

Joseph B. Comerford, Paolo Salvaneschi, Marco Lazzari, Paolo Bonaldi, Giovanni Ruggeri, Michele Fanelli, Gabriella Giuseppetti, Guido Mazzà, "The role of AI technology in the management of dam safety: the DAMSAFE system", *Dam Engineering*, 3(4), 1992

The role of AI technology in the management of dam safety: The DAMSAFE system

Joseph B. Comerford, Paolo Salvaneschi, Marco Lazzari, Paolo Bonaldi, Giovanni Ruggeri, Michele Fanelli, Gabriella Giuseppetti, Guido Mazzà[§]

SUMMARY

This paper derives from a project in progress at ISMES which aims to investigate the application of Artificial Intelligence techniques in the field of dam safety, and to develop a prototype software system. In order to carry out this task it was necessary to develop a conceptual framework within which the techniques of AI could be employed.

Therefore the first part of this paper describes the approach to dam safety adopted in this project. It is founded on the view that safety of structures is a problem of continuing management from design through construction to operation, and that this management of safety is a quality management problem, requiring the determination of quality procedures and information flows. In describing the reasons for adopting this approach to safety, the status of such measures of safety as probability of failure are discussed. It is argued that factors of safety and probabilities of failure are features of theoretical models to be used in the management of safety rather than attributes of the dam itself. The management of safety process involves identification of hazards, defined in this context as precursors to failure, through hazard auditing as part of the quality management procedure. The application of these quality procedures is realised through testing information about the project against quality standards or some form of normative reference models. Dependability indices are suggested as possible measures designed to reflect the degree of auditing to which a project has been subjected. This approach to dam safety is seen as being in the same spirit as that of the SEED method of USER.

The second part of the paper describes how AI techniques can assist engineers in the management of this process. The view taken in this paper of AI is that it consists of new methods, which have been developed in recent years, of modelling systems and their behaviour, of representing and manipulating information, and of reasoning about both of these. The subject of AI is not covered in detail but the reader is referred to the appropriate sources. AI is seen as contributing to the problem of managing dam safety through providing an environment for integrating information relevant to the dam, for innovative modelling of dam behaviour, and for developing agents to reason about both of these.

An expert system is described, DAMSAFE, which is being developed at ISMES.

Keywords: Artificial Intelligence, Automatic Monitoring Systems, Causal Networks, Dam Safety, Decision Support Systems, Expert Systems, Knowledge-Based Systems, Safety Management, Structural Health Monitoring, Structural Monitoring, Structural Safety, Visual Inspections

Introduction

In recent decades there has been increasing attention paid to the problem of safety of existing dams. These efforts have arisen, partly in response to legislation in a number of countries, laying down

[§] JBC, PS, ML, PB, GR: ISMES S.p.A, Bergamo, Italy; MF, GG, GM: ENEL Centro Ricerca Idraulica e Strutturale, Milan, Italy

statutory requirements for inspection and assessment of dams. The legislation has been enacted generally in response to dam failures which have occurred in a number of countries in this century. The concern for dam safety has paralleled a general increase in public awareness of issues of safety of engineered artefacts (structures, industrial installations and power generation plants).

The concern with dam safety has led to the development of procedures for periodic dam inspections the establishment of monitoring systems in some dams and the development of methodologies for assessment of all the information concerning a particular dam in periodic safety checks. The approach taken by USBR (USBR, 1983) through the SEED programme is an example of a systematic method of collecting and evaluating information about dam safety.

1 Safety and failure

In recent years, there has been an increasing use of methods of quantitative risk assessment, to make predictions about the level of safety or risk associated with structures and industrial plants particularly those with catastrophic potential. These techniques have been extended to dams for assessment of safety. Parameters such as probability of failure, factor of safety and level of risk have been calculated (Kreuzer and Bury [1991], Oosthuizen et al. [1991]) as part of this prediction of safety.

These methods involve hypothesising a closed set of failure scenarios, attributing a probability to the occurrence of each scenario, to arrive at an overall parameter which is attributed to the structure itself and has an objective existence like the strength of the concrete or the height of the dam. However, the meaning of the parameters resulting from such analyses is not always clear and is rarely discussed in the literature, as Fanelli [1992] has pointed out.

