



From the Chair

The ICT industry in Queensland lately has not fared well. The on-going problems with Queensland Health's payroll system and the collapse of Telstra's 850MHz mobile phone network in most of the major centres state-wide for some 14 hours on May 06, 2010.

The problems at Queensland Health appear to be due to a combination of system complexity, systemic project management issues, insufficient testing and no roll-back contingency plan despite some of the biggest and experienced ICT organisations being involved. The Queensland Government has commissioned KPMG to review the Queensland Health payroll system. A Government [media release](#) on May 10, 2010 indicates that a more forensic examination was yet to commence. No doubt the report, when it is released, will become a case study on how not to do it.

The Telstra problems were caused by a botched planned update to the core network which resulted in a state-wide outage in the Next G mobile network. This however was not disclosed to the media and in fact the Telstra outages webpage indicated that there were no major outages!



The June 2009 newsletter contained an article on the tail strike by a United Arab Emirates Airbus A340-500 on March 20, 2009. Last December, the ATSB issued an [Interim Factual](#) report. There is an article on this incident later in the newsletter.

In my June 2009 newsletter editorial I made mention of a commuter train smash in Washington DC. On May 04, 2010 there was a collision involving a commuter train at Craigieburn, a northern Melbourne suburb. The collision occurred around 8.33pm. Fortunately there were no fatalities. Had this occurred during the afternoon commuter peak then the result may have been much different. Whilst the investigations are in progress, the circumstances of the accident seem to be not unlike the 1999 Glenbrook, NSW in which seven people died. There is an article on the Craigieburn collision in the newsletter.


The aSCSa for the sixth consecutive year hosted in association with the Australian National University the five day York University course - *Introduction to System Safety Engineering and Management*. I thank the ANU again for co-hosting this event. If you were unable to attend the course, I recommend The University of Queensland course being planned for July 2010 (see advert in this newsletter).

I'm looking forward to seeing you all at the ISSEC Brisbane Conference.

George Nikandros
Chairman



Co-locating with Project Management Australia Conference. Click here for weblink.



23 - 26 August 2010

Brisbane Convention & Exhibition Centre

ISSEC - Rising to the Challenge

In 2009, the inaugural Improving Systems and Software Engineering Conference (ISSEC) successfully achieved the vision to narrow the gap between current systems and software engineering practice; to integrate cross-functional perspectives and improve process capability and maturity; by bringing together in the one forum system engineers, software engineers, safety engineers, system integrators and process improvement professionals. In 2010, ISSEC is "Rising to the Challenge" to continue narrowing the gap, providing an environment for these engineering disciplines to come together and share ideas.

Keynote Speakers

Dr Ed Hoffman, Director of the NASA Academy of Program/Project and Engineering Leadership (APPEL).

Dr Mark C. Paulk, Senior Systems Scientist at the Institute for Software Research in the School of Computer Science at Carnegie Mellon University.

Conference Streams:

- Systems Engineering
- Software Engineering
- Process Improvement
- Systems Integration
- Software Assurance
- Safety Management and Engineering

More Information?

Visit [ISSEC Website](#) for more information and to register for the event.

See Page 2 for more information

Association Matters

Annual General Meeting

The 2010 Annual General Meeting in Brisbane during ISSEC 2010; the time, date and venue will be advised.

Nominations to join the committee can be made up to the time of the AGM. Please contact the Chairman. There is no requirement for aSCSa committee members to be ACS members.

National Committee

George Nikandros	Chairman (until 30 June 2010)
Kevin Anderson	Secretary
Chris Edwards	Treasurer
Tony Cant	Workshop Program Chair
Clive Boughton	Chairman (from 01 July 2010)
Rob Weaver	
Derek Reinhardt	
Allan Coxson	
Tariq Mahmood	
BJ Martin	

Web Site www.safety-club.org.au

The term of the current committee expires 30 June 2009. As per the constitution the 2009/10 chairman is elected by the outgoing committee and all other committee positions are declared vacant. In accordance with the Constitution, the 2010/11 chairman was elected by the committee at the June 2010 Committee meeting. Clive Boughton will be the chairman for 2010/11. Except for Allan Coxson, all other committee members have agreed to re-nominate.

Allan Coxson joined the committee in 2002. The committee thanks Allan for his contribution over the eight years.

Membership

In May 2009, a new membership application and renewal system was introduced which required change to the membership year from the financial year to the calendar year.

There were deemed to be 130 members financial until December 31, 2009. As of May 2010, only 24 are financial for 2010.

