dass ein periodisches Ab- und Abschalten von Photovoltaikanlagen vorkommen kann.

This book constitutes the refereed proceedings of the 10th International Conference on Computer Information Systems, CISIM 2011, held in Kolkata, India, in December 2011. The 30 revised full papers presented together with 6 keynote tasks and plenary lectures were carefully reviewed and selected from 67 submissions. The papers are organized in topical sections on networking and its applications; agent-based systems; biometric applications; pattern recognition and image processing; industrial applications; algorithmic applications and data management; information and network security.

The work presents new approaches to Machine Learning for Cyber Physical Systems, experiences and visions. It contains some selected papers from the international Conference ML4CPS – Machine Learning for Cyber Physical Systems, which was held in Karlsruhe, September 29th, 2016. Cyber Physical Systems are characterized by their ability to adapt and to learn: They analyze their environment and, based on observations, they learn patterns, correlations and predictive models. Typical applications are condition monitoring, predictive maintenance, image processing and diagnosis. Machine Learning is the key technology for these developments.

[Copyright: 8c47dfd6c3998f574fab96a94fdc1896](https://doi.org/10.1007/978-3-642-25118-6)