Australian Safety Critical Systems Association

A National Special Interest Group of the

AUSTRALIAN COMPUTER SOCIETY

Newsletter

Dec 2011

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. Just two months later on September 27, 2011, at about 2.51pm, two metro commuter trains collided in Shanghai resulting in 271 people being taken to hospital of which 61 were hospitalised.

Chinese rescue workers by the wreckage of train cars in Wenzhou

From press reports it is generally accepted that the two accidents resulted from different direct causes, although there are some indirect commonality; both accidents were initiated by a failure of the signalling system. The signalling system on the Shanghai Metro Line 10 failed about 2.10pm requiring trains to be directed over the phone by subway staff rather than by signals. The failure of the driver of the train at fault was not to obey the proceed-with-caution instructions, similar in many ways to the accident at Glenbrook, NSW on December 2, 1999 where a Sydney commuter train crashed into the rear of the Indian Pacific after proceeding past a signal at stop due to a failure of the signalling system.

However the Wen Zhou accident was caused by a failure of a safety-critical system; at least that seems to be the consensus. In the absence of an official accident report, there continues to be much speculation even conjecture as to why and how the signalling system failed so catastrophically. The on-line Wall Street Journal (October 03, 2011) even suggests that protection of intellectual property (copyright) was a contributing factor.

Hopefully there will eventually be an official report released as there would be valuable lessons for the railway industry.

According to a Railway Gazette article, the recently-appointed head of the Shanghai Railway Bureau An Lusheng, appearing before the independent investigation panel established by the State Council, said that 'design flaws' in the signalling on the Ningbo – Wenzhou high speed line led to the fatal rear-end collision near Wenzhou on July 22. An added that 'having been struck by lightning, the signal system at Wenzhou South station failed to turn a green light to red'. On the same day, the Beijing National Railway Research & Design Institute of Signal & Communication issued an apology for the accident.

The railway between Ningbo and Wenzhou South is equipped with line-side signals overlaid with CTCS-2 to provide automatic train protection. This has a similar functionality to the ETCS (European Train Control System) Level 1, using balises to provide intermittent updates to the on-train equipment. The line is designed for mixed traffic operation with a maximum speed of 250 km/h.

The sequence of events leading up to the high speed train collision near Wen Zhou is included in this newsletter and provides some insight as to what went wrong.

CPD Events

Australian System Safety Conference 2012 - details of the conference, including the call for papers, registration and sponsorship opportunities can be found at www.assc2012.org.

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 2012. 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

Contents

From the Chair

This year has been very busy for aSCSa and all the members of the committee. Without the energy and dedication of committee members various things such as this newsletter wouldn't happen. So, as Chair I would like to especially thank all committee members for their efforts with helping achieve the successful operation of aSCSa this year.

Particular praise must go to the aSCSa/SSS Joint Conference team who helped us achieve a great conference event with the best turnout ever and by lining up many top quality presenters and papers. A really great job well done: Brett Martin, Derek Reinhardt (aSCSa) and Holger Becht (SSS). There is also our stalwart Program Chair Tony Cant who has taken charge of conference program and paper reviews. Of course we cannot forget the fantastic support of the Melbourne ACS event managers Ksenija Catic and Daphne Kechagias. By the way, it seems that the conference organising bug has infected Brett, Derek and Holger - they've put their hands up to do it all again this year. Thank you so much guys!

A special thank you goes to George Nikandros (Immediate Past Chair) for willingly undertaking to continue putting together the aSCSa Newsletter. What follows is yet another one of his successful editions for the rest of the safety community to read and ponder about. Thank you George!

Of course the rest of the aSCSa committee put their oar in too. There's our long-time treasurer Chris Edwards who ensures the rest of the committee spends aSCSa money very wisely. Another long-time member is our secretary Kevin Anderson who manages membership and nearly always does our committee meeting minutes. Also there's Tariq Mahmood our webmaster who keeps event information, as well as links to other safety societies etc., all up-to-date on the aSCSa website.

