

16 Safety-Related Engineering Design

Although most of the projects in the Programme were concerned with computers or programmable electronics which are in direct control of safety-related equipment, issues of safety also arise where computers are used in the design of engineering artefacts where there is the possibility of major damage or danger to life. There are many such engineering works, from the layout of road junctions, through the design of bridges and aircraft, to the design of nuclear reactors.

In many of these types of artefact, the computer is used for some form of modelling. It might be physical stress modelling in constructive works, as addressed by the SAFESA project, or dynamic performance modelling, such as the patterns of mixing and scavenging which occur in water treatment - whether purification or sewage processing - as addressed by the SAFE-DIS project.

Although starting from very different backgrounds, and using quite different terminology, these projects focused on similar aspects of the problem - that of validation of the design model. Both projects recognised that getting the model right depends upon human judgement. Both projects also broadened their scope to address safety aspects of other parts of the overall design process. And both projects developed support for the safety-related part of the design process so as better to guard against errors in design. But their approaches were interestingly different. SAFESA concentrated on formalisation of the process, so as to ensure appropriate checks and balances were applied to validate the modelling process throughout its life. SAFE-DIS took a slightly different tack and provided expert system support - initially to the designer so that he could access the best available knowledge on the appropriateness and adequacy of various models, and later to all those involved in management of a project to ensure that safety issues of all kinds were being addressed properly.

16.1 Safe structural analysis

Over the last two decades the engineering design environment has been changed radically by the emergence of the Finite Element Method. Its use within the design process is giving rise to situations in which increasing reliance is being placed on the results of uncorroborated analysis. This brings with it the question of whether structures can be demonstrated fit for purpose in respect of its ability to carry loads by using analysis alone, and the extent to which supporting tests are required.

Many practitioners argue that finite element analysis methods are mature enough to be used routinely and confidently. The mathematical basis is well established and great progress is evident in the control of discretisation and procedural error. At the same time standards covering the management and use of finite element methods in industrial practice are emerging, for example NAFEMS QSS¹. Notwithstanding these developments, there can still be very real difficulty in achieving a computer model which is an adequate representation of the real world.

¹ Supplement to ISO 9001 relating to Finite Element Analysis in the Design and Validation of Engineering Products. NAFEMS, 1993.

The difficulty is compounded by the power and utility of modern graphics-based pre-processors, which, although facilitating the structural modelling process, tend to mask its underlying details and make it more difficult to produce a satisfactory audit trail. Moreover, the widespread availability and apparent ease of use of pre-processing packages tends to encourage people with inadequate training to undertake finite element analysis. Accordingly, there is growing anecdotal evidence of significant differences between analytical predictions and the actual measured behaviour of structures.

It is against this background that the SAFESA project (SAFE Structural Analysis) developed the SAFESA™ approach. The purpose of the approach is to minimise the opportunity for error and to provide a basis from which confidence bounds can be established, so that the accuracy of the analysis is consistent with the requirement to demonstrate fitness for purpose.

Qualification

Structures are required to be designed, constructed and maintained to provide a level of integrity appropriate to their intended use and to the possible consequences in the event of failure. The process of demonstrating that a structure can meet its required level of integrity is referred to in the SAFESA approach as *qualification*. Different structures have different levels of integrity. Commercial civil aircraft and nuclear power stations, for example, are expected to meet high standards of structural integrity, while lower requirements would be imposed on a harbour tug or a wind turbine.

There are a large number of measures of structural performance used in different industries to determine a structure's fitness for purpose. Such measures are referred to in the SAFESA approach as qualification criteria. In broad terms, qualification criteria may be divided into three classes:

The first class comprises *empirical rules*. These largely pre-date the use of sophisticated analytical techniques and are based on experience. Frequently they are concerned with the specification of geometric parameters. Examples include rules for rivet spacing, slenderness ratios for compressive members, panel stiffening rules and blend radii for geometric discontinuities. They require little or no formal structural analysis. Nevertheless they are enormously useful in providing independent, albeit conservative, corroboration of structural adequacy.

The second class are criteria based on *permissible stress*. These are derived largely from the development of elastic stress theory in the nineteenth century. With these criteria, stresses under the various loadings are calculated and compared with 'allowable values'. The allowables are themselves largely based on experience, being set at such a level that regimes leading to failures are avoided, and thus they implicitly include a 'factor of safety'. The weakness of permissible stress criteria is that they cannot directly allow for the actual failure mechanism of the structural system, nor for the post-failure behaviour (failure being associated with inability to carry further load). Thus a highly redundant structure may have a considerable capacity beyond the first indication of failure, but this is not explicitly recognised in permissible stress based codes of practice.