This section seeks to show that safety of dams (and structures in general) is a continuing management problem through the life of the dam, linked to quality, and though measures of the level of safety may assist in this problem, they only form part of the overall picture. Before discussing the relationship between safety and quality it is worth first examining the status of measures arising from quantitative risk analysis.

1.1 Measures of safety

Comerford and Blockley [1992] have argued that the "probability of failure" of a structure is not an attribute of the structure but an attribute of the mathematical model within which it is calculated.

In fact it only has a meaning within the context of the model. The concept probability of failure is often used as if it were an attribute of the structure (with the same status as the height) for decision making about safety.

Due to the uncertainty and incompleteness associated with failure models and the civil engineering process in general, other more complete measures of the quality of a project are required in decision making about safety. The relationship between the calculated "probability of failure" or "factor of safety" (derived in models) and the frequency (or "chance") of failure of civil engineering structures is necessarily always unknown. These parameters are design criteria which, if satisfied, contribute to the quality (and safety) of the structure together with other important factors (for example, a dam may have a high design factor of safety but may be poorly constructed)

The introduction and use of probability theory in structural safety has apparently provided a theoretical framework for dealing with uncertainty. However there are problems of completeness with all theories and though probability is suited to modelling the uncertainty associated with the parameters of a theory, the incompleteness remains.

A theory cannot include all of the phenomena in a problem, only those specifically chosen to be represented.

Moreover, the scope (in space, time or other variable) within which the theory remains reliable may be to some extent unclear. Similarly, when a theory is used to represent the behaviour of some engineering system in order to form a theoretical model, then only certain features are abstracted. The model is constructed from a particular point of view with certain objectives

(for decision making) in mind. All models are thus partial representations of the world built for a particular purpose and can only be satisfactorily and safely used when that purpose and the scope of the model are clearly understood.

For civil engineering structures, failure models are characterised by high levels of uncertainty and incompleteness due to: the difficulties of assessing probabilities of extreme events, of representing an exhaustive and realistic set of failure scenarios, the socio-technical nature of many failures (Pidgeon, Blockley and Turner [1986]), and the impossibility of testing such models.

It is argued, therefore, that factors of safety and probabilities of failure should be viewed as features of the necessarily incomplete models we have developed to represent certain types of behaviour and have meaning only in the context of the model. They are evidence to be used with other evidence in the management of safety.

1.2 Failures

Investigations and case studies of failures indicate that many failures arise from problems at the sociotechnical interface of engineering. This source or set of common causes of failure is sometimes referred to as "human error" and sometimes as "gross error". Neither of these terms seems very helpful in thinking about such problems. Turner's model [1978] of how failures occur is one where precursors to failure can build up through the course of a project (through design, construction and operation) and which when combined with a trigger event precipitate a failure. It is clear from studies that failures are rarely due to one single "gross error" but are in fact due to a number of factors, or precursors coming together in an unforeseen way. The fact that they are unforeseen means that they necessarily fall outside the set of scenarios of failure modelling used in the probability of failure calculations described above. The use of the terms "gross error" and "human error", tends to obscure the fact of the fallibility of the models that we use to represent the possible behaviours of the dam and its surrounding environment. As mentioned earlier, this fallibility means that the "chance or likelihood of failure" of a structure is essentially unknowable. The approach where dam safety is viewed only as a problem of periodically establishing that a probability of failure of the dam is satisfactorily small could lead to a false sense of security.

Research into the nature of failures and disasters in a general sense (Fischhoff et al [1981], Perrow [1984], Pidgeon, [1988]) has indicated that the failure modelling itself fails to account for the occurrence of many failures of technical systems due to the system complexity and sociotechnical nature of many of these systems. This obviously raises the question "If we cannot know the likelihood of failure of a dam, what approach must we take to safety?" Management of safety is seen as depending on management of quality, through the application of quality testing (or hazard auditing) procedures, management of information flows, and the consequent decision making/action.

2 Management of safety

Whereas assessment or prediction of risk is an act, a calculation made at some point of time, management of safety is a continuous procedure. Management of safety requires a continuing feedback of information. The incompleteness and uncertainty surrounding the models used, and the fact that the structure and its environment are undergoing continuous change require that any conclusions about safety must be always under review. Since most concern about safety in dam engineering is directed at existing structures, where design and construction has already taken place, such quality procedures can only be applied to these phases retrospectively. The extent to which this can be done depends on the information available concerning the design (drawings calculations, and investigations) and construction records (site records and laboratory test results). Alternatively the information can be extended by posts analysis and site re-investigation and structural testing. Therefore since safety is dependent on the implementation of quality procedures, which require information, safety depends to some degree on the quality and extent of information available.

