OECD-CCA Workshop on Human Factor in Chemical Accidents and Incidents

8 – 9 May 2007, Potsdam, Germany

Discussion Document

April 2007

Prepared by:

Babette Fahlbruch
Jörk Dubiel
Lutz Neumann
Oliver Raupach

TÜV NORD SysTec GmbH & Co. KG
Große Bahnstraße 31
22525 Hamburg
Germany

Under participation of: Peggy Frommann

Content:

1 Introduction and Overview

1.1 General purpose of the workshop

This OECD-CCA workshop is sponsored and hosted by the Federal Ministry for the Environment of Germany and the Government of the Federal State Brandenburg.

Human performance remains a critical element in risk prevention. Analyses of accident data show that human factors play a causal or contributing role in 50-80% of significant accidents (Working Group on Chemical Accidents /1/ according to Gross and Ayres, 1998). The 600K report (dated 2000) of the US Chemical Safety and Hazard Investigation Board showed that among cases for which the cause was known, 49% resulted from mechanical factors and 39% from human factors. Among cases involving mechanical factors, an overwhelming 97% were attributed to general equipment error; 63% of human factors cases were attributed to human errors. A German review on the causes of major accidents reported to the ZEMA database attributed only 25% to human failure /2/. Despite of the different amount of "human contribution" to accidents, it is widely recognised that human failure in industrial operations is a major source of risk.

In 1997, an OECD Workshop on Human Performance in Chemical Process Safety: "Operating Safety in the context of Chemical Accident Prevention, Preparedness and Response" already took place in Germany[1]. The purpose of this workshop was to discuss the role of human performance in chemical processes and consider ways to minimise the number of abnormal events.

From the OECD Workshop on Lessons Learned from Chemical Accidents and Incidents (2004) recommendations for a Workshop on Human Errors were drawn[2].

The 2007 OECD/CCA-Workshop will explore all the aspects of the relationship 'human factors – chemical accident prevention' with focus on crucial and new human factors issues. The overall objective of the workshop is to explore human factors related to management and operation of a hazardous installation, and to share information on assessment tools for identification of the potential for, analysis and reduction of human errors in the chemical industry, including the small and medium size enterprises. Human action is involved in designing machines, operations and work environments, in managing and operating the facility at all levels (production, processing, use, handling, storage, transport, and disposal of hazardous substances). The objectives are to present the approaches dealing with these issues and to develop recommendations for best practices. If best practices cannot be defined, further research and co-operation needs will be identified.

[1] http://www.olis.oecd.org/olis/1999doc.nsf/LinkTo/env-jm-mono(99)12

[2] http://appli1.oecd.org/olis/2005doc.nsf/linkto/env-jm-mono(2005)6

1.2 Overview of workshop objectives

The scope of the Workshop includes any fixed installation/facility where hazardous substances are produced, processed, used, handled, stored, transported (i.e. transport interfaces including railroad marshalling yards, road terminals, airports, loading and unloading facilities, port areas and pipelines) or disposed of, with the potential for fire, toxic emission, explosion, spill, or other type of accident involving hazardous substances. Other sectors of industrial activity will be considered, in particular with respect to transfer of knowledge and experience (e.g. offshore, nuclear industry, aerospace industry), and the relationship between 'Best Practices' and the safety procedures in such high risk technologies.

A more detailed description of the workshop objectives is as follows:

- Acceptance of definitions to be added to Annex I (Explanation of Terms Used) of the OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response[3]. These harmonised definitions could be used by industry and the authorities in incident investigation, documentation and lessons learnt communication
- Make recommendations on the best ways to assess safety cultures, because the quality of the safety culture of an organisation strongly determines the effectiveness of its safety management system
- Make recommendations on appropriate human factors competence taking into account the types of responsibilities involved and the different management and staff levels in organisations (industries, authorities, expert organisations/ consultants)
- Make recommendation on the allocation of function at interfaces between safety systems and operators taken
- Make recommendation on alarm management, i.e. the adequate support of the operator in handling alarms including dealing with alarm flooding, suppression and prioritising of alarms etc.