This is despite offering on-line renewal.

Contents

From the Chair	1
Association Matters	2
Education – Introduction to System Safety	3
Technical Report: ALARP Explored	4
Book Review: The Grown-Ups' Book on Risks	4
Aircraft Incident – Melbourne, March 2009	5
Train Collision – Craigieburn May 04, 2010	6

ISSEC 2010 Program

Program Overview

NEW to 2010: More innovative program structure, more international perspective, more intensive networking.

The event program will consist of two days of conference program, two days of workshops, Trade Business Centre, Networking and Social Functions.

Monday, 23 August

09:00 – 17:00 Conference Workshops (Included)
18:30 – 23:30 Conference Dinner

Tuesday, 24 August

08:30 – 17:00 Conference Program & Poster Display
08:30 – 17:00 Trade Business Centre open
17:00 – 19:00 Industry Networking Function

Wednesday, 25 August

08:30 – 17:00 Conference Program & Poster Display
08:30 – 15:30 Trade Business Centre open

Thursday, 26 August

08:30 – 17:00 Post conference Workshops (Additional)

This information is correct at time of publication and is an outline only, provided as an overview and is subject to change without notification. Timings are not confirmed and subject to change without notice.

ISSEC 2009 Proceedings



The conference proceedings for ISSEC 2009 have been published electronically around March 02, 2010.

Electronic Publication ISBN: 978-0-9807680-0-8

<http://www.issec.com.au/web/leas/tpcommon/src/tp1FullPage.cfm?idPageCopy=14899&idClient=969>

Research Award



In the December 2006 Newsletter, the aSCSa announced the establishment of student research award. The rules governing the award and associated forms are available from the [aSCSa website](http://www.ascsa.org.au).

The purpose of this annual award is to encourage Australian research in the science of software/system engineering or the application of that science for safety and/or mission critical software-intensive systems. At \$5000, it is a substantial award.

The nominated closing date requirement has now been removed; nominations can now be made any time.

Development of Safety Critical Systems

Public course

next offering: 13-16 July 2010

Safety is a whole life cycle issue that relates to all aspects of the system. Hardware, software, operating procedures, planning, development, testing, maintenance, installation, commissioning, decommissioning, disposal and other aspects are considered in a safety program.

For most safety-critical systems, it is insufficient to simply develop a safe system; the system must be shown to be acceptably safe. The lecture component of this course explains the principles and practice of safety management and engineering and the unique challenges of computer-based systems. The content blends discussion of management and development issues with practical experience in safety analysis techniques. Topics covered include: hazard identification and risk analysis, safe system design, safety analysis techniques, safe software engineering, system hazard analysis, safety cases, safety management and human factors, and formal methods for system specification. Techniques covered include: Hazard and Operability Studies (HAZOP) and Computer Hazard and Operability Studies (CHAZOP), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Failure Modes and Effects Analysis (FMEA) and Failure Modes Effects and Criticality Analysis (FMECA), and Goal Structured Notation (GSN).

Assumed Background

It is recommended that participants have taken ENGG7000 or have had other experience of systems development and the system lifecycle. Familiarity with software engineering principles is desirable but not essential.

Cost & Venue:

\$3300 incl. GST, Nancy Leveson's book "Safeware: System Safety & Computers" ISBN 0201119722 Addison Wesley course notes, lunch & refreshments

Room (TBC), The University of Queensland, St Lucia

To Register:

Contact [Claire Pomery](#), ITEE Academic Admin Officer (P: 07 3365 3984). Registration deadline is 5 July 2010

For further information:

<http://www.itee.uq.edu.au/~engg7020/DSCScourse.htm>

contact the Course Coordinator **Prof Peter Lindsay**

Phone: (+61 7) 3365 2005

Email: p.lindsay@uq.edu.au

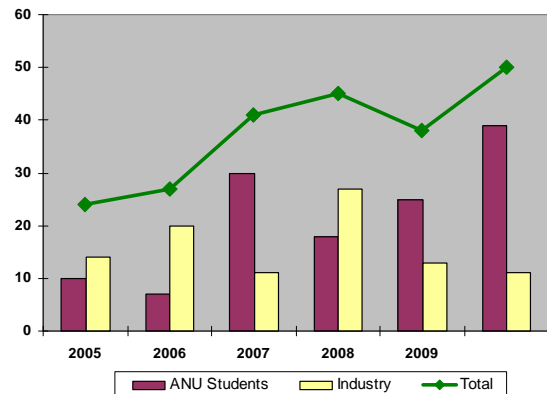
Education - Introduction to System Safety

For the sixth consecutive year, the aSCSa and the ANU facilitated the University of York's High Integrity Systems unit's 5 day intensive course on *Introduction to System Safety Engineering and Management*. The course is an elective within the ANU Masters of Software Engineering program and industry participants

are encouraged to attend through advertising by aSCSa.