3 Quality testing or hazard auditing of dams

Comerford and Blockley [1992] have suggested that the change of emphasis from assessment of safety, or and calculation of risk to the notion of management of safety can be facilitated by moving from the concept of the safety of a dam to one of dependability.

Standards for the absolute "level of safety" cannot be established for the reasons given above, but an accepted degree of dependability by specifying what type of "testing" a dam of any given type must endure. The development of a "safe" dam, we argue, is obtained by the process of critical testing of the design, construction, and operation of the dam throughout its life.

This quality testing can be viewed as "Hazard Auditing". Since a hazard is a set of preconditions to failure then a hazard audit may be aimed at detecting whether an accident is incubating by testing for the sorts of factors which can lead to failure. The dependability of the dam accrues from the carrying out of these audits throughout the life of the dam. This approach is similar to that used in HAZOP studies in the chemical industry (Chemical Industries Health and Safety Council [1977]), which is a structured discovery technique for identification of hazards in a project design and operation.

Comerford and Blockley [1992] have suggested the use of dependability indices as measures of the quality of a structure. There is an important difference between a dependability index and hazard indices of the type developed by Hagen (Committee on Safety of Existing Dams [1980]) and used in the chemical industry (Lewis [1980]), which reflect the level of hazards identified. The dependability index reflects the quality testing procedures a dam has undergone.

In the field of software engineering, whose tasks and products have many similarities with those of civil engineering (usually one off products which are difficult to test extensively) a similar approach to that outlined above has been adopted for problems of software reliability. Qualitative measures of attributes of the design and development process, and of the product itself are used as quality measures. These indices of quality are seen as measures of reliability of the software (Forse [1989]).

The monitoring of dams in Italy is a procedure of the type described above for operational safety management (Fanelli [1992], Bonaldi et al. [1988], Bonaldi et al. [1982]). In this approach, values of monitored variables are compared with the predictions of mathematical models of dam behaviour to make judgements about the behaviour of the dam. Effectively the state of the dam is tested against normative reference models as a hazard testing procedure. These normative models represent "quality models" for behaviour of the structure. They derive from numerical "deterministic" theories and analysis of past behaviour of the dam. In both cases the behaviour of the structure represents desirable or required states of the dam. This concept of desirable states (and undesirable states) as quality modelling of dams for use in hazard auditing can be extended.

The SEED programme has identified in a general way much of the data required to be tested A concerning the design, construction and operation of the dam. The quality models obviously have to be defined by owner and operator organisations in accordance with their own outlook, objectives and preferences.

4 Required states and undesirable states

The representation of two distinct sets of states, defining the zones of the state space, in which the behaviour of a complex system is regarded as desirable (or required) and conversely undesirable, has been used in control of complex systems (Salvaneschi [1984]). The two-set states can be defined for a dam in a number of ways but are essentially some form of model of the design, construction and operation which represents a set of required states and a set of undesirable states of the dam. The fact that the undesirable states are not necessarily the area outside the desirable states reflects firstly, the uncertainty, incompleteness, and vagueness, associated with the description of the states and the

knowledge of the position (in the state space) of the dam itself; secondly, the various origins of their definition (theoretical, empirical, and statutory).

We can distinguish the following ways of defining these states:

1. Where the required or undesirable states of the actual dam are based on engineering judgement. These are states not easily represented numerically (e.g. condition of concrete, degree of cracking). The test of the dam is the comparison of the actual state of the dam, revealed through visual inspections and assessments of the dam, with such a desirable state to make a judgement about its condition.
2. Where the required states of the actual dam are based on the predictions of some formal model of desirable behaviour (for example, deflections and stresses predicted by finite element analysis). The predictions of the formal model are compared with results of monitoring to test the dam.
3. Where the past state defines a desirable state and the test of the dam lies in comparison of present observations with past observations. This is based on the concept of continuity and equilibrium, where, since the dam has not failed in the past, its past state constitutes in some sense a desirable state and any departure from this state is a cause for alarm.
4. They are given by some specification of the management and organisational factors (for example, monitoring, site inspection, operational procedures), which are either desirable or undesirable.

