

Editor

Tomas Zelinka



Transport Telematics - Systemic View

Authors:

*Miroslav Svitek
Zdenek Votruba
Tomas Zelinka
Vaclav Jirovsky
Mirko Novak*

Transport Telematics - Systemic View

ISBN: 978-1-61804-144-9



Transport Telematics - Systemic View

Editor

Prof. Tomas Zelinka

Authors

**Miroslav Svitek
Zdenek Votruba
Tomas Zelinka
Vaclav Jirovsky
Mirko Novak**

Transport Telematics - Systemic View

Published by WSEAS Press

www.wseas.org

Copyright © 2013, by WSEAS Press

All the copyright of the present book belongs to the World Scientific and Engineering Academy and Society Press. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the Editor of World Scientific and Engineering Academy and Society Press.

All papers of the present volume were peer reviewed by two independent reviewers. Acceptance was granted when both reviewers' recommendations were positive.
See also: <http://www.worldses.org/review/index.html>

ISBN: 978-1-61804-144-9



World Scientific and Engineering Academy and Society

Preface

Intelligent transport systems (ITS) link information technologies with transport engineering. The ITS objective is to achieve principal transport, travel and forwarding processes services improvement within the existing transport infrastructure. ITS services cover requirements from an individual local case up to the complex wide area solutions with wide scale of services complexity. The telematics services are an integral part of the ITS. They do not represent the only telecommunications solutions, but they are tightly connected with a wide variety of transportation services. “Intelligent” services with the ability to support the relevant environment of the complex system structures are provided. Consequently, this discipline is closely linked with managerial and legal topics due to their ability to principally influence the system behavior.

There are numerous books and publication proceedings on the topic of ITS or transport telematics available but their approach and scope is different from ours. Typically, they describe the impact of ITS systems on traffic management e.g. real-time traffic management, planning of commercial vehicle operations, environmental management, etc. or they present parts of ITS solutions in big detail: e.g. electronic fare management, car navigation systems, fleet management, digital maps, strategies to reduce transport congestions, etc. In this book we introduce a very new system-oriented approach to the ITS design, operation and evaluation with respect to all predefined performance indicators like reliability, safety, security, integrity, etc.

Systems Theory represents a significant theoretical background for any professional undertaking within the branch of ITS. There are several approaches to elaborating this kind of theory, however, for engineering purposes such as the ITS the classical approach called General Theory of Systems (GTS) is usually accepted as the most beneficial. The Systems science within its application areas means resolving tasks. Efficient handling of the systems ideas implies functional knowledge of a wide range of specific mathematical tools.

The ITS applications require wireless seamless secure communications solutions with selectable level of services quality and mostly also with a wide-area coverage. Even though publically available wireless services usually provide reasonable coverage under acceptable cost conditions, most of the public providers do not offer any data service with the guaranteed quality. The principal improvement of the service quality can be reached by the selection of the best possible alternatives from the set of currently identified available services. Efficient decision processes must be adopted to reach the relevant service quality guarantee. Success of such approach relies on profound understanding of applied technologies and their performance described by the performance indicators.

Critical system properties are represented by security aspects. The difference between security and safety must be well understood. Safety assures that a life-critical system behaves as needed even when certain elements fail. Security is a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. Due to the fact that the human being has been a part of a system, security must be understood as a complex of measures leading to the survival of human beings in the system under the influence of an external hostile environment or any other influences. Analysis of potential threats and other security vulnerabilities specific for the telematic system represents the rest of this area. The behavior of a system consists of interactions among elements and it is to be assumed that these interactions have to be undisturbed, i.e. to be secure.

The ITS solutions resolve interactions between systems of a dissimilar nature. The differences can be in its nature, the types of these systems or in the role a particular human subject plays in such an interaction. The functional reliability has to be considered as an important factor specifying the practical applicability of any real system. The ITS system requires to be designed with high functional reliability. The original approach is based on understanding that reliable systems have to be constructed from adequately reliable parts. Such approach can, however, lead to unrealistic and extremely expensive solutions. Besides the usage of solely reliable components the method of lifetime minimization of system functional sensitivity to system parameter changes has been applied. The newest approach developed and used only quite recently has been based on the concept of the so-called prediction diagnostics.

This book addresses scientists, R&D specialists and transport systems designers, as well as students. While the articles were written by experts that are actively involved in the discussed areas research, our intention was to present the texts at a level suitable for a general science and R&D audience. Each article contains a list of references as a point of entry to the comprehensive resources. The preparation of this publication involved generous support from an extended specialist team and we would like to express our sincere thanks to each one of our colleagues.

The Authors

Acknowledgements

The materials used for preparation of this book were reached by research supported by programs of the Czech Ministry of Industry and Business (MPO), Czech Ministry of Transport (MD) via following grants: e-Ident (Electronic identification systems within transport process) MPO 2A-2TP1/108, DOTEK (Communication module for transport telematic applications), MPO 2A-2TP1/105, SRATVU (System Requirements and Architecture of the universal Telematic Vehicle Unit), MPO 2A-1TP1/138, and the project ME 949 of the Czech Ministry of Education.

The Authors

About Authors



Miroslav SVÍTEK
Czech Technical University in Prague, Faculty of Transportations Sciences
Chapter:
<ul style="list-style-type: none"> • Advanced Design of Intelligent transport systems
<p><i>Professor Miroslav Svítek</i> was born in Rakovník, Czech Republic, in 1969. He graduated in radioelectronic from Czech Technical University in Prague, in 1992. In 1996, he received the Ph.D. degree in radioelectronic at Faculty of Electrical Engineering, Czech Technical University in Prague. Since 2002, he has been associated professor in engineering informatics at Faculty of Transportation Sciences, Czech Technical University in Prague. Since 2005, he has been nominated as the extraordinary professor in applied informatics at Faculty of Natural Sciences, University of Matej Bel in Banská Bystrica, Slovak Republic. Since 2008, he has been full professor in engineering informatics at Faculty of Transportation Sciences, Czech Technical University in Prague and Honorary professor at Universidad Autonoma de Bucaramanga in Colombia. He is currently teaching courses and doing research in theoretical telematics, intelligent transport systems, quantum system theory and quantum informatics. Miroslav Svítek is president of Association of transport telematics of the Czech and Slovak Republic (it covers more than 70 public and private organization), Dean of Faculty of Transportation Sciences and Head of Department of Control Engineering and Telematics, Czech Technical University in Prague. He is author or co-author of more than 200 scientific papers and 6 monographs.</p>

