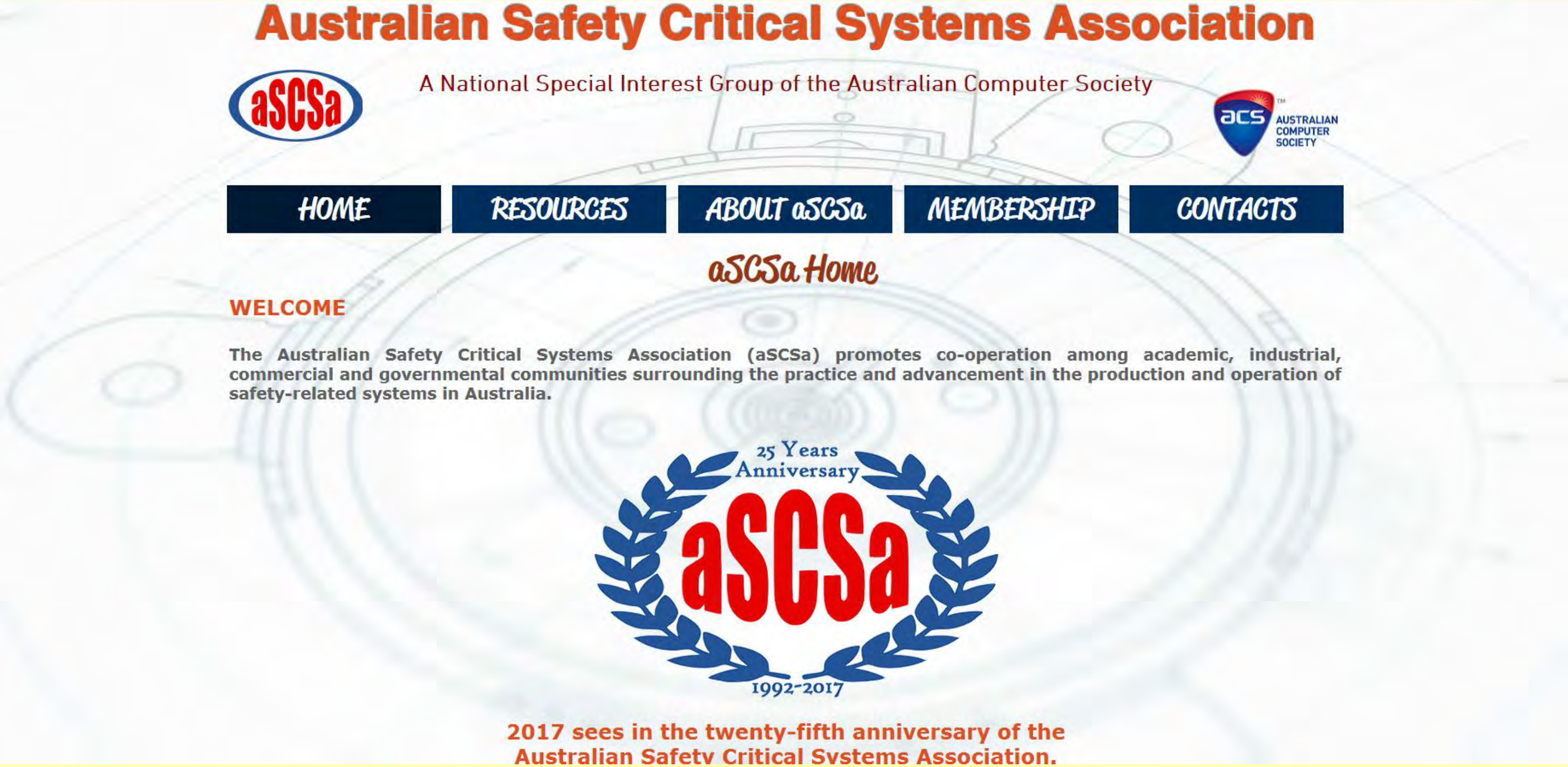


Australian Safety Critical Systems Association

A National Special Interest Group of the Australian Computer Society

aSCSa Home

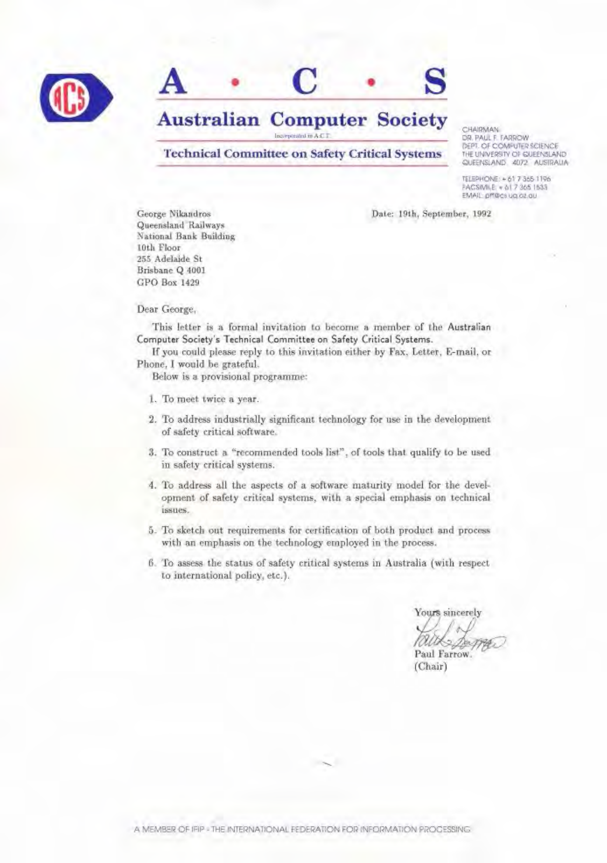
WELCOME

The Australian Safety Critical Systems Association (aSCSa) promotes co-operation among academic, industrial, commercial and governmental communities surrounding the practice and advancement in the production and operation of safety-related systems in Australia.

2017 sees in the twenty-fifth anniversary of the Australian Safety Critical Systems Association.

Since 1992

www.ascsa.org.au



A • C • S

Australian Computer Society

Incorporated in A.C.T.

Technical Committee on Safety Critical Systems

CHAIRMAN:
DR. PAUL F. FARROW
DEPT. OF COMPUTER SCIENCE
THE UNIVERSITY OF QUEENSLAND
QUEENSLAND 4072 AUSTRALIA

TELEPHONE: + 61 7 365 1196
FACSIMILE: + 61 7 365 1533
EMAIL: pff@cs.uq.oz.au

George Nikandros
Queensland Railways
National Bank Building
10th Floor
255 Adelaide St
Brisbane Q 4001
GPO Box 1429

Date: 19th, September, 1992

Dear George,

This letter is a formal invitation to become a member of the Australian Computer Society's Technical Committee on Safety Critical Systems.

If you could please reply to this invitation either by Fax, Letter, E-mail, or Phone, I would be grateful.

Below is a provisional programme:

1. To meet twice a year.
2. To address industrially significant technology for use in the development of safety critical software.
3. To construct a "recommended tools list", of tools that qualify to be used in safety critical systems.
4. To address all the aspects of a software maturity model for the development of safety critical systems, with a special emphasis on technical issues.
5. To sketch out requirements for certification of both product and process with an emphasis on the technology employed in the process.
6. To assess the status of safety critical systems in Australia (with respect to international policy, etc.).

Yours sincerely

Paul Farrow.
(Chair)

A MEMBER OF IFIP - THE INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING

A • C • S

Australian Computer Society

Incorporated in A.C.T.

Technical Committee on Safety Critical Systems

CHAIRMAN:
DR. PAUL F. FARROW
DEPT. OF COMPUTER SCIENCE
THE UNIVERSITY OF QUEENSLAND
QUEENSLAND 4072 AUSTRALIA

TELEPHONE: + 61 7 365 1196
FACSIMILE: + 61 7 365 1533
EMAIL: pff@cs.uq.oz.au

George Nikandros
Queensland Railways

Date: 19th, September, 1992

Dr Paul Farrow (Chairman)	The University of Queensland
Prof Alan Underwood	Queensland University of Technology
George Nikandros	Queensland Railways
Charles Page	Westinghouse Brake & Signal
Group Captain Dennis Street	RAAF
Jonathon Holbrook	Ford Motor Company
Peter James	EASAMS
Dr Tony Cant	DSTO
Peter Hodder	Admiral Computing
Greg Royle	CSA

Formed in1992

Chairman

National Technical Committee on Safety-Critical Systems

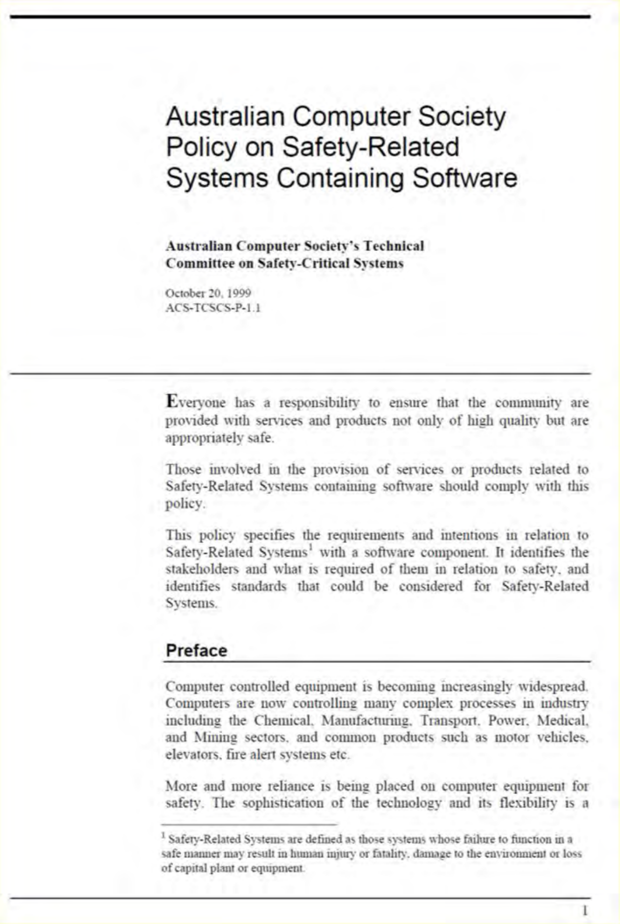
Term	*Chairman*
1992-1994	Dr Paul Farrow
1994-1996	Charles Page
1996-1998	George Nikandros
1998-2000	Dr Peter Lindsay
2000-2002	Kevin Anderson

Australian Safety-Critical Systems Association

Term	*Chairman*
2002-2010	George Nikandros
2010-2015	Prof Clive Boughton
2015-	Brett (BJ) Martin

- *In 2002 the National Technical Committee morphed into the Australian Safety-Critical Systems Club.*
- *The “Club” became the Australian Safety Critical Association was renamed as an “association” in 2005.*

Providing Guidance



Australian Computer Society Policy on Safety-Related Systems Containing Software

Australian Computer Society's Technical Committee on Safety-Critical Systems

October 20, 1999
ACS-TCSCS-P-1.1

Everyone has a responsibility to ensure that the community are provided with services and products not only of high quality but are appropriately safe.