5 The contribution of AI

In this section, a general view of the aspects of the set of techniques and tools which come under the heading of AI will be given, in so far as they are of interest to the problem of dam safety management.

The discussion above has emphasised the importance of collection and management of information and the testing of this information against normative "quality" models for safety management. Developments in the field of software engineering have provided a wealth of new tools and techniques

which can assist engineers in this task (Comerford and Stone [1992]). From the safety management point of view the utility of these methods lies in the ability to integrate within a software environment, representations of information of various types, new ways of modelling physical systems, and different ways of reasoning with both of these. This extends the capabilities of traditional software technologies allowing the development of new and more complex software systems.

Conventional computer programs used in engineering have proved successful in many tasks where a procedural execution of an algorithm for analysis, prediction or simulation is required. However, they are less well suited to the task of safety management in a more general sense for a number of reasons. Firstly, the models of the behaviour of the system used in the calculations are represented implicitly in the code; therefore, the model is usually neither easily accessible or changed in the light of new information. Secondly, there is no explicit representation of the uncertainty associated with the model used in the calculations. Thirdly, the boundaries of the model, that is the limits to what is represented and what is not, are not obvious. Finally, the operation of the model is a fixed concept to produce certain types of outputs given certain types of inputs.

AI concepts and technologies provide new methods and approaches to modelling physical systems, such as qualitative physical models (models expressed in non-numerical terms) which can be integrated with conventional engineering models, to provide descriptions of a system at different levels of detail and from different points of view (Comerford and Stone [1992]). Knowledge concerning the structure of the problem domain, strategies for reasoning within the domain under different circumstances and knowledge of the limits, relevance and competence of the models and strategies can be represented as models of human reasoning. Knowledge arising from different sources: domain theories, codes of practice and experience can be integrated and used to interpret and manipulate the qualitative and quantitative data of interest (Comerford, Lazzari, Pina et al. [1992]). AI environments can provide extensive communication between the user, the models, and the reasoning mechanisms to produce a type of cooperative system of user and machine.

6 DAMSAFE

The Damsafe is a system being developed at ISMES as an environment to implement the approach to dam safety described earlier, using the tools of artificial intelligence. It is a system in which different types of information (design records, photographs, design drawings, test and monitoring data, qualitative assessments of condition) concerning a dam and different types of models of the dam system (numerical structural models, data models, normative models for behaviour) can be united to assist the engineer in carrying out the procedures of hazard testing on the dam project information. The system provides a platform in which the state of the project can be represented and then tested against a variety of normative models. The system is intended as a co-operative management tool assisting the engineer to carry out a hazard auditing process.

The extended modelling capabilities of an environment provided by AI described above enables a wide variety of normative models to be constructed. These normative models which represent the desired and undesired states can be both quantitative and qualitative, data models (thresholds on data values), as well as numerical structural models.

The system developed so far is a prototype which enables hazard audits to be carried out on descriptions of the dam and behaviour of the dam coming from operational monitoring. The structure of the system from a software engineering point of view is described in detail elsewhere (Comerford, Lazzari, Pina et al. [1992], Salvaneschi [1991]). However, there are three main entities within the system's conceptual design which are contained within an integration environment:

- models of the physical world; These models can be divided into:
 - those which describe the present state of the physical world
 - those that describe desirable states of the physical world
 - those that describe undesirable states of the physical world.These models are constructed utilising the variety of modelling techniques described earlier.
- models of human reasoning (reasoning agents); These are models of reasoning about the problem domain, including mathematical reasoning, logical reasoning and strategies for problem solving (Comerford and Stone [1992])
- communication mechanisms; The communication mechanisms take the form of interfacing systems which enable the user to "co-operate" with the system. This takes place through open access to the reasoning agents and physical world models contained within the environment.

6.1 Structure of the prototype system

The system is comprised of two physical world models, three reasoning agents and an interface. The structure of the prototype is shown in Figure 1. There are two physical worlds which make up the problem domain. The data world, in which are represented all the relevant concepts related to data received from monitoring, and the dam world containing all the relevant concepts related to the physical world of the dam. The reasoning agents act on the physical world models, and contain the knowledge required to reason about the concepts of these models. They perform a variety of tasks, the most important being that of relating the concepts in the data world to those in the dam system world.

