

5 Assessment

Both purchasers and suppliers of safety-related systems need to assure themselves that the systems they purchase or supply are indeed safe. This chapter describes firstly a framework for third party assessment and certification against an accepted standard, and then guidelines for carrying out safety assessments.

5.1 A Framework for Assessment

The FRESCO project (Framework for the Evaluation of Safety Critical Objects) began in December 1993 with the objective of investigating the assessment and certification of safety-critical systems and identifying a scheme which would enable this assessment and certification to be conducted in the process industries.

At that time (and indeed currently) organisations requiring independent software assessments found it difficult to select between proposals from competing assessment companies because their offerings were usually based on very different views of the work that should be done. This meant that it was difficult to ensure that a cost-effective solution was adopted.

A number of benefits of conformity assessment and certification of safety-critical or safety-related systems were identified during the project. These included:

- systems will be safer
- a legal defence of following “best practice” is provided
- in-house validation costs may be reduced if purchased systems are known to be safe
- developers of certified systems will have a competitive advantage
- industry may exploit the advantages of programmable technology
- public confidence in industry will be increased

The project studied the existing approach to assessment that is taken in the Information Technology Security Evaluation and Certification Scheme and identified lessons that could be learnt from the approach that is taken. This study was conducted in parallel with a requirements survey which identified the needs of industry relating to this area. The requirements survey involved questionnaires, interviews and study of European legislation.

In addition to the survey (and to contacts with forty individuals in twenty five organisations) the project ran an Interest Group (FIG) with twenty two organisations as active members. The Group held eight formal meetings and fourteen interactive workshops. Average attendance at these meetings was 80% of the membership. In the project’s view these meetings provided an ideal opportunity for technology transfer and dissemination amongst the membership and meetings were notable for their openness and frankness (considering that some members were directly competing with each other).

The project went on to develop a generic assessment and certification framework which can be used to develop schemes for individual industry sectors. The framework identifies the parties that should be involved, the components that need to be assessed and certified, and the rules that

govern the process of assessment and certification. The framework was validated using the existing TickIT and Security schemes and then used to propose a scheme for the process industries.

The technical approach to assessment was based on IEC 1508 which was identified during the requirements survey as a key future influence. The technical approach meets the requirements that were expressed by members of the FRESCO Interest Group, including:

- flexibility to allow phased take-up of the standard
- meets the needs of all parties involved in the supply chain
- focuses on the safety of a particular PES
- covers the entire lifecycle, including maintenance and modification
- supports in-house as well as third party assessment.

The legal aspects of assessment and certification of Safety Related Programmable Electronic Systems were studied. This includes the liabilities that exist in the current law, the commercial implications of such liabilities and the liabilities that would exist in the proposed scheme. The influence that FRESCO assessment and certification might have on insurance premiums was also investigated.

Two case studies were conducted in order to validate the approach. These were drawn from the process chemical and pharmaceuticals sectors. The case studies provided valuable input in the development of the approach and demonstrated that the principles of the approach were sound.

A number of reports are available including:

- the results of the requirements survey [FRESCO *ref 3/1*]
- the organisational framework [*ref 4/1*]
- the technical approach [*ref 5/1*]
- the insurance survey results [*ref 6/5*]
- the final project report [*ref 9/3*].

Requirements Survey

The conclusions from the requirements survey were that the demand for assessment and certification in the process industries is currently of uncertain size and there may be limited take-up by industry. There is also only a limited amount of independent assessment performed within the sector in respect of safety-related systems.

Within the sector, in-house procedures are followed and better understood than public domain standards such as the HSE PES guidelines although company procedures do include recognised analysis techniques such as HAZOP for hazard identification and analysis.

However, the process industries sector feels that there are a number of benefits to be gained from assessment and certification, especially if there is a wide scope and applicability of the assessment approach. Overall system safety was of prime interest rather than software safety issues in isolation. The anticipated benefits include:

- improvements in the safety and performance of systems
- reduction of in-house assessment and validation costs through effective use of third party resources and expertise

- reduction in product recall and modification costs
- market advantage from having products that are certified being clearly differentiated from uncertified products
- demonstration of “due diligence” in the development and procurement of safety systems
- possible reductions in insurance premiums
- may alleviate the potential need for future prescriptive legislation if major incidents occur.