The primary focus over the two workshop days will be to understand and to discuss human factors issues under the above mentioned scope.

1.3 Thematic structure of the workshop

The Workshop is organized according to the following five thematic sessions.

Session 1: Types of Human Error, Definition of Related Terms
Session 2: Assessment of Safety Cultures
Session 3: Appropriate Human Factors competence
Session 4: Interfaces between Safety and Operators
Session 5: Human factors in Alarm Management

[3] http://www.oecd.org/dataoecd/10/37/2789820.pdf

Speakers have been selected to "set the scene" by describing the current frameworks, methodologies and interventions. These presentations are expected to highlight emerging issues related to the thematic sessions with the aim of focusing discussions and stimulating constructive dialogue among participants.

In each session, the speakers' presentations will be followed by a general discussion where conclusions and recommendations will be drawn.

The workshop organizers are appreciative of the considerable contributions of government and industrial sector experts from Europe, North America, Oceania and Asia involved with chemical accident programs in their respective countries.

1.4 Introduction to the discussion document

This discussion document (DD) is based on information extracted from laws, regulations and directives from OECD member countries and regions on the analysis of major databases on chemical accidents as well as on a literature research on the relevant topics.

The discussion document is charged with achieving the following objectives:

- Describe the themes of the sessions
- Identify some of the key issues for consideration

2 Thematic session 1: Types of Human Error, Definition of Related Terms

Key objectives to be covered in the session

1. Make recommendations about the terminology and definitions to distinguish the different human factors aspects when analysing and documenting incidents;
2. Define related terms like human error[4], human failure, human (un)reliability, human behaviour, human performance, human contribution, human factors etc. to be include and/or revise in the OECD Guiding Principles;
3. Define relevant terms used in the recommendations of the Workshop.
4. Address the different types of human error which can occur at the various stages of management and operation of a hazardous installation (e.g. design, construction, start-up, processing; handling, storage, shut-down, etc.), and link them to causes;
5. Explain how existing tools to investigate the human contribution to accidents and near-misses are used, and how they should be improved;
6. Make recommendations on the improvement of investigation techniques and incidents databases to provide useful and detailed information about different types of human errors and the barriers that were breached in the incident or the safety management system responsible for those barriers;

2.1 Introduction

The workshop on lessons learned from chemical accidents recommended further efforts to harmonise terminology across industrial sectors and countries, so that information including accident data, data evaluation techniques, investigation methodologies and communication of lessons learned can be easily shared. Such a recommendation also applies to harmonisation of terminology related to human error.

Recommendations concerning definitions and terminology used to identify the different types of human error when analysing and documenting chemical accidents and incidents, and communicating lessons learnt will be presented in the following.

[4] The translation of the term "human error" in other languages may lead to misinterpretation. Human error is not just to be considered as a mistake, but also includes errors of judgement and perception, errors due to lack of physical capability or mental capacity, errors brought about due to lack of understanding, or due to confusing or conflicting requirements from the system concerned. It is not restricted to operators but may be experienced by all levels within a concern or institution in which interactions occur. Human error can occur in management, design, maintenance, inspection, licensing, governance and operational capacities. The term "human factors" includes additional aspects of human involvement, in particular human behaviour and ability to promote safety (human factors can be positive or negative while human errors are always negative)

For the preparation of this section of the discussion document the following sources were analysed:

- Technical standards
- Selected analysis reports of accident and incidents
- Scientific literature from the field of psychology, human factors, organization studies

2.2 Technical standards

Definitions could be identified in documents of the HSE, OECD, VDI, IEC, ISO and Namur. The definitions are either relevant for incident investigation and documentation or for sessions of this workshop.

