Australian Safety Critical Systems Association

A National Special Interest Group of the

AUSTRALIAN COMPUTER SOCIETY

Newsletter

Dec 2010

Raising the Safety Conference bar

The aSCSa received a proposal from the recently formed Australian Chapter of the System Safety Society to co-host the inaugural Australian System Safety Conference in May 2011. The committee sees this as an excellent opportunity raise the profile of system safety in Australia, by working with an internationally renowned safety organisation.

The conference theme is ***Managing Systems & Software Safety Risks in Emerging Technologies***.

The conference aims to share research, government and industry knowledge and practice in the field of systems and software safety. The theme of this conference focuses on emerging technologies and their impact of managing systems and software risks. The conference is intended to bridge the domains of Defence, aviation, rail, utilities, mining and resources, medical engineering, telecommunications, and information technology. The conference topics are:

- Safety Engineering
- Safety Management
- Software Engineering
- Software Assurance
- Software Safety
- Systems Integration

For further information about this conference, please visit the conference website at www.assc2011.org.

Invited keynote speakers include:

Len Neist - Chief Executive of the NSW Independent Transport Safety Regulator

Dr Jeffrey Joyce - President and co-founder of an engineering consultancy, Critical Systems Labs Inc.

Dr David Ward - General Manager for Functional Safety at MIRA Limited

Dr Carl Sandom - Director and Principal Consultant of iSys Integrity Limited

Human Factors Tutorial

Interested in human factors?

Tasair Piper Chieftain Picture: CHRIS KIDD

At about 11:00am on December 9, 2010, a charter plane skidded terrifyingly down the runway with its propellers bent and its belly loudly scrapping the surface before coming to a halt blocking two of the three runways at King Island Airport. The upset pilot apologised repeatedly to the seven passengers aboard for forgetting to engage the plane's landing gear after the plane slewed off the runway and finally came to a halt.

[***Source:*** The Mercury http://www.themercury.com.au/article/2010/12/09/191851_tasmania-news.html]

Do to the ever increasing interest in the role of the human in the development, operation and maintenance of safety systems, the ASSC 2011 organising committee is negotiating a human factors pre-conference tutorial by an international expert.

Other CPD Events

THE UNIVERSITY of York Department of Computer Science — ANU THE AUSTRALIAN NATIONAL UNIVERSITY

Introduction to System Safety

The aSCSa is again hosting the University of York's Introduction to System Safety at the Australian National University in April 2011. See inside for details.

The aSCSa is again a supporter of annual rail safety conference. For details of the conference please see the conference website:

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.

Contents

From the Chair

<article from Clive>

Clive Boughton
National Chairman

Association Matters

Annual General Meeting

The 2010/11 Annual General Meeting was held on Wednesday, 25 August 2010 at ISSEC 2010 at the Canberra Convention Centre. There were 5 aSCSa members and 2 guests in attendance.

At the meeting it was announced that Clive Boughton was elected chairman at the June 2010 aSCSa Committee meeting. The only nominations for the 2010/11 committee received were those of the outgoing committee members, with the exception of Allan Coxson. The nominations for the 2010/11 committee were accepted.

A motion for the provision of an annual membership certificate for all financial members was accepted.

The date for the next AGM was not set.

Membership

Membership renewal notices for 2011 to be issued in December 2010.

There are currently 128 members, although only 100 have valid contact details, and of those 30 are financial for 2010.

National Committee

Clive Boughton	Chairman (ACT)
Kevin Anderson	Secretary (VIC)
Chris Edwards	Treasurer (ACT)
Tony Cant	Conference Program Chair (SA)
George Nikandros	Immediate Past Chairman (QLD)
Robert Weaver	(ACT)
BJ Martin	(ACT)
Tariq Mahmood	(VIC)
Derek Reinhardt	(VIC)
Web Site	www.safety-club.org.au

The term of the current committee expires 30 June 2011. As per the constitution the 2010/11 chairman will be elected by the outgoing committee and all other committee positions are declared vacant.

Website

The committee is currently seeking quotations to update the website by adding more feature pages and resources.

