4th IET International Conference on Systems Safety 2009

Incorporating the SaRS Annual Conference
IET Conference Publications 555

London, United Kingdom
26-28 October 2009

ISBN: 978-1-61738-382-3

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© (2009) by the Institution of Engineering and Technology
All rights reserved.

Printed by Curran Associates, Inc. (2010)

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

Uncertainty, Change Management the Application to Risk & Safety for Infrastructure Projects How it Happens in Australia 1
T. C. Haskins

A Safety Enhancement Model of Software System for Railways 7
S. Chandrasekaran, T. J. Madhumathy, M. Aparna, R. S. Jain

Open-DO: An Open-source Initiative for the Development of Safety-Critical Software 13
C. Comar, F. Gasperoni, J. F. Ruiz

A Unified Approach for System Safety and Software Safety 18
D. Mizuguchi, M. Hirayama, S. Yoshizawa

Relevance of Measurement Theory to Safety and Safety Integrity 23
I. H. A. Johnston

Making Robust ALARP Decisions for In-service Systems 29
A. J. Rae, M. Nicholson

A Deviation Based Systems of Systems Safety View for Modelling Architectural Frameworks 35
G. Despotou, T. Kelly

Deriving Safety Cases from Automatically Constructed Proofs 41
N. Basir, E. Denney, B. Fischer

The Role of the Human in an Autonomous System 47
R. D. Alexander, N. J. Herbert, T. Kelly

Safety Analysis of Sub-systems 53
B. Bradshaw, D. Madeley, I. Herath

Stability of Public Transportation Systems in Case of Random Failures and Intended Attacks - A Case Study from Switzerland 59
R. Dorbritz, U. Weidmann

Process and Structural Safety: Do We Need to Have Hazards? 65
A. B. Buchan, C. J. Bolton

IEC 61508 and IEC 61511 Assessments - Some Lessons Learned 68
M. H. Lloyd, P. J. Reeve

Goal-based Safety Standards and COTS Software Selection 74
C. Menon, J. McDermid, P. Hubbard

Software Safety Assurance - What is Sufficient? 80
R. D. Hawkins, T. Kelly

Is a Common UK Competency Scheme a Bear-Trap? 86
A. D. Bain

Skills and Competence Underpin Safety in the UK Electrical Power Industry 93
J. C. Steed

Creating a Competence Argument to Support a Safety Case 99
P. R. Mayo

Towards a Comprehensive Consideration of Epistemic Questions in Software System Safety 105
C. M. Holloway, C. W. Johnson

The MOD Procurement Guidance on Software Safety Assurance Assessing and Understanding Software Evidence 110
P. R. Caseley, T. A. D. White

Politics and Patient Safety Don't Mix: Understanding the Failure of Large-scale Software Procurement in Healthcare 122
C. W. Johnson

Safety Arguments in Aircraft Certification 128
Linling Sun, T. Kelly

The Integration of Alarm Device Into Socio-technical Systems: The Case of an Onboard Alert Device (ACAS) 134
P. Amaldi, A. Chellappah

Towards Establishing a Self-management Architecture for Dynamic Risk Management in 'Intelligent' Aero-Engine Control 141
Z. Kurd, T. Kelly, J. McDermid, R. Calinescu, M. Kwiatkowska

A Pragmatic Integration of Risk Management Processes 148
M. Brownsword

Hydrogen Fuel Cell Taxi: Safety Analysis Experiences 153
I. Herath, D. Madeley, B. Bradshaw

Investigating the Potential Use of System Dynamics As a Tool for Event Analysis in the Nuclear Industry 159
N. J. Carhart

What Does Safety Mean for Networks? 165
J. Muller, G. Perruchoud, H. Borel, P. Bomme

Predicting the Future: The Integrated Risk Picture 171
E. Perrin, B. Kirwan

Integrated Safety & Quality Framework for ATM/CNS Technical Services 178
P. Bomme

Dynamic Temporal Risk Allocation in Complex Hazard Management 184
R. L. Maguire

Proposed Methodology for Performing Risk Identification Workshops Based on Safety Climate 188
K. Choi, K. Yeung, A. Saleem

Safety Critical Task Risk Assessment in Offshore Installation Decommissioning: A Methodology 194
A. P. Bradbeer, E. Butterworth, G. M. Rolt

Electrical Safety - A Perspective Based on Incidents 200
W. F. Bates

Safety Tactics for Reconfigurable Process Control Devices 205
A. E. Hill, M. Nicholson

Replacing SIS on Live Processes Plant 211
C. Timms

Success is Not Merely Absence of Failure - A Systems-Engineering Approach to Safety Assessment 218
D. Fowler, E. Perrin, R. Pierce

Safety Assessment of the SESAR Operational Concept - European Air Traffic Management in 2020 and Beyond 224
D. Fowler, E. Perrin, R. Pierce

Deriving a Generic System Definition for Railway Risk Assessments Applied to BP-Risk 232
S.-L. Bepperling

Severity of Harm in Semi-quantitative Risk Assessment Method 237
B. Milius

Some Observations on Novel Concepts in New IEC 61508 Draft 243
J. Braband, S. Griebel

Arguing the Safety of FPGAs Within Safety Critical Systems 249
J. R. Clegg

The Human Contribution to System Safety 255
J. Reason

Securing the Interface: Safety-Critical Interaction Between Humans and Mobile Robots 285
P. B. Ladkin

Safety Cases & Safety Assessments 296
D. Kritzinger

Safety Culture Enhancement in European Air Traffic Management - Rising to the Challenge 357
B. Kirwan, K. Mearns, R. J. Kennedy, R. Gordon

Author Index