Annex 3:

Best Practice Guidance on Human / Computer & Human / Machine Interaction for Small and Medium Sized Enterprises

for

The PRISM Project

Prepared by Rob Cotterill
Human Factors Specialist
DNV Consulting
Highbank House
Exchange Street
Stockport UK
SK3 0ET
Tel: +44 161 477 3818
Fax: +44 161 477 3819
Email: rob.cotterill@dnv.com

Revision 1
May 2004

Table of Contents

1 Introduction

Human-Machine Interaction or *Human-Computer Interaction* can be defined as the applied study of how people interact with machines or computers. It is therefore a very broad field, as some level of human interaction is required to control all processes. This guidance concentrates on the key areas of Control room design, alarm handling, design for maintenance and computer interface design and testing.

Information, protocols, standards and guidelines are manifold in these areas and details of some of them are given in the section on "Useful References". Information is also available in the guidance produced from other PRISM focus groups, especially FG3: human factors in high demand situations and FG4: human factors in the design process. To avoid repetition and replication of information, this guide provides a higher level overview.

The following sections describe current good practice, which will help the small and medium sized business to address human machine and human computer interaction in many issues affecting the workplace. While it may be difficult for some companies to achieve best practice in all the areas mentioned, following at least some of the guidance and recommendations will aid in the achievement of good practice in human factors issues. The next chapters cover:

- Control room design and assessment
- Alarm handling
- Computer interface design
- Design for maintainability
- Useful references

The chapter on useful references is particularly important, as this guide can offer no more than an introduction to this very large field. It contains a list of sources of detailed information, which will be invaluable to anybody wishing to apply human factors to human-computer and human-machine systems.

The information should be usable by anyone with a normal understanding of plant operations or human factors. In any case, it is usually beneficial to have a combined team of operators, maintainers, managers and in complicated cases, a human factors expert.

2 Control Room Design and Assessment

2.1 Introduction

In recent years, the development of new control room solutions has resulted in increased performance demands on the control room operator. Typical trends include:

- Allocation of new functions and tasks to the control room (radio communication, transport, surveillance etc).
- Increasing amounts of information and more complex interfaces.
- New display and control technologies challenge traditional concepts of independence and separation of process control and emergency functions.
- The complexity of modified control rooms evolve beyond original design goals and requirements.
- Process output is increasing towards the limit of design specifications, leading to increased time pressure and operator demands.
- Reduction of number of operators due to cost saving.

These changes may seriously affect safety and working environment. However, a lack of an integrated human factors perspective is often the main reason why control room designs fail to provide sufficient overview and support to control room operators. Assessing the control room to ensure that human factors are taken into account is therefore necessary.

Control room assessments refer to a set of analyses performed to evaluate the design of a control room. The purpose of the approach is to review the design process to ensure that human factor principles and methods have been appropriately considered and integrated into the control room design in new projects, modifications and upgrades to installations. For further information, see the Useful References section and the guidance from PRISM FG3: human factors in high demand situations.

2.2 Control room assessments

A pro-forma for assessing control room installations has been developed, which can be used to prioritise remedial actions necessary to improve safety management in existing control centres. A series of elements are described, and criteria are given, which allow the control centre to be compared against best practice, typical industry norms, and against levels which are sub-standard.

The best practice criteria can also be used as a guide to aid design of new systems. Where it is not possible to achieve best practice, then as a minimum, a control room should aim to meet the industry average level. It should not be acceptable for aspects of a control room to be at the substandard level.

In this section the assessment criteria used are:

- BP represents best practice
- AV represents industry average
- RI represents requires improvement

Priority should be given to improvement where factors are sub-standard and score RI. Consideration can then be given to those factors where an AV score was given.

Element	Rating	Criteria
Display and Control Organisation		
Are displays and controls which are used together located next to each other	BP	Controls and displays used in this way are located next to each other. Controls and displays are arranged in functional groups that enable clear and easy identification.
	AV	Some effort has been made to ensure appropriate location of displays and controls but due to situational factors this layout is not optimal.
	RI	Associated displays and controls are separated by large distances. No easy way of relating a particular control to the relevant display.
Where displays and controls are used in a sequence are they laid out in this sequence?	BP	Controls and displays laid out in sequence according to cultural expectations.
	AV	Some effort has been made to ensure sequential layout of displays and controls but due to situational factors this layout is not optimal.
	RI	Poor sequential relationships which mean that the operator has to follow a complex pattern of activities in order to carry out the task.
Where displays are not sequentially used, are they laid out to convey the information most important for the operator's task?	BP	Most important displays and controls within operator's normal line of sight.
	AV	Some effort has been made to ensure the layout of the most important of displays and controls but due to situational factors this layout is not optimal.
	RI	Important displays and controls all over the place.
Is the display control relationship appropriate?	BP	Display control relationships match with cultural requirements.
	AV	N/A for this element
	RI	Display control relationships do not match cultural expectations. This can be a significant source of error.
Is the labelling of displays and controls consistent	BP	Position and clarity of labelling entirely consistent. E.g. all labels above the related control display.
	AV	Some variation in position but the relationship of the label to the associated control /display is very clear.
	RI	Labels appear above, below to the side off depending on the panel in question.
Is the position and flexibility of communications equipment adequate?	BP	Communications equipment can be used from the normal operating position.
	AV	Relevant information is easily seen from where the communications equipment is positioned.
	RI	Cannot see relevant information and equipment cannot be easily moved to a better position.
Posture and Movement		
Are the control stations adjustable?	BP	Control station fully adjustable

