

7 The Interface with the Operator

Many accidents in safety-related operations are traced to 'operator error' or 'pilot error'. Inadequate design, however, may have placed the operator in a situation where an error was inevitable, or at least very likely. Conversely, the contribution which operators can, and habitually do, make to safe operation may be undervalued.



The design of a good operator interface is not a last-minute task concerned merely with the superficial layout of displays and controls; it reaches deep into the requirements and design process and is concerned with *what* should be automated and *how* it should be automated (if at all). It is inevitably concerned with social and psychological issues as well as technical ones. For this reason this chapter starts with some results from a project which was concerned with supporting team operations and then moves on to look at the analysis of human error and the modelling of the interaction between operator and system.

The first project, LIFETRACK, began with an assessment of the 'soft' risks in the management of safety-critical plant (Cf. RATIFI in Chapter 6) and derived some software support to reduce those risks. Its success may be judged from the fact that the software is now installed in a real petrochemical plant and in use every day.

The other two projects both developed other ways to identify risks associated with human failure. DATUM took a holistic view of an organisation and used techniques like HAZOP to focus on critical areas of the human-computer interaction. A key feature of this approach is identification of 'windows of opportunity' for human failure. SADLI, again using HAZOP but applied rather differently, assessed a given design of a computer-based system with complex operator interactions, so as to identify weaknesses and thereby improve the design. This approach has now been adopted commercially.

7.1 Supporting team operation

Many industrial processes are inherently risky. This risk is compounded by the practicalities of plant maintenance and the need for incremental improvements to the technology infrastructure. As a result the operational teams consisting of the plant operators, engineers and management have to cooperate closely to manage inherent risks and maintain safe operation.

Human error and the associated 'soft', people-oriented issues which influence behaviour are important factors affecting industrial accidents. An important soft factor is the information which underpins communication within the operator team and between the operators and other groups and individuals on the plant.

An example of a clear operational need is for effective communication between the shifts of operators who operate the plant. These people act as a "virtual team" occupying the same seats in the control room, but due to the shift structure, there may be little direct personal communication between individual shift members. However, effective communication during handover between shifts is crucial to carry out ongoing tasks and operating activities safely.

If human factors, including information and communication issues, are badly managed, the result can be considerable economic loss through downtime, injury or loss of life. The LIFETRACK project has explored how an organisation can go about planning and installing a team information support system with full awareness and management of these 'soft' factors.

Soft Organisational Factors

The focus of LIFETRACK has been on soft controllable factors within the operator team which influence the safe operation of a plant in the petrochemical environment. Of particular interest have been information, communications and teamwork issues, including:

- Better shift handover and team communication.
- Reinforced teamworking and a safety culture.
- Enhanced corporate memory of plant teams and “active” operational knowledge.
- Design of an information management framework using recognised standards.
- Communication of lessons learnt and/or best practices across shifts, assets, industry.

An objective, systematic review approach and benchmarking framework has been developed which incorporate the established KNOVA knowledge and team factors checklist [LIFETRACK refs 1 and 2], together with a detailed information usage questionnaire and assessment process [LIFETRACK refs 3 and 4].

KNOVA is essentially a management framework for reviewing the soft organisational factors which influence team performance, for example the quality of decision making. This framework provides a convenient way to identify areas of risk in the team environment. A knowledge-oriented view is taken of the operator team environment. Knowledge is viewed as being both formal and informal in nature, and comprises expertise, know how, information and data. A key principle is that ongoing investment to foster knowledge in the operator team reduces operational risk.

Alongside the knowledge and operator team focus is the need to explicitly include corporate, management and supervisor perspectives. The move towards lower hierarchy organisations and consolidated operational activities means that the different individuals and groups at the various organisational levels need to be consulted to ensure that longer term organisational directions are accommodated.

From an operational management point of view, explicit identification of project risks, success factors and performance measures, including estimates of cost savings, are necessary for monitoring and review purposes. This ensures that the benefits of focusing on soft organisational factors are obtained and recognised. These project measures need to be agreed with operational staff and put in place before steps are taken to improving the support environment of the operator team.

Identifying and agreeing such details is made easier if the operational processes, sub-processes and activities carried out by the operator team and other operational staff are identified and explicitly accommodated.

To set the context for the detailed review of the operator team, general concerns of operational management were identified. The main areas which were seen as capable of improvement included:

- corporate memory and “active” (rather than “passive”) operational knowledge;
- communications between shifts, teams and operational groups, and
- maintaining a positive attitude towards safety.

Particular interest was expressed in providing lessons from Loss Investigation Reports (LIRs) to the operators in a readily accessible and suitably structured electronic form.

