

B The Genesis of the Programme

By Bob Malcolm, Programme Coordinator 1990 - 1995

The projects described in this book were supported as part of the Safety Critical Systems Advanced Technology Programme. This was a collaboration between the Department of Trade and Industry (DTI) and the Science and Engineering Research Council (SERC) - which during the life of the programme became the Engineering and Physical Sciences Research Council (EPSRC).

B.1 The background

Early technical concerns

The starting point for the programme was the increasing concern during the 1980's about the introduction of computer-based sub-systems into safety-critical applications which had previously used tried and tested electromechanical techniques. The safety-related implications of many off-line applications, such as medical records, legal databases, and computer-aided design packages, were also becoming more apparent.

Now, computers can provide cheap, compact, functionality of a sophistication undreamed of with earlier technology, and with high hardware reliability. But there was, and still is, concern about specification, design, and programming of the computer software. This led to a sometimes confused debate in both industry and academia over the appropriateness of different software development techniques for safety-critical applications. The confusion was compounded by the big differences between safety engineering practices in different sectors.

Then there were developments in the market-place which were - and still are - putting increased pressure on current techniques. Some sectors, such as parts of the avionics industry, have always had the problem of 'continuous control', where systems cannot be made safe simply by stopping their operation. Now new applications of microelectronics in hitherto low technology application areas, such as active vehicle suspension, were facing the same problem.

Other sectors are faced with mounting pressure for increased availability. Where previously it would have been sufficient to add fail-safe protection to an unreliable system, this is becoming less acceptable, either because of the economic impact or because of knock-on safety effects because of the integration of systems. 'Systems' are usually in fact subsystems of other systems, and 'safe unavailability' of one such 'system' can jeopardise the safety of the whole. Shutting down a power generator may maintain the safety of the generation plant, but if it means losing all the city traffic-lights, then safety of the 'city system' is impaired. The consequence of this is a trend to more 'continuous control' systems with their much higher demands for dependability.

All this has been in addition to the urge for ever greater functionality despite concern about our ability to manage present levels of complexity.

Official responses

During the 1980's the UK Health and Safety Executive had been developing guidelines on '*Programmable electronic systems in safety related applications*'. Then in 1986 the Cabinet Office Advisory Council on Applied Research and Development (ACARD) published a report entitled '*Software: a vital key to UK competitiveness*'. That report was primarily concerned with the health of the UK software industry, but in an appendix it made some suggestions for approaches to the development of safety-critical software-based systems, including a recommendation that the Institution of Electrical Engineers (IEE) should lead a study of the subject. At the time, the IEE made an initial position statement to the Cabinet Office, together with a draft guide to the subject.

The IEE-BCS Study of Software in Safety-related Systems

In its response to the ACARD report, the IEE maintained that software should not be treated in isolation; that 'safe software' is a meaningless concept. Software may well play a significant role in the safety of a system, and there are indeed potential safety-related problems specific to software, and software-specific techniques which may ameliorate some of those problems. Nevertheless, the safety-related aspects of software should, in general, be considered in the context of the system of which it is a part. It is but one element of design which must be set alongside overall system specification, design, construction, and operation.

The IEE then established a working party, drawn from a wide range of industry sectors, to study the subject in depth. The British Computer Society (BCS) was invited to participate in the study; and the DTI both participated in and made a financial contribution to its support.

During the life of the working party, there were a number of other related initiatives. The Health and Safety Executive published its guidelines in 1987. The International Electrotechnical Commission issued early drafts of international standards in 1989. The UK Ministry of Defence issued draft defence standards during 1990 and 1991, though early drafts had been discussed for some time before that. The European Commission issued its Product Liability Directive. So much activity generated as much confusion as clarification. The ambition of the IEE-BCS study was to bring together representatives of all interests and achieve a consensus on the way forward.

The objectives of the study were to survey regulatory practice and trends in a range of application areas and sectors of industry, in order to provide a firm basis from which to propose options for improvements. The potential role of certification was specifically addressed, and the position with respect to liability and insurance requirements investigated.

The working party delivered its report in 1989. The report summarised the important issues for professional engineers - both those familiar with safety engineering practices in their industrial sectors, but who were facing the introduction of computers into their systems, and those familiar with software engineering but unfamiliar with safety engineering.

The report also contained recommendations on the way forward for the profession, for the regulatory authorities, and for government. There were many such recommendations - for awareness, dissemination of information on safety concerns arising from emerging technology, standards, competence requirements, adoption of the safety case approach, and a programme of research. Perhaps the key recommendation was for pan-sector harmonization of safety engineering practices. It was agreed that such harmonisation should be achieved on an international basis, as all standardization of any significance is internationally based for most industry sectors. The conclusion was that it was in the UK's interest to take a leading role in such standardization, especially the development of what has become IEC 1508.

Finally the report identified requirements for research which would put 'engineering judgement' on a firmer footing, and which would help cut through some of the arguments - such as the 'formal methods debate' - which prevailed at the time (and still do, though to a lesser extent).