The third class, *limit state* qualification criteria address these weaknesses. The basic idea in the limit state approach is to compare the resistance of the structure under various loadings

with their strength in appropriate limiting (cf. 'failure') states. The separate identification of resistance and limiting strengths, in principle requires separate calculations (i.e. finite element analyses), although in practice the quantification of strength is often determined from experience and embodied in codes of practice.

The role of finite element analysis in a structural qualification thus varies depending on the qualification criteria. The nature of the criteria and the requirements of any associated codes of practise strongly influence the type of analysis carried out and dictate what parameters are calculated and assessed. Nevertheless, the principles set out in the SAFESA approach are seen as applicable in all cases.

The SAFESA approach

The basis of the SAFESA approach is to formalise the structural qualification process such that the opportunity for error is minimised. Accordingly there are three stages:

Stage 1 - Defining the Scope

This is the initial stage before starting any detailed assessment or finite element analysis. It involves defining the qualification criteria, defining and bounding the structure to be analysed, initial planning of the analysis approach together with consideration of how the analysis is to be validated.

Stage 2 - Detailed Assessment

This stage involves detailed analysis and preliminary qualification according to the scope defined in Stage 1. A key aspect is the error assessment procedure. The procedure involves identification, quantification and treatment of errors. The idea is that errors are identified by their sources, then progressively reduced to an acceptable level.

There are eight sub-stages within the Detailed Assessment. In Stage 2.1, the process of idealisation continues to develop the high level description of the real structure, initiated in stage 1 into the structural model. The idealisation provides the basis of the computer model, which is subsequently generated by the process of discretisation and meshing (Stage 2.2).

The finite element analysis is then run to obtain a numerical solution for the computer model (Stage 2.3). Some post-processing (Stage 2.4) may be required to obtain a result set. This result set is then further manipulated (Stage 2.5) to obtain the response to be qualified. This can involve a reversal of the idealisation process. The allowable response of the real world structure is then calculated by application of the qualification criteria (Stage 2.6) and an initial assessment is made of how closely the qualification response compares with the allowable response. The level of effort needed in Stages 2.4 to 2.7 depends on the complexity of the idealisation and the nature of the qualification criteria. In some cases it may be trivial. Moreover, judgement is needed to ensure that the effort spent on these stages is consistent with the likely outcome of the validation review (Stage 2.8).

Finally, in Stage 2.8 the validation plan is reviewed to check that all its objectives are met and in particular that the appropriate model(s) have been adequately validated. This can include a follow-up error assessment and the creation of a test programme or the use of experience data.

Since SAFESA concentrates particularly on idealisation error Stage 2.1 (idealisation) is given particular attention.

Stage 3 - Conclusions

In this final stage the calculated results are compared with the acceptance criteria and conclusions are drawn as to the structures fitness for purpose.

Although listed sequentially above, the stages in the approach are not always executed sequentially nor in a single pass. Particularly in the Detailed Assessment (Stage 2) feedback loops often occur and several passes through a sub-stage may be required.

<p>1 Defining the Scope</p>	<p>1.1 Initial structural description 1.2 Problem overview 1.3 Structural issues 1.4 Analysis approach 1.5 Structural model 1.6 Validation plan 1.7 Review and approval</p>
<p>2 Detailed Assessment</p>	<p>2.1 Idealisation 2.2 Discretisation and meshing 2.3 Solving 2.4 Post-processing 2.5 Qualification response 2.6 Allowable response 2.7 Initial qualification 2.8 Validation review</p>
<p>3 Qualification Conclusions</p>	<p>3.1 Full qualification 3.2 Reporting 3.3 Approval</p>
<p>Figure 16.1. The SAFESA Qualification Process</p>	

Uncertainty in Structural Qualification

Inevitably many of the differences between the actual behaviour of a structure and that predicted by analysis are due to uncertainty in the physical description of the structure used in the analysis.

Uncertainty arises from a lack of understanding of the real world and its natural variability. It exists in numerous aspects such as the frequency and level of loading, the nature of accidental loading, the environmental conditions, the method of manufacture and the operating regime. For example, wind loads on buildings are random and highly variable; the level of loading on the gear lever of a car depends very much on how the vehicle is to be driven and the temperament of the driver; and the limited seismological data currently available means that engineers do not really know how frequently catastrophic earthquakes occur.