Information storage and access using electronic approaches is seen as an important element. However the human element is dominant, with a clear need to manage “soft” people and team factors relating to knowledge, corporate memory, sharing lessons and communications. A common shared view by all operational staff of the operational context is needed, with an ability to recall past experiences or lessons, apply them to current situations and maintain an ongoing focus on safe practices.

Demonstration system

A detailed review of the operator team information needs at a state-of-the-art BP petrochemical plant was carried out with the help of sixteen operators to identify options for improving information practice and communications. Unstructured discussions along with a formal questionnaire were used.

The communications review revealed that operators communicated regularly with other team members and operators from other shifts during handover. There was occasional communication with operational staff who were

not shift members, for example laboratory staff. However there was effectively no communication with operators on other similar plants - either within the same petrochemical organisation, or in another organisation. Direct sharing of lessons and experiences at the operator team level is not a standard practice in the industry .

A large amount of information is to be found in a petrochemical operational environment. However, much of this is not directly relevant to the everyday activities of the operator team. A detailed questionnaire on information usage and importance from the operator's point of view was carried out, together with elicitation of suggestions on how important information could be better used through electronic and other approaches. These suggestions were collated and then ranked by the operators to provide a prioritised list of options for improving information use. Input from operational management was then used to select a limited number of options, and group them in a way which could be handled practically.

The functionality selected for the demonstration system included:

- On-screen logkeeping and recording of shift highlights.
- Electronic delivery and access to the Night Order Book.
- Electronic access to a future Loss Investigation Report Database
- Electronic access to operating instructions and supporting plant documentation.

The Night Order Book

A night order book (NOB) is produced daily by a technical supervisor or some other person of similar standing. Multiple paper copies are made and circulated to the night shift team. The purpose of the NOB is to allow day-staff to inform the night-shift team of important process facts and developments.

A NOB normally consists of several pages containing fixed sub-headings, which relate to different aspects of the production process (eg, Effluent, Feeds, Furnaces, etc.). Each sub-section contains a few paragraph-sized blocks of text.

There are several important reasons for replacing the existing paper-based NOB with an electronic equivalent. These reasons are continuous with the motivations behind LIFETRACK and include:

- Delivery delays: there may be some delay between the production of a paper-based NOB and its delivery to operators. Network delivery of an electronic NOB would be instantaneous and remove the printing and photocopying steps.
- Data loss and confusion: pages or entire copies of NOBs may be lost or crumpled. Large amounts of paper may also clutter the control room.
- Data access limitations: an operator typically has to go some distance to a library/archive and search through files of paper. Such tasks are error-prone and unnecessarily laborious. Electronic searches would be significantly faster and more accurate, and would release the operator to do more immediate work. In addition, access to past knowledge would improve operator decision making, thereby reducing process errors and the risk to safety.

The electronic NOB/Log system stores each entry in a database table indexed by date, author and topic; over time this table will grow to contain thousands of entries, representing useful team memory of past experience. The DBMS provides simple retrievals of every entry in the NOB/Log, history lists for a given aspect of the production process, and rapid free-text searches.

Design Criteria and Constraints

Discussions with the operators at the plant indicated the following preferences for ease of use and acceptance of an electronic NOB/Log:

- Low response times;
- Uncluttered, consistent interface style across all applications;
- Important information listed at-a-glance on all screens (date, title, etc.);
- Large buttons;
- Avoidance of pull-down menus and excessive typing;
- Use of keyboard, cursor and tab keys in preference to mouse activation;
- A few basic query types should support all operator requests;
- Information access should be achieved with a minimal number of actions;

- Authorised input only; and
- Data security.

In particular, the ability to access information rapidly in a stressful environment was given high priority. Additional design criteria included compatibility with existing BP site IT practices and legacy systems; compatibility with the Oracle DBMS; interoperability with non-Oracle DBMSs; object-oriented information management to support complex, heterogeneous data; and scalability, flexibility and supportability.

The Electronic NOB/Log

The NOB system user has access to the screens listed in Table 7.1:

Screen	Purpose
Main Menu Screen	The master screen allowing users to select required functions. Displayed at Start-up.
Display Screen	Displays NOB entries. Allows user to scroll through NOB.
Entry Input Screen	Similar to Display Screen but allows authorised users to create new NOB entries.
Free Search Screen	Prompts the user for a phrase that is used to search the entire NOB database. Entries containing: the phrase are displayed.
Password Dialogue Box	Displayed when asking for user Passwords.
Invalid Entry Form	Displayed if an invalid user or password is entered.
Store in Master Dialogue Box	Prompts the user for verification before irrevocably storing new NOB entries in the master database.

