Australian Safety Critical Systems Association

A National Special Interest Group of the

AUSTRALIAN COMPUTER SOCIETY

Newsletter

June 2012

2nd Australian System Safety Conference a success!

The second two-day Australian System Safety Conference which incorporated the 2012 International System Safety Regional Conference, held in May 2012 was a resounding success. The conference hosted by the aSCSa and the Australian Chapter of the System Safety Society attracted an attendance of 90 and included representatives from the USA, UK, Germany, China, France, and Singapore.

The theme of the conference was ***Value Adding & Improving Efficiencies in System Safety.***

There was representation from a broad cross section of the safety-related industry; procurers, developers, safety assurance, government, academia, and private industry, associated with the defence aerospace, rail, process and mining industries. Conference sponsors were:

- Hyder
- Airservices Australia
- Ansaldo-STS
- RGB Assurance
- BAE Systems
- Nova Systems
- Defence Materiel Organisation
- Australian Computer Society (ACS)

Feedback from the delegates indicated that the conference achieved its aims to share research, government and industry knowledge and practice in the field of systems and software safety.

As had been the norm for conferences since 2002, this conference was supported by several keynote speakers from USA, Germany and Australia.

The conference was supported by two pre-conference tutorials; a half-day tutorial Essential Questions in Software Safety presented by Terry Hardy and a half-day tutorial Rapid Risk Assessment of Technical Systems by Jens Braband. The tutorials were also a success with a total of 37 attendees.

The successful conference was very much due to the good collaboration between the aSCSa, the Australian Computer Society and the System Safety Society Australian Chapter. In particular, the administration support provided by the Barry Snashall and Colleen Garard of the Queensland Branch Office of the ACS and Brian Clegg for modifying the ACS Events on-line system for the special registration needs was very much appreciated by the organising committee.

The conference papers will be published under the CRPIT banner in due course. Conference delegates will be provided with a link to access pre-publication versions and the presentation slides. The conference papers for the 2011 conference will be published as Volume 133 under CRPIT.

Annual General Meeting Notice

The 2012/13 Annual General Meeting will be held in conjunction with the next aSCSa Committee meeting, expected to be before August 31, 2012, in Canberra.

The date, time and venue will be advised when confirmed.

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

At the last meeting of the 2011/12 fiscal year held May 23, 2012, the committee re-elected Clive Boughton to continue as chairman.

The current committee members have indicated their intention to continue. Any member wishing to nominate for committee membership should *e-mail to George Nikandros*

Contents

From the Chair

In the last aSCSa newsletter (December 2011) I mentioned how busy all the members of the committee had been during 2011. Well, that busy-ness hasn't waned. So, to start with, I would like to thank all committee members for their continued efforts for this first half of 2012. So, what's happened? Please continue reading and you'll find out!

For the eighth year in a row, the joint aSCSa, Australian National University (ANU) and University of York (UoY) masters course on "Systems Safety Management" was conducted at ANU in April. A total of 39 students attended the course - 31 masters students enrolled at ANU and 8 industry participants from various organisations/companies around Australia. David Pumfrey and Dr Andrew Rae (both from UoY) delivered the lecture component of the course, and Gordon Stone, Lenny Bruce, Malcolm Newey and Brian Molinari conducted the tutorial component. Over the eight years, the course has evolved into a good mixture of theory and practice treating both hardware-intensive and software-intensive systems. The aSCSa committee hopes to continue to support this excellent course, but is also planning a further course for managers and executives concerning good business and legal reasons for addressing safety considerations effectively, whether their organisations acquire or develop systems possessing implicit/explicit safety-related characteristics.

For the second year, the running of a very successful aSCSa/SSS Joint Conference brought about so professionally by the same organizing team as for 2011. Attendance reached the same levels as 2011 with an equally good line up of top quality presenters and papers. Again, special thanks go to Brett Martin (aSCSa), Derek Reinhardt (aSCSa) and Holger Becht (SSS). Additions to the team this year were Glen Larsen and Nigel Hulse who carried out lots of supporting activities.