This year there were 50 participants. There were 39 MSE students (25 in 2009) and 11 industry participants (13 in 2009). Over the five years 225 people have undertaken the course.

Course Participation



The course is expected to continue next year. Once the dates are confirmed by the ANU, the aSCSa will advertise for industry participants. There are no prerequisites for participation.



Engineering Education Australia



AMOG
Consulting
Leading Engineering Solutions

System Safety Engineering Master Class

Engineering Education Australia (EEA), on behalf of Engineers Australia in partnership with AMOG Consulting, offer a System Safety Engineering. This five day intensive master class delivers the critical aspects of system safety engineering and management. The key delivery areas of system safety engineering, development and maintenance of the safety case, hazard identification/analysis and risk reduction, and software safety management, are brought to life by detailed case studies, practical trouble shooting and real life worked examples.

For details of future courses see [EEA website](#).

(Next course is 16 to 20 August 2010, Canberra)

IEC 61508 – New revision

Parts 1 to 7 of IEC 61508 Edition 2 became available for purchase from the IEC web store <http://webstore.iec.ch/> on May 01, 2010.

Technical Report - *ALARP Explored*



Redmill, F
School of Computer Science
CS-TRN° 1197, March 2010

<http://www.cs.ncl.ac.uk/publications/techreports/>

This report explores the ALARP Principle. It explains its tenets, presents its history, examines its practical application, and discusses the concepts which underpin it and to which it is related.

It is narrative in nature and clearly describes the relationships between safety law with respect to the so far as is reasonably practicable principle, to the ALARP principle and to the safety integrity level concept. The report provides to the reader clear and practicable guidance on how to apply the ALARP principle.

Whereas the report's narrative is continuous, each chapter covers its topic fully, is largely self-contained, and may be read in isolation – except that Chapter 4 is a necessary preliminary to Chapter 5.

Chapter 1 introduces the subject of risk, the variability of its perception between individuals, and the nature and need of risk-tolerability decisions. Chapter 2 introduces and explains the ALARP Principle, and Chapter 3 recounts its development from a legal perspective. Chapter 4 derives the preparatory processes essential to the Principle's application, and Chapter 5 describes the processes necessary for its central purpose – the making of risk-tolerability decisions. Section 6 offers a discussion of the main risk-based concepts on which the Principle depends and with which it interacts. Finally, Chapter 7 draws conclusions and discusses the relationship between the Principle and the law of the land.

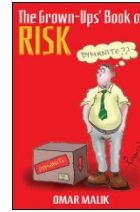
This report provides a good reference source for those associated with technology that may cause harm.

About the author

Felix has been with the Centre for Software Reliability (CSR) since 1991, when he became the inaugural Co-ordinator of the Safety-Critical Systems Club. He holds degrees in Electrical Engineering and Computation and is a Fellow of both the Institution of Electrical Engineers and the British Computer Society. He has studied, written on, and lectured on the subjects of Software Engineering, Project Management, and Safety Risk Engineering and Management, and his current primary research interest is safety risk.

Felix Redmill has supported the aSCSa as a keynote speaker and workshop presenter on a number of occasions, since the formation of the aSCSa in 2002. His expertise in risk management and safety technology is evident by his list of publications and the continuing demand for his services in many parts of the world.

Book Review - *The Grown-Ups' Book of Risk*



Author: Omar Malik
New Insight Press, 338pp
ISBN 9780956022400
Published 1 November 2008
Reviewer: James T. Crouse

Investigating aircraft and other accidents for more than 30 years, I have read several works on their cause and prevention. Omar Malik's work portended to be a more practical one - his background as a Royal Air Force flight instructor and British Airways captain with 12 years' experience in accident investigation, focusing on accident prevention, were indications that this fellow might know what he was talking about (helped by his strong education background, which includes a doctorate in aviation security).

