Safety-Critical Systems Club

Seminar Information

4th April 2019

Hilton London Euston Hotel, London

Evolution of Assurance Case Practice

Evolution of Assurance Case Practice

Thursday 4th April 2019

09:00 – 09:30	Registration and Coffee	
Main Programme		
09:30 – 09:35	Introduction	
09:35 – 10:20	Robin Bloomfield Adelard	**Evolution of Assurance Cases for Autonomous Systems**
10:20 – 11:05	John Birch Horiba MIRA	**What's the case for safety in Automotive?**
11:05 – 11:35	Coffee	
11:35 – 12:20	Tim Kelly, Simon Foster and Nungki Selviandro University of York	**Evolving Assurance Case Practice using the Structured Assurance Case Metamodel (SACM) 2.0**
12:20 – 13:20	Lunch	
13:20 – 13:25	SCSC Events Update	
13:25 – 14:10	Tim Kelly, Simon Foster and Nungki Selviandro University of York	**Evolving Assurance Case Practice…ctd.**
14:10 – 14:55	Andy Scott NATS	**Assurance Cases for Air Traffic Services**
14:55 – 15:25	Tea	
15:25 – 16:10	Paul Chinneck Altran Yvonne Oakshott Leonardo	**Dialectic Arguments**
Extras		
16:10 – 16:50	Panel Session	**A wrap-up session chaired by Mike Parsons giving delegates an opportunity to put further questions to the speakers**
16:50	Tea and snacks with opportunities for networking	

Evolution of Assurance Cases for Autonomous Systems

Robin Bloomfield
Adelard

ABSTRACT

This talk will describe how we have been evolving the CAE (Claims, Arguments and Evidence) methodology in the light of experience, research on informal logics and the challenge of assuring autonomous vehicles.

~

Robin E Bloomfield FREng is a founder of the specialist safety and security consultancy Adelard LLP and is Professor of System and Software Dependability at City University London. His work in the past 30 years has focused on the need to evaluate, challenge and communicate the trustworthiness of critical infrastructures and computer-based systems and has combined policy formulation, engineering and research.

What's the case for safety in Automotive?

John Birch
HORIBA MIRA Ltd

ABSTRACT

The automotive industry is experiencing a period of unprecedented change with the move to shared, electric and autonomous road-based transportation services. The purpose of this talk is to take a look back at the journey that the industry has been on with regards to safety assurance before looking at, and evaluating, current practice and how the industry might address its forthcoming challenges.

~

John Birch is a Functional Safety Chief Engineer at HORIBA MIRA Ltd. He is a Chartered Engineer and holds a post-graduate certificate in Systems Safety Engineering from the University of York. He is co-author of the MISRA 'Guidelines for Automotive Safety Case Arguments' document, first-named author of a number of academic papers and named inventor on several patents in the field of functional safety.

Evolving Assurance Case Practice using the Structured Assurance Case Metamodel (SACM) 2.0

Tim Kelly, Simon Foster and Nungki Selviandro
University of York

ABSTRACT

The Structured Assurance Case Metamodel (SACM) is an Object Management Group (OMG) standard that has been developed over the last ten years. Now at version 2.0, SACM has been defined to supported well established and widely used approaches to structuring assurance cases, such as the Goal Structuring Notation (GSN) developed by the University of York, and the Claims-Argument-Evidence approach developed by Adelard. Over the years, there have been several developments of GSN, including Assurance Case Patterns (in 1997) and Modular Safety Case Construction (in 2001). SACM incorporates and extends these developments within a new unified standard. Alongside this, SACM has been designed not only to support current practice, but also to provide an enabling framework for new developments in assurance case practice, such as improved support for dialectic argumentation, better management of evidence, reasoning about confidence, automated reasoning support for assurance case arguments, and dynamic assurance cases that are processed and executed at run-time. This talk will introduce SACM 2.0 and explain how it support both current and emerging assurance case practice.

~

Tim Kelly is Professor of High Integrity Systems within the Department of Computer Science at the University of York. He is best known for his work on system and software safety case development. His research interests include safety case management, software safety assurance, modular certification, and the certification of adaptive and learning systems. He has supervised many research projects in these areas with funding that spans industry, government, research councils, and the European Union. He has published over 150 papers on high integrity systems development and justification in international refereed journals and conferences. He has also been involved the development of a number of international standards in the area of system and software safety assurance (such as the automotive standard ISO 26262).

Nungki Selviandro is a PhD student in the Department of Computer Science at the University of York, under the supervision of Tim Kelly and Richard Hawkins. He is a member of the High-Integrity Systems Engineering research group. Nungki is currently working on the development of an approach in designing an argumentation notation, specifically, the development of the SACM argumentation notation.

Simon Foster is a postdoctoral research fellow in Computer Science from the University of York. He has worked predominantly in formal methods, and in particular the application of the Isabelle/HOL theorem prover to build automated verification tools. He is currently undertaking an EPSRC-UKRI Innovation Fellowship called CyPhyAssure, which aims to produce technology for mechanical assurance case development with evidence provided by a variety of integrated formal methods

Assurances Cases for Air Traffic Services

Andy Scott
NATS

ABSTRACT

This talk will look how an Air Navigation Services Provider is changing the scope and structure of its Safety Cases in response to a number of external and internal drivers. It will explore some of the implications of broadening the focus to an overall 'Assurance Case' and summarise the approach being adopted for the alignment of safety and security risk management.

~

Andy has been a Systems Safety Engineer for over 15 years, with the last 8 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 sits on the Civil Air Navigation Services Organization (CANSO) Assessment of Changes Expert Group. Andy is currently updating the ANSP's safety assessment procedures to reflect the revised EU common requirements for providers of air traffic management/navigation services, as draw a greater distinction between the treatment of services that directly influence safety risk vs. those lower-tier services that support them.

Dialectic Arguments

Paul Chinneck
Altran

Yvonne Oakshott
Leonardo

ABSTRACT

Assurance Cases have been criticised in the past for presenting a "rose-tinted" view of safety, by focussing on the resolution of positive safety goals. This talk explores what it means to constructively criticise an Assurance Case as part of its authorship, by using "dialectical argumentation" (to be explained during the talk!). It will touch on how to deal with necessary elements of any robust modern safety approach, such as counter-evidence, present a specific approach of checking the completeness of Assurance Cases, and include examples to demonstrate how has worked in the real world.

~

Paul Chinneck is a senior safety engineer at Altran UK, and a recognised expert in safety argumentation using GSN. He works mainly in the aerospace and defence industry, with specific expertise in unmanned systems, but has also applied his safety experience to automotive projects.

Yvonne Oakshott is a Principal Software and System Safety Engineer at Leonardo MW in Yeovil. She is a Chartered Engineer and has over 35 years of experience in the Aerospace sector. Yvonne was previously the software and programmable hardware assurance lead for a Leonardo aircraft; she is currently working on a cross industry project developing certification approaches for future air systems. She was a primary contributor to the development of the IAWG (Industrial Avionic Working Group) Modular Software Safety Case Process (IMSSC) from initial concept to final delivery into the public domain and to the subsequent application on a number of programmes, including Weapons Integration UK (WIUK). Yvonne is co-author of several papers and is an experienced presenter.