2.2.1 Terms relevant for incident investigation and documentation

Error
Mismatch between the user's goal and the response of the system. Errors can include navigation errors, syntax errors, conceptual errors, etc" (ISO/TC 159/SC 1/WG 1 N 88, 2006 /99/).

Human error
"In this regard, it should be recognised that humans will, on occasion, fail and the majority of accidents are in some part attributable to human error, meaning human actions or inactions which unintentionally exploit weaknesses in equipment, procedures, systems and/or organisations" (HSE /3/, p.2 in HSG48 /4/)

"Human errors are not limited to operator errors but may occur at different points in the hierarchy of the enterprise including, for example, at the level of those responsible for maintenance, management of change or permit to work systems, or at the level supervisors and management. Examples of human failures, in addition to operator errors, can involve: problems with transmission of knowledge, especially when experienced specialists retire; the complexity of the system, including process design and engineering; the ageing of plants and related repairs, without adequate maintenance and inspection; and the need to cope with changes in organization or technology, including automation." (OECD, Guiding Principles for Chemical Accidents Prevention, Preparedness and Response /5/, p.135)

"Human error / working error / erroneous action / error, i.e. all human actions which exceed defined acceptance limits" (VDI 4006.1, 12.85: Human reliability /6/)

"Human error / mistake: Commission or omission which results in unintended consequence" (IEC 61511, DE /7/)

Human failure and human error
"A human error is an action or decision which was not intended, which involved a deviation from an accepted standard and which led to an undesirable outcome'. Human failure refers to errors AND violations (i.e. non-compliance with rules or procedures)." (HSE, 2005, /94/ p. 83 according to HSG48)

Human factors

"Human factors refer to environmental, organisational and job factors, and human and individual characteristics, which influences behaviour at work in a way which can effect health and safety" (HSE /3/, p.2 in HSG48 /4/).

"The term "human factors" is often used in a negative context (equating it to human error). However, humans are often the only means for effectively responding to abnormal situations since they have the capability to reason, and then to override automatic reactions of machines. Humans have the capacity to forecast action, integrate complex and fuzzy information, and understand how to address unusual situations based on experience and training."(OECD, Guiding Principles for Chemical Accidents Prevention, Preparedness and Response /5/, p.55)

"Human factors involve designing machines, operations and work environments so that they match human capabilities, limitations and needs (and, therefore, is broader than concerns related to the man-machine interface). It is based on the study of people in the work environment (operators, managers, maintenance staff, and others) and of factors that generally influence humans in their relationship with the technical installation (including the individual, the organisation and the technology)" (OECD, Guiding Principles for Chemical Accidents Prevention, Preparedness and Response, /5/, p.179).

Human failure

"refers to errors made by those at the sharp end of incident causation that have directly triggered the incident" /41/, p. 9. According to the HSE definition it is " important to remember that human failures are not random; there are patterns to them. […] There are three different types of human failures (unsafe acts) that may lead to major accidents:

Intentional errors:

Violations differ from the above in that they are intentional (but usually well-meaning) failures, such as taking a short-cut or non-compliance with procedures e.g. deliberate deviations from the rules or procedures. They are rarely wilful (e.g. sabotage) and usually result from an intention to get the job done despite the consequences. Violations may be situational, routine, exceptional or malicious." /3/, p. 2f

Unintentional errors:

Errors (slips/lapses) are "actions that were not as planned" (unintended actions). These can occur during a familiar task e.g. omissions like forgetting to do something, which are particularly relevant to repair, maintenance, calibration or testing. These are unlikely to be eliminated by training and need to be designed out.

Mistakes are also errors, but errors of judgement or decision-making ("intended actions are wrong") - where we do the wrong thing believing it to be right. These can appear in situations where behaviour is based on remembered rules or familiar procedures or unfamiliar situations where decisions are formed from first principles and lead to misdiagnoses or miscalculations. Training is the key to avoiding mistakes.

