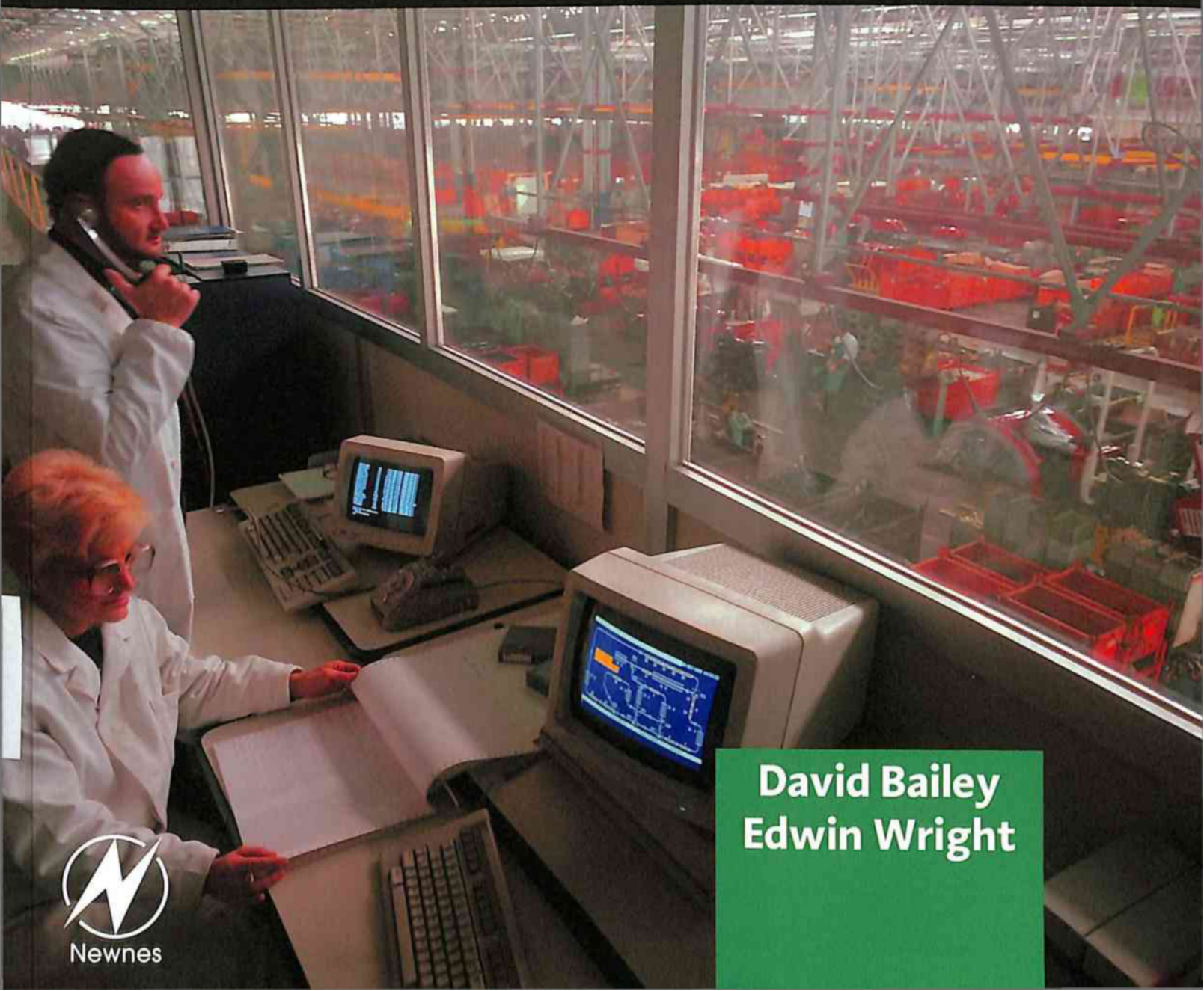
ELSEVIER

Practical SCADA for Industry



David Bailey
Edwin Wright

Newnes

Newnes is an imprint of Elsevier
Linacre House, Jordan Hill, Oxford OX2 8DP, UK
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA

First published 2003
Reprinted 2005, 2006

Copyright © 2003, IDC Technologies. All rights reserved

The right of IDC Technologies to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988

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 publisher

Permissions may be sought directly from Elsevier's Science & Technology Rights Department in Oxford, UK: phone (+44) (0) 1865 843830; fax (+44) (0) 1865 853333; email: permissions@elsevier.com. Alternatively you can submit your request online by visiting the Elsevier web site at http://elsevier.com/locate/permissions, and selecting *Obtaining permission to use Elsevier material*

Notice
No responsibility is assumed by the publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Because of rapid advances in the medical sciences, in particular, independent verification of diagnoses and drug dosages should be made

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

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN–13: 978-0-7506-5805-8
ISBN–10: 0-7506-5805-3

For information on all Newnes publications visit our website at www.newnespress.com

Transferred to Digital Printing in 2009

Working together to grow libraries in developing countries
www.elsevier.com | www.bookaid.org | www.sabre.org
ELSEVIER BOOK AID International Sabre Foundation

Practical SCADA for Industry

Titles in the series

Practical Cleanrooms: Technologies and Facilities (David Conway)

Practical Data Acquisition for Instrumentation and Control Systems (John Park, Steve Mackay)

Practical Data Communications for Instrumentation and Control (John Park, Steve Mackay, Edwin Wright)

Practical Digital Signal Processing for Engineers and Technicians (Edmund Lai)

Practical Electrical Network Automation and Communication Systems (Cobus Strauss)

Practical Embedded Controllers (John Park)

Practical Fiber Optics (David Bailey, Edwin Wright)

Practical Industrial Data Networks: Design, Installation and Troubleshooting (Steve Mackay, Edwin Wright, John Park, Deon Reynders)

Practical Industrial Safety, Risk Assessment and Shutdown Systems (Dave Macdonald)

Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems (Gordon Clarke, Deon Reynders)

Practical Radio Engineering and Telemetry for Industry (David Bailey)

Practical SCADA for Industry (David Bailey, Edwin Wright)

Practical TCP/IP and Ethernet Networking (Deon Reynders, Edwin Wright)

Practical Variable Speed Drives and Power Electronics (Malcolm Barnes)

Practical SCADA for Industry

David Bailey BEng, Bailey and Associates, Perth, Australia

Edwin Wright MIPENZ, BSc(Hons), BSc(Elec Eng), IDC Technologies, Perth, Australia

AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK • OXFORD
PARIS • SAN DIEGO • SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Newnes is an imprint of Elsevier

Contents

Preface xiii

1 Background to SCADA 1

1.1 Introduction and brief history of SCADA 1
1.2 Fundamental principles of modern SCADA systems 2
1.3 SCADA hardware 4
1.4 SCADA software 5
1.5 Landlines for SCADA 6
1.6 SCADA and local area networks 7
1.7 Modem use in SCADA systems 7
1.8 Computer sites and troubleshooting 8
1.9 System implementation 9

2 SCADA systems, hardware and firmware 11

2.1 Introduction 11
2.2 Comparison of the terms SCADA, DCS, PLC and smart instrument 12
2.2.1 SCADA system 12
2.2.2 Distributed control system (DCS) 15
2.2.3 Programmable logic controller (PLC) 15
2.2.4 Smart instrument 16
2.2.5 Considerations and benefits of SCADA system 17
2.3 Remote terminal units 17
2.3.1 Control processor (or CPU) 19
2.3.2 Analog input modules 19
2.3.3 Typical analog input modules 26
2.3.4 Analog outputs 27
2.3.5 Digital inputs 28
2.3.6 Counter or accumulator digital inputs 29
2.3.7 Digital output module 31
2.3.8 Mixed analog and digital modules 33
2.3.9 Communication interfaces 33
2.3.10 Power supply module for RTU 33
2.3.11 RTU environmental enclosures 33
2.3.12 Testing and maintenance 34
2.3.13 Typical requirements for an RTU system 35
2.4 Application programs 36
2.5 PLCs used as RTUs 36
2.5.1 PLC software 37
2.5.2 Basic rules of ladder-logic 38
2.5.3 The different ladder-logic instructions 40
2.6 The master station 46
2.6.1 Master station software 48