Policy / Principles

The committee is currently establishing a number of guiding principles with respect to the development, use and maintenance of safety-critical systems containing software.

These principles will build on the policy first established in 1997.

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.

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.

ISSEC 2010

ISSEC 2010

Following the aSCSa support of the inaugural *Improving Systems and Software Engineering Conference* in August 2009, the aSCSa was again invited to support ISSEC in 2010 held at the Brisbane Convention Centre during the week of 23-25 August 2010.

From both quality and attendance perspectives this was a poor conference. Despite the two-day conference program (day 1 was a tutorial day), there were only five peer reviewed papers published; three of which were under the Safety stream.

The papers have been published and are available at the ISSEC website. The direct link is http://issec.com.au/weblease/tpcommon/src/tp1FullPage.cfm?idPageCopy=15091&idClient=969.

The aSCSa support for the conference was in-kind - a half-day tutorial, the safety stream committee chair and peer reviewers.

From the aSCSa's perspective, ISSEC 2010 did not meet expectations. In fact from an attendance and technical program perspectives there was a decline with respect to ISSEC 2009.

The conference organisers sought feedback by an electronic post-conference. At the time of publication, the aSCSa had not received and results of that survey.

The Safety Stream Tutorial

The attendance was 13, which was surprisingly good considering there was no advertising of the topic prior to the day.

The topic was ***ICT – Are we meeting our safety obligations?*** The tutorial discussed various Australian legislative safety requirements and the obligations these impose on those in the safety-critical systems space.

Feedback from tutorial participants on the day was very positive.

Professional Development

The University of York Department of Computer Science — ANU The Australian National University

Introduction to System Safety

For the 7th consecutive year, the aSCSa in conjunction the Australian National University will be running the highly successful *Introduction to System Safety* developed and delivered by the University of York.

This five day introductory University of York course is offered as graduate coursework by the ANU College of Engineering and Computer Science and to industry through the aSCSa.

Prerequisite knowledge

There are no prerequisites for this course. An introductory book such as Aircraft System Safety (Kritzinger, 2006) before hand may be helpful to look at prior to the course.

Workload

The teaching for this module combines traditional lectures with a number of exercises and case studies which will be tackled in small groups.

Formative Feedback

Formative feedback is given in the form of answers to questions in class, comments from case study demonstrators, model answers for case studies where available and individual written feedback on the assessment paper.

Description

This module provides an introduction to system safety engineering. It is intended to provide a basic understanding of safety processes and of certification which are required by all engineers. This module is an introduction to the principles of system safety and dependability by design, including risk, basic terminology, and the main types of hazard and safety assessment techniques employed within a control system development project. This module therefore aims to provide:

- An awareness of the primary concepts and range of issues associated with achieving and assuring safety;
- An understanding of the role of safety analysis techniques in achievement and assurance of safety;
- An initial ability to apply key safety analysis techniques.

Learning Outcomes

On completion of this module, students will be able to:

- Understand (safety) risk, and the factors influencing perception and acceptability of risk;

- Be able to give definitions of safety-related terminology, and discuss how the use of terminology varies between countries and industrial sectors;
- Have an understanding of typical control system safety lifecycles, and the roles of the major groups of safety and dependability techniques within the lifecycle, including their roles in driving and evaluating designs and design alternatives;
- Understand the approach to certification in domains such as civil aerospace, and the role of safety analysis techniques in certification.

Content

- Introduction and Concepts (Introduction to accidents, hazards and risk; Formal definitions of terminology; Accident and incident analysis; Introduction to system safety lifecycles; Preliminary Hazard Identification; Basic risk concepts; Role of safety process in certification.)
- Safety Requirements (Types of safety requirement, including derived requirements; Setting of safety requirements, including role of FFA; Systematic Failure and DALs; Introduction to dependability and dependability data; Reliability, availability and dispatchability.)
- Analysis of Dependability (Overview of analysis techniques (FMEA, FMECA, FTA, common cause analysis); FMECA for mechanical elements, and links to safety cases; Role of Markov analysis; Preliminary System Safety Assessment (PSSA) process.)
- Design to Achieve Safety (Strategies and priorities for controlling risk; Technical approaches to controlling risk such as fault tolerance; Value and drawbacks of different classes of architecture; Relationship between maintenance and availability.)
- Management of Safety (Safety Cases: safety argument and evidence; Certification processes and practices; Safety management overview; Overview of continued airworthiness issues.)