Human performance

"Human performance: All aspects of human action relevant to the safe operation of a hazardous installation, in all phases of the installation from conception and design, through operation, maintenance, decommissioning, and shutdown"(OECD, Guiding Principles for Chemical Accidents Prevention, Preparedness and Response /5/, p.179).

Violation

"A deliberate breach of rules and procedures." (HSE Human Factors Briefing Note No. 3, Humans and Risk, /98/ p. 3).

"An error that occurs when an action is taken which contravenes known operational rules, restrictions and/or procedures. The definition of violations excludes actions taken to intentionally harm the system, i.e., sabotage." (HSE, 2005, /94/ p. 83)

2.2.2 Terms relevant for sessions of this workshop

Alarm

"Indication requiring immediate response by the operator. The response may be, for example, manual intervention, increased watchfulness or initiation of further investigation. Note: *This is a more extended notion of alarm than the VDI/VDE 3699 definition, and follows the common usage of English and the use of the term in the context of PCS"* (Namur-Worksheet NA 102 /8/, p.6).

"warning of existing or approaching danger" (ISO/TC 159/SC 1/WG 1 N 88, 2006 /99/).

"Traditionally, alarms were used to provide safety information to plant operators. This included alarms on process conditions that could result in injury to personnel and/or equipment damage, if no action was taken. When computer control systems were introduced into process plants, alarms could be easily added, and they are now used for a much wider range of uses. This includes event logging, indication of process deviations, plant status, abnormal process conditions, etc." (HSE, 2005, /94/ p. 2)

Alarm flooding (alarm shower)

"Situation in which alarms occur faster than they can be perceived and processed by the operator" (for "alarm shower" in Namur-Worksheet NA 102 /8/, p.6).

"Alarm flooding is a condition where alarms appear on the control panels at a rate faster than the operator can comprehend or deal with. Alarm flooding prevents the operator from determining the cause of the process upset or process emergency and therefore limits the scope for effective and quick emergency response." (HSE, 2000 /95/)

"An alarm "flood" is when operators are presented with too many alarms within a short space of time so that they cannot identify individual alarms and take action upon them. In these circumstances operators will often miss or ignore alarms. Alarm floods often occur during process disturbances e.g. power failure when the information they supply the operator is most critical." (HSE, 2005 /94/, p. 2)

Alarm Management
"Alarm management systems support the operator in avoiding and controlling abnormal conditions" (Namur-Worksheet NA 102 /8/, p.6).

Alarm rate
"Number of alarms that occur per unit of time" (Namur-Worksheet NA 102 /8/, p.6).

Behaviour
"skill-based behaviour
Behavior mostly related to frequent tasks. Only a small degree of conscious thinking activity is required.

rule-based behaviour
Behaviour mostly related to less-familiar tasks, which are based on the experience and capabilities of the person in question. The behaviour is the result of comparing the information with familiar patterns or rules on an if-then-basis.

knowledge-based behaviour
Behaviour mostly related to new tasks, whereas familiar patterns and rules cannot be applicated directly. Requires a high degree of conscious thinking." (VDI 4006 Part 1 /6/, p.2)

Critical alarm
"safety critical alarms are distinguishable from other operational alarms" (HSE, 2005 /94/, p. 1)

"For critical (all?) alarms, the expected operator action is documented. The state of all critical alarms is always visible. Critical alarms are tested on some plant-defined frequency." (HSE, 1998 /96/, p. 217)

Ergonomics
"The area of ergonomics with the purpose of designing working conditions adapted to human beings. The discipline which deals with the design and handling of machines as well as with working environments so that these match human capabilities and limitations" (VDI 4006 Part 1 /6/, p.3).

Human reliability
"The capability of human beings to complete a task under given conditions within a defined period of time and within the acceptance limits" (VDI 4006 Part 1 /6/, p.3).

Man-machine-system (MMS)
"The combinations and the total of interactions between human beings and operational means during the work" (VDI 4006 Part 1 /6/, p.3).