Table 7.1. Night Order Book screens

Typical queries to this ‘team memory’ include:

- a) “Show me the NOB for today”

A simple retrieval of every entry in the NOB database indexed by today’s date has the effect of displaying the NOB for today. The same may easily be done for any day in the past.

- b) “Show me a history for furnaces for the previous 16 days”

Alternatively, an operator may wish to obtain a history of, say, furnaces between now and 16 days previously. To do this, the system retrieves paragraphs indexed by the topic ‘furnace’ and the appropriate dates.

- c) “Show me any entries containing the phrase ‘C-1 trip’

The computer performs a rapid free-text search on the stored entries and display the paragraphs containing this or any other chosen phrase.

There are three main agents involved in using the NOB system.

- 1) The author (e.g. the plant Technical Supervisor) who creates the NOB daily.
- 2) The reader (e.g. the plant Operator) who refers to the information in the course of his work. Authors and others may also be readers.
- 3) The master database server where the master copies of all the NOBs are stored. It is important that a single central repository is used for this purpose. This repository provides a reference point for legal and audit purposes and a secure back-up facility. All client terminals used by the readers and author retrieve their NOB entries from this single source.

All the agents are connected via a network as shown in figure 7.1. The software present on the clients and server is also shown.

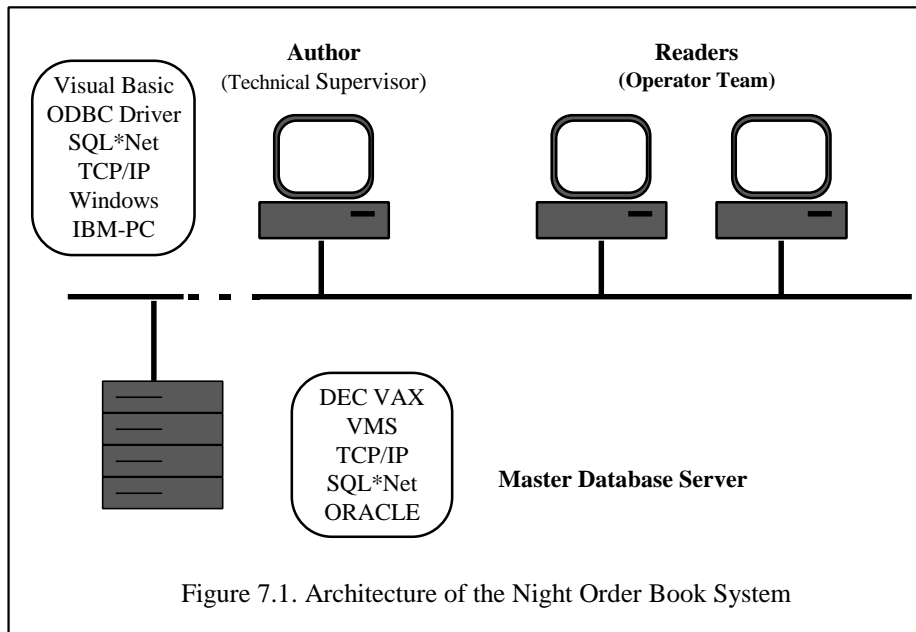


Figure 7.1. Architecture of the Night Order Book System

Although not a trivial system, the NOB/Log system is not very elaborate in IT terms. The focus of the LIFETRACK project has been on developing a system which will serve the needs of the operator team and which will consequently be used by the operators. Measurements have been taken of actual use on the working plant. In an eleven week period, 2,800 queries were made, indicating a satisfactory degree of acceptance.

Information Process and Architecture

Computer-based technology provides a means to support and sustain improved operational practice. Figure 7.2 illustrates the information infrastructure needed to support an operational team and provide an enhanced organisational memory. This architecture is necessary to aid integration of existing (legacy) data and provide uncomplicated retrieval of heterogeneous information contained in text, pictures, engineering drawings and database tables.

When delivering an information architecture and operator support system into an operational environment, a user-oriented approach is essential, with the operators involved in the design and development process, and training for using the system provided in advance of final deployment. The roles and responsibilities of the various operational individuals in supporting the new or modified information practices must be clearly communicated.