Those involved in the provision of services or products related to Safety-Related Systems containing software should comply with this policy.

This policy specifies the requirements and intentions in relation to Safety-Related Systems[1] with a software component. It identifies the stakeholders and what is required of them in relation to safety, and identifies standards that could be considered for Safety-Related Systems.

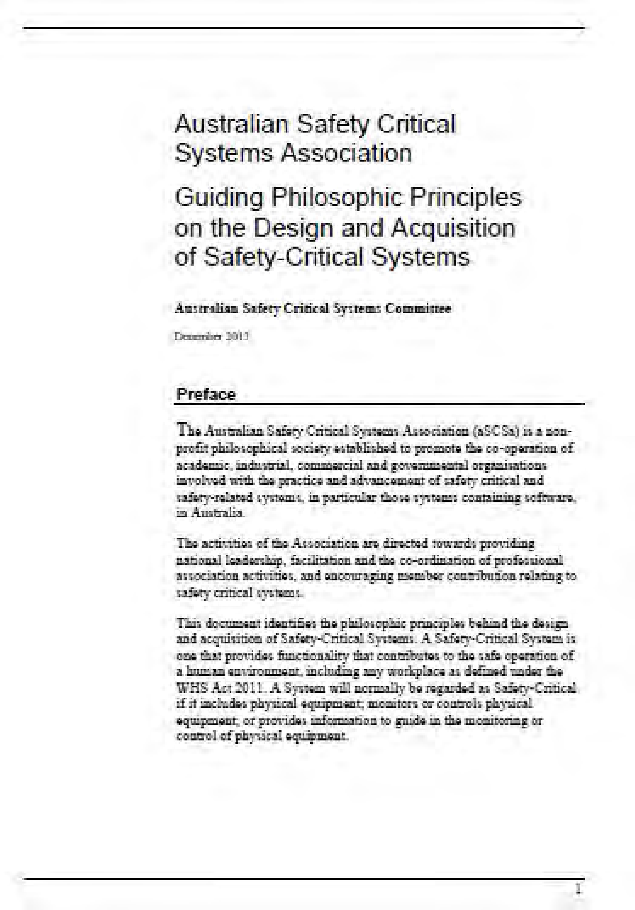
Preface

Computer controlled equipment is becoming increasingly widespread. Computers are now controlling many complex processes in industry including the Chemical, Manufacturing, Transport, Power, Medical, and Mining sectors, and common products such as motor vehicles, elevators, fire alert systems etc.

More and more reliance is being placed on computer equipment for safety. The sophistication of the technology and its flexibility is a

[1] Safety-Related Systems are defined as those systems whose failure to function in a safe manner may result in human injury or fatality, damage to the environment or loss of capital plant or equipment.

1



Australian Safety Critical Systems Association

Guiding Philosophic Principles on the Design and Acquisition of Safety-Critical Systems

Australian Safety Critical Systems Committee

December 2013

Preface

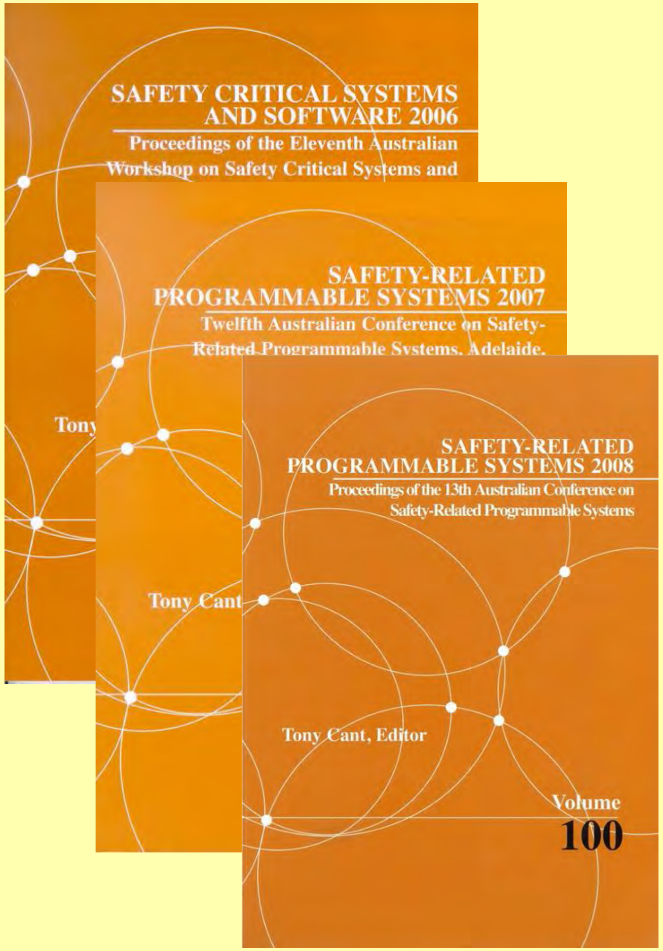
The Australian Safety Critical Systems Association (aSCSa) is a non-profit philosophical society established to promote the co-operation of academic, industrial, commercial and governmental organisations involved with the practice and advancement of safety critical and safety-related systems, in particular those systems containing software, in Australia.

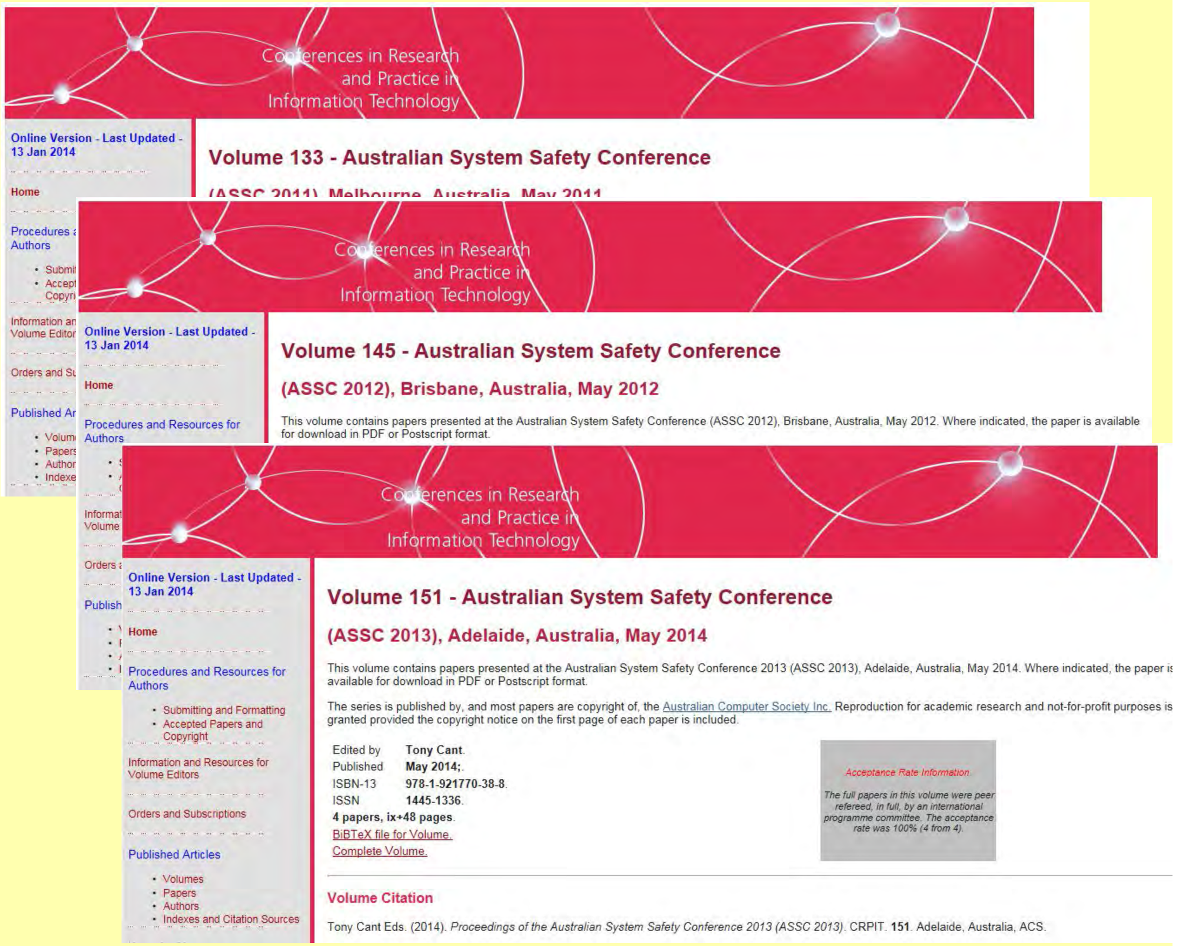
The activities of the Association are directed towards providing national leadership, facilitation and the co-ordination of professional association activities, and encouraging member contribution relating to safety critical systems.

This document identifies the philosophic principles behind the design and acquisition of Safety-Critical Systems. A Safety-Critical System is one that provides functionality that contributes to the safe operation of a human environment, including any workplace as defined under the WHS Act 2011. A System will normally be regarded as Safety-Critical if it includes physical equipment; monitors or controls physical equipment; or provides information to guide in the monitoring or control of physical equipment.