Message
"Indication or report of an occurrence i.e. transition from one discrete status to another (according to VDI/VDE 3699). Note: *The term "message" or "notification" is used in the literature both as a generic and a particular term.* In this worksheet, the

term is used for those messages that do not necessitate an immediate response from the operator."(Namur-Worksheet NA 102 /8/, p.6).

Qualification

"The existence of physical, mental, and personal qualifications for tasks with specific requirements, whereby it is essential to dispose of capabilities (physical as well as psychological) and skills (behaviour learned and trained) to react according to the requirements" (VDI 4006 Part 1 /6/ p.3).

Safety culture

"Safety Culture is a term that was first introduced after the Chernobyl disaster in 1986. The safety culture of an organisation is the product of the individual and group values, attitudes, competencies and patterns of behaviour that determine the style and proficiency of an organisation's health and safety programmes." (postnote, 2001, /97/ p. 5)

"safety culture" is seen as being something that operators have and it has been found, following the investigation of major accidents, that management have not acknowledged that the development and maintenance of a safe culture lie within the bounds of their responsibility." (HSE, 2005, /94/ p.7)

"The safety culture of an organisation is the product of individual and group values, attitudes, perceptions, competencies, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation's health and safety management. Organisations with a positive safety culture are characterised by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures." (HSE, 2005, /94/ p. 59 according to ACSNI, 1993)

Safety culture is an amalgamation of values, standards, morals and norms of acceptable behaviour. These are aimed at maintaining a self-disciplined approach to the enhancement of safety beyond legislative and regulatory requirements. Therefore, safety culture has to be inherent in the thoughts and actions of all the individuals at every level in an organization. The leadership provided by top management is crucial. Safety culture applies to conventional and personal safety as well as nuclear safety. All safety considerations are affected by common points of beliefs, attitudes, behaviour, and cultural differences, closely linked to a shared system of values and standards. (According to INSAG-4 /47/, p. 3)

Safety climate

"the workforce's attitudes and perceptions at a given place and time. It is a snapshot of the state of safety providing an indicator of the underlying safety culture of an organisation." (PRISM, 2003, /91/ p.6)

Safety function

"function to be implemented by an SIS, other technology safety related system or external risk, reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event

NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology." (IEC 61511-1, 2003 /7/, p. 25)

Safety instrumented system (SIS)

"instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements (s) (IEC 61511-1, 2003 /7/, p. 25f)

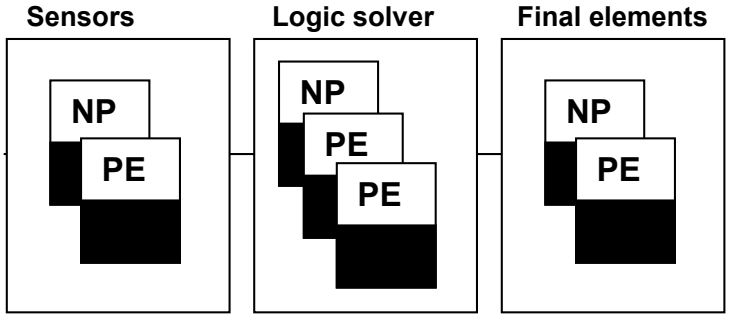


Figure 1: Example of SIS architecture (IEC, 61511-1, /7/, p. 25)

Task analysis

"Analytical process for determining the behavior of persons within a man-machine system. The goal of the task analysis in the framework of the HRA is to decompose action sequences into single steps (action elements) which then in turn are accessible for a qualitative and quantitative assessment and representation according to the chosen modeling approach" (VDI 4006 Part 2 /9/ p. 5).

"analytical process employed to determine the specific behaviours required of people when operating equipment or doing work (ISO 9241-5:1998). Note: The task analysis is not a risk assessment of the workplace according to legal requirements" (ISO/TC 159/SC 1/WG 1 N 88, 2006).

Training

"Organized education which is designed to increase and maintain the physical and psychological performance capabilities of human beings" (VDI 4006 Part 1 /6/ p.4).

