Beginning to Define a Body of Knowledge for Safety Practitioners

Dr. Clive Boughton
Software Improvements Pty Ltd
20/16 National Cct
BARTON ACT 2600
clive@softimp.com.au

Abstract

The Australian scene with respect to safety critical systems learning is relatively empty except for a few pockets of expertise. As to certification it seems there are no providers except through overseas links. On a world wide perspective, only the UK, USA and Germany are somewhat better in that there are several learning centres but only two providers of any form of certification appropriate to functional safety practitioners or engineers. Most safety critical systems specialists and courses reside in the USA or the UK.

Within industry world wide there seems to be a great deal of ignorance about evaluating, constructing, managing and maintaining, software-based safety critical systems. This is especially so in Australia. The Australian Computer Society National Technical Committee on Safety-Critical Systems (ACS-SCSC) has known of the general ignorance and lack of skills within Australia for some time and so, has recently embarked on a program to set up a new (software) safety critical systems course so that it is more accessible, affordable and appealing to a broader audience than most of the current offerings.

It is proposed that a new (software) safety critical systems course be made available via the vehicle of a specialist subject within the Certified Member of the Australian Computer Society (CMACS) offerings. In part, such a course is intended to make the broader Australian IT industry more aware of the importance of software safety issues within today's IT developments.

Keywords: CMACS, Software Safety Critical Systems.[1]

1 Introduction

Particularly within Australia, access to, and availability of knowledge with respect to software safety critical systems (SSCS) is not obvious, and can be difficult and/or expensive to obtain. The general ignorance of software safety critical issues within the Australian IT industry has meant that current course providers tend to treat particular areas of software and systems safety which are largely related to the specific needs of their cliental. Hence it might be inferred that there is little commonality of purpose and information among the current providers of the courses that are currently available within Australia.

The ACS-Safety Critical Systems Committee, which comprises people representing some of the providers and major users of safety critical systems knowledge in Australia, has recognised the need for more generic and more public SSCS offerings than are currently available. To that end the ACS-SCSC has engaged Software Improvements Pty Ltd to conduct a workshop focussing on issues and undertakings surrounding such a proposal. The workshop centred on the following subject matters:

- Need for such a course;
- Course objectives;
- Course content;
- The way ahead for developing a course.

The following sections provide brief descriptions of the outcomes relating to the above listed subject matters.

2 Needs

The committee decided that any new SSCS course should focus on systems of the type that, in the event of failure, could lead to human injury, death, or damage to the environment. "Mission critical" provided an additional attribute to help characterise the type of systems upon which any new course should focus.

Whilst a large set of stakeholders could easily be identified in relation to SSCS's in general, the committee narrowed the field down to those who are perceived to have the greatest need for knowledge/capability concerning safety critical systems issues and decisions. These are:

Procurers/Specifiers/Systems Engineers: Who need to be –

- able to identify safety risks;
- able to specify system safety targets and the regulatory framework;
- sufficiently knowledgeable to accept safety critical systems;

- able to identify when safety requirements have to be re-assessed (as assumed owner).

Maintainers: Who need to understand –

- the affects of adaptation, alternate technologies, and system enhancements;
- how to ensure that the system will continue to provide the intended levels of safety.

Systems Integrators: Who need to be able to –

- interpret safety targets and provide evidence that they are met;
- understand the limitations of the systems that they are integrating and be able to assess accordingly;
- put together the safety case in order to justify that the system will be appropriately safe.

Independent Assessors and Certifiers: Who need to be capable of investigating and judging the validity of safety cases (including targets and requirements).

Operators: Who need to be able to understand the basis for laying down procedures of operation.

The main reasons for the ACS-SCSC focussing on the above stakeholders are:

- software safety-related awareness is growing, but at a very slow rate;
- software safety-related concerns are dealt with erratically and inconsistently.

Some specific weaknesses that the ACS-SCSC identified concerning the current typical stakeholders mentioned above, include:

- Lack of proper specification of safety targets and requirements;
- Mute acceptance of COTS without evidentiary safety data/functions;
- Almost no assessment of systems integrator capability with respect to software safety;
- Little questioning of safety and risk arguments;
- Little understanding of the role of human factors and that software can fail;
- Virtually no understanding of legal and legislative issues concerning safety-related systems;
- Little realisation of the long-term ramifications to victims and businesses caught up in safety failures.

The ACS-SCSC members agree that the current courses in Australia are either too specialised or assume (at least) the pre-requisite of several years experience within a particular safety-related domain. There seems to be no comprehensive course that provides a base qualification for students who frequently work in the capacity of general safety critical specialists/experts. Most current safety critical experts in Australia have become so through experience and on-the-job-training.