1

Adding to the body of knowledge since 1996


SAFETY CRITICAL SYSTEMS AND SOFTWARE 2006
Proceedings of the Eleventh Australian Workshop on Safety Critical Systems and
Tony
SAFETY-RELATED PROGRAMMABLE SYSTEMS 2007
Twelfth Australian Conference on Safety-Related Programmable Systems, Adelaide,
Tony Cant
SAFETY-RELATED PROGRAMMABLE SYSTEMS 2008
Proceedings of the 13th Australian Conference on Safety-Related Programmable Systems
Tony Cant, Editor
Volume
100


Conferences in Research and Practice in Information Technology
Online Version - Last Updated - 13 Jan 2014
Home
Procedures and Resources for Authors
Submitting and Formatting
Accepted Papers and Copyright
Information and Resources for Volume Editors
Orders and Subscriptions
Published Articles
Volumes
Papers
Authors
Indexes and Citation Sources

Volume 133 - Australian System Safety Conference

(ASSC 2011), Melbourne, Australia, May 2011

Volume 145 - Australian System Safety Conference

(ASSC 2012), Brisbane, Australia, May 2012

This volume contains papers presented at the Australian System Safety Conference (ASSC 2012), Brisbane, Australia, May 2012. Where indicated, the paper is available for download in PDF or Postscript format.

Volume 151 - Australian System Safety Conference

(ASSC 2013), Adelaide, Australia, May 2014

This volume contains papers presented at the Australian System Safety Conference 2013 (ASSC 2013), Adelaide, Australia, May 2014. Where indicated, the paper is available for download in PDF or Postscript format.

The series is published by, and most papers are copyright of, the Australian Computer Society Inc. Reproduction for academic research and not-for-profit purposes is granted provided the copyright notice on the first page of each paper is included.

Edited by	**Tony Cant**.
Published	**May 2014;**.
ISBN-13	**978-1-921770-38-8**.
ISSN	**1445-1336**.

4 papers, ix+48 pages.

BiBTeX file for Volume.

Complete Volume.

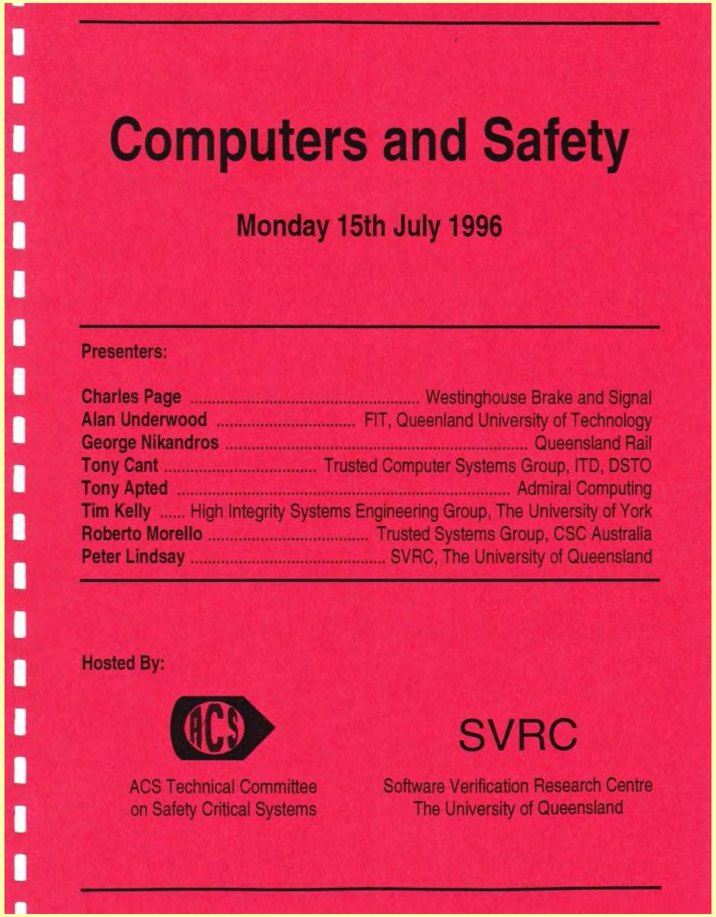
Acceptance Rate Information

The full papers in this volume were peer refereed, in full, by an international programme committee. The acceptance rate was 100% (4 from 4).

Volume Citation

Tony Cant Eds. (2014). *Proceedings of the Australian System Safety Conference 2013 (ASSC 2013)*. CRPIT. **151**. Adelaide, Australia, ACS.

First Conference 15 July, 1996



Computers and Safety

Monday 15th July 1996

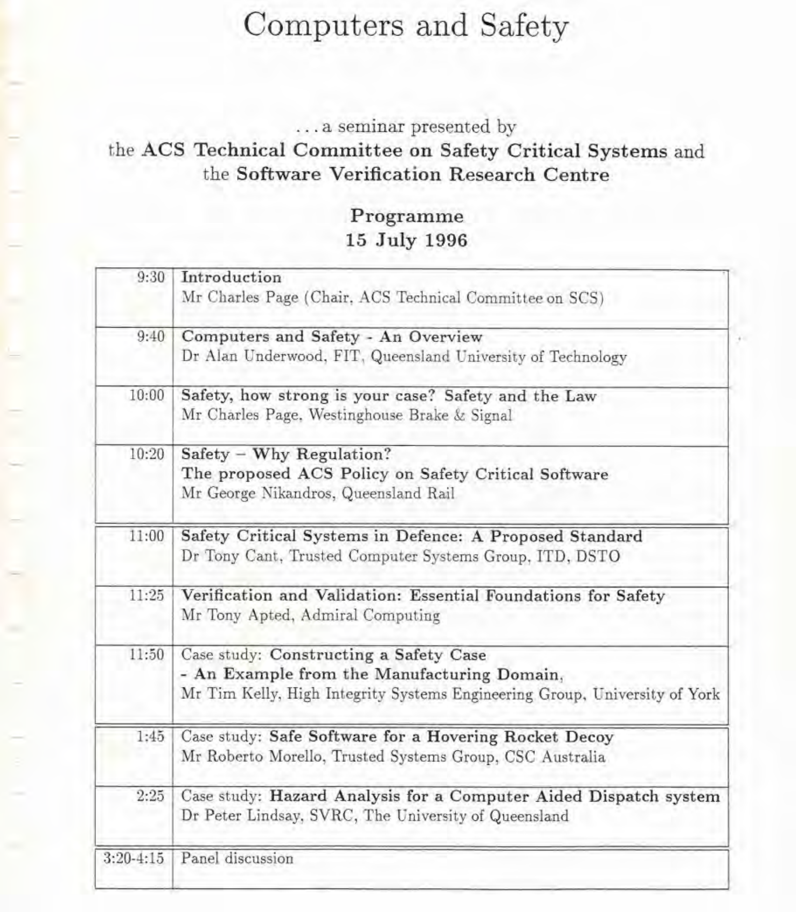
Presenters:

Charles Page	Westinghouse Brake and Signal
Alan Underwood	FIT, Queenland University of Technology
George Nikandros	Queensland Rail
Tony Cant	Trusted Computer Systems Group, ITD, DSTO
Tony Apted	Admiral Computing
Tim Kelly	High Integrity Systems Engineering Group, The University of York
Roberto Morello	Trusted Systems Group, CSC Australia
Peter Lindsay	SVRC, The University of Queensland

Hosted By:

ACS Technical Committee
on Safety Critical Systems

SVRC
Software Verification Research Centre
The University of Queensland



Computers and Safety

. . . a seminar presented by
the **ACS Technical Committee on Safety Critical Systems** and
the **Software Verification Research Centre**

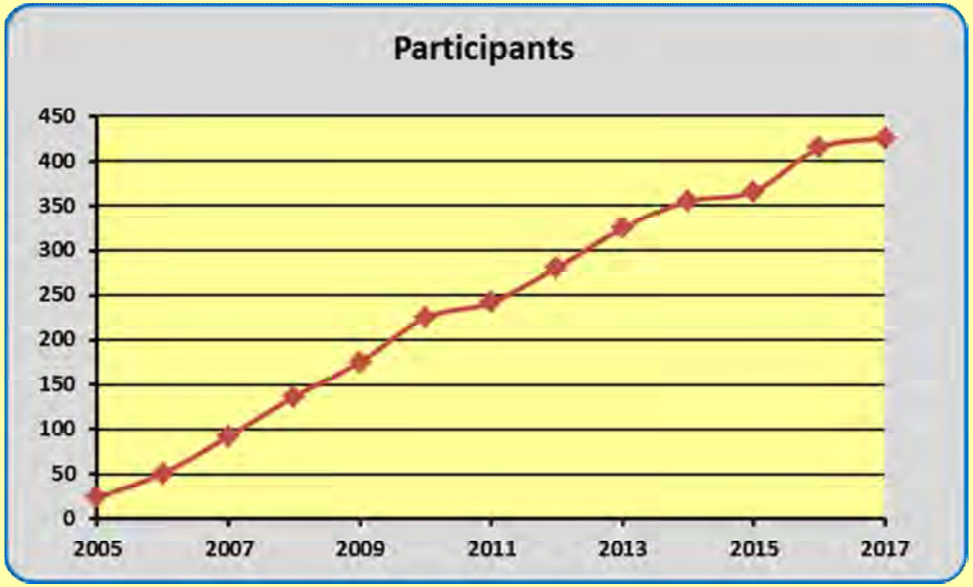
Programme
15 July 1996

9:30	**Introduction** Mr Charles Page (Chair, ACS Technical Committee on SCS)
9:40	**Computers and Safety - An Overview** Dr Alan Underwood, FIT, Queensland University of Technology
10:00	**Safety, how strong is your case? Safety and the Law** Mr Charles Page, Westinghouse Brake & Signal
10:20	**Safety – Why Regulation?** **The proposed ACS Policy on Safety Critical Software** Mr George Nikandros, Queensland Rail
11:00	**Safety Critical Systems in Defence: A Proposed Standard** Dr Tony Cant, Trusted Computer Systems Group, ITD, DSTO
11:25	**Verification and Validation: Essential Foundations for Safety** Mr Tony Apted, Admiral Computing
11:50	Case study: **Constructing a Safety Case** **- An Example from the Manufacturing Domain,** Mr Tim Kelly, High Integrity Systems Engineering Group, University of York
1:45	Case study: **Safe Software for a Hovering Rocket Decoy** Mr Roberto Morello, Trusted Systems Group, CSC Australia
2:25	Case study: **Hazard Analysis for a Computer Aided Dispatch system** Dr Peter Lindsay, SVRC, The University of Queensland
3:20-4:15	Panel discussion

Promoting Professional Skills Development

- *426 participants since 2005 (167 from industry)*

Systems and Software Safety
A short course from the University of York Masters degree course in Safety Critical Systems Engineering



The course is provided annually, usually in April.