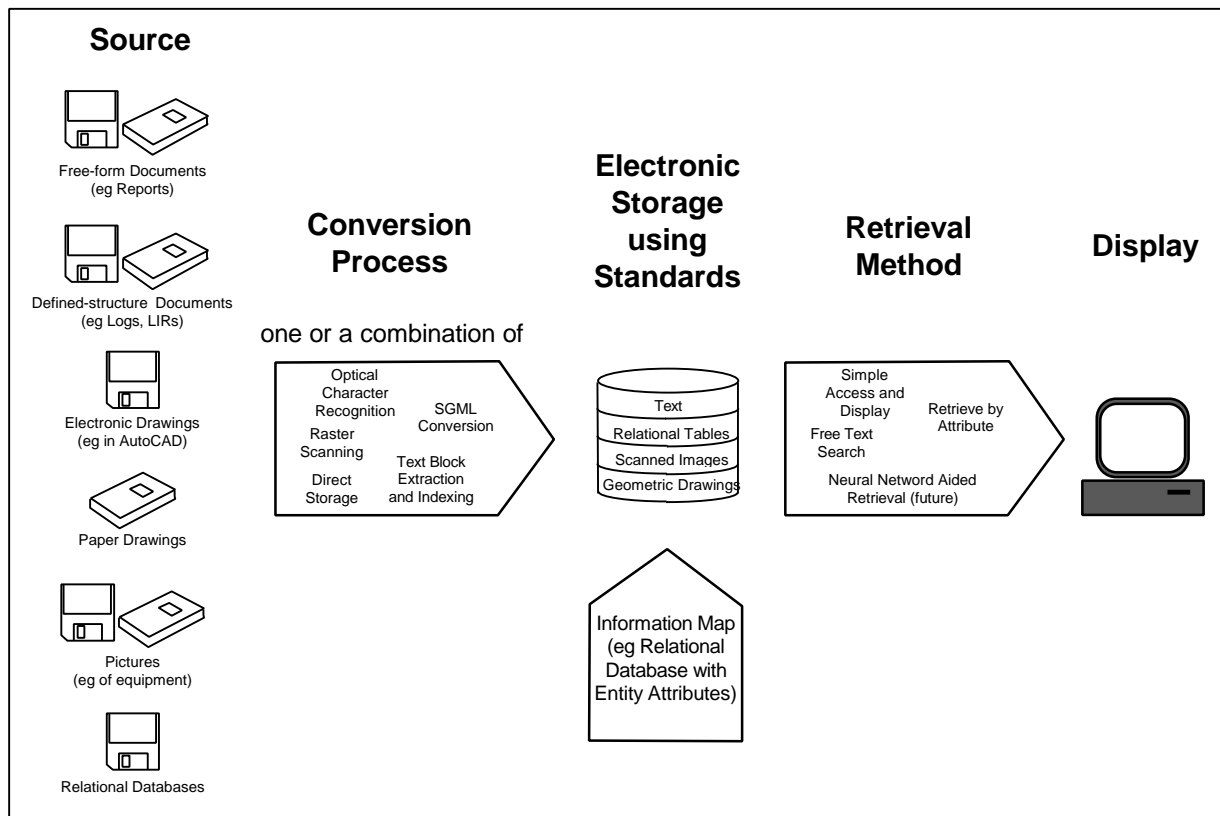


Figure 7.2 Information Infrastructure

Further information

The LIFETRACK project has completed a detailed information and communications review of a process plant operator team, and this experience has provided the basis of an integrated, systematic assessment approach to identify team information and communication risks, benchmark petrochemical operations, and develop an operator decision support system to reduce risk. Further information about this approach can be obtained from the references quoted above and listed on the project page in Appendix A.

7.2 Analysing Human Error

Systems are operated by human beings so sound system design requires an understanding of the strengths and weaknesses which humans display under operational conditions.

The DATUM project conducted a literature survey of human error and cognitive factors in human operation of dependable systems and from this synthesised a framework for analysing human error and associated risk in human-computer operation. This involved extending the work of Reason, Hollnagel and Rasmussen to create a taxonomy of human failure which might occur in skilled operation and in more general problem solving. The taxonomy was then applied to analyse accidents reported in the literature, so a multi-level model of causation could be deduced, e.g. the causation was attributed to failings in the social context, errors at the cognitive level in human decision making and in design of human computer interfaces and other machinery.

The taxonomy starts by drawing attention to social and organisational issues. First, management and safety culture is examined with questions about the level of safety training, monitoring of potential hazards, continuous safety awareness, etc. Then management of the controlled system is investigated to find factors contributing to potential failure; in particular, poor maintenance, lack of quality assurance in the original design and construction, poor operating procedures and lack of management attention to these problems. The second level focuses on human operators and asks questions about their training and the design of their work tasks. Complex tasks which make undue demands on people are one cause of error, while inadequate training can also lead to failure. The taxonomy provides categories of error at the skill and rule based level of normal operation and knowledge based level for

diagnosis of system failures and decision making for remedial action¹. The errors can be traced to design of operational procedures, the system (human-computer) interface, so potential risks can be assessed in terms of likely errors in skilled operation, possible mistakes by novice operators and support for failure diagnosis by operators. The final layer of the taxonomy provide generic design features which should be present in the human computer interface to support normal operation and failure recovery in safety-critical systems.

