

Safety Report Assessment Guide: Human Factors

Technical Criterion	Human Factors Topic	Evidence for Full Demonstration
Link with Predictive Criteria		
<p>12.1 The safety report should show a clear link between the measures taken and the major accident hazards described.</p>		<p>There is a clear, logical link between representative major accident hazards (MAHs) in the safety report and the measures designed to optimise human performance and minimise the potential for human failure:</p> <ul style="list-style-type: none"> ! safety-critical tasks relevant to each major accident hazard scenario have been identified; ! systematic human error analysis is carried out on each safety-critical task, based upon a thorough, real-world understanding of the task in question; ! potential human failures for each safety-critical task are actively managed in line with the hierarchy of control; measures match the types of potential human failure identified; ! performance influencing factors are identified and addressed ! error recovery is actively managed. <p>For further evidence of demonstration, see the following criteria:</p> <ul style="list-style-type: none"> ! 12.2.1.2 ! 12.2.1.6 ! 12.2.1.12 ! 12.2.3.1 ! 12.2.4.2
General Principles		
<p>12.2 The safety report should demonstrate how the measures taken will prevent foreseeable failures which could lead to major accidents.</p>	<p>This Criterion Completed Last</p>	<p>This is a high-level demonstration informed by the quality and depth of demonstrations made for the full range of human factors technical criteria.</p> <p>The report demonstrates a structured, systematic approach to managing human performance in the context of major accident hazards. Control measures, and the supporting Major Accident Prevention Policy and safety management system, are built upon a real understanding of how human failure plays a part in initiating, escalating, and failing to mitigate the consequences of, major accidents. In particular, the safety report demonstrates that measures are informed by systematic human error analysis of key safety-critical tasks, and that relevant performance influencing factors have been taken into account.</p> <p>Overall, the safety report clearly demonstrates <u>how</u> measures taken on site will assure human reliability, and <u>why</u> those measures are considered adequate, for the full range of MAHs identified.</p>

Safety Report Assessment Guide: Human Factors

Technical Criterion	Human Factors Topic	Evidence for Full Demonstration
Design		
12.2.1.1 The safety report should show that the establishment and installations are designed to an appropriate standard.		Not Normally Applicable to Human Factors Aspects
12.2.1.2 The safety report should show that a hierarchical approach to the selection of measures has been used.	Allocation of Function	<p>Function Allocation is an important element within the human-centred design process. It is undertaken prior to detailed task analysis and is used to help determine the degree of automation required within a system or process (for both monitoring and control purposes). The overall system or process is broken down into logical phases which must be accomplished to meet the overall goal. These phases are broken down further into high-level tasks or 'functions' which, at this stage, are not assessed in detail. The analysis then considers whether each function should be allocated to a human, a machine, or both (the latter accounting for the fact that some automatic functions require manual override, or that some manual tasks require automated assistance). Relevant considerations during the function allocation process may include:</p> <ul style="list-style-type: none"> ▪ human strengths (e.g. processing qualitative information; drawing upon experience to adapt to new situations; making subjective estimates and evaluations; inductive reasoning; sensing unusual events etc.); ▪ machine strengths (e.g. monitoring for tightly-defined, pre-determined events; deductive reasoning; processing quantitative information; maintaining performance under heavy information overload etc.); ▪ cognitive support: keeping the user 'in the loop' so they are ready to act / intervene at short notice (providing mental models and info. about status of system at any one time; by maintaining situational awareness etc.); ▪ affective support: considers the emotional requirements of the user (maintaining job satisfaction and motivation by providing challenging work; measures to ensure users feel 'in control' etc.). <p>Such considerations may also help determine key design, procedural and training requirements.</p> <ul style="list-style-type: none"> ! there is a clear policy and/or procedure to ensure the application of inherent safety principles at the outset of the design and modification process; ! the safety report clearly explains the basis for allocation of function: automation is well-justified and selected for the right reasons; ! where appropriate, the human contribution to failure is removed (e.g. by a more reliable, automated system); ! the implications of introducing human failure into an automated system (via design, inspection, testing, maintenance etc.) are acknowledged and addressed; ! the need for manual intervention in critical high-hazard systems (e.g. manual emergency shut down of a continuous process) is clearly justified; ! where possible, human performance is further assured by mechanical or electrical means (e.g. sequentially interlocked valves; butane tank valves incompatible with propane-rated connectors); ! training and procedures are not viewed as the sole defence against human error; they form an