- **The ANU course jointly facilitated with aSCSa, annually until 2014, now every two years.**
- **From 2015, the aSCSa in the other years through Griffith University.**

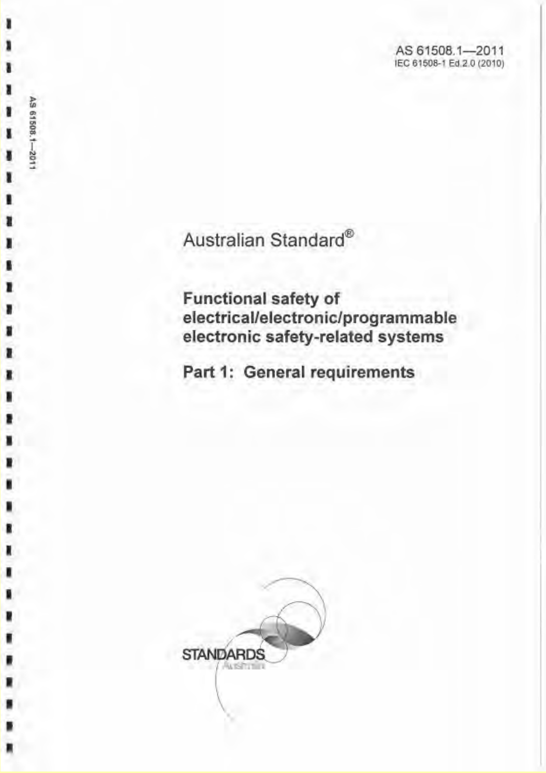
Encouraging Research

Research Award

To encourage research in the science of software/system engineering or the application of that science for safety and/or mission critical software-intensive systems.

$5000.00

Standards Involvement – AS 61508 - 2011



AS 61508.1—2011
IEC 61508-1 Ed.2.0 (2010)

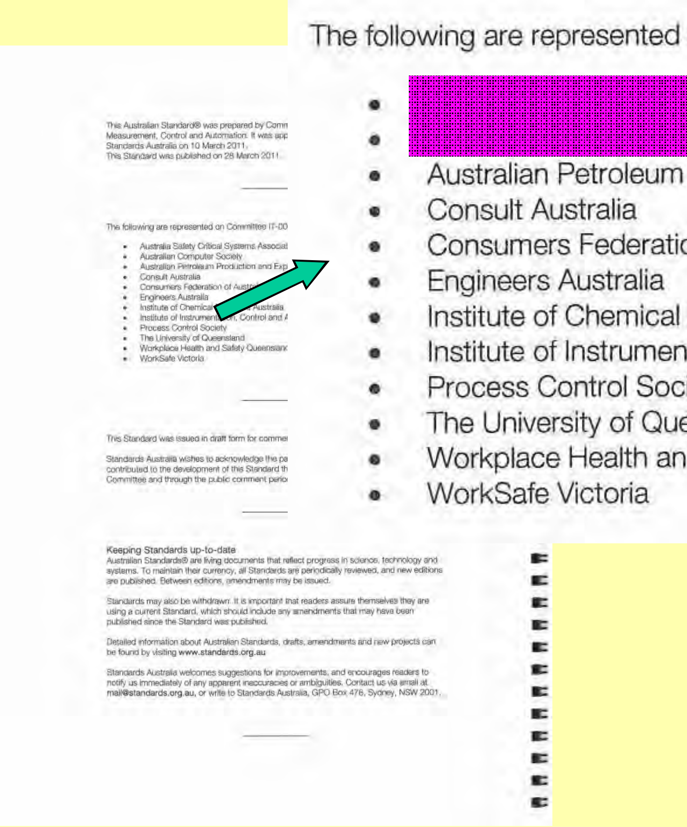
AS 61508.1—2011

Australian Standard®

Functional safety of electrical/electronic/programmable electronic safety-related systems

Part 1: General requirements

STANDARDS Australia



This Australian Standard® was prepared by Comm
Measurement, Control and Automation. It was app
Standards Australia on 10 March 2011.
This Standard was published on 28 March 2011.

The following are represented on Committee IT-00

- Australia Safety Critical Systems Associat
- Australian Computer Society
- Australian Petroleum Production and Exp
- Consult Australia
- Consumers Federation of Austr
- Engineers Australia
- Institute of Chemical Australia
- Institute of Instrument, Control and A
- Process Control Society
- The University of Queensland
- Workplace Health and Safety Queenslanc
- WorkSafe Victoria

This Standard was issued in draft form for commer

Standards Australia wishes to acknowledge the pa
contributed to the development of this Standard th
Committee and through the public comment perioc

Keeping Standards up-to-date
Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

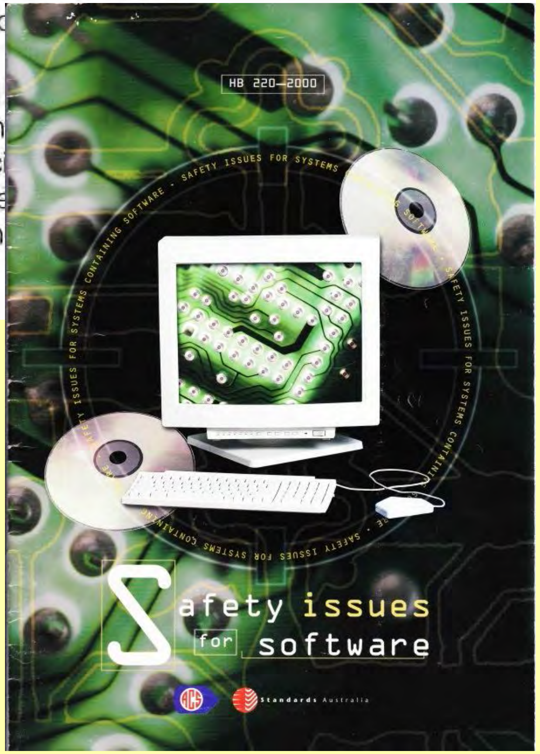
Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

The following are represented on Committee IT-006:

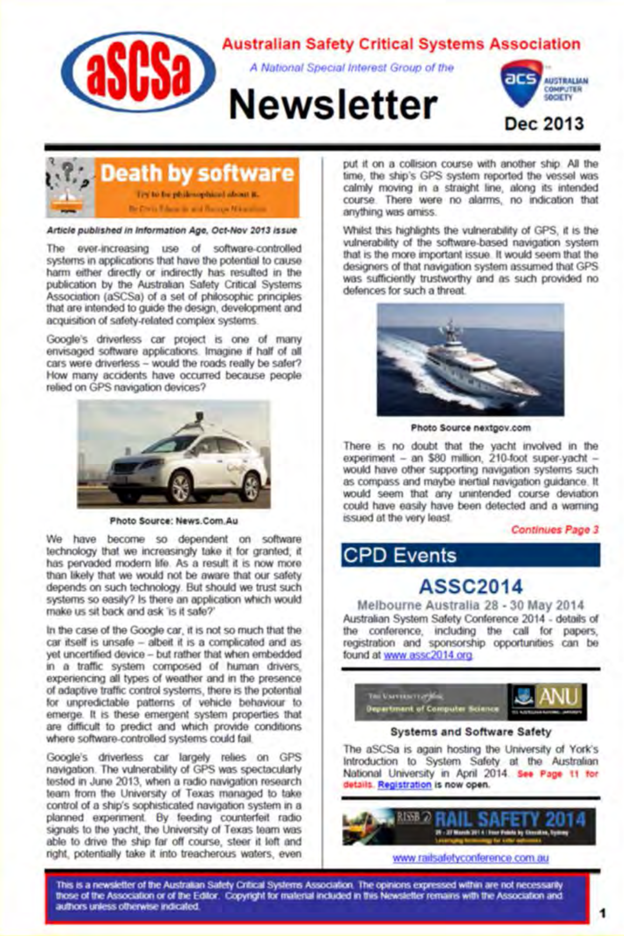
- [illegible]
- [illegible]
- Australian Petroleum Production and Exploration Association
- Consult Australia
- Consumers Federatio
- Engineers Australia
- Institute of Chemical
- Institute of Instrumen
- Process Control Soci
- The University of Que
- Workplace Health an
- WorkSafe Victoria



HB 220—2000

Safety issues for software

Increasing awareness through newsletters



aSCSa **Australian Safety Critical Systems Association**
A National Special Interest Group of the acs AUSTRALIAN COMPUTER SOCIETY

Newsletter **Dec 2013**

Death by software

Try to be philosophical about it.

Article published in Information Age, Oct-Nov 2013 issue

The ever-increasing use of software-controlled systems in applications that have the potential to cause harm either directly or indirectly has resulted in the publication by the Australian Safety Critical Systems Association (aSCSa) of a set of philosophic principles that are intended to guide the design, development and acquisition of safety-related complex systems.

Google's driverless car project is one of many envisaged software applications. Imagine if half of all cars were driverless – would the roads really be safer? How many accidents have occurred because people relied on GPS navigation devices?

Photo Source: News.Com.Au

We have become so dependent on software technology that we increasingly take it for granted; it has pervaded modern life. As a result it is now more than likely that we would not be aware that our safety depends on such technology. But should we trust such systems so easily? Is there an application which would make us sit back and ask 'is it safe?'

In the case of the Google car, it is not so much that the car itself is unsafe – albeit it is a complicated and as yet uncertified device – but rather that when embedded in a traffic system composed of human drivers, experiencing all types of weather and in the presence of adaptive traffic control systems, there is the potential for unpredictable patterns of vehicle behaviour to emerge. It is these emergent system properties that are difficult to predict and which provide conditions where software-controlled systems could fail.

Google's driverless car largely relies on GPS navigation. The vulnerability of GPS was spectacularly tested in June 2013, when a radio navigation research team from the University of Texas managed to take control of a ship's sophisticated navigation system in a planned experiment. By feeding counterfeit radio signals to the yacht, the University of Texas team was able to drive the ship far off course, steer it left and right, potentially take it into treacherous waters, even put it on a collision course with another ship. All the time, the ship's GPS system reported the vessel was calmly moving in a straight line, along its intended course. There were no alarms, no indication that anything was amiss.

Whilst this highlights the vulnerability of GPS, it is the vulnerability of the software-based navigation system that is the more important issue. It would seem that the designers of that navigation system assumed that GPS was sufficiently trustworthy and as such provided no defences for such a threat.

Photo Source nextgov.com

There is no doubt that the yacht involved in the experiment – an $80 million, 210-foot super-yacht – would have other supporting navigation systems such as compass and maybe inertial navigation guidance. It would seem that any unintended course deviation could have easily have been detected and a warning issued at the very least.