In a separate exercise a set of ‘cognitive pathologies’ were described based on research in the psychology of skill, reasoning and problem solving. The pathologies were structured using Rasmussen’s layers of reasoning (skill, rule-based, knowledge-based) and then associated with different steps in cognitive models for generic tasks such as assessment, analysis and design. This produced a model of possible human error in these generic tasks so the requirements for any computerised support system could be checked against them, furthermore the pathologies could be used to determine training requirements for human operators.

Further details of the framework and taxonomy can be found in [DATUM ref 13], [DATUM ref 14] and of the multi-level model of error causation in [DATUM ref 15].

A method for designing user interfaces

The taxonomy and results from the related work were combined with knowledge from the empirical studies of design practice (reported in Chapter 11) to create a method for designing user interfaces for dependable system. The method covers assessment of risk in human operation, and in the human computer interface, with guidelines for the design of the user interface. The designer is guided through analysis of the physical systems, the users’ tasks, requirements for information for safe operation and for warnings about abnormal states, and then progresses to design of the user interface to ensure safe operation and control of emergencies [DATUM ref 16].

The method builds on traditional approaches to safety-critical assessment e.g. HAZOP and event tree analysis. This motivation is grounded on the need to introduce new methods via practices which are already familiar to industrial practitioners. The method adds a set of techniques for diagnosing potential risk exposures which may result from task and environmental demands made on the human operator. The analysis is structured to separate concerns into different layers, as potential causes of failure and corresponding safety arguments are inevitably multifaceted, e.g.

- System operation - analysis of hardware and software failure in a designed system.
- Task and Environment - analysis of the operator’s task, cognitive workload, events and interruptions from the environment, to establish a baseline of demands being made on the human operator.
- Human Computer interface - analysis of usability and error protection afforded by the user interface design.
- Operator Training - assessment of operators’ abilities, their skills and task related training, in light of the task demands and workload.
- Management and Social environment - awareness of safety culture, incentives for safe operation, safety training, prevention of risk, and good maintenance practices.

The method is intended to function as a set of quality assurance procedures and design guidelines which fit within existing software design methods. The overall approach is to build upon and integrate three traditions: software engineering, human computer interaction and safety-critical assessment methods.

A perennial problem in risk assessment is to anticipate a priori all the possible ‘windows of opportunity’ which may exist for human error. While no silver bullet solution can be provided, the method does propose heuristics for scenario generation and challenging assumptions in a system design, e.g. failure of human responsibilities, effect of unexpected hardware/software failures, dealing with rare events, etc. Validation rules are provided to direct the assessor’s attention towards system features which may, (or may not, as the case may be) deal with the consequences of a violated assumption. Questions draw the assessor’s attention to possible failures at specific stages of interaction between the user and the system and at specific stages of system operation. Supplementary questions draw attention to possible risks according to the level of user knowledge and cognitive workload.

¹ Compare Rasmussen J., Information processing and human-machine interaction. Amsterdam: North Holland, 1986.

Many safety problems have no ideal solutions and involve trade-offs between desirable properties, e.g. usability of an interface may conflict with system security. Design rationale templates are proposed to help assessors discover conflicts between system requirements and to reason about appropriate trade-offs to deal with potential risks. The scope of the method is illustrated in figure 7.3. The term controlled system is used for the physical system which is subject to the controlling system. The latter is composed of human operators and interactive computer control processes in a social /environmental setting.

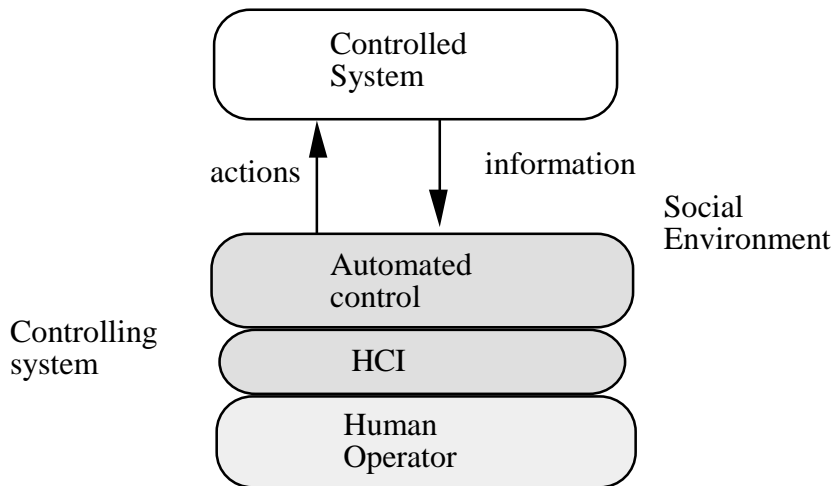


Figure 7.3. Scope of the method and relationships between the controlled (physical) systems and the controlling system.

Method Description

The method is structured as a ‘walkthrough’ for testing a system by asking pertinent questions about potential errors in different stages of design. The overview of the method stages is illustrated in figure 7.4. Many activities are familiar to HCI (human computer interaction) designers, e.g. task analysis, task allocation and task design. These involve modelling the system’s goals and activities from a human viewpoint and deciding which activities operators will be responsible for and which will be automated.

Window of Opportunity Analysis

A significant feature of the method is the concept of a window of opportunity analysis. This term is borrowed from Reason’s conception of system failure¹. He points out that many failures are multi-variate and their cause is often not the event which appeared to trigger the failure, but a set of circumstances that either permitted the event to happen or made a normally non-lethal event dangerous. This stage focuses on the system context to tease out possible causes of failure and their facilitating conditions. Window of opportunity analysis may be applied to a prototype design or a specification, so the technique acts as an evaluation/assessment procedure as well as providing design guidance. Although figure 7.3 shows this method sub-section occurring after task analysis and task allocation, it may be interleaved with those activities.

For further details of the method, see [DATUM ref 17].

The method has been tested on a small case study but is still seen as just a first step towards a fully effective, industrial strength, safety design method. Improvements are seen as necessary in some of the guidelines; industrial testing will be needed to assess the method’s utility and usability.

¹ Reason J. Human Error. Cambridge University Press, 1990.