Malik's main thrust is how to control risk, and to give us a working understanding of risk, he describes the world of risks, their geneses and relationships, and presents laws, lists, tables and concepts which, although sensible, are daunting in their number and interrelationships. In his defence, every book I have read in this area contains many lists and terms, so perhaps it comes with the subject. In this work, however, I found myself wishing for a separate glossary in order to avoid returning to prior pages to remind myself of what a particular concept meant. An index would have been helpful.

All the information is prologue for what Malik calls "Failure Path Analysis" which, at first reading, is similar to the "Swiss cheese" theory of accident causation, depicted in hundreds of works by showing several separated pieces, adjusted so that some of their random holes align with an arrow through them, the point being that when these holes (in other words, events) align, an accident happens. Similarly, Malik says that most failures occur when a number of deficiencies lying dormant become operative, creating a "failure path" through all preventative efforts. But here he ploughs new ground when he turns it around and looks for what would have prevented the accident rather than what caused it - "Possible Opportunities to Prevent Loss" or PO2PL, a process that identifies failure points within the system and traces the path through them. It is a fundamental alteration of the Swiss cheese model.

Via discussion of many of the best-known aviation disasters of the 20th century (including the loss of the Space Shuttle Challenger, the Black Hawk shoot-down in Iraq and a number of catastrophic failures involving the de Havilland Comet) and other non-aviation tragedies, Malik points out not only the failures that produced the terrible results but also the failures in the post-accident investigations that constitute missed opportunities to prevent future horrors. He blames this, in part, on non-independent bureaucracies' ineptness and unwillingness to think beyond their own inherent viewpoints, augmented by a healthy portion of CYA, or Covering Your Ass. With sharp insight, he notes that one of the necessities of accident investigation is closure, which often pinpoints a simple, singular cause

of an accident, such as the failure of a person or a component. But the failure of a system of operation, or elements thereof, is too nebulous to enable closure. In my experience, systems (in other words, organisations) are much more difficult to alter - institutions are highly resistant to change, even after tragedies.

The Grown-Ups' Book of Risk makes a number of other excellent points, centred on Malik's core point that the world is and will remain a dangerous place, and one that constantly presents new risks and alters the ones already here. One example is that the introduction of a new safety measure itself creates risk, because it is new, adding another layer of complexity to an operation, and because safety measures themselves can produce complacency.

Malik deserves praise for many of his insights, especially his scepticism on investigative findings of "operator error" that often should more accurately be attributed to system flaws, management choices, or equipment design defects - not to mention the failure of governmental regulators and regulations. Amen.

Simply stated, this is a worthy book. As I read it, I thought of many acquaintances in the aviation safety field who I would hope would read it. Safety is big business in aviation now, with alphabetised systems aplenty. Malik brings the focus back home to where it belongs - to us, the human component.

As Malik points out, perhaps this self-published work does not contain enough scientifically defined terms to merit inclusion in academic journals. That may well be a flaw to some, but those people aren't in the cockpit. I'll take his "common sense" approach to accident prevention. That is a term with which I, and others who fly and operate in this hazardous world, can live.

About James T. Crouse

James T. Crouse teaches aviation law at Duke Law School and practises law at Crouse Law Offices. He has practised aviation law for more than 28 years and was lead counsel in the world's largest civilian helicopter disaster. He is a veteran US Army senior aviator.

Aircraft Incident – Melbourne March 2009 - Update

Source: Tail Strike, Melbourne Airport, VIC: 20 March 2009: A6-ERG Airbus A340-500: [ATSB Transport Safety Report: Accident Occurrence Investigation – AO-2009-012 Preliminary](#).

[ATSB Media Release, December 18, 2009](#)

At 2231 on March 20, 2009, Australian Eastern Daylight-saving time, a United Arab Emirates Airbus A340-500, registered as A6-ERG, commenced take-off on a scheduled passenger flight to Dubai. On board were 257 passengers, 14 cabin crew, and 4 flight crew.

The take-off was planned as a reduced-power take-off. As the name suggests, a reduced-power take-off is a take-off carried out at less than available engine thrust.

The first officer was the handing pilot. At 53 seconds into the take-off, the captain called for the first officer to raise the nose of the aircraft in order to become

airborne. The plane did not immediately respond, so the first officer applied a greater nose-up command.

The nose of the aircraft was raised and the tail made contact with the runway surface but the plane failed to climb. The captain then selected the take-off and go-around (TOGA) thrust setting, the maximum thrust the engines can apply. The engines responded immediately and the plane began to climb.

The crew notified air traffic control of the tail strike and returned to Melbourne. The aircraft landed safely with no reported injuries. The tail strike resulted in substantial damage to the tail of the aircraft and damage to some airport lighting and the instrument landing system.