Continues Page 3

CPD Events

ASSC2014

Melbourne Australia 28 - 30 May 2014

Australian System Safety Conference 2014 - details of the conference, including the call for papers, registration and sponsorship opportunities can be found at www.assc2014.org.

The University of York Department of Computer Science ANU

Systems and Software Safety

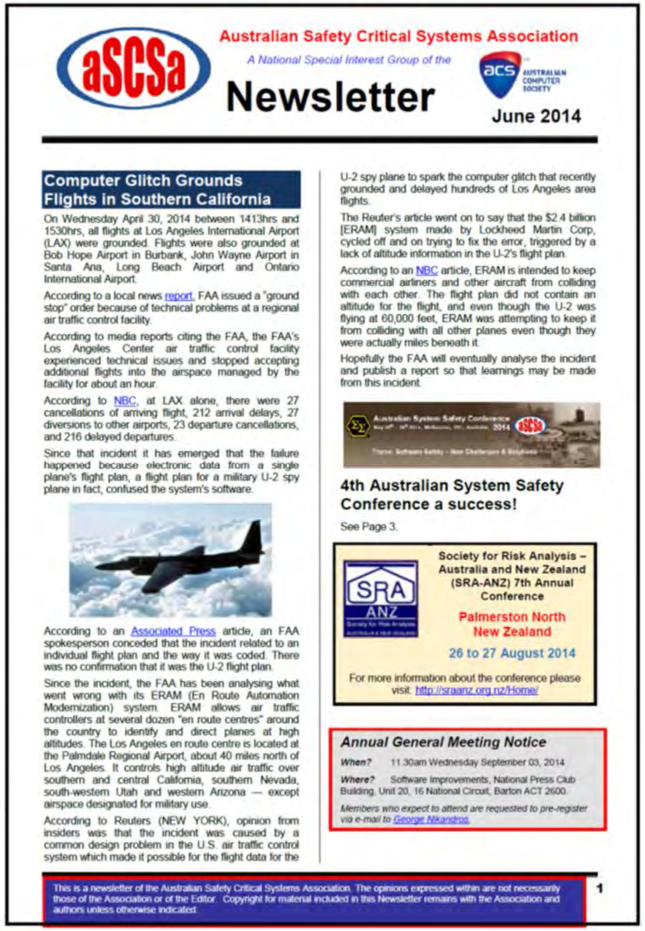
The aSCSa is again hosting the University of York's Introduction to System Safety at the Australian National University in April 2014. **See Page 11 for details.** Registration **is now open.**

RISSB RAIL SAFETY 2014

www.railsafetyconference.com.au

This is a newsletter of the Australian Safety Critical Systems Association. The opinions expressed within are not necessarily those of the Association or of the Editor. Copyright for material included in this Newsletter remains with the Association and authors unless otherwise indicated.

1



aSCSa **Australian Safety Critical Systems Association**
A National Special Interest Group of the acs AUSTRALIAN COMPUTER SOCIETY

Newsletter **June 2014**

Computer Glitch Grounds Flights in Southern California

On Wednesday April 30, 2014 between 1413hrs and 1530hrs, all flights at Los Angeles International Airport (LAX) were grounded. Flights were also grounded at Bob Hope Airport in Burbank, John Wayne Airport in Santa Ana, Long Beach Airport and Ontario International Airport.

According to a local news report, FAA issued a "ground stop" order because of technical problems at a regional air traffic control facility.

According to media reports citing the FAA, the FAA's Los Angeles Center air traffic control facility experienced technical issues and stopped accepting additional flights into the airspace managed by the facility for about an hour.

According to NBC, at LAX alone, there were 27 cancellations of arriving flight, 212 arrival delays, 27 diversions to other airports, 23 departure cancellations, and 216 delayed departures.

Since that incident it has emerged that the failure happened because electronic data from a single plane's flight plan, a flight plan for a military U-2 spy plane in fact, confused the system's software.

According to an Associated Press article, an FAA spokesperson conceded that the incident related to an individual flight plan and the way it was coded. There was no confirmation that it was the U-2 flight plan.

Since the incident, the FAA has been analysing what went wrong with its ERAM (En Route Automation Modernization) system. ERAM allows air traffic controllers at several dozen "en route centres" around the country to identify and direct planes at high altitudes. The Los Angeles en route centre is located at the Palmdale Regional Airport, about 40 miles north of Los Angeles. It controls high altitude air traffic over southern and central California, southern Nevada, south-western Utah and western Arizona — except airspace designated for military use.

According to Reuters (NEW YORK), opinion from insiders was that the incident was caused by a common design problem in the U.S. air traffic control system which made it possible for the flight data for the U-2 spy plane to spark the computer glitch that recently grounded and delayed hundreds of Los Angeles area flights.

The Reuter's article went on to say that the $2.4 billion [ERAM] system made by Lockheed Martin Corp, cycled off and on trying to fix the error, triggered by a lack of altitude information in the U-2's flight plan.

According to an NBC article, ERAM is intended to keep commercial airliners and other aircraft from colliding with each other. The flight plan did not contain an altitude for the flight, and even though the U-2 was flying at 60,000 feet, ERAM was attempting to keep it from colliding with all other planes even though they were actually miles beneath it.

Hopefully the FAA will eventually analyse the incident and publish a report so that learnings may be made from this incident.

Australian System Safety Conference 2014 aSCSa

4th Australian System Safety Conference a success!

See Page 3.

Society for Risk Analysis – Australia and New Zealand (SRA-ANZ) 7th Annual Conference

SRA ANZ

Palmerston North New Zealand

26 to 27 August 2014

For more information about the conference please visit: http://sraanz.org.nz/Home/

Annual General Meeting Notice

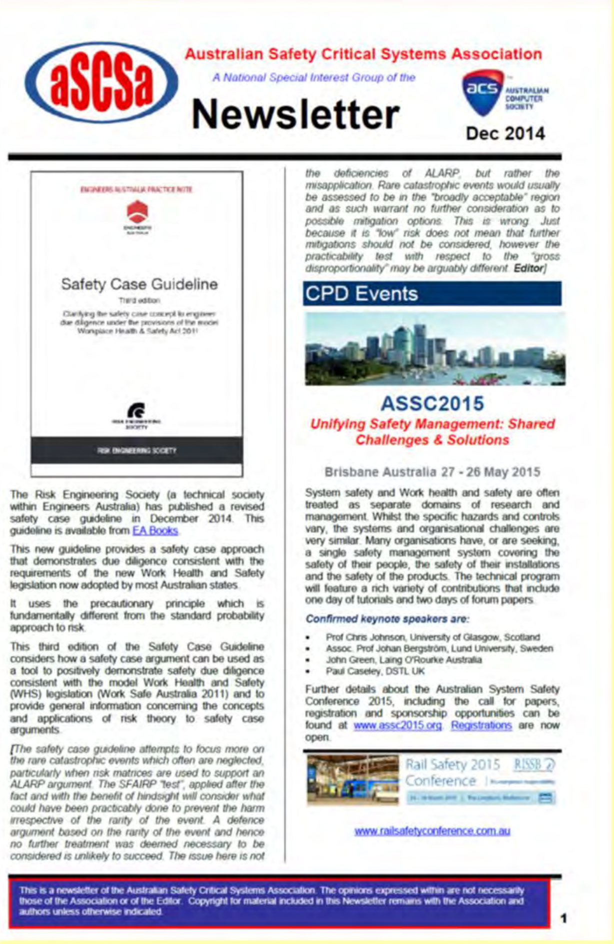
When? 11.30am Wednesday September 03, 2014

Where? Software Improvements, National Press Club Building, Unit 20, 16 National Circuit, Barton ACT 2600.

Members who expect to attend are requested to pre-register via e-mail to George Nikandros.

This is a newsletter of the Australian Safety Critical Systems Association. The opinions expressed within are not necessarily those of the Association or of the Editor. Copyright for material included in this Newsletter remains with the Association and authors unless otherwise indicated.

1



aSCSa **Australian Safety Critical Systems Association**
A National Special Interest Group of the acs AUSTRALIAN COMPUTER SOCIETY

Newsletter **Dec 2014**

ENGINEERS AUSTRALIA PRACTICE NOTE

Safety Case Guideline

Third edition

Clarifying the safety case concept to engineer due diligence under the provisions of the model Workplace Health & Safety Act 2011

RISK ENGINEERING SOCIETY

The Risk Engineering Society (a technical society within Engineers Australia) has published a revised safety case guideline in December 2014. This guideline is available from EA Books.

This new guideline provides a safety case approach that demonstrates due diligence consistent with the requirements of the new Work Health and Safety legislation now adopted by most Australian states.

It uses the precautionary principle which is fundamentally different from the standard probability approach to risk.

This third edition of the Safety Case Guideline considers how a safety case argument can be used as a tool to positively demonstrate safety due diligence consistent with the model Work Health and Safety (WHS) legislation (Work Safe Australia 2011) and to provide general information concerning the concepts and applications of risk theory to safety case arguments.

[The safety case guideline attempts to focus more on the rare catastrophic events which often are neglected, particularly when risk matrices are used to support an ALARP argument. The SFAIRP "test", applied after the fact and with the benefit of hindsight will consider what could have been practicably done to prevent the harm irrespective of the rarity of the event. A defence argument based on the rarity of the event and hence no further treatment was deemed necessary to be considered is unlikely to succeed. The issue here is not the deficiencies of ALARP, but rather the misapplication. Rare catastrophic events would usually be assessed to be in the "broadly acceptable" region and as such warrant no further consideration as to possible mitigation options. This is wrong. Just because it is "low" risk does not mean that further mitigations should not be considered, however the practicability test with respect to the "gross disproportionality" may be arguably different. ***Editor****]*

CPD Events

ASSC2015

Unifying Safety Management: Shared Challenges & Solutions

Brisbane Australia 27 - 26 May 2015

System safety and Work health and safety are often treated as separate domains of research and management. Whilst the specific hazards and controls vary, the systems and organisational challenges are very similar. Many organisations have, or are seeking, a single safety management system covering the safety of their people, the safety of their installations and the safety of the products. The technical program will feature a rich variety of contributions that include one day of tutorials and two days of forum papers.

Confirmed keynote speakers are:

- Prof Chris Johnson, University of Glasgow, Scotland
- Assoc. Prof Johan Bergström, Lund University, Sweden
- John Green, Laing O'Rourke Australia
- Paul Caseley, DSTL UK

Further details about the Australian System Safety Conference 2015, including the call for papers, registration and sponsorship opportunities can be found at www.assc2015.org. Registrations are now open.

