SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

www.scsc.uk/events

This seminar is an opportunity to hear a range of talks by industry experts on the practical integration of safety and security.

It is aimed at those involved in assurance activities in any sector. It will also be useful for those reviewing, auditing and regulating where both safety and security is involved.

Details of this and other events at: www.scsc.uk

How to integrate safety and security practice

www.scsc.uk

THE SAFETY-CRITICAL SYSTEMS CLUB

Seminar: Safety and Security Integration

26th April 2018, DoubleTree by Hilton Hotel - West End
92 Southampton Row, Bloomsbury, London WC1B 4BH

This seminar will look at the latest developments in practical integration of Safety and Security: in analyses, processes, management, assessments and assurance cases.

There will be a variety of speakers across a range of sectors explaining how these two critically important aspects of systems and services can work together in a coherent manner.

Practical techniques for integrating safety and security in a safety context across lifecycle phases will be identified. The ways in which risk assessments, analysis techniques and justifications, including assurance cases, can be linked and combined will be highlighted.

Methods that combine traditional safety analysis with cyber-based penetration testing practices and techniques to enable production of test cases will be described.

Real-life case studies and examples will be used to demonstrate the techniques, across the Rail, Aviation, Automotive and other sectors.

There will be a wrap-up session at the end of the afternoon chaired by Tim Kelly; Tim will summarise the day and present the way forward. It also gives the delegates a further opportunity to put further questions to the panel.

Cost and registration: To Club members the cost is £195, including lunch and refreshments (no VAT). Non-members pay an extra £95 for Club membership. Joining instructions and the programme will be sent to registered delegates about two weeks before the event. Delegates must book their own accommodation (if required).

Safety-Critical Systems Club: I would like to attend the seminar on Apr 26th, 2018

Name ..... Organisation .....

Address .....

Telephone ..... Email ..... Vegetarian: Yes/No

❑ I am not an SCSC member, so need to join and pay £290 ❑ I qualify for the SCSC member rate of £195

To pay by cheque, please enclose a cheque for £195 or £290, payable to: University of York

To pay by credit card, please complete the following: ❑ MasterCard ❑ Visa ❑ American Express

Name on card ..... Card number .....

Amount to be charged ..... Expiry date ..... Security No .....

Cardholder's Address .....

Booking and payment can now be made through the Safety-Critical Systems Club website.
Please see the Events page at www.scsc.uk/events to secure your place.

Please return this slip and payment to: Alex King, Department of Computer Science, University of York, Deramore Lane, York, YO10 5GH.
Phone: 01904 325402 Fax: 01904 325599 Email: alex.king@scsc.uk

Safety and Security Integration

April 26th 2018

DoubleTree by Hilton Hotel - West End, 92 Southampton Row, London WC1B 4BH

Programme

09:00	**Registration and coffee**	
09:25	**Introduction**	
09:30	**Paul Hampton** CGI	*Safety & Security of future SATCOM-based Aviation Data Links*
10:10	**Paul Dart** NCC	*Practical Methods to Integrate Cyber Security Testing and Safety Critical Systems*
10:50	**Coffee**	
11:15	**Nikita Johnson** University of York & BAE Systems	*Safety is from Mars, Security is from Venus: Exploring the Practical and Socio-technical Challenges of Safety-Security Co-assurance*
11:55	**Jan Tobias Muehlberg** KU Leuven	*VulCAN: Efficient Component Authentication and Software Isolation for Automotive Control Networks*
12:35	**Lunch**	
13:25	**SCSC Update**	
13:30	**Bob Oates** Rolls-Royce PLC	*A Data Focussed Approach to Mapping Security Failures to Safety Impacts*
14:10	**Andy Scott** NATS	*Aligning Safety and Security Risk Management*
14:50	**Tea**	
15:15	**Robert Stroud** Adelard LLP	*Security-Informed Risk Assessment for Safety Critical Systems*
15:55	**Andrew Eaton** CAA	*A model for addressing cyber security threats in behavioural safety cases*
16:35	**Panel Session**	A wrap-up session at the end of the day chaired by Tim Kelly. It also gives the delegates a further opportunity to put questions to the speakers
17:15	**Close and opportunities for networking**	

Safety & Security of future SATCOM-based Aviation Data Links

Paul Hampton
CGI

ABSTRACT

Ground to air data links, especially those utilising satellite-based communications, are increasingly seen as a way to resolve increasing congestion around controller/pilot radio comms in civil aviation. In the near future these links will be used to supplement existing communications and position reporting. This presents two challenges for the integration of safety and security: (i) spoofing of data link messages could result in major safety issues, yet applying traditional safety assurance methodologies can conflict with the security of the link in a dynamic and unpredictable threat landscape, (ii) the certification route for such systems is not well defined: historically, safety and security of European commercial aircraft have been treated separately from those of ground based systems. However, regulators are starting to realise that it may not be sustainable to consider ground and air segments in isolation. For example, there is little benefit in highly securing the aircraft side of a secure Air Traffic Control/Pilot network if the ground-based systems are easily compromised. Paul has been working in the safety and certification aspects of SATCOM-based datalinks for the last four years. He will present the challenges and current approaches used in integrating safety and security in this domain.

~

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 current appointed safety engineer for a number of high profile CGI engagements and in recent years has been working on certification cases for satellite-based data links between controllers and aircraft, the precursor to revolutionising the future of air traffic control.

Practical Methods to Integrate Cyber Security Testing and Safety Critical Systems

Paul Dart
NCC Group

ABSTRACT

Software is increasingly adopted in complex systems that require high dependability, e.g., control units in cars and commercial vehicles, interlocking systems for rail applications, marine and avionics systems or medical systems. For many of these systems, safety is a crucial aspect of dependability, since a malfunction may directly harm human beings. Therefore, such systems demands that various constructive and analytic measures are carried out to ensure the safety risks are correctly identified and appropriate treatments are defined, correctly implemented and demonstrated to be effective. With the convergence of IT and OT technologies, traditional model-based testing do not take into consideration information derived from networked non-safety critical rated systems or network protocols on safety critical networks. The paper sets forth a method that combines traditional safety analysis with cyber-based penetration testing practices and techniques such that test cases can be derived and integrated into both initial delivery and day-to-day assurance activities. Jim will discuss real world examples in transportation.

~

Paul is currently the Rail Technical Lead at NCC Group responsible for managing all rail work in for the Transport Assurance Practice worldwide. His background is working for Thales from radio design, through hardware specifications, systems integration and most recently working on 4LM re-signalling with London Underground. Paul joined NCC Group to be a subject matter expert in Rail and due to his previous work has lived in the sometimes muddy waters between security and safety. His security work has ranged from complete rolling stock network assessments to control centre penetration testing, and he has a particular interest in sharing good practice across industry verticals.

Safety is from Mars, Security is from Venus: Exploring the Practical and Socio-technical Challenges of Safety-Security Co-assurance

Nikita Johnson
University of York & BAE Systems

ABSTRACT

This talk aims to critically survey the current state-of-the-art techniques and standards for addressing safety-security co-assurance. It draws focus to the, often overlooked, socio-technical challenges that serve as barriers to integrating the two attributes. It concludes by identifying possible future directions and opportunities.

~

Nikita Johnson is a PhD student in the High Integrity Systems Engineering research group at the University of York. Nikita has a background in Computer Science and Artificial Intelligence and has worked on projects managing Big Data and risk for IBM and Lloyds Banking Group. Nikita is currently working with BAE Systems to develop a safety-security assurance framework for complex systems-of-systems such as UASs.

VulCAN: Efficient Component Authentication and Software Isolation for Automotive Control Networks

Jan Tobias Muehlberg
KU Leuven

ABSTRACT

Vehicular communication networks, specifically CAN, have been subject to a growing number of attacks that put the safety of passengers at risk. This results in millions of vehicles being recalled and lawsuits against car manufacturers. While recent standardisation efforts, e.g. AUTOSAR, address security of CAN networks, no such solutions are implemented in current cars.

In this talk I will outline attacks against automotive control networks and derive a basic threat model for these networks. I will present this in the light of the security features of AUTOSAR and discuss why these features are difficult to combine with safety requirements and economic constraints, while still being insufficient to protect against a range of established attacks.

I will further outline VulCAN, a generic solution to provide efficient and standard compliant message authentication in automotive control networks. VulCAN also implements software component attestation based on lightweight embedded trusted computing technology. This combination results in strong security guarantees that go beyond the standardised requirements. In particular, we protect against network attackers but also against substantially stronger adversaries capable of arbitrary code execution on electronic control units.

~

Jan Tobias Muehlberg works as a research manager at imec-DistriNet, KU Leuven (BE). He is active in the fields of software security, formal verification and validation of software systems, specifically for embedded systems and low-level operating system components. Tobias is particularly interested in security architectures for safety-critical embedded systems and for the Internet of Things.

Before joining KU Leuven, Tobias worked as a researcher at the University of Bamberg (DE), obtained a Ph.D. from the University of York (UK) and worked as a researcher at the University of Applied Sciences in Brandenburg (DE), where he also acquired his Masters degree.

A Data Focussed Approach to Mapping Security Failures to Safety Impacts

Bob Oates
Rolls-Royce PLC

ABSTRACT

The increased demand for higher-performance safety-critical systems in turn drives increased connectivity and software complexity. However, digital technologies introduce new risks in the form of vulnerabilities to cyber-attack. For a modern cyber-physical system to be safe, it must also be secure. This talk explores a technique for identifying the potential safety impacts of cyber-attacks, even if the attacker did not intend to undermine the safety case of the system. It does so by mapping between traditional cyber-security properties and the data safety properties highlighted by the SCSC's Data Safety Working Group. The result is a bridge between the disciplines of safety and security that can lead to more effective trade-off analysis and more resilient systems.

~

Dr Robert Oates is the Head of the Global Software Capability Team for Rolls-Royce. His specialism is Product Cyber Security, specifically, the interaction between engineering for safety and engineering for security. He is responsible for the organisation's global software capability strategy and acts as a consultant on projects in the marine, aerospace, defence and nuclear sectors.

Aligning Safety & Security Risk Management

Andy Scott
NATS

ABSTRACT

Increasing attention is being given by service providers and, (where present) their Regulators, to demonstrating control of security-related causes to safety hazards. However, safety and security do not typically describe or manage risk in equivalent ways.

This talk will look at a number of models for aligning safety and security risk management that have been explored by an Air Navigation Services Provider, as a stepping-stone toward greater integration of these two risk domains. It will reflect on the relative merits and impacts of each model with a particular focus on the design and implementation of future change to operational services and will also consider the implications for the risk management framework once a change has been deployed.

~

Andy has been a Systems Safety Engineer for 15 years, with the last 7 years spent working for an Air Navigation Services Provider (ANSP). He is the ANSP's Business Process Expert for the safety assessment of change and will sit on the Civil Air Navigation Services Organization (CANSO) Assessment of Changes Expert Group. Andy is currently developing the roadmap for the ANSP's future integration of safety and security risk management, to accommodate both the continually evolving Regulatory environment as well as to better serve the needs of the company's on-going business transformation programme

Security-Informed Risk Assessment for Safety Critical Systems

Robert Stroud
Adelard

ABSTRACT

In this talk, I will discuss some general approaches towards security-informed risk assessment and some of the challenges for security-informed safety, before describing the approach we have developed at Adelard for doing security-informed risk assessment for safety critical systems. The talk will be illustrated with examples from our experience of assessing the security of railway systems.

~

Robert Stroud is a Principal Consultant at Adelard LLP with a background in security and fault tolerance. He has worked on behalf of government and the rail industry on a number of projects concerned with the security of ERTMS and is a member of the High Integrity Systems Group at the Railway Standards and Safety Board (RSSB). He has a particular interest in security-informed safety and has developed and delivered a course on security-awareness for railway safety engineers to over 200 railway professionals. Prior to joining Adelard, he was a Reader in Security and Dependability at City University London and University of Newcastle upon Tyne.

A model for addressing cyber security threats in behavioural safety cases

Andrew Eaton
CAA

ABSTRACT

A now often-heard quotation is that "An unsecure system cannot be a safe system". This presentation looks at how an objective behavioural safety case needs to be informed by cyber security assurance measures and analysis to be considered valid. Fundamentally, the safety argument requires any additional cyber-induced behaviour to be identified and evaluated for its potential impact on the system, and then assurance to be given of the safety of any cyber-induced changes in behaviour, taking into account responses to such changes, when detected.

~

Andrew Eaton is a National Requirements & Strategy Specialist for the Safety Regulation Group of the United Kingdom Civil Aviation Authority. His field of responsibility is safety assurance of safety-related Air Traffic Control and Management services. In this role he is responsible for advancing the UK's capabilities in these areas and consequently sits on several international standards and regulatory committees. Andrew has worked for the Civil Aviation Authority's Safety Regulation Group for the past twenty-eight years and has an MSc in safety-critical systems engineering from the University of York.