Unfortunately we've lost Rob Weaver from the committee this year. However, he will keep in touch by continuing the task he started to put in place a safety management course for executives - an important endeavour to instil better safety culture, especially within organisations that own safety responsibilities.

I hope you enjoy this newsletter, and I hope you all have a wonderful Christmas and New Year break.

Dr Clive Boughton
Chairman aSCSa

Association Matters

Annual General Meeting

The 2011/12 Annual General Meeting was held on Thursday, July 14, 2011 at Airservices Australia, Canberra. There were 7 aSCSa members in attendance.

At the meeting it was announced that Clive Boughton was elected by the outgoing committee to continue as chairman. The only nominations for the 2011/12 committee received were those of the outgoing committee members. The nominations for the 2011/12 committee were accepted.

The date for the next AGM was not set.

National Committee

Clive Boughton	Chairman (ACT)
Kevin Anderson	Secretary (VIC)
Chris Edwards	Treasurer (ACT)
Tony Cant	Conference Program Chair (SA)
George Nikandros	(QLD)
Robert Weaver	(ACT) – Resigned 20-Oct-2011
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.

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.

Editorial

According to the Online Wall Street Journal, the rail accident at Wen Zhou, China was in some way related to theft of intellectual property.

The supplier of the on-board ATP (automatic train protection) system was Hollysys Automation Technologies Ltd, a Beijing based company. According to the Wall Street Journal article, the systems supplied by Hollysys were branded as proprietary to Hollysys contained tailor-made components from Hitachi (Japan).

Apparently, Hitachi concealed the inner workings of the tailor-made components fearing loss of their intellectual property, so as to make it harder to clone. Whilst one can understand the action to conceal the inner workings to protect their intellectual property, Hitachi's view that Hollysys would not integrate the equipment into a broader safety-signalling system without Hitachi's intimate knowledge and know-how appears to have been a major miscalculation.

It is well known that China does not abide by or support international laws with respect to copyright and intellectual property.

This however raises the ethical issues. In Australia and many other countries there is a requirement to provide information on the safe use of your goods; not only for their intended use, but also with respect to foreseeable misuse. Purposely hiding information, particularly relating to something that may not be obvious, that could prevent harm, would be a contravention of laws governing the supply of goods and services. It would also contravene the ethics of most professional bodies.

The nature of the relationship between Hollysys and Hitachi is unknown; however it is clear that Hitachi did not trust Hollysys with respect to their intellectual property, but "trusted" them enough to supply them with the components they required.

It is unknown if Hitachi provided any warnings on the use of their components. If they did, would have Hollysys heeded them? Probably not.

At the committee meeting held 20-Oct-11, Rob Weaver decided to stand down as a committee member. The committee thanks Rob for his support.

The aSCSa committee wishes members and readers all the best for the festive season and a happy, healthy and safe 2012 - ***The Editor.***

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/sc_list.php for access.

Human traits and safety

Recently I read some of the newspaper reports on the Royal Commission of inquiry into 29 deaths at the Pike River Coal mine in New Zealand. Of course most of the reports contained much the same commentary. In particular there were many quotations of Dr Kathleen Callaghan from University of Auckland's Faculty of Medical and Health Sciences where she is Director of the Human Factors Group. According to The Australian she is an "expert on human strengths and weaknesses". Dr Callaghan holds an MSc in Psychology and a PhD in both Medicine and Psychology, and prior to entering academia she was Principal Medical Officer for New Zealand's Civil Aviation Authority. Some of her quoted remarks from the inquiry are as follows:

"In crude terms, the evidence I have seen indicates that Pike River mine was *an accident waiting to happen*, in the sense that an accident was probable."

"Sadly, but of crucial relevance for future safety, Pike River proves that we have failed to learn from previous accidents."

"Organisational factors may be identified at the level of the company, but more importantly reflect at the level of the regulator, and also government decision-making about the regulator's functions."

"Pike River was a workplace accident that occurred in a mine, but should not be categorised simply as a mining accident."

According to *The Australian*, Dr Callaghan also criticised an independent report carried out for the New Zealand Government Labour Department into its interactions with the Pike River mine, saying it (the report) *dismissed the importance of safety culture*.