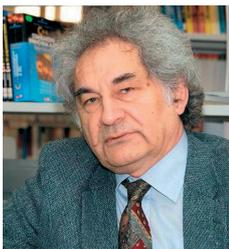


Zdeněk VOTRUBA
Czech Technical University in Prague, Faculty of Transportations Sciences
Chapter:
<ul style="list-style-type: none"> • Systems Theory applied in Intelligent Transport Systems
<p><i>Professor Zdeněk Votruba</i> born in Prague, April 22, 1942. Graduated at the Faculty of Electrical Engineering of the Czech Technical University in Prague in 1964. Carried out his postgraduate studies in Computer Research Institute, Prague (VÚMS) and at the Faculty of Mathematics and Physics of the Charles University, Prague, respectively; PhD degree in Applied Physics received in 1975. In the seventies studied postgraduate course of applied mathematics at CTU in Prague and seminar on informatics and computer architectures at VÚMS. In the period of 1966-1993 worked with VÚMS as a researcher (1966-1976), scientist (1976-1983), director of technological dept. (1983-1990) and technical director respectively (1990-1993). Interested in measurement and instrumentation technologies, computer peripherals, HMI, in the research of thin magnetic films and Computer Systems. Involved in managing of the complex technological projects (e.g. bipolar gate arrays, testers). In 1990-1993 participated in the transformation of an “eastern-style“. Research Institute into the group of market-oriented private companies. In one of them, VUMS-EPOS was active in 1994-5 in the post of managing director. Involved in consultancy services, both for domestic (state administration) and international bodies.</p> <ul style="list-style-type: none"> - In 1996 joined Czech Technical University in Prague, Faculty of Transportation Sciences. - In 2000 gained the scientific – pedagogical degree of Associate Professor in the scientific branch “Engineering Informatics”. - In the period of 2000-2008 he was in the posts of the head of Dept. of Control and Telematics and vice - dean of Faculty. - Since 2005 full professor of Engineering Informatics in Transportation and Telecommunication; Czech Technical University in Prague, Faculty of Transportation Sci. - Reads Lectures in Systems Science and Electronics. - Carries - out research in the fields of Systems Science, HMI, Telematics and Reliability. <p><u>Further activities:</u> In seventies: teaching in postgraduate courses at CTU in Prague, Faculty of Electrical Engineering, 1980-1990: Seminars, consultancy and research at the Charles University, Faculty of Mathematics and Physics.</p>

<p><u>Awards:</u> Gold and Silver Felber's Medals of CTU in Prague; Perner's Medal of Jan Perner University in Pardubice</p> <p><u>Membership in professional communities / bodies:</u></p> <ul style="list-style-type: none"> - Union of Czech and Slovak Mathematicians and Physicists - IEEE (USA) - Scientific Council of the Faculty of Transportation Sciences - Grant Agency of the Czech Republic - Evaluating Committee of the Ministry of Transport, Czech Republic - Branch Council of Engineering Informatics CTU in Prague, Faculty of Transportation Sciences. - Cybernetic Society of the Czech Republic
--



<p>Tomas ZELINKA.</p> <p>Czech Technical University in Prague, Faculty of Transportations Sciences</p> <p>Chapter:</p> <ul style="list-style-type: none"> • Preface • Telecommunications systems for ITS solutions <p><i>Professor Tomas Zelinka</i> - Informatics - CTU in Prague, Ph.D. (CSc.) - experimental physics in the Czechoslovak Academy of Sciences, mgr. (Ing.) - Cybernetics and computer sciences at the Czech Technical University Praha, FEL</p> <p>2005 – Czech Technical University in Prague, Faculty of Transportations Sciences</p> <ul style="list-style-type: none"> - Lectures: basic and advances lectures in area of the telecommunications sciences, legal issues of telecommunications, new trends in telecommunications applied in the Intelligent Transport Systems (ITS), - R&D: theoretical background of specific telecommunications solutions dedicated for the ITS, vehicles Electronic Fee Collection (EFC) and related Value Added Services (VAS), On Board Units architecture, system security etc. <p>1993 – 2005 Communications business</p> <ul style="list-style-type: none"> - Development of the new products, the business development e.g. in area of alternative global voice and data communications in the Czech Republic and the other countries of the CEEMEA region - EuroTel/Nextel/Global One (Sprint Int., France Telecom, Deutsche Telekom) - External lecturer and mentor at the FTS of the CTU in Prague <p>1976 – 1993 Geophysical Institute of the Czechoslovak Academy of Sciences</p> <ul style="list-style-type: none"> - Experimental laboratory and observatory methods in geophysics, studies of the variations and drift of the Earth magnetic field, data communication solutions within international and national observatory system, - Computer modeling of the magnetic material structures with on-line experimental identification, laboratory study of the magnetic properties of rocks, <p>1972 – 1976 Industrial R&D</p> <ul style="list-style-type: none"> - Automatic control systems for the technological processes – CNC, Data communications and computer based control in technological processes.
--