Teaching Materials

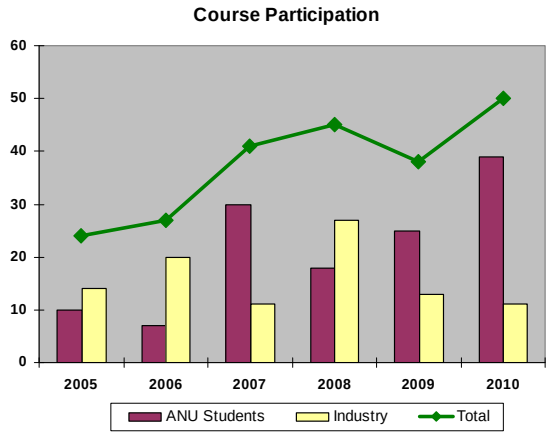
Copies of all lecture slides, case studies and exercises will be provided.

Recommended Books

Rating	Author	Title	Publisher	Year
★★★★	D. Kritzinger	Aircraft System Safety	Woodhead	2006
★★★★	JD Andrews TR Moss	Reliability and Risk Assessment	Professional Engineering Publishing	2006
★★★	C.A. Ericson II	Hazard Analysis Techniques for System Safety	Wiley	2006
★★★	FAA	System Safety Handbook	FAA on web	2007
★★	Nureg	Fault Tree Handbook	Nureg	1973

Interested in this course?

The course has been popular since its launch in 2005.



The venue for this course will be at the Australian National University, Canberra.

This course will be held 13 to 15 April 2011.

The full course fee will be $3080 (incl. $280 GST) per participant. For those registering early (date to be determined) a discounted fee of $2530 (incl. $230 GST) per participant will apply. A discounted fee is available to aSCSa members and students. Members and students are also offered a discounted early-bird fee. The member / student rate also applies for group bookings (3 or more).

Registration will open in January 2011. Please contact an aSCSa committee member if you are interested in attending the 2011 course.

EEA Engineering Education Australia

ENGINEERS 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.

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.

Common Sense Common Safety

The UK could be on the brink of shedding some of the heavy obligations applied to low-hazard workplaces, in an attempt to free employers from "unnecessary bureaucratic burdens" associated with safety obligations.

The Prime Minister's health and safety advisor, Lord Young of Graffham, who has drafted a series of "common sense" safety recommendations, says the standing of health and safety in the eyes of the public has never been lower.

"Last year over 800,000 compensation claims were made in the UK... and there is a growing fear among business owners of having to pay out for even the most unreasonable claims," he says in the "Common sense, common safety" report.

"The incentives for claiming compensation have to change. The system must be fair and proportionate without placing an excessive financial burden on the losing party."

A key to reform is the insurance industry, says Lord Young. "Insurance companies should draw up a code of practice on health and safety for businesses and the voluntary sector. If the industry is unable to draw up such a code, then legislation should be considered."

Further, companies and personal injury lawyers should be prevented from advertising in a way that suggests people "can easily claim compensation for the most minor of incidents and even be financially rewarded once a claim is accepted".

Consultants adopt "overcautious" approach

According to Lord Young, risk-based principles contained in UK safety legislation have been "eroded" by an overly-prescriptive, compliance-driven approach.

A "climate of fear" has been compounded by health and safety consultants - many without any professional qualifications - "who have a perverse incentive to take an overzealous approach to applying the health and safety regulations", he says.

"As a consequence they employ a goal of eliminating all risk from the workplace instead of setting out the rational, proportionate approach that the *Health and Safety at Work etc. Act* [1974] demands."

Lord Young says there should be a system of accreditation for health and safety consultants and a web-based listing for employers.