It would be very remiss of me not to mention the ongoing efforts of our unassuming Program Chair, Tony Cant, who (for 20 years) has so successfully managed the conference program and paper reviews. Stellar, Tony! I propose that Tony receive a special award for his dedication and contributions to the safety arena, including always making the yearly conference something well worthwhile attending.

Actually, we should all be very appreciative of the efforts of the conference organising team and program chair. They are all volunteers and they all give up much of their own precious time to make the conference a real success. This year's conference was truly international with attendees and speakers from China, France, Germany, Singapore, UK and USA.

The theme of the conference "System Safety … What's the Value-add?" certainly provided the opportunity for speakers to deliver some interesting and challenging views. The conference began with a couple of challenges. The first surrounded the very first (key-note) speaker (Dr Claire Marrison) who was almost late due to air traffic congestion – ironically the topic of her presentation centered on improving air traffic control. Nonetheless, Claire kicked off the conference to a very good start by presenting a clear picture of some of the 'safety' challenges needing to be addressed (globally) in air traffic space. Terry Hardy (the next keynote) presented his views on why we all should be "skeptical" about many safety practices. Dr Andrew Rae (who won the best philosophy paper of the conference) presented a significant challenge to the safety community concerning the general lack of 'scientific method' relating to the seeming plethora of (often unproven) safety methods available. A challenge that many of the following speakers took to heart when presenting their own papers. The other keynotes included Professor Manfred Broy, Dr Jens Braband, and Robert Schmedake whose collective wisdom added great depth to the theme of the conference.

All the papers and keynotes were of high interest and quality. This was exemplified by the fact that two best papers were chosen. The best philosophy paper (mentioned above), and the best practical application paper; the latter being awarded to Benjamin Marsh who provided a great interpretation of ALARP. Additionally, Anthony Acfield received a special mention for his performance (dressed in a well-cut suit) as part of a joint presentation with Rob Weaver, on the Bowtie Concept. Neither presenter wore a tie!

As in 2011, all attendees at ASSC-2012 were offered free membership to aSCSa for the remainder of the year. However, this year the committee decided that an opt-in rather than an opt-out basis be used.

All current and new members need to note that the aSCSa website will shortly be undergoing some changes that will make it more obvious that aSCSa is a special interest group (SIG) of the Australian Computer Society (ACS). The ACS will perform the actual changes in the next few weeks.

Finally, all members are invited to the annual general meeting (AGM), which will precede the next (regular) aSCSa Committee meeting. The AGM provides opportunity for any current member to be nominated and elected to any position on the committee, except for the Chair who must be an ACS member. Date, time and location for the AGM will be advised by email.

Dr Clive Boughton
Chairman aSCSa

ASSC 2012 Awards - Congratulations to Drew Rae and Ben Marsh

Association Matters

National Committee

Clive Boughton	Chairman (ACT)
Kevin Anderson	Secretary (VIC)
Chris Edwards	Treasurer (ACT)
Tony Cant	Conference Program Chair (SA)
George Nikandros	(QLD)
Anthony Acfield	(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 2012. As per the constitution the 2011/12 chairman will be elected by the outgoing committee and all other committee positions are declared vacant.

Policy / Principles

The committee has established a number of guiding principles with respect to the development, use and maintenance of safety-critical systems containing software. Comments are invited on the document titled Draft Guiding Philosophic Principles on the Design and Acquisition of Safety-Critical Systems which is available on the aSCSa Website. These principles will build on the policy first established in 1997.

Safety Leadership Course

After seven years of hosting the *Introduction to System Safety Engineering and Management* course, the committee came to the view that it is time to consider professional development for practitioners and mangers in the safety technology area. The committee has initiated the development of a course relating to Safety Leadership. The course is intended for managers who find themselves in a safety leadership role. The envisaged objectives, bearing in mind that this is just the initial thinking, are:

- Making managers aware of the key issues associated with leading a safety function within a safety critical or safety related organisation;
- Providing understanding of the fundamental components associated with the key issues and how these are integrated to ensure safety within an organisation;
- Providing a working knowledge of critical safety techniques that assure the effectiveness of a safety function within an organisation

It is envisaged that this would be a two or three day course.