<p>Václav JIROVSKÝ</p> <p>Czech Technical University in Prague, Faculty of Transportations Sciences</p> <p>Chapter:</p> <ul style="list-style-type: none"> • Telematics System Security <p><i>Professor Václav Jirovský</i> had graduated at Czech Technical University, Prague (CTU), Czech Republic, in radioelectronics. In his Ph.D. thesis he introduced application of theory of homogeneous structures in different areas of electronic and especially in the computer modeling. Lately he joined the Regional University Computing Center where he led department of Research and Development. His team had developed a new system for the city transport monitoring and control for Prague City Transport Corporation (PCT), based on combination of radio navigation and microwave communication. For short time he had entered the position of Executive Director for Development in the PCT, but after successful completion of the project he went back to</p>

academia taking senior scientist position at Department of Software Engineering at Faculty of Mathematics and Physics, Charles University, Prague. In 1991 he had received position in Research and Development department of Advanced Computer Applications, Inc. in Newtown, Pennsylvania, U.S.A. finally becoming a director for R&D in the company. He left the company at 1998 joining his original team at Charles University. During years 2001/2002 he accepted position of Executive Director for Technology at Czech Telecom Corporation, lately returning back to Charles University as Associated Professor of Computer Sciences. In the year 2008 he changed position to the Czech Technical University, Faculty of Transportation Sciences, taking chair of Department of Security Technologies and Engineering. In 2007, as a member of Expert Group of the Minister of Transportation of the Czech Republic, he designed a new concept of hybrid system for electronic tolling services. His design of hybrid toll system anticipate ISO/CEN standard for European Electronic Tolling Service and had been evaluated by standardization group as the nearest implementation of EETS.

Mirko NOVÁK

Czech Technical University in Prague, Faculty of Transportations Sciences

Chapter:

- Prediction diagnostics for system reliability

Professor Mirko Novak was born on September 29, 1930 in Prague, Czechoslovakia.

In 1956 he joined the Institute of Radioengineering and Electronics of the Czechoslovak Academy of Sciences in Prague, where was the head of the Department of System Theory.

In 1965 and 1966 he has been the visiting professor of the Department of Electrical Engineering of New York University.

- In 1975 he has founded a new Institute of Computer Science of the Czechoslovak Academy of Sciences. He has been in the position of the director of this Institute for almost 15 years. Since 1965 he is the senior member of the Institute of Electrical and Electronic Engineers, Inc. and in 1988 he becomes the Corresponding member of the Czechoslovak Academy of Sciences.
- His present research interest in the field of neural networks is mainly in the theory of sensitivity and tolerances of neural networks and of their applications for signal processing, time series prediction and system reliability improvement. He is also interested in internal information systems of living bodies and of cells and in the field of the human subject – artificial, namely transportation system interaction reliability. Prof. Dr. Mirko Novák has written more than 150 research reports, about 110 scientific papers, has presented about 200 contributions on scientific conferences, colloquia and seminars and has published almost 30 scientific books in Czech, English and Russian, total - about 500 scientific presentations.

At the end of 1994 he was one of the founders of the Joint Laboratory of System Reliability between the Czech Technical University, Prague, Faculty of Transportation Sciences and the Institute of Computer Science of the Academy of Sciences, Czech Republic.

In 1999 he joined the activity of the workgroup for Neuroinformatics of the Global Science Forum OECD and took part in the preparing of the world research program in neuroinformatics. Since 2000 he is the full professor at the CTU, Faculty of Transportation sciences. He was to 2010 the chairman of the Czech National Node for Neuroinformatics and the Czech representative in INCF (International Neuroinformatic Coordination Facility) of GSF OECD.



Table of Contents

Preface	iii
Acknowledgements	v
Author's Affiliation	vi
1 Advanced Design of Intelligent Transport Systems <i>by Miroslav Svitek</i>	1
1.1 Introduction	1
1.2 ITS Design Methodology	4
1.2.1 ITS System Model	4
1.2.1.1 ITS Architecture	5
1.2.1.2 ITS Market Packages	11
1.2.1.3 ITS Standards	13
1.2.1.4 ITS Data Registry	16
1.2.2 ITS Performance Parameters	17
1.2.2.1 Definition of Performance Parameters	17
1.2.2.2 Quality of Measured Performance Parameters	19
1.2.2.3 Estimation of Performance Parameters	20
1.2.2.4 Illustrative Examples - Simulation Results	24
1.2.2.5 Assessment of Safety Performance Parameters	25
1.2.2.6 Illustrative Example - Geo-Object Detection	26
1.2.2.7 Illustrative example - Cluster of ITS Applications using GNSS	28
1.2.3 ITS Technological Platform	29
1.3 ITS Effectiveness Assessment	30
1.3.1 ITS Evaluation Processes	30
1.3.2 ITS Effectiveness Analyse	30
<i>References</i>	33
2 Systems Theory Applied in Intelligent Transport Systems <i>by Zdenek Votruba</i>	35
2.1 Introduction	35
2.2 Basic Concepts of Systems Sciences	35
2.3 Systems Identification Task	37
2.3.1 Systems Identification - An Intuitive Approach	37
2.3.2 Systems Identification - Elaboration of Concepts	39
2.3.3 Recommended Sequence of Systems Identification	41
2.3.4 Systems Recording	41
2.3.5 Model - System Relationship	41
2.3.6 Ensuring Systems Existence	41
2.3.7 Specific Types of Systems / Models	42
2.4 Interface Task	42
2.5 Systems Structural Tasks	43
2.5.1 Path Task	43
2.5.2 Antecedent and Subsequent Elements Finding Task	43
2.5.3 Feedback Identification Task	44
2.5.4 Finding Elements or Relations with Specific Parameters Task	44
2.5.5 Flow Network Task	44
2.5.6 Systems Decomposition and Integration Task	44
2.5.7 Systems Goals Task	45
2.6 Cybernetics Essentials	46
2.6.1 Control	46
2.6.2 Logic Systems	48