Processes should also be put in place to ensure their assessments are proportionate, he says.

Low-risk workplaces should have fewer obligations

Only about three per cent of all workplace injuries in Great Britain involve offices, and no office workers died as a result of accidents at work in 2009, says Lord Young.

Even so, low-hazard workplaces are obliged to carry out the same written risk assessments as high-hazard workplaces.

The UK should take the lead in ensuring EU health and safety rules for low-risk businesses "are not overly prescriptive, are proportionate and do not attempt to achieve the elimination of all risk", he says.

Further, employers should be exempt from conducting "unnecessary and intrusive" risk assessments for employees working from home in a low-hazard environment.

Self-employed people in low-hazard businesses should also be exempt from conducting risk assessments, he says.

Welcoming Lord Young's report, the Prime Minister said "good, straightforward legislation designed to protect people from major hazards" was all too often "extended inappropriately".

"We simply cannot go on like this," he said, pledging to carry out all of the recommendations.

Source: OHS Alert (www.ohsalert.com.au)
Date: October 26, 2010

Qantas A380

The ATSB has issued a preliminary report into the Qantas A380 incident over Indonesia.

On 4 November 2010, at 0157 Universal Coordinated Time (UTC), an Airbus A380 aircraft, registered VH-OQA (OQA), being operated as Qantas flight 32, departed from Changi Airport, Singapore for Sydney. On board the aircraft were five flight crew, 24 cabin crew and 440 passengers (a total of 469 persons on board).

Following a normal take-off, the crew retracted the landing gear and flaps. The crew reported that, while maintaining 250 knots in the climb and passing 7,000 ft above mean sea level, they heard two almost coincident 'loud bangs', followed shortly after by indications of a failure of the No 2 engine.

The crew advised Singapore Air Traffic Control of the situation and were provided with radar vectors to a holding pattern. The crew undertook a series of actions before returning the aircraft to land at Singapore. There were no reported injuries to the crew or passengers on the aircraft. There were reports of minor injuries to two persons on Batam Island, Indonesia.

A subsequent examination of the aircraft indicated that the No 2 engine had sustained an uncontained failure of the Intermediate Pressure (IP) turbine disc. Sections of the liberated disc penetrated the left wing and the left

wing-to-fuselage fairing, resulting in structural and systems damage to the aircraft.

Figure 1

As a result of this occurrence, a number of safety actions were immediately undertaken by Qantas, Airbus, Rolls-Royce plc and the European Aviation Safety Agency. On 1 December 2010, the ATSB issued a safety recommendation to Rolls-Royce plc in respect of the Trent 900 series engine high pressure/intermediate pressure bearing structure oil feed stub pipes.

Recent examination of components removed from the failed engine at the Rolls-Royce plc facility in Derby, United Kingdom, has identified the presence of fatigue cracking within a stub pipe that feeds oil into the High Pressure (HP) / Intermediate Pressure (IP) bearing structure. While the analysis of the engine failure is on-going, it has been identified that the leakage of oil into the HP/IP bearing structure buffer space (and a subsequent oil fire within that area) was central to the engine failure and IP turbine disc liberation event.

Further examination of the cracked area has identified the axial misalignment of an area of counter-boring within the inner diameter of the stub pipe; the misalignment having produced a localised thinning of the pipe wall on one side. The area of fatigue cracking was associated with the area of pipe wall thinning (Figure 2).

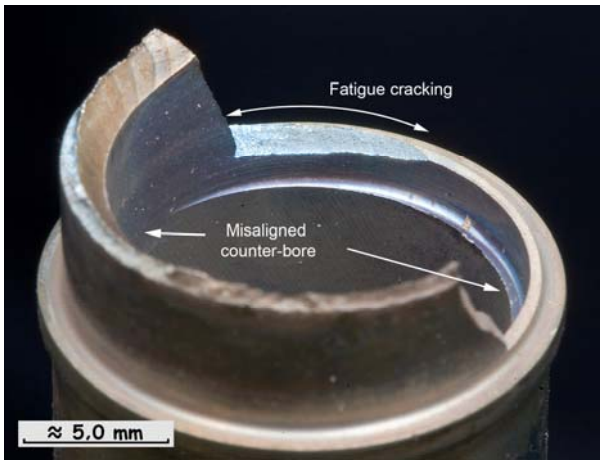


Figure 2

In addition, the Civil Aviation Safety Authority issued a Regulation 38 maintenance direction that addressed the immediate safety of flight concerns in respect of Qantas A380 operations with the Trent 900 series engine.