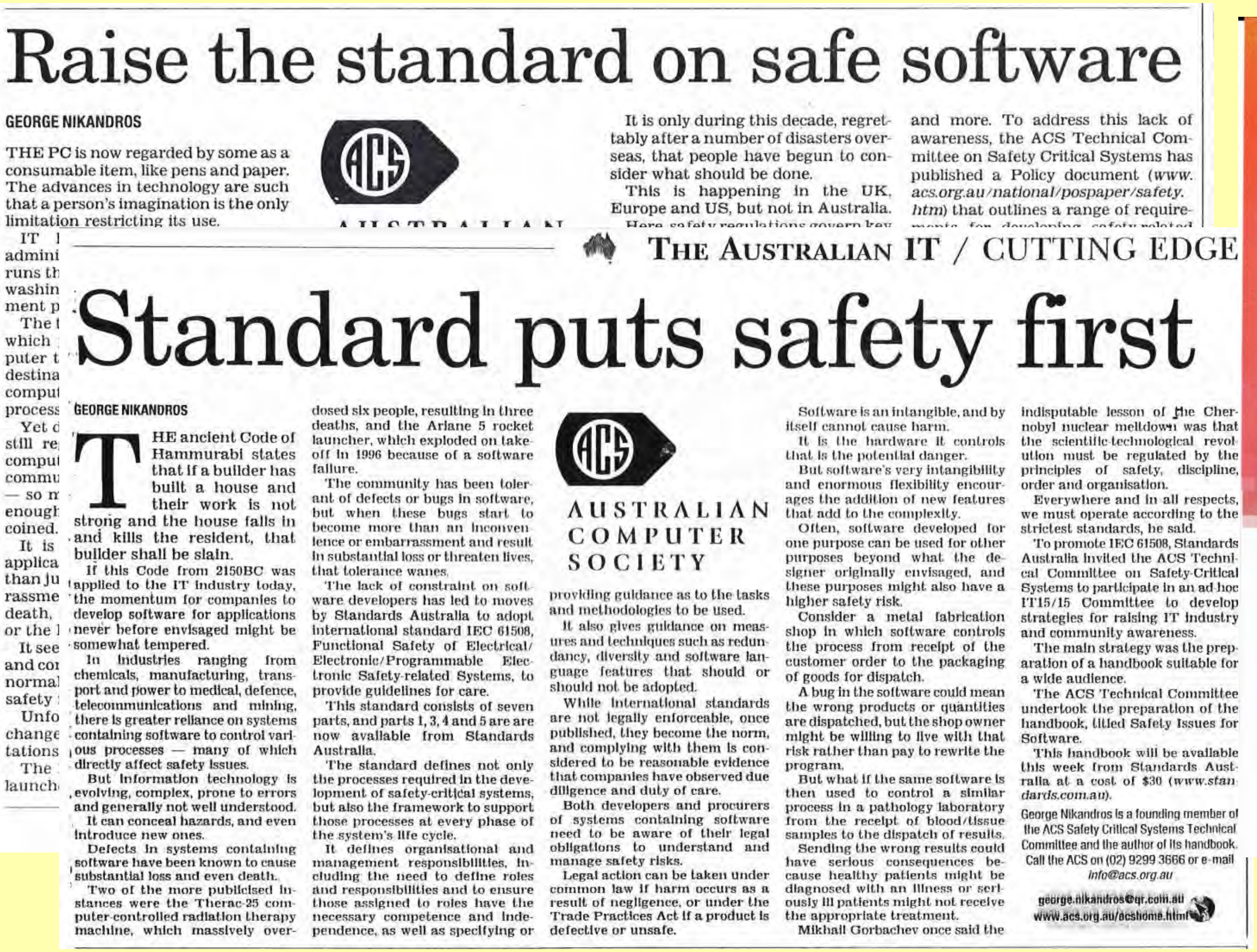
Rail Safety 2015 Conference RISSB

www.railsafetyconference.com.au

This is a newsletter of the Australian Safety Critical Systems Association. The opinions expressed within are not necessarily those of the Association or of the Editor. Copyright for material included in this Newsletter remains with the Association and authors unless otherwise indicated.

1

Increasing awareness through articles



Raise the standard on safe software

GEORGE NIKANDROS

AUSTRALIAN

THE PC is now regarded by some as a consumable item, like pens and paper. The advances in technology are such that a person's imagination is the only limitation restricting its use.

IT l
admini
runs th
washin
ment p
The t
which
puter t
destina
comput
process
Yet d
still re
comput
commu
— so m
enough
coined.
It is
applica
than ju
rassme
death,
or the l
It see
and co
normal
safety
Unfo
change
tations
The
launch

It is only during this decade, regrettably after a number of disasters overseas, that people have begun to consider what should be done.

This is happening in the UK, Europe and US, but not in Australia.

Here safety regulations govern key

and more. To address this lack of awareness, the ACS Technical Committee on Safety Critical Systems has published a Policy document (*www.acs.org.au/national/pospaper/safety.htm*) that outlines a range of requirements for developing safety-related

THE AUSTRALIAN IT / CUTTING EDGE

Standard puts safety first

GEORGE NIKANDROS

THE ancient Code of Hammurabi states that if a builder has built a house and their work is not strong and the house falls in and kills the resident, that builder shall be slain.

If this Code from 2150BC was applied to the IT industry today, the momentum for companies to develop software for applications never before envisaged might be somewhat tempered.

In industries ranging from chemicals, manufacturing, transport and power to medical, defence, telecommunications and mining, there is greater reliance on systems containing software to control various processes — many of which directly affect safety issues.

But information technology is evolving, complex, prone to errors and generally not well understood.

It can conceal hazards, and even introduce new ones.

Defects in systems containing software have been known to cause substantial loss and even death.

Two of the more publicised instances were the Therac-25 computer-controlled radiation therapy machine, which massively overdosed six people, resulting in three deaths, and the Ariane 5 rocket launcher, which exploded on takeoff in 1996 because of a software failure.

The community has been tolerant of defects or bugs in software, but when these bugs start to become more than an inconvenience or embarrassment and result in substantial loss or threaten lives, that tolerance wanes.

The lack of constraint on software developers has led to moves by Standards Australia to adopt international standard IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, to provide guidelines for care.

This standard consists of seven parts, and parts 1, 3, 4 and 5 are are now available from Standards Australia.

The standard defines not only the processes required in the development of safety-critical systems, but also the framework to support those processes at every phase of the system's life cycle.

It defines organisational and management responsibilities, including the need to define roles and responsibilities and to ensure those assigned to roles have the necessary competence and independence, as well as specifying or providing guidance as to the tasks and methodologies to be used.

AUSTRALIAN COMPUTER SOCIETY

It also gives guidance on measures and techniques such as redundancy, diversity and software language features that should or should not be adopted.

While international standards are not legally enforceable, once published, they become the norm, and complying with them is considered to be reasonable evidence that companies have observed due diligence and duty of care.

Both developers and procurers of systems containing software need to be aware of their legal obligations to understand and manage safety risks.

Legal action can be taken under common law if harm occurs as a result of negligence, or under the Trade Practices Act if a product is defective or unsafe.

Software is an intangible, and by itself cannot cause harm.

It is the hardware it controls that is the potential danger.

But software's very intangibility and enormous flexibility encourages the addition of new features that add to the complexity.

Often, software developed for one purpose can be used for other purposes beyond what the designer originally envisaged, and these purposes might also have a higher safety risk.

Consider a metal fabrication shop in which software controls the process from receipt of the customer order to the packaging of goods for dispatch.

A bug in the software could mean the wrong products or quantities are dispatched, but the shop owner might be willing to live with that risk rather than pay to rewrite the program.

But what if the same software is then used to control a similar process in a pathology laboratory from the receipt of blood/tissue samples to the dispatch of results.

Sending the wrong results could have serious consequences because healthy patients might be diagnosed with an illness or seriously ill patients might not receive the appropriate treatment.

Mikhail Gorbachev once said the indisputable lesson of the Chernobyl nuclear meltdown was that the scientific-technological revolution must be regulated by the principles of safety, discipline, order and organisation.

Everywhere and in all respects, we must operate according to the strictest standards, he said.

To promote IEC 61508, Standards Australia invited the ACS Technical Committee on Safety-Critical Systems to participate in an ad-hoc IT15/15 Committee to develop strategies for raising IT industry and community awareness.

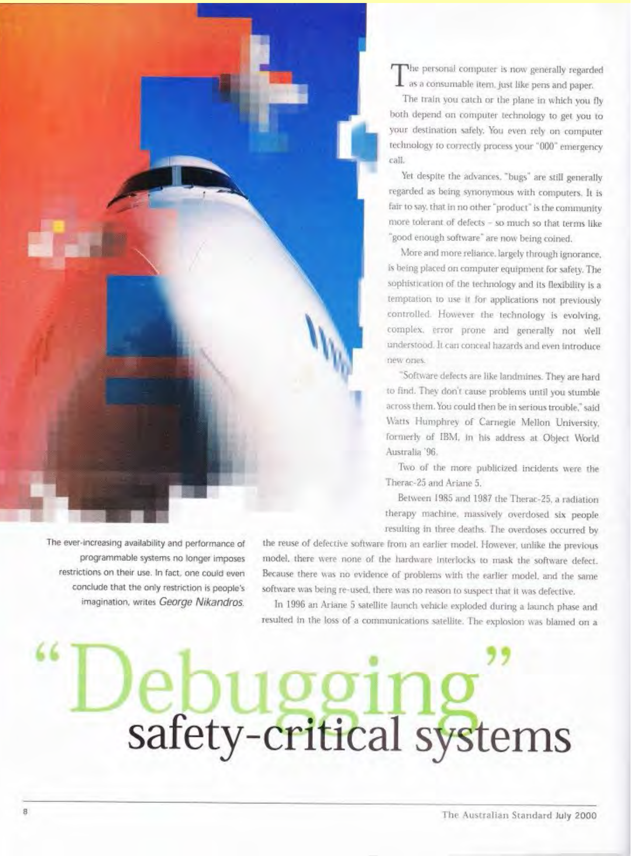
The main strategy was the preparation of a handbook suitable for a wide audience.

The ACS Technical Committee undertook the preparation of the handbook, titled Safety Issues for Software.

This handbook will be available this week from Standards Australia at a cost of $30 (*www.standards.com.au*).