The survey suggested that a FRESCO assessment and certification scheme is relevant to other sectors but would need to reflect established safety procedures and practices in those sectors.

The study of European legislation suggested that the EU global approach to conformity assessment will become increasingly important as new directives and harmonised standards appear. There are no directives that deal directly with safety-related software systems but this means that a PES assessment and certification scheme would be well placed to provide a harmonised framework to underpin existing and future directives.

Any assessment scheme which aims for widespread acceptance within the EU must reflect the key principles of transparency and harmonisation. Similarly the issue of alternative routes to conformity through specified assessment “modules” would be an important influence on the structure of an assessment scheme.

IEC 1508 provides a feasible basis for an assessment scheme based on standards. Although the standard is in draft form and has a broad scope, it contains specific requirements on both the hardware and software aspects of a PES which can be used by an assessment scheme. The international standing of the standard should ensure that it is supported by national regulatory bodies and its generic scope makes it relevant to a number of industrial sectors. Although there will have to be a sector-specific interpretation for the standard to be fully accepted, this should give good scope for harmonisation activities in the EU.

Technical Approach

As noted above, the results of the Requirements Survey indicated that the emerging IEC 1508 standard would be a major influence on the development of safety-related systems in the future. It was therefore decided that the FRESCO Technical approach to the assessment of such systems should be based on this standard.

Other requirements for the FRESCO technical approach that were identified from the FRESCO Interest Group included:

- it must be flexible, robust, cost effective and acceptable to the users
- the method should be generic, with an initial instantiation based on IEC 1508
- it should accommodate the concept of component assessments which can be used together to provide assessments of entire products and systems
- the method should enable PES application independent features, application dependent features and operations and maintenance activities to be certificated, if required by the community
- assessment activities should focus on a specific PES
- the method should accommodate supply chains
- it should build on and complement existing assessment and certification schemes

- the components, their attributes and criteria for assessment should be readily available
- the method should accommodate an anticipated phased take-up of IEC 1508
- the method should have sufficient generality to be able to be used across many industry sectors.

The approach builds on the Functional Safety Assessment Process which is identified in IEC 1508. The expected development deliverables were identified from the standard and the required attributes were identified from the various clauses within the standard. The functional safety assessment process was broken down into stages and substages and the deliverables which need to be assessed at each of these were identified.

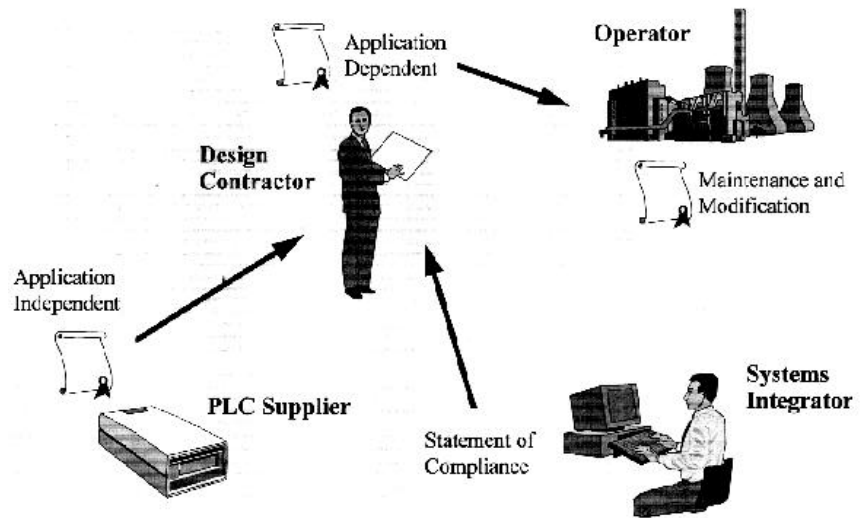


Figure 5.1. An example supply chain

Criteria for the assessment of deliverables were developed for each attribute that needs to be assessed. These criteria were based on previous assessment experiences within the project team. Application of the criteria enables an assessor to determine whether the deliverable in question conforms to the standard.

