Institution of Engineering and Technology

3rd IET International Conference on System Safety 2008

IET Conference Publications 542

October 20-22, 2008
Birmingham, UK

Printed from e-media with permission by:

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

ISBN: 978-1-60560-706-1

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

Copyright© (2008) by the Institution of Engineering and Technology
All rights reserved.

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

TABLE OF CONTENTS

Development of an Intelligent System for Railway Risk Analysis 1
Min An, Yao Chen, Chris Baker

Developing and Maintaining Competence - Experiences from the Rail Industry 7
J.P. Baker, P. Durrant

Improving Safety by Enhancing Technical Competence Management 13
P. Bomme, G. Boppe, E. Steinmann, J.-P. Martin-Flatin

Using Data from Simulation Training in Modelling Emergency Response Outcome 19
M.N. Lyons

The Incompetence of Competency Assurance 25
C.E. Shea, R. Popplestone

An Environment for Testing Safety-critical Protocols 31
C. Bergenhem, J. Karlsson

Circuit Fault & Failure Description Language 37
J. Rocheteau, J.-L. Boulanger

The Pace Towards Protocol-independent Safety Requirements for Serial Buses in the Automotive Environment 42
L.D. Kabulepa, A.K.H. Amjadi

Model Based Requirements Elicitation 48
P.G. Tate

Safety-critical Shortage 53
F. Gasperoni

Implementing and Sustaining Human Reliability Programmes of Work - a Manager's Guide 57
A. Hubbard, J. Henderson, D. Embrey

The Operator Or the Automation: in Whom Should We Place Ultimate Trust? 63
A.J. Rae

The Role of Human Factors in Planning for Nuclear Power Plant Decommissioning 69
C. Blackett

Characteristics of Human Behaviour in Safety Critical Systems by the Example of European Railway Control Centres 75
T. Zahler

Development of an Electronic Safety Case for a Military Communication, Command and Control System 81
R. Maguire, A. Garside

Safety Case Notations: Alternatives for the Non-graphically Inclined? 87
C.M. Holloway

Safety Cases for Legacy Warships: a Systematic Approach 93
A.D. Bain, S. Dobson

Automotive Safety Cases - an Empirical Case Study of Requirements 99
F. Torner, P. Ohman

Explosion Protection:Risk Assessment & Hazard Management in Manufacturing 106
D.J. Powell

Case Study in Risk Evaluation for a Small-scale Sea-based Trial to Satisfy a New Operational Requirement 112
E. Uren, R. Maguire

Considerations of ALARP for Complex Safety Related Systems 117
G.E. Jolliffe

Using Mathematical Models to Guide the Simulation of Improvised Explosive Devices in Public Spaces 121
L. Nilsen-Nygaard, C.W. Johnson

EMC and Functional Safety Requirements for Integrated Electronics Systems 127
A. Ogunsola, B.W. Jaekel

IEC 61508 Certification of a Code Generator 134
T. Glotzner

Progress Report on Some Proposed Upgrades to the Conceptual Underpinnings of DO-178B/ED-12B 138
M.S. Jaffe, R. Busser, D. Daniels, H. Delseny, G. Romanski

'Act in Haste, Repent at Leisure': an Overview of Operational Incidents Involving UAVs in Afghanistan (2003-2005) 144
C.W. Johnson

ESARR6-compliant Software Engineering Framework 150
V. Behe, P. Bomme, C. Gingins

The Air Traffic Management Risk Classification Scheme - Why So Difficult? 156
M. Oliver

Evidence-based Development – Applying Safety Engineering Techniques to the Progressive Assurance and Certification of Complex Systems 161
A.J.J. Dick, S.C.B. Wills

How Can Active HUMS Safeguard Towards the Increasing Complexity of Avionics? 167
J. Melentis, I. Ibarra, E. Stipidis, P. Charchalakis, F.H. Ali

Military Risk Assessment in Counter Insurgency Operations: Case Study in the Retrieval of a UAV, Nr Sangin, Afghanistan, 11 June 2006 172
C.W. Johnson

Through-life Capability Risk Management for Evolutionary Complex Military Vetronics 178
I. Ibarra, J. Melentis, D. Summers, E. Stipidis, P. Charchalakis, F.H. Ali

Towards a Calculus for Software SIL 184
R.C. Short

Questioning Human Error Probabilities in Railways 189
F. Feldmann, M. Hammerl, S. Schwartz

Defence Standard 00-56 Issue 4 and Civil Standards - Appropriateness and Sufficiency of Evidence 195
J.R. Evans, T.P. Kelly

Structuring Safety Cases for Autonomous Systems 201
R.D. Alexander, N.J. Herbert, T.P. Kelly

Novel Validation Algorithms for Safety Critical Embedded Software 207
M. Nanda, J. Jayanthi, S. Rao

How Past Loss of Control Accidents May Inform Safety Cases for Advanced Control Systems on Commercial Aircraft 213
C.M. Holloway, C.W. Johnson

Automotive Telematics System for Safe Driving 219
T. Kumagai, K. Shidoji, Y. Matsuki

Ensuring the Safety of Satellite Navigation Systems for Aviation 225
M.C. Neville, M.I. Konaktchiev

Computational Support for Identifying Safety and Security Related Dependencies Between National Critical Infrastructures 231
C.W. Johnson, R. Williams

Tools for Local Critical Infrastructure Protection: Computational Support for Identifying Safety and Security Interdependencies Between Local Critical Infrastructures 237
C.W. Johnson, K. McLean

Defining Safety Requirements for Hybrid Electric Vehicles Using System Simulation 243
D. Gollub, M. Kretschmer, A. Heyl

A Brief Paper on Improving Active Safety Systems Via HMI and Dependability Analysis 248
J. Nilsson, P. Falcone, J. Vinter, J. Sjoberg, L. Nilsson, J. Jacobson

Risk Management's Role Within Management of Change Project Lifecycle 253
T. Haskins

Culture Management in the UK Rail Industry 259
R.E. Luther, C.E. Johnson

Hazard Modelling for Electronic Systems in Railway Operation and Control 265
B. Evers

The Impact of the ON-S1 Standard on Railway Risk Levels in Australia 270
A.L. Aas, M. Baysari, C. Caponecchia, T. Skramstad

Combining Safety and HCI Arguments to Increase Confidence in Information-only Systems 276
P.R. Symons

Estimating the Accuracy of Opposing Left-turn Potential Conflict Model Via Programming in Matlab 282
J. Shahi, B.N. Araghi, A. Mehdizadeh

Design of Systematic Safety Program Based on Work-group 287
Fan Yunxiao, Luo Yun, Liu Chao

Investigating the Use of Argument Modularity to Optimise Through-life System Safety Assurance 292
G. Despotou, T. Kelly

A Design Process for Constructing a User Interface Pattern Library for Touch-based Applications in Safety-critical Environments 298
T. Zahler

Author Index