Embedded Software Design for Safety Critical Systems

Date: 3rd Nov 2009       Venue: TRW Conekt, Solihull, West Mids, UK

Register at: www.regonline.co.uk/safety_critical_systems

Registration fee: £50 for Electronics KTN members, £100 for non-members

Introduction

Modern electronic systems increasingly make use of embedded computer systems to add functionality, increase flexibility, controllability and performance. However, the increased use of embedded software to control systems brings with it certain risks. The increased flexibility and complexity can lead to new and different failure modes which cannot be addressed with traditional fault tolerance techniques. This is especially significant in “safety-critical systems”.

A safety critical system is a system where human safety is dependent upon the correct operation of the system. An obvious example of a safety critical system is an aircraft fly by wire control system, where the pilot inputs commands to the control computer using a joystick, and the computer manipulates the actual aircraft controls. The lives of hundreds of passengers are totally dependent upon the continued correct operation of such a system.

The development of safety critical systems has traditionally been pioneered within the avionics and automotive industries but, as awareness has developed, of how software can impact safety, the scope of safety critical software has expanded into many types of systems such as medical instruments and devices, transport, process control, nuclear and oil and gas facilities.

Safety requirements and failure modes and consequences in medical systems will be quite different from those in avionics systems or automotive systems for instance, and the approaches used to ensure safety may consequently be different too. This event is aimed at exploring the approaches used to develop embedded software in some of these different safety-critical applications, with a view to establishing any common approaches and identifying opportunities for sharing best practice and development tools and techniques.

A series of speakers will present their experiences of developing embedded software in various different safety critical applications. This will be followed by a panel session where the audience will have the opportunity to ask questions and voice their opinions.
Agenda

09:00  Registration & Refreshments

09:30  **Daniel Dearing** – Technology Business Manager, *Electronics KTN*
Introduction to EKTN and Embedded Software Design for Safety Critical Systems event

09:45  **Dr Ben Bradshaw** – Principal Engineer, Systems & Safety, *TRW Conekt*
Safety Analysis of Sub-Systems

10:15  **Chris Quigley** – Managing Director, *Warwick Control Technologies*
Design of High Integrity Distributed Automotive Embedded Systems

10:45  Refreshment Break

11:15  **Paul Evans** – Chief Engineer, Transport Projects, *BAE Systems*
From Planes to Trains: Applying a Common Safety Critical Software Development Process Across Domains

11:45  **Andrew Larkins** – Operations Director, *Triteq*
‘Utilising embedded microcontrollers for safety critical medical electronic products’

12:15  **Tony Hedge** – Principal, *Benthic Sciences LLP*
‘Safety Critical and High Reliability Software – A Small Company Perspective’

12:45  Networking Lunch

14:00  **Dr Pete Scotson** – Technology Leader, Control Systems, *TRW Conekt*

14:30  **Ibrahim Habli** – Research and Teaching Fellow in Safety-Critical Systems, *York University*
The Application and Justification of Formal Analytical Software Techniques

15:00  Refreshment Break

15:30  **Chris Hills** – Chief Technology Officer, *Phaedrus Systems*
Debugging is Hard – so why do it?

16:00  **Michael J Pont** – CEO, *TTE Systems*
Time Triggered Architectures in High Reliability Systems

16:30  Close

[www.electronics-ktn.co.uk/embedded.aspx](http://www.electronics-ktn.co.uk/embedded.aspx)  Copyright © 2009 Electronics KTN

*Knowledge For Growth*
Presentation Abstracts

Title: Safety Analysis of Sub-Systems
Speaker: Dr Ben Bradshaw

Abstract: In an ideal world, system design and safety analysis are performed simultaneously in a top-down manner. Typically, the overall system concept is analysed first, followed by detailed analysis of the sub-systems that make up the system. However, due to the need to develop complex products quickly and due to different parts of the system being supplied by different companies, design and safety analysis of a sub-system sometimes takes place in isolation from design and safety analysis of other sub-systems. In order for sub-system analysis to be valid, a number of issues need to be addressed. This paper considers these issues and provides examples taken from the road transport domain.

Title: Design of High Integrity Distributed Automotive Embedded Systems
Speaker: Chris Quigley, Warwick Control

Abstract: The presentation will discuss some of the issues to be considered when designing high integrity distributed automotive electronic systems which will ultimately affect the design of the software. Many of the principles discussed will be relevant for other industries.