The technical approach recognises the existence of complex supply chains and is sufficiently flexible to accommodate this. A Statement of Compliance will be issued for staged assessments, and ultimately three levels of certification will be established in order to meet the requirements of different companies in the supply chain:

- Application Independent (eg PLC product)
- Application Dependent (eg plant protection system)
- Maintenance and Modification (eg for persons responsible for maintenance and modification activities).

Accreditation to the EN45000 series of standards is not mandatory for an assessment and certification scheme. However, these standards are a widely recognised means of assuring the competency and transparency of such schemes. They include specific requirements for impartiality, independence and the use of a quality management system with defined procedures for assessment and certification. Accreditation by a national or international body would provide clear recognition of compliance to these requirements by an assessment and certification provider.

Further details of the technical approach can be found in [FRESCO ref 5/1] which covers the development of the technical approach, the assessment method and procedures, work package definitions, assessment techniques, the definition of objects, attributes and criteria, and assessor competences.

Organisation Framework

A good assessment and certification scheme requires a sound organisational framework. It was originally planned to define an organisational approach which would meet the requirements of the process industries and then determine whether this approach could be made more generic. It was found, however, that the study of existing certification schemes enabled a generic framework to be defined and this could then be used to define a scheme for the process industries. This framework enables the organisation of assessment and certification to be described and the roles, responsibilities and interactions between the parties involved to be defined.

The project concluded that the FRESCO Framework can be used to define schemes which meet the requirements of particular industry sectors. This was validated by using the Framework to describe the Information Technology Security Evaluation Scheme and the TickIT (ISO 9000) Scheme. The Framework was then used to define a possible scheme for PES assessment and certification in the Process industries.

The framework identifies three groups of elements:

- Objects Anything which may be assessed against a set of criteria and a statement made about its compliance with those criteria;
- Rules Statements regarding invariant relationships between objects and subjects within a scheme;
- Subjects Those persons involved in the assessment and certification process.

Two case studies were conducted in order to validate the principles of the FRESCO approach and to test the detailed criteria. The first involved an existing control system for a batch manufacturing plant in the process chemicals sector. The second case study concerned a control system for a secondary manufacturing plant in the pharmaceuticals sector.

Each case study exercised particular aspects of the FRESCO assessment approach. In particular the first study demonstrated that the overall structure of the approach was usable and that the criteria, as had been defined at that time, could be applied with further refinement. The second study exercised the FRESCO assessment procedures and further demonstrated that the technical approach, including the criteria, was usable. In each case, the mapping of development deliverables and processes onto the requirements of IEC 1508 provided useful feedback regarding the system.

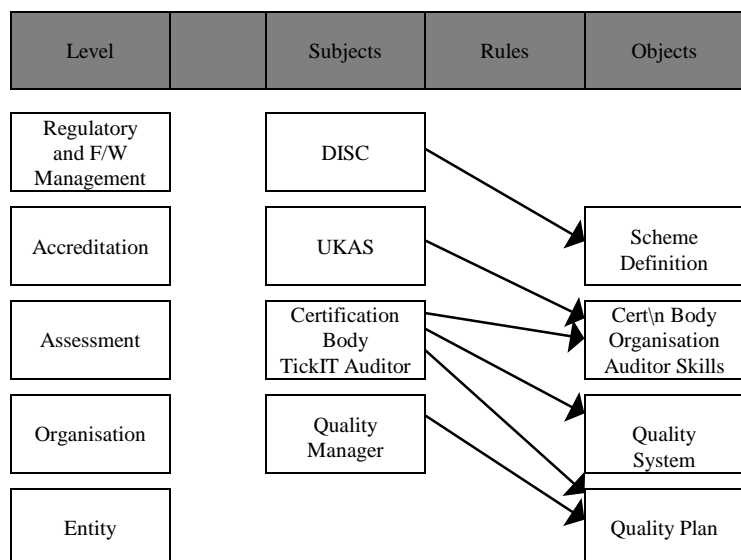


Figure 5.2. The FRESCO Framework applied to the TickIT Scheme

In a particular scheme, there may be a large number of objects and subjects which leads to quite complex relationships. In order to ease understanding, the above groups have been structured using five distinct levels:

- Regulatory and Framework Management
- Accreditation
- Assessment
- Organisation
- Entity.

A standard template for the definition of a scheme was developed. This contains:

- Statement of Objectives
- Identification of elements (subjects and objects present at each scheme level)
- Rules
- Roles and Responsibilities
- Certification Issues.

Legal Aspects

One FRESCO report [6/1], on “Current Law on Liability for Defective Safety-Critical Systems”, presented an overview of the current law in respect of the legal liability of suppliers of safety-critical systems. It concentrated on the basic principles of civil liability under the laws of contract, misrepresentation, tort and other common law doctrines and European Community (EC) law including Directives. It also noted how liability might be limited and the possible defences under the different heads.

Liability under the above heads can fall upon the manufacturer, supplier, distributor or certifier/assessor of products and components. Liability can sometimes be limited, for example by the use of limitation clauses and indemnities in contracts. However, certain liability can never be excluded altogether, for example death and personal injury. Therefore, if a component is used in a product which is exposed to the general public, the extent of potential liability can be enormous.

The report also touched upon criminal liability where necessary. For example, the possible exposure of company directors to a manslaughter charge.

A report [6/2] on the “Commercial Implications of the Current Law and Liability for Safety Critical Systems” looked at implications of the findings of the first report, particularly in respect of suppliers and assessors. The report summarised where, in the event of a claim arising from a defective safety-critical system, legal liability could fall. It concluded that liability could fall upon regulators, accreditors, assessors and the organisation that was assessed.

The report also examined the implications of potential civil liability in terms of financial cost and risk assessment, the costs of assessment and certification, the potential benefits of assessment and certification to both users of the assessment services and to society as a whole, and the public’s expectations regarding safety issues.

Finally, it briefly examined these issues in the context of the exploitation of FRESCO. The conclusion was that in establishing a scheme, FRESCO must ensure that the services provided offer sufficient benefit to justify the cost of participation in the scheme, as such a scheme is unlikely to be mandatory and will therefore have to be “sold” to users in terms of potential benefits.

See Chapter 2 for further information from the FRESCO project on the law concerning safety-related systems.

Insurance

An insurance survey was conducted to investigate the current attitude of the insurance sector to the introduction of a certification/assessment scheme and ultimately whether there would be any potential benefit to users of such schemes. A number of insurance experts, including underwriters and insurance brokers were interviewed and asked about various types of insurance relevant to a FRESCO scheme, how risks were assessed, and their own views on the advantages or disadvantages of such a scheme.

The general view was that participation in such a scheme would not affect the premium payable. This is mainly due to the fact that the assessment of risks is an art (based on experience of the underwriters and “feel good” factors) and not a science. It is, therefore, difficult to pinpoint what factors carry the most weight or the precise effect a certification scheme may have.

Further, the insurance industry tends to be reactive rather than proactive and generally it is only when things go wrong that the potential benefits of such schemes are looked at in more detail. However, if the scheme became well known, it might become the “norm” and therefore participation could be a positive attribute which might ultimately have an effect on premiums. The experts stressed that the scheme must be independent to be of value.

The general conclusion was that a FRESCO certification/assessment scheme would not have adverse effects on insurance and would be likely to be viewed as a “feel good” factor and, although in the short term may not reduce premiums, participation might help a company obtain the insurance in the first place and/or obtain insurance on more favourable terms.

