Institution: City University London

Unit of Assessment: 11 Computer Science and Informatics

Title of case study: Reducing risk in critical computer-based systems by using assurance cases

1. Summary of the impact

Failure of critical computer systems could result in death, injury, financial loss and damage to the environment. To help address this concern, academic staff at City University London have developed an approach to assurance case construction to demonstrate that the risk posed by critical computer systems is acceptably low. Initially the primary focus was the justification of safety-related systems in UK industry (i.e., by introducing more structure and rigour) but it has been extended to cover other aspects such as reliability and security and has been taken up internationally. This approach has been commercialised by a company with close links to City University London (Adelard LLP). The approach is used in critical areas including:

- the UK nuclear industry
- USA Food and Drugs Administration approval of new infusion pump designs for use in healthcare
- key elements of the UK financial infrastructure
- rail signalling and air traffic control.

Industry feedback has been positive and our assurance approach, in the form of updated regulations and procedures, has been adopted as standard practice in these sectors. This has led to significant and wide-ranging impact on practice and the consequent safety and security of systems, benefiting both the industries concerned and the public who use or are affected by their services.

2. Underpinning research

A safety case is a set of documentation justifying the safety of system within an organisation (such as the nuclear industry). While safety cases have a long history in the UK, the objective of our research was to define a sound justification approach that is more broadly applicable: an “assurance case”. The goal of an “assurance case” is to demonstrate that the risk posed by a critical system is low enough to be acceptable. Research undertaken in the Centre for Software Reliability (CSR) at City University London has highlighted the importance of taking into account disparate sources of evidence and marshalling them in a rational and structured way. Such justifications are designed to be open to review and audit (e.g., by regulators and by company safety departments).

The overall approach makes use of a generic “claim-based” framework where claims (e.g., about security or safety) are supported by rigorous arguments that link to the underlying evidence. The research underpinning this approach included:

- deriving methods for structuring safety justifications based on a “Claims, Arguments, Evidence” structure (CAE) which can represent the justification in a graphical form
- rigorous critique of unsound practices in assessment and regulation of software based systems
- study of the limits of the levels of dependability that can be claimed given specific evidence
- study of long term reliability prediction based on residual fault estimates
- applications of the Bayesian formalism to lend rigour and verifiability to arguments that are usually stated in intuitive and informal fashion

- introducing formal reasoning about the notion of *confidence* in a claim.

The research was funded through a series of projects e.g., SHIP (EU), DIRC (EPSRC), QUARC (UK nuclear industry sub-contract), INDEED (EPSRC), UnCoDe (Leverhulme Trust) and SESAMO (EU ARTEMIS), with funding to date totalling in excess of £3.5M. The academic staff involved were Professor R Bloomfield (2000 to present), Professor P Bishop (2000 to present), Professor B Littlewood (1986 to present), Professor L Strigini (1995 to present) and research staff Drs Povyakalo (now Senior Lecturer, 2001 to present), Alberdi (2001 to present), Wright (1986 to present) and Gashi (now Lecturer, 2004 to present).

3. References to the research

1. Littlewood, B. & Strigini, L. (1993). Validation of Ultrahigh Dependability for Software-Based Systems. *Commun. ACM*, 36(11), 69-80 10.1145/163359.163373
2. Bishop P.G. & Bloomfield, R.E. (1998). *A Methodology for Safety Case Development*, Safety-critical Systems Symposium (SSS 98), Birmingham, UK, Feb. 1998
3. Bishop, P.G. & Bloomfield, R.E. (1996). A Conservative Theory for Long-Term Reliability Growth Prediction, *IEEE Trans. Reliability*, 45(4) 550-560 10.1109/24.556578
4. Littlewood, B. & Wright D. (2007). The Use of Multilegged Arguments to Increase Confidence in Safety Claims for Software-Based Systems: A Study Based on a BBN Analysis of an Idealized Example, *IEEE Transactions on Software Engineering*, 33(5) 347-365 10.1109/TSE.2007.1002
5. Bloomfield R.E., Littlewood B. & Wright, D.R. (2007). *Confidence: Its role in dependability cases for risk assessment*. In 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Proceedings, pp. 338-346 10.1109/DSN.2007.29
6. Bishop P.G., Bloomfield R.E., Littlewood B., Povyakalo A. & Wright D.R. (2011). Towards a Formalism for Conservative Claims about the Dependability of Software-Based Systems, *IEEE Transactions on Software Engineering*, 37(5), 708-717 10.1109/TSE.2010.67

The selected research is published in highly-regarded journals and conferences which apply rigorous peer review prior to approval for publication.

4. Details of the impact

The concepts, overall CAE approach and supporting analytical models have been taken up in the nuclear, financial, aviation and medical sectors. While simple in concept, the CAE approach requires a shift from a prescriptive box-ticking to a clear statement of the top-level assurance claims or goals which are progressively broken down into sub-claims with each supported by convincing evidence.

CSR has a long-established collaboration with Adelard LLP, a company specialising in system and safety assurance with two staff jointly employed by Adelard and City. The concepts and models developed by CSR have had direct impact through Adelard LLP's application to assurance cases for a variety of real systems, supported via Adelard's tool, ASCE, for the development and management of assurance cases and safety cases (www.adelard.com/asce/choosing-asce/index.html). This tool has been licensed to many industry users to produce their own assurance cases (around two thousand user licences have been issued).