There are some comprehensive (mostly post-graduate) courses available overseas. However, they are typically residential and rely on a small population of experts – hence the course fees and cost of attendance make these courses expensive to undertake. Also their completion may constitute an over-qualification for working on mainstream safety critical systems in Australia.

3 Objectives

The greatest benefit from a new course and therefore at whom the course should be aimed are considered to be:

- Novices to safety critical systems but expert/practiced in their own domain;
- Postgraduates who wish to enter a position requiring safety critical skills;
- System architects and analysts who currently work on safety-related systems but who (perhaps) lack adequate knowledge to undertake appropriate analyses of such systems;
- Project managers who need to know the overall risks and methods associated with developing systems containing safety critical components;
- Anyone directly responsible for safety.

At this stage the ACS-SCSC wish to provide one generic course, preferably via the vehicle of CMACS (Certified Member of the Australian Computer Society), which is recognised by the Association of Professional Engineers, Scientists and Managers, Australia (APESMA), Open Learning Australia (OLA), and Australian universities. The objective is to construct and run the course according to the CMACS requirements of a "specialised subject". Different/additional possible course proposals will be considered once this first, generic course is well underway.

CMACS is an appropriate study vehicle as courses are able to be conducted in a self-study style, and are aimed at the post-graduate level on the basis of a recommended four years IT experience. Additionally, assessments are typically carried out through a combination of assignments and an examination that (perhaps) provides a better quantitative indication of capability than some of the existing courses.

The ACS-SCSC has approached the CMACS Certification Manager in relation to the proposal for a course in safety-related systems containing software. The proposal has been positively received and it has been agreed that this proposal be submitted to the ACS Council."

As to whether the current CMACS course prerequisites are appropriate to a course that is strongly oriented to software safety will need further thought and analysis. However it is likely that anyone undertaking the course will need to possess either a degree in software

engineering or an IT degree with a software development/management major, and/or possess some minimal experience as a practicing software engineer who understands most aspects of the typical software development lifecycle and its management.

With these objectives in mind together with the proposed course content, an Expression of Interest (EOI) will be issued to discover the parties that are capable of constructing the proposed course.

4 Content

The ACS-SCSC has outlined some mandatory, optional and specialty components for a proposed "specialty subject" CMACS course in software safety critical systems. These various components are listed in Appendices A and B. Many of the mandatory components align with the Certificate in System Safety Engineering and/or Masters in System Safety Engineering courses offered by the University of York. The main reason for this approach is so that students who wish to further their studies or obtain formal certification can then more easily do so by arrangement with the University of York.

Alignment of proposed course elements from the Certified Functional Safety Expert (CFSE) Board or Technischer Überwachungs Verein (TÜV) programs on CFSE Safety Software Development and Safety Hardware Development were also suggested by the ACS-SCSC.

Further to the new course elements suggested in Appendices A and B, the ACS-SCSC has suggested that there be a section that covers the IEE Competency Guidelines for Safety-Related Systems Practitioners.

Appendix B represents the current thinking on proposed course (detailed) content based only on the mandatory components suggested by the ACS-SCSC.

Some optional topics were also suggested by the ACS-SCSC however the likelihood of such inclusions is slim in the light of the considerable range of mandatory components.

The ACS-SCSC has also suggested that specialised topics such as:

- Operational solutions;
- Software vs hardware solutions;
- Railway systems;
- Aircraft systems;
- Passenger car vehicles;
- Commercial road vehicles;
- System constraints;

might be covered within the context of a CMACS style course via assignments and essays. Treatments of such topics are likely to be very dependent on the requirement of students' employers and the capacity of course convenors.

5 The way ahead

Assuming the continued support and cooperation of the ACS/CMACS Program Manager to have the proposed new safety critical course included as a part of the "specialised subject" offerings within the CMACS program, the current plan for the further development of the proposed course is as follows:

1. Search for existing course offerings – *Refer to Appendix A*.
2. Evaluate existing courses for relevant content – *Refer to Appendix B.*
3. Construct plan for design, implementation and delivery of course(s) under CMACS program and present to the ACS Council.
4. Determine effort / cost estimates to develop course(s).
5. Seek agreement / approval to fund the development through ACS Council.
6. Determine schedule for development.
7. Construct an EOI to invite interested parties to indicate their ability to undertake the course development.

6 Conclusions

Software safety critical systems capability within the Australian environment is vary patchy and not broadly serviced. The ACS-SCSC has identified various shortcomings of the typical practitioners who fill the various openings in safety critical developments and management. A greater understanding of a broad set of topics in safety critical systems is required in order that system failures and costs be reduced and for there to be less dependence on acquiring safety critical systems knowledge through on-the-job-training alone.