Element	Rating	Criteria
	AV	Adjustable chair and workstation at an appropriate height to accommodate different operators
	RI	No adjustments possible or desk height such that some operators have difficulty getting a comfortable position. (see also below)
If fixed are the dimensions appropriate?	BP	Dimensions have been determined using appropriate anthropometric data
	AV	Dimensions appear to be satisfactory for most operators
	RI	Operators have difficulty reaching controls, seeing displays or experience discomfort whilst performing their job.
If workstations are adjustable are operators trained in how to adjust them?	BP	Operators have been trained in how to make adjustments to the workstation and in attaining an appropriate posture.
	AV	Operators have adjusted the workstation to feel comfortable.
	RI	Operators are experiencing postural problems or feelings of discomfort have been reported.
Are key displays within the normal line of sight of the operator?	BP	Key displays and controls are within normal line of sight. Usually this is just below the horizontal from eye height.
	AV	Most are within normal line of sight. Those that are not have supplementary information such as audible alarms to indicate problems to the operator.
	RI	Apparently random arrangement of displays and control which require constant head movement in order to perform routine tasks.
Environment		
Is there glare on the VDU screens/panels	BP	Lighting within the control room has been designed to minimise glare
	AV	Potential for glare exists but some mitigation is provided e.g. blinds on windows etc.
	RI	Glare constantly experienced on VDU screens.
Is there adequate lighting to read display/labels?	BP	Displays and labels clearly visible.
	AV	Most displays and labels clearly visible but some variation in lighting levels occurs.
	RI	Insufficient lighting to read displays/labels.
Is the noise level acceptable?	BP	Noise levels are such that normal conversation can be heard. Audible alarms are clearly audible.
	AV	Generally noise levels are acceptable may rise at certain times or on the operation of printers etc.
	RI	Normal conversation cannot be heard. Audible alarms masked by background noise.
Is there sufficient space provided to do any necessary paperwork, store manuals and procedures etc.	BP	Requirements for this space have been considered as part of the overall control room design.
	AV	Space is available e.g. a desk but it is not necessarily in the optimum position.

Element	Rating	Criteria
	RI	Paperwork has to be carried out on the operator's lap or by resting on control panels/displays.
Information Requirements		
Can frequently used controls and displays be located quickly and easily?	BP	Hardwired are in normal line of sight. VDU systems include easy way to reach each screen or dedicated screens are available.
	AV	A low effort is required to access the relevant controls/displays.
	RI	The operator has to search for the relevant controls and displays.
Can important or frequently used displays and controls be assessed easily?	BP	All within easy reach of the operator from normal working position.
	AV	The majority are within reach of normal working position. Other are situated as close to this position as possible.
	RI	Operator has difficulty reaching or reading these displays and controls because of their location.
Is all relevant information supplied?	BP	Information provided based on thorough analysis of operators role.
	AV	Majority of information provided. Where it is not specifically provided it is easy to infer from other information.
	RI	Information provided has been determined on what can be measured and does not match the operator's task.
Is displayed information directly derived from the function it represents?	BP	E.g. Valve position derived from position of the valve stem.
	AV	Function is inferred and can be verified easily be reference to other information.
	RI	Indirect indications used such as; confirmation of control signal.
Is the operator's central display space restricted to information used by the operators?	BP	All information in this area is for operators use.
	AV	Some other information included but this does not interfere with the operators tasks.
	RI	Large amounts of information presented which are more relevant to other functions such as; management or maintenance.
Is information for maintenance/management presented elsewhere?	BP	Provision of dedicated facilities so information can be accessed without disturbing the operators.
	AV	Some disturbance to operators, or operators are required to produce a limited number of maintenance/management reports.
	RI	Constant interruptions to operators from maintenance and management requiring information.
Is it easy to communicate with related groups of workers?	BP	Communications facilities provided and reliable.
	AV	Communications provided but response may not be immediate.
	RI	Poor communications leading to operators having increased workload.

Element	Rating	Criteria
Are all sound signals easily distinguishable?	BP	The use of different sounds for alarms etc designed according to ergonomic guidance.
	AV	A small number of variations used or a single tone in those situations where the use of different tones is not essential.
	RI	Single tone or no tone used for a large number of different signals. Operator has to search to identify reason for the tone sounding.
Paged VDU Displays		
Are there sufficient VDUs such that all information required for decision making can be displayed at the same time?	BP	Number of screens determined by a structured analysis of operator requirements. The appropriate number of screens provided
	AV	Sufficient VDUs such that most decisions can be made in this way. Easy movement between screens for other situations.
	RI	Operator continually has to remember information from other parts of the system when making decisions.
Is there a process overview screen?	BP	Process overview provided such that operator can gain a quick and clear overview of the pertinent process conditions.
	AV	Part of the system covered by process overview.
	RI	No overview provided. Operator has to piece together a picture of the overall situation.
Is there a dedicated VDU screen for alarms?	BP	Dedicated VDU provided
	AV	Complexity of system does not warrant this. VDU screen easy to access e.g. within one keystroke.
	RI	Small area for alarm presentation that involves the need to constantly scroll through the alarm list.
Do alarms have to be acknowledged?	BP	Each alarm has to be acknowledged.
	AV	N/A for this element.
	RI	Alarms can scroll off the system and the operator is unaware that it has not been acknowledged.
Does the presentation of alarms help diagnosis?	BP	Alarm philosophy developed on best practice guidelines (see appendix II). Some level of prioritisation incorporated.
	AV	Alarms presented consistently within an area of suitable capacity to avoid the necessity for continual scrolling.
	RI	Alarms presented in such a number and with no prioritisation that necessitates the operator searching the list to identify the appropriate alarms.
Is a hard print out available?	BP	Hard print out available.
	AV	Sufficient capacity on the system to view all the current alarms.
	RI	No print out, alarms constantly scroll off system display.
Is there an indication that alarms	BP	Clear indication available.