Apparently, Dr Callaghan had looked at more than 508 incident reports from the mine and could not understand why some of the incidents frequently recurred. Apparently, incidents included explosives being found in the engine bay of a vehicle, injuries, a failure to file breakdown reports, a lack of knowledge of gas levels, manuals not readily available and lack of communication. Dr Callaghan also said there was a need to understand why unsafe behaviour became routine and that workplace safety culture was a core element of the Pike River disaster.

According to *Stuff.co.nz*, Pike River suffered other safety risk factors, including high staff turnover, inexperienced staff, financial problems, and was said to be in "start-up mode".

Prior to the Royal Commission it was reported in *The Australian* that Peter Whittall (an Australian and an experienced mine manager, operator and developer) was General Manager of Mines for Pike River and, according to its website, was the person "responsible for all operational aspects of the business including mine design and development, and the essential areas of safety and environment." Whittall had apparently claimed that the safety standards at the Pike River mine were high. A claim which came into question when Peter Sattler, who had been deputy or supervisor at Pike River until four months before the blast, made a counter-claim that the safety program at the mine was grossly deficient.

The general secretary of NZ's Energy, Printing and Manufacturing Union Andrew Little is critical of Pike River Coal as well as successive NZ governments, which have done little to address known weaknesses in mine safety regulation.

According to *The Australian*, Little says Whittall, as a mining engineer who had worked underground in Australia with all the benefits of that country's superior mine safety provisions, in his opinion, should have provided them to his workers at Pike River from day one, not just when they were deemed commercially appropriate.

Of course, when an accident involving death and/or serious injury does occur, the tracing and analysis of events and failures leading to it are typically carried out thoroughly.

According to James Reason[1] accidents are rarely the result of a single cause; they are more likely the result of a conjunction of failures. Alternatively, it must be acknowledged that individual failures, which could potentially lead to dramatic events, occur more often than we think. This means that a safety study must not only focus on what appears to be the main causes of accidents, but also pay attention to all "accidents facilitators", and take into consideration human factors issues.

In support of Reason's concepts, Donald Fritz[2] maintains that the objective of causal factor analysis is to identify the failures that caused an incident/accident. Fritz also purports that, generally, failures can be categorized, primarily as cultural-related, engineering-related, systems-related, or human-related factors. These primary categories represent barriers erected, in the order stated, to prevent incidents/accidents. When barriers 'harbour' failures, the opportunity exists for an incident/accident to occur. The more failures, the more likely an incident will occur.

It seems that the path to the awful tragedy at Pike River Coal mine began with a less than satisfactory systemic safety culture - *as intimated by Dr Callaghan in one of her comments on the independent report mentioned above*. However, it is also clear that all of engineering-related, systems-related and human-related factors contributed. What brings all these factors into play? Humans, of course!

Certainly human frailty is a contributing factor to incidents/accidents. It is a sympathetic view, held on the basis that humans are doing their best to do the right thing. However, human traits such as apathy, greed, dishonesty and cowardice (which may all be regarded as frailties, of course) exist as catalysts for not doing the right thing and thus setting up opportunity for disasters like Pike River. Taking advantage of a poorer regulatory climate when it is known that superior regulations are in place elsewhere is both unethical and dishonest. Keeping various stakeholders in the dark about what is appropriate, best safety practice, and providing a sub-optimal safety system is not only dishonest but suggests no care or respect for any employees at the operational level. It can even suggest greed. To sit by and observe recurring incidents due to poor practice without somehow raising the attention of other employees/regulators, is mere cowardice. Apathy seems ever-present, but can be counteracted to some extent by having diligent and responsible people in place who understand the need for effective safety programs. However, when no one assumes responsibility, the opportunity for incidents/accidents increases.

[1] James Reason; Managing the Risks of Organisational Accidents, 1997.

[2] Donald F. Fritz; iP: incident Prevention, April 2009. http://incident-prevention.com/ip-articles/article/16-incident-analysis.html.