Differences due to uncertainty should be distinguished from those due to error. The former are embodied in the description of the real world. The latter are associated with the way the description of the real world is manipulated into a computational model and the accuracy with which the subsequent analysis is carried out. The SAFESA approach is concerned with error, particularly quantifying and minimising that error.

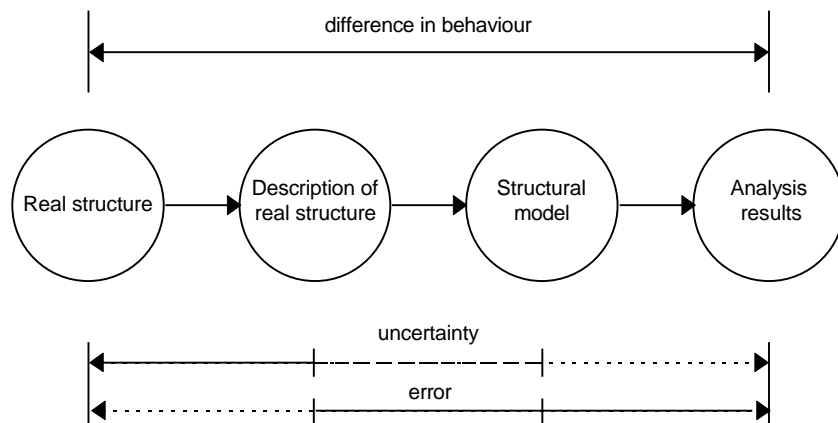


Figure 16.2. Uncertainty and Error

In carrying out the analysis one moves from the real structure (with its uncertainties) to a description of it and eventually to a structural model. This process is called *idealisation*.

Idealisation involves a series of approximations and assumptions about the structural behaviour which should be consistent with the use to which the results of the analyses are put (i.e. the qualification). The description of the real structure necessarily involves identifying and in some cases, removing sources of uncertainty in the real world structure. The description is influenced directly by the qualification criteria against which the structure is assessed, and the uncertainty is often explicitly accounted for in the qualification codes. For example, most building codes of practice address the uncertainty in wind loading by prescribing a design wind speed based on conservative probabilistic considerations. Similarly in some codes of practice material strength variability may be accounted for by stipulating 'lower shelf' values. However, not all uncertainties are so treated and others have to be addressed directly in the qualification. In this context it may be convenient to recognise three basic types of uncertainty, namely, physical (from natural sources), measurement (inability to identify and measure accurately the right quantity), epistemic (e.g. dearth of information about extreme events or future events).

Various sources of uncertainty will be identified in the course of a structural idealisation. With these identified and treated, all other differences between the results of an analysis and the real behaviour are attributed to idealisation 'error'. Sources of error can be identified concurrently with uncertainties and error treatment procedures applied to limit the error to acceptable bounds.

Error Assessment

The objective of the SAFESA error treatment technique is to locate error sources within the structural qualification procedure and reduce their effect to an acceptable threshold. Error treatment procedures involve the following tasks:

- identification of error sources
- quantification
- treatment.

The starting point in this process is the classification of errors. The SAFESA approach recognises four main classes of error according to the stage of the finite element process in which they are created:

- Modelling Errors - Resulting from the idealisation process (Stage 2.1)
- Procedural Errors- Due to discretisation, meshing and subsequent post-processing (Stages 2.2 and 2.4)
- Formulation Errors - Associated with the process of solving the finite element model (Stage 2.3)
- System Software Errors - Errors typical of any computer system.

The SAFESA approach concentrates on the treatment of modelling or idealisation errors.

Error treatment is effected in a variety of ways which include application of experience, simple calculations, comparison with tests, hierarchical modelling and sensitivity analysis.

Identification of idealisation errors

The classification above is useful to the analyst in identifying the type of errors which can occur in each stage of the qualification process. It does not, however, locate the error source in a very exact way within the finite element analysis or allow its effects to be assessed. In order to do this the concepts of *features* and *primitives* have been introduced into the analysis process. A feature is a component or part of the structure which can logically be treated as a separate item for idealisation purposes. Features should have clearly defined boundaries. Sub-division of a feature into another feature is possible and can be repeated as often as required by the analyst. The last feature to be identified in any hierarchy of sub-divisions is called a primitive and will have the following characteristics:

- A primitive is the irreducible entity in a feature beyond which the process of idealisation stops.
- A primitive should be well defined, i.e. it should have a well defined domain, boundary conditions, loading and material properties.

