Institution of Engineering and Technology

2nd IET International Conference on System Safety 2007

IET Conference Publications 532

October, 22-24, 2007
London, UK

Printed from e-media with permission by:

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

ISBN: 978-1-60560-760-3

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

Copyright© (2007) 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

The Systemic Effects of Fatigue on Military Operations 1
C.W. Johnson

Human Factors Engineering of Interfaces-connecting Control Centres 7
L.M. Collis

Assurance Levels for ATM Elements: Human (HAL), Operational Procedure (PAL), Software 13
P. Mana, J.-M. De Rede, and D. Fowler

Negligible Risk for European Railway Risk Assessments 20
S.-L. Kurz and B. Milius

Acceptable Residual Risk - Principles, Philosophies and Practicalities 26
A.J. Rae

Putting Risk Into Context 32
M. Brownsword and R. Setchi

Model-based Framework for Addressing Diversity, Usability and Reliability for Safety Critical Interactive Systems 38
D. Navarre, P. Palanque, and J.-F. Ladry

Planning for Cost Effective Human Factors Engineering and System Safety 44
C.J. Ives

Validation and Verification Techniques for EMC for Functional Safety 49
E.K. Armstrong

Study on Risk Assessment and Control of Ship Safety Navigation 55
Fang Quangen, Hu Shenping, and Xi Yongtao

The Dangers of Failure Masking in Fault-tolerant Software: Aspects of a Recent In-flight Upset Event 60
C.W. Johnson and C.M. Holloway

EP2002 - Distributed Brake Control System 66
S. Albert

Software Safety Assurance Process for Railway Platform Software 72
S. Patra

The Normal Operations Safety Survey (NOSS): Measuring System Performance in Air Traffic Control 78
C. Henry

Harmonised Risk Acceptance Criterion for Technical Systems in European Railways 84
J. Braband

A Comparison of the Role of Degraded Modes of Operation in the Causes of Accidents in Rail and Air Traffic Management 89
C.W. Johnson and C. Shea

Certification of Object Oriented Programs 95
R.K. Dewar and C. Coma

Safety Process Improvement: Early Analysis and Justification 100
D. Mannering, J.G. Hall, and L. Rapanotti

Hazard Analysis for Programmable Automotive Systems 106
P.H. Jesty, D.D. Ward, and R.S. Rivett

Review of the Use of the Department for Transport Value for Preventing a Fatality in Non Road-transport Systems 112
R. Maguire

Practical Experiences in Upgrading and Standardising the Safety & Environmental Systems (SEMS) for the RN Marine Power & Propulsion Systems Division 118
J.P. Olivier and C. Blake

Integrated Safety Strategy to Model Driven Development with SysML.................................... 124
M.C. Hause and F. Thom

A Case Study of the Application of BS:EN 61508 in Electrical Power Generation 130
P.M. Wyman

The Who, Where, How, Why and When of Modular and Incremental Certification.................. 135
J.L. Fenn, R.D. Hawkins, P.J. Williams, T.P. Kelly, M.G. Banner, and Y. Oakshott

Pedestrian Behaviour and Safety in the Presence of Guard Railing.. 141
Pengjun Zheng, R. Hall, and M. McDonald

Energise Or De-energise to Trip?.. 147
A.G. Foord and C.R. Howard

Formalised Implementation of Safety Related HW/SW Architectures in Compliance with Functional Safety Requirements 153
J. Berthing and T. Maier

Combining Security and Safety Principles in Practice 159
T.J. Cockram and S.R. Lautieri

Penetrating the Fog of Safety Assessment - and Vice Versa.. 165
D. Fowler and S.P. Grand

Tailoring a Generic BBN Model for the Quantitative Safety Analysis of Complex Systems 175
R. Greenberg and S.C. Cook

Railway Safety Risk Assessment Using FRA and FAHP Approaches - a Case Study on Risk Analysis of Shunting at Waterloo Depot 181
Sheng Huang, Min An, Yao Chen, and C. Baker

Explosives Safety - an Oxymoron?.. 187
C. Marriott

Practicality of Implementing Risk Based Protection System Design to Vendor Packages in the Petrochemical Industry.. 194
J. Virdee

RAMS Program for Electromechanical Systems of Railway Applications 200
Z. Vintr and M. Vintr

Worst-case Software Safety Level for Braking Distance Algorithm of a Train......................... 206
S. Patra

Radiological Pollution Monitoring Using Composite Sampling.. 211
N.S. Lane

The Use of Goal Structuring Notation As a Method for Ensuring That Human Factors is Represented in a Safety Case.. 217
K.J.N. Rich, H. Blanchard, and J. McCloskey

A Review of Automotive Human Machine Interface Technologies and Techniques to Reduce Driver Distraction 223
C.A. Pickering, K.J. Burnham, and M.J. Richardson

Good Automated Safety Practice 229
J. Beresford

A Look at Aircraft Accident Analysis in the Early Days: Do Early 20th Century Accident Investigation Techniques Have Any Lessons for Today? 235
C.M. Holloway and C.W. Johnsont

System Safety Process and Design Process in Road Tunnel Control Systems 241
A. Mahdmina, M. Kolat, M. Frazer, and R. Williams

Safety Case Depictions vs. Safety Cases - Would the Real Safety Case Please Stand Up? 245
I. Habli and T. Kelly

Risk of Trust in Safety: Confidence Games 249
M. Felici

Dynamic Lifecycle System Integrity Management (DLSIM) by Use of Layers of Degradation Analysis (LODA) 253
I.K. Ramsay-Connell