REFERENCES

1. Sauder, R.L., and Westerman, W.M. 'Computer Aided Train Dispatching: Decision Support Thru Optimization,' Norfolk Southern, 1982.
2. 'Management of Train Operations and Train Handling,' *Air Brake Association*, 1972.
3. Wright, P.C., 'Computer Assisted Dispatching,' *Proceedings of the Railway Fuel and Operating Officer's Association*, 1985.

Reliability and Availability Considerations about Electronic Train Detection System

E. Spina, M. Martucci, Jr.

Department of Computer Science and Digital Systems, Polytechnic School, University of São Paolo, Brazil

ABSTRACT

This paper presents some considerations about the reliability and availability evaluation of a Trains Detection System designed using axle counter method and implemented with redundant distributed microprocessor architecture.

The System was designed using modern and structured design methodology for software and hardware which provides better degrees of reliability with low money expenses.

The System architecture and design methodology furnished estimated failure rates of 52.475 x 10E-6 per hour or a MTTF (Mean Time To Fail) of 2.2 years for each counting point and a availability of five nines. By the way was obtained a MTBUF (Mean Time Between Unsafe Failures) of 69 years.

The paper presents a brief description of the system hardware architecture, showing the modules and elements, specially the axle counter. Following the Reliability and Availability of all system is discussed comparing the degrees obtained for the system.

INTRODUCTION

This paper presents the estimation method for the Reliability and Availability Index for the Electronic Train Detection System (DET) developed at Digital Systems Laboratory of Escola Politécnica da Universidade de São Paulo, through Foundation for

The project had been sponsored by CMSP (São Paulo Metropolitan Subway Company) to be installed at Itaquera Train Yard where the new equipment would be homologated.

In the next sections it will be described the parts of DET and the process used for estimation of its Reliability and Availability marks.

BRIEF DESCRIPTION OF THE DET

DET implements the first level of data aquisition for the signalling system, that assures reliability for the railway. With the status informations of the "track circuits" (train detection) the Trains Movement Controler (CMT) makes the route interlocking to the safe trains movement in the yard.

DET uses the axle counter method. The axle counter is a very usual method in many countries, but there are no informations of its commercial use, in such application, in Brazil. The operation principle is: count the number of axles in a track section delimited by axles sensors, subtract the number of outgoing axles and add the number of incoming ones. This method uses puntual sensors in a continuous signalized sector. The basic system is presented in figure 1.

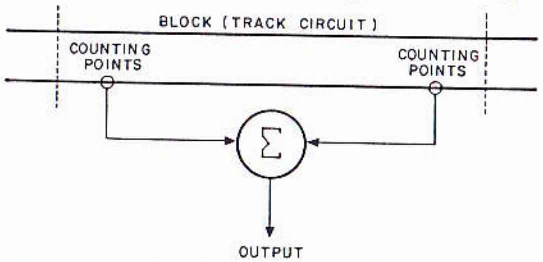


Figure 1 - Axle counter basic schema

DET is implemented by a number of wheels sensors and by a computing equipment (of the number of axles in each sector). The sensors are implemented with infra-red light technology, designed with fail-safe philosophy, and the axle counter is implemented by a number of microprocessor boards interconnected in a triplicated computing array. The fail-safe design and the compared redundancy adds an appropriate reliability and availability to the system, as will be evaluated in this paper.The great number of sectors needed for convenient yard departu[illegible] operations lets to its division in blocks. Each bl[illegible] receives a axle counter equipment.

Each axle counter equipment is responsible for the supervision of 64 counting points. This division makes easy the implementation of the axle counters and minimizes the cable needs [1] [2] [3].

The electronic interlocking, that receives the information about the occupation of each track-circuit, is triplicated and works in the compared redundancy, with the accordance of, at least, two of the three processors systems. The control actions takes place after the vital voting [4].