It is clear that there was insufficient thrust applied during the initial stage of the take-off such that there was insufficient runway available which forced the captain to select the TODA thrust setting resulting in the tail strike.

Why the insufficient thrust? A review of the aircraft's performance documentation showed that the take-off weight was understated by some 100 tonnes (100,000kg).

The magnitude of the take-off weight underestimate was significant. So why was the error not detected?

On December 18, 2009, the Australian Transport Safety Bureau (ATSB) released its [Interim Factual](#) report into the tail strike involving Airbus A340-500 aircraft, registered A6-ERG. The report states:

The investigation has determined that the pre-flight take-off performance calculations were based on an incorrect take-off weight that was inadvertently entered into the aircraft's portable flight planning computer by the flight crew. Subsequent crosschecks did not detect the incorrect entry and its effect on performance planning, and the resulting take-off speeds and engine thrust settings that were applied by the crew were insufficient for a normal takeoff.

As a result of this accident, the aircraft operator has undertaken a number of procedural, training and technical initiatives across its fleet and operations; with a view to minimising the risk of a recurrence. In addition, the aircraft manufacturer has released a modified version of its cockpit performance-planning tool and is developing a software package that automatically checks the consistency of the flight data being entered into the aircraft's flight computers by flight crews.

The investigation has found a number of similar take-off performance-related incidents and accidents across a range of aircraft types, locations and operators around the world. As a result, the ATSB has initiated a safety research project to collate those events and examine the factors involved. The findings of that project will be released by the ATSB once completed.

Train Collision – Craigieburn May 04, 2010

At around 8.33pm (AEST) on May 04, 2010, a commuter train operated by Metro Trains collided with the rear of a freight train operated by Pacific National.

According to media reports, fourteen passengers and the train driver were injured. One of the injured was 15 year girl suffered spinal injuries and was hospitalised. The girl was expected to make a full recovery.



The Age, May 05, 2010: Emergency workers took 20 minutes to remove the injured passengers and driver from the Metro train after last night's collision with the freight train (inset). Photo: Michael Clayton-Jones

At least two investigations have commenced; an internal investigation by Metro Trains and an investigation by Public Transport Safety Victoria.

According to the Herald Sun article *"Train driver on indefinite leave as investigations continue into crash"* [Ashley Gardiner, May 07, 2010], The Pacific National freight train was correctly stopped at a "controlled" signal when it was hit from behind by the Metro Trains commuter train. It is believed that the commuter train passed an "automatic" signal at STOP. The operational rules allow for trains to pass with caution "automatic" signals at STOP; the rules do not allow trains to pass "controlled" signals at STOP.

The aspect displayed in an automatic signal is determined automatically by the location of the train ahead and aspects of other signals between it and the train ahead. A controlled signal is one that displays a STOP aspect unless requested by a train controller (or signalman) otherwise.

It is believed that the commuter train, after leaving Roxburgh Park (the previous station stop), stopped on one occasion before taking off and running into the rear of the Pacific National train. This would be consistent with the signalling system design for the line; each signal capable of displaying a STOP aspect has an associated trip mechanism which automatically triggers the train's emergency brake should the train pass the signal when at STOP. If this happens the driver needs to get out of driving cab to reset it before proceeding.

In Australia only the Sydney and Melbourne commuter rail networks allow trains to pass automatic signals at STOP. This is allowed to minimise train delays should a signalling failure occur.

Passing an automatic signal at STOP resulted in a Sydney morning peak commuter train colliding with the

rear of the Indian Pacific, a long distance passenger train, at Glenbrook, NSW at 8.22am on December 02, 1999. Six passengers died and 51 passengers were taken to hospital with injuries. According to the [Inquiry Final Report](#), poor communication, procedural errors and pressures of on-time running were key causal factors. Unlike the Craigieburn collision, the driver of the Sydney commuter train did seek authorisation to pass automatic signals at STOP. However he was not told of the Indian Pacific ahead. Nevertheless the operational rules require the driver to drive the train cautiously after passing an automatic signal at STOP, such that the train can be stopped short of any obstruction.

There has been no mention of the driver of the Metro Trains commuter train driver requesting permission to pass the automatic signal at STOP. This suggests that it is not normal practice to do so. As it is a commuter line, the driver of the commuter train would most likely be expecting another short commuter train ahead; not the longer Pacific National freight train.