The committee will be seeking feedback of the proposed course when the course content is better developed. If you are interested in contributing to the development of this course, please contact an member of the committee.

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.

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.

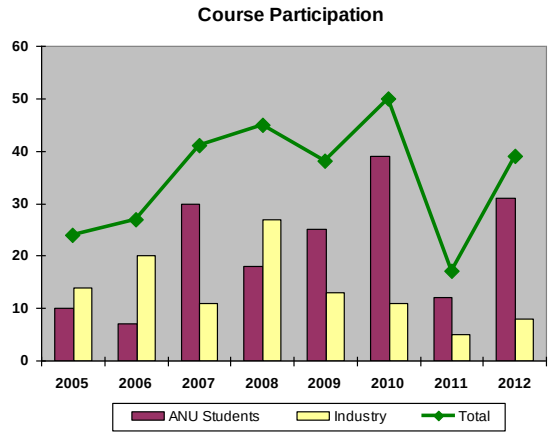
Professional Development

Introduction to System Safety

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

This year there were 39 participants. There were 31 MSE students (12 in 2011) and 8 industry participants (5 in 2011). Over the eight years 276 people have undertaken the course.

Industry attendance has trended lower since 2009 despite a small increase this year. However organisations have piggy-backed on this course by arranging in-house courses, thus depleting the delegate pool. This year, BAE Systems hosted two in-house courses. In the June 2011 newsletter, it was reported that the ANU indicated that they no longer host this course. However continued student demand has forced a rethink which should see the annual course continue for the foreseeable future.



Course – Introduction to System Safety – Participation

MIL-STD-882E - An Opportunity Lost

Chris Edwards, AMW Pty Ltd

MIL-STD-882E was formally released on 11 May 2012, more than twelve years after the release of the previous version. The latest release represents an enormous lost opportunity to modernise the standard as well as representing a loss of leadership by the US DoD safety community.

For more than a decade there has been discussion within the academic and safety communities about the limitations and misapplication of the concept of risk embodied within earlier versions of MIL-STD-882. The discussion has focussed on the use of a risk matrix to rank risks associated with the development and deployment of systems. Cox (2008) provides a useful summary of that discussion, while Pickering and Cowley (2010) reinforce arguments about risk matrix limitations in a different context.

The essence of the problems emerges from consideration of two disciplines, i.e., measurement and statistical theory. Additionally, the issue of risk interpretation and acceptability of that risk to communities outside the DoD community is only partially addressed in the standard.

In summary the problems that continue to exist in MIL-STD-882E are:

a) an endorsement of qualitative assessments, or Risk Assessment Codes (RACs), used to rank identified risks;

b) a failure to recognise that hazard probabilities have a natural variability and are best represented as a distribution or Probability Density Function (PDF);

RACs

Measurement theory defines four scales of measurement, i.e., nominal, ordinal, interval and ratio. RACs are an example of an ordinal measure. This allows RACs to be ranked, e.g., largest to smallest, but not compared in size. The problem comes when attempting to compare RAC's from different rows and columns in the risk matrix. In short, such comparisons are meaningless and have the propensity to lead to false conclusions about the relative risk rankings. Of course if all RACs have been derived from the same row or column of the risk matrix the ranking (but not the comparative size) has meaning, but this is rarely the case.

Hazard Probabilities

Problems encountered when attempting to estimate hazard probabilities are not so clear cut. The first step in resolving the problem is to recognise that hazard realisation results from a series (of often unlikely) events, and that the probability of each of event in the sequence has natural variation. Such variation is best represented by a probability distribution. It is also important to note that any uncertainty about the distributions can also be modelled. Whatever distributions are chosen to represent events the metric used to represent a specific event probability should be taken from the event distribution, e.g., a measure of central tendency such as the mean, median, mode or some percentile value of the distribution.