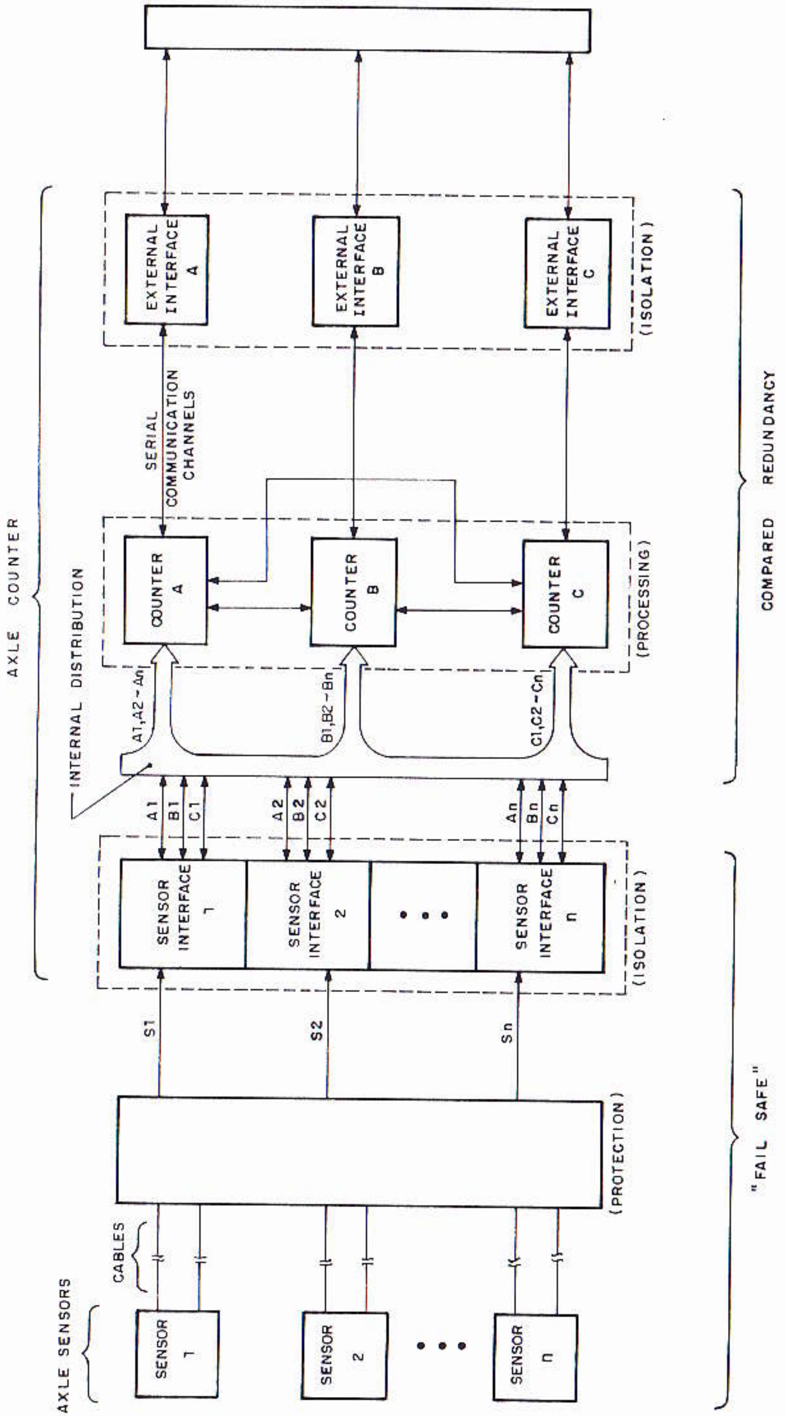
The axle counters are triplicated allowing a simple interconnection scheme, with each channel of the counter (interlocking processor system) interconnected to each wheel sensor. The security of the detection is also assured by the vital votation to generate the outputs. There exists an internal votation in the DET, that performs the auto-diagnosis functions. A block diagram of the DET may be observed at figure 2.

AXLE COUNTER

The historical development efforts of the axle counters induces some choices about the technological aspects of a new development in this area. The way of the evolution, from the electromechanical counters [5], passing through the logic gates and fail-safe memories [6], to the digital gates with TTL technology associated with a functional supervisor for better reliability [7], and the natural increasing of digital circuits integration, the auto-test, the diagnosis and the software votation technics, leads to microprocessors systems.

The axle counter of the DET system was developed and implemented with digital technology, considering its simplicity and low costs without compromising its reliability level.

The axle counter analyses the signals generated by the sensors and performs the characterization of the wheel passage, determining the direction of the movement, counting the axles in a block, and determining the occupation state of the block. This is a simple job when the implementation of the system is made by microprocessors in a convenient architecture.



The reliability characteristics are based on compared redundancy, where two or more elements do the same job in an independent way, and each result is compared and voted. In case of doubt, the system provides the safe state. The compared redundancy is the most adequate solution, because it permits the use of microprocessors in reliable systems, considering that microprocessors themselves are not enough reliable.

