

1 ***Introduction***

Programmable electronic systems (conventional computers, programmable logic controllers (PLCs) and specialised microprocessors) are playing an increasing role in applications where a failure or incorrect operation could lead to serious injury or even the death of one or more people, to significant environmental damage or to other major accidents.

On the one hand, the correct and well-considered use of programmable electronic systems can improve both the overall safety and the efficiency of the processes which they are used to control. On the other hand, the increased flexibility and complexity which programmable systems permit can, if not properly designed and managed, pose a threat to safety.

It is therefore important from the point of view of both competitiveness and safety that organisations developing, supplying and using programmable electronic systems in safety-related applications use the best and most up-to-date techniques in the development and management of these systems.

1.1 The Safety Critical Systems Programme

In the light of these imperatives, and because of the comparative immaturity of the technology, the Department of Trade and Industry and the Engineering and Physical Sciences Research Council decided to fund a collaborative programme of research and development in Safety-Critical Systems which would:

- improve the technology and management practices used in the development of safety-critical systems;
- explore the rationale for current traditional practice in a variety of industry sectors;
- seek to cross-fertilise the best experience and practice from different sectors;
- investigate avant-gard technologies to determine under what circumstances their use could improve safety and how this might be justified.

The first project within the Programme started in October 1991. The last industrial project is due to finish in August 1997 and the last academic project in January 1998. In all there have been 32 projects involving some 99 organisations. Of these projects, 13 have been University-led (although with participation by industry) and 19 larger projects have been led by industry, usually with some academic involvement. The total investment by industry, DTI and EPSRC has been of the order of £28.4m of which about half has been contributed by industry. The technical scope has been correspondingly broad. Details of the individual projects, including timescales, costs and participants can be found in Appendix A.

This has been a substantial programme by any standards, and some impressive work has been done. This book sets out to highlight the most interesting and useful results. It cannot, however, cover everything that has been done and the reader is encouraged to follow up the multitude of references to general papers and detailed reports in Appendix A.

The Programme has been one of research and development ('R&D'). Research is the business of finding answers to questions. The development component of research and development is also concerned with finding answers to questions, usually questions of the form "what are the problems involved in producing such and such, and how can we solve them?" In figure 2.1 therefore the work of the Programme is presented in terms of the questions which the research and development programme set out to answer.

The projects have been seeking to advance the state of the art. The system developer with little experience of safety-critical work should therefore not turn to a chapter with the expectation of finding a primer on the relevant topic. In most cases the projects have grappled with difficult issues and have advanced the state of the art in one or more respects. Their reports are reports from the battlefield. In most cases they have not set out to provide a handbook on developing safety-critical systems. The Editor, however, has tried to present each chapter in such a way that it will be intelligible and interesting to the less experienced, as well as being a useful statement of the main results and achievements of the projects for the specialist.

The exception to the caution about not expecting a handbook is chapter 8. The projects described in that chapter have indeed set out to provide Guidelines or Codes of Practice which can be of assistance to those who find their work developing into the area of safety-critical or safety-related software-intensive systems and who wish to become better informed about what is involved.