Safety Report Assessment Guide: Human Factors

Technical Criterion	Human Factors Topic	Evidence for Full Demonstration
	<p>Human Factors in SIL Determination</p>	<p>integral part of a broader range of measures to control the potential for human failure.</p> <p>The following key standards (the latter being a sector-specific version of the former) provide clear guidelines for the use of electric, electronic and programmable electronic systems to achieve functional safety:</p> <ul style="list-style-type: none"> ➤ IEC 61508: Functional safety of electric / electronic / programmable electronic safety-related systems ➤ IEC 61511: Functional safety – safety instrumented systems for the process industry sector <p>Safety function is defined as one which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event. Duty-holders are required to undertake risk assessment to justify the choice of any safety instrumented functions and establish their 'safety integrity level' (SIL). The SIL defines the required performance level for a safety instrumented function (in terms of the relative level of risk reduction provided by the safety function, or the probability of failure on demand). Four SILs are defined, with SIL 1 being the lowest level of safety integrity and SIL 4 being the highest (SIL 3 & 4 are uncommon at onshore process chemical plant, and more usually associated with nuclear process plant, fly-by-wire technology in aircraft etc.).</p> <p>SIL determination may be based on quantitative or semi-quantitative analysis methods such as Fault Tree Analysis (FTA), Layers of Protection Analysis (LOPA), Risk Graphs etc. Both standards require that human factors are included in the assessment (the contribution of human error in SIL assessment can be especially significant at SIL 2 and above). A quantitative, top-down approach to human reliability is often used: Generic Human Error Probabilities (HEPs) are determined via a range of techniques (HEART; THERP; SLIM etc.), then refined to take account of Error Producing Conditions (EPCs) etc.</p> <p>The safety report illustrates how the potential for human failure is acknowledged and systematically treated in the design of safety instrumented systems. The design process prompts a multi-discipline, team approach (including input from operators and human factors specialists). Human factors are considered in the risk assessment process for both SIL Determination <u>and</u> SIL Verification.</p> <p><u>SIL Determination</u>: for each safety instrumented function, and for each mode of operation (normal; start-up; shut-down; abnormal; emergency; maintenance etc.), the safety report identifies and addresses key human tasks where:</p> <ul style="list-style-type: none"> ▪ human failure could lead to a demand on the safety function (conflicting responsibilities that may distract the operator's attention; knowledge and rule-based mistakes; acts of non-compliance, such as unauthorised use of system overrides etc.); ▪ human action could reduce the demand rate on the safety function (e.g. responding to alarms); ▪ failure of the safety function requires actions to mitigate the consequences of the event; <p>The safety report is realistic about levels of risk reduction claimed for alarm systems and considers:</p> <ul style="list-style-type: none"> ▪ availability of the operator to respond; ▪ adequacy of time to respond; ▪ the potential for alarm flooding;