The counter function is executed by an equipment implemented by a chain of microprocessors, operating in a parallel mode. The architecture was especially developed for this application. The information about the state of each block is sent to the higher level systems, like the Centralized Traffic Control System and the Interlocking System, by serial communication channels.

The performance and the flexibility of the counter system are provided by its multiprocessors architecture, that permits till sixteen microprocessor boards working in parallel, with communication between them provided by internal serial channels. The architecture of the counter system permits the combination of configurations, with redundant elements and functions, that become manifest in the improvement of the availability and reliability on all system.

The axle counter module (MCX) is implemented by a group of printed circuit boards of digital processors, interconnected by a bi-directional multipoint internal serial channel. This arrangement characterizes the MCX as a multiprocessor system, where each processor executes distinctive work and may cooperate with other processor by the communication channel. This characteristic allows a distribution of the entire job in a number of processors working together, and new works can be made by the allocation of new jobs in the microprocessors of the array, without degradation at the system performance.

RELIABILITY OF THE COUNTER SYSTEM

In this item the reliability and availability indexes of the DET system are evaluated.

The designers had evaluated the reliability index of each element, to get better design decisions. This indexes can not be considered in a formal reliability analysts. These dependency may carry all the polarizations that could be present in the conception design, but it is useful and necessary as a way to evaluate the goals. The references [8] [9] made equivalent analysis.

All the indexes were obtained by the component counting method, all the failure rates was gotten from the MIL-HDBK-217-D of the Defense Department of the United States [10]. The ambient was defined as "Ground-mobile", Gm, that means severe conditions. The obtained failure rates are listed in table 1.

TIV	3,86472	10E-6/h	72.126 h
RIV	8,21842	10E-6/h	35.438 h
PRS	0,19242	10E-6/h	98.112 h
IRS(sensor side)	0,2	10E-6/h	5 E+6 h
IRS(count.side)	6,20837	10E-6/h	161.07 h
PP	26,99255	10E-6/h	37.047 h
PM	49,18040	10E-6/h	20.333 h
ISO	17,61816	10E-6/h	56.760 h
FCM	36,54126	10E-6/h	27.366 h

TIV - Optical Transmitter
RIV - Optical Receiver
PRS - Voltage pre-regulator of the sensor
IRS - Isolation interface
PP - Parallel processor
PM - Serial processor
ISO - Isolation interface
FCM - Power supply for the counter

Table 1 - Failure rates of the PCBs

The failure rate of each counting point may be obtained by the adequate summation of the failure rates of its components. In that way, a group of one TIV, one RIV, one PRS and the part of an IRS (the side of the sensor) have an estimated failure rate of 52.47556x10E-6 /h, or a MTTF of 19,056.49 hours, that means 2.2 years.

Considering that, when the counting point is in fail, the maintenance team can join the boundary blocks together leading to another bigger one, and that always exists a maintenance team available in the yard, any maintenance may be done in two hours, what furnishes a repair rate of 0.5. This maintenance is

maintenance is needed, because in this case all information stored in the system memories is loosed and it is necessary restart all blocks with its occupancy status; for this the repair rate is taken to be 0.25 or four hours of work, it is important note that this kind of failure is extremely improbable.

By Markov modeling (born and death [11] [12] [13] with a MTTF (Mean Time to Fail) and a MTTR (Mean Time to Repair) given by the inverses of the failure and repair rates, respectively), the availability (A) would be given by:

$$A = \frac{MTTF}{MTTF + MTTR}$$

This furnishes A = 0.9998, or two hours out of order for each 10.000 hours (1.6 years) of work.

With the numbers of table 1 is easy to find the rates for the axle counter system. One channel of the redundant module has a failure rate that is the summation of the failures rates of each one of its parts, i.e., eight PP boards, two PM boards, one ISO board, one FCM board and one channel of one IRS board. The failure rate of the axle counter system is 364,669x10E-6/h (2.669 hours).

Using the Markov modeling one can find an availability (A) of 0.999993 (five nines). This means seven hours of unavailability for a million hours of work (116 years). This is a good result for a initial system specification of four nines.