Element	Rating	Criteria
have scrolled off the screen?	AV	N/A for this element
	RI	No indication that alarms have scrolled off the screen.
Are alarms prioritised?	BP	Alarms are prioritised and are presented according to prioritisation.
	AV	Different types of alarms are easily distinguishable
	RI	All alarms are presented in the same manner.
Are alarm set points set to avoid an unnecessarily high number of false alarms, but which still gives the operator sufficient time to intervene?	BP	Alarm set point determined according to these criteria.
	AV	Alarm set points determined through practice having previously erred on the false alarm side.
	RI	System generates a large number of false alarms or do not allow sufficient time for operator intervention.
Is the structure easily navigable?	BP	Flat wide structure, multiple means of accessing screens e.g. function keys, links from other screens etc
	AV	Operators may occasionally need to refer to aide memoir to help them negotiate the system.
	RI	Difficult to navigate system. Operators constantly need to refer to system plan to identify where they are.
Are appropriate input devices used?	BP	Operator given a selection of devices e.g. mouse or tracker ball, keyboard, numerical pad etc
	AV	Variety of devices limited but appropriate for the tasks required.
	RI	Input devices not appropriate for task. E.g. use of arrow keys on a keyboard to position a cursor.
Are error messages presented if inappropriate input?	BP	Error message indicates the range or type of input required.
	AV	System does not tolerate inappropriate input and gives an indication of input required.
	RI	System does not identify inappropriate input until completion.
Indications and Codes		
Are codes easy to distinguish?	BP	Codes and abbreviations are meaningful and do not necessitate the requirement for reference to explanatory notes. Rules for developing codes are consistently applied.
	AV	Operators occasionally need to refer to guidance until they are familiar with the system.
	RI	Codes not meaningful. Operators constantly have to look up references.
Is the information displayed suitable for the purpose?	BP	Operators do not have to make interpretations of the information in order to make decisions.
	AV	Some interpretation is required but this is very straightforward. E.g. no flow rate indicated but it can be seen that the tank level is increasing.

Element	Rating	Criteria
	RI	Operators have to interpret information of convert information to other units in order to make decisions.
Is the use of colour consistent and according to U.K. expectations?	BP	Use consistent and according to U.K. expectations e.g. Red danger etc.
	AV	Not applicable to this element.
	RI	Operator interface present a 'Xmas' tree effect of a mix of red and green which is not meaningful to the operators.
Actions and Effects		
Do displays clearly and directly indicate what the effect of an operator action has been?	BP	Operator gets immediate feedback on action
	AV	Operator gets confirmatory signal but has to wait for system response before appropriate action can be confirmed. E.G. operator gets indication that the pump is running but would have to wait a few moments before the tank level will change.
	RI	Operator is given little feedback on actions and by the time feedback is given has little time to intervene effectively.
Can an error be corrected?	BP	Operator has an easy route to correct errors
	AV	Errors can be mitigated prior to any consequence on the system but this may involve a number of operator actions.
	RI	Single operator error cannot be recovered and can lead to undesired consequences.
Instrument or Plant Failure		
Is it immediately apparent that an instrument/display has failed?	BP	Display changes colour to indicate this. Real time indicator stops.
	AV	Operator can easily deduce failure through the lack of change of other indications.
	RI	No indication given. System appears to function as normal.
For indications of high integrity, is there other information available for cross checking?	BP	Diverse and or redundant indications available?
	AV	Operator has to seek other information.
	RI	No possibility for cross checking available.
Are there instruments or displays that the operators consider unreliable	BP	No such problems exist
	AV	Availability of information to cross check if the operators are concerned about the item.
	RI	Operators have little confidence in the reliability of the information provided.

2.3 Control room design process

A methodology to aid in the designing process for control room is given in ISO 11064-1. It provides a framework, through which a structured approach is taken to control room design.

Designs for new control rooms and upgrades/modification to existing designs should follow all the phases described below, while audits of existing control rooms need include only Phases D and E. This guidance is in line with the approach described in ISO 11064, which readers are recommended to review (see "Useful References" section) and integrates regulations, standards and principles of a human centred control room design.

2.3.1 Phase A: Programme management, goals and requirement

This phase covers the organisational and management aspects of the process:

- Design programme management
- Composition of the design team and the management of human factors issues related to the design process.
- Clarification of goals and requirements
- Identification of relevant regulatory requirements and standards related to human factors.
- Operational experience review (OER).
- Setting of human factor goals and requirements for the projects.

The activities can be carried out by a variety of means, but can be achieved with the following approaches:

- Reviewing project documentation (including initial designs, safety / security requirements, operational / control requirements, company / industry standards and functional goals).
- Interviewing key personnel (including plant management, operations, plant engineering and maintenance) as well as personnel with experience from other similar control centres.
- Conducting technical reviews of interface methods and techniques (including ergonomic standards, codes and regulations and audits of control centres with significant similarities in design, environmental factors or other issues.
- Conducting ergonomic trade off studies, to ensure that risks are as low as reasonably practicable while the plant or site still remains viable.

2.3.2 Phase B: Analysis and definition

This phase includes detailed analyses to determine specific requirements.

Functional description

For new designs; a detailed analysis of the functions in the control room should be performed. For an upgrade, analysis of changes is appropriate. Tools for this include:

- Walk through / talk through operational modes
- Definition of operational safety and reliability requirements
- Top-down functional process diagrams
- Topologies of plant / site etc

Function allocation

The functions are allocated to either the control room or automated systems. It must be ensured that the allocating is not based on what is possible for the machines to do,

but rather the relative strengths and weaknesses of the human operator and the machine or system. A basic procedure for allocation of tasks is shown in the Best Practice guide on task design the steps of which are as follows:

- Allocation to meet mandatory or regulatory requirements
- Allocation according to performance characteristics
- Allocation according to cognitive and affective support criteria
- Allocation according to feasibility of automation
- Allocation according to feasibility of human performance
- Review of allocation

Define task requirements
The tasks are analysed to determine what is needed of information, equipment, knowledge skills etc. to carry them out. For suitable task analysis methodologies, refer to the PRISM FG3 guide and to Kirwan & Ainsworth (1992) in the Useful References section.