2.6.3	Communication	49
2.6.4	Language	49
2.6.5	Homeostasis	50
2.6.6	Artificial Intelligence (AI)	50
2.7	Behavior Tasks	50
2.7.1	Review of Concepts	50
2.7.2	Basic Model of Behavior	51
2.7.3	Extended Model of Behavior	51
2.7.4	Parallel Behavior Task	55
2.7.5	Alternative Behavior Task	55
2.7.6	Genetic Code (CG) Behavior Task	56
	2.7.6.1 Classes of Behavior in Relation to the Genetic Code (Qualitatively)	56
	2.7.6.2 Analysis of Deviations from the GC (Quantitatively)	56
2.8	Systems Architecture Task	57
2.9	Interoperability Task	57
2.10	Identity Task	58
2.11	Systems Reliability Task	58
	2.11.1 Reliability	59
	2.11.1.1 Reliability of the System Element or a System as a Whole in the Finite Deterministic Automaton	59
	2.11.1.2 Reliability of a System can be Defined in Several Ways [24]	59
	2.11.1.3 Reliability of Complex Heterogeneous Systems	59
	2.11.2 Homogenization	59
	2.11.2.1 Technological level	60
	2.11.2.2 Macro-Physical / Chemical Level	60
	2.11.2.3 Biological Level	60
	2.11.2.4 Social Level	60
	2.11.2.5 Hybridization of Levels	61
	2.11.3 Information Power	61
	2.11.3.1 Information Field	61
	2.11.3.2 Specific Subtasks of Messages Interpretation	61
	2.11.3.3 Definition	63
	2.11.3.4 Relation of IP and Systems Time	63
	2.11.3.5 Information Action	64
	2.11.3.6 Relation IP / Ordering	64
	2.11.3.7 Approaches to the IP Analysis	64
	2.11.4 IP Reliability	65
	2.11.4.1 Interface as a Fictitious System Element	65
	2.11.4.2 System Uncertainty	66
	2.11.4.3 Specification of the Subtask	66
	2.11.4.4 Reliability of the Non-Interacting IF	66
	2.11.4.5 Generalization of the Model for Interacting Interfaces	67
	2.11.4.6 Geometric Re-Interpretation of the Model	68
	2.11.4.7 Model Analysis	68
	2.11.4.8 Discussion of the Combined Effect of IF Dimension and Uncertainty	69
	2.11.5 Reliability in Information Systems	69
	2.11.6 Reliability of Complex Heterogeneous Systems	70
	2.11.7 Reliability of IP - System Abstraction	70
	2.11.8 Construction of Systems Approach to the Reliability of Information Power	70
	2.11.9 Discussion	71
2.12	Alliances Task	72
	2.12.1 Introduction	72
	2.12.2 Essentials of the Theory of Systems Alliances	73

2.12.3	Alliances and Information Power	74
2.12.4	Models of Interfaces in Alliances	74
2.12.5	Alliance Control	75
2.12.6	Conclusions	77
2.13	Soft Systems Tasks	78
2.13.1	Overview of Basic Concepts	78
2.13.2	Sources of Systems Uncertainty	78
2.13.3	Comparison of "Hard" and "Soft" Methodologies	78
2.13.4	Soft Systems Analysis Techniques	79
2.13.4.1	SWOT Analysis	79
2.13.4.2	Force Field Analysis	80
2.13.5	Soft Systems Methodologies (SSM)	81
2.13.5.1	Action Research - Jenkins	81
2.13.5.2	Checkland Soft - Systems Methodology [23]	82
2.13.6	Meta-Level Process Model for Systems Analysis of Soft Systems - NIMSAD	83
	<i>References</i>	84
3	Telecommunications Systems for ITS Solutions <i>by Tomas Zelinka</i>	87
3.1	Introduction	87
3.2	Position of Telecommunications Solutions in ITS Solution	88
3.2.1	Telecommunications Performance Indicators	90
3.2.1.1	Service Activation Time (SAT)	90
3.2.1.2	Service Availability	90
3.2.1.3	MTBF (Mean Time Between Failure)	90
3.2.1.4	MTTR (Mean Time to Restore)	90
3.2.1.5	Delay	91
3.2.1.6	Packet/Frames Loss	91
3.2.1.7	Security	91
3.2.1.8	Class of Service - (CoS)	92
3.2.2	Communications Design Methodology	92
3.2.3	Wireless Telecommunications Alternative used in ITS Solutions	94
3.2.3.1	Publically Available Services with National/Global Coverage (Europe based)	94
3.2.3.2	Locally Available Mostly as No Publically Served Services	94
3.3	Telecommunications Systems	95
3.3.1	Basic Telecommunications Solutions Properties	96
3.3.2	Types of Network According to Topology	96
3.3.3	Types of Network According to the Hierarchy within a Network	97
3.3.4	Types of Networks According to the used Physical Layer	97
3.3.4.1	Metallic	97
3.3.4.2	Fiber	98
3.3.4.3	Radio Frequencies Solutions	98
3.3.5	Circuit and Packet Oriented Telecommunication Systems	98
3.3.6	TCP/IP Architecture	99
3.3.6.1	TCP - Transport Control Protocol	99
3.3.6.2	IP - Internet Protocol	99
3.3.6.3	IP Addressing	100
3.3.6.4	Routing	101
3.3.6.5	AS - Autonomous Systems	101
3.3.6.6	Summary of TCP/IP Properties	101
3.4	Backbone Networks	102
3.4.1	Basic Description of WDM	102
3.4.1.1	DWDM	104
3.4.1.2	CWDM	104

