Australian Safety Critical Systems Association

A National Special Interest Group of the

Newsletter

Dec 2015

Car Hacking!

As widely reported in the media recently, a pair of veteran cybersecurity researchers have used the internet to turn off a car's engine as it drives, sharply escalating the stakes in the debate about the safety of increasingly connected cars and trucks.

In a controlled test, Former National Security Agency hacker Charlie Miller, now at Twitter, and IOActive researcher Chris Valasek used a feature in the Fiat Chrysler telematics system Uconnect to break into a Jeep Cherokee's radio and activated other inessential features before rewriting code embedded in the entertainment system hardware to issue commands through the internal network to steering, brakes and the engine. Further details of the test are available in an article reported in Wired.

Uconnect is an Internet-connected computer feature in hundreds of thousands of Fiat Chrysler cars, SUVs, and trucks. It controls the vehicle's entertainment and navigation, enables phone calls, and even offers a Wi-Fi hot spot. The cellular connection feature within Uconnect also lets anyone who knows the car's IP address gain access from anywhere in the country.

The test highlighted a serious safety and security vulnerability, prompting Fiat Chrysler to issue a software patch release.

FCA US Releases Software Update to Improve Vehicle Electronic Security and Communications System Enhancements

July 16, 2015, Auburn Hills, Michigan USA - The security and confidence of our customers is important. As part of its ongoing software security and quality efforts, FCA has an Embedded System Quality Engineering team dedicated to identifying and implementing software best practices across FCA globally. The team's responsibilities include development and implementation of cybersecurity standards for all vehicle content, including on-board and remote services……. Today's software security update, provided at no cost to customers, also includes Uconnect improvements introduced in the 2015 model year designed to enhance customer convenience and enjoyment of their vehicle.

Continues Page 4

CPD Events

ASSC2016

Conference on Safety and Security in Critical Infrastructure and Systems

Adelaide Australia 25 – 27 May 2016

Safety and Security in Critical Infrastructure and Systems is the theme for the 2016 Australian System Safety Conference. Critical infrastructure and systems are expected to manage complex and uncertain environments, containing both natural and manmade hazards, to ensure a high level of continued service. Intrinsic hazards range from natural disasters to terror and cyber-attack, as well as system design hazards.

Whilst the specific hazards and controls vary, the systems and organisational challenges are very similar. Many organisations have, or are seeking, a single safety management system covering the safety of their people, the safety of their installations and the safety of their products. The technical program will feature a rich variety of contributions and as with recent conferences this will be a two-day event, with a preceding tutorial day.

Confirmed keynote speakers are:

- Prof Jens Braband, Siemens, Germany
- Dr Patrick Graydon, NASA, USA
- Prof Jill Slay, ADFA, Australia

Please visit the conference website (assc2016.org) for more details surrounding the technical program, event sponsorship, and to submit a paper.

Registrations are now open via the ACS Events. Register early to take advantage of the early-bird rate.

Contents

From the Chair

Season's Greetings in my first piece from the Chair of the aSCSa. As we all head in to a period of down time, and bring a busy 2015 to a close, the aSCSa Newsletter hopefully provides some diverse and thoughtful examples of how system safety thinking about requirements and robustness in design can benefit many aspects of our society. I hope it also inspires time to be taken for further holiday professional readings throughout our community, while we may have time to digest, away from other deadlines. I thank George Nikandros for once again for maintaining the vigilance on news sources and bringing together some topical news items, and providing editorial comment.

For myself, I have to admit to a very slow start in taking up the reigns from Clive Boughton, and injecting the energy he spoke of at mid-year. I'm afraid my primary day job has absorbed a deal of that energy, which I aim to rebalance in the new year. Part of the challenge of volunteer professional associations is not just knowledge and enthusiasm for the profession but the discretionary time and fundamental dedication required to pursue such an undertaking on behalf of the community of professionals and at large. We have been very well served for 23 years by our founders in Clive, George, Kevin, Tony, Chris, and Allan who now are transitioning to a well-earned respite. The soon to be formally elected new (young blood) Committee members are charged with moving the legacy forward, continuing the good works and evolving the association and it's ideals into new endeavours and towards new audiences. This is not a challenge of the mind or good intent, but that of busy mid-career professionals maintaining some useful time for their profession and community in this critical but underappreciated space. I encourage us all to take some positive steps (not least myself) to bring that balance back in 2016. We have much to do – Google cars are coming!