The following quote from Adelard summarises the impact of the CAE approach on the nuclear industry:

> "*CAE is core to the Generic Design Assessment of nuclear plant design for new build in the UK. The approach was considered so successful that it is stated as one of the major risk reduction factors for new build in the UK by EDF and Areva and it is being considered by other countries (e.g., Sweden) for their own nuclear new build. CAE is also common practice in the nuclear industry in the UK for existing plant, and all their safety justifications follow this approach (although not all cases use graphical representations). Recently, there has been a push by other nuclear regulators to adopt CAE, and we see it being used and defended as a project risk mitigation in some of the largest software safety projects in the nuclear industry, including Sweden, Finland and China.*" – Sofia Guerra (Partner Adelard LLP)

In response to increasing and unacceptable fatalities and incidents (several hundred per year) related to infusion pumps, used to deliver fluids for nutrition or medication in healthcare, in 2010 the US Food and Drugs Administration (FDA) called explicitly for a new approach and the use of assurance cases and CAE by manufacturers to support the safe use of these vital medical devices[11] CSR staff are currently working with the FDA on developing templates for use on medical devices with formal research collaboration in the process of approval.

Following the application of the CAE and dependability case approach between 2004 and 2006 to a UK electronic funds transfer system (BACS) (classified by the Government as part of the UK critical infrastructure), two further electronic fund transfer systems were assessed using the CAE approach in 2009 and 2011: the Department of Work and Pensions Emergency Payment System and an immediate payment system (IPS) for medium size countries. This involved both reasoning relating to the overall risks from deploying the system and use of some of the underlying models on conservative worst case bounds developed by CSR. These systems were all deployed successfully under tight project timescale constraints.

In addition, CAE has been used:

- To structure the safety assurance evidence produced for the rail interlocking and signalling system to be installed on part of the West Coast Main Line (2005). This case was accepted and the rail interlocking and signalling system has been operated successfully since that time.
- In the security assessment of large critical UK information infrastructures in 2009, funded by the Communications-Electronics Security Group, the branch of the Government Communications Headquarters (GCHQ) which works to secure the communications and information systems of the government and critical parts of British national infrastructure.

The basic concepts have been standardised within the International Organization for Standardization (ISO/IEC 15026-2, 2011)[9] and work continues within the Object Management Group (OMG), the not-for-profit computer industry standards consortium; and the Open Group, a global consortium which leads the development of open IT standards and certifications, which has harmonised the structures used in CAE and Goal Structuring Notation (GSN), an additional approach developed by the University of York.

CSR staff have also disseminated goal-based justification principles into industry standards in current use:

- A UK Ministry of Defence (MoD) Standard for software-based system safety (Defence Standard 00-56)[8], incorporating the safety assurance concepts from the earlier Defence

Standard 00-55, co-authored by Robin Bloomfield. This addresses requirements for the management of safety in MoD projects to be used by Defence Contractors. While a new version of Defence Standard 00-56 is due for an update in 2013/14, the same approach to safety is expected to be retained.

- The Civil Aviation Authority Regulatory Objectives for Software Safety Assurance in Air Traffic Services (ATS) Equipment defines the assurances to be provided for an ATS system to enter service (in relation to people, procedures and equipment) including the behaviour of software. The document makes explicit use of CAE standards in the assessment of software for Air Traffic Management computer systems (CAA CAP670 SW01)[7] via Bishop and Bloomfield.
- The FDA guidance applying to infusion pumps as previously mentioned[12] which is now used internationally by manufacturers wishing to sell infusion pumps in the USA.

Often cases require evidence that the reliability of software is adequate. CSR has been heavily involved in the development of such models. One can make conservative estimates at an early stage (i.e., prior to development)[2] and can derive estimates based on tests applied to the developed system.[1,6] These methods have been successfully applied in these assurance cases (including the nationally important BACS fund transfer system mentioned earlier).

The work undertaken by CSR has led to the adoption of the team's assurance approach, in the form of updated regulations and procedures, as standard practice in several important industry sectors, leading to significant and wide-ranging impact on practice and consequent safety and security of systems. This has benefited both the industries concerned and the public who use or are affected by their services.

5. Sources to corroborate the impact

7. Civil Aviation Authority, CAP 670 SW01, Regulatory Objectives for Software Safety Assurance in ATS. Equipment, plus AMC Guidance for Producing SW 01 Safety Arguments for COTS Equipment
8. Ministry of Defence, Safety Management Requirements for Defence Systems Def Stan 00-56 Issue 4, 2007 (Section 9)
9. ISO/IEC, Systems and software engineering -- Systems and software assurance --
   Part 2: Assurance case, ISO/IEC 15026-2:2011,
   www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52926
10. EDF Energy Company Technical Standard: Control & Instrumentation C&I Modifications and Replacements, BEG/SPEC/ENG/CTS/214
11. US Food and Drug Administration, Guidance for Industry and FDA Staff - Total Product Life Cycle: Infusion Pump - Premarket Notification [510(k)] Submissions, http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm206153.htm#6

Corroboration can also be provided by contacts at Adelard, CAA Safety Regulation Group and Vocalink.