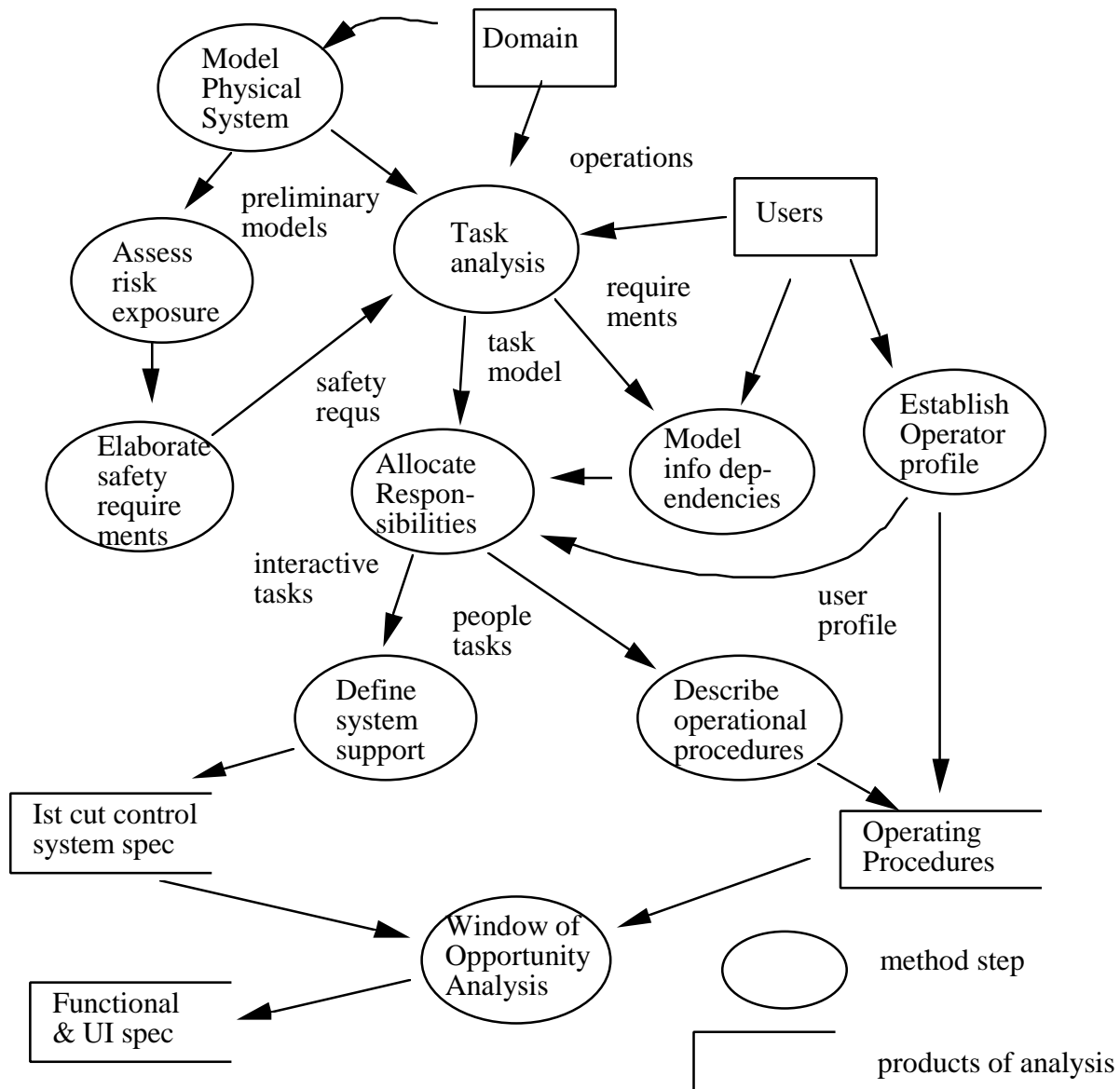


Figure 7.4. Overview of the method in data flow diagram format

7.3 Hazard Analysis of Human Interaction

The growth of structured design methods in software development has led to a variety of methods, with various conventions for producing an explicit representation of the system. Key amongst these approaches are various dataflow, process-flow and state-transition representations, such as CORE and Yourdon. These various descriptions provide a powerful means of representing the software design and are more or less suitable for differing categories of software system.

A continuing problem in the design of systems, however, is the way in which one understands and models the role and tasks of the human operator. In many cases the approach taken is to treat the operator as a completely separate entity. The system is designed with an external source/sink labelled 'HCI'. This is treated as a separate design entity under the responsibility of the HCI specialist. In complex process instructions there may well be a separate activity to analyse the operator tasks using some form of hierarchical task analysis. This analysis will be aimed at defining appropriate manning levels, training requirements, etc, but rarely addresses hazard issues in detail.

Problems arise because each of these analysis/design activities requires there to be a stable view from the other design perspectives. The underlying cause of the problem is that there is no common representation for the different

viewpoints, with the result that it is difficult to imagine the consequences of changes in one representation or another.

The approach to this problem taken by the SADLI project was to adopt a notation for representing the human processes and dataflows which is consistent with that used for the software. Such an approach was seen as valid as long as the human activity is primarily information-intensive where the human processes are:

- decision taking;
- information transfer; and
- classification and sorting.

On the other hand, this type of representation was seen as less effective when the human processes have significant components of motor skills or introspective reasoning. The vast majority of human work, however, falls into the former, information-intensive, class, especially where automation has been used to remove the manual labour aspects of jobs.

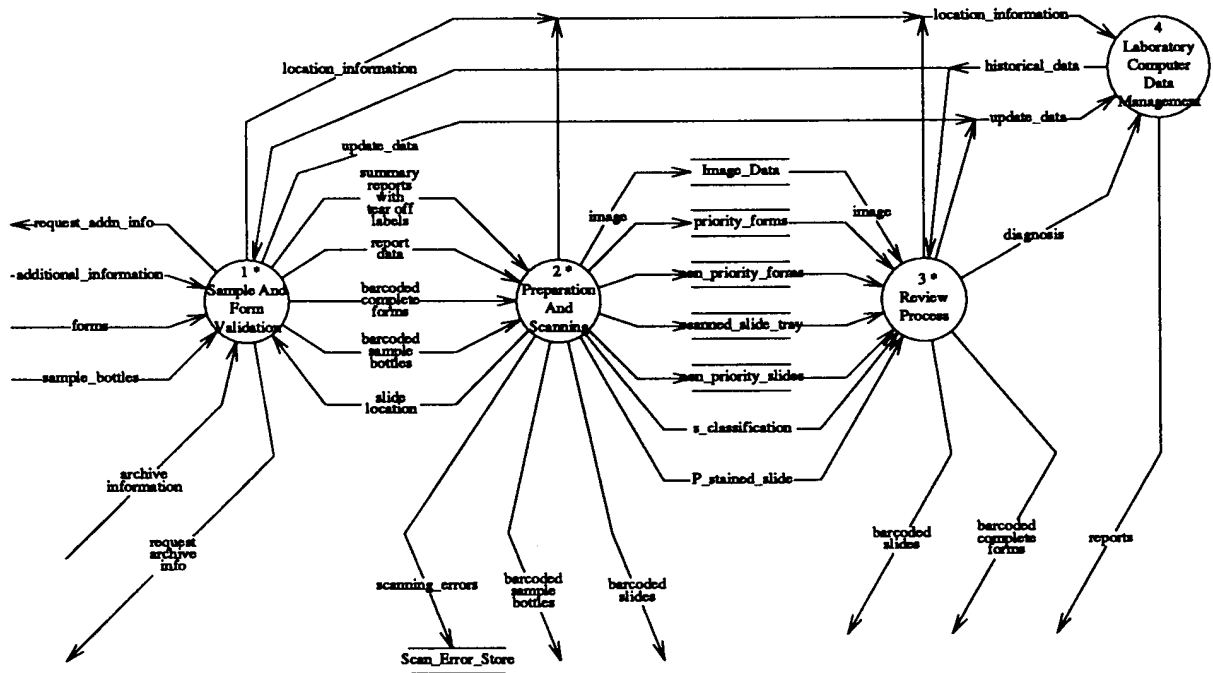
In adopting a model for the human components of a system based on dataflow and processes it becomes possible to generate an integrated representation of the overall system. Using this integrated representation one can explore the consequences of failure in a consistent manner across the whole system.