The CMACS specialty subject course proposed in this paper is a positive step forward in overcoming some of the shortcomings in safety critical systems development, assurance, maintenance and management expertise that currently exists in the Australian industry.

APPENDIX A

REQUIRED CONTENT	SVRC UQ	R2A	NL MIT	SC	UY UK	CFSE	WU	OU	MJ ERAU	UG	UT	ERA
Intro to System Safety	X	X	X	X	X	X	X		X	X	X	X
Hazard & Risk Assessment	X	X	X	X	X		X	X	X	X	X	X
System Safety Assessment	X	X	X		X		X	X		X		X
Safety Critical Project Management			X		X		X			X		
Design for Safety	X		X	X	X		X			X		X
Hazard & Risk Management		X			X		X			X	X	
Safety Cases	X	X			X					X		X
Computers & Software & ISA	X		X		X					X		
Human Factors Engineering	X		X		X				X	X		
IEC-61508	X					X		X		X		
Safety Lifecycle Concepts & Objectives						X	X			X	X	X
Requirements for Management of Functional Safety		X				X						
Methods for Avoidance of System H/W Faults										X		
SIL Verification Concepts & Procedures	X	X				X	X					X
General Design Concepts & Procedures						X	X	X		X		X
Detailed Design Concepts & Procedures						X				X		
Safety Validation Concepts & Procedures	X		X	X			X			X		X
Management of Change Concepts & Procedures	X					X	X					
Case Studies	X	X	X		X					X	X	

OPTIONAL TOPICS												
Detailed Legal Issues		X										
Specialised Testing Techniques						X	X	X		X		X
Recommended Safe Practice		X										
S/W Coding Standards												X
Project Management Beyond Risk Management												
Standards in Addition to IEC 61508	X							X		X		
SPECIALTY TOPICS												
Operational Solutions	X	X									X	
S/W vs H/W Solutions										X		
Railway Systems	X											
Aircraft Systems	X									X		
Passenger Car Vehicles	X											
Commercial Road Vehicles	X											
System Constraints												
Acquisition of Safety Critical Systems							X					X

TABLE A.1: Existing Safety Critical Course Offerings as apparent *only* from various websites.

Website references:

- SVRC UQ: Software Verification Research Centre – University of Queensland http://www.svrc.uq.edu.au/Training/dscs.html
- R2A: Risk and Reliability Associates http://www.r2a.com.au/
- NL MIT: – Nancy Leveson http://sunnyday.mit.edu/safety.html
- UY UK: University of York http://www.cs.york.ac.uk/MSc/SCSE/modules/iss.html
- SC: Safeware Corporation http://www.safeware-eng.com/software-safety/accident-causes.shtml
- CFSE: Certified Functional Safety Expert Governance Board http://www.cfse.org/software.htm
- UW: University of Washington http://www.engr.washington.edu/~uw-epp/sss/
- OU: Oxford University http://www.softeng.ox.ac.uk:8080/$?4KM1vBEd?$/
- MJ ERAU: Embry-Riddle Aeronautical Uni – Matt Jaffe http://salmosa.kaist.ac.kr/~rehas/English.htm
- UG: University of Glasgow – Chris Johnson http://www.dcs.gla.ac.uk/~johnson
- UT: University of Teeside – Short Course http://www-scm.tees.ac.uk/hazop/html/course.htm
- ERA: ERA Technology http://www.era.co.uk/conf/software1.htm

APPENDIX B

Proposed course content

The ACS-SCSC suggested the ***required content*** (as listed in Table A.1) primarily because the topics link in well with existing courses that lead to certification. A later option for the proposed CMACS specialisation subject for Safety Critical Systems, may be to obtain some high level of credit from institutions currently providing certification. Then students who successfully complete the CMACS Safety Critical Systems course could easily take up further study towards full certification.

The two courses offering certification are from the University of York, UK and the CFSE Governance Board, US respectively. Currently it is known that the former requires around 9 full time weeks (say 270- 300 hours) of study plus a 6 person-month project to complete. The length of course study sits well with the CMACS requirements that indicate that each of the two specialisation subjects contributing to the course require around 8 – 10 hours of study per week for 4 – 5 months. This represents a range between 130 – 210 hours per subject.

The following is an initial draft of the structure of the proposed CMACS specialisation in Safety Critical Systems.