3.4.1.3	CWDM vs. DWDM	105
3.4.1.4	WDM - Conclusions	106
3.4.2	SDH/SONET	106
3.4.2.1	PDH	106
3.4.2.2	SDH Architecture	107
3.4.2.3	SDH Network Architecture	107
3.4.3	The ATM	108
3.4.3.1	ATM Architecture	108
3.4.3.2	Protocols of ATM Adaption Layer	108
3.4.3.3	ATM Performance	108
3.4.4	ETHERNET - IEEE 802.3 and ISO 8802	109
3.4.4.1	IEEE 802.3 and IEEE 802.1q Standards - Alternative Telecommunication Networking	109
3.4.4.2	“Ethernet” and its Applicability in WAN	110
3.4.4.3	Convergence Times Reduction	111
3.4.4.4	Backbone Solutions based on “Ethernet”	112
3.4.5	IP Virtual Private Networks (VPN) Solution	112
3.4.5.1	MPLS IP VPN	113
3.4.5.2	MPLS IP VPN vs. L2 VPN	113
3.5	Access Wireless Mobile Solutions	113
3.5.1	Mobile Telecommunications Services	115
3.5.1.1	DTMF (Dual Tone Multiple Frequency)	115
3.5.1.2	CSD (Circuit Switched Data)	115
3.5.1.3	HSCSD (High Speed Circuit Switched Data)	115
3.5.1.4	IBS (Inband Software modem)	115
3.5.1.5	SMS (Short Message Service)	116
3.5.1.6	GPRS (General Packet Radio Service)	116
3.5.1.7	EDGE (Enhanced Data Rates for GSM Evolution)	116
3.5.1.8	CDMA (Code Division Multiple Access)	116
3.5.1.9	UMTS (Universal Mobile Telecommunication System)	117
3.5.1.10	LTE	117
3.5.2	WiFi - IEEE 802.11	119
3.5.2.1	MAC (Media Access Control) Layer of WiFi Networks	119
3.5.2.2	IEEE 802.11a	119
3.5.2.3	IEEE 802.11b	119
3.5.2.4	IEEE 802.11g	120
3.5.2.5	IEEE 802.11e - Wireless QoS	120
3.5.2.6	IEEE 802.11i	121
3.5.2.7	IEEE 802.11n	121
3.5.2.8	IEEE 802.11p	122
3.5.2.9	IEEE 802.11r	122
3.5.2.10	IEEE 802.11 - Conclusions	122
3.5.3	WiMax	122
3.5.3.1	WiMax– IEEE 802.16d	122
3.5.3.2	Mobile WiMax - IEEE 802.16e	123
3.5.4	PAN	123
3.5.4.1	Bluetooth - IEEE 802.15.1	124
3.5.4.2	UWB (Ultra-WideBand) - IEEE 802.15.3	124
3.5.4.3	ZigBee - IEEE 802.15.4	125
3.5.5	DSRC (Dedicated Short-Range Communications)	127
3.5.5.1	DSRC 5.8	127
3.5.5.2	DSRC 5.9 - WAVE	128
3.5.6	Wireless Access Telecommunications Solutions Conclusions	129

3.6	Selected Wireless Telecommunications Services Performance	129
3.6.1	Mobile Services GSM	129
3.6.1.1	Methodology of Experiment	130
3.6.1.2	CSD Measurement Results	130
3.6.1.3	HSCSD Measurement Results	131
3.6.1.4	GPRS Measurement Results	131
3.6.1.5	EDGE Measurement Results	131
3.6.1.6	GSM data Services Summary	132
3.6.2	WiMax (IEEE 802.16d) Measurement Results	132
3.6.3	WiFi (IEEE 802.11) Measurement Results	133
3.7	Multi-Path Access Solution Structure	134
3.7.1	Basic Ideas of the CALM Approach	134
3.7.2	The IEEE 802.21 Standard	138
3.7.2.1	The IEEE 802.21 Reference Model	138
3.7.2.2	Media-Independent Event Service	139
3.7.2.3	Media-Independent Command Service	139
3.7.2.4	Media-Independent Information Service	139
3.7.2.5	Service Management	140
3.7.2.6	Media-Independent Handover Protocol	140
3.7.2.7	MIH Communication Model	140
3.7.2.8	Handover Execution	140
3.7.3	Alternative Approach based on the “Intelligent Routing”	140
3.7.3.1	The DOTEK	141
3.7.3.2	Generalized DOTEK Architecture	143
3.7.4	Adaptive Decision Processes	143
3.7.4.1	Estimation and Prediction of Measured Performance Data Vector $p(n)$	144
3.7.4.2	Path Selection as Classification Process	145
3.8	Conclusions of Section Telecommunication Systems for ITS Solutions	147
	<i>References</i>	148
4	Telematics System Security by Vaclav Jirovsky	151
4.1	Introduction	151
4.2	Security Models	153
4.3	Cryptography	154
4.3.1	Basic Cryptosystems	155
4.3.1.1	Transposition Ciphers and Substitution Ciphers	156
4.3.1.2	Vigenere Cipher and one Time Pad	158
4.3.2	Data Encryption Standard - DES	160
4.3.2.1	Feistel Networks	161
4.3.2.2	DES Modes of Operation	163
4.3.2.2.1	Electronic Codebook (ECB) Mode	163
4.3.2.2.2	Cipher Block Chaining (CBC) Mode	164
4.3.2.2.3	Cipher Feedback (CFB) Mode	164
4.3.2.2.4	Output Feedback (OFB) Mode	165
4.3.2.3	Strengthening DES	165
4.3.2.3.1	Double-DES (2DES)	165
4.3.2.3.2	3.5.2 Triple-DES (3DES)	166
4.3.2.3.3	3.5.3 DESX	166
4.3.3	Other Used Ciphers	167
4.3.4	Public Key Cryptography	167
4.3.4.1	Diffie-Hellman Coding	168
4.3.4.2	Mathematical background for RSA	168
4.3.4.3	RSA Cryptography	169
4.3.5	Cryptographic Checksum	171