The objective of a safety investigation in the aftermath of a safety incident or disaster is clear. However, such investigations occur after all the damage is done and people have lost their lives. It is fairly obvious that the results and messages of previous safety investigations didn't help prevent the Pike River disaster. What's worse is that several nasty human traits are likely to have played a part or even been the main cause.

If the essential finding is "it was an accident simply waiting to happen" after an accident investigation, then it is damning to all parties concerned. As implied above, it seems that it was more than human frailty (in the usual sense) that caused the Pike River disaster.

Was the accident preventable? I believe so! However, the influence of some of those nastier human traits was apparently quite strong, and any counteractions (if there were any) to them quite weak by comparison. It seems that the safety fraternity's preventative tool kit needs to be expanded to include better understanding of the connections between the nastier human traits (human factors) and poor safety culture, and also to have the authority to disempower those who are obviously infected with vested/self interest from preventing good safety culture being established.

[Article provide by Dr Clive Boughton, Adjunct Associate Professor, Australian National University and Chairman & Director, Software Improvements]

Automation Addiction

In August, a number of press articles appeared concerning a US Federal Aviation Administration (FAA) advisory committee draft study report which found pilots sometimes abdicate too much responsibility to automated systems.

The study examined 46 accidents and major incidents, 734 voluntary reports by pilots and others as well as data from more than 9,000 flights in which a safety official rode in the cockpit to observe pilots in action. It found that in more than 60 percent of accidents, and 30 percent of major incidents, pilots had trouble manually flying the plane or made mistakes with automated flight controls.

In the article "*Are airline pilots forgetting how to fly automated jets?*" Joan Lowy (Associated Press) wrote:

> "Pilots' "automation addiction" has eroded their flying skills to the point that they sometimes don't know how to recover from stalls and other mid-flight problems, say pilots and safety officials. The weakened skills have contributed to hundreds of deaths in airline crashes in the last five years.
>
> "We're seeing a new breed of accident with these state-of-the-art planes," said Rory Kay, an airline captain and co-chair of a Federal Aviation Administration (FAA) advisory committee on pilot training. "We're forgetting how to fly."

Lowy cites two relatively recent accidents; the accident involving a regional airliner in 2009 near Buffalo, NY, and an accident two weeks later where a Turkish Airlines 737 crashed while trying to land in Amsterdam.

In the Buffalo, NY crash where 49 people died, the co-pilot had programmed incorrect information into the plane's computers, causing it to slow to an unsafe speed, triggering a stall warning. Not noticing that the plane had slowed too much, the pilot in charge responded by repeatedly pulling back on the control yoke, overriding two safety systems, when the correct procedure was to push forward.

In relation to the Turkish Airlines crash where 9 people died and 120 injured, the circumstances were similar in that speed was reduced to a dangerously slow level, which the crew did not notice, that the plane lost lift and stalled. A faulty altimeter had fed incorrect information into the plane's flight computers which caused the auto-throttle to reduce speed.

Another example of wrong action by the flight crew, albeit after a technical failure, is the 2009 Air France crash in the Atlantic Ocean, off the coast of Brazil, whilst en-route to Paris resulting in the 228 deaths.

However "automation addiction" is not just an issue for the aviation industry; the increasing automation of industrial plants, railways, power generation and even the car you drive is progressively making us to "forget how".

Risk Tolerability

In the article "Weighing up the risk factors" published in the Spring 2011 edition of Track & Signal, Len Neist, the CEO of the NSW Independent Transport Safety Regulator states that:

> *The limits of "unacceptable risk" and "acceptable risk" are an organisation's guideposts. Without an understanding of these limits, an operator is unable to demonstrate the tolerability of its risks.*

This statement is made in the context of the so far as is reasonably practicable (SFAIRP) obligation that the rail safety and soon to be enacted workplace health and safety statutes require.

SFAIRP obligates duty holders to demonstrate that the level of risk cannot reasonably be reduced. According to Len Neist:

> *All reasonable, available safety measures must be implemented to eliminate or reduce risk unless it is grossly disproportionate to the safety benefit to do so.*

The closer the risk is to the unacceptable threshold, the greater the disproportion between the safety benefit and the trouble to implement the safety mitigation; the trouble being more than the benefit.