The future

The ultimate goal of the project was to set in motion a process which would lead to general UK acceptance of the proposed assessment framework. Ensuring that there is available to UK industry a cost-effective means of assuring that safety-related software meets its safety criteria was and is seen as an important step in enabling UK industry to be competitive in the European and world markets.

5.2 Guidelines for assessment

As noted above, in the absence of an established framework for conducting assessments there are no absolute scales on which to base the judgements made while performing a system safety

assessment. In addition the assessor may be required to perform many different types of analysis on many types of system. Similarities can be identified in both the types of system and the analysis techniques, but so can many detailed differences.

The type of assessment approach required will be determined by a number of factors including:

- What the contract states: this could be to follow a specific standard, perform a specific task or solve a particular problem.
- Resource availability: how much to spend?, how much time is available?, what information is available? is there access to the users or developers?
- Technical feasibility: is the task feasible (often a factor of the contract, resources and the problem domain).

An analysis of these factors will determine the type of assessment to be applied to the system under investigation. As part of its work, the MORSE project developed a set of guidelines for safety assessment which seeks to relate the technical analysis process to these factors.

The proposed analysis method consists of a number of stages:

- a. Establish scope of the work and investigate the boundary of the system under investigation. The aim of this phase is to determine the exact nature of the required task, and then to establish what system elements require investigation to satisfy the task.
- b. Identify system hazards at the level of the system in its operating environment.
- c. Investigate these hazards and develop safety properties assigned to the system components.
- d. Collect evidence aimed at discharging the obligations raised by the safety properties.
- e. Form an assessment opinion, based results of (d).
- f. Each task of the analysis process (a, b, c, d and e) will be validated using a review procedure undertaken by a suitably qualified expert - who will be independent of the task under review.

The techniques used are problem-orientated, that is they are based on identifying hazards at the top level, and then analysing the system with respect to these hazards. These techniques have a strong theoretical basis and have proved useful in a wide variety of practical applications.

The activities involved are team-based and rely for their success on the dynamic interactions of the team members. The idea is that these teams will solve the problem of interpretation (which is a major source of error and misunderstanding) as a result of the interaction and discussions amongst the team members who will be highly experienced in a wide range of appropriate skills.

Points a to d are expanded on below.

The Scope and Boundary

The first step is to establish the scope of the work and to identify the boundary of system under investigation. The aim being to determine the exact nature of the required task, and then to establish what system elements require investigation to satisfy the task. The scope will be derived from consideration of the contract, resources and the problem domain.

The scope determines precisely what needs to be done, the next step is to identify what it needs to be done *on*. There is no definitive method of identifying the boundary of the task. However, some guidance can be given for a typical task type of the form “assess the safety of this software component”. In this case, the boundary which identifies all the sub-systems involved can be formulated by tracing the path from the overall system’s interaction with its environment back through the various sub-system levels to the software component of interest. This will identify an expansive list of sub-systems, some of which might be removed from consideration during the hazard identification phase. That is, the boundary will identify all those systems that might be involved, whilst the hazard identification will identify those that are relevant. Therefore, the hazard identification list will be a subset of this boundary list.

Hazard Identification

The objective of the analysis is to take the hazards identified at the level of the overall system in its operating environment and relate these to the sub-systems that constitute the overall system. In particular, the goal is to refine these system hazards into safety properties to make them applicable to the software components of the system where appropriate. That is, the refined hazard will be directly related to the software component if it is reasonable to do so and a suitable causal relationship exists. This indicates that techniques are required to:

- assist with the process of refining the top level hazards into safety properties so that they can be assigned to the appropriate sub-system component (especially software components)
- assist with the process of discharging these safety properties.

The hazard identification phase must occur at the level of the system in its operating environment. Ideally a number of different techniques should be used, since experience indicates that the different techniques tend to be best at identifying different classes of hazard:

- a. System specific checklist, based on previous experience of similar systems and/or similar environments;
- b. HAZOP
- c. FMEA (Failure Modes and Effects Analysis)
- d. Functional Block Analysis - where each sub-component is considered in terms of it occurring in the wrong place, not occurring at all and incorrect functionality.