4.3.6	Keyless hash function HMAC	173
4.3.7	Cipher Techniques - Block and Stream Ciphers	173
4.3.8	Cryptography in Networks	176
4.4	Attack Analysis	179
4.4.1	Attacks by a User	180
4.4.1.1	Attacks on Sensors and OBU Input Data	180
4.4.1.2	Attacks on OBU itself	181
4.4.1.3	Attacks on OBU Data	181
4.4.1.4	Specific User's Attacks	182
4.4.1.5	Foiling the System	182
4.4.1.6	Protecting the User Own Privacy	182
4.4.2	Attacks by Service Provider	183
4.4.2.1	Attacks to Increase Revenue from Customer or Overcharging Customer	183
4.4.2.2	Attacks to Profile a Customer	183
4.4.2.3	Attacks to Resale Data on Customers	183
4.4.2.4	Attacks on Reduction in Payments to Toll Charger	184
4.4.3	Attacks by Service Charger	184
4.4.3.1	Attacks to Increase Revenue	185
4.4.3.1.1	Attacks on Charge Data	185
4.4.3.1.2	Attacks on Billing Details	185
4.4.3.1.3	Data Repudiation Attacks	185
4.4.3.2	Reselling the Data and Specific Information	185
4.4.4	Attacks by Hacker	185
4.4.4.1	Demonstration of System Vulnerability	186
4.4.4.2	Exhibitionism	186
4.4.4.3	Research Attacks	187
4.4.5	Attacks by Hacktivist or Terrorist	187
4.4.5.1	Social Destabilization through Manipulation of the Telematic System	188
4.4.5.2	Raise in Profile of the Activists Cause	188
4.4.5.3	Direct Furthering of Activists Cause	188
4.4.5.4	Reduction in Credibility of the System	189
4.4.6	Communication Provider Attacks	189
4.4.6.1	Change in Network Utilization	189
4.4.6.2	Collecting the Travel Behavior	189
4.4.7	Attacks by Enterprise	189
4.4.7.1	Movement Tracking	189
4.4.7.2	Creation and Distribution of Cloned Equipment	190
4.4.7.3	Attack to Disable or Compromise System Encryption	190
4.4.7.4	Stealing Equipment	190
4.4.7.5	Racketeering	190
4.4.8	Attacks by Government	191
4.4.8.1	In Theatre Commercial Advantage	191
4.4.8.2	Political Targeting of Individuals and Organizations	191
4.4.8.3	Tracking of Individuals	191
4.4.9	Attacks by Foreign Power	192
4.4.9.1	Social Destabilization	192
4.4.9.2	Movement Tracking	192
4.4.9.3	Racketeering	192
4.4.9.4	International Prestige	193
4.5	Asset based Threat Analysis	193
4.5.1	Threatened Assets	193
4.5.2	Taxonomy of Threats	194

4.5.2.1	The Basic Threats	194
4.5.2.2	The Activation Threats	194
4.5.2.3	The Underlying Threats	195
4.5.3	Threats, Objects and Assets	197
4.6	Technology of Wireless Attacks	199
4.6.1	Eavesdropping	199
4.6.1.1	Security on Physical Layer of the System	200
4.6.2	Attack on Authentication	204
4.6.2.1	Passwords and Attack on Passwords	205
4.6.2.2	Challenge-Response Method	206
4.6.3	Skimming	207
4.6.4	Hiding and Jamming	207
4.6.4.1	Antijamming Techniques at Physical Layer	208
4.6.4.2	Antijamming Security Schemes	211
4.6.4.2.1	Proactive Countermeasures	211
4.6.4.2.2	Reactive Countermeasures	214
4.7	Conclusion	215
	<i>References</i>	216
5	Prediction Diagnostics for System Reliability <i>by Mirko Novak</i>	221
5.1	Introduction	221
5.2	General Aspects of System Reliability Theory	222
5.2.1	System Structures	222
5.2.2	Structures of Heterogeneous Systems	225
5.3	System Operation Reliability and Safety	227
5.3.1	Prediction Diagnostic	228
5.3.2	Hybrid Systems	229
5.4	Brief Survey of Conventional Prediction Diagnostic Methodology	231
5.4.1	System (or Alliance) Models	231
5.4.2	Investigation of Regions of Acceptability	232
5.4.2.1	Direct Approach	237
5.4.2.2	Indirect Methods of RA Analysis	247
5.4.2.3	Stochastic Approaches to RA Investigation	253
5.5	Failure Risks (Hazards) Analysis	255
5.5.1	Contemporary Artificial Systems and System Alliances and Data Structures Representing them	259
5.5.2	Possibilities of Multidimensional Data Storing	261
5.5.3	Possibilities of Multidimensional Data Analysis and of Mining the Hidden Knowledge	264
5.5.4	Possibilities of Multidimensional Data Representation and Analysis, especially for Reliable Human Subject Interaction	274
5.6	Prediction Diagnostic in Multi-Parameter Systems	278
5.7	Conclusion	281
	References	283
	Subject Index	285

SUBJECT INDEX

A

Access Network, 31, 97, 98, 123, 138, 139
 Access Wireless Mobile Solutions, 113
 Accident, 28, 50, 74, 151, 179, 193, 199, 208, 227, 256
 Accuracy, 17, 19, 21, 22, 24, 28, 37, 70, 79, 81, 87, 92, 226, 231, 274
 Activation Threats, 194
 Adaptive Decision Processes, 143
 Alliance Control, 73, 75, 265
 Alternative Behavior, 55
 Antecedent, 43, 44, 45
 Antijamming, 206, 210-216
 Artificial Intelligence, 50
 Artificial systems, 221, 255, 259
 AS, 101
 ASN.1, 13, 15, 16
 ATM, 95, 96, 100, 101, 102, 107-112, 121, 123, 177
 ATM Architecture, 108
 Attack by Enterprise, 189
 Attack by Foreign Power, 179, 192
 Attack by Government, 191
 Attack by Hacker, 185
 Attack by Service Charger, 184
 Attack by Service Provider, 183
 Attack on OBU, 181
 Attack on OBU Data, 181
 Attack on Sensor, 180
 Authentication, 91, 101, 117, 121, 169, 172, 173, 178, 204
 Availability, 4, 18, 19, 28, 87, 90, 96, 106, 112, 129, 141, 147, 152, 199, 215

B

Backbone Networks, 97, 102
 Back-door, 195
 Base Station, 88, 89, 116, 118, 122, 130, 138, 214
 Basic Encoding Rules (BER), 16
 Basic Threats, 194, 195, 196
 Behavior, 40, 50, 51, 55, 56, 189
 BER (Bit Error Rate), 137
 Block Cipher, 163, 165, 174
 Bluetooth, 89, 114, 124