The AGM has now been scheduled for the 18th Jan in Melbourne, after some delay and will welcome attendance and dial-in involvement from members. Importantly including nominations for the all-important secretary role, and generally to provide us with the shared horsepower necessary to get things done. If you wish to dial-in or attend in person or nominate for the committee, please contact myself for details.

Nonetheless, we managed to get reasonable numbers (past break-even!) to our first Griffith University running of the Introduction to System Safety Course run in August, and I got very positive feedback from one of my Nova colleagues, who was new to the field. Well done to Dr Drew Rae on course organisation and delivery and George Nikandros for marketing and administration of the event. Next year we'll be back at ANU, with Drew and University of York colleague Mark Nicholson.

Finally, our collective has commenced work and made commitments for the 2016 Conference in Adelaide, which will formally bring the subject of Security into our scope of concern as a professional body. Inspired by the interest in Chris Johnson and Paul Caseley talks at the 2015 ASSC, as well as the transition of IET in the UK to being formally a Cyber Security and System Safety Conference and generally events transpiring in our world. While you will read of our keynote speaker list firming up, we have yet to see an influx of abstracts for papers or Industry talks. I suspect partly due to the very mild promotions that have not occurred. I strongly encourage members and interested parties and researchers to spread the word, consider some options and propose topics to address the audience with their experience or studied views in these key fields. The conference is most important to our community, in knowledge sharing and keeping the national dialogue of system safety application vibrant.

Enjoy your summer break and bring you're energies back for promoting safer systems in 2016, through your aSCSa.

BJ Martin
Chairman aSCSa

Best wishes to all for the festive season and sincerely hope that 2016 brings good health and good change in your lives.

Research Award

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 rules governing the award are available from the aSCSa website

The nominated closing date requirement has now been removed; nominations can now be made any time.

Association Matters

Annual General Meeting

The 2015/16 Annual General Meeting will be held on Monday, 11.30am (Melbourne time) January 18, 2016 at the offices of Advisian Level 15, 607 Bourke Street, Melbourne VIC. If you wish to participate but are not able to physically attend, a dial-in option is available upon request to BJ Martin

The meeting will be chaired by BJ Martin, the aSCSa Chairman elected by the outgoing 2014/15 aSCSa committee. Clive Boughton has now assumed the role of Immediate Past Chairman.

The purpose of the meeting is to elect the committee for 2015/16 and office bearers and to vote on the changes to the Constitution announced in the June 2015 newsletter. The changes relate to the removal of the requirement for membership fees, the establishment of chapters within the association, and for consistency with the ACS Regulations.

The only nominations received thus far for the 2015/16 committee are those from the outgoing committee members. Nominations should be forwarded to the aSCSa Chairman, BJ Martin.

National Committee (to be confirmed)

BJ Martin	Chairman (ACT)
Clive Boughton	Immediate Past Chairman (ACT)
(Vacant)	Secretary (VIC)
George Nikandros	Treasurer (QLD)
Drew Rae	(QLD)
Holger Becht	(QLD)
Tariq Mahmood	(VIC)
Derek Reinhardt	(NSW) (currently in the UK)
Luke Wildman	(QLD)
Rob Worthington	(VIC)
Web Site	www.safety-club.org.au

Drew Rae and Holger Becht joined the committee during 2014/15.

Kevin Anderson, Chris Edwards, Tony Cant, Allan Coxson, and Antony Acfield have decided to step down.

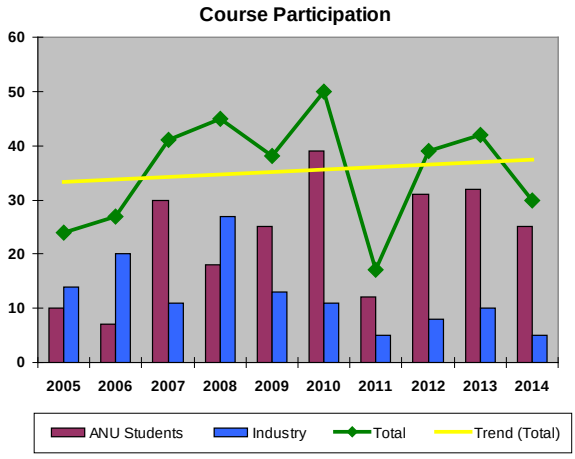
Professional Development

THE UNIVERSITY of York
Department of Computer Science

ANU
THE AUSTRALIAN NATIONAL UNIVERSITY

Introduction to Systems Safety

After ten consecutive years, the Australian National University has advised that they would now be offering the course to students every second year from 2014. The next ANU offering will be 4 to 8 April 2016 (see advert).