Each of the two subjects contributing to the specialisation component should contain the equivalent study and reading content for 25 – 30 lectures. Nominally this represents between 80 – 100 hours. The remaining time for the course should be dedicated to exercises and assignments – representing a further 80 – 100 hours of effort.

The notion of running the course using specified texts is not without some appeal, as then the student could be directed to focus on particular material from the text with the intent of using well constructed exercises together with a question and answer technique to help the student build up practical knowledge. Any assignments could then be based on an expansion of such knowledge, enabling the student a deeper, less scatter-gun learning approach.

The mandatory topics to be covered for Part 1 of the specialisation include: (figures in parentheses indicate nominal hours of study)

1. Introduction to Safety (8).
2. Hazard and Risk Assessment (14).
3. System Safety Assessment (14).
4. Safety Cases (14).
5. IEC 61508 (12).
6. Safety Lifecycle Concepts and Objectives (12).
7. Computers and Software (but not the ISA) (14).
8. Requirements for Management of Functional Safety (14).

The mandatory topics to be covered for Part 2 of the specialisation include:

1. Safety Critical Project Management (14).
2. Hazard and Risk Management (12).
3. Introduction to Human Factors Engineering (16).
4. General Design Concepts and Procedures (10).
5. Design for Safety (12).
6. Management of Change Concepts and Procedures (12).
7. SIL Verification Concepts and Procedures (12).
8. Safety Validation Concepts and Procedures (12).

Optional topics initially be restricted to:

1. Detailed Legal Issues (16).
2. Specialised Testing Techniques (12).
3. Detailed Design Concepts and Procedures (12).

4. Acquisition of Safety Critical Systems (16).

Specialty topics can be any one of the remaining topics among those listed in the Table A.1, or any other approved topic. However, these topics should be integrated with assignment work as far as is possible.

Exercises and assignments need to be designed to provide the student with further exposure to as many of the mandatory topics as possible. It is desirable for exercises and assignments to become the main vehicle of learning in a progressive fashion.

Details on the mandatory topics to be covered for Part 1 of the specialisation:

1. **Introduction to Safety (8)**
   - A brief history of some well-known safety failures – of all types;
   - Root causes of accidents;
   - Do humans cause most accidents?
   - Problems in ascribing causality;
   - Are humans needed to run automated systems?
   - Statutory requirements for safe systems of work, regulations and codes of practice, roles and responsibilities.
2. **Safety Lifecycle Concepts and Objectives (12)**
   - The system and software safety process;
   - Scope;
   - Hazard and Risk Analysis;
   - Safety Requirements;
   - Planning;
   - Implementation;
   - Installation and commissioning;
   - Safety validation;
   - Operation, Maintenance and Repair;
   - Modification and Retrofit;
   - Decommissioning and disposal;
3. **Hazard and Risk Assessment (14)**
   - Introduction to hazards and risk;
   - Approaches to hazard identification and risk assessment for the early stages of system development;
   - What is a hazard?
   - What is a risk?
   - What is hazard analysis?
   - What is risk analysis?
   - What are the different types of risk/hazard analysis?
   - How to identify system and software hazards;
   - How to eliminate or mitigate hazards/risks;
   - Modelling hazards;
   - Software hazard analysis and requirements analysis;
   - Measures of accident severity and probability;
   - Event Trees;
   - As Low As Reasonably Practicable (ALARP);
   - Functional Failure Analysis;
   - HAZOP;
   - Probabilistic risk assessment (PRA);
   - Techniques for Human Error rate Reduction (THERP);
   - Cognitive Reliability and Error Analysis Method (CREAM);
   - Fault trees and software fault trees;
   - Software PRA (Backward reasoning, weakest pre-condition approach, theorem proving);
   - Limitations of risk/hazard analysis.
4. **System Safety Assessment (14)**
   - Classical system safety analysis techniques;
   - Formal definitions of terminology;
   - Self assessment (UK-HSE and IEE);
   - Reliability Block Diagrams;
   - Using Fault Trees (Gates and Events);
   - Failure Modes and Effects (Criticality) Analysis (FME(C)A);
   - Common mode failure analysis;
   - Zonal Hazard Analysis;
   - Practical Risk Assessment;
   - Cause-consequence Analysis;
   - Selecting appropriate techniques;
   - Management Oversight and Risk Tree (MORT) – (SMART – UK MOD);

- Documenting Safety Analysis.