C

CALM, 90, 92, 94, 114, 122, 131, 134
 CAT, 97
 CDMA, 106, 116, 118

Cellular Layer, 136
 Classes Separability, 146
 Communication, 49, 127, 140, 189
 Communication Architecture, 5
 Complementary Information, 204
 Complementation Functions, 204
 Constant Jamming, 212
 Consumer Privacy, 152
 Continuity 18, 87, 92
 Core Business, 88, 95, 132
 CoS, 92, 96
 Cost-Benefit Analyze (CBA), 4, 30
 Cryptographic Checksum, 171
 Cryptography, 154, 167, 169, 176, 204
 CSD, 94, 113, 115
 CSD Measurement Results, 130
 CWDM, 102
 Cybernetics, 37, 46

D

Data Privacy, 152
 Deceptive Jamming, 208
 Decomposition, 44, 51, 87, 125, 197
 Delay, 19, 91
 Denial of Service, 188, 194
 Design Centering, 233
 Distinguished Encoding Rules (DER), 16
 DOTEK, 141, 143, 147
 DSRC, 6, 29, 94, 113, 127
 DSRC 5.8, 94, 127, 210
 DSRC 5.9 – WAVE, 95, 127, 128, 129
 DTMF, 94, 113, 115
 Duplex, 98, 117, 122
 DWDM, 98, 102, 103

E

Economic Impact, 118
 EDGE Measurement Results, 131
 Electronic Toll Collection (ETC), 2, 127, 184
 Elementary Catastrophe, 249
 Elements, 39, 44
 Environmental Functions, 223
 ERTICO, 1, 2
 ETHERNET, 89, 95, 109, 110, 113, 122
 Expectation-Maximization (EM) Algorithm, 146
 Exposure, 256
 Extended Kalman Filtering, 145

F

Fail Safe, 28, 151
 Failure Risks Analysis, 255
 False Alert, 26, 27, 151
 Feedback, 44, 92, 154, 165, 175, 214, 237
 Feistel Networks, 161
 First Generation of Handover, 136
 Flow Network Task, 43, 44
 Frequency Hopping Spread Spectrum, 124, 210
 Functional Architecture, 5
 Functional Blocks, 28, 221, 225, 231, 237, 252

G

Galileo, 88
 Generalized DOTEK Architecture, 143
 Genetic Code, 40, 45, 56, 73, 229
 Global Navigation Satellite Systems (GNSS), 28
 GNSS, 6, 28, 88, 127, 180
 Goals, 45, 50, 70, 80, 122, 178, 187, 193
 GPRS, 94, 113, 116, 130, 141
 GPRS, Measurement Results, 131, 141
 GPS, 27, 88, 101, 106, 132
 GSM, 29, 94, 113, 127, 137, 147
 GSM Date Services, 132

H

Half Duplex, 98
 Handoff, 134
 Handover, 92, 114, 118, 122, 129, 134, 138, 140, 143
 Hazard Criteria, 256
 Hazards, 256, 261, 281
 Heterogeneous IEEE 802 Networks, 134
 Heterogeneous Systems, 59, 70, 222
 HMI (Human Machine Interface), 89
 Homeostasis, 50
 Homogenization, 38, 59, 60, 222, 230
 Homogenous Systems, 224
 HSCSD, 94, 113, 130
 HSCSD Measurement Results, 131
 Hybrid Systems, 59, 68, 72, 224, 230
 HYPER-Ring, 111
 Hysteresis, 248, 252

I

IBS, 115, 116
 Identification, 36, 37, 41, 44
 Identity, 40, 58, 204, 229
 IEEE 802.11a, 119, 128
 IEEE 802.11b, 119, 120
 IEEE 802.11e, 119, 120, 122, 128, 134

IEEE 802.11g, 120
 IEEE 802.11i, 121
 IEEE 802.11n, 121
 IEEE 802.11p, 122, 129, 137
 IEEE 802.11r, 122
 IEEE 802.15, 134
 IEEE 802.15.1, 114, 124
 IEEE 802.15.3, 124
 IEEE 802.15.4, 123, 125
 IEEE 802.16d, 94, 114, 122, 123, 132, 147
 IEEE 802.16e, 114, 123, 129
 IEEE 802.1q, 109, 110, 111
 IEEE 802.21 Reference Model, 138
 IEEE 802.21 Standard, 90, 134, 138
 IEEE 802.3, 109, 112, 122
 Independent Variables, 68, 72, 221, 228, 231, 236, 247, 274, 281
 Information Architecture, 5, 7
 Information Power, 59, 61, 69, 71
 Initiator, 5, 87
 Integration, 7, 19, 44, 115, 125
 Integrity, 18, 28, 44, 59, 87, 92, 153, 194
 Intelligent Routing, 90, 140
 Intelligent Transport Systems (ITS), 1, 87
 Interaction, 35, 151, 187, 221, 255, 258, 274, 277
 Interaction Coupling, 229
 Interface, 42, 89, 91, 180, 198, 225
 Internal Rate of Return (IRR), 4, 30
 Interoperability, 2, 17, 57, 71, 118, 199
 IP, 61, 63, 71, 74, 89, 99, 109, 112, 130, 141
 IP Addressing, 100, 128
 ISO, 255
 ITS, 1, 5, 11, 13, 16, 29, 30, 79, 88
 ITS Architecture, 4, 5, 12, 29, 87
 ITS Data Registry, 4, 13, 16
 ITS Databases, 4
 ITS Effectiveness, 4, 30
 ITS Market Packages, 4, 11, 12, 29
 ITS Performance Parameters, 17
 ITS Requirements, 95, 117
 ITS Standards, 4, 13, 17
 ITS System Model, 4
 ITS Technological Platform, 29

J

Jamming, 181, 193, 207, 208, 211-215

K

Kalman Filtering Algorithm, 145
 Kernel Function, 145
 Keyless Hash Function, 173

L

Language, 41, 49, 65, 76, 155, 230
 Laplace Density Function, 146
 Laplace Kernel, 146
 Life Curve, 224, 229, 231, 236, 278
 Life-Time, 221, 280
 LTE 94, 113, 115, 117, 129