A case study

The procedure adopted, referred to as SUSI (Safety analysis of User System Interaction), was based on previous studies conducted by one of the partners (CCL). The case study analysed a conceptual design for a total laboratory for cervical screening, with the current laboratory practice modified to incorporate the semi-automated system. The dataflow design was produced by a team consisting of a human factors specialist, a cytopathologist, and a member of the design team of the experimental automated system. The team approach ensured that the various viewpoints on the design were captured in an effective manner and partitioned activities between human and machine in a way that was readily understandable to all those involved. This level of common understanding had not been achieved previously despite regular and detailed liaison.

Figure 7.5, representing part of the medical imaging system, illustrates the conventions used. The key components are:

- a circle represents a process (human or machine);
- a solid line is a dataflow;
- a dashed line is a control flow (stop, start, etc) (not used in this diagram); and
- two parallel lines represents a data store. Part of the convention is to show displays as data stores on the basis that this data may be written to a screen, but there has to be an explicit human process to read the data.



Data and Control flows within process 0: CERVICAL_SCREENING_SYSTEM

Figure 7.5. Example data and control flows

The Hazard Analysis Procedure

The basis of a HAZOP procedure is to review the system description and to ask a set of specific questions about each component of the system. For the representation of a system using dataflow diagrams, the project developed a vocabulary of discrete entities and associated deviations (ie guidewords prompting the analyst to consider what might go wrong), as shown in table 7.2¹.

Entity	Deviation	Comments
Process	Failure	Execution fails data used appropriately
	Error	Process algorithms wrong or contain flaw(s)
	Wrong process	Wrong process selected (including algorithms) also covers human short cuts
	Interrupted	Process not restarted appropriately (especially true for humans)
Dataflow	Corrupted	Data changed in transit
	None	Data does not exist
	Wrong source/sink	Data taken/sent from/to wrong place
Data Store	Corrupted	Data changed in store
	None	Data not stored not located
Control Flow	Corrupted	Wrong control signal

¹ Work has proceeded since the end of the project and has advanced somewhat beyond what is reported here. It is now being applied by Cambridge Consultants to systems in the fields of sea and road transportation.

	None	Process indicated with control signal
	Wrong source/sink	Sent to / received from wrong place

Table 7.2. Proposed HAZOP Guidewords

Conclusions

The approach adopted in the SUSI methodology is a natural extension of standard hazard analysis procedures. The principal development has been in the creation of an appropriate representation of user system interaction. In applying the methodology, the following observations were made.

- A major advantage of this process is that the dataflow representation gives an overview of the complete system. This means that if all processes, data stores and associated data and control flows are reviewed there is a check on the completeness of the safety analysis.
- The representation of the system as processes and data/control flows is understood by individuals with no software design training, such as operators and users.
- The review process can lead to detailed insights into potential flaws in the procedures and processes (in the example case it was realised that physically attaching labels to slides would be difficult as regulation requires the wearing of gloves).
- Designers with different viewpoints are able to use a common representation and believe that it increases their understanding of the total system.

The conclusion of the experience to date is that the SUSI methodology provides a useful extension to standard hazard analysis procedures. There are, however, some areas where further experience is required, these are:

- systems where there are significant sequencing factors ie where tasks or processes have complex orders in which they must be completed. It is possible that a state transition representation may be more appropriate.
- where systems have been designed without using a Yourdon design approach. Further studies will help establish efficient procedures by which the relevant representation may be produced. It should be noted that if the equivalent design documentation does not exist then this should raise concerns over the integrity and completeness of the actual design.
- in widening the user community. The SUSI methodology has demonstrated the advantage of incorporating user interactions in the system dataflow representation. Further applications in this area will contribute towards establishing a common method for system representation and communication.

For further detail of this work on human interaction, see [SADLI *ref* 2].