Safety Report Assessment Guide: Human Factors

Technical Criterion	Human Factors Topic	Evidence for Full Demonstration
	QRA	<ul style="list-style-type: none"> ▪ whether the operator knows <i>how</i> to respond (i.e. there is a clear, documented response for each critical alarm, supported by training). <p>SIL Verification (i.e. demonstration that the required SIL level is being achieved – critical for SIL 2 and above): the safety report identifies and addresses human failures that increase the likelihood of the safety function failing to work on demand (inspection, testing, maintenance, calibration etc.).</p> <p>In addition, the potential for dependency between successive human tasks has been recognised and accounted for e.g.:</p> <ul style="list-style-type: none"> ! the HEP for one task may be significantly influenced by an error in a previous, related step/task; ! different people doing the same task may make the same error; ! the same person may make the same error during a number of tasks; ! a checker may fail to detect an error, for the same reason the user made the error; <p style="text-align: center;">See CRR 373/2001: Proposed framework for addressing human factors in IEC 61508 www.hse.gov.uk/research/crr_htm/2001/crr01373.htm</p> <p>The limitations of quantitative methods for determining human reliability are acknowledged, e.g.:</p> <ul style="list-style-type: none"> ! lack of up-to-date data on human performance in onshore major hazard industries; ! specialist human factors knowledge is required to use quantitative tools effectively; ! HEPs are generic, rather than site- or task-specific. <p>In general, and especially where the generic probability for the whole task is unrealistic, a bottom-up approach is preferred (e.g. local task analysis followed by human error analysis / human HAZOP).</p>
12.2.1.3 Layout of the plant should limit the risk during operations, inspection, testing, maintenance, modification, repair and replacement.	Maintenance Error	<p>The safety report describes how systems are designed for maintainability, to help reduce the likelihood of maintenance error (see criterion 12.2.4.2):</p> <ul style="list-style-type: none"> ! plant and equipment, including layout on site, are designed with maintenance in mind (e.g. accessibility for inspection, testing and maintenance); ! human error analysis has been undertaken on key safety-critical maintenance tasks; ! the working environment (noise; temperature; lighting etc.) has been considered; ! plant and components are clearly identified and labelled; ! up-to-date P&IDs, schematics, job-aids and other diagnostic tools are available; ! relevant maintenance personnel are involved in the design and task analysis process; ! audit and review arrangements specifically address maintainability.

Safety Report Assessment Guide: Human Factors

Technical Criterion	Human Factors Topic	Evidence for Full Demonstration
		! http://www.hse.gov.uk/humanfactors/topics/06maintenance.pdf
12.2.1.4 Utilities that are needed to implement any measure defined in the safety report should have suitable reliability, availability and survivability.		The safety report considers the human factors aspects of utility failure: ! Uninterruptible Power Supply (UPS) systems provide sufficient time to enable orderly shutdown and/or evacuation; ! UPS systems support all necessary instrumentation and equipment: ○ control room interfaces; SCADA systems; mimic panels; ○ level monitoring and gauging equipment; ○ process alarms; site-wide evacuation alarms; ○ radio base stations; land-line communication systems; ○ ROSOVs and other remotely operated shut-down equipment; ! there is adequate emergency lighting to carry out relevant shut-down tasks; where appropriate, hand-held torches are available.
12.2.1.5 The safety report should show that appropriate measures have been taken to prevent and effectively contain releases of dangerous substances.		Not Normally Applicable to Human Factors Aspects
12.2.1.6 The safety report should show that all foreseeable direct causes of major accidents have been taken into account in the design of the installation.	Managing Human Performance	A robust, structured approach to identifying and managing human failure is described: ! safety-critical tasks (i.e. those activities where human action or inaction has the potential to initiate, escalate, recover from, or mitigate the consequences of, a major accident) have been identified and are clearly linked to major hazard scenarios in the safety report; ! routine and non-routine tasks have been considered (operations; maintenance; inspection and testing; start-up and shut-down; abnormal and upset conditions; emergencies etc.); ! there exists a suitably prioritised, rolling programme to undertake human error analysis on all safety-critical tasks identified at the establishment; ! the analysis process is informed by a thorough, real-world understanding of the task and considers decision-making, communication, information gathering etc., as well as physical actions and checks; ! key steps in each safety-critical task are identified by talking to front-line personnel; reviewing