There are a number of schools of thought about probability theory, the two main ones being the Bayesian and the Frequentist schools. When it comes to estimating the probability of a hazard it is the availability or absence of statistical data about the hazard that determines which statistical approach should be used. Thus for example, the availability of reliability data about a system may lead to the use of analytical statistics to estimate a hazard probability, while the absence of such data is more likely to require a Bayesian approach. Whatever the approach taken the natural variability of the event probability being estimated needs to be considered. Edwards and Westcott (2010) propose a methodology for estimating hazard probabilities based on combining probability

distributions of each of the events leading to the realisation of a hazard.

Estimating Risk

The process of combining hazard probability and outcome severity is a complex process and is not suited to the application of simplistic ordinal measures such as RACs. Ideally entries in the risk matrix should be ratio measures derived from system specific data. This implies the availability of data describing the hazard probability and the consequence severity, together with a defensible methodology for combining the two measures.

Suggested Changes to MIL-STD-882E

So what needs to be done to bring MIL-STD-882 into the 21st century? The actions divide naturally into two groups. The first are relatively easy changes to the standard that simply recognise the theoretical limitations of RACs and the intrinsic variability of event probabilities. The standard needs to provide guidance on dealing with these issues. The second group of changes are the more difficult longer term methodological changes which remove the use of RACs and replace them with a mathematically sound process.

Immediate changes to MIL-STD-882E could include:

a) Section 4.3.3.b – Add an additional paragraph along the lines

   Hazard probabilities intrinsically possess natural variability which must be taken into account when assessing hazard probability levels. The reason for the choice of metric used to document the hazard probability, e.g., mean, median, upper 5th percentile, together with any statistical arguments shall be documented and be formally approved by the relevant safety authority.

b) Section 4.3.3.c – Add an additional paragraph along the lines

   Ranking of Risk Assessment Codes from different rows and columns of the Risk Assessment Matrix must be made very carefully. Such comparisons will usually require external assessment and be the subject to engineering judgement. Results of such judgement calls shall be documented and formally approved by the relevant safety authority.

Conclusion

Longer term changes to MIL-STD-882E must aim to remove the use of RACs and replace entries in the Risk assessment Matrix with numerical values that allow direct comparison and ranking of identified risks. For example Jarrett (2008) provides a semi quantitative methodology for ranking risks that appears to have application in a number of risk domains. Another approach using Monte Carlo simulation of mishap scenarios to estimate risk values has been proposed by Edwards & Westcott (2012).

References:

Cox, L.A. (2008): What's wrong with risk matrices? Risk Analysis 28: 497-512.

Edwards, C.B.H. and Westcott, M. (2010): Estimating accident likelihood. In: A. Tuffley (ed.) Proceedings of Improving Systems and Software Engineering Conference (ISSEC), Brisbane, August 2010, 41-60. ISBN: 978-0-9807680-1-5

Edwards, C.B.H. and Westcott, M. (2012): Risk Based Safety Assurance: towards a defensible and practical methodology, 17th Australian System Safety Conference on Value Adding & Improving Efficiency in System safety, Brisbane. Conferences in Research and Practice in Information Technology (CRPIT).

Jarrett, R. (2008) Developing a quantitative and verifiable approach to risk assessment. CSIRO Presentation on Risk, August 2008

Pickering, A. and Cowley, S. (2010): Risk Matrices: implied accuracy and false assumptions: Volume 2 issue 1, October 2010, Journal of Health & Safety Research & Practice

---

Over-reliance on GPS

In the May 2012 issue of Australasian Science, Drew Turney wrote on the Future of GPS. The article cites an incident involving two US Navy ships in San Diego harbour involved in a test to loss of communications through a denial of service (jamming) simulation. The article claims that an air traffic control system, hospital emergency pagers and other services were taken out. The incident happened occurred in January 2007, not last year as stated in the article.

A report by Dr James Carroll of the John A. Volpe National Transportation Systems Center, Cambridge Massachusetts and Kirk Montgomery of Symmetricom Inc, dated December 01 2008, gives an account of the denial of service test conducted by the US Navy in San Diego.

Australasian Science -Credit: iStockphoto

From that report the U.S. Navy was conducting a scheduled communications jamming training exercise in the Port of San Diego. Two Navy ships participated in the exercise for approximately 2 hours.