6.11 Data world

The concepts which constitute the data world are those used by engineers in discussing and interpreting the data for dam safety. Some of these concepts, are expressed quantitatively, that is, numerically,

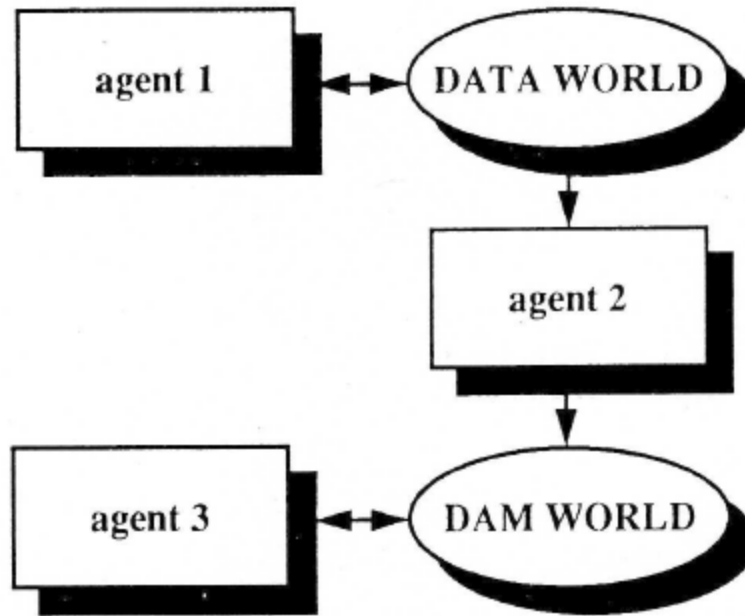


Figure 1. Structure of DAMSAFE prototype system

others are expressed qualitatively. Within this model are the features of data which are significant for identifying particular behaviours and states of the dam system. Therefore this model contains time series of instrument readings, details of the type of variable represented and how and where the data were obtained. Features such as peaks, trends and cycles, identified in different types of time series are recorded in this model.

6.12 Dam world

This world contains a model of the physical world of the dam and its environment, concepts describing the possible states of this world and a set of concepts modelling the possible behaviours of the dam and its environment. The physical dam model describes the dam and its environment as a hierarchy of objects (a hierarchical object-oriented model). These objects have attributes, which taken as a set, describe the state of the system. The model of the behaviours of the dam system is a set of processes connected in a causal network (Figure 2).

The causal network models how behaviours of the dam and its environment can interlink in a causal way resulting in scenarios as one process leads to another. The full net includes eighty different processes describing possible dam behaviour. This network has been derived from published case studies of dam failures and accidents and from discussions with experts in the field of dam design and safety. The conditions under which one process can lead to another have been included. Each of these processes has been documented along with descriptions of how evidence of these processes might be manifested in the monitoring data and also in reports from visual inspections.

6.13 Reasoning agents

There are three reasoning agents. The first (Figure 1) operates solely on the data world to manipulate the data and extract features from the data sets of importance. The second reasoning agent performs the task of interpretation identifying the possible behaviours of the dam in terms of set of processes