Safety Report Assessment Guide: Human Factors

Technical Criterion	Human Factors Topic	Evidence for Full Demonstration
		<p>risk assessments, procedures, training, relevant incidents etc.; walk-through/talk-throughs;</p> <ul style="list-style-type: none"> ! human error analysis is undertaken at each, critical task step; where appropriate, human HAZOP techniques and guide words are used; ! all types of human failure are considered (slips; lapses; mistakes; non-compliance); the different human failure modes identified are clearly linked to appropriate controls measures; ! Performance Influencing Factors at individual, job and organisational levels have been identified and optimised (especially management failures such as planning; allocation of resources; allocation of roles and responsibilities etc.) – see criteria 12.2.1.12 & 12.2.3.1; ! representative examples of completed task analysis documents are included within the report; ! there is evidence that potential human failures identified are actively managed according to the hierarchy of control; improvement plans are in place - see criterion 12.2.1.2; ! there is evidence that error recover is also managed (via detection, diagnosis and correction). <p style="text-align: center;"> http://www.hse.gov.uk/humanfactors/topics/humanfail.htm http://www.hse.gov.uk/humanfactors/topics/improvecompliance.pdf </p>
12.2.1.7 The safety report should show how structures important to safety have been designed to provide adequate integrity.		Not Normally Applicable to Human Factors Aspects
12.2.1.8 The safety report should show how the containment structure has been designed to withstand the loads experienced during normal operation of and all foreseeable operational extremes		Not Normally Applicable to Human Factors Aspects
12.2.1.9 The safety report should show that materials of construction used in the plant are suitable for the application.		Not Normally Applicable to Human Factors Aspects
12.2.1.10 The safety report should show that adequate safeguards have been provided to protect the plant against excursions beyond design conditions.		Not Normally Applicable to Human Factors Aspects

Safety Report Assessment Guide: Human Factors

Technical Criterion	Human Factors Topic	Evidence for Full Demonstration
	Alarm Handling	<ul style="list-style-type: none"> ➤ EEMUA 201:2002 (Process plant control desks utilising human-computer interface) ➤ NUREG-0700 (Human-system interface design review guidelines) ➤ CRR 432/2002 (Human factors aspects of remote operation in process plants) <p style="text-align: center;">http://www.hse.gov.uk/humanfactors/topics/hci.htm</p> <ul style="list-style-type: none"> ! there is a clear link between major hazard risk assessment and the on-site alarm philosophy, such that all alarms can be justified and are suitable prioritised; ! alarm handling is fully integrated into the design process and is considered at the outset; ! the design process acknowledges and accommodates human capabilities and limitations (including operator availability to respond; time to respond; the potential for alarm flooding etc.) ! alarms are useful and relevant: the report describes how alarm systems alert, inform and guide required operator action (including a defined, documented response for each safety-critical alarm, supported by training); ! alarm systems are subject to continuous improvement (for example, there is a clear link between process change and alarm system upgrade); ! relevant performance measures are defined and monitored (average alarm rate; average number of standing alarms etc.) ! specific examples are included within the report to show how relevant standards and good practice (see below) have been applied on site: <ul style="list-style-type: none"> ➤ EEMUA 191: 2007 (Alarm systems: a guide to design, management and procurement) ➤ CRR 166/1998 (The management of alarm systems) <p style="text-align: center;">http://www.hse.gov.uk/humanfactors/topics/alarm-management.htm</p>
12.2.1.13 The safety report should describe the systems for identifying locations where flammable substances could be present and how equipment has been designed to take account of the risk.		Not Normally Applicable to Human Factors Aspects
Construction		
12.2.2.1 The safety report should show that installations have been constructed to appropriate standards to prevent major		Not Normally Applicable to Human Factors Aspects

Safety Report Assessment Guide: Human Factors

Technical Criterion	Human Factors Topic	Evidence for Full Demonstration
	Audit & Review	<ul style="list-style-type: none"> ! maintenance backlogs; trends in down-time; quality and timeliness of safety-critical inspections. <p>An appraisal system exists whereby the performance of front-line personnel and managers, with key major hazard roles and responsibilities, is monitored against realistic targets and objectives.</p> <p>Key organisational lessons are captured, learned and fed into a programme of continuous improvement (which is tracked by management). A system exists to ensure regular, structured review of major hazard performance by senior management. The safety report describes how key human factors topics (see below) fall within the scope of existing audit and review arrangements;</p> <ul style="list-style-type: none"> ! human error analysis; maintenance error; ! human factors in design; allocation of function; control rooms and alarm systems; ! procedures & competence assurance; safety-critical communication (incl. PTW & shift handover) ! organisational change; staffing levels & workload; fatigue from shiftwork and overtime.
Maintenance		
12.2.4.1 The safety report should show that an appropriate maintenance scheme is established for plant and systems to prevent major accidents or reduce LOC.		Not Normally Applicable to Human Factors Aspects
12.2.4.2 The safety report should show that there are appropriate procedures for maintenance that take account of any hazardous conditions within the working environment.	Maintenance Error	<p>The potential for human error during maintenance activities is clearly acknowledged; i.e. that even highly-trained, well-motivated technicians can make simple slips and omissions, and that such errors can initiate major accidents, as well as result in personal injury to maintenance personnel.</p> <ul style="list-style-type: none"> ! the safety report describes how plant & equipment is designed for maintainability, to reduce the likelihood of maintenance error (see criterion 12.2.1.3); ! human error analysis has been undertaken on safety-critical maintenance tasks; ! maintenance tasks are well designed (work is interesting and challenging; diagnostic tools are provided; adequate time is available; distractions are minimised; PPE is realistic etc.); ! up-to-date procedures exist for safety-critical maintenance tasks (see criterion 12.2.3.1); ! relevant maintenance personnel are involved in plant and equipment design, job design, task analysis, writing procedures etc.; ! supporting resources are readily available (P&IDs; schematics; job-aids; tools and spares etc.); ! in-house and contractor maintenance activities are well supervised and controlled (effective PTW; robust isolation procedures; systematic hand-back; independent cross-checks etc.); ! effective communication channels exist between shifts, and between operations, maintenance and contractor personnel (see criterion 12.2.3.1);

Safety Report Assessment Guide: Human Factors

Technical Criterion	Human Factors Topic	Evidence for Full Demonstration
		<ul style="list-style-type: none"> ! management ensure that adequate numbers of competent maintenance personnel are available; where activities are out-sourced, the duty-holder retains an intelligent customer capability (i.e. retain adequate technical competence to judge whether, and ensure that, work is done to the required quality and safety standards); ! maintenance performance is monitored and reviewed (backlogs; excessive repair times etc); <p style="text-align: center;">http://www.hse.gov.uk/humanfactors/topics/error.htm</p>
<p>12.2.4.3 The safety report should show that systems are in place to ensure that safety critical plant and systems are examined at appropriate intervals by a competent person.</p>		<ul style="list-style-type: none"> ! suitable procedures exist for examination, inspection & proof testing, with clear pass/fail criteria; ! arrangements exist within the CMS to ensure personnel/contractors who conduct such activities are competent to do so, and are fully aware of related major hazards and their consequences; ! where activities are out-sourced, the duty-holder retains an intelligent customer capability; ! examination, inspection and testing activities are included within arrangements for performance monitoring, audit and review.
<p>12.2.4.4 There is a system in place to ensure the continued safety of the installations based on the results of periodic examinations and maintenance.</p>		<p>Not Normally Applicable to Human Factors Aspects</p>
<p>Modifications</p>		
<p>12.2.5.1 The safety report should describe the system in place for ensuring modifications are adequately conceived, designed, installed and tested.</p>	<p>Organisational Change</p>	<p>Human factors are fully integrated into arrangements to manage plant & process modifications;</p> <ul style="list-style-type: none"> ! each major project is assessed against defined inherent safety principles at the concept stage; ! human factors are considered at each stage of the modification process (design; installation; testing; hand-back etc.); ! the change process prompts a multi-discipline, team approach (including active input from relevant front-line personnel and human factors specialists). ! relevant procedures are updated to reflect the change; additional training is provided. <p>The safety report recognises that even subtle changes to organisations (reducing staff numbers; combining departments; de-layering; introducing self-managed teams; multi-skilling; other changes to roles & responsibilities etc.) can have a significant impact on the management of major hazards. The report describes robust, systematic arrangements to manage organisational change.</p> <ul style="list-style-type: none"> ! there is a clear policy and procedure, framed around recognised good practice e.g. <i>Chemical Information Sheet No CHIS7 – Organisational Change and Major Accidents</i>; ! changes are carefully planned and staggered (e.g. to avoid too many simultaneous changes); ! the assessment process considers risks and opportunities resulting from the change (where you

