Safety-Critical Systems Club

Seminar Information

6th December 2016
Hilton London Green Park Hotel, London

New Challenges in Systems Safety
New Challenges in Systems Safety

December 6th 2016
Hilton London Green Park Hotel, London

Programme

09:30  Registration and coffee

09:45  Introduction

09:50  Ken Wallace  
BAE Systems  
Addressing The Emerging Challenges of Software Heavy Systems Through Evidence-Based Practice

10:35  Ibrahim Habli  
York University and  
Sean White  
NHS Digital  
Mind the Gap – addressing the variability of clinical practice in Health IT Safety Management

11.20  Bob Oates  
Rolls-Royce  
Future Challenges for Data Safety

12:05  Lunch

13:00  SCSC update

13:05  Chris Johnson  
University of Glasgow  
The Role of Offensive Techniques in the Cyber Defence of UK Critical Infrastructure

13:50  Michael Fisher  
University of Liverpool  
The Problem with Autonomy

14:35  Tea

15:00  Bernard Twomey  
Bernard Twomey Consulting Ltd  
The 'cyber enabled ship' - What does it mean for the operators and regulators?

15:45  Alex Wilson  
Wind River  
E-enabled Aircraft

16:30  Panel Discussion  
Led by Paul Hampton, CGI  
An open discussion between the presenters and the delegates covering the issues raised during the day.

17:15  Close and opportunities for networking
Addressing The Emerging Challenges of Software Heavy Systems Through Evidence-Based Practice

Ken Wallace
BAE Systems

ABSTRACT

A response to rising societal demands and expectations, evidence-based practice (EBP) has emerged in disciplines such as medicine and education as a means of managing complex socio-technical systems and the challenges these systems present. More recently evidence-based practice has been adapted as the basis for Evidence-Based Software Engineering (EBSE): an approach that seeks to achieve comparable outcomes in respect of the practice of software engineering. This talk considers how such practice can contribute to effective treatments of the emerging challenges that current and future generations of complex software-intensive systems present. It does so by reference to the application of EBP in the development of advanced naval platforms. Although defined historically by their physical characteristics such vessels are evolving into complex systems-of-systems heavily dependent upon software to achieve their intended operational capabilities.

~

Ken Wallace has been with BAE Systems and antecedent companies since 2001 having previously held management and engineering positions in a number of SMEs working on the development and application of software-intensive systems. Prior to this he spent a number of years in academia in the field of neuroscience. Since joining BAE he has continued his involvement in the development of large-scale software-intensive systems in both engineering and management capacities. He retains links with academia having previously acted as an Associate Lecturer in Computing with the Open University and through participation in software engineering research initiatives. A Chartered Engineer, Ken is a Fellow of the IET and a member of the IEEE and INCOSE
Mind the Gap – addressing the variability of clinical practice in Health IT Safety Management

Ibrahim Habli
York University

Sean White
Senior Safety Engineer
NHS Digital

ABSTRACT

Health IT (HIT) is deployed in dynamic health and social care environments where high degrees of variability are often deemed irreducible. That is, flexibility in clinical practice is seen as inevitable in order to deal with different patient cohorts, health conditions and social settings. For such complex environments, HIT safety analysis and management is challenging as most hazardous behaviours emerge only once the organisational, human and technology elements interact within different clinical and social care settings. In this talk, we examine the challenges involved in assuring the safety of HIT, drawing on the findings of a series of multi-disciplinary workshops and structured reviews of domain-specific safety cases. We discuss current initiatives within NHS Digital for promoting and establishing systematic safety management practices for modelling the care settings and the HIT functionality and developing and maintaining the hazard log and safety case in an integrated, traceable and collaborative manner.

~

Ibrahim Habli’s interests are in software engineering and safety-critical systems. He maintains active collaborative links with the aviation and automotive industries and more recently with healthcare. He currently holds a Royal Academy of Engineering Industrial Fellowship that funds a collaborative project with NHS Digital on evidence-based assurance of health IT safety. He teaches on the University of York’s postgraduate and CPD programmes in system safety engineering and supervises a number of PhD students, mainly in the field of safety assurance.