George Nikandros is a founding member of the ACS Safety Critical Systems Technical Committee and the author of its handbook. Call the ACS on (02) 9299 3666 or e-mail *info@acs.org.au*

george.nikandros@qr.com.au
www.acs.org.au/acshome.html



The ever-increasing availability and performance of programmable systems no longer imposes restrictions on their use. In fact, one could even conclude that the only restriction is people's imagination, writes *George Nikandros*.

“Debugging” safety-critical systems

The personal computer is now generally regarded as a consumable item, just like pens and paper.

The train you catch or the plane in which you fly both depend on computer technology to get you to your destination safely. You even rely on computer technology to correctly process your "000" emergency call.

Yet despite the advances, "bugs" are still generally regarded as being synonymous with computers. It is fair to say, that in no other "product" is the community more tolerant of defects – so much so that terms like "good enough software" are now being coined.

More and more reliance, largely through ignorance, is being placed on computer equipment for safety. The sophistication of the technology and its flexibility is a temptation to use it for applications not previously controlled. However the technology is evolving, complex, error prone and generally not well understood. It can conceal hazards and even introduce new ones.

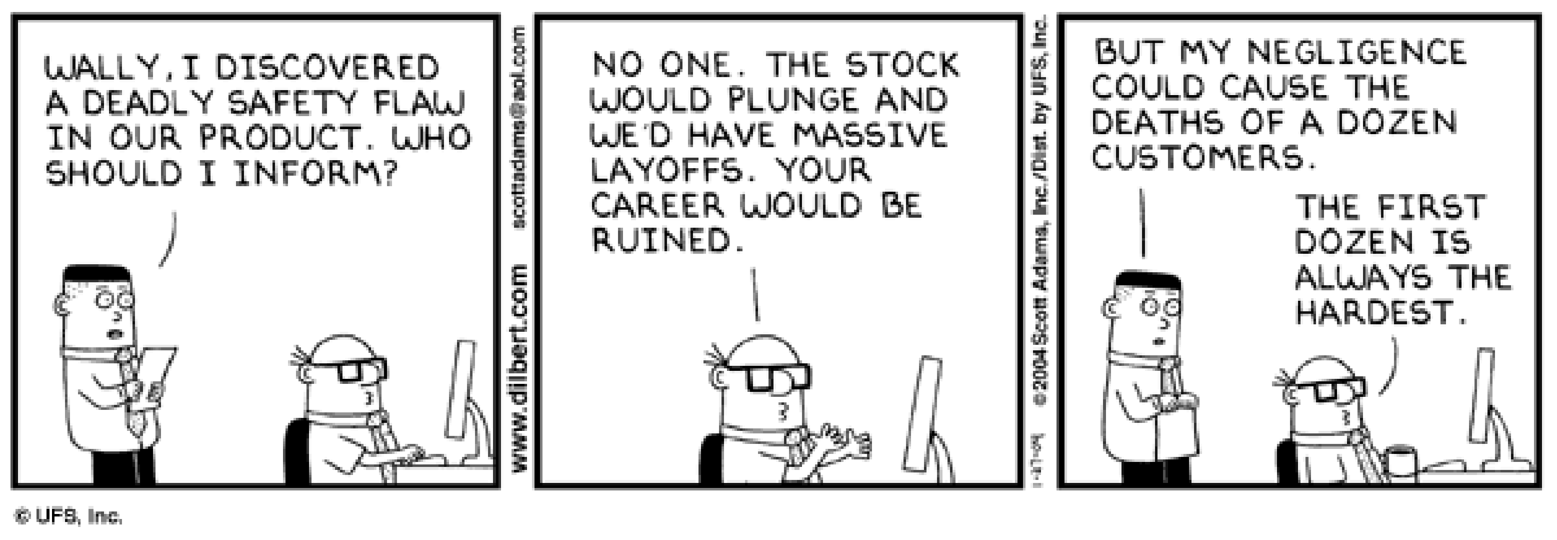
"Software defects are like landmines. They are hard to find. They don't cause problems until you stumble across them. You could then be in serious trouble," said Watts Humphrey of Carnegie Mellon University, formerly of IBM, in his address at Object World Australia '96.

Two of the more publicized incidents were the Therac-25 and Ariane 5.

Between 1985 and 1987 the Therac-25, a radiation therapy machine, massively overdosed six people resulting in three deaths. The overdoses occurred by the reuse of defective software from an earlier model. However, unlike the previous model, there were none of the hardware interlocks to mask the software defect. Because there was no evidence of problems with the earlier model, and the same software was being re-used, there was no reason to suspect that it was defective.

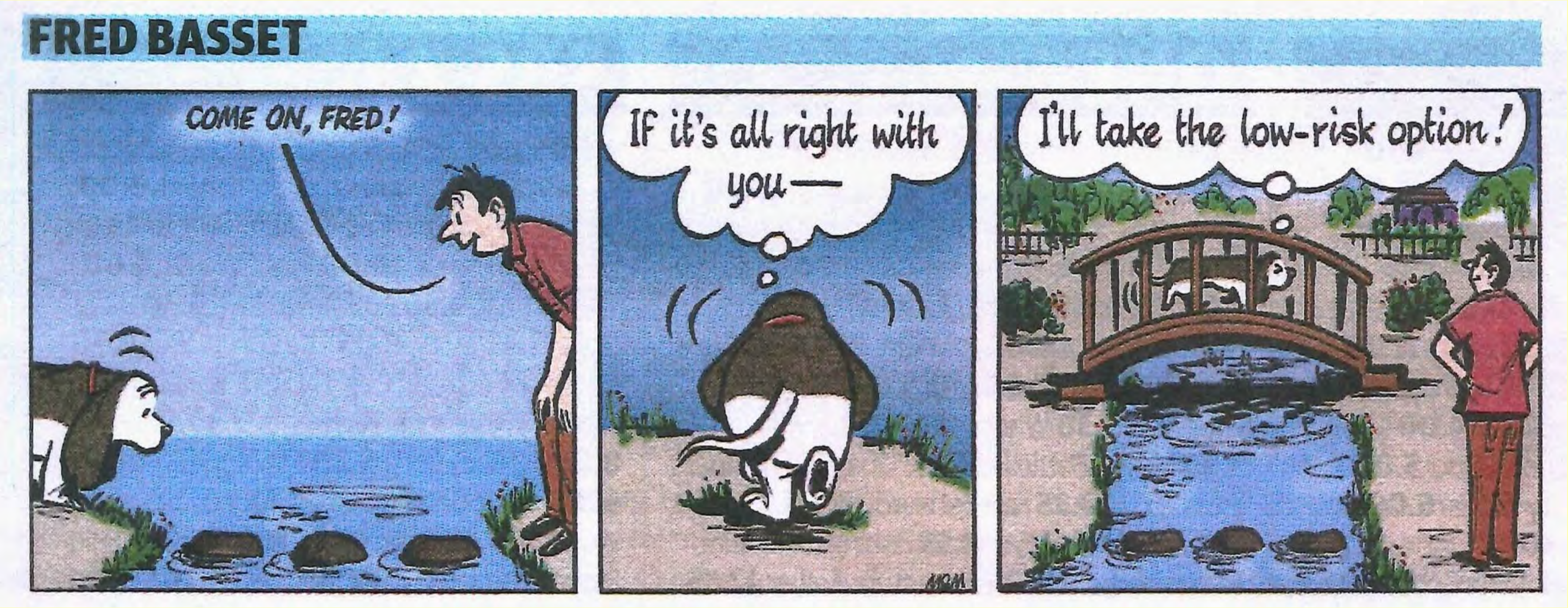
In 1996 an Ariane 5 satellite launch vehicle exploded during a launch phase and resulted in the loss of a communications satellite. The explosion was blamed on a

8 The Australian Standard July 2000


WALLY, I DISCOVERED A DEADLY SAFETY FLAW IN OUR PRODUCT. WHO SHOULD I INFORM?
NO ONE. THE STOCK WOULD PLUNGE AND WE'D HAVE MASSIVE LAYOFFS. YOUR CAREER WOULD BE RUINED.
BUT MY NEGLIGENCE COULD CAUSE THE DEATHS OF A DOZEN CUSTOMERS.
THE FIRST DOZEN IS ALWAYS THE HARDEST.
scottadams@aol.com
www.dilbert.com
© 2004 Scott Adams, Inc./Dist. by UFS, Inc.
© UFS, Inc.

DILBERT – SCOTT ADAMS

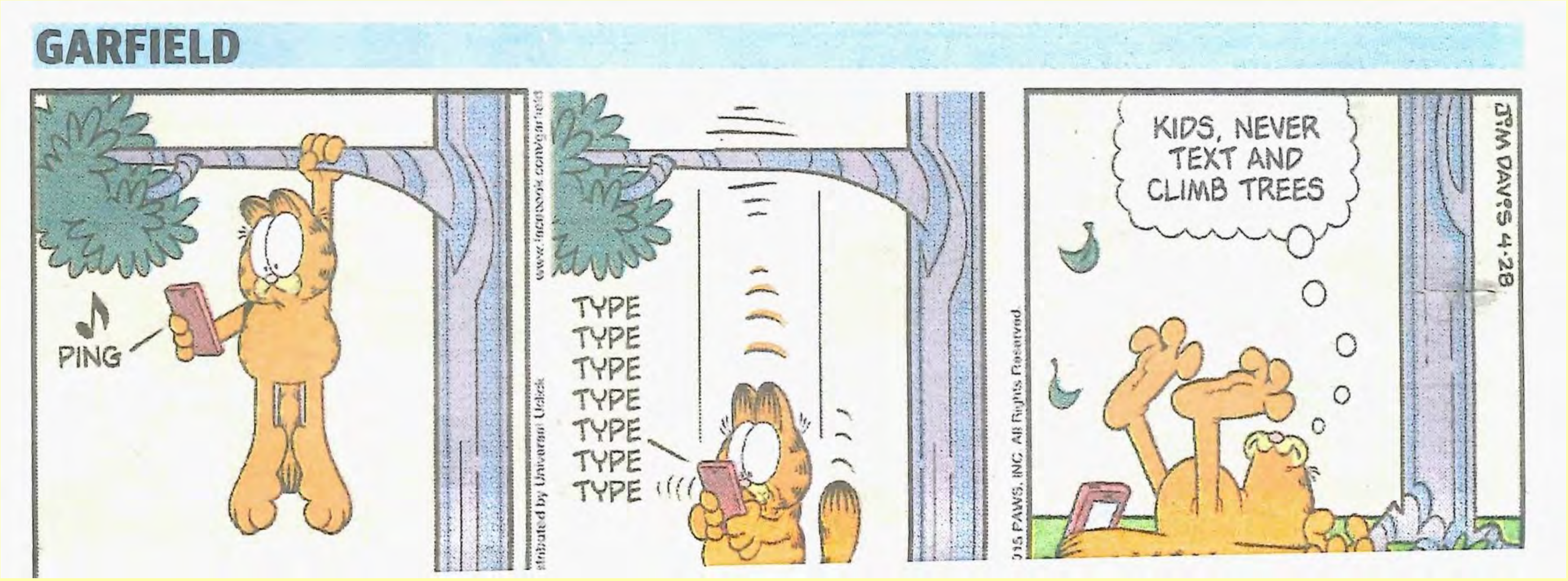
The precautionary principle according to Fred