When the assessed safety risk is near the limit of tolerability threshold, a disproportion factor of 10 is considered appropriate, whereas for an assessed safety risk near the lower acceptable bound a factor of one is appropriate.

The article however provides no guidance for setting the "guideposts"; there is no guidance as for determining the tolerability region. In fact, whilst the article explains what is generally known as the ALARP (as low as reasonably practicable) principle, there is no mention of the term "ALARP".

[Len Neist was a keynote speaker at the 2011 Australian Safety Conference held in Melbourne in May.]

China – Wen Zhou Accident Time Line

A link to a timeline of events from the Wen Zhou Control Centre published by a Chinese newspaper in Mandarin Chinese was posted to the Safety Critical Mailing List by Oleg Lisagor on July 28, 2011. The timeline was considered to be from a trustworthy source. An interpretation of the translated timeline of events follows:

7:34pm Wen Zhou south advised that train D3212 on the 4th road whilst approaching the starter signal at Proceed, had passed the station starter signal at Stop. [The signal appears to have changed to stop as the train D3212 approached it.] Control (Shanghai Control Centre) then asked the driver if the train was moving. Upon confirmation from the driver that the train was not moving, Control cancelled the re-clearing request of this signal.

7:36pm Because Wen Zhou south 4th road station starter signal has no way of clearing, control arranged for Wen Zhou south station to be transferred to emergency control.

7:39pm: The Yong Jia to Wen Zhou South down line section, three approach track sections to Wen Zhou south station showed up as occupied / failed as a result of a lightning strike. Civil/Signal maintenance staff and traction overhead maintenance staff were notified.

7:44pm Control (Shanghai) received the following report from Wen Zhou south station: Station communication centre screen showed that three consecutive approach sections in the down direction were failed/occupied, station (Control) CTC screen didn't show anything. After train D3212 departed the 4th road, control arranged for normal station control to be returned to Wen Zhou South station.

7:45pm Wen Zhou South station reported to Yong Jia and Ou Hai station that the approaching and departing sections were shown as occupied.

7:51pm Train D3115 arrives at Yong Jia station

7:53pm Control (Shanghai) arranged for Wen Zhou south station to transfer to emergency control

7:54pm: Yong Jia station was transferred to emergency control.

7:55pm Control (Shanghai) arranged for Ou Hai to transfer to emergency control

Wen Zhou south station transferred to emergency control

8:06pm The officers in charge of Yong Jia station made a special call to the driver of D301 advising Yong Jia station is under emergency control

8:12pm Train D301 arrives at Yong Jia station

8:14pm Control (Shanghai) arranged for train D3115 to depart Yong Jia station, informing the driver to proceed with vigilance On-Sight mode at 20km/h upon encountering a Red signal (aspect) within the section.

8:15pm Train D3115 departs Yong Jia station

8:20pm Wen Zhou south station reported that four approach down line (track) sections had failed (they showed up as flashing on the screen), but the section going to Ou Hai was clear.

8:24pm Train D301 departs Yong Jia station.

8:25pm Train D3115 stopped at three track sections from Wen Zhou, and then proceeded on On-Sight mode.

8:26pm Control (Shanghai) contacted Wen Zhou south station. (Wen Zhou south) station reports train D3115 was approaching and was three signal sections away. CTC (Control) system showed that the occupied sections had already cleared.