Job and work organisation
Individual tasks are designed and allocated to each operator to optimise safety and efficiency. Requirements for training, communication, information control and operating procedures are also defined. This can be achieved with Job assessment criteria checklists including the following:

- Workload
- Job sharing
- Information requirements
- Predictability of the controlled system
- Tools, space and facilities requirements
- Conditions where operations tasks are performed

See the best practice guide on task design, and the PRISM FG4 application guide.

Verification and validation of Phase B
The allocations and assignments made in Phase B are checked and approved.

2.3.3 Phase C: Conceptual design

Conceptual design framework for the control room
A conceptual design of the control room is performed, addressing issues like equipment selection, layout, traffic patterns, information flow and space allocation. Models can be built by using mock-ups, 3-D CAD or Virtual Reality models. See the PRISM FG3 guide on VR modelling.

Conceptual design approval
A check of the proposed design before starting detailed design is performed. Any changes are verified before proceeding. Methods include:

- Scenario talkthroughs and walkthroughs
- Interface simulations
- Computer animation studies
- Standards compliance audit

2.3.4 Phase D: Detailed design

Detailed design requirements
Detailed design specifications are reviewed for:

- Control Suite Arrangement
- Control Room Layout
- Workstations layout and controls
- Environmental design
- Operational and managerial requirements
- Training
- Procedures

Design methods can include the following:

- Suitability reviews of commercially available (COTS) equipment
- Rapid prototyping of control equipment and suites
- Development of styleguides

Verification of the detailed design
A verification of the design is performed to ensure that it conforms to human factors principles.

2.3.5 Phase E: Operational feedback

Feedback should be gained once the new system has been implemented. This is useful to designers regarding the successes and problem areas of the design, and offers necessary input to private future design projects. It is therefore a valuable input to phases A to C. Feedback can be obtained from comments from operators and maintainers or from structured methods like the usability and user assessments described in section 4.

2.4 Resource requirements

2.4.1 Data requirements

The following information sources should all be considered and as many as possible should be obtained and used in control room design.

- Regulatory requirements and standards (e.g. ISO 11064, NPD).
- Company standards and policies.
- Documents related to project planning and management.
- Technical information on existing systems and control room (including information on modifications that have been made).
- List of requirements for the control room.
- Operational and safety philosophy documents.
- Risk assessment documents.
- Process descriptions.
- Safety and licensing documentation.

- Control room design documentation.
- Plant design documentation.
- Operations and commissioning documentation.
- Design constraint documents (budgets, time requirements, safety etc).
- Results of any previous relevant analyses, e.g. task analyses, error analyses, walk-throughs, talk throughs, modelling, simulation, desktop reviews, personnel performance problems, reasons for shutdown and working environment surveys.
- Existing procedures/instructions or procedures/instructions development guidance.
- Accident records.
- Operators experience documentation (event reports, internal memoranda, surveys, interviews, exercises, logs etc).

2.4.2 Expertise requirements

The human factors expertise needed in the control room assessment will vary according to the scope of the project, but should include:

- Designers.
- Operators.
- Maintainers.
- Managers/supervisors.

In more complex control room design situations, human factors experts should be included in the design team or may be called in for specific topics related to different parts of the assessments. The team can thus change as the project proceeds.

2.5 Benefits and potential Problems

A control room assessment in the design phase will not only lead to cost saving to the facility operators, but it will also create opportunities for improvements to system safety and produce operational benefits such as better process and quality control. Designing the control room by taking human factors into consideration from the beginning prevents the need for modifications in the future. Control room assessments will also benefit the client because a good control room design contributes to accident prevention: in a critical situation, the operator's understanding of information feedback from the system is vital.

Thorough control room assessments can however, be very extensive. This may be a problem, as it could well involve taking a plant out of commission and the company may find the implications of this too expensive and time-consuming. This should be balanced against the benefits it would bring and could be controlled with a well drawn up improvement plan.

3 Alarm handling

3.1 Introduction

Alarm systems are essential in process control. A well planned alarm system helps ensure safe operation of a plant and also helps to control the process to ensure an efficient operation. However, an alarm system that is not well handled can lead at best to inefficient plant control, unnecessary shut downs and lost production. At worst, it can lead to catastrophic failure and potential loss of life.

Simple steps can be taken, which can bring immediate benefits to plant operation and safety. One of these is a review of system alarms, to reduce the number of unnecessary, conflicting or confusing alarms, which detract from significant information in a control room.

3.2 Issues in alarm handling

This section of the document presents a method for the identification of potential problems with alarm handling. The method is presented in the form of two protocols: the first protocol examines the general aspects of alarm management while the second protocol examines detailed aspects of the presentation of alarms on the system. This is followed by a pro-forma to aid the assessment of individual alarms.

The protocols and pro-formas should be completed with participation from operators, supervisors and (where appropriate) maintainers. Responses can be made after direct observation of alarms, or from interviews and discussions with control room operators.

3.2.1 Identifying a potential problem

The first section of the assessment protocol is on general alarm management. There are a series of questions, most of which are answerable with “yes”, “no” or “n/a”. Additional information can be made in the comments box for each question. The information gained can be compared with current best practice, which is given in section 3.3, and the areas of direct concern can be identified.