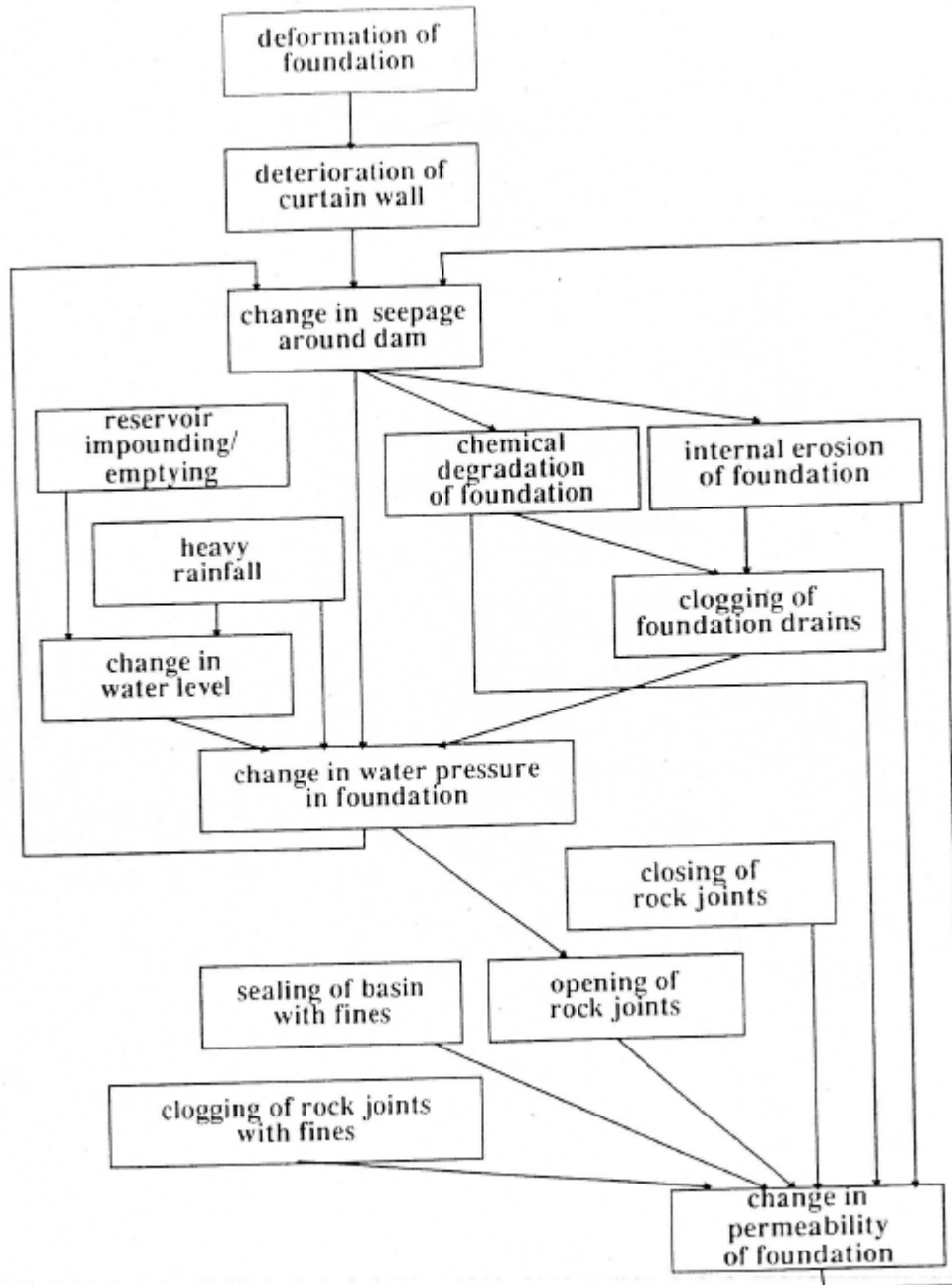


Figure 2. Section of causal network of dam processes

in the causal net, and the values of various attributes of the dam, based on evidence in the data. The set of processes linked in a causal chain are highlighted by the system and describe a scenario which demonstrates the evolution of the dam behaviour. The third reasoning agent acts on the dam world to extend the implications of the state identified by reasoning agent 2, over the model of the dam and its environment thus establishing the values of the attributes. Once a model has been built of the state of the dam system in terms of a set of active processes (behaviours) and a set of attributes, this state can be tested against normative models to make judgements about the safety of the dam.

6.14 Management of information

As stated in the introduction, the system assists in the management of safety by facilitating the integration of information about the dam. Drawings, maps and pictures of the dam form part of the information base (Figure 3). Databases of past measurements of the dam can be integrated with the reasoning and modelling system described above. In this sense the system functions as an integration tool for different types of information and knowledge about the dam system.

6.15 Applications

The system is aimed to be general in that it may be used (in different forms), offline to assist in investigations of safety or for training, and also on-line for the generation of warnings at the dam site through interpretation of automatic measurements. The system is a decision-support system and in that sense does not provide answers, but assists engineers in managing the problem. It is co-operative and interactive, drawing on the relative strengths of man and machine to manage information for safety of dams.