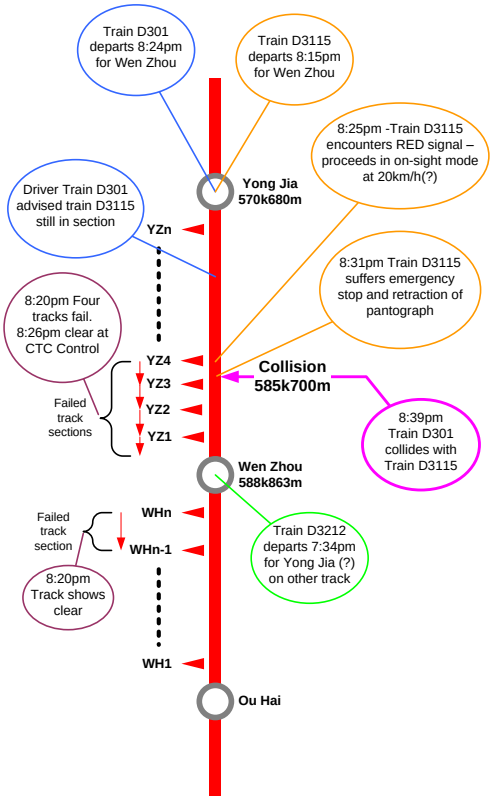
Because train D3115 train spent a long time in the section, Southern Wen Zhou station contacted the driver of D3115 train. The driver answered saying that the signal aspects within the section were not stable. The officers in charge of Wen Zhou south station reported this to the officers in charge of Yong Jia station.

8:??pm When D301 was within 6-7 signal sections away from D3115, Wen Zhou South station made a special call to the driver of D301 advising the driver that "Train D3115 is within this section, proceed with caution." The driver of D301 acknowledged this in response. [The precise time is unknown; however it must some time after the departure of train D301from Yong Jia i.e. after 8:24pm.]

8:31pm Driver of train D3115 reported (to Shanghai Control) that passengers have pressed the emergency stop button and the train pantograph has retracted.

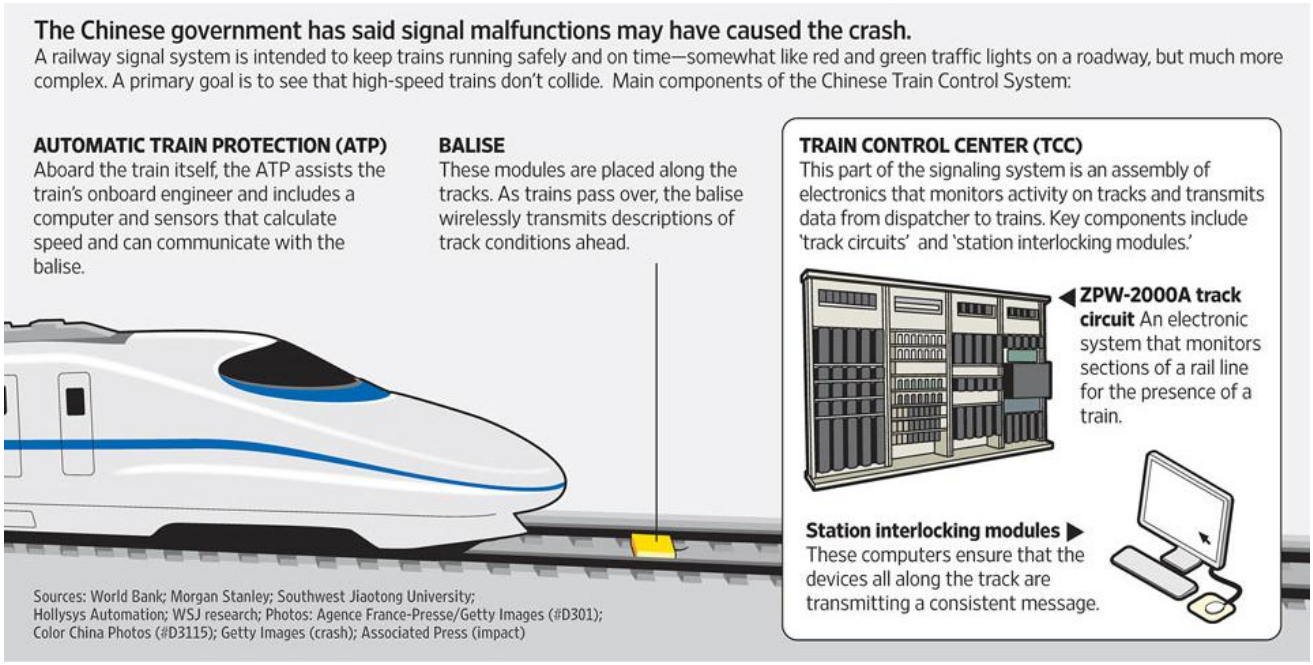
8:37pm Control (Shanghai) arranged for Wen Zhou South station to contact the driver of D301 to apply braking

8:39pm Control (Shanghai) received the following report from Wen Zhou south station: The train driver for D3115 reported that the rear carriages of the train had derailed, and there is half a section of carriage hanging off the bridge.