Sean White is a Senior Safety Engineer at NHS Digital and has provided safety assurance for large scale projects such as the Electronic Prescribing Service, Patient Demographic Service and acute Trust’s EPR and PAS systems. He has made a significant contribution to NHS Digital’s revised safety training courses and frequently delivers the associated training. He is a co-author and Maintenance Manager of the national health IT system safety standards SCCI 0129 and SCCI 0160 and contributed to IEC/TR 80001-2-4:2012. He also co-authored NHS Digital’s Clinical Safety Management System. He is currently working with Ibrahim Habli at the University of York exploring evidence based approaches to assuring health IT.
Future Challenges for Data Safety

Robert Oates
Product Cyber Security Specialist, Rolls-Royce’s Software Centre of Excellence
Cyber Security Lead, Rolls-Royce’s Ship Intelligence programs

ABSTRACT

The SCSC’s data safety guidance has been formed through the sharing of knowledge and experience across a number of different organisations, crossing sectors, and spanning a range of system platforms and architectures. However, the future promises new and exciting technologies and an explosion in the volume and uses of data within industrial settings. How will technical trends such as the Internet of Things, Cloud Computing and Machine Learning interact with data safety? How can we embrace the colossal benefits without exposing people and organisations to colossal risks?

~

Dr Robert Oates is a Product Cyber Security Specialist for Rolls-Royce’s Software Centre of Excellence and the Cyber Security Lead for Rolls-Royce’s Ship Intelligence programs. He is a member of the IET and the (ISC)2 and a Certified Ethical Hacker through the EC-Council. His primary technical interest is exploring how safety and security interact and specifically the security of safety critical systems that form part of the critical national infrastructure. His PhD was awarded by the University of Nottingham and was an exploration of biologically inspired security techniques and their application to mobile robotics.
The Role of Offensive Techniques in the Cyber Defence of UK Critical Infrastructure

Chris Johnson
Professor and Head of Computing
University of Glasgow

ABSTRACT

The Chancellor of the Exchequer recently announced a robust change of public policy, stressing that the UK must be able to retaliate against cyber-attacks when foreign actors are developing techniques that threaten the country’s electrical grid and airports. In this talk, I will summarise publicly available information about recent attacks and provide an engineer’s view of the technologies that can be used to implement Philip Hammond’s response to these threats. In particular, I will introduce the cyber-range in Glasgow, which supports pen testing for SCADA/industrial control systems. At the end of the talk, I will summarise the ethical issues that arise when cyber weapons are proposed to deter others from launching future attacks.

~

Chris Johnson is Professor and Head of Computing at the University of Glasgow. His research focuses on the cyber security of safety-critical systems. He supported the United Nations in improving the cyber security of Chemical, Biological, Radiological and Nuclear facilities (CBRN).

Johnson designed the cyber incident reporting processes under Article 13a of the Framework Directive (2009/140/EC) and Article 4 of the e-Privacy directive (2002/58/EC) on behalf of the European Network and Information Security Agency (ENISA). Prior to that he helped develop European guidelines for contingency planning in aviation for EUROCONTROL and accident investigation for the European Railway Agency.

Johnson has held fellowships from NASA (Langley Research Centre and Johnson Space Centre) and the US Air Force. He also supports safety and cyber security in the US Navy and the Federal Aviation Administration.

In 2016, Johnson was elected to the UK Computing Research Committee. He was also appointed to the EPSRC Strategic Advisory Team. Since 2014, he has been a member of the Scottish Government's Public Sector Cyber Resilience group. He helps to lead the Scottish Universities Computing Science Alliance (SICSA) in cyber security. Previously, Johnson chaired the scientific advisory board to the EC SESAR programme for the modernisation of Air Traffic Management. He helped develop cyber risk assessments for both the aviation and maritime industries on behalf of the UK Department of Transport; reporting to the Cabinet Office.
The Problem with Autonomy

Michael Fisher
Professor of Computer Science and
Director of the multi-disciplinary Centre for Autonomous Systems Technology
University of Liverpool

ABSTRACT

Autonomous systems must make their own decisions, increasingly without direct human control. They are set to become more prominent in our homes, workplaces, and environment. But can we be sure what these systems will do and, crucially, that these systems will always make the decisions we would want them to? In this talk I will examine high-level decision-making in autonomous systems, the formal verification of this decision making, and the impact of this verification on safety, legality, ethics, trust, etc.

Michael Fisher is Professor of Computer Science and Director of the multi-disciplinary Centre for Autonomous Systems Technology (www.liv.ac.uk/cast) at the University of Liverpool. He is a Fellow of both the BCS and the IET, is on the editorial boards of both Applied Logic and Annals of Mathematics and Artificial Intelligence journals and is a corner editor for the Journal of Logic and Computation.

Prof. Fisher's research mainly involves formal verification for the certification, safety, ethics, and reliability of autonomous systems, and he has led numerous EPSRC projects (currently on "Verifiable Autonomy" and "Science of Sensor Systems Software"). He is a member of the British Standards Institution committee on "Robots and Robotic Devices" and leads the "UK Network on the Verification and Validation of Autonomous Systems" (vavas.org).
The ‘cyber enabled ship’
What does it mean for the operators and regulators?

Bernard Twomey
Director
Bernard Twomey Consulting Ltd

ABSTRACT

Can you disable a ship or sink a ship through the use of data - fact or fiction? The introduction of ‘Cyber Technology’ into the marine environment has certain benefits, ranging from increased efficiencies through to remote diagnostics, remote operations and ultimately full autonomy. This technology is not an exact substitute for electromechanical and/or crew tasks but they can provide opportunities for improved situation awareness and a host of manufacturers declared benefits. But what is the impact if these systems are not designed or managed in a systems engineering context? Is it possible to disable a ship or even sink it through the use of data? This will be a discussion with examples given of the practical experience to date.

~

Bernard Twomey has just left Lloyd’s Register where he spent 23 years ending up as the Global Head of Electrotechnical Systems. He is now an independent consultant to the marine industry; his previous experience includes 13 years in the Merchant Navy and deputy course director at Cranfield University. He is now involved with the assessment of emerging technologies and has close links with academic institutes to ensure that the potentially disruptive technologies now being proposed do not result in an unsafe state for the vessel, and actually provides business benefits for the clients. His research interests include assurance case management, and the dependability of “Systems of Systems”. He is an advisor to the UK NA on Power and Propulsion and supports academic research in areas of mutual interest.
E-enabled aircraft

Alex Wilson

Director of Business Development, Aerospace and Defence
Wind River

ABSTRACT

E-enabled aircraft provide increased connectivity for passengers and also allow increased bandwidth to implement new services such as predictive maintenance. However, this new connectivity introduces new security threats and exposes new vulnerabilities to aircraft that were previously isolated from commercial ground systems. To protect against these threats new standards are evolving that show how to analyse and protect systems.

This presentation examines the implementations of the well-known information security components of Confidentiality, Integrity, and Availability (the CIA triad) as applied to avionic systems and how these implementations can be used to defend against various attacks. It maps the new RTCA DO-355 standard to a commercial implementation of both an airborne ARINC 653 environment and to a ground based Linux implementation, and shows how you can satisfy these new requirements.

~

Alex Wilson obtained a BSc (Eng) in Electrical Engineering from Imperial College, London in 1986. Prior to Wind River, Alex worked at British Aerospace on Automated Test Equipment for various Inertial Navigation Systems using VME and RTOS technology. He then worked as a Field Applications Engineer (FAE) for Motorola Computer Group working with 68k and PowerPC VME boards and 3rd party Real Time Operating Systems. He joined Wind River in the UK as an FAE in 1996 supporting VxWorks and Tornado. In 2002 he became European Business Development Manager for Wind River focusing on the Aerospace and Defence market. As Director of Aerospace and Defence Solutions for Wind River, he is responsible for A&D business development strategy for EMEA and APAC, and is part of the Wind River Operating Systems Product Group.
Panel Chair

Paul Hampton
Safety Engineer and Sector Safety Consultant
CGI UK

Paul is a Chartered Engineer with over 25 years’ experience in IT. He has spent 15 of those designing and developing enterprise systems in sectors such as Energy & Utilities, Government, Criminal Justice and Health. He has been involved in Systems Safety for many years in a variety of capacities including safety engineering, independent auditing and corporate governance and assurance. He is the currently appointed safety engineer for a number of high profile CGI engagements and also acts as a Sector Safety Consultant at Business Unit level, policing all the units’ bids to ensure safety is considered in our proposals. More recently he has been working on certification cases for satellite based data links between controllers and aircraft, a precursor to revolutionising the future of aircraft control.

Paul is also active in championing system safety in the wider community and is a member of an industry steering group (the SCSC DSIWG) developing a new standard for data safety. He has published a number of articles and papers and has presented these at many industry seminars and symposiums. Recently he has been working in the Healthcare sector assessing how safety related data is managed in health organisations and is seeking to publish guidance for healthcare standards on how to manage the identified issues.