These concepts are familiar to all analysts who traditionally divide a structural model according to its characteristic behaviour patterns. However, in the present application the role of the

primitive is to locate errors. For example, in a specific structure two panels riveted together along their edges might be regarded as a primitive and analysed as a plate. The associated error is the difference between the behaviour as portrayed by plate theory and that which could in principle be observed as the real joint. The detailed qualification requirements have a critical bearing on the selection of the primitive. If the qualification requires assessing the growth of a crack under the rivet head, then the primitive could be the head region. The latter would obviously involve a more detailed finite element model. Thus, the decisions relating to the error control process are the key issues in deciding on the level of detail in the idealisation.

Publications

The SAFESA project has produced three publications defining the method.

The 'SAFESA Management Guidelines' provides a high level description of the technical issues to be addressed when using finite element analysis in the qualification of structures. [SAFESA ref 2]

The SAFESA Technical Manual provides a detailed description of the approach and an explanation of the underlying rationale for it. [SAFESA ref 3]

A companion document, named 'The Quick Reference Guide' provides a succinct description of the SAFESA approach and is primarily intended as a reference for experienced practitioners. [SAFESA ref 1]

16.2 Safe Design of Networks

Networks are all-pervasive: civilisation as we know it would not exist without the hazard-free design and operation of energy networks (electricity, gas, oil networks), of communications networks (telephone, radio networks), and of water-carrying networks. Developments in information systems, particularly document management, knowledge-based systems, and simulation systems, can be used to help in safely maintaining, extending and, if necessary, decommissioning such strategic networks.

The **SAFE Design of Networks using Information Systems (SAFE-DIS)** project was concerned with safety-related questions regarding the safe design, cost-effective repair and the subsequent hazard-free operation of large *in-situ* water-carrying networks. These networks serve large conurbations and comprise hundreds if not thousands of conduits (pipes) interconnected through an equal number of nodes (including inflows, outfalls, pumps, storage locations). Changes in the design and subsequent repair, sometimes termed *rehabilitation*, of such networks are classed as capital projects.

Previously the sophisticated nature of simulation modelling software for water distribution and drainage networks required highly skilled experts to apply them in order to derive some degree of confidence in the results produced. Increasingly however, such modelling tools are now regarded as being appropriate and necessary for practising engineers. This has led to concern whether the application of the software in terms of building, developing and applying models is done adequately for safe engineering design. Because of the complexity of the modelling process there is no way that results from a model application can be guaranteed to be safe. Instead the

project concluded that the users of the software have to be encouraged to develop safe models through interaction with and the support of an intelligent information system.

This knowledge of safe modelling is distributed literally and metaphorically. In parts this knowledge is personal - usually the privy of experienced design engineers - and is passed on literally by word of mouth to the novice designers. Supplementing this experiential, undocumented knowledge is the textual archive comprising text books, learned journals, and manuals, etc. The experiential knowledge interprets and amplifies the textual knowledge. This textual knowledge is the repository of verified and validated experiential knowledge.

The SAFE-DIS project has demonstrated how this word-of-mouth knowledge or experiential knowledge can be archived and used in conjunction with the textual archive. Sometimes the experiential knowledge is used to interpret and amplify contents of the textual archives, and, at other times, the experiential knowledge can be validated and verified using the archives

The project has identified four distinct groups of tools and techniques that may help in the safe rehabilitation of complex networks:

- intelligent access to electronic documents
- semi-automatic procedures for 'pockets' of knowledge
- sensitivity, uncertainty and risk analyses
- model history and audit

The project collected, structured and organised knowledge related to the safe and cost-effective rehabilitation of water networks from experts, from specialist texts and elsewhere, and built a knowledge-based system that can (a) help experts to examine their own knowledge and (b) help novices to a greater or lesser degree throughout various phases of the complex rehabilitation process.

Round Table

The SAFE-DIS project was joined by a group, the *SAFE-DIS Round Table*, comprising members from the private sector (three UK Water Companies), public sector (two local government-related organisations) and a UK civil engineering consultancy.