***Source*:** ATSB

Link:
http://www.atsb.gov.au/publications/investigation_reports/2010/aair/ao-2010-089.aspx

Model OH&S Regulations released for comment

On December 08, 2010, the draft model Work Health and Safety Regulations and priority model Codes of Practice were released on December 08, 2010 for public comment.

A leading OHS lawyer has already raised concerns about some "significant omissions".

"The most significant omission is that of general risk management obligations and particularly the omission of the hierarchy of controls," Norton Rose partner Michael Tooma says.

"The decision to exclude [them] is inconsistent with the objects of the model Work Health and Safety Act which require that workers and other persons should be given the highest level of protection against harm to their health, safety and welfare."

Tooma also criticises the absence of additional guidance on the new duty of officers to exercise due diligence, and what he describes as "very little guidance" on the new horizontal consultation obligations.

Further, stress, bullying and fatigue "are barely mentioned", he says.

Safe Work Australia chair Tom Phillips last night said the proposed harmonised laws would allow employers to more effectively manage workplace safety and "increase profitability and productivity", and urged individuals and organisations to comment on the draft Regulations, an Issues Paper (designed to "stimulate discussion and encourage written submissions").

***Source**: OHS Alert (08-Dec-10) – a service Specialist News, publisher of market leading publications Workplace Express and Shortlist*.

"Common-sense" approach to safety set to lift "bureaucratic burdens"

The UK could be on the brink of shedding some of the heavy obligations applied to low-hazard workplaces, in an attempt to free employers from "unnecessary bureaucratic burdens" associated with safety obligations.

The Prime Minister's health and safety advisor, Lord Young of Graffham, who has drafted a series of "common-sense" safety recommendations, says the standing of health and safety in the eyes of the public has never been lower.

"Last year over 800,000 compensation claims were made in the UK... and there is a growing fear among business owners of having to pay out for even the most unreasonable claims," he says in the "Common sense, common safety" report.

"The incentives for claiming compensation have to change. The system must be fair and proportionate without placing an excessive financial burden on the losing party."

A key to reform is the insurance industry, says Lord Young. "Insurance companies should draw up a code of practice on health and safety for businesses and the voluntary sector. If the industry is unable to draw up such a code, then legislation should be considered."

Further, companies and personal injury lawyers should be prevented from advertising in a way that suggests people "can easily claim compensation for the most minor of incidents and even be financially rewarded once a claim is accepted".

Consultants adopt "overcautious" approach

According to Lord Young, risk-based principles contained in UK safety legislation have been "eroded" by an overly-prescriptive, compliance-driven approach.

A "climate of fear" has been compounded by health and safety consultants - many without any professional qualifications - "who have a perverse incentive to take an over-zealous approach to applying the health and safety regulations", he says.

"As a consequence they employ a goal of eliminating all risk from the workplace instead of setting out the rational, proportionate approach that the *Health and Safety at Work etc Act* [1974] demands."

Lord Young says there should be a system of accreditation for health and safety consultants and a web-based listing for employers.

Processes should also be put in place to ensure their assessments are proportionate, he says.

Low-risk workplaces should have fewer obligations

Only about three per cent of all workplace injuries in Great Britain involve offices, and no office workers died as a result of accidents at work in 2009, says Lord Young. Even so, low-hazard workplaces are obliged to carry out the same written risk assessments as high-hazard workplaces.

The UK should take the lead in ensuring EU health and safety rules for low-risk businesses "are not overly prescriptive, are proportionate and do not attempt to achieve the elimination of all risk", he says.

Further, employers should be exempt from conducting "unnecessary and intrusive" risk assessments for employees working from home in a low-hazard environment.