Title: From Planes to Trains: Applying a Common Safety Critical Software Development Process across Domains
Speaker: Paul Evans, BAE Systems

Abstract: BAE Systems Ael have recently completed a project in the transport domain which included the development of real-time safety critical software. This success was achieved by applying a software development process previously developed and used in the aerospace domain. This presentation will consider the application of a common development process across dissimilar domains and explore the pertinent issues when moving to an unfamiliar domain. An overview of the current safety critical software development process applied by BAE Systems Ael will be provided. Key sub-processes and decisions will be explored in detail, including the mechanisms to allow continuous process improvement.

Title: Utilising Embedded Microcontrollers for Safety Critical Medical Electronic Products
Speaker: Andrew Larkins, Triteq

Abstract: Single chip microcontrollers are utilised extensively in consumer applications. These low cost devices can also be used in safety critical medical electronics products. The embedded software design must allow for potential single point failures within these devices. The presentation will describe a risk based approach to system design, likely failure modes and the implications on the requirements for the embedded software.
Title: Safety Critical and High Reliability Software - A Small Company Perspective  
Speaker: Tony Hedge, Benthic Sciences LLP

Abstract: This paper examines some typical design problems from the perspective of maritime systems. Maritime systems are commonly required to integrate data from a dozen or more "sensors", each quite complex in their own right, but rarely designed to any safety critical standard. Serial data links (RS-422 or RS-485) are still by far the most common interconnection techniques. Sensors are commonly upgraded during the lifetime of the system, and message structures and timings may change accordingly. Careful consideration must be given to synchronisation issues, and we look at some of the appropriate real-time design techniques for ensuring integrity is maintained, and at the role that appropriate tools can fulfil. A real-life (but anonymous!) example will be presented to give delegates a chance to spot a real "specification level" hazard.

Title: Software Testing of Dynamic Control Systems for Safety Critical Systems  
Speaker: Dr Pete Scotson

Abstract: Over a number of years TRW have developed a process for the testing of the integer implementation of mathematically intensive dynamic control functions used in the closed-loop control of electric power-steering systems. The original aim of the testing was to re-assure the designers that the embedded code implementation was robust to numerical extremes beyond those encountered in normal operation and standard software tunes. As such, the method required the development of a floating-point model of the specification to generate test vectors that were then compared with the output of the integer implementation. This produced a vast quantity of test results requiring tedious examination by the most experienced staff. This presentation will outline an alternative approach that focuses the engineer's attention away from the test results and on to the cause and effect of the floating-point vs. integer mis-match.

Title: An Assurance Argument for the Justification of Formal Software Analysis  
Speaker: Ibrahim Habli

Abstract: Formal mathematical methods are powerful specification and verification techniques for establishing high confidence in safety-critical software systems. However, there are a number of concerns about the use of evidence generated from formal methods, when used in place of conventional testing, for satisfying certain certification objectives. In this presentation, I address this issue in the context of the software aerospace guidance DO-178B/C. I also present a generic goal-based assurance argument which can be instantiated to facilitate the justification and presentation of formal analysis to the certification authorities.

Title: Debugging is Hard, so why do it?  
Speaker: Chris Hills, Phaedrus Systems

Abstract: When you are debugging, all you are doing is taking out the bugs that you put in when writing the program. This is clearly a waste of time and energy, particularly when there are pressures on budgets and timescales. So why not do a better job from the beginning? Drawing on several decades of
developing high reliability systems, Chris Hills will look at what works and what doesn’t and answer questions such as: Is Agile useable? Is the V model dead? Does the Waterfall only flow one way? And does any of it actually work in the real world?

**Title: Time-Triggered Architectures for Reliable Embedded Systems**

**Speaker: Dr. Michael J. Pont**

**Abstract:** In a time-triggered embedded system, we have one (and only one) interrupt enabled. This interrupt is usually linked to a timer, which will generate “ticks”: these ticks will, in turn, drive an appropriate (often very simple) operating system.

Time-triggered architectures are widely used in safety-related systems (for example in aerospace or medical sectors) because they are known to provide highly predictable behaviour, which in turn reduces testing, maintenance and (where relevant) certification costs. During this talk it will be argue that TT architectures can be (and should be) used more widely. Numerous examples of the use of TT architectures will be presented. Strengths and weaknesses of the TT approach will be considered.