Safety Report Assessment Guide: Human Factors

Technical Criterion	Human Factors Topic	Evidence for Full Demonstration
	Staffing Levels & Workload	<p>want to get to), as well as risks arising from the process of change (how you get there);</p> <ul style="list-style-type: none"> ! personnel (and, contractors) actively participate before, during and after the change; ! all safety-critical tasks and key major hazard responsibilities are identified and successfully transferred to the new organisational structure; ! training, support and supervision for staff with new or changed roles is provided; there is adequate planning for competent cover during the training period; ! where roles and responsibilities are outsourced, intelligent customer capability is retained; ! a full review is undertaken prior to 'go-live'; performance is monitored post-change; ! specific examples, of how organisational change has been managed at the site, are included. <p style="text-align: center;">http://www.hse.gov.uk/humanfactors/topics/orgchange.htm</p> <p>Staffing arrangements are formally assessed pre- and post-change using recognised models (e.g. CRR 348/2001: 'Entec Report' and the Energy Institute user guide). See Criterion 12.2.3.1.</p>

Technical Criterion	Actual Evidence versus 'Evidence for Full Demonstration'	Next Steps
met	<ul style="list-style-type: none"> ! for the criterion in question, the safety report contains most of the evidence required for a full demonstration; ! all assertions are backed by a clear understanding of the potential for human failure – the report explains <u>how</u> human performance has been optimised for the criterion, rather than simply states it has been; ! specific examples are given of how relevant standards / good practice for the criterion have been implemented on site; ! human factors are fully integrated into the overall demonstration of the technical criterion in question. <p>Example: a particular plant isolation activity has been identified as a safety-critical task; task analysis and human error analysis have been undertaken; specific control measures, linked directly to the types of human failure and PIFs associated with each task step, are in place (e.g. easy access to well-labelled plant; suitable tools available; interlocked valves; reliable two-way communication with control room; specific training in a robust, up-to-date procedure; supporting PTW with active cross-checks; compliance is monitored & audited).</p>	verify by inspection

Safety Report Assessment Guide: Human Factors

partially met	<ul style="list-style-type: none"> ! for the criterion in question, the safety report includes <i>some</i> of the evidence required for a full demonstration; ! some assertions are backed by an understanding of the potential for human failure – the report attempts to explain <u>how</u> human performance has been optimised for the criterion, but falls short in certain areas; ! relevant standards and good practice for the criterion are cited, but no specific, applied examples are given; ! human factors are partially integrated into the overall demonstration of the technical criterion in question. <p>Example: the report describes a range of effective measures to prevent human failure during road tanker delivery, but there is no evidence that formal human error analysis has been undertaken: existing measures appear to have evolved organically over time. Consequently, key potential human failures and their related control measures (e.g. break-away couplings in the event of a drive-away; dedicated connection valves to prevent wrong product being delivered to the wrong bulk tank) appear to have been missed.</p>	<ul style="list-style-type: none"> ! request for further info. <ul style="list-style-type: none"> ○ readily available ○ no additional work ○ adds value ○ not verification ! Revision Plan item ! verify by inspection
not met	<ul style="list-style-type: none"> ! for the criterion in question, the safety report contains little or none of the evidence required for full a demonstration; ! broad, high-level assertions about human failure are made, with little apparent understanding of the underlying issues – the report simply states that human performance has been optimised; ! no relevant standards or good practice for the criterion are cited or referenced; ! human factors have not been considered as part of the overall demonstration of the technical criterion in question. <p>Example: the safety report fails to recognise the human tendency to break rules or fail to follow instructions; it does not attribute acts of non-compliance to Performance Influencing Factors such as time pressure, inconvenience, workload, culture etc. Claims are made such as “failure of employees to follow safety-critical procedures is not considered credible”, or “if product is released, employees will manually shut the system down and evacuate the premises”, without qualification.</p>	<ul style="list-style-type: none"> ! request for further info. ! priority inspection ! Revision Plan item ! serious deficiency?