Although it involved communications jamming, GPS agencies, including the US Coast Guard Navigation Centre, were not notified because the intended jamming was not planned to be in the GPS spectrum. GPS was jammed and the jamming continued for approximately 2 hours.

The jamming was terminated only after the technicians involved in the exercise could not get their GPS on the second ship (the one being jammed) to initialize. They correctly suspected the first ship was inadvertently

jamming GPS, immediately returned to the first ship, and shut down the jammer.

In less than 30 minutes from the time the inadvertent, yet highly effective jamming began, the GPS agencies started receiving calls concerning GPS outages in the San Diego harbour area. These outages affected both telephone switches and cellular phone operations and even shut down the Naval Hospital's mobile paging system. General aviation GPS navigation equipment outages were reported, but no commercial airlines were affected, or at least none officially reported any outages. Reports continued to flow in for more than 4 hours.

The Navy technicians shut down the unintentional jamming signal, but did not report the incident outside of normal channels. Consequently, it took the US Coast Guard Navigation Centre and supporting agencies a longer time to pinpoint the jamming source.

This incident highlights the vulnerability of the low-power GPS signal to jamming and interference. It also clearly demonstrates that procedures are not yet in place – despite determined efforts of coordinated agencies – to pinpoint jamming in a timely manner and take actions to mitigate it. Despite the clarity of this message, some experts claim that GPS or timing backups are not needed.

In March 08, 2011, the Royal Academy on Engineering issued a report warning of the over-reliance on global satellite navigation systems.

According to the Academy's report, society may already be dangerously over-reliant on satellite radio navigation systems like GPS. The range of applications using the technology is now so broad that, without adequate independent backup, signal failure or interference could potentially affect safety systems and other critical parts of the economy.

The Academy's report focuses on our increasing reliance on Global Navigation Space Systems (GNSS) and the current limited use of GNSS-independent backups for Position Navigation & Timing (PTN) data. The vulnerabilities of GNSS to deliberate or accidental interference, both man-made (such as jamming) and natural (such as solar flares) are also highlighted.

GNSS dependency is now widespread across the UK. As well as the ubiquitous satellite navigation, the signals are used by data networks, financial systems, shipping and air transport, agriculture, railways and emergency services. The European Commission, in its mid-term review of the European satellite radio navigation programmes (18 January 2011) estimated that an, €800 billion chunk of the European economy is already dependent on GNSS.

All GNSS applications are vulnerable to failure, disruption and interference and the report looks at a range of possible consequences of these, from the inconvenient (such as passenger information system failures) to possible loss of life (such as interruptions to emergency services communications).

The severity of the errors may be so large as to give noticeably suspect results which can immediately be identified by the users, but the real threat lies in "dangerously misleading" results which may not seem obviously wrong - a ship directed slightly off course by faulty data could steer it into danger.

There is also a concern over the criminal use of jamming equipment to bypass GNSS systems - easily available technology can be used to block tracking of consignments of goods or to defraud systems that collect revenue using GNSS (such as toll-road charging).

Dr Martyn Thomas CBE FREng, Chairman of the Academy's GNSS working group, says: "GPS and other GNSS are so useful and so cheap to build into equipment that we have become almost blindly reliant on the data they give us.

"A significant failure of GPS could cause lots of services to fail at the same time, including many that are thought to be completely independent of each other. The use of non-GNSS back ups is important across all critical uses of GNSS."

The Academy's report looks at security awareness and recommends that critical services include GNSS vulnerabilities in their risk register and that these are reviewed regularly and mitigated effectively. It says the provision of a widely available PNT service as an alternative to GNSS is an essential part of the national infrastructure - a terrestrial radio navigation system called eLORAN is already in development for this purpose.

Dr Thomas adds: "The deployment of Europe's Galileo system will greatly improve the resilience of the combined GPS/Galileo system, but many of the vulnerabilities we have identified in this report will remain. No-one has a complete picture of the many ways in which we have become dependent on weak signals 12,000 miles above us."

What is eLoran?

Source: Megapulse

The US Department of Homeland Security (DHS) in a recent policy decision announced the implementation of an independent national position, navigation, and timing ("PNT") system that complements the GPS in the event of an outage or disruption in service. The enhanced Loran, or eLoran, system will be a land-based, independent system and will mitigate any safety, security, or economic effects of a GPS outage or disruption. In addition to providing backup coverage, eLoran will provide support to operators in environments that GPS cannot support.

The General Lighthouse Authorities in the United Kingdom view eLoran as an independent, dissimilar complement to Global Navigation Satellite Systems (GNSS) that allows users to retain their GNSS-levels of navigational safety even when their satellite services are disrupted. They strongly advocate that the international maritime community needs an internationally agreed alternative system to GNSS and that eLoran is the only viable candidate.

LORAN (**LO**ng **RA**ng **N**avigation) is a terrestrial radio navigation system which is based on low frequency

radio signals (around 100 kHz) transmitted by fixed land based radio beacons.

Wen Zhou Accident Update

This article builds on the article published in the December 2011 newsletter.

On July 22, 2011 at about 8.37pm two high speed trains collided on a viaduct near Wen Zhou, resulting in 40 deaths and more than 200 injuries (China.org.cn) and raising concerns about the safety of high speed rail in China. In December 2011, an official report (in Mandarin Chinese) was released; however the cause of the accident still remains a mystery. The report however supports the media statements made by Chinese Government and Railways officials since the accident.

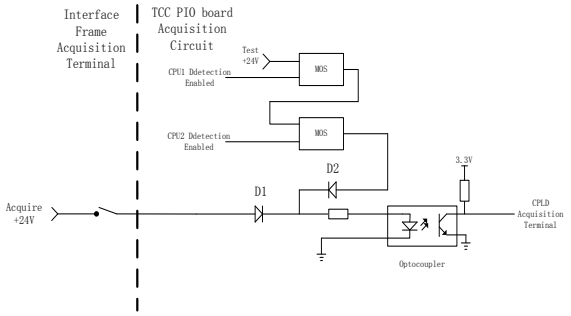
The official accident report gives the cause of the accident, translated as thus:

“As a result of investigation we firmly believe that what caused the accident to happen was the chaotic management of the Communications and Signalling Group subsidiary, the Communications and Signalling Design Institute, in the development of the LKD2-T1 train control centre equipment. The Communications and Signalling Group did not use best endeavours to fulfil its responsibilities as contractor for the communications and signalling for the Ningbo - Wenzhou line.

“The result was a latent critical design defect resulting in a major safety hazard in the Type LKD2-T1 train control centre equipment supplied for Wenzhou South Station and on the Ningbo - Wenzhou line. The work of the Ministry Of Railways was irregular and their checking was not rigorous in allowing the deployment of the LKD2-T1 train control centre equipment; there was no technical review.

There is no technical description of the circuit sketch available. However it appears that the “MOS” labelled devices are some form of switch controlled by a signal from the CPU. Because of the diode “OR” arrangement, the output from the Optocoupler is Low when the interface input contact is closed or both CPU1 and CPU2 Detection Enabled are enabled. Only if the interface input contact is open can the Optocoupler be tested i.e. the output would be HIGH except when both CPU1 and CPU2 Detection Enabled inputs are enabled.

“A lightning strike resulted in the rupture of fuse F2 (a fuse at Wenzhou) in the power supply circuit for the Wenzhou South Station train control centre Input-Output Unit (data) acquisition circuits thus preventing any update.



Sketch Map of PIO Board Acquisition Circuit of LKD2-T1 Type TCC

“After testing of the Input / Output Unit by the accident investigation team, a joint testing team made up from relevant testing organisations from the Ministry of Industry and Information Technology carried out testing of the software in the train control centre's host computer and Input / Output (PIO) boards. After simulated tests with actual EMU vehicles and repeated analyses and demonstrations, it was established that after fuse F2 blew in the Wenzhou South Station LKD2-T1 train control centre, the Input / Output unit detected that a fault had appeared in the Input circuits, sent the fault information to the train control centre host computer, but the computer did not process the received information in accordance with the "fail-safe" principle, by continuously retaining the state information received before the fault. After the train control centre host computer received the fault information, it only transmitted the fault information to the monitoring maintenance terminal, and did not adopt any protective measures; it continued to receive the track occupancy information that the Input / Output Unit sent before the fault, and controlled the signal aspects and track circuits on the basis of the Input state information at the very last moment before the fault.