5. **Safety Cases (14)**
   - System Acceptance;
   - What is the role and purpose of safety cases?
   - What standards are there?
   - What does a safety case contain? (Requirements, Evidence, Arguments, Context);
   - Putting together a safety case argument;
   - Producing evidence for a safety case;
   - Maintaining safety cases through the system lifecycle;
   - General requirements;
   - Requirements for electronic, electrical and PLC hardware;
   - Changing safety cases.
6. **IEC 61508 (12)**
   - Risk Classes;
   - Software Requirements;
   - Methods for determining Safety Integrity level (SIL);
   - Guidelines;
   - Techniques and Measures;
   - Comparing IEC 61508 with DO 178B
7. **Computers and Software (14)**
   - Why is building software problematic;
   - Overview of the system/software development process;
   - Tailoring the software process;
   - How does software affect safety?
   - How to undertake hazard analysis of software;
   - Commercial off-the-shelf (COTS) software within the safety picture;
   - Microprocessors (COTS, VIPER, PLCs, 1750A,B);
   - Safe operating systems (the certification process);
   - Software reliability;
   - Software defects and their prevention.
8. **Requirements for Management of Functional Safety (14)**
   - Safety management strategies;
   - The role of management;
   - Setting policy;
   - Setting up a system safety organization;
   - Allocating responsibility;
   - Promoting awareness;
   - Providing safety advice;
   - Monitoring compliance;
   - Handling safety incidents;
   - Regulatory and legal compliance;
   - Managing resource allocation;
   - Assuring staff competency;
   - Effective communication;
   - Eliciting information;
   - Organisation systems;
   - Functional safety practices;
   - Promoting a safety culture.

Details on the mandatory topics to be covered for Part 2 of the specialisation:

1. **Safety Critical Project Management (14)**
   - Why systems and software engineering is important;
   - Professional standing and personal integrity;
   - Teams (management, communication, effectiveness);
   - Safety management systems;
   - Safety plans;
   - Specifying safety requirements;
   - Derived safety requirements;
   - Roles and responsibilities;
   - Required skills and competencies;
   - Hiring subcontractors for safety critical systems;
   - Resolving conflicts;
   - Auditing (including systems, software and safety).
2. **Hazard and Risk Management (12)**
   - Hazard monitoring and hazard logs;
   - Hazard reduction;
   - Management of safety during operational service;
   - Failure Reporting, Analysis, and Corrective Action System (FRACAS);
   - Management of a FRACAS;
   - Classification categories of corrective action for failures;
   - Management to achieve ALARP;
   - Fault injection.
3. **Introduction to Human Factors Engineering (16)**
   - Slips, Lapses and Mistakes;
   - Generic Error Modelling;
   - Skill, Rules and Knowledge-based errors;
   - Risk Homeostasis;
   - Workload, Situation Awareness and Crew Resource Management (CRM);
   - Modelling human behaviour;
   - Identifying end user requirements;
   - Providing human factors safety input;
   - Operational analysis;
   - Task analysis;
   - Developing procedures;
   - Human reliability theory;
   - Multi-discipline systems viewpoint.
4. **General Design Concepts and Procedures (10)**
   - A systems perspective;
   - Use cases and scenario analysis;
   - Conceptual thinking and domain knowledge;
   - Modelling system and software requirements;
   - Dataflow models; natural language techniques; functional models; causal logics;
   - Specification of non-functional requirements (the “ilities”);
   - From requirements to design;
   - Architecture;
   - Software design techniques.
5. **Design for Safety (12)**
   - Common architectural styles;
   - Fault-tolerant architectures;
   - Describing the architecture;
   - Specifying safety-related system architecture;
   - Evaluation of architectures and architectural trade-offs;
   - Transposing from requirements into design;
   - Evaluating design solutions;
   - Safe languages;
   - Implementation issues.
6. **Management of Change Concepts and Procedures (12)**
   - When is change necessary?
   - The effects of change;
   - Configuration management concepts (configuration items, baselines);
   - Configuration control concepts;
   - Version control concepts;
   - Change control;
   - Change requests;
   - Change control authority;
   - The change process;

- Configuration audit;
- Status reporting;
- Configuration management standards.

7. **SIL Verification Concepts and Procedures (12)**
   - Verification of safety (testing, software fault tree analysis);
   - Applying IEC 61508.
8. **Safety Validation Concepts and Procedures (12)**
   - Safety validation plans;
   - Test and evaluation methods for safety critical systems;
   - Specifying software and system tests in a safety critical environment;
   - Reviewing software (inspections, walk-throughs, static and dynamic analysis);
   - Witnessing and executing tests;
   - Reporting results;
   - Analysing results;
   - Analysing the system/software design in a safety context;
   - Analysing the code for safety.

Case Studies (suggestions)

- Ariane 5;
- London Ambulance System;
- Department of Energy – USA;
- NASA – GCS;
- Space shuttle GPC;
- Therac 25.