Self-employed people in low-hazard businesses should also be exempt from conducting risk assessments, he says.

Welcoming Lord Young's report, the Prime Minister said "good, straightforward legislation designed to protect people from major hazards" was all too often "extended inappropriately".

"We simply cannot go on like this," he said, pledging to carry out all of the recommendations.

***Source**: OHS Alert (26-Oct-10) – a service Specialist News, publisher of market leading publications Workplace Express and Shortlist.*

Employers can't rely on operator judgement for safety

Employers cannot rely solely on the judgement of operators – particularly those engaged in repetitive work – to ensure a safe workplace, a South Australian judge has ruled in fining a company over a thumb amputation.

A factory hand was operating a drill press when he noticed the clamp's retaining bolt was loose. The worker raised the drill bit without switching off the machine. As he went to tighten the clamp, the bit caught his clothing and drew in his hand, breaking bones and ripping off his thumb (which was later attached).

The company was charged with and pleaded guilty to failing to implement adequate physical control measures: namely, a guard between the drill bit and the clamp.

In the South Australian magistrates Court, the Industrial Magistrate accepted the employer had attempted to ensure a safe workplace and mistakenly thought the drill press was safe. Its culpability lay in its failure to take "all reasonably practicable steps to reduce the specific risk to an operator of entanglement….whilst adjusting the clamp", he said.

The employer instructed workers to stop the drill before releasing the clamp – which did reduce the risk of injury – but its efficacy relied on operators who were engaged in repetitive work, and might take short cuts.

"If the instruction was not followed, as was reasonably foreseeable, there was no protection," the Industrial Magistrate said.

Hillman v Allin Towbars Pty Ltd [2010] SAIRC 51 (1 September 2010)

***Source**: OHS Alert (10-Sep-10) – a service Specialist News, publisher of market leading publications Workplace Express and Shortlist.*

National Australia Bank: A glitch, in time

The computer glitch at the National Australia Bank on or about November 26, 2010 which locked thousands of customers out of their bank accounts and resulted in pay checks being unprocessed and transactions frozen was, as it turned out, anything but a "glitch".

By the time NAB resolved the flaws that brought its payment processing system to a standstill, the clock had been ticking. Not for minutes, not hours, but a week.

Millions of payments were delayed; thousands of statements showed phantom transactions, hundreds of customers couldn't reconcile transactions and balances.

So when management faced shareholders yesterday they came armed with the answers.

In part, explained CEO Cameron Clyne, a fat finger had caused the debacle that kicked off on November 25, spanning seven excruciating days.

But the "miscoding error" was just part of a perfect storm that sparked a logistical and public relations nightmare.

A "software amendment" carried out nine years earlier was at its root, introducing a bug that was lying dormant, just waiting for the fat finger to pry it free.

And the bug would have been exterminated if only a "maintenance patch" had been applied.

But that wasn't scheduled until next year.

Source: *Herald Sun*, (Peter Taylor), 17-Dec-2010

A 'due diligence' approach to verification of integrity presented to APSEC Cloud Workshop – 30 November 2010 by Kevin Anderson Associate Technical Director, Risk & reliability, Hyder Consulting, Melbourne.

This paper addresses the twin topics of risk mitigation on the one hand and reliability /quality assurance on the other. It sets out a three step approach to establishing risk and reliability through due diligence. By "due diligence" is meant the common law tests of negligence – causation, foreseeability, preventability and reasonableness.

First step - Concept & scope

The first step is to address the common law test of *causation*. The sub-text must cover understanding and documenting your concept, adopting relevant standards, setting the social, legal, economic and environmental context, engaging with relevant Stakeholders, consult with experts and generally do all that one can to establish 'good' practice.

Cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid. Critical success factors include: abstraction, dynamic scalability, virtualized resources, online applications, data servers, and service level agreements.

Cloud computing and its characteristics of elastic provision, equivalence to a public utility and online illusion of infinite supply. Reliability however, is never infinite, but a matter of how many 'nines'.

The front end of the cloud comprises the client's network or computer and applications used to access the cloud and a user interface such as a web browser.