The talk will not try to argue that a TT approach is a perfect match for all embedded systems. However, the talk will conclude by suggesting that – as you start your next project – you should ask yourself: “Should we use a TT architecture this time?” By the end of this talk, you may be surprised how often the answer is: “Yes”.

**Speaker Bios**

**TRW Conekt – Event Sponsor**

Dr Ben Bradshaw, TRW Conekt

Dr Ben Bradshaw has gained substantial experience working on safety analyses and has applied safety engineering techniques to a number of safety critical automotive applications (service brakes, parking brakes, steering system, smart ignition key).

**Pete Scotson, TRW Conekt**

Pete Scotson has over 28 years of experience in Automotive systems. His foundation in physics and electronics and later PhD in control systems have made him particularly adept at resolving system level problems, and have led to a keen eye for the implementation and fundamental issues in product development. His first job was on vehicle instrumentation and man-machine interfaces from where he progressed to engine management, specialising in diesel engine transient and idle speed control across many platforms, including work on cruise control systems and the first electronic diesel engine controllers. Most recently, Pete has been working on steering control systems, including steer-by-wire, and testing of embedded software.

[www.electronics-ktn.co.uk/embedded.aspx](http://www.electronics-ktn.co.uk/embedded.aspx)
Warwick Control
Chris Quigley

Chris is director and co-founder of Warwick Control, a company that is now in its 10th year, specialising in distributed embedded system technologies based on CAN, LIN and FlexRay. Previous roles included development of powertrain controls for Formula-1 motor racing. Chris also worked as a Research Fellow at the University of Warwick focusing on optimised hybrid electric vehicle control strategies.

BAE Systems
Paul Evans

Paul graduated from UMIST in 1994 with a BSc in Computation. Later that year he joined Aerosystems International (Aei) as a graduate software engineer. Throughout his career at Aei Paul has worked in a variety of roles in the software engineering domain. These roles have ranged from engineering (i.e. analyst, designer, coder, tester), through team leading, lead engineer and project manager. He is currently the chief engineer for the Aei High Integrity Solutions (HIS) group, responsible for technical governance.

Paul has worked on safety-related, safety critical and mission-critical systems. This variety of projects has covered both real-time embedded systems (running on bespoke hardware), GUI systems (running on a variety of operating systems) and database systems (utilising RDBMSs such as Ingres). Paul's expertise is in the analysis and design of software systems, and he has utilised a number of methodologies (such as Yourdon, Shlaer-Mellor and UML) and CASE tools (such as Teamwork, System Architect and Artisan RTS) as they have evolved over time.

Triteq
Andrew Larkins

Andrew joined Triteq in February 2005. He brings to the organisation 20+ years experience of electronic product design, manufacture, service and repair, both as an engineer and a project manager. Projects have ranged from integrated circuit design and manufacture for devices produced in the millions to one off special test systems. Specialist skills include the development of medical devices and radio products

Benthic Sciences
Tony Hedge

Tony has spent longer than he cares to admit developing real-time systems, but his extensive knowledge of the PDP-11 instruction set may something away. Benthic Sciences specialise in providing technical and management expertise to a wide customer base, and all Partners have experience not only at developer level but have held management positions at the level of Engineering Manager or above. Tony's own areas of expertise include Real-Time Design, particularly in the marine sector, both military and commercial. He strongly believes that design is all too often neglected as part of the project life cycle, with expensive consequences. He lives in rural Norfolk, where he keeps sheep.
York University
Ibrahim Habli

Ibrahim Habli is a research and teaching fellow in safety-critical systems at the High Integrity Systems Engineering (HISE) research group at the University of York. He currently teaches on the MSc in Safety-Critical Systems Engineering. His main research interests include model-based safety assessment, safety case development, software safety assurance and safety-critical product lines.

TTE Systems Ltd
Michael J. Pont

Michael J. Pont is CEO of TTE Systems Ltd and Head of the Embedded Systems Laboratory at the University of Leicester. Since the mid 1990s, Michael has worked with an internationally-recognised research team to develop tools and techniques which support the rapid development of reliable embedded systems. This research work has resulted in a number of patent applications and the creation of the RapidTTy™ tool family, which is now being further developed and sold by TTE Systems Ltd. Michael is author or co-author of more than 100 technical papers, and is the author of three books (including “Patterns for Time-Triggered Embedded Systems” and “Embedded C”).

Phaedrus Systems
Chris Hills

Biography Not Available