Schematic showing location of time line events

Train D301 and train D3115 collided head to tail between Yong Jia (570k680) and Wen Zhou South (588K863) close to 585K700, causing train D3115 carriages 13, 14, 15, 16 to derail, and train D301 carriages 1 to 4 to derail (of which carriages 1 and 2 fell off the bridge; the bridge being approximately 15 metres in the air).



Chinese Train Control System components [Source: The Online Wall Street Journal**]**

From the extent of physical damage to the trains, it is reasonable to conclude that this was a high speed collision. So what caused the driver of train D301 to travel at such a high speed knowing that train D3115 being ahead and travelling at slow speed and that there was signalling problems at Wen Zhou?

The most plausible explanation is that the driver of train D301 must have got an "all clear" signal despite train D3115 was ahead and travelling at 20km/h. This can only arise if the signalling system fails in an unsafe way. A Ministry of Railways official supposedly said that a lightning strike damaged a fuse which caused the lights in the line-side signals to go out; thus there were no signals at RED for the driver of train D301 to see.

One event that does not seem plausible is the application of the emergency brake by a passenger on train D3115, particularly as the train had not long stopped when it encountered a signal at RED and was travelling slowly (20km/h), assuming that the driver was following the instructions from Train Control. Also, given that the pantograph retracted strongly suggests that this was a system response to a signalling violation i.e. the train passed a signal at RED or some other system failure.

The Red signal encountered by train D3115, the indications of failed track sections to the station staff at Wen Zhou is evidence that the signalling system was failed in the usual safe mode. The report from the driver of train D3115 that the "signal aspects were not stable", suggests that the maintenance staff were on-site attempting repair; they were notified at 7:39pm, well before train D3115 departed Yong Jia for Wen Zhou at 8:15pm.

It appears that the part of the signalling system which creates and issues the movement authority for train D301 contained a state of the track ahead which was not consistent with state of the track at the local signalling system at Wen Zhou.

Without knowledge of the particular signalling system technology or its architecture it is not possible to draw any conclusions as to how such an inconsistency eventuated. It may be that the data might not have been refreshed due to equipment damage cased by lightning; there was a storm at the time.

Hopefully the findings of the investigation will be made public. There is no doubt that there would be important lessons for the rail industry. It would be a shame if pride and reputation prevents learning from this accident.

Professional Development

THE UNIVERSITY of York
Department of Computer Science

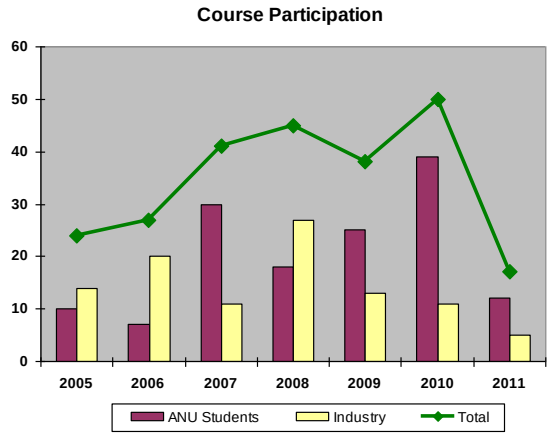
ANU THE AUSTRALIAN NATIONAL UNIVERSITY

Introduction to System Safety

For the 8th 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.

The course has been popular since its launch in 2005. Over the seven years 242 people have undertaken the course.



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

This course will be held 16 to 20 April 2012.

The non-member course fee will be $3080 (incl. $280 GST) per participant; for ACS and aSCSa members the fee will be $2530 (incl. $230 GST) per participant.

For more details of the course and registration, please visit the aSCSa website. Registration is now open.

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.

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.