

9th IET International Conference on System Safety and Cyber Security 2014

IET Conference Publications 634

**Manchester, United Kingdom
15 - 16 October 2014**

ISBN: 978-1-5108-0019-9

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2014) by the Institution of Engineering and Technology
All rights reserved.

Printed by Curran Associates, Inc. (2015)

For permission requests, please contact the Institution of Engineering and Technology
at the address below.

Institution of Engineering and Technology
P. O. Box 96
Stevenage, Hertfordshire
U.K. SG1 2SD

Phone: 01-441-438-767-328-328
Fax: 01-441-438-767-328-375

www.theiet.org

Additional copies of this publication are available from:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2634
Email: curran@proceedings.com
Web: www.proceedings.com

TABLE OF CONTENTS

AN APPROACH TO THE CERTIFICATION OF AUTONOMOUS SYSTEMS	1
<i>N. Tudor, K. Wharen</i>	
PROVING PROPERTIES OF AUTOMOTIVE SYSTEMS OF SYSTEMS UNDER ISO 26262 USING AUTOMATED FORMAL METHODS	7
<i>N. Tudor, J. Botham</i>	
INTEGRATED ARCHITECTURE FRAMEWORK AND SECURITY RISK MANAGEMENT FOR COMPLEX SYSTEMS	13
<i>C. Andrews, C. Monk, R. Johnston</i>	
ATTACK VISUALISATION FOR CYBER-SECURITY SITUATION AWARENESS	20
<i>M. Evangelopoulou, C. Johnson</i>	
PROBATIVE BLINDNESS: HOW SAFETY ACTIVITY CAN FAIL TO UPDATE BELIEFS ABOUT SAFETY	26
<i>A. Rae, J. McDermid, R. Alexander, M. Nicholson</i>	
HOW DID SYSTEMS GET SO SAFE WITHOUT ADEQUATE ANALYSIS METHODS?	32
<i>J. McDermid, A. Rae</i>	
SAFETY ASSESSMENT OF SMART INSTRUMENTS FOR THE NUCLEAR INDUSTRY	38
<i>G. Corrao, S. Hatton, J. Lewthwaite</i>	
TRUSTWORTHY SOFTWARE: LESSONS FROM 'GOTO FAIL' & HEARTBLEED BUGS	43
<i>H. Boyes, P. Norris, I. Bryant, T. Watson</i>	
SOME POTENTIAL ISSUES WITH THE SECURITY OF HTML5 INDEXEDDB	50
<i>S. Kimak, J. Ellman, C. Laing</i>	
LEARNING FROM EXPERIENCE – HOW CAN WE PRODUCE A NUCLEAR SAFETY CASE TO OUTLAST THE STATION?	56
<i>J. Brain</i>	
SAFETY CASE DEVELOPMENT: A PROCESS TO IMPLEMENT THE SAFETY THREE-LAYERED FRAMEWORK	62
<i>M. Standish, H. Auld, P. Caseley, M. Hadley</i>	
THE SAFETY THREE-LAYER FRAMEWORK: A CASE STUDY	73
<i>M. Standish, H. Auld, P. Caseley, M. Hadley</i>	
TOOLS AND TECHNIQUES FOR REPORTING AND ANALYSING THE CAUSES OF CYBER-SECURITY INCIDENTS IN SAFETY-CRITICAL SYSTEMS	81
<i>C. Johnson</i>	
MULTICORE MILS: EVOLUTION OF THE MULTIPLE INDEPENDENT LEVELS OF SECURITY SOFTWARE ARCHITECTURE TO ENABLE MULTI-LEVEL SECURE MULTICORE SYSTEMS	88
<i>P. Parkinson</i>	
SYNTHESIZING OPTIMAL SECURITY CONFIGURATIONS FOR ENTERPRISE NETWORKS : A FORMAL APPROACH	96
<i>S. Majht, P. Bera, S. Kumar, E. Al-Shaer, M. Satpathy</i>	
A PRAGMATIC APPROACH TO CAPTURING SAFETY AND SECURITY RELEVANT INFORMATION FOR REUSABLE EUROPEAN COMPONENT ORIENTED ARCHITECTURE SOFTWARE COMPONENTS	102
<i>J. Fenn, T. Cornilleau, Y. Oakshott, A. Britto</i>	
SPARK 2014: A LANGUAGE FOR SAFETY AND SECURITY	108
<i>F. Schanda, S. Matthews</i>	
SOFTWARE DESIGN DECISION VULNERABILITY ANALYSIS	113
<i>P. Avery, R. Hawkins</i>	
SAFETY AND SECURITY OF THE SMART CITY – WHEN OUR INFRASTRUCTURE GOES ONLINE	119
<i>M. St.John-Green, T. Watson</i>	
GOVERNANCE, RISK AND COMPLIANCE: IMPEDIMENTS AND OPPORTUNITIES FOR MANAGING OPERATIONAL TECHNOLOGY RISK IN INDUSTRIAL CYBER SECURITY AND SAFETY	125
<i>R. Piggin</i>	
SECURING A RAILWAY CONTROL SYSTEM	133
<i>D. Milligan</i>	

DEFENCE STANDARD 00-56 ISSUE 5: CONCEPTS, PRINCIPLES AND PRAGMATICS	139
<i>J. McDermid, P. Williams</i>	
THE APPLICATION OF "HUMAN SYSTEMS INTEGRATION" TO SAFETY-CRITICAL- SYSTEMS DESIGN	145
<i>C. Senling, S. Norton</i>	
CYBER SECURITY OF THE RAILWAY SIGNALLING & CONTROL SYSTEM.....	149
<i>M. Bastow</i>	
SAFE AND SECURE: RE-ENGINEERING A SOFTWARE PROCESS SET FOR THE CHALLENGES OF THE 21ST CENTURY	154
<i>K. Wallace</i>	
Author Index	