The initial MTBUF (Mean Time Between Unsafe Failure) specification (greater than 100,000 years) is difficult to be directly verified. A pessimist trial would be possible if considering unsafe all the time that the system is with two channels out of order like the state two in figure 4, what is not totally true, but it is hypothesis. With this hypothesis, with a modeling like a used in [14] one may say that the medium time interval that the system stay in any state m_{ii} is given by:

$$m_{ii} = \frac{\text{medium time in state } i}{P\ (\text{being in } i\text{, for finite time } t)}$$

Considering state 2 as an unsafe state, one may

$$m_{22} = \frac{1}{\mu_2 * P2}$$

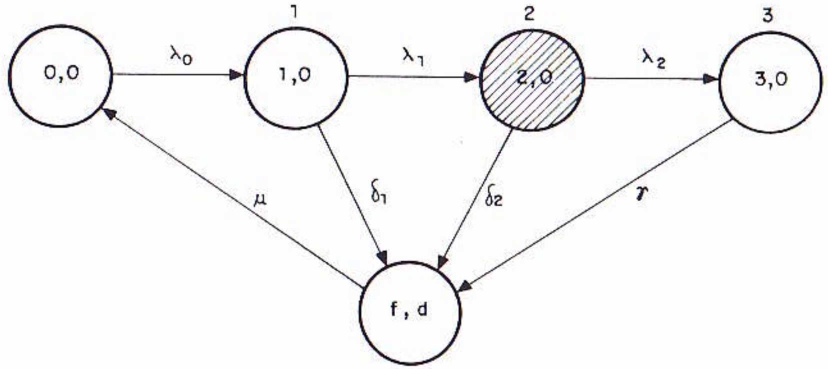
getting 594,880 hours (69 years) as result. This number do not fit the specified 100,000 years.

In order to get more detailed analysis, it is necessary consider the software reliability functions, which have been neglected until now. A very important function performed by software is the verification of the correct functioning of the involved hardware. This is a auto-diagnoses function that isolates the processor in case of doubt about its integrity. This function analyses all message exchange verifying the correct functioning of the processors. Any doubt about the integrity of any processing channel inhibit the answers. This failure detection system assures the veracity of information at the system's output.

With this reliability function implemented by software, the repair rate in the formula is substituted by the failure detection rate. The system would have unsafe outputs only while the software doesn't detect the failure; during the time between the detection and the repair the system is safe. The model that considers this situation can be seen in figure 3.

If a one second failure rate detection is considered, a very reasonable number is 4,34x10E+9 hours (the M22 may be calculated as in the previous case), or 495,000 years, exceeding the original specification.

Its important to note that, in all these calculations, the software is considered to be perfect, i.e., the software reliability itself was not taken into account. For that this restriction could be released it would be necessary an equivalent analysis in the software, the references [15] [16] [17] [18] [19] and [20] analyses this problem.



(f,d) NUMBER OF FAILURES, NUMBER OF DETECTED FAILURES

$f \neq 0$: ANY > 1

$d \neq 0$: ANY > 1

δ_1 = DETECTION RATE WITH ONE FAILED UNIT (MTTD = 1 sec)

δ_2 = DETECTION RATE WITH TWO FAILED UNIT (MTTD = 2 sec)

γ = DETECTION RATE WITH THREE FAILED UNIT (MTTD = 3 sec)

γ = DETECTION BY EXTERNAL ELEMENT (e.g. CMT)

μ = REPAIR RATE

λ = FAILURE RATE OF ONE UNIT

$\lambda_0 = 3\lambda$

$\lambda_1 = 2\lambda$

$\lambda_2 = \lambda$

$\mu = 0,5$

$\lambda = 374,7 \cdot 10^{-6}$ f/h

$\delta_1 = 3600$ d/h

$\delta_2 = 1800$ d/h

$\gamma = 1200$ d/h

$$P_2 = 1,28 \cdot 10^{-13}$$

$$m_{22} = \frac{1}{P_2\,(\lambda_2 + \delta_2)}$$

Figure 3- Markov's model with software detection

CONCLUSIONS ABOUT THE QUALITY LEVELS

The initial challenge, the implementation of a system with four nines of availability, had been reached with advantages. The five nines is the result of the triplication of the counter and the high reliability achieved in the field equipment [21].

This results suggests that the triplication was not needed in a departure yard, but the index are important to let the system be homologated for use in a commercial line application.

It is very dificult to compare the results obtained with the indexes of other systems, because there are no normalization or any consensus about them [15].

The international tendency of microprocessors utilization in the implementation of reliable functions takes time to get the railway systems, because the cost competitivety and the incredibility of designers in the new digital technology.