Work load

"The entirety of all external conditions and requirements in the working system, which could influence a person physically and/or psychologically (VDI 4006, Part 1 /6/, p.4).

Work stress/ external load

"sum of those external conditions and demands in the work system which act to disturb a person's physiological and/or psychological state" (ISO/TC 159/SC 1/WG 1 N 88, 2006).

2.3 Analysis of accidents and incidents

In the reports no definitions of human errors were identified, but the following classifications.

In the MARS[5] database which is used by both EU and OECD member countries to report industrial accidents in the MARS standard format and to exchange accidents information 603 events are reported, about 40% classified are as “Cause Human”. The single descriptions do not result in a useful classification, because their variation is too broad and results in about 70 different causes (see table 6 in the annex for the descriptions).

A comparable picture shows the German database ZEMA: 502 events are reported, 124 with “cause is human error”. Descriptions are similar to those in the MARS database.

The Chemical Safety and Hazard Investigation Board (CSB) of the United States of America is an independent federal agency charged with investigating industrial chemical accidents. The CSB conducts root cause investigations of chemical accidents at fixed industrial facilities. CSB-reports are available in the internet, but without selection functions according to causes. Three reports on events with a human contribution are summarized in the annex as an example.

The U.S. Nuclear Regulatory Commission (NRC) collects data from its own inspection reports and from Licensee Event Reports (LERs), which are submitted by the operators of the nuclear power plants and other nuclear facilities. NRC uses this information to assess training procedures, organizational processes, human-system interface, communication, and inspections. Using defined criteria, NRC sorts the descriptions of human performance issues into the following eight categories and codes them:

1. Training
2. Procedures and Reference Documents
3. Fitness for Duty
4. Oversight [6]
5. Problem Identification & Resolution
6. Communication
7. Human-System Interface and Environment
8. Work Planning and Practices

Each category is further divided into areas, and each area contains a series of details that describe the human performance issue (updated January 2006) See the table 7 in the annex for a listing of the possible codes.

[5] Major Accident Hazards Bureau (MAHB), http://mahbsrv.jrc.it/

[6] Oversight as the activity that managers carry out to prevent things being over-looked.

The HSE suggest a classification scheme for human failures in which a differentiation between action errors, checking errors, information retrieval errors, information communication errors, selection, planning errors, and violations is made HSE, 2004 /93/, p.5f):

Action Errors
A1 Operation too long / short
A2 Operation mistimed
A3 Operation in wrong direction
A4 Operation too little / too much
A5 Operation too fast / too slow
A6 Misalign
A7 Right operation on wrong object
A8 Wrong operation on right object
A9 Operation omitted
A10 Operation incomplete
A11 Operation too early / late

Checking Errors
C1 Check omitted
C2 Check incomplete
C3 Right check on wrong object
C4 Wrong check on right object
C5 Check too early / late

Information Retrieval Errors
R1 Information not obtained
R2 Wrong information obtained
R3 Information retrieval incomplete
R4 Information incorrectly interpreted

Information Communication Errors
I1 Information not communicated
I2 Wrong information communicated
I3 Information communication incomplete
I4 Information communication unclear

Selection Errors
S1 Selection omitted
S2 Wrong selection made

Planning Errors
P1 Plan omitted
P2 Plan incorrect

Violations
V1 Deliberate actions

The Health & Safety Laboratory (HSL) of the United Kingdom published a report on the causes of major incidents (HSL /10/). One of the main findings points to the importance of organizational factors: “The literature on the control of human factors in the major hazard industry points to a focus on organizational factors (via safety culture) more than individual behaviours.”(HSL /10/, p. iv) or “The numerous case studies and analyses of incident reports show that human error influenced by human and organisational factors are implicated as a cause of incidents in the major hazard sector. It is recognised that controls on human and organisational factors are even more important than technology because significant improvements have been made to ensure increasingly inherent safety of machinery, technology and equipment (e.g. Lee /11/).” (HSL /10/, p. 4).