Questions	**Y/N**	**Comments**
How many alarms are there on the system?		
Do all alarms require operator action?		
How many standing alarms are there?		
How many alarms occur during a plant upset? (Look for a record of alarms following a plant upset)		
How many alarms occur during a normal shift?		
Are operators ever overwhelmed by floods of alarms?		
Are there any nuisance alarms?		
Is alarm prioritisation used in a helpful or meaningful way?		
Have operators been trained to deal with alarms?		

Questions	Y/N	Comments
Is on screen written help available?		
Have there been any critical incidents or near misses where operators missed alarms or made an incorrect response?		
Is there a written policy for the use and definition of alarms?		
Is there a company standard on alarms?		
How are new alarms added to the system and existing alarms modified?		
How many alarms did your last HAZOP produce and how were they justified?		
Was the impact on operator considered?		
Do the alarms help operators keep process within safe envelope? (Where is this defined?)		
Prevent unnecessary emergency shutdown?		
Is there a defined response for each alarm?		
Does the alarm allow sufficient time for action, including 'diagnosis time'		

The second section is on presentation of alarms. A series of elements are described, and criteria are given, which allow the alarm system to be compared against best practice, typical industry norms, and against levels which are sub-standard.

The best practice criteria can also be used as a guide to aid design of new systems. Where it is not possible to achieve best practice, then as a minimum, the alarm system should aim to meet the industry average level. It should not be acceptable for aspects of alarm systems to be at the substandard level.

In this section the assessment criteria used are:

- BP represents best practice
- AV represents industry average
- RI represents requires improvement

Priority should be given to improvement where factors scores RI. Consideration can then be given to those factors where an AV score was given.

Area/Question	BP	Guidance
Is there a dedicated VDU screen for alarms?	BP	Dedicated VDU provided
	AV	Complexity of system does not warrant this. VDU screen easy to access e.g. within one keystroke.
	RI	Small area for alarm presentation that involves the need to constantly scroll through the alarm list.
Do alarms have to be acknowledged?	BP	Each alarm has to be acknowledged.
	AV	N/A for this element.
	RI	Alarms can scroll off the system and the operator is unaware that it has not been acknowledged.
Does the presentation of alarms help diagnosis?	BP	Alarm philosophy developed on best practice guidelines. Some level of prioritisation incorporated.
	AV	Alarms presented consistently within an area of suitable capacity to avoid the necessity for continual scrolling.
	RI	Alarms presented in such a number and with no prioritisation that necessitates the operator searching the list to identify the

Area/Question	BP	Guidance
		appropriate alarms.
Is a hard print out available?	BP	Hard print out available.
	AV	Sufficient capacity on the system to view all the current alarms.
	RI	No print out, alarms constantly scroll off system display.
Is there an indication that alarms have scrolled off the screen?	BP	Clear indication available.
	AV	N/A for this element.
	RI	No indication that alarms have scrolled off the screen.
Are alarms prioritised?	BP	Alarms are prioritised and are presented according to prioritisation.
	AV	Different types of alarms are easily distinguishable
	RI	All alarms are presented in the same manner.
Are alarm set points set to avoid an unnecessarily high number of false alarms, but which still gives the operator sufficient time to intervene?	BP	Alarm set point determined according to these criteria.
	AV	Alarm set points determined through practice having previously erred on the false alarm side.
	RI	System generates a large number of false alarms or do not allow sufficient time for operator intervention.
Is the number of alarms monitored and subject to review?	BP	Monitoring takes place and changes are made in accordance with a formal procedure. Operators are included in this process.
	AV	
	RI	No monitoring, number of alarms often unmanageable.
Is alarm grouping used?	BP	Alarms are grouped in overview displays only, where they are of the same priority and require a similar operator response
	AV	Alarm grouping is not used
	RI	Alarms are grouped on different levels of display without an assessment of risks or commonality of cause and response
Are the operators flooded with the numbers and type of alarms that occur during an incident/event?	BP	Alarm management presents information to the operators that supports the detection and diagnosis of an event often by using a hierarchical approach.
	AV	
	RI	Operators often inundated with alarms and important alarms missed.
Are all alarms relevant to operator involvement or action?	BP	All alarms are relevant to operators.
	AV	
	RI	Alarms are presented that are used for management/maintenance record keeping.
Are there any nuisance alarms?	BP	
	AV	Large percentage of spurious alarms occur during maintenance activities.
	RI	Certain alarms are routinely acknowledged and cancelled due to frequency, unimportance and false alarm.
Is there an appropriate system to help operators understand and act on alarms?	BP	Online facility or expert system to guide operator.
	AV	Immediate supervisory/ peer/ procedure support readily available.
	RI	Operators guess.
Are the alarms used familiar to the operator and consistent with those used outside the control room?	BP	High level of consistency.
	AV	
	RI	Operators often confused.
Is there a standard or guidance for alarm system design?	BP	Yes, a formal procedure is used in the design and modification of alarms systems.
	AV	
	RI	Alarm systems design differs within the asset and/or across assets.

Area/Question	BP	Guidance
Is a formal procedure applied for managing changes in the alarm systems and alarm set points?	BP	Changes are managed, risk assessed and made in accordance with a formal procedure. Operators are included in this process.
	AV	
	RI	No formal process exists for management of changes to the alarm system.
How often are alarms tested?	BP	A regular schedule of tests are in place and up to date. Actions are taken on the results of these tests.
	AV	
	RI	Nor formal system is in place, testing takes place only as a result of an incident or work conducted on the alarm systems.

3.2.2 Review of existing alarms

This section of the document describes a review process of existing alarms on the system. A sample of alarms should be taken, representing low, high and emergency level alarms. Where possible, all parts of the process should be represented in the sample as well. Ideally, this process should be rolled out across all alarms, especially if the analysed sample shows a large amount of alarms requiring modification.

The following pro forma demonstrates how individual alarms may be assessed. The results can then be compared against current best practice (as given in section 3.3) and decisions made as to whether each alarm needs to be modified, or should even be removed entirely.

Alarm Ref:	
Description:	
Consequence of no / wrong action	

Issue:	**Y/N**	**Comments**
Is a response required?		
Is the response defined?		
Is the alarm easily understood?		
Is this a nuisance alarm?		
Does the alarm relate to a piece of equipment that is currently out of service?		
Can the set points be adjusted to provide fewer false alarms?		
Following adjustment is there sufficient time for the operator to act?		

Actions Required				
Alarm removed		Priority:		
Alarm suppressed		Current		Suggested
Actions defined			Emergency	
Alarm set points adjusted			High	
Alarm re-engineered			Low	

3.3 Best practice in alarm management

3.3.1 Alarm handling

Better alarm handling can have a significant effect on process safety. The EEMUA guidance (see Useful References section) makes the following recommendations for best practice:

- Alarm system handling can be improved by ensuring that the average alarm target rate in steady operation should be:
  - no more than one alarm every ten minutes
  - no more than ten in the first ten minutes following a major plant upset

- Effective Prioritisation of alarms should use about three priorities based on consequences if the operator fails to respond:
  - 5% high priority
  - 15% medium
  - 80% low

- There should be less than an average of ten Standing alarms at any one time.

3.3.2 Alarm Rationalisation

There are a number of relatively easy technical solutions that can be implemented quickly and that can give substantial improvements to the performance of the system. For example:

- Eliminate and review alarms with no defined response or which are not understood
- Tune alarm settings on nuisance alarms (consider replacing digital with analogue)or re-engineering repeating alarms
- Adjust dead bands on repeating alarm
- Suppress alarms from out of service plant

The pro-forma in section 3.2.2 should help identify where alarms may need attention.

3.3.3 Developing A Company Standard

Where possible, a company standard should be developed which gives guidance on the development and management of alarm systems. This standard should describe:

- The philosophy on the use of alarms
- Incorporation into the procurement of new systems
- Details of the ergonomic issues associated with the presentation of alarms
- Details of desired standards in terms of the performance of the system with respect to:
  - alarm target rates
  - effective prioritisation
  - standing alarms
- Details of operations involvement in alarm development
- Definition of an appropriate management of change process

- Details of requirements for the ongoing review and assessment of the system
- Standards for operator training and associated help facilities

3.3.4 Implementing A Company Standard

In order to implement the requirements of a company standard on alarm management the following points should be noted:

- Responsibility for the performance of the alarm management system and compliance to the company standard should be allocated to a job/individual
- All roles affected by the management system should be fully trained and aware of the roles, responsibilities and procedures involved
- Appropriate records should be kept relating to:
  - changes made to the system
  - measurements of performance parameters
  - formal Reviews of performance.

4 Computer Interface design

The following sections discuss the issues surrounding interface design and go through the steps of designing or commissioning a system. These apply equally to a control room as to a stand alone desk top application.

4.1 Bespoke or off the shelf?

Software, whether for control systems, management, training or any other purpose can be bought in a ready to use, mass produced format (known as “off the shelf”) or as an individually designed and built product (“bespoke” products). There are stages of development in between, but the rules for choosing a system are common to both.

Bespoke software is designed to meet the exact requirements for a system. The main advantage of this is that the functionality will be precisely what is necessary for the purpose (both in process control or in other uses) and computer resources are not wasted providing unnecessary capabilities. Additionally, the software will fit in with the work practices of the organisation. One disadvantage of bespoke systems is cost: development of software can take time and is therefore expensive. It is also necessary to be very specific in defining the requirements of the system: misinterpreted requirements can be very costly to fix at a later date.

Off the shelf software is much cheaper, because the cost of development is spread over many more products. Testing of the product will also have been thoroughly performed by the producer, so it is less likely that there will be any problems, once installed. The disadvantage of off the shelf software is that its design criteria will not necessarily match the requirements for a company’s systems: it may not fully integrate with other systems and it may not have exactly the right set of capabilities required.

The time & effort needed to carry-out thorough testing of software systems can be very large. Where a high degree of reliability is required this is more likely to be achieved through the use of systems where the cost of testing has been shared across a number of applications.

The following section describes the stages that should be followed in procuring a new software system, by either method. The initial stages are common to both approaches, and where they differ, this is indicated.

4.2 Stages

The following stages should be followed if a system is to be procured from scratch, i.e. a need has been identified but not formally defined. If requirements, designs, or concepts have been produced, they should be reviewed to ensure that they are systematic and based on a systematic process. The usability heuristics shown in section 4.3 can be used to guide usability assessment at each stage of development, but also see the PRISM FG4 guidance and the Useful References section.

4.2.1 User requirements definition (URD)

This can be described as “finding out what you want the system to do”. The URD can be based on a structured task analysis or on inputs from operators, process engineers, chemical engineers, and all other stakeholders in the system. Ideally, it should contain information from both sources. It should also contain a target audience description (TAD), which describes the end users of the system. The TAD might contain information on the age range, educational and skills level, expertise and roles of the user population. There may be several user levels (e.g. operator, supervisor, maintainer, super-user) with different characteristics. For each user level, information collected could include:

- Role definition;
- Cognitive capability;
- Skills profile;
- Experience and training.

The URD should contain information in the following areas:

- What information is required by the operator;
- What actions the operator should be able to perform;
- Of what functions the system should be capable;
- Style guides and colour schemes that must be followed.

This should be a “living” document, in that it should evolve throughout the procurement process, becoming more detailed as the designs are developed.

If the requirements of the system match the capabilities of commercial off the shelf software, then it is a good idea to consider this as an alternative to having bespoke software developed. However, off the shelf software should also undergo evaluations to ensure it is suitable for its purpose.

4.2.2 Design process

User centred design follows some simple rules that, if followed, should ensure that an interface performs as expected and can be easily operated correctly:

- Understand the operational environment, working conditions &, constraints
- Know what is technically possible
- Identify potential causes & consequences of error or hazards, and eliminate them
- Map the design to the users needs by matching tasks to functionality
- Identify and adhere to applicable standards
- Design iteratively, evaluate early and seek end user involvement
- Maintain a common look & feel with other systems as appropriate
- Ensure the consistent implementation of functions and features
- Avoid unnecessary complexity

The following sections describe the stages of interface design, and how a consideration of the above points can improve system usability. Various usability assessment methods should be used at each stage, to ensure that the end user is considered throughout the design process.

4.2.3 Design specification

A design specification will be based on the requirements for control of the system. However, a good design specification will also consider the URD and how the system will be operated by the end-user.

4.2.4 Concept design

Following from the design specification, the concept design should produce a definition of how the operator will control the system through the interface. In other words, while the design specification describes *what* the system will need to do, the concept design describes *how* it will do this. As well as considering the design specification, it should consider any existing standards, style guides and "common look and feel" requirements.

Reviews by representative end users and system experts can help guide and refine the concept design, to ensure that the designers' understanding of the system reflects the expectations of potential operators.

4.2.5 Paper / rapid prototyping

Rapid prototyping is a cheap way of demonstrating the look and feel of an interface, without the cost of producing a fully developed system. The level of functionality and detail can be varied to match the level of confidence in the design, or the requirements for demonstration purposes. It is often best to start with paper prototypes: drawings or images of how the interface will look. A series of images can be produced, to mimic the response of a display to changes and user actions, which helps to demonstrate functionality at low cost. Computer models can also be made, which might mimic responses to user interaction or process events. These require some commitment of time and resources, but the result can be more representative.

Depending on the level of sophistication of the rapid prototype, it will be possible to perform scenario or cognitive walkthroughs. In a scenario walkthrough, a prepared set of images can be shown in sequence, to demonstrate how the interface would respond to one or more pre-defined scenarios. A cognitive walkthrough is a more sophisticated version, where a user can interact with the prototype to test how it might respond to various actions. Feedback from either method should be used to refine (or if necessary redesign) the operation of an interface.

4.2.6 Initial design

Once any early issues have been solved, the main design and build can proceed with more confidence. Full scale working systems can be developed, which allow for complete user interaction. Once these are ready, further usability testing should be considered. Testing should consider a threefold approach:

- Usability criteria
- User testing
- Consistency testing

Testing against usability criteria uses a set of usability heuristics which are generally recognised as being good practice in system design (see the section on usability heuristics). This can be performed by anyone with an understanding of user interaction and usability issues. User testing involves one or more end users or operators trying the interface in a set of real situations. Comments about positioning of functions, clarity of displays, ease of operation and ability to respond to situational changes should be noted and considered. Consistency testing is appropriate when a system designed is part of a larger system or needs to be compatible with existing equipment. Designers or operators with usability experience from the other systems should inspect the interface to ensure that it operates in the same way as those other systems. Inconsistencies should be identified, and along with feedback from the user and usability inspections be used to make refinements to the design of the interface.

4.2.7 Detailed design

Once a system has been fully designed and tested by users and usability experts, adjustments can be made as necessary, the system can be retested and the solution implemented.

System design for usability is an iterative process. That is, it is not intended that the stages listed above are performed in a set order to make the system complete. Rather, usability testing and inspection is performed, the design is refined, and testing is repeated as necessary, until all usability issues have been resolved. Once a solution has been implemented, note should be taken of any usability issues that arise: these can be taken forward to future versions of the interface, or updated into the new system at some future point.

4.3 Usability heuristics

Usability heuristics are established usability principles that need to be recognised when designing a system interface. The following list (developed by Jakob Nielsen, see the “useful references” section) can be used to guide interface design, or as tool for evaluation and testing.

- **Visibility of system status**

The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.

- **Match between system and the real world**

The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.

- **User control and freedom**

Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support undo and redo.

- **Consistency and standards**

Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.

- **Error prevention**

Even better than good error messages is a careful design which prevents a problem from occurring in the first place.

- **Recognition rather than recall**

Make objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.

- **Flexibility and efficiency of use**

Accelerators -- unseen by the novice user -- may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.

- **Aesthetic and minimalist design**

Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.

- **Help users recognize, diagnose, and recover from errors**

Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.

- **Help and documentation**

Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, list concrete steps to be carried out, and not be too large.

5 Design for maintainability

5.1 Introduction

Maintainability is the ability to carry out rapid and reliable activities on a system, in order to maintain the desired level of performance. Such activity might be proactive, or reactive: the former being performed to prevent failure, and the latter being responsive to a failure or degradation in performance.

A system should be designed with maintainability in mind, so that maintenance activities may be carried out in an efficient and usable manner. As such, the rules for usability, usability testing and prototyping described in the previous section apply equally to maintenance activities: the maintainer is as much a user as the operator.

5.2 Issues in maintenance

This subject is covered in great depth in the UK DEF STAN 00-25 part 11 (see "Useful references") and applies equally well to the process sector. Some key points are described here.

5.2.1 Layout of units

A maintainer will require sufficient space to work safely, in and around the equipment. Design of apparatus (e.g. control room consoles, process machinery) should consider the needs of maintainers in considering not just the layout, but also the position, in relation to the control room, process area etc. Equally, there should be adequate lighting for the maintainer to clearly see the task area and where possible, components should be easily accessible or removable.

Consideration also needs to be given to space needed to fit and use tools and similar equipment in and around apparatus. This should include the ability to see and control what is being performed. Where possible, the use of standard tools should be designed for.

5.2.2 Maintenance operations

Where equipment is housed in casing that needs to be removed for maintenance in-situ, the case should lift off the unit, not the other way around. However, it might be preferable for a unit to be entirely removed for maintenance, in which case the removal and replacement should be easily achieved, with little scope for damage to the equipment or its housing.

Any important information on equipment (including identification, safety and removal instruction labels) should be clearly visible when in position. That is, important labels should not be obscured by other equipment or by unit housing.

It may be appropriate to fit handles to some larger pieces of equipment in order to assist their removal. This should be considered where units are over 10kg, but units

over 60kg should only be removed with the aid of mechanical lifting equipment, and provision should be made for access of such equipment to the unit.

5.3 Benefits and potential Problems

As with control room and software design, time invested at the design stage will provide greater benefit later. All equipment requires maintenance to varying degrees during its lifetime and a system well planned for maintenance will mean that maintenance activities can be carried out with greater speed, accuracy and efficiency, reducing failure rates and limiting down time.

Designing for maintainability may require that extra space and resource is allocated to maintenance tasks – which account for a relatively small proportion of utilisation time - and therefore may seem inefficient. However, time saved in maintenance activities is a saving on non-productive time.

6 Useful References

6.1 Control room design

NUREG 700 (1996) *Human-system interface design review guidelines*

Institute for Energy Technology (2000) *A Method for Reviewing Human Factors in Control Centre Design. Developed for the Norwegian Petroleum Department*. (See http://www.npd.no/norsk/safety/mmi-metodikk.PDF).

International Atomic Energy Agency (1993) *Control Room Systems Design for Nuclear Power Plants*. Vienna: IAEA-TECDOC-812.

International Electrotechnical Commission (1998) *Design for Control Rooms of Nuclear Power Plants*. Geneva: IEC 964.

International Instrument Users' Associations (1998) Ergonomics in Process Control Rooms. Part 2: Design Guideline. The Hague: International Instrument Users' Association WIB (M 2656 X 98).

Kirwan, B. & Ainsworth, L. K. (1992). *A Guide to Task Analysis*. Taylor & Francis, London.

ISO 11064:2000 *Ergonomic design of control centres*-
Part 1: Principles for the design of control centres.
Part 2: Principles for the arrangement of control suites.
Part 3: Control room layout.

DEF STAN 00-25 human *factors for designers of equipment*:
http://www.dstan.mod.uk/
(1997) Part 2: Body size.
(1991) Part 4: Workplace design.
(1997) Part 6: Vision and lighting.
(1986) Part 7: Visual displays.
(1989) Part 8: Auditory information.
(1991) Part 9: Voice communication.
(1992) Part 10: Controls.
(1989) Part 12: Systems.
(1996) Part 13: Human computer interaction.

6.2 Alarm handling

Engineering, Equipment and Materials Users Association, 1999. *'Alarm systems, a guide to design, management and procurement,'* No 191. ISBN 0 8593 1076 0.

HSE, 2000. *'Better alarm handling'*, Chemicals Sheet No 6, dated 3/00.

6.3 Interface design / heuristics

ISO 9241 Ergonomic *requirements for office work with visual display terminals* (VDTs)

ISO 9241-1:1997 Part 1: General introduction
ISO 9241-2:1992 Part 2: Guidance on task requirements
ISO 9241-3:1992 Part 3: Visual display requirements
ISO 9241-4:1998 Part 4: Keyboard requirements
ISO 9241-5:1998 Part 5: Workstation layout and postural requirements
ISO 9241-6:1999 Part 6: Guidance on the work environment
ISO 9241-7:1998 Part 7: Requirements for display with reflections
ISO 9241-8:1997 Part 8: Requirements for displayed colours
ISO 9241-9:2000 Part 9: Requirements for non-keyboard input devices
ISO 9241-10:1996 Part 10: Dialogue principles
ISO 9241-11:1998 Part 11: Guidance on usability
ISO 9241-12:1998 Part 12: Presentation of information
ISO 9241-13:1998 Part 13: User guidance
ISO 9241-14:1997 Part 14: Menu dialogues
ISO 9241-15:1997 Part 15: Command dialogues
ISO 9241-16:1999 Part 16: Direct manipulation dialogues
ISO 9241-17:1998 Part 17: Form filling dialogues

DEF STAN 00-25 *human factors for designers of equipment*:
http://www.dstan.mod.uk/

(1986) Part 7: Visual displays.
(1989) Part 8: Auditory information.
(1992) Part 10: Controls.
(1989) Part 12: Systems.
(1996) Part 13: Human computer interaction.

Nielsen, J. (1994). *Heuristic evaluation*. In Nielsen, J., and Mack, R.L. (Eds.), Usability Inspection Methods, John Wiley & Sons, New York, NY

Nielsen, J. (1994). *Usability Engineering*, Morgan Kaufmann, San Francisco.

6.4 Design for maintainability

DEF STAN 00-25 "*human factors for designers of equipment*"
http://www.dstan.mod.uk/

(1997) Part 3: Body strength and stamina.
(1992) Part 10: Controls
(1988) Part 11: Design for maintainability

HSE/HFRG (2000) *Improving Maintenance - A Guide to reducing error*, HSE Books, UK.

Reason, J. & Hobbs, A. (2003) *Managing Maintenance Error*, Ashgate Publishing, Aldershot, UK