The back end – the cloud itself comprises computers, servers and data storage devices – often in huge numbers. 30% utilization of Google servers has been quoted as a driver to move into the cloud to offer more services. But is the vulnerability of reduced redundancy really appreciated. 90% may be good for business for a while but dangerous to one's reputation when it does fail, as it will.

Understandably, service providers do not make their predictions public. However, failures generally reported as they occur. A brief search for "Internet outages" found numerous examples of individual services providers standing their customers up.

The systems architecture typically involves multiple communications over API, usually web services. Most systems are thought to be protected against single points of failure but can suffer criticalities from unwanted synergies and common mode failures.

Second step - Hazard & risk analysis

Foreseeability and preventability go hand in hand, else you may face long lists of unmitigated hazards. You ought to have known (something would go wrong) and you should have identified options to prevent or respond to that.

For each Critical success factor,, consideration is given to what could go wrong (a hazard being an incipient situation), how this situation could be caused and what will result if it did happen.

In Cloud computing, a major claim is made for economics:

- Capital expenditure is avoided (but substituted for by renting usage)
- Server utilization rates are improved
- Small and medium enterprises (SMEs) have access to a broad range of applications and services

On the downside, crucial corporate data may be compromised; ability to operate independently may be sacrificed; and rental charges may soon overtake initial savings.

Third step - Requirements definition & allocation

The final test of due diligence is 'reasonableness'. This is the hard part. The choice of options includes: 'do nothing', select the cheapest fix, rely on standards and past practice, and be truly generative, matching all credible threats with sensible precautions.

A balance must be reached and defended as to the significance of the risk versus the cost of necessary risk reduction. The issue therefore is to what extent the cloud concentrates resources in a handful of

companies, thereby defeating the very purpose of the distributed Internet.

The risk-based concept of Safety Integrity Level (SIL) provides assurance that say, for SIL 1, the dangerous failure rate is better than 3.0 E-6 per hour. This represents reliability of 99.9997%.

Whilst cloud computing may not of itself give rise to harm to humans (as distinct from economic loss), there are increasing numbers of examples where ubiquitous data can be turned to social purpose. For example:

- LaTrobe University are researching 'mobile phone style' integrated GPS technology to warn motorists as they are approaching a level crossing and there is /will soon be danger.
- Loss of data and communications was a major factor in loss of life in the Feb 2009 'Black Saturday' bushfires.
- The Waterfall Train Crash Inquiry was highly critical of the lack of a Precise Train Location System. With near ubiquitous deployment of GPS in phones and in cars, why are trains not so equipped?
- Computers are omnipresent in avionics. And implicated in various crashes and mid-air collisions. Independent verification

Independent verification (IV) is employed in all major critical infrastructure projects as insurance against failure. The role of the Independent assessor is to investigate and arrive at a judgment as to the level of integrity afforded by a system.

When the standards were written, it was considered that modern computer systems were incapable of reducing dangerous failure rate below 1.00 E-9 per hour (roughly 100,000 years).

The author's experience is based on application of international standards to recognised safety-critical applications such as airspace risk management, railway train control, road and rail tunnel fire and life safety systems. The domains of airspace, train control and tunnel life safety systems each provide specific lessons and comfort. However, a detailed and rigorous explanation of safety critical assurance techniques here would miss the point that cloud computing provides no such assurances.

A recent airline reservation system failure led to compensation and ticket refunds for all prospective passengers delayed by more than four hours. The backup reservation systems was supposed to cut in within two hours but took twelve, despite a service agreement with the IT outsourcer requiring any mission critical system outages to be remedied within a short period of time. Consequences were reportedly in the order of $20m.

Conclusions

This paper has scratched the surface, so to speak, of a potentially ultra–catastrophic risk. It would require much detailed study and openness on the part of Cloud service providers before the advantages of the safety-critical assurance approach could be appreciated in detail.

It concludes that, in the absence of use of trusted risk /reliability assurance techniques there is no guarantee that the concentration of services /data in the cloud will not result in catastrophic consequences.