In essence the retention of the state prior to failure resulted in authority to proceed at full speed to Wenzhou, originally intended for the first train, train D3115, being issued to the following train, train D301 whilst train D3115 was immediately ahead.

From the viewpoint of hardware design, the Type LKD2-T1 train control centre equipment principally has the following problems: the PIO input power supply only has one independent power source, it did not use a design of two independent power sources as stipulated, once the power supply fails, all the PIO boards in the PIO cabinet will lose their input power supply. After train control centre fuse F2 blew, it caused the Input / Output Unit input circuits to lose their power supply; two inputs come from a single source, cannot make a safe comparison of the input information. These two hardware design defects led to the equipment not conforming to safety requirements.

After the fuse blew, the CPU software of PIO board was designed such that: when the software finds there is

any abnormal situation during the acquisition circuit self-test, it treats acquired data is invalid without updating acquired data but keeps sending the previous known valid state to the main frame unit of TCC. As long as self-test failure exists, this status will be retained and a failure alarm will be sent to main frame of TCC. The TCC main frame does not make use of the failure alarm in processing the state of the input from the PIO.

The “Test” and “Acquire” power inputs share a common power supply.

There is no technical description of the circuit or any explanation as to what “MOS” is. That said, the arrangement seems flawed, in that the self-test seems inadequate.

Organisation Factors

The official report dispels the rumours that the accident was the result of protection of intellectual property as suggested by the on-line Wall Street Journal (October 03, 2011).

A major contributor to the accident was the procurement process and the awarding of contracts for adjoining sections of line (not for the line on which the accident occurred) which resulted in an interface issue.

In September 2006, the Ministry Of Railways invited tenders for four contracts for integrated turnkey construction projects for the He-Wu line (Hefei to Wuhan, including Hefei station) and for the He-Ning line (Hefei to Nanjing, not including Hefei station).

The Communications and Signalling Group consortium won the contract for the He-Wu line, and selected the Type K5B train control centre equipment that the Communications and Signalling Design Institute had developed; the China Railway 2nd Institute won the He-Ning line, and selected the Type LKD2-H train control centre equipment that the Beijing HollySys Company had developed.

The He-Wu line equipment and He-Ning line equipment had to be interfaced at the intersection of the two lines, namely at Hefei station. However because the two lines have selected different types of train control centre equipment, they could not communicate with each other. As Hefei station must open at the same time as the He-Ning line, the Ministry Of Railways Transport Bureau Passenger Special Technology Bureau convened a discussion forum on June 2nd 2007, the He-Ning Railway CTCS-2 Train Control System Integrated Programme Discussion Forum). Its purpose was to define this interface. This lead to the Communications and Signalling Design Institute developing the Type LKD2-T1 train control centre equipment.

In October 2007, the newly developed Type LKD2-T1 train control centre equipment was installed on site. In November 2007, the Ministry Of Railways Science And Technology Department organised a technical review of both the Beijing HollySys Company's Type LKD2-H train control centre equipment and the Communications and Signalling Design Institute's Type LKD2-T1 train control centre equipment. This review was a joint review with the Fundamentals Department of the Transport Bureau's Passenger Special Technology Bureau (which is responsible for policy and regulation of signalling systems etc. etc.).

On December 26th 2007 the findings of the review were handed-down in the document “Dedicated Passenger Line Train Control Centre (LKD2-T1, LKD2-H) Review Comments” [Science and Technology Transport (2007) No. 224]. The review allowed the He-Ning and He-Wu dedicated passenger lines project to progress as “on-site trials and on-track application processes continually improve the system capabilities” i.e. to refine the product as necessary to suit the application.

On December 21st 2007, the Type LKD2-T1 train control centre equipment was brought into use at Hefei station. In April 2008, the Ministry Of Railways Transport Bureau (Passenger Special Technology Department, the Fundamentals Department) approved the LKD2-T1 train control centre equipment used on the He-Wu line.