Hopefully the investigations will shed light on the cause of the Craigieburn collision. However the continued use of procedures which allow for the overriding of safety systems at will to meet a commercial objective, in the Craigieburn and Glenbrook cases, on-time running, is counter to the principles of safety. Why safety regulators allow such practices to persist when there are examples of the serious consequences is difficult to understand.

Recruitment

Looking for change in career or to recruit? Kinetic Recruitment Australia initially a defence recruitment organisation has since expanded to aerospace, ICT, rail, transport infrastructure and more.



www.kineticrecruitment.com.au/

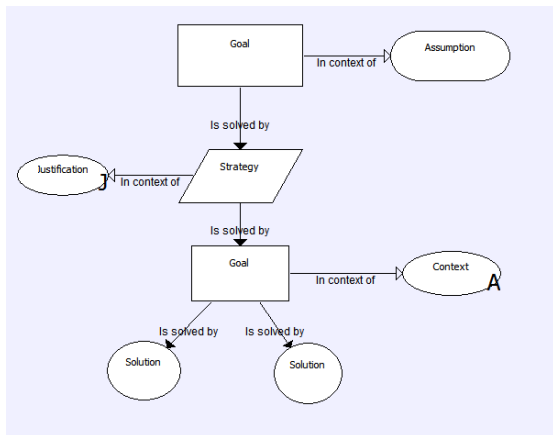
System Safety Society now in Australia



The aSCSa is corporate member of the System Safety Society. They have just established an Australian chapter, visit www.asssc.org.

GSN Draft Standard

The drafting committee for a future GSN Standard have issued a draft for GSN user community and other interested parties to comment.



The draft standard may be downloaded from:

www.goalstructuringnotation.info

Consultancy Period: May 19th to August 27th 2010

The Drafting Committee welcomes comments on this interim, incomplete Draft Standard. They have set up a Google Wave to handle comments and discussion about the Standard. To join the wave, please email details of your Google Wave account or your email address to katrina.attwood@cs.york.ac.uk. If you are unable to access the Wave, please email comments to the above address, and they will be added to the Wave for you.

The Drafting Committee is intending to meet at the end of the Consultancy Period, and revise the draft in the light of comments received. It is their intention to publish Issue 1 of the Standard by November 01, 2010

STAMP Course

The aSCSa has received a request to arrange a course for January 2011, on STAMP, an accident causation model based on systems engineering conceived by Dr. Nancy Leveson.

Dr Leveson offers a System Safety for Software Intensive Systems Course which includes STAMP.

Course Topics

- The Problem:
 - Accident Causes
 - Computers and Risk
 - Safety vs. Reliability
- A New Holistic, Control-Based Approach to System Safety
- System Hazard Analysis for Complex, Software-Intensive Systems
- Software Hazard Analysis
- Software Requirements Specification/Modelling and Analysis
- Principles of safe design
 - System and Software
 - Human-Machine Interaction
- Verification and Validation of safety
- Organization and Management of Safety-Critical Projects

You can find more details about STAMP and other related topics on Dr. Leveson's website, <http://sunnyday.mit.edu/>.

Dr. Leveson is a Professor in the MIT Aeronautics and Astronautics Dept. and in the Engineering Systems Division and is head of the MIT Complex Systems Research Lab (CSRL). Previously, she was Boeing Professor of Computer Science and Engineering at the University of Washington. Dr. Leveson is a founder of the field of software safety and has worked in this area since 1980. Before becoming a professor, she was a system engineer for IBM. Dr. Leveson consults widely on safety-critical systems for both government and industry and has worked with aerospace, nuclear power, transportation, aircraft, and medical systems. In 1995, Dr. Leveson was awarded the AIAA Information Systems Award for "developing the field of software safety and system engineering practices where life and property are at stake." She received the 1999 ACM Allen Newell Award for "pioneering work in establishing the foundations of software safety," and the 2004 ACM Outstanding Software Research Award. In 1999, Dr. Leveson was elected to the National Academy of Engineering (NAE).

The costs in arranging such a course are not inconsiderable for such an eminent international presenter.

To assess viability, the aSCSa will soon be seeking expressions of interest from organisations in terms of delegate numbers and sponsorship and from the general safety-related systems community. Details as to where you can register your interest will soon be posted on the aSCSa website. Courses fees in the USA are typically \$3500USD and numbers are limited to 40. The fee for the course in Australia has not yet been determined.



**Risk
Reliability
Resilience**

Contact: kevin.anderson@hyderconsulting.com

RRR