aSCSa

acs AUSTRALIAN COMPUTER SOCIETY

Griffith UNIVERSITY

Introduction to Systems Safety

As announced in the June 2015 newsletter, the aSCSa hosted the "Introduction to System Safety" course developed by the University of York, in Brisbane in September 2015. The aSCSa contracted Griffith University to deliver the course on behalf of the aSCSa. The course was delivered by Drew Rae.

There were eleven industry attendees, coincidently all from the rail industry.

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.

Introduction to System Safety

The Introduction to System Safety course is a five-day primer in system safety engineering. The course contains a mix of lectures, discussions and small group exercises, supported by Australian and international examples.

Whilst the course touches on broader issues in theorizing risk and managing safety within organisations, its main focus is to equip safety practitioners with the practical understanding necessary to engage with safety activities.

The course was developed by the University of York for their MSc in Safety Critical Systems Engineering program. The course is jointly hosted by the aSCSa and ANU.

Content:

The course is structured according to the engineering lifecycle of a service or physical system, and covers:

- Concepts and terminology for safety
- Overview of the engineering lifecycle from a safety perspective, including the role and intent of key safety activities
- Hazard identification and setting of safety requirements
- Techniques for safety analysis to support design, including:
  - Failure Modes and Effects Analysis (FMEA)
  - Functional Failure Analysis (FFA
  - Hazard and Operability Studies (HAZOP)
  - Fault Tree Analysis (FTA)
- Safety cases, including notations for recording arguments and evidence
- Specific issues in safety analysis, including, Human Factors, Software and Data Safety.

Presenters:

The course is a University of York course and will be presented Dr Mark Nicholson, Senior Research and Teaching Fellow, University of York and Dr Drew Rae, Program Director of the Graduate Certificate in Safety Leadership at Griffith University.

Australian National University

CSIT Building 108, Room N101

(Room to be confirmed

Canberra, ACT

04 to 08 Apr 2016

GST Inclusive Fees
$2750 (Member), $3080 (Non-Member)

Registration opens mid-January 2016
Check ACS Events

For more information contact Dr Clive Boughton

EDITORIAL

Urgent need to raise awareness of system safety in the ICT industry

The failure of Queensland Education's OneSchool IT system to pass on suspected child abuse to police highlights the level of ignorance of system safety standards. The failure to report was, according to the investigation report by Deloitte, due to the lack of project oversight and governance, and people undertaking tasks for which they were not competent to perform. The Deloitte investigation in reaching their findings, conclusions and recommendations did not refer to system safety standards. In fact the only use of the word "safety" in the Deloitte report is in the phrase "child safety"; nowhere in the report is there any mention of safety requirements, safety integrity, or hazard analysis.

The functionality to pass on reports of suspected child abuse to police was a later add-on; it was in response to recommendations of the Queensland Child Protection Commission of Inquiry Report (the Carmody Report) issued in July 2013. Clearly this functionality is "safety-related" and as such the OneSchool technology platform, system architecture and application as a whole should have been reviewed as to its appropriateness to host the safety-related suspected child abuse reporting function.

Failure to recognise suspected child abuse reporting as a safety-related function by all those involved with the procurement, development, operation and maintenance of the OneSchool IT system and by the investigator commissioned by the Queensland Government, demonstrates the level of ignorance of safety standards for systems containing software by the general IT industry. A level of ignorance which needs addressing urgently.

Wireless Carjackers

From Page 1

In a control test to demonstrate the vulnerability of the Uconnect feature, the Jeep whilst travelling at a speed of 70 mph, the test driver (without touching the dashboard controls) reported that the vents in the Jeep started blasting cold air at maximum setting. Next the radio changed channel and blared at full volume. The volume control and power button were of no avail to quieten or turnoff the radio. Next the windshield wipers turned on.