Conclusion

1. In recent years there has been an increase in the amount of resources devoted to the monitoring and assessment of dam safety.
2. Measures of safety such as probability of failure, factor of safety should be seen not as attributes of a structure but of the model within which they are calculated. The likelihood of failure of a dam is necessarily unknown. These measures are, however, important parameters to be used in the management of dam safety.
3. The importance of the management of dam safety as a process of applying quality procedures designed to test for hazards through design, construction, and operation and the subsequent decision making/action, is stressed.
4. The quality procedures require the collection and testing of information concerning the dam against normative or reference models. The application of these procedures is viewed as a method of hazard auditing where the precursors to failure which can accumulate through a project can be identified and dealt with.
5. Developments in the field of AI have produced techniques and modelling environments which can assist engineers in the management of dam safety. These methods and technologies provide new possibilities for representation and manipulation of information relevant to a dam project and of building models of observed behaviour and normative reference models.
6. A system DAMSAFE is under development at ISMES to explore these possibilities.

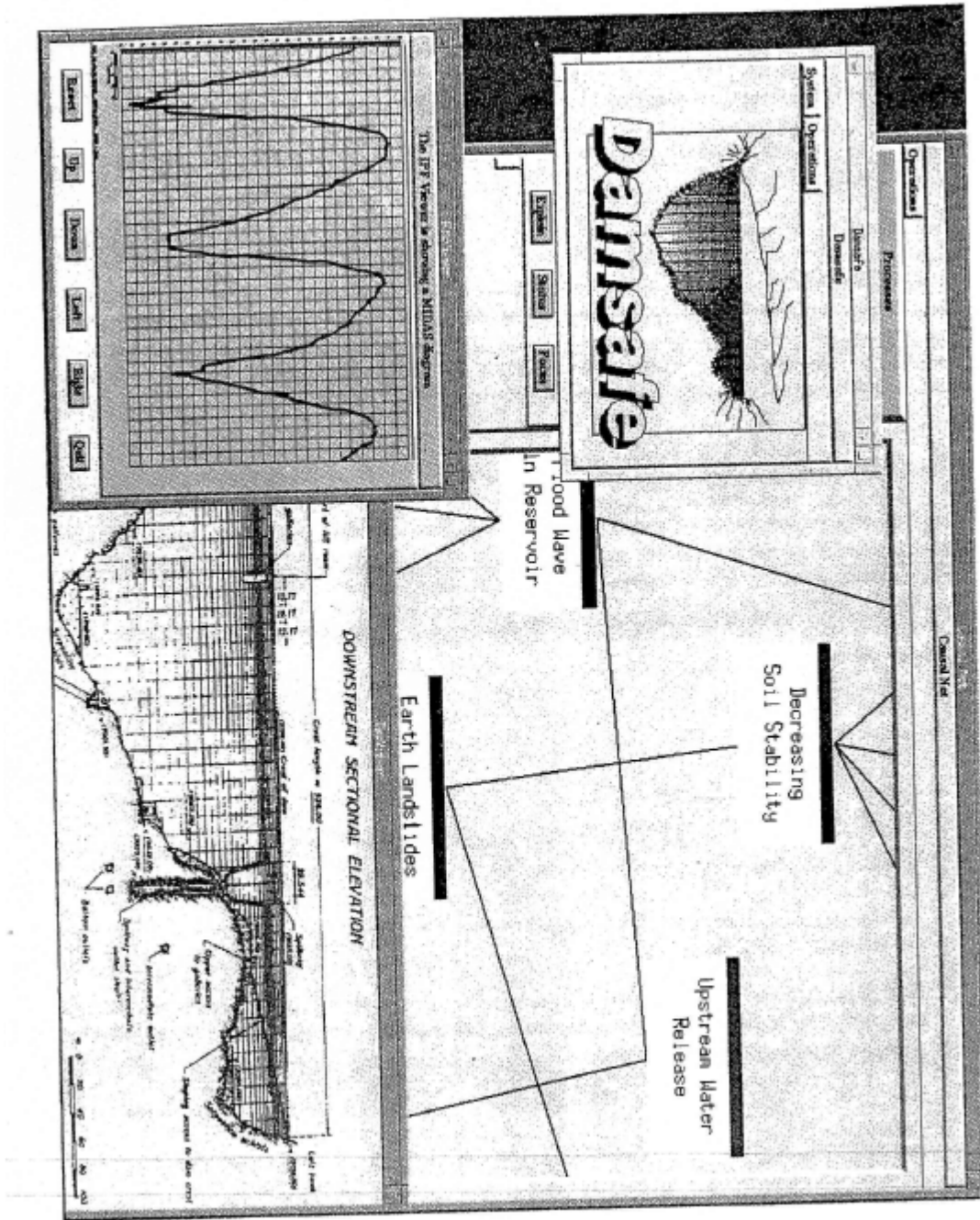


Figure 3. Information representation in DAMSAFE

Bibliography

- BONALDI, P., FANELLI, M., GIUSEPPETTI, G. AND RICCIONI, R., "Safety control of concrete dams: the role of automated procedures and management of surveillance", *Proceedings*, 16th ICOLD Congress, Rio de Janeiro, Brazil, May 1982.
- BONALDI, P., CARRADORI, G., FANELLI, M., GIUSEPPETTI, G. AND RUGGERI, G., "Modern techniques for dam safety surveillance and evaluation", *Proceedings*, 14th ICOLD Congress, San Francisco, CA, June 1988.
- BUREAU OF RECLAMATION, "Safety Evaluation of Existing Dams (SEED)", *Publication*, Washington, D.C.: Government Printing Office; 1983.
- CHEMICAL INDUSTRIES HEALTH AND SAFETY COUNCIL, "Hazard and Operability Studies", *Publication*, Chemical Industries Association, London; 1977.