SAFE-DIS: An Information System for ensuring safety during network rehabilitation

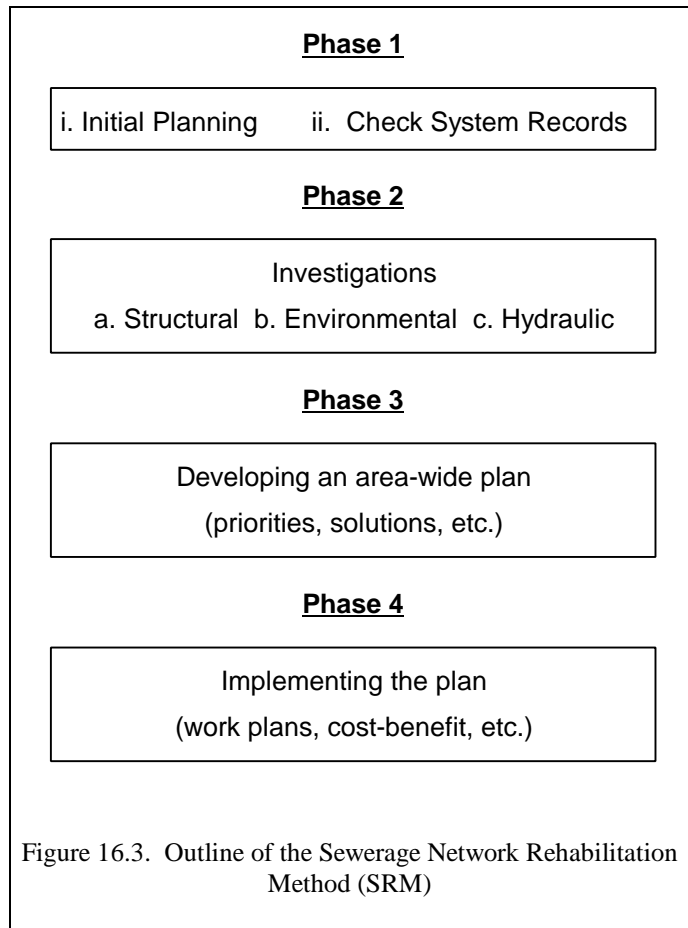
The information system developed by the project team animates the behaviour of an experienced engineer setting a number of tasks for a less-experienced engineer to execute. This animation is based on an industry-wide rehabilitation procedure, the Sewerage Network Rehabilitation Method (SRM) established by the UK Water Research Centre through a consultation with the UK water industry lasting over 10 years. This method is outlined in figure 16.3. Some of the phases, like Phases 1 and 2, are divided into sub-phases. Each (sub-)phase is subdivided into independent tasks. In all there are over 20 specialist tasks distributed over the 4 major phases. SRM was devised when the water industry was in the state sector.

The SAFE-DIS system (strictly SAFE-DIS II) acts within the framework of the SRM method. During the execution of individual phases, and tasks within a phase, the system provides *expert advice*, based on rules of thumb and other heuristics obtained from experts. Proactively, the system can access excerpts and (optionally) full-text from a corpus of texts, some of which are linked through hypertext links: a digital library that was built in close collaboration with the Round Table. The advice is supplemented by access to *data bases* containing details of the various components of a given network and its geographical location, and supplemented by access to an industry-standard *simulation model*, namely *HydroWorks* developed and marketed by Wallingford Software.

Equally importantly the system keeps a ‘*diary*’ of advice it gives to a user and the user can also enter his or her comment on the advice given. *Risk analysis*, an important tool in the safety community, can be undertaken through SAFE-DIS by the use of a low-cost, easy-to-use, and off-the-shelf system (namely Crystal Ball marketed by Decision Engineering Ltd). The information system also provides access to the World-Wide Web and through the Web provides access to up to date information related to engineering, legal and safety aspects of the aquatic environment as and when it becomes available on the Web. More advanced users of the information system have access to a text analysis system (namely *System Quirk*).

In ‘professional’ mode, experts can browse through the system, add more knowledge, modify or delete existing knowledge, and select some or all the phases, and tasks within the phases, for execution by less-experienced engineers. ‘Roster’ mode refers to operation of the system by novices, where advice is provided and the novice can browse through the text corpus and access data bases and simulation models.