The DET have been submitted to field tests with good results. The tests had taken place at Itaquera Departure Yard, in a region of maximum dust and vibration (line of break tests).

REFERENCES

[1] IRLAND, E.A. Assuring quality and reliability of complex electronic systems: hardware and software. Proceedings of the IEEE, New York, v.76, n.1, p.5-18, Jan.1988.

[2] SOUZA,B.J.; KOBAYASHI, G. Um controlador digital tolerante a falhas para um sistema de detecção de trens. In: SIMPÓSIO DE SISTEMAS DE COMPUTADORES TOLERANTES A FALHAS, 2, Campinas, Anais. Campinas, Unicamp, 1987. p.85-96.

[3] SIQUEIRA NETO, P.R. Aspectos de tolerância a falhas no projeto do sistema de controle integrado no pátio de Itaquera. In: SIMPÓSIO DE SISTEMAS DE COMPUTADORES TOLERANTES A FALHAS, 2, Campinas, Anais. Campinas, Unicamp, 1987. p.97-106.

[4] PEDROSO, G. Intertravamento em estado sólido ... In: ENCONTRO NACIONAL DE SINALIZAÇÃO

FERROVIÁRIO DA ABNT. SCB6:17, 1, São Paulo, 1986. 21p.

[5] SIEMENS AKTIENGESELLSCHAFT. The axle counter, a means for trains detection. Braunschweig, Siemens AG., s.d.. 4p. (Siemens Railway Signalling F533/104.101).

[6] SCHMIDT, W.;HANKE, R. The Siemens electronic axle counter type AzS70. Braunschweig, Siemens Aktiengesellschaft, 1974. 10p. (Siemens Railway Signalling Technique D533/103.101)

[7] BAPAT, M.K.; KUMAR, R. Development and applications of axle counters on the indian railways In: International Conference on Railways Safety Control and Automation Towards the 21st Century, London, 1984. Proceedings. London, Institution of Railway Signal Engineers, 1984 p.238-44.

[8] BAZOVSKY, I. Reliability: theory and practice. Englewood Cliffs, Prentice Hall, 1961. (Space Technology Series).

[9] CHRISTIANSEN, D. et al. Reliability vignettes special issue. IEEE Spectrum, New York, v.18, n.10, Oct.1981.

[10] US DEPARTMENT OF DEFENSE. Military Standadization Handbook: Reliability Prediction of Electronic Equipement MIL-HDBK-217D, Washington (DC), 1983.

[11] LALA, P.K. Fault tolerant e fault testable hardware design. 2.ed. Englewood Cliffs, Prentice Hall International, 1985. 263p.

[12] KIRRMANN, H.D. Fault tolerance in process control: an overview and examples of european products. IEEE Micro, New York, Oct.1987, p.27-50.

[13] DRAKE, A. Fundamentals of applied probability theory. New York, McGraw-Hill, 1967. 283p.

[14] HOWARD, R.A. Dynamic probabilistic systems. New York, John Wiley, 1971.

[15] MATHEUS, W.;MOSCATO, L.A. Qual é o risco aceitável em sistemas de segurança? In:

TOLERANTES A FALHAS, 2, Campinas, 1987. Anais. Campinas, Unicamp, 1987. p.13-26.

[16] THEURETZBACHER, N. A system architecture that applies new principles to electronic interlocking. In: IFAC SYMPOSIUM, Viena, 1986, Proceedings. Viena, Institute für Praktishe Informatik Techical University, 1986, p.453-560.

[17] OSSEIRAN, A. et al. Design of a self checking microprocessor for real time applications. In: IFAC SYMPOSIUM, Viena, 1986, Proceedings. Viena, Institute für Praktishe Informatik Techical University, 1986, p.461-68.

[18] LIST, G. Investigations of data protection measures with coding redundancy for safety control. In: IFAC SYMPOSIUM, Viena, 1986, Proceedings. Viena, Institute für Praktishe Informatik Techical University, 1986, p.469-74.

[19] VALANCOGNE, J.; GALIVEL, C. Systeme d'aide ala conduite, a l'exploitation et a la maintenance. In: IFAC SYMPOSIUM, Viena, 1986, Proceedings. Viena, Institute für Praktishe Informatik Techical University, 1986, p.493-98.

[20] POSTON, R.M.; BRUEN, M.W. Counting down to zero software failures. IEEE Software, New York, Sept.1987. p.54-61.