The DTI-SERC Joint Framework for Information Technology

Shortly after the IEE-BCS Report was published, the DTI and SERC were considering their future programmes of research within their Joint Framework for Information Technology (JFIT), to follow on from the Information Engineering Advanced Technology Programme, itself a successor to the Alvey Programme of IT research. It was decided that instead of a single all-embracing IT research programme there should be a range of smaller, more focused programmes to tackle specific topics. The Systems Engineering community put, at the top of their priority list, a recommendation for a programme in safety-critical systems research.

A £35M, 5-year programme was then planned, starting from the recommendations of the IEE-BCS Report. The programme was approved by the Secretary of State for Industry in April 1990 and launched in September 1990. The first proposals were submitted in January 1991 and the first grant for a project was offered in July of that year. A second call for proposals was made in 1993, and the final projects, some having had extensions, will come to an end during 1997.

B.2 The Programme

Objectives

A key requirement was to gain a better understanding, in the UK industrial and academic communities, of how safety may be achieved and assured, so that industry could achieve greater and more cost-effective safety in practice, and also derive commercial benefit thereby.

The desire for harmonisation, expressed in the IEE-BCS Report, was not meant to imply any intention to seek uniform standards for all applications in all sectors. But it was hoped that by achieving some greater degree of commonality, the UK supply community would become less fragmented, allowing greater diversity of supply and opening markets for both users and suppliers. One aim of the research programme was, then, to bring different sectors together, both in the programme as a whole and even within cross-sectoral projects. The intention was that by comparing and contrasting their approaches, the reasons for their differences would become more apparent, as would the ways in which they could be the same.

Through collaborative research, with sharing of results, the programme was intended to help industry, and the participants in particular, to increase the assurance of safety, simplify compliance with standards, satisfy legal requirements, reduce supply costs, and facilitate the introduction of computer-based safety-related systems with all their consequential benefits. An added benefit for participants was that they should also gain valuable market intelligence and contacts in both their own markets and others, so as to facilitate business development and diversification.

In order to resolve the software techniques debate, a further ambition for the programme was to bring together not only different sectors, but diverse software techniques. Then, again through comparison and contrast of the very different ways in which they address the design problem, industry would come to understand better what new techniques can contribute in what way to what kind of application, and, most importantly of all, why.

If a more coherent and better informed UK position could be established, and if open, international standards could be developed with strong UK participation and UK industry understanding the implications and readily able to satisfy the standards, then the hope was that UK industry would also be better placed to address international markets.

Scope

The programme addressed a very wide range of issues as will be realised from the diversity of the work described in this book. In addition to the exploration of improvements in specific technologies and techniques, there was the search for understanding and unification of criteria and techniques for safety assurance. What is the basis for present practice? Where do sectors fundamentally differ and why? How common can they be? Can we characterise systems so that they and their appropriate procedures and techniques can be fitted into a common framework, so as to facilitate harmonisation across industrial sectors?

The programme elicited proposals on three main research themes: 'technologies'; 'human factors'; and 'unification'. 'Technologies' was to include many aspects of the development process and both process and product evaluation. A software design technique would be considered to be technological; so would organisational techniques and procedures relating to parts of the overall process; so would support tools. The relationship between these different facets of development is also of interest. For instance, techniques for design should be considered for their suitability for assessment and for after-the-event fault diagnosis.

'Human factors' was meant in a much fuller sense than just ergonomics and consideration of the human-computer interface. It was intended to encompass all aspects of human involvement, and particularly human fallibility from system conception to operation and beyond. 'Unification' was a term coined for the development of means to integrate diverse knowledge about particular systems, and for the development of a common basis for comparison of alternative sectoral and technological approaches.

The programme followed the International Electrotechnical Commission in taking a broad definition of 'safety'. At that time the IEC included risk of widespread environmental damage and economic loss, as well as danger to human life and limb.

There was no intention to prescribe particular items of research. Instead, some indication was given of the range of technical problems which we knew must be addressed and the range of research themes which might contribute to their solution. It was recognised that these were not likely to completely delineate the field, and they were not intended to be constraining. The aim was to encourage lines of enquiry rather than exclude them.

Structure

All the projects had to have at least two collaborating partners, one of which was an industrial organisation. Only sparse coverage could be expected with such a broad scope, but the intention was to maximise impact through awareness activities, through interaction with other related activities, and through involvement of leading opinion-formers, both individuals and organisations, who would influence the rest of the community through their procurement policies and through their role in setting industrial standards. So participation of more than the minimum number of participants was encouraged as long as the management of the project was not jeopardised, and a number of projects, such as CONTESSE, SAFEDIS, SEMS-PLC, and ISSAFE were established with associated influential user-groups. Such projects also acted as vehicles for cross-sectoral consensus building. The concept was of a set of projects inter-meshing with each other and with the world outside the programme.

To help the inter-meshing process, a community club - the Safety Critical Systems Club - was established. This was also intended to have a major role in achievement of consensus. It is a means of dissemination of intermediate and final results of the programme, and a sounding board for them; it is the forum in which workers in very different areas can compare notes; it is the focus for newcomers to the safety-critical 'scene', where they can quickly find out who knows what about what.