The text corpus comprises: safety guidelines and procedures, transcripts of expert interviews, learned papers and technical notes, legal texts including the complete Water Resources Act 1991 and a 450 page book that interprets the Act. The text corpus also includes a terminology data base. All the texts relate in one way or another to the rehabilitation of water-carrying networks. During the execution of each of the rehabilitation tasks, the user of the system, is guided through a question and answer session that includes display of *safety labels* on advice excerpts.



Structure of the SAFE-DIS Workbench

The SAFE-DIS Workbench comprises the following subsystems:

Subsystem	Function
Task Selection & Display Manager	Enables an expert or manager to select rehabilitation tasks for a given project to be executed by a less experienced engineer.
Knowledge Manager	Manages the knowledge base of the SAFE-DIS system and contains rules related to various rehabilitation tasks
Yellow Pages Manager	Tracks the task a given user is executing and selects relevant excerpts (paragraphs and pages) from a full text-data base.
Safety Labels Manager	Displays 'safety labels' during or after the execution of a rehabilitation task
Diary Manager	Tracks when and how successfully each task was executed and notes it in a diary. The diary can be annotated by the end-user also.
Report Generator	Generates an 'audit' report based mainly on the contents of the 'diary'
Plug-In Manager	Helps access data in proprietary data bases and acts as a front end for simulation software.

SAFE-DIS can be configured by senior design engineers in two important respects. The first level of (re-)configuration is at the knowledge-levels whereby a designated user can add or delete subtasks to any of the four phases of the SRM method. The second level of configuration is one where the senior engineer selects specific subtasks from one or all the four phases which he or she thinks should be investigated by one or more engineers reporting to him or her.

During interaction the workbench provides pro-active advice: excerpts of texts shown in the so-called 'Yellow Pages'. Safety labels are sometimes displayed concurrently with the Yellow Pages. The labels come in three 'colours': *red* for mandatory warnings; *amber* for potential hazards; and *green* for safety notes. The access to full documentation, including Technical Notes (about 10 in number) authored by leading rehabilitation experts in the UK together with expert interviews and legislation is also provided by the workbench.