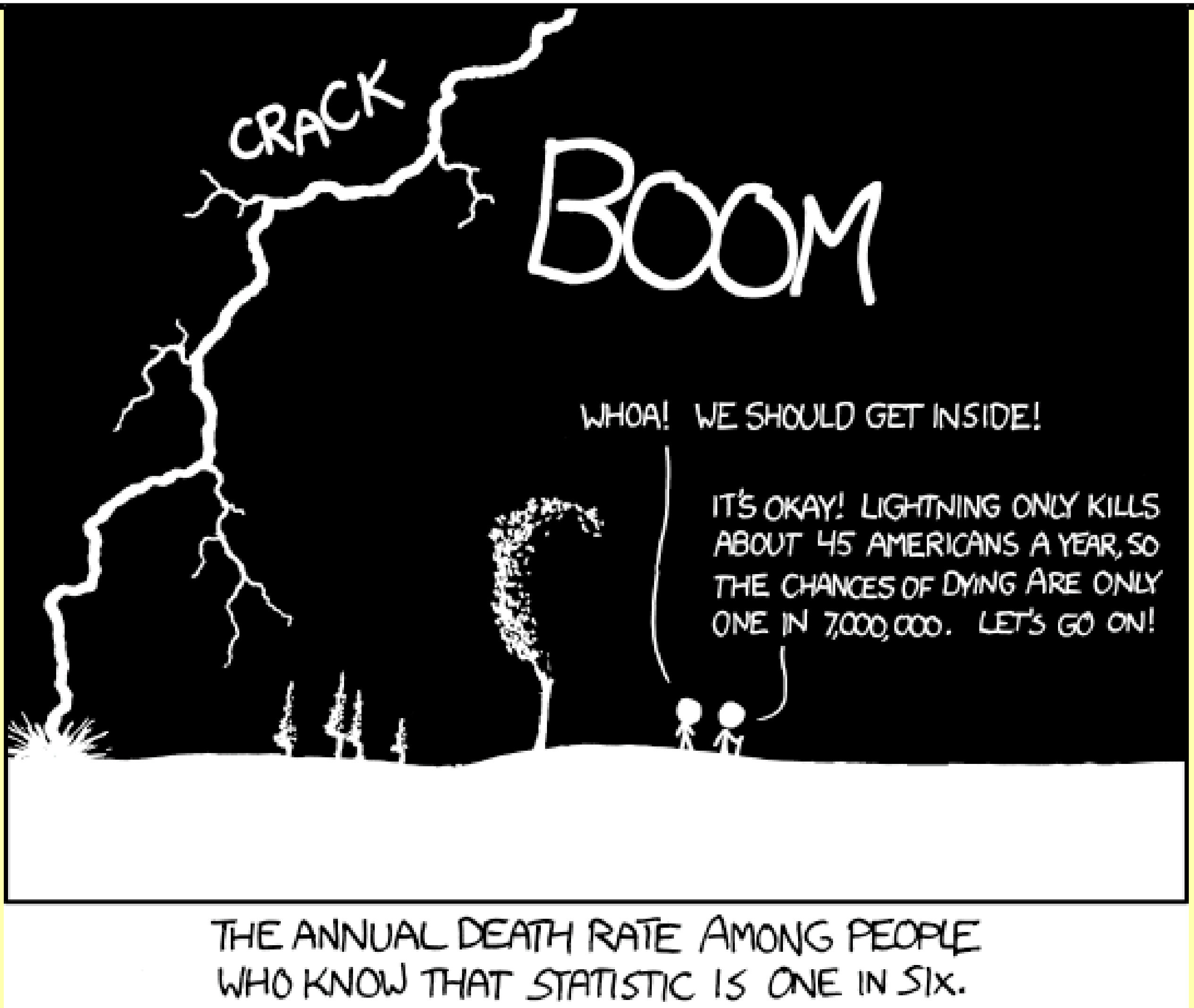


What can possibly go wrong?

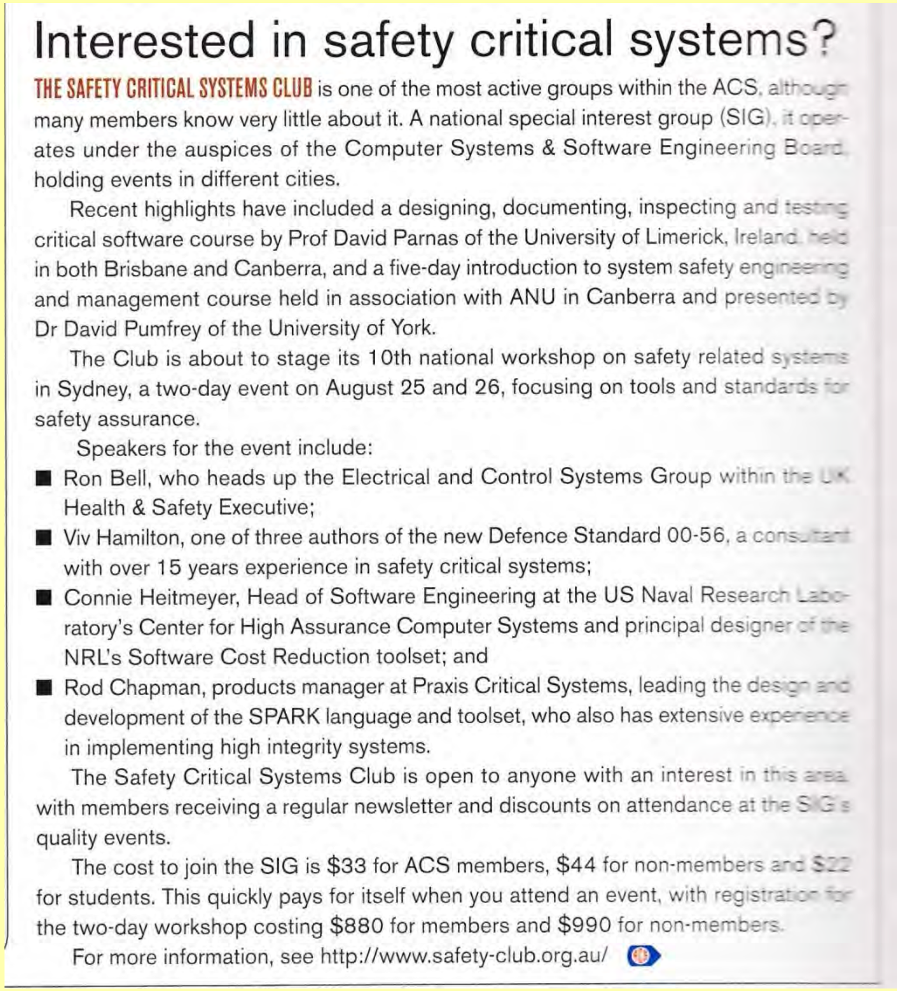
SWAMP
THEORY EXAM
Q3. To maintain flight, what law must be continually overcome?
www.swamp.com.au
?
Clark © 2012 - 9729
MURPHY'S LAW.!!

A safety share


GARFIELD
PING
TYPE
TYPE
TYPE
TYPE
TYPE
TYPE
TYPE
KIDS, NEVER TEXT AND CLIMB TREES
JIM DAVIS 4-28
www.gocomics.com/garfield
Syndicated by Universal Uclick
015 PAWS, INC. All Rights Reserved


CRACK
BOOM
WHOA! WE SHOULD GET INSIDE!
IT'S OKAY! LIGHTNING ONLY KILLS ABOUT 45 AMERICANS A YEAR, SO THE CHANCES OF DYING ARE ONLY ONE IN 7,000,000. LET'S GO ON!
THE ANNUAL DEATH RATE AMONG PEOPLE WHO KNOW THAT STATISTIC IS ONE IN SIX.

The last time in Sydney – August 2005



Interested in safety critical systems?

THE SAFETY CRITICAL SYSTEMS CLUB is one of the most active groups within the ACS, although many members know very little about it. A national special interest group (SIG), it operates under the auspices of the Computer Systems & Software Engineering Board, holding events in different cities.

Recent highlights have included a designing, documenting, inspecting and testing critical software course by Prof David Parnas of the University of Limerick, Ireland, held in both Brisbane and Canberra, and a five-day introduction to system safety engineering and management course held in association with ANU in Canberra and presented by Dr David Pumfrey of the University of York.

The Club is about to stage its 10th national workshop on safety related systems in Sydney, a two-day event on August 25 and 26, focusing on tools and standards for safety assurance.

Speakers for the event include:

- Ron Bell, who heads up the Electrical and Control Systems Group within the UK Health & Safety Executive;
- Viv Hamilton, one of three authors of the new Defence Standard 00-56, a consultant with over 15 years experience in safety critical systems;
- Connie Heitmeyer, Head of Software Engineering at the US Naval Research Laboratory's Center for High Assurance Computer Systems and principal designer of the NRL's Software Cost Reduction toolset; and
- Rod Chapman, products manager at Praxis Critical Systems, leading the design and development of the SPARK language and toolset, who also has extensive experience in implementing high integrity systems.

The Safety Critical Systems Club is open to anyone with an interest in this area, with members receiving a regular newsletter and discounts on attendance at the SIG's quality events.

The cost to join the SIG is $33 for ACS members, $44 for non-members and $22 for students. This quickly pays for itself when you attend an event, with registration for the two-day workshop costing $880 for members and $990 for non-members.

For more information, see http://www.safety-club.org.au/

Information Age

August/ September 2005

We thank our 2017 sponsors

RGB ASSURANCE

Australian Government

Department of Defence

Nova Systems

Experience Knowledge Independence

www.NovaSystems.com

acs AUSTRALIAN COMPUTER SOCIETY

SYSTRA

SCOTTLISTER