In the report it was highlighted that a complex chain of events including factor from organisation, individual and technology existed for the majority of accidents. This combination of events resulted in the incident. Key factors that contributed to the accidents were:

- Poor management practices, e.g. inadequate supervision
- Pressure to meet production targets
- Inadequate safety management system
- Failure to learn lessons from previous incidents
- Communication issues e.g. between shifts, between personnel and management etc.
- Inadequate reporting systems
- Complacency
- Violation/non-compliance behaviour
- Inadequate training e.g. emergency response, fire and safety
- Lack of competency
- Excessive working hours resulting in mental fatigue
- Inadequate procedures
- Modification/ updates to equipment without operator knowledge and /or revised risk assessments
- Inadequate / insufficient maintenance
- Maintenance errors

Similar factors were identified ten years before in a HSE-report on the contribution of attitudinal and management factors to risk in the chemical industry (HSE CRR 81 /12/): Although there was little detail in the accident reports on underlying causes, as the reports were focussed on the immediate causes, some main human factors issues could be identified as contributing:

- Maintenance errors
- Inadequate procedures
- Inadequate job planning
- Inadequate risk assessment
- Inadequate training of staff
- Unsafe working condoned by supervisors / managers
- Inadequate control and monitoring of staff by managers
- Inadequate monitoring of contractors working on site

A review on documented methods / instrument for event analysis showed the following picture /13/: The majority of the evaluated methods (*Change Analysis*, ASSET – *Assessment of Safety Significant Events Teams*, CREAM – *Cognitive Reliability and Error Analysis Method*, HPES – *Human Performance Enhancement System*, MORT – *Management Oversight and Risk Tree* , SOL – *Safety through Organizational Learning,* STEP – *Sequentially Timed Event Plotting,* TOR – *Technique of Operations and Review)* cover intermediate causes as well as underlying mechanism. Although there are some differences according to the causal categories, the above mentioned main human factors issues are taken into account in the methods, except in Change Analysis and STEP, which have no categories or classification scheme for causes.

2.4 Scientific literature from the field of psychology, human factors, organization studies

In the literature there are various definitions of human errors as the following examples show:

"The fundamental semantic problem is that the term "human error" has at least three different denotations, so that it can mean either the cause of something, the event itself (the action), or the outcome of the action." /14/, p.1:

- "Human error "as cause: "The oil spill was caused by human error". Here the focus is on the action (the "human error") as the alleged cause of the observed outcome (the oil spill).

- "Human error "as event or action: "I forgot to check the water level". Here the focus is on the action or process itself, whereas the outcome or the consequence is not considered. […]

- „Human error "as consequence: "I made the error of putting salt in the coffee". Here the focus is on the outcome, although the linguistic description is of the action. […] A more serious example is the use of the term "latent human error". This implies, wrongly, that one or more "human errors" are hidden somewhere in the system in the system and that they have yet to manifest themselves. The intended meaning is rather that the system hides one or more latent consequences of a "human error" that already have occurred" /14/, p.1. In industry usually, only errors having non acceptable consequences (i.e. outside the field of safety operations, as defined by procedures, instructions and safety analyses) are labelled 'errors' On the other hand, psychologists define error as an erroneous act, whatever its consequences, or the level at which it is detected and recovered. /15/, S. 112.

"Rasmussen, Duncan, and Leplat (1987) defined human errors as an act that is counterproductive with respect to the person's (private or subjective) intentions or goals. A group of experts at the OECD defined human error as behaviour, or its effects, which lead a system to exceed acceptable limits (Nicolet, 1987). For Mashour (1974), error is the deviation of actual performance from the desired performance of

criterion. Kruglanski and Ajzen (1983) described error as the type of experience a person might have following an encountered inconsistency between a given hypothesis, conclusion, or inference, and a firmly held belief." /16/, p. 420.

"Human error is a feature of human activity: