Australian Safety Critical Systems Association

A National Special Interest Group of the

AUSTRALIAN COMPUTER SOCIETY

Newsletter

Dec 2007

From the Chair

Since the last newsletter the aSCSa Committee has been very much preoccupied hosting the 2007 Conference and the two associated workshops, and identifying new activities for 2008 and beyond.

The 2007 human factors themed conference held in August in Adelaide was a success. The attendance of 41 was typical of recent years. The late cancellation of Nancy Leveson due to medical reasons caused some panic for the committee. Nancy was to also deliver a course on the STAMP analysis technique. However the committee is most grateful to Felix Redmill for stepping in being both a conference presenter and delivering a half-day course at very short notice.

Ironically, I had only in May 2007 met up with Felix in London and had invited him to the 2008 Conference. On returning home, Felix e-mailed the aSCSa committee:

> *"Congratulations on a very good conference. Every paper was interesting (to me), and that's unusual."*

In March 2007, there was air accident at Yogyakarta, Indonesia. The report of that accident was published in October 2007. This accident was entirely due to human factors. An article is included in this newsletter.

Seasons greetings to all and I wish everyone a healthy and safe 2008.

George Nikandros
National Chairman

Association Matters

Annual General Meeting

The 2007/08 Annual General Meeting was held on Thursday, 30 August 2006 in conjunction with the 2007 Conference at the Stamford Grand Hotel, Adelaide.

The meeting was attended by 20 members and unanimously accepted the proposed amendment to the tenure of the position of chairman. The 5 year continuous limit was removed.

Continues Page 2

Association Matters (cont.)

At the meeting there were two nominations received for the committee vacancies created by the retirement of Peter Hartfield and Alex Moffatt. The meeting accepted the nominations of Tariq Mahmood and BJ Martin.

At the meeting the continuing 2006/07 committee was re-elected.

The next AGM will be held in Canberra on 28 August 2008 in conjunction with the 13th Australian Conference on Safety-Related Systems.

Constitution

The aSCSa Constitution has been updated to include the accepted mission statement.

National Committee

George Nikandros	Chairman (QLD)
Kevin Anderson	Secretary (VIC)
Chris Edwards	Treasurer (ACT)
Tony Cant	Conference Program Chair (SA)
Clive Boughton	Certification & Canberra Chapter Chairman (ACT)
Robert Worthington	(VIC)
BJ Martin	(ACT)
Allan Coxson	(VIC)
Tariq Mahmood	(VIC)
David Goedecke	(VIC)
Web Site	www.safety-club.org.au

The term of the current committee expires 30 June 2008. As per the constitution the 2008/09 chairman will be elected by the outgoing committee and all other committee positions are declared vacant.

Membership

Membership renewal notices for 2007/08 were issued in July 2007.

Of the 118 members to date, 66 are financial. A reminder notice will be issued.

Continues Page 3

2008 Conference

Once again the aSCSa will be hosting a conference event along the same lines of recent conferences.

The 2008 (13th) conference - to be held 29 -30 August 2008, in Canberra – will have a regulation theme. Like recent conference events, the two day programme will include invited internationally-renowned speakers. A post conference course is also being planned.

Following on its success in Sydney (2005), Melbourne (2006), and Adelaide (2007), the programme will include a dinner function on the Thursday evening. The dinner event rates extremely well in the feedback from delegates.

See advert this page.

13th Australian Workshop

21 – 22 August 2008

CANBERRA ACT

Regulating for Safety – Is it Enough?

CALL FOR PAPERS

The Australian Safety Critical Systems Association (aSCSa) announces its 13th National Conference on Safety Related Systems. The theme will be the role of regulation in the development and deployment of safety-related software intensive systems.

Apart from specific hazardous industries where some level of regulation exists, the only direct governance for the development and deployment of safety-related software intensive systems is occupational health and safety legislation which is often applied after the fact. Tort (Common) Law could also be considered as an after-the-fact control.

As with recent conferences there will be a number of international keynote speakers.

Important Dates

- Abstract: 14th March 2008 (text, rtf, MS-Word, pdf)
- Submission: 2nd May 2008 (rtf, MS-Word, pdf)
- Notification of acceptance: 6th June 2008
- Camera-ready copy: 28th July 2008 (pdf only)

For paper format details see www.crpit.com.

Questions? More Information?

Dr Tony Cant (Program Chair)
Trusted Computer Systems Group
Information Networks Division
Defence Science and Technology Organisation
PO Box 1500, Edinburgh SA 5111 Australia
Phone: +61 8 8259 6700, Fax: +61 8 8259 5589
Mobile: (0412) 348 367,
Email: Tony.Cant@dsto.defence.gov.au

(Conference Chair)

Contents

Wishing to advertise a course or event?

Then place your advert here for $110.00 (incl. GST)

Contact aSCSa Secretary
kevin.anderson @
hyderconsulting.com

Association Matters (continued)

Website

The website will be undergoing a change in the near future. The focus of the change is to have more resources available from the main page via menus.

Research Award

One of the objectives of the aSCSa is to provide prizes and funds for the purpose of promoting education, research and excellence in relating to safety and/or mission critical software-intensive systems.

In 2007, the aSCSa launched a Research Award for all Australia citizens undertaking research at an Australian University as a student.

The rules governing the award and the application form are available from the aSCSa website[1].

Sponsorships

The aSCSa being a non profit organisation welcomes sponsorships to support and expand the activities and events of the organisation. Current sponsorship opportunities are the annual August conference and the Research Award. Details are provided on the aSCSa website[2].

The aSCSa is receptive to sponsorship proposals.

Event Report – 2007 Conference

The 2007 Australian Conference on Safety Critical Systems was held in Adelaide on 30 -31 August 2007 at the Stamford Grand Hotel. This was the 12th such conference.

The two-day conference had a human factors theme. The programme included four invited international renowned speakers:

- ***John Knight*** – Dr Knight is a Professor at the Computer Science, University of Virginia, USA
- ***Chris Johnson*** – Dr Johnson is a Professor of Computer Science, University of Glasgow, UK.
- ***Carl Sandom*** – Dr Sandom is a Consultant, iSys Integrity, Dorset, UK
- ***Felix Redmill*** – Prof Redmill is Coordinator of the Safety-Critical Systems Club, UK and Visiting Professor and the University of Lancaster, UK.

Attendance at the conference was a typical 41.

The program included a panel session comprising of the invited international speakers. The topic of human factors certainly generated much discussion.

Figure 1: Panel Session. Panellists seated from left: Chris Johnson, John Knight, Felix Redmill, Carl Sandom; standing, Program Chair Tony Cant.

There is lot of effort required to put together such a quality event. For this we thank the Program Chair, Tony Cant.

The conference again included a dinner event which was rated very high, in fact the highest rating possible, and contributed to the high rating of the networking benefit of the conference.

The event's success would not have been possible without the generosity of the event sponsors. This year there were five sponsors.

[1] http://www.safety-club.org.au/research_award.html

[2] http://www.safety-club.org.au/downloads/sponsorships_V0p2.doc

CEDISC (Centre of Excellence in Defence and Industry Systems Capability is sponsored by the Government of South Australia and the University of South Australia).

In order to improve the workshop, survey forms were issued to all attendees. The committee received 18 responses. The feedback is summarised in Figures 2 and 3.

The results show that the event well met the expectations of the attendees.

Figure 2: Delegate Feedback re conference value [Rating range is from 1 (poor) to 5 (excellent)]

The feedback in relation to the registration fee was the best result to date, despite a modest rise on recent conference fees. This year the registration fee included discounts for two associated courses and it may be that overall more of the delegates considered the package to be good value.

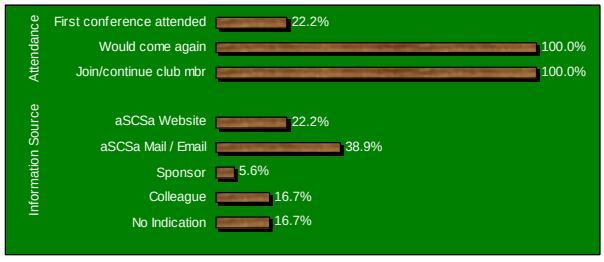


Figure 3: Delegate Feedback re the aSCSa

From the feedback, direct mail/email is the most effective means of communication. However this is the first time that the website has rated second.

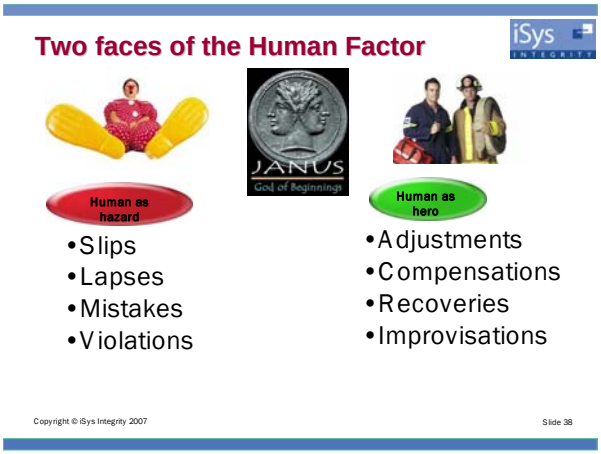
The papers for the conference will be made available through the ACS Conferences in Research and Practice in Information Technology website (http://crpit.com/) as Volume 86.

Hard copies will be distributed to conference attendees and financial members who did not attend.

The presentations for which we have obtained permission will also be made available via the aSCSa website.

Event Report – Tutorial Human Factors

A two-hour tutorial titled *An Introduction to Human Factors and System Safety* was presented by Carl Sandom. The course was aimed at providing engineers and project managers in a range of sectors (e.g. Defence, Aerospace, Rail etc.) with an appreciation of the human factors and ergonomics issues relating to safe systems development. The tutorial provided an overview of some of the main human factors tools and techniques required for designing safer systems. Carl introduced the concept:



Human as hazard, human as hero!

The tutorial preceded the 2007 aSCSa Conference. This tutorial was included at no additional cost to the conference delegates. There were 15 delegates and the feedback from 13 of the delegates is summarised in Figures 4 and 5:

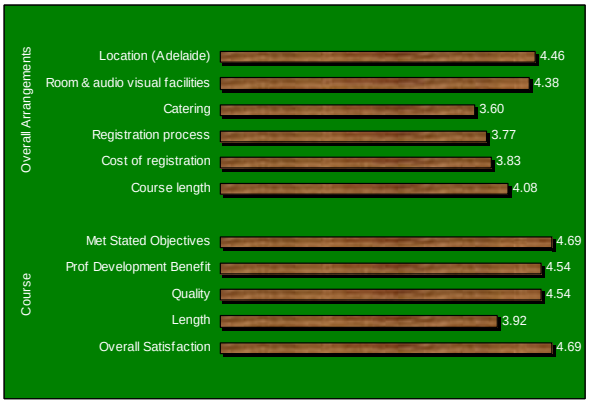


Figure 4: Delegate Feedback re tutorial value [Rating range is from 1 (poor) to 5 (excellent)]

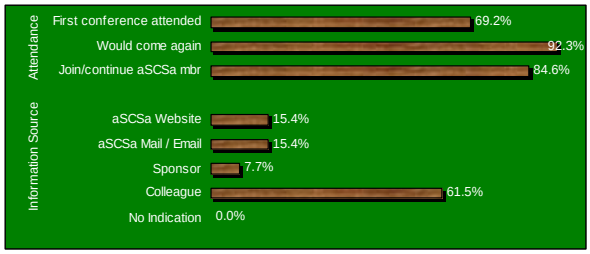


Figure 5: Delegate Feedback re the aSCSa

Carl agreed to make his tutorial available.

SAFECOMP 2008

The 27th International Conference on

Computer Safety,

Reliability and Security

22 – 25 September 2008

Newcastle-upon-Tyne, United Kingdom

http://www.safecomp2008.org

Event Report – Course Subjectivity in Risk Analysis

A four-hour course titled *the subjectivity that we bring to risk analysis and who we can neutralise it* was presented by Felix Redmill. The course objectives were:

- To define and examine the processes involved in risk analysis and management;
- To appreciate the ways in which human subjectivity (including our own) influences these processes;
- To become acquainted with the principal biases that psychologists have identified as influencing human judgment.

Where we look for hazards, and what we identify as hazards, depend on our "knowledge", beliefs and assumptions:

- It won't rain because it's summer.
- He can't make a mistake because he's done this a thousand times.
- It can't fail because it's new.
- It's good because I made it (wrote it, checked it).

Felix traced through the risk assessment and management processes and gave examples which clearly demonstrated how personal biases can influence the outcomes. It was a very enlightening course.

The course preceded the 2007 aSCSa Conference. Conference delegates were offered a substantial discount. There were 17 delegates and the feedback from 10 of the delegates is summarised in Figures 6 and 7:

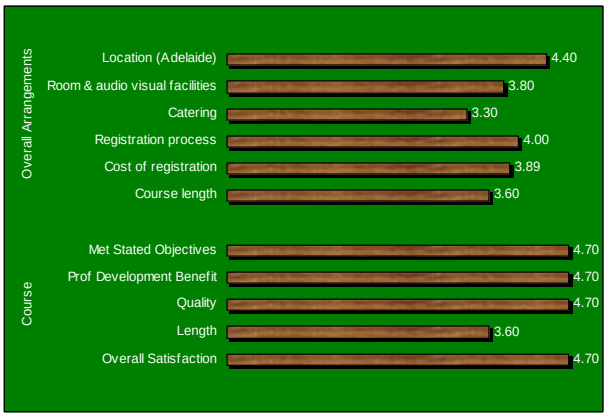


Figure 6: Delegate Feedback re course value [Rating range is from 1 (poor) to 5 (excellent)]

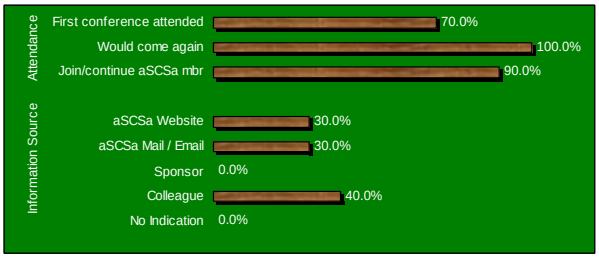


Figure 7: Delegate Feedback re the aSCSa

Accident Report
Garuda Indonesia – 07-Mar-07

On 07 March 2007, a Boeing 737-497 aircraft was being operated by Garuda Indonesia on a scheduled passenger service to Yogyakarta. There were two pilots, five flight attendants, and 113 passengers on-board. The aircraft overran the departure end of the runway, crossed a road, and impacted an embankment before stopping in a rice paddy field 252 metres from end of the runway. The aircraft was destroyed by the impact forces and an intense fuel-fed fire, post impact fire. There were 119 survivors; one flight attendant and 20 passengers were fatally injured; one flight attendant and 11 passengers were seriously injured.

According to the official report[3] "*the flight crew's compliance with procedures was not at a level to ensure safe operation of the aircraft*".

At 10.1 miles from the runway, the aircraft was 1427 feet above the 2500 feet published in the approach chart. The pilot descended the aircraft steeply in an attempt to reach the runway. In so doing the airspeed increased excessively. As the aircraft approached the runway, there were 15 warnings issued by the Ground Proximity Warning System. Despite requests from the co-pilot to go around, the pilot persisted with the

[3] Report available via Australian Transport Safety Bureau – www.atsb.gov.au/publications/investigation_reports/2007/AAIR/aair2007015.aspx

approach. The steep angle of approach and excessive speed resulted in an unstable approach.

The investigators finding was that the pilot's attention was fixated on landing the aircraft on the runway and he either did not hear, or disregarded the Ground Proximity Warning System alerts and calls from the co-pilot to go around.

Why didn't the co-pilot take control as required by the company procedures when such situations arise? The answer according to the investigators relates to the fact that the co-pilot's proficiency records contained no evidence of training or proficiency checks in the vital actions and responses to be taken in the event of Ground Proximity Warning System alerts, such as "TOO LOW TERRAIN" and "WHOOP, WHOOP, WHOOP PULL UP".

The lack of training evidence is difficult to accept as being the reason for the co-pilot's inaction to such urgent warnings. One would have expected that the basic survival instinct would have spurred the co-pilot to act. The difference in seniority level between the pilot and the co-pilot may be a possible factor in the co-pilot not usurping control. There is however no comment in the report of this possibility.

One clear finding of the investigation is that having robust and well documented procedures do not ensure that they are observed. The absence of any surveillance by the airline company and the air transport regulator was considered a key factor in not identifying breaches.

The accident is certainly a most interesting event in relation to human factors.

Computer Crash
International Space Station

The BBC reported[4] 0n 14 June 2007 that according to NASA officials the Russian computers controlling the International Space Station's (ISS) orientation and supply of oxygen and water failed.

According to an article[5] in IEEE Spectrum by James Oberg, a 22-year veteran of NASA mission control, and no a writer and consultant in Huston, because the critical computer systems were designed, built and operated incorrectly.

Russia defended the integrity of their computer systems and tried to the blame external factors i.e. essentially blaming NASA for the failure.

The initial assumption was that some external interference, such as noise on the power supply, was responsible for generating false commands inside the computer system. On the assumption that the bad commands were coming from inside a power-monitoring device, the crew bypassed it on two of the three downed computers, using jumper cables. By the time the shuttle undocked on 19 June, the computers began to function normally—or so it seemed. Replacement parts were quickly manifested on a robot supply ship, while ground engineers wrestled with the fundamental question of cause and effect.

Analysis teams still had to determine why the computers failed, and why the jumper cables seemed to fix the problem. More important, they needed to know whether the problem really was fixed, or whether something could again trigger the system-wide crash of the supposedly triply redundant architecture.

In the weeks that followed the crisis and apparent recovery, the crew on the space station disassembled the boxes and cabling and inspected every angle of the hardware. Multiple scopes and probes had failed to find the flaw, but their eyes and fingers eventually did. The connection pins from the power-monitoring device they'd bypassed earlier, they found, were wet—and corroded.

Continuity checks found that specific wires, called command lines, in the cable coming out of the device had failed. And one of those lines had short-circuited. Also, in a shocking design flaw, there was a "power off" command leading to all three of the supposedly redundant processing units. The line was designed to protect the main computers, which are downstream of the power monitor, from power glitches too great for normal power filters to protect against. It does so by turning the computers off when it senses trouble. But in a failure unanticipated by its designers, this one command path itself was able to kill all three processing units due to a single corrosion-induced short.

The bypass jumper cables circumvented the false "power off" command by forcing that command line to remain dormant.

Water corrosion was the cause of the failure. The dehumidifier had been malfunctioning, and its frequent on-off cycles led to surges of water vapour. Also, a stream of cold air from another location on the dehumidifier helped drive the cable temperatures occasionally below the dew point.

It was poor design that allowed one spot of corrosion to totally fail a supposedly triply redundant control computer complex.

Bulletin Boards

ACM Risk Forum On Risks To The Public In Computers and Related Systems – http://catless.ncl.ac.uk/Risks.

Safety-Critical Mailing List Forum hosted by the University of York. Need to join using the form located at www.cs.york.ac.uk/hise/text/sclist/form.php for access.

Military RoboGun Incident

On Friday 12 October 2007, a computerized Swiss/German Oerlikon 35mm MK5 anti-aircraft twin-barrelled gun spun in all directions as it sprayed around 500 high-explosive, .5kg 35mm cannon shells killing nine and wounding fifteen South African soldiers. The incident happened during a live fire exercise involving 5,000 South African soldiers. It is believed that the gun

[4] BBC News Item posted 14-Jun-2007 http://news.bbc.co.uk/1/hi/sci/tech/6752459.stm

[5] IEEE Spectrum http://www.spectrum.ieee.org/print/5598

jammed shortly after the exercise began, causing a chain reaction which lead to the gun emptying its magazines.

The anti-aircraft weapon, an Oerlikon GDF-005, is designed to use passive and active radar, as well as laser target designators range finders, to lock on to high-speed, low-flying aircraft, helicopters, unmanned aerial vehicles (UAV) and cruise missiles. In "automatic mode," the weapon feeds targeting data from the fire control unit straight to the pair of 35mm guns, and reloads on its own magazine when emptied.

According to an article published by The Star on 13 October 2007, the accident occurred just before 9am when a battery from 10 Anti-Aircraft Regiment in Kimberley began a live-fire exercise at the Army Combat Training Centre at Lothtlha as part of the South African National Defence Force Exercise Seboka. The deaths and injuries occurred when one gun jammed moments after the exercise began.

During the attempt to clear the blockage, another shell was accidentally fired, causing some of the unspent ammunition in nearly-full magazines to explode. This, in turn, caused a “runaway”. The rogue gun began firing wildly, spraying high-explosive shells at a rate of 550 a minute, swinging around through 360 degrees like a high-pressure hose.

According to a spokesperson of the South African National Defence Force, Brigadier-General Kwena Mangope, Exercise Seboka was aimed at preparing troops for battle.

Brigadier-General Mangope assumed that there was a mechanical problem, which led to the accident. It appeared as though the gun, which is computerised, jammed before there was some sort of explosion and then it opened fire uncontrollably, killing and injuring the soldiers.

Whether the computerised control system was a factor in this incident will not be known until the investigation and inquiries set up to report on this incident release their reports.

What’s In Your Safety Lexicon?

In an article in the July-August 2007 edition of the *Journal of System Safety*, Cliff Ericson and Danny Brunson highlight major anomalies in the definition of common terms used in by the system safety community. Whilst the there is much debate in relation to the meaning of the term hazard, there are many other common terms that have surprisingly different meanings. The following anomaly examples are from the Eriscon and Brunson article.

Accident vs. Mishap

Out of 35 industry references, there were only four definitions of the term accident and six for the term mishap, and only two of the sources were common. Only two of the industry sources contained definitions for the both accident and mishap. Two of the accident definitions indicated that accident and mishap were synonymous, as did two of the mishap definitions. One source stated that accident and mishap were not the same.

Hazard

Out of 35 industry references there were thirteen definitions. May of the definitions contained substantial differences, and some were obvious copies from the MIL-STD-882 definition. Some of the definitions were:

- A condition that is a prerequisite to a mishap
- A condition that is a prerequisite to an accident
- A potential source of harm
- A potential unsafe condition
- An inherent characteristic of a thing or situation that has the potential for causing a mishap
- Any phenomenon having the potential to induce an adverse effect
- The presence of a potential risk situation caused by an unsafe act or condition

Safety-Critical

Out of 35 industry references, there were eleven vastly different definitions. Just what makes something safety-critical? Something is safety-critical when it:

- Results in a hazard
- Results in a mishap
- Results in a serious or catastrophic mishap
- Leads to a loss of life
- Leads to a system failure
- Is essential to the safe system operation
- Is essential to the overall reduction of system risk

Safety-Related

Out of 35 industry references, there was only one definition despite the term being widely used in safety literature. How is it that the safety community uses the term widely, yet fails to properly define it? Is safety-related a valid term? How does it differ from safety-critical?

Fail-Safe

Out of 35 industry references, there were five different definitions. Although the definitions are close in meaning, they are still somewhat vague for someone

trying to implement the concept. Below are five definitions from the different sources:

1. A design feature that ensues that a system remains safe or, in the event of a failure, will cause the system to revert to a state that will not cause a mishap.
2. A design feature that ensures the system remains safe, or in the event of a failure causes the system to revert to a state that will not cause a mishap.
3. A characteristic of a system whereby any malfunction affecting safety will cause the system to revert to a state that is known to be within acceptable risk parameters.
4. Ability to sustain a failure and retain the capability to safely terminate or control the operation. A design feature that ensures that the system remains safe or will cause the system to revert to a state that will not cause a mishap.
5. A characteristic that prevents faults from becoming critical faults. A fail-safe design is one that ensures the system is put into a safe condition if a fault occurs e.g. a fusing system.

Hazard Risk or Mishap Risk

Risk and risk reduction are important elements in the system safety discipline. Unfortunately, many safety analysts refer to both hazard risk an mishap risk. MIL-STD-882C used the concept of hazard risk and Hazard Risk Index [HRI], while MIL-STD-882D switched to mishap risk and Mishap Risk Index [MRI]. Is there any real difference in meaning between hazard risk and mishap risk? Hazard risk really means the potential mishap risk presented by a hazard, while mishap risk means the potential mishap risk that could result from an actuated hazard.

Ericson and Brunson conclude that the present lexicon of system safety is inadequate and out of date and that in order to advance the state of the art and the credibility of the system safety discipline, a formal safety dictionary in which the terms are properly and thoroughly defined is needed.

About the authors

Clif Ericson works for EG&G Technical Services as a system safety project manager and has some 40 years experience in the system and software safety fields. He spent 35 years at Boeing working on projects ranging from missile systems, aircraft and spacecraft to people-mover systems. Whilst at Boeing, he conducted considerable research on software safety and fault tree analysis. He also worked at Applied Ordnance Technology Inc, where he was a safety project manager and wrote a 900-page system safety manual for the US Navy and provided technical support to the US Navy's Software System Safety Technical Review Panel. He is a former president of the System Safety Society (2001-2003).

Danny Brunson is a senior technical specialist employed by EG&G Technical Services after recently retiring from the US Navy after some 40 years service where he was the executive director of the US Navy Ordnance Safety and Security Activity and chairman of the US Navy's Weapon Systems Explosive Safety Review Board. Prior to that, he served as head of the Weapons Systems Department, US Naval Surface Warfare Center Dahlgren Division.