	2.6.2	System SCADA software	48
	2.6.3	Local area networks	48
	2.6.4	Ethernet	49
	2.6.5	Token ring LANs	51
	2.6.6	Token bus network	52
2.7		System reliability and availability	52
	2.7.1	Redundant master station configuration	52
2.8		Communication architectures and philosophies	54
	2.8.1	Communication architectures	54
	2.8.2	Communication philosophies	56
	2.8.3	Polled (or master slave)	56
	2.8.4	CSMA/CD system (peer-to-peer)	59
2.9		Typical considerations in configuration of a master station	61
3		SCADA systems software and protocols	64
3.1		Introduction	64
3.2		The components of a SCADA system	64
	3.2.1	SCADA key features	65
3.3		The SCADA software package	67
	3.3.1	Redundancy	70
	3.3.2	System response time	72
	3.3.3	Expandability of the system	72
3.4		Specialized SCADA protocols	72
	3.4.1	Introduction to protocols	73
	3.4.2	Information transfer	74
	3.4.3	High level data link control (HDLC) protocol	78
	3.4.4	The CSMA/CD protocol format	80
	3.4.5	Standards activities	81
3.5		Error detection	82
	3.5.1	Causes of errors	83
	3.5.2	Feedback error control	84
3.6		Distributed network protocol	87
	3.6.1	Introduction	87
	3.6.2	Interoperability	87
	3.6.3	Open standard	87
	3.6.4	IEC and IEEE	88
	3.6.5	SCADA	88
	3.6.6	Development	88
	3.6.7	Physical layer	88
	3.6.8	Physical topologies	88
	3.6.9	Modes	89
	3.6.10	Datalink layer	92
	3.6.11	Transport layer (pseudo-transport)	96
	3.6.12	Application layer	97

3.6.13	Conclusion	97
3.7	New technologies in SCADA systems	97
3.7.1	Rapid improvement in LAN technology for master stations	97
3.7.2	Man machine interface	97
3.7.3	Remote terminal units	98
3.7.4	Communications	98
3.8	The twelve golden rules	98
4	**Landlines**	**100**
4.1	Introduction	100
4.2	Background to cables	100
4.3	Definition of interference and noise on cables	101
4.4	Sources of interference and noise on cables	102
4.4.1	Electrostatic coupling	103
4.4.2	Magnetic coupling	104
4.4.3	Impedance coupling	105
4.5	Practical methods of reducing noise and interference on cables	107
4.5.1	Shielding and twisting wires	107
4.5.2	Cable spacing	108
4.5.3	Tray spacing	110
4.5.4	Earthing and grounding requirements	111
4.5.5	Specific areas to focus on	111
4.6	Types of cables	112
4.6.1	General cable characteristics	112
4.6.2	Two wire open lines	114
4.6.3	Twisted pair cables	114
4.6.4	Coaxial cables	116
4.6.5	Fiber optics	116
4.6.6	Theory of operation	116
4.6.7	Modes of propagation	118
4.6.8	Specification of cables	120
4.6.9	Joining cables	120
4.6.10	Limitations of cables	121
4.7	Privately owned cables	121
4.7.1	Telephone quality cables	121
4.7.2	Data quality twisted pair cables	122
4.7.3	Local area networks (LANs)	122
4.7.4	Multiplexers (bandwidth managers)	122
4.7.5	Assessment of existing copper cables	125
4.8	Public network provided services	125
4.9	Switched telephone lines	126
4.9.1	General	126
4.9.2	Technical details	126
4.9.3	DC pulses	128