Note that checklists can be used as a technique on their own, but will also form an important component of the other techniques. For more information see [MORSE *ref* D8]. Another important role for the hazard identification work is to confirm the elements in the system boundary.

Hazard Analysis - Refining Hazards

The approach for refining the hazards is based on the use of functional FTA. Fault Tree Analysis (FTA) is a top-down, deductive technique which starts with a single major effect and tries to

determine or deduce its cause from more basic events. It can be applied to functional or hardware (component) level systems, or to a suitable combination of the two. FTA is essentially a systematic qualitative technique to which a quantitative analysis can usually be applied if suitable failure data exists. Even in situations where failure data does not exist, it may still be useful to perform a FTA due to the insight it yields concerning a system's potential failure behaviour.

Success with the FTA technique depends on careful attention to detail concerning the method of construction. There is a need to avoid the tendency to rush into producing the fault tree without first carefully working through the initial steps of system definition and analysis. Further, even during the fault tree construction phase, the tendency to take short cuts must be avoided, lest important information is inadvertently discarded. The correct use of the FTA technique is a skilled operation which relies on the experience and expertise of the practitioner. to ensure that the many pitfalls are avoided.

Functional FTA is event orientated and is generally used at the higher system representation levels, for example at the specification or high level design stages. The system components are treated as "black boxes" and are formed into a hierarchical tree structure. At the root of the tree is the top event, which is the major undesired event under analysis. At the next or second level down are the events which directly and immediately contribute to the top event. The tree construction then proceeds by introducing the sub-events at the third level, which immediately and directly contribute to the failures of the events at the second level and so on. Eventually, the leaf nodes will contain the set of basic events which cause the failure at the top event.

The aim of the FTA is to produce a sound failure model of a (usually complex) system in terms of a specific disastrous or undesired event. The model explores the causes of this undesired event in terms of the system functions. This means that the technique can be applied at any level within the system design process where a coherent system description exists. Its role is to identify the system failure modes (qualitative, skilled process), and then, where possible, quantify them.

Evidence to Discharge Obligations

Verification and validation (V&V) techniques such as static code analysis, reviews and testing can be used to supply evidence to support the discharge of the safety obligations raised by the system's safety properties. This supply of supporting evidence can be:

- **direct**, where the evidence can be drawn directly from the V&V activities undertaken by the developer. This has the advantage of being relatively inexpensive, although there may be some costs associated with interpreting the evidence.
- **indirect**, where the safety investigation team uses the V&V tools used by the developer to perform specific analyses targeted at discharging specific obligations. This is most likely to involve the use of test harnesses, test stubs and test pro-formas.
- **independent**, where the safety investigation uses tools such as MALPAS or SPADE to perform specific analyses.

Overall the conclusion is that assessment cannot be regarded as a simple case of collecting measures, plugging them into an algorithm and presenting the results, since all the techniques, tools and judgements used will require careful justification. This means that assessment can be regarded as an exercise in obtaining a level of confidence by an appropriate examination of suitable evidence. The Guidelines produced by the project are available as report [MORSE *ref* D38].

	—A—		—I—
accreditation, 6		IEC 1508, 2, 3	
assessment, 1, 8		insurance, 7	
		ISO 9000, 5	
	—C—		—L—
case study, 5		legal, 6	
certification, 1		legal defence, 1	
checklist, 10			
	—D—		—M—
directors, 6		MALPAS, 11	
	—E—		—P—
European legislation, 3		pharmaceuticals sector, 2	
		process chemicals sector, 2	
	—F—	process industries, 1	
Failure Modes and Effects Analysis, 9			—S—
Fault Tree Analysis, 10		safety property, 9	
Functional Block Analysis, 9		SPADE, 11	
Functional FTA, 10			—T—
	—G—		
Guidelines, 11		team, 8	
		TickIT, 2, 5	
	—H—		—V—
hazard identification, 9		validation, 1	
HAZOP, 2, 9		verification and validation, 10	