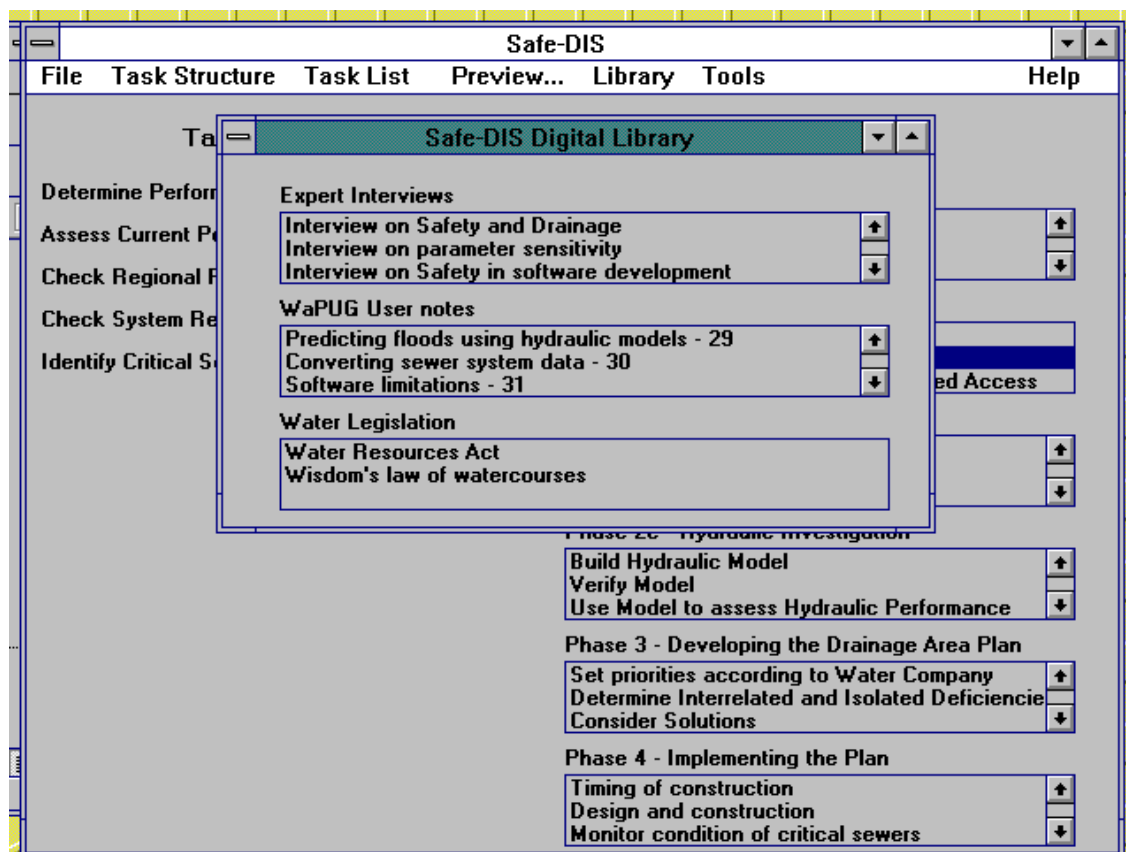


Figure 16.4. SAFE-DIS Workbench providing access to its 'digital library'

Knowledge Documentation

The project used a number of knowledge acquisition techniques including face-to-face video taped interviews, brainstorming, structured walk-throughs, questionnaires, and interactive rule elicitation. Face-to-face interviews between experts and system builders were held on topics related to the safe rehabilitation of networks based on a case study. The questions in the interview were devised by the Round Table. Each interview was video-taped and the transcript of each interview was discussed by the Round Table. The system builders extracted specialist terminology from the interviews, and extracted heuristics and rules. The transcript was marked up such that key parts of the interview could be extracted and linked to other documents through a hypertext browser.

The brainstorming sessions were focused on specific phases of the rehabilitation procedures. Individual members of the Round Table were given responsibility for providing knowledge related to given tasks in a specific phase; a detailed transcript of each of the sessions was prepared and circulated to the other members.

Corrections and modifications to the transcripts of the interviews and the brainstorming sessions were agreed by the Round Table as a whole. This consensus enabled the system builders to use verified and validated knowledge rather than the (unrevised) knowledge of a single expert as is the case in many knowledge-based systems projects.

Structured walk-throughs helped in establishing the manner in which the various tasks within a phase are to be structured and in adding more knowledge for a task which the SAFE-DIS system could already execute.

The interviewees and the participants in the brainstorming and structured-walk-throughs, were reminded that what the systems' builders were keenly interested in was safety-related information. In order to stress the point, questionnaires were specifically sent that comprised questions that dealt with safety assurance and hazard elimination in specific tasks that make up the rehabilitation phases.

Rule elicitation was used to develop automated / standardised procedures. These procedures, mini knowledge-bases, are particularly useful where the task is amenable to formal description; automating according to a procedure agreed upon by experts will then improve safety. During the structured walk-throughs the engineers provided rules and algorithms for various stages of the modelling process, e.g. choosing coefficients of discharge, accounting for unmodelled storage and checking for limits when doing catchment breakdown.

Safe Hydroinformatics

Hydroinformatics is a multidisciplinary subject that deals with the management of the aquatic environment using information technology. Because of the complexity of both the natural aquatic environment and any corresponding hydroinformatics system, and the need to be assured that the management is properly executed, it is inevitable that questions arise as to the reliability and safety of the decision making based on the IT system. This raises questions about the reliability and safe operation of the IT system that is at the heart of a hydroinformatics system.

The fail-safe operation of an IT system is dependent on a number of factors including the elicitation of accurate requirements, formally correct design, plausible simulation models, appropriate user navigation, and so on. 'Safe hydroinformatics', like its generic counterpart 'safe IT', is about safe management of information concerning the aquatic environment, including the safe processing of input to and output from a simulation model through a complex mix of heuristic knowledge-based, database management, and feedback systems.

Design, operation and repair of complex networks is a knowledge-based task that involves the use of experiential knowledge, the use of simulation models and access to data bases. Safety in the design of such networks is seldom discussed, but it is assumed that the knowledge of the expert designer will help in minimising a plethora of risks leading to the failure of the network. Much of the knowledge of designing 'fail-safe' and 'hazard-free' networks is experiential and qualitative. Such knowledge can, in principle, be captured and represented through the use of interview- and text-based knowledge acquisition techniques. This semi-formalised knowledge can then be used in conjunction with simulation software for disseminating knowledge related to safe design of complex networks, like water carrying networks.

The SAFE-DIS project has created a generic environment that engenders the implementation and application of safety-critical hydroinformatics systems using urban drainage as an exemplar. For further information about the SAFE-DIS Workbench and the other outputs of the project, see the references listed on the 'Project Poster' in Appendix A.