4.9.4	Dual tone multifrequency – DTMF	128
4.10	Analog tie lines	128
4.10.1	Introduction	128
4.10.2	Four wire E&M tie lines	129
4.10.3	Two wire signaling tie line	130
4.10.4	Four wire direct tie lines	131
4.10.5	Two wire direct tie lines	131
4.11	Analog data services	131
4.11.1	Introduction	132
4.11.2	Point-to-point configuration	132
4.11.3	Point-to-multipoint	132
4.11.4	Digital multipoint	133
4.11.5	Switched network DATEL service	134
4.11.6	Dedicated line DATEL service	134
4.11.7	Additional information	135
4.12	Digital data services	135
4.12.1	General	135
4.12.2	Service details	135
4.13	Packet switched services	136
4.13.1	Introduction	136
4.13.2	X.25 service	138
4.13.3	X.28 services	138
4.13.4	X.32 services	139
4.13.5	Frame relay	139
4.14	ISDN	139
4.15	ATM	141
5	**Local area network systems**	**142**
5.1	Introduction	142
5.2	Network topologies	143
5.2.1	Bus topology	143
5.2.2	Bus topology advantages	144
5.2.3	Bus topology disadvantages	144
5.2.4	Star topology	144
5.2.5	Ring topology	145
5.3	Media access methods	146
5.3.1	Contention systems	146
5.3.2	Token passing	147
5.4	IEEE 802.3 Ethernet	147
5.4.1	Ethernet types	148
5.4.2	10Base5 systems	148
5.4.3	10Base2 systems	150
5.4.4	10BaseT	151
5.4.5	10BaseF	153

	5.4.6	10Broad36	153
	5.4.7	1Base5	153
	5.4.8	Collisions	153
5.5		MAC frame format	154
5.6		High-speed Ethernet systems	155
	5.6.1	Cabling limitations	155
5.7		100Base-T (100Base-TX, T4, FX, T2)	156
	5.7.1	Fast Ethernet overview	156
	5.7.2	100Base-TX and FX	157
	5.7.3	100BASE-T4	157
	5.7.4	100Base-T2	158
	5.7.5	100Base-T hubs	158
	5.7.6	100Base-T adapters	159
5.8		Fast Ethernet design considerations	159
	5.8.1	UTP Cabling distances 100Base-TX/T4	159
	5.8.2	Fiber optic cable distances 100Base-FX	159
	5.8.3	100Base-T repeater rules	160
5.9		Gigabit Ethernet 1000Base-T	160
	5.9.1	Gigabit Ethernet summary	160
	5.9.2	Gigabit Ethernet MAC layer	161
	5.9.3	1000Base-SX for horizontal fiber	162
	5.9.4	1000Base-LX for vertical backbone cabling	163
	5.9.5	1000Base-CX for copper cabling	163
	5.9.6	1000Base-T for category 5 UTP	163
	5.9.7	Gigabit Ethernet full-duplex repeaters	163
5.10		Network interconnection components	164
	5.10.1	Repeaters	164
	5.10.2	Bridges	165
	5.10.3	Router	165
	5.10.4	Gateways	166
	5.10.5	Hubs	166
	5.10.6	Switches	167
5.11		TCP/IP protocols	169
	5.11.1	The TCP/IP protocol structure	170
	5.11.2	Routing in an Internet	170
	5.11.3	Transmission control protocol (TCP)	171
5.12		SCADA and the Internet	172
	5.12.1	Use of the Internet for SCADA systems	173
	5.12.2	Thin client solutions	173
	5.12.3	Security concerns	174
	5.12.4	Other issues	175
	5.12.5	Conclusion	175