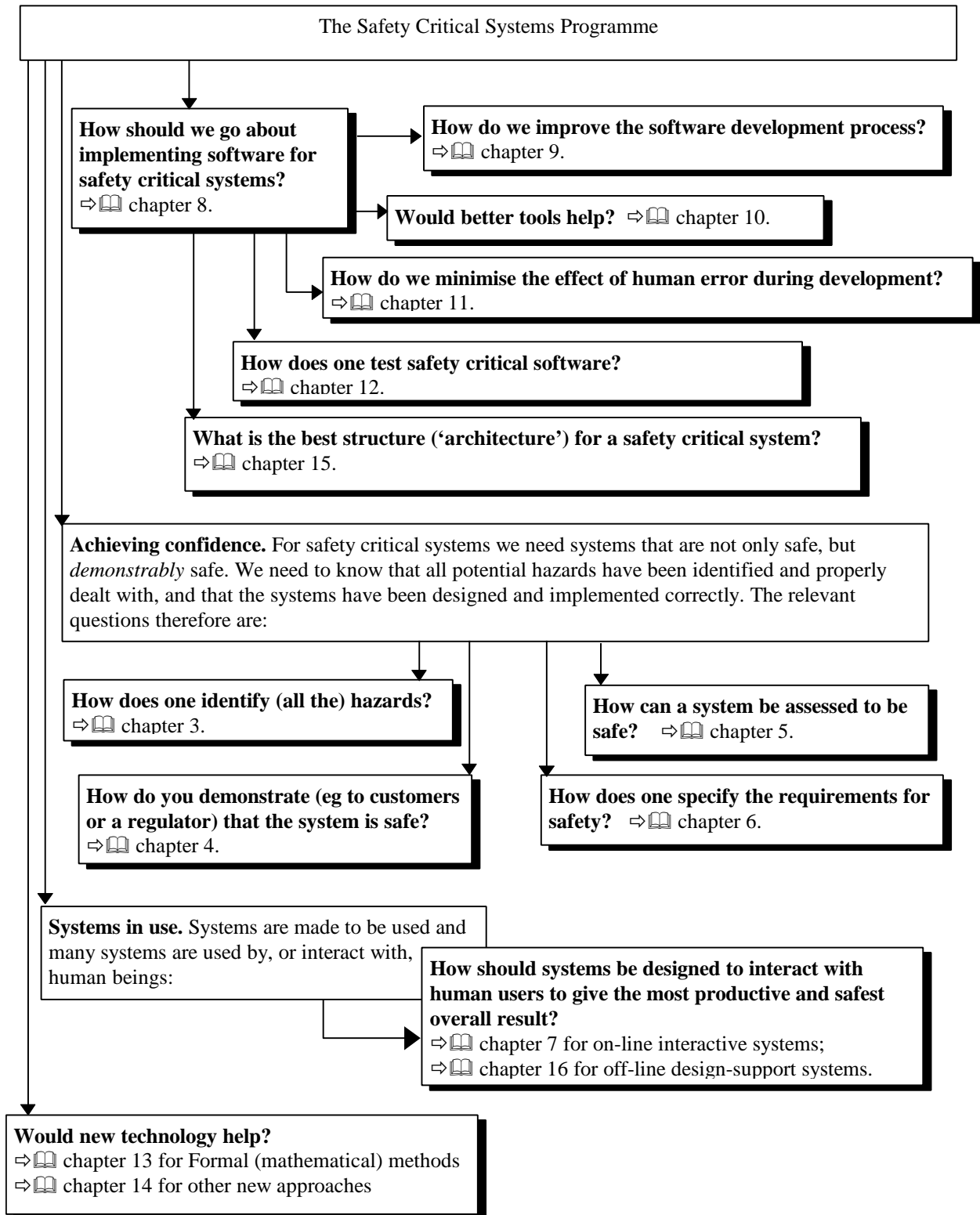


Fig 1.1 The questions addressed by the Programme

Industry sectors

The results of most of the projects are relevant to all sectors of industry. Some projects, however, have produced results which are of particular relevance to a particular sector. These are:

Sector	Project	Section	
Automotive	MISRA	8.1	Guidelines for the automotive industry
Process industries	FRESCO	5.1	A framework for assessment
	LIFETRACK	7.1	Supporting team operation
Medicine	RED	14.1	Knowledge-based systems and safety-critical decisions
	MORSE	13.2.3	Case study of using RAISE - a laboratory information system
	SADLI	3.4	Hazard analysis in a medical case study
Railways	HUFIDESAC	11.2	Avoiding human error in design
	SSI TOOLS	10.1	Tools for railway signalling
Robots	ROBUST	8.3	A methodology for safe advanced robots
	SAFE-SAM	3.5	Hazard analysis in advanced robots
		and	15.2
Water	SAFE-DIS	16.2	Safe design of networks

1.2 Purpose and structure of this book

The Programme has involved many hundreds of person-years of effort across industry and academia. In a book of this size it is possible only to indicate some of the principal results and the main points of interest. References to project publications are included so that you can follow up in more detail any topic which is relevant to your work or to the work of your organisation. These references are in square brackets and consist of the name of the project followed by the word '*ref*' and then a number. Details of the reference will be found in Appendix A under the project heading, indexed by the reference number. (Thus, for example, [LIFETRACK *ref* 6] is a reference to the LIFETRACK Final Report.)

Each chapter addresses a particular area (eg 'hazard analysis' or 'the human element in the development process') and describes the results of the projects which have worked in that area. Some projects have worked in more than one subject area and therefore appear in more than one chapter. If you would like to get an overview of what a particular project has done, this can be found in the project's entry in Appendix A. Wherever possible, references to published reports and papers are included so that you can obtain more detail if you wish. In all cases, Appendix A includes the name of a contact who can be approached for more substantial enquiries about the results of the project and possible commercial or other exploitation of these results.

The descriptions of the results and achievements emerging from the various projects have been based on extracts from project reports or on text supplied specially by the projects. The source of each contribution is credited in Appendix D. The accuracy of the descriptions obviously depends on the accuracy of these sources and on the vagaries of the process of compilation and editing. You should obviously go to the original sources and other references before adopting any of the technology described here or incurring any significant costs.