As the hackers continue their attack from a laptop 10 miles away, the Jeeps transmission system was disabled; the accelerator stopped working, and the Jeep lost half its speed and then slowed to a crawl.

The most disturbing manoeuvre was when the hackers disabled the Jeep's brakes resulting in the 2-ton SUV sliding uncontrollably into a ditch.

The Hack

The attack by Miller and Valasek was through the Wi-Fi facility in Uconnect. The attack was directed to a specific chip in the vehicle's entertainment system. The nature of the attack was in the rewriting the chip's firmware to plant their code. That rewritten firmware was then capable of sending commands through the car's internal computer network, known as a CAN bus, to its physical components like the engine and wheels.

The Impact

On July 24, 2015, Chrysler issued a recall for 1.4 million vehicles as a result of the research of Miller and Valasek. Chrysler has also blocked the ability to launch an attack using Sprint's cellular network to protect vehicles with the vulnerable software (Uconnect computers are linked to the Internet by Sprint's cellular network).

Safer Schools?

In August 2015, the ABC reported on that Queensland Government IT system OneSchool failure in which more than 600 suspected cases of child abuse (reported by school principals) were not forwarded to police.

Education Minister Kate Jones launched internal and external reviews and a manager and a contractor who worked on the system were stood aside. In a media release, Kate Jones announced that Deloitte Australia will undertake an independent investigation of the Department of Education's failed implementation of an update of OneSchool that resulted in suspected cases of child abuse not being reported to police. The update was designed to allow principals to report suspected child abuse directly to Child Safety and Queensland Police.

The software defect related to reports of child abuse that were directed to only the Queensland Police Service. The fault prevented these reports from being received.

In October 2015, Kate Jones announced in a media statement that during their investigation, Deloitte carried out a full forensic search of OneSchool Student Protection Reporting emails. They identified 344 reports dating back to 2013 – in addition to the original 644 – for which they were unable to verify receipt by Police or Child Safety.

Some of the key findings of the Deloitte Report included

- The process formality (reviews and oversight) in place for implementing changes to the OneSchool application had been reduced for the development and release of smaller changes.
- The OneSchool technology team did not apply an integrated software development life-cycle approach, hence risking the quality of the key project artefacts.
    - Individuals in the OneSchool technology and operations teams assumed (developer and tester) roles such as and responsibilities that would typically be divided amongst multiple individuals in line with accepted ICT industry good practice.
- Some project team members were performing key project roles without the appropriate skills and experience.
- The criteria used to assess the impact of changes to the OneSchool Student Protection Module were insufficient to appropriately assess risk. Assessing application enhancements was biased toward size, cost and complexity of delivery as opposed to the consideration of the potential business, stakeholder and technical implications of the changes.
- High risk and impact changes were not assessed and treated individually; all changes were assessed as a group under a single master change.
- The Student Protection Module did not consider the wider business and information security implications of adopting email as the transmission method. There is no guarantee that an email is delivered.

Basis of the investigation

The review by Deloitte was not structured as a compliance audit. However the following industry good practices were considered in determining the findings and recommendations:

- CMMI: Capability Maturity Model Integration – a guide for process improvement in projects, divisions or organisations
- COBIT: Control Objectives for Information and Related Technology – a framework and toolset for IT management governance control
- ITIL v3 and ISO 20000: Information Technology Infrastructure Library – a set of practices for IT service management that focus on business requirements
- ISO 12207 Systems and Software Engineering – Software Lifecycle Processes for developing and maintaining software
- ISO 14764 Systems and Software Engineering – Software Development Lifecycle Maintenance
    - ISO 9126 Software Engineering – Software Quality: Quality model for software

development and operation [*now ISO 25000: Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE)*].

- International Software Testing Qualification Board – Testing qualification certification organisation
- V-Model – Software development process

The fallout

According to an ABC news item (21-Oct-2015), two senior Queensland Department of Education officers, an assistant director-general and an executive director in relation to the OneSchool failure, were sacked for their roles in an IT bungle that prevented almost 1,000 cases of possible child abuse being reported to police. A *show cause* notice was also issued to another departmental officer.

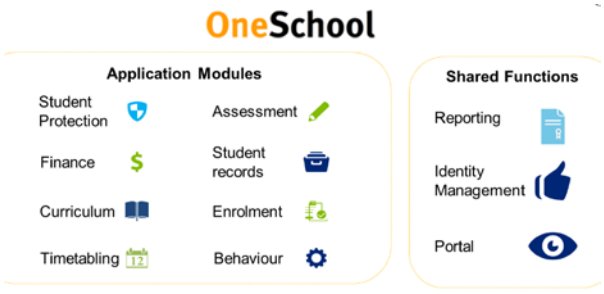
Two contractors who were directly responsible for coding and testing the upgrade have already had their contracts terminated.

About OneSchool

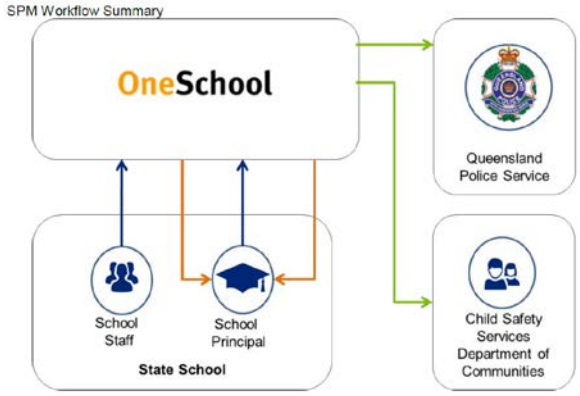
The OneSchool system provides Queensland State Schools with a range of business functionalities. The system consists of a number of integrated software modules which work together in order to provide schools with support for the following:

- Student management
- Curriculum and learning management
- Finance and asset management
- Resource management
- Performance, reporting and analysis
- Student protection

The OneSchool application has been progressively enhanced since its first release in 2008 including releases in 2009 (Release 2), 2010 (Release 2.1), 2011 (Release 3), and in October 2013 (Release with the Student Protection Module).



OneSchool Functionality



OneSchool Student Protection Module Workflow

So what did go wrong? Why police never received hundreds of alleged abuse reports?

The following is from an article in Information Age.

According to Deloitte, a "significant number" of Student Protection Reports were being sent to Queensland Police that "did not meet evidential standards". A software update was scheduled in January 2015 "to reduce this from occurring" and ensure only the most serious reports were referred to police.

The software update was created by a third party developer who mistakenly left an old logic step in the code that caused referrals to police to fail.

Deloitte found the update was not peer reviewed before being released to a testing environment – a best practice method of detecting defects in code early. The reason cited was that it "was not a documented requirement within OneSchool" change management process.

The code was passed straight to a tester, who Deloitte found used inadequate test scripts and incorrectly interpreted test results. As the testing was not done by the OneSchool developer Testing team there were no test scripts developed and approved, Testing was performed by the OneSchool Education Business Support team although Deloitte found no documentary evidence.

It was subsequently passed and signed off as "production ready" by executives, allowing it to progress through a change stakeholder committee and "into the live production environment" on January 19, 2015.

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.

Tail-strike - QANTAS

Source: ATSB Report AO-2014-162

On August 01, 2014 a Qantas Boeing 737-838 suffered a tail-strike during take-off from Sydney Airport for a scheduled passenger service from Sydney NSW to Darwin NT.

The tail-strike was reported by a cabin crew member while the aircraft was climbing to cruise level. The crew member reported hearing a "squeak" during rotation.

Suspecting a trail-strike, the flight crew worked through the trail-strike checklist which did not reveal any indication of a trail-strike event. During the checklist process, the captain recalled seeing the "dumb bell" symbol in the head-up guidance system during take-off indicating that the tail-strike pitch limit was reached. The flight continued to Darwin as normal.

After landing, the captain noticed some paint was scraped off the protective tailskid, indicating that the tail had just made contact with the ground during take-off. However the contact was not sufficient to result in activation of the tail-strike sensor.

