

7th IET International Conference on System Safety and the Cyber Security Conference 2012

IET Conference Publications 607

**Edinburgh, United Kingdom
15-18 October 2012**

ISBN: 978-1-62748-123-6

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© (2012) by the Institution of Engineering and Technology
All rights reserved.

Printed by Curran Associates, Inc. (2013)

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

Ensuring Supplier Safety Analysis is Not Performed in Isolation! The Gulf Between the Project Safety Engineer and the Front Line User	1
<i>N. B. Durston</i>	
Unplugged Perils, Lost Hazards and Failed Mitigations	6
<i>N. Barton, A. J. Rae</i>	
ISO 26262 Concept Phase Safety Argument for a Complex Item	12
<i>I. Ibarra, S. Hartley, S. Crozier, D. Ward</i>	
Evidence-based Development - Coupling Structured Argumentation with Requirements Development	17
<i>A. J. J. Dick</i>	
Towards Understanding the DO-178C / ED-12C Assurance Case	22
<i>C. M. Holloway</i>	
A Practical Proposal for Ensuring the Provenance of Hardware Devices and Their Safe Operation	28
<i>Y. Kovalchuk, W. G. J. Howells, H. Hu, D. Gu, K. D. McDonald-Maier</i>	
What Does the Assurance Case Approach Deliver for Critical Information Infrastructure Protection in Cybersecurity?	34
<i>A. C. Goodger, N. H. M. Caldwell, J. T. Knowles</i>	
Preparing for Cyber-attacks on Air Traffic Management Infrastructures: Cyber-safety Scenario Generation	40
<i>C. W. Johnson</i>	
Cost Effective Assessment of the Infrastructure Security Posture	46
<i>G. P. Williams</i>	
Analysis and Optimization of Mixed-Criticality Applications on Partitioned Distributed Architectures	52
<i>D. Tamas-Selicean, S. O. Marinescu, P. Pop</i>	
Capitalize on Complexity	58
<i>N. McGuire, M. Kreidl, Sheng Cheng</i>	
Applying Failure Mode Modular De-composition (FMMD) Across the Software/Hardware Interface	67
<i>R. Clark, A. Fish, C. Garrett, J. Howse</i>	
Generic Security Cases for Information System Security in Healthcare Systems	73
<i>Y. He, C. W. Johnson</i>	
On the Relationship of Hazards and Threats in Railway Signaling	79
<i>J. Braband, M. Seemann</i>	
Assessing and Improving Software Quality in Safety Critical Systems by the Application of a Software Test Maturity Model	85
<i>F. I. Duncan, A. G. Smeaton</i>	
Failure Mode and Effects Analysis (FMEA) and Model-checking of Software for Embedded Systems by Sequential Scheduling of Vectors of Logic-labelled Finite-state Machines	89
<i>V. Estivill-Castro, R. Hexel, D. A. Rosenblueth</i>	
Combined Safety and Security Certification	95
<i>G. Romanski</i>	
‘You Don’t Know Jack’: Using 3D Anthropometric Modelling Techniques to Identify, Assess and Aid in the Early Resolution of Safety Issues Relating to Military Vehicle Design	100
<i>G. R. Hudson, D. Barker, J. H. Barton, D. G. B. Varney</i>	
Security in Integrated Vetrionics: Applying Elliptic Curve Digital Signature Algorithm to a Safety-Critical Network Protocol-TTP/C	105
<i>A. Deshpande, O. Obi, E. Stipidis, P. Charchalakis</i>	
The Application of Data Diodes for Securely Connecting Nuclear Power Plant Safety Systems to the Corporate IT Network	110
<i>R. T. Barker, C. J. Cheese</i>	
A Holistic Approach to Trustworthy Software	116
<i>I. Bryant</i>	
Comparing the Identification of Recommendations by Different Accident Investigators Using a Common Methodology	122
<i>C. W. Johnson, H. A. Oltedal, C. M. Holloway</i>	
Analysis and Modelling of Space Shuttle Challenger Accident Using Management Oversight and Risk Tree (MORT)	129
<i>S. K. Appicharla</i>	

Towards Parsimonious Resource Allocation in Context-aware N-version Programming	137
<i>J. Buys, V. De Florio, C. Blondia</i>	
Securing the Human to Protect the System: Human Factors in Cyber Security	143
<i>M. G. Lee</i>	
Safety Enhancement Through Situation-aware User Interfaces	148
<i>V. De Florio, C. Blondia</i>	
System Security Assessment Using a Cyber Range	154
<i>H. Winter</i>	
Emerging Good Practice for Cyber Security of Industrial Control Systems and SCADA	159
<i>R. S. H. Piggin</i>	
The Uses and Abuses of ASIL Decomposition in ISO 26262	165
<i>D. D. Ward, S. E. Crozier</i>	
Agonising Over ASILs: Controllability and the In-wheel Motor	171
<i>M. Ellims, H. E. Monkhouse</i>	
The Four Principles of Product Safety	179
<i>N. Sibley, B. Walby, D. Priestley</i>	
Trust and Control: A Safety Model for People and Organisations	183
<i>W. A. Hoskins</i>	
The Save Me Project Real-time Disaster Mitigation and Evacuation Management System	188
<i>I. Tsekourakis, C. Orlis, D. Ioannidis, D. Tzovaras</i>	
(SMA)² - A Social Media Audience Sharing Model for Authorities to Support Effective Crisis Communication	194
<i>S. Raue, C. W. Johnson, T. Storer</i>	
A Framework for Determining the Sufficiency of Software Safety Assurance	200
<i>R. D. Hawkins, T. P. Kelly</i>	
Emerging Technologies with the Potential to Impact Safety in Defence	206
<i>P. R. Caseley, G. T. Strong, D. J. H. Smith, K. J. Bown, B. K. Madahar</i>	
Author Index	