[21] SPINA, E. Sistema de Detecção Eletrônica de Trens MSc. Dissertation, Department of Computer Engineering and Digital Systems, Polytechnic School, University of São Paulo, 1990.

Object Oriented Constraint Representation for Railway Traffic Optimisation

G. Sissa (*), M. Missikoff (**), F. Camurri (*)

(*) Ansaldo Trasporti, Via dei Pescatori 35, 16129 Genova, Italy

(**) IASI-CNR, Viale Manzoni 30, 00185 Roma, Italy

ABSTRACT

Railway Traffic Management is basically a constraint satisfaction problem.
Optimisation problems are traditionally approached by the operation research. Constraint programming is a more recent approach.
We propose an innovative approach, based on expert system technology, which is centered on the representation of the constraints that the Railway network has to satisfy and on the management of such constraints.
Object Oriented paradigm is very natural and intuitive in knowledge representation and Object Oriented programming is very efficient. In particular Object Orientation looks very suitable and promising for constraint representation.
This paper will explain why railway traffic management is concerned with constraint representation problem, how this approach has been applied to railway traffic optimisation, allowing the implementation of the PORT (Planning for Optimisation in Railway Traffic) Expert System.

RAILWAY TRAFFIC MANAGEMENT SYSTEM

Railway Traffic Management Problems and Automatic Supervision Systems

The continuing evolution in Information Technology is taking place in centralized control system for railways and rapid transit networks.
Modern railway traffic management systems are usually highly

Computers in Railways III

Vol 1: Management

Editors:
T.K.S. Murthy J. Allan R.J. Hill
G. Sciutto S. Sone

Computational Mechanics Publications
Southampton Boston

This volume contains the edited version of some of the papers presented at the Third International Conference on Computer Aided Design, Manufacture and Operation in the Railway and other Advanced Mass Transit Systems, held in Washington, DC, U.S.A., during 18 - 20 August 1992.

The objective of the conference was to update the use of computer-based techniques in the design, manufacture and operation of railway and other passenger and freight systems. The first volume, *Management*, deals with Planning and Development; Management and Information Systems; Manufacture, Testing, Maintenance and Diagnostics; Signalling Train Control and Safety and lastly, System Simulation Techniques and Simulation Techniques.

The companion volume *Vol 2: Technology* deals with Power Supply; Traction Drives and Performance; Train Operations; Vehicle Structure and Dynamics; Track and lastly, Electromagnetic Compatibility and Environment.

ISBN 1-85312-207-6
ISBN 1-56252-132-2
Set
ISBN 1-85312-176-2
ISBN 1-56252-105-5

Computers in Railways III

Vol 1: Management

Proceedings of the Third International Conference on Computer Aided Design, Manufacture and Operation in the Railway and other Advanced Mass Transit Systems (COMPRAIL 92), held in Washington DC, U.S.A., during 18-20 August 1992

Editors:
T.K.S. Murthy, Wessex Institute of Technology, U.K.
J. Allan, London Underground Ltd, U.K.
R.J. Hill, University of Bath, U.K.
G. Sciutto, Universita Degli Studi di Genova, Italy
S. Sone, The University of Tokyo, Japan

Computational Mechanics Publications
Southampton Boston

T.K.S. Murthy
Wessex Institute of Technology
University of Portsmouth
Ashurst Lodge
Southampton
SO4 2AA, U.K.

R.J. Hill
University of Bath
School of Electronic and
Electrical Engineering
Claverton Down
Bath BA2 7AY, U.K.

S. Sone
University of Tokyo
Department of Electrical Engineering,
Faculty of Engineering
7-3-1 Hongo
Bunkyo-ku
Tokyo 113, Japan

J. Allan
London Underground Ltd
Professional Services Group
Telstar House
Eastbourne Terrace
London W2 6LG, U.K.

G. Sciutto
University of Genova
Department di Ingegneria Elettrica
Via all'Opera, 11a
I-16145 Genova GE, Italy

British Library Cataloguing in Publication Data
A Catalogue record for this book is available
from the British Library

ISBN 1-85312-207-6 Computational Mechanics Publications, Southampton
ISBN 1-56252-132-2 Computational Mechanics Publications, Boston, USA

Set
ISBN 1-85312-176-2 Computational Mechanics Publications, Southampton
ISBN 1-56252-105-5 Computational Mechanics Publications, Boston, USA

Library of Congress Catalog Card Number 92-81589

Printed and bound by Bookcraft Ltd, Avon