The development of the LKD2-T1 was undertaken under severe schedule pressures. The accident investigation findings indicate that the interface requirements at Hefei were not realised until late in the project leading to the quick LKD2-T1 solution.

The accident investigators believe that the Communications and Signalling Group management for the development of the LKD2-T2 was chaotic; the Group did not conscientiously implement national laws, regulations, systems and standards concerning product quality; its oversight of the Communications and Signalling Design Institute's scientific research quality management work was inadequate, the Group's leadership and its relevant departments did not conscientiously perform their duties.

The Ministry Of Railways Transport Bureau (Passenger Special Technology Department, the Fundamentals Department) procedure for carrying-out capital construction projects was not standardised; it one-sidedly pursued engineering construction speed and did not attach sufficient importance to safety. The management of dedicated passenger line system integrated projects was poor, standards and systems of rules were inadequate; the technical system integrated project team and system integration office that were established, did not establish appropriate systems of work, resulting in overlapping functions and unclear responsibilities. For many tasks such as equipment tendering, technical reviews, putting-into-service etc. there were no rigorous checks on violations of the rules; technical reviews were carried out with no basis and no specification, and agreement that the Type LKD2-T1 train control centre equipment did not have to undergo on-site testing before putting-into-service because it was already in use, albeit for a relatively short time (from December 2007).

The relevant technical standards for the CTCS-2 train control system were incomplete, and as such the selection of fixed bids for the Hefei - Nanjing and Hefei - Wuhan lines train control equipment was careless, resulting in the interfaces to the train control equipment on the two lines being incompatible and unable to mutually inter-communicate, initiating the modifications to the types of train control centre equipment at Hefei station and on the Hefei - Wuhan line, resulting in a subsequent series of non-standard work processes; when guiding and coordinating the invitations to tender.

The supervision of the choice of supplier and design approach for the Hefei station train control centre equipment was ineffective. Following the Hefei - Nanjing railway CTCS-2 train control system integrated programme discussion forum resolution that the type of train control centre equipment for Hefei station was to be identical to the type of train control centre equipment for the Hefei - Nanjing railway, the Bureau failed to discover and overlooked the decision of the Communications and Signalling Design Institute to change the type of the train control centre equipment at Hefei station.

The technical reviews undertaken by the Bureau were without a defined basis and without a specification and were pushed through. The Bureau pressured the Science and Technology Department and the Fundamentals Department of the Transportation Bureau into carrying out a technical review of the Type LKD2-T1 train control centre equipment without technical review requirements or criteria, and also countersigned an agreement that the Type LKD2-T1 train control centre equipment need not undergo field tests and trials before being put into service on the Hefei - Nanjing and Hefei - Wuhan lines.

The Fundamentals Department did not act in accordance with their required obligations; they did not establish system improvement management systems and methods for tests, reviews and trials of new signalling technology and products and for putting them into service on the railway. They failed to make special provisions to assure safety during the evaluation and trials period of new signalling products. As the professional department responsible for signalling equipment, its review of the readiness of the Type LKD2-T1 train control centre equipment to be put into service was not rigorous; it allowed the Type LKD2-T1 train control centre equipment without any field testing and when the review material was incomplete. The Department counter-signed and agreed the technical review recommendation that the Science and Technology Department had drafted.

Editor's Comment

High speed rail in China is not only a necessity to move the ever increasing population, but is seen as a measure of the nation's technological advancement and capability and its international image.

It is this high and urgent demand to sustain China's economic growth and prosperity that the lead to failure of the management systems to ensure that safety; the government owned industry corporations the Ministry for Railways including the departments which oversaw the procurement of the technology and the approvers of the technology were focussed on delivery schedule.

This is not the first time delivery pressures have usurped regulations and obligations; Queensland Health's payroll system where a decision to go live without the proper testing resulted in catastrophic failure. Alas it probably won't be the last.

Acknowledgements

This article was made possible by the translation of parts of the official investigation report by John Salmon, UK following the publication of the corresponding article the December 2011 Newsletter and IRSE News.