M

M from N, 25
 M5, 122, 135, 137
 MAC, 109, 120, 140, 172, 209, 212
 MAN, 95, 109, 111, 113
 Masquerading, 194, 197
 Mass Market, 88, 96, 118
 Medical Privacy, 152
 Mobile WiMax, 94, 123, 129, 132, 136, 141, 147
 Model, 41, 51, 68, 83, 138, 140
 MPLS, 91, 95, 99, 101, 113
 MTBF (Mean Time Between Failure), 19, 90
 MTTR, 19, 90, 102, 109, 112
 Multi Mode Optical Fiber, 98
 Multi-Path Access, 134
 Multipath Regime, 88

N

Natural Hazard, 256
 Natural Systems, 221
 Net Present Value (NPV), 30

O

OBU (Out Board Unit), 88
 Optimization, 47
 Organisation Architecture, 5
 Organization Security, 153

P

Packed Encoding Rules (PER), 16
 Packet/Frames Loss, 19, 91
 PAN, 113, 123
 Parallel Behavior, 55
 Parameter Synchronization, 14
 Parts, 5, 31, 38, 42, 60, 76, 88, 100, 175, 188, 199, 222
 Password, 197, 204, 205, 206
 Path, 43, 52, 56, 82, 94, 101, 108, 134, 145
 PBT, 102, 107, 110, 111, 112, 113
 PDH, 106, 107
 Performance, 4, 17, 19, 25, 28, 87, 90, 108, 129, 144, 147, 201
 Personal Security, 153
 Physical Architecture, 5, 11, 30

Physical Layer, 97, 100, 109, 119, 122, 177, 200, 208
 Political Privacy, 152
 Prediction Diagnostic, 228, 231, 278, 281
 Prediction Diagnostic in Multi-Parameter Systems, 278
 Prediction Diagnostic Methodology, 231
 Probability, 17, 18, 20, 25, 54, 71, 90, 146, 152, 171, 203, 228, 236, 254, 256, 276
 Product Security, 153
 Production Wreck, 234
 Profitability Index (NPV/I), 30
 Protocol Synchronization, 13, 15
 Public Key Cryptography, 167
 Public Providers, 88, 115
 Public Telecommunications, 88, 115

Q

QoS, 94, 102, 108, 119, 120, 140
 Quality, 19, 47, 50, 88, 102, 120, 125

R

Radial Sprouting, 254
 Random Jamming, 212
 Reactive Jamming, 212
 Reference Architecture, 5, 6
 Regions of Acceptability, 226, 232
 Relations, 35, 44
 Reliability, 18, 21, 54, 58, 59, 65, 70, 222, 227
 Restoration Procedure, 234, 275, 279
 Right Detection, 26
 Risk Analysis, 18, 58, 91, 197, 256
 Risk Criteria, 256
 RM OSI, 100, 127, 134
 Routing, 90, 101, 113, 125, 140, 177, 214
 RSTP, 111, 113
 RTD (Round Trip Delay), 130, 136

S

Safety, 11, 25, 151, 221, 227
 SAT, 90
 SDH, 102, 106, 107
 SDH Architecture, 107
 Second Generation of Handover, 129, 136, 143
 Security, 19, 88, 91, 126, 151, 179, 200, 211
 Security Models, 153
 Service Activation Time, 19, 90
 Service Availability, 90
 Services Performance, 95, 129
 Simplex, 98
 Single Mode Optical Fiber, 98
 SLA, 89, 96, 102, 111, 129
 SMS, 94, 113, 116

Social Engineering, 199
 Social Destabilization, 188, 192
 Soft Systems Analysis Techniques, 79
 Soft Systems Methodologies (SSM), 81
 Soft Systems Tasks, 78, 81
 SONET, 102, 104, 106, 111
 STP, 97, 110, 111, 112
 Stream Cipher, 165, 174, 175
 Structural Tasks, 43
 Subsequent Elements, 43
 Subsystem, 5, 44, 75, 87, 180
 System, 4, 36, 37, 41, 42, 44, 50, 87, 151
 System Alliances, 68, 77, 222, 256, 259, 281
 System Approach, 31, 70
 System Functions, 18, 51, 221, 223-226, 247, 251, 278
 System Parameters, 5, 6, 17, 87, 101, 119, 125, 133, 183, 223, 247, 281
 System Reliability, 222, 228, 236
 System Reliability Theory, 222
 System Safety, 221
 System Security, 153
 System Structures, 137, 222
 System Vulnerability, 186
 Systems, 1, 35, 39, 40, 42, 73, 78, 87, 98, 147, 151, 215, 221, 259
 Systems Architecture, 57, 71, 134
 Systems Reliability, 58, 59, 70, 226
 Systems Uncertainty, 59, 78

T

TCP, 99, 102
 TCP/IP, 91, 95, 101, 109, 123, 134, 140
 TCP/IP Architecture, 89, 99, 135
 Technological Hazard, 256
 Telecommunications Performance Indicators
 88, 90, 95, 134
 Telematic System 19, 119, 152, 179, 188, 215
 Terminator, 5, 87
 The Data Encryption Standard, 160
 Theory of Systems Alliances, 73
 Time Synchronization, 13, 184, 214
 Trans-European Network for Transport (TEN-T), 2
 Transport Telematics, 1, 13, 28, 79, 95, 134, 141
 Transposition Cipher, 156, 161
 Trojan Horse, 195, 197

U

UMTS, 94, 113, 117, 129, 132, 147
 Underlying Threats, 194, 195
 UTP, 97
 UWB, 114, 123, 124, 135, 211

V

Vigenère, 158, 160, 175
 VPN, 111, 112, 113
 Vulnerability, 167, 175, 186, 190, 196, 215, 256

W

WAN, 31, 95, 109, 110, 180, 198
 WDM, 102, 106
 Well Designed System, 233
 WiFi, 29, 94, 115, 122, 133, 147, 199
 WiFi (IEEE 802.11) Measurement Results, 133
 WiMax, 94, 122, 147
 WiMax - IEEE 802.16, 94, 141
 WiMax (IEEE 802.16d) Measurement Results, 132

Y

Yield, 168, 223, 233

Z

ZigBee, 89, 114, 123, 125, 134