- COMERFORD, J. B AND BLOCKLEY, D. I., "Managing Safety and Hazard through Dependability", *Journal of Structural Safety*, (In Press).
- COMERFORD, J. B AND STONE, J. R., "AI in risk control" in "Engineering Safety", *Book*, Blockley, D. I. (Ed.), McGraw Hill, London; 1992.
- COMERFORD, J.B., LAZZARI, M., PINA, D. AND SALVANESCHI, P., "An AI approach to the integration of engineering knowledge: water resources case studies", *Proceedings*, AIENG 92: 7th International Conference on Applications of Artificial Intelligence in Engineering, Univ. of Waterloo, Ontario, July 1992.
- COMMITTEE ON SAFETY OF EXISTING DAMS, "Safety of Existing Dams; Evaluation and Improvement", *Publication*, Washington, D.C.: National Academy; 1983.
- FANELLI, M., "The safety factor of dams - an abstract concept or a measurable quantity", *Dam Engineering*, Vol. II, Issue 2; 1991.
- FANELLI, M., "The Safety of Large Dams", in "Engineering Safety", *Book*, D.I. Blockley (Ed), McGraw Hill: London; 1992.
- FISCHHOFF, B., LICHTENSTEIN, S., SLOVIC, P., DERBY, S.L. AND KEENEY, R.L., "Acceptable risk", *Publication*, Cambridge: Cambridge U.P.; 1981.
- FORSE, T., "Qualimétrie des systèmes complexes: mesure de la qualité du logiciel", *Publication*, Les éditions d'organisation: Paris; 1989.
- KREUZER, H. AND BURY, K., "Safety assessment of concrete dams: safety factor versus reliability index", *Dam Engineering*, Vol. 2, Issue 2; 1991.
- LEWIS, D.J., "The Mond Fire, Explosion and Toxicity Index", *Loss Prevention*, Vol. 13, Am. Soc. Chem. Eng.; 1980.
- OOSTHUIZEN, C., VAN DER SPUIJ, D., BAKER, M.B. AND VAN DER SPUIJ, J., "Risk based dam safety analysis", *Dam Engineering*, Vol. 2, Issue 2; 1991.
- PERROW, C., "Normal accidents", *Book*, Basic Books: New York; 1984.
- PIDGEON, N. F., BLOCKLEY, D. I. AND TURNER, B. A., "Design Practice and Snow Loading: Lessons from a Roof Collapse", *The Structural Engineer*, Vol 64A, No 3, March, 1986.
- SALVANESCHI, P., "Controllo di Processi e Reti di Petri", *Note di Software*, No. 25/26, Università degli Studi di Milano, Dip. Science dell'Informazione Bull 8; Italia; 1984.
- SALVANESCHI, P., "The use of Integration tools in software maintenance", *Proceedings*, IEEE Conf on Software Maintenance, Sorrento, Italy; October 1991.
- TURNER, B. A., "Man Made Disasters", *Book*, Wykeham Press: London; 1978.