Head-up guidance system

The Boeing 737 has a head-up guidance system (HGS) fitted on the captain's side. The HGS overlays various flight parameters and navigation data in line with the captain's outside view. This enables the captain to access, among other parameters, aircraft speed while maintaining view of the runway.
During rotation, the aircraft tail strike pitch limit symbol will appear when the aircraft is approaching the tail strike angle. As well as the tail strike pitch limit indication, the aircraft reference symbol is also displayed and if the two symbols come in contact, a tail-strike has probably occurred.

The ATSB found that the tail-strike was the result of two independent and inadvertent data entry errors in the calculation of the take-off parameters. The errors resulted in a 10 tonne lower weight being used in the calculation. The lower weight resulted in the calculated take-off speeds and engine thrust settings for take-off being too low.

The Errors

One of the data entry errors involved the captain, who recorded zero fuel weight and fuel load on a notepad in order to derive the take-off weight. It was during this calculation that the leading "1" was dropped from the (10,000 kg) fuel figure, resulting in a take-off weight of 66,400 kg (the weight should have been 76,400 kg). The 66,400 figure was entered into the captain's on-board performance tool to derive the take-off speeds and engine setting.

The second error occurred when the first officer entered the take-off weight into their on-board performance tool. While the first officer correctly reported the zero fuel weight and fuel weight to get the take-off weight value of 76,400 kg, the actual weight entered was 66,400 kg; a simple data entry error.

As the take-off weight figures of 66,400 kg "matched" when the flight crew compared them, the error was not detected.

The take-off weight of 66,400 kg was not unusual and hence provided no prompt to re-check. Apparently the captain had had recent experience with similar take-off weights.

Due to runway variances, the calculated take-off speeds and engine thrust settings will vary for same take-off weight such that the calculated take-off speed and engine thrust settings seemed sensible even for a 76,400 kg take-off weight.

A risk to be managed

This is not the first time for such data entry incidents. In March 2009, an Emirates Airbus A340 suffered a tail-strike on take-off from Melbourne airport, resulting in significant damage to the aircraft and airport infrastructure. According to the ATSB report, the error was due to a significantly low take-off weight being used to determine the take-off speed and engine thrust settings.

Data input errors remain a significant safety concern. According to the ATSB, the correct operating data is a foundational and critical element of flight safety, but errors in calculation, entry, and checking of data are not uncommon.

Factory of the future

The IEC Market Strategy Board (MSB) released the Factory of the Future White Paper at the 79th IEC General Meeting in Minsk.

The White Paper assesses the potential global needs, benefits, concepts and pre-conditions for the factory of the future; it identifies the business trends in related technologies and markets, and their impact on data, people, technologies and standards.

The ultimate goal of the factory of the future is to interconnect every step of the manufacturing process. Factories are organizing unprecedented technical systems integration across domains, hierarchy, geographic boundaries, value chains and life cycle phases. This integration will only be a success if the technology is supported by global consensus-based International Standards.

The White Paper was developed by the IEC Market Strategy Board (MSB) in cooperation with the Fraunhofer Institute for Manufacturing Engineering and Automation IPA.

iRobot Car

The robotic laws of Isaac Asimov surfaced in an article published in the Sydney Morning Herald.

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2. A robot must obey orders given it by human beings except where such orders would conflict with the First Law.
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

Eric Schwitzgebel, a professor of philosophy at UC Riverside who wrote the article for the Los Angeles Times, poses the question “Will your driverless car kill you so others may live?”

This isn't an idle thought experiment. Driverless cars will be programmed to avoid collisions with pedestrians and other vehicles. They will also be programmed to protect the safety of their passengers. What happens in an emergency when these two aims come into conflict?

According to the article, whilst road regulators are trying to draft safety regulations for autonomous vehicles, Google, which operates most of the driverless cars being street-tested in California, prefers that the regulators not insist on specific functional safety standards. Instead, Google proposes that manufacturers "self-certify" the safety of their vehicles, with substantial freedom to develop collision-avoidance algorithms as they see fit.

How rigid should vehicle safety regulations be? Should there be consumer freedom to allow people the opportunity to choose collision avoidance algorithms that reflect their values and risk appetite?

Whilst the robot car will never get drunk and always drive with due care and attention, who will pay the fine if it speeds though a temporary speed restriction zone? Who is responsible if the robot car swerves to avoid a collision with another road vehicle only to collide with a pedestrian on the side of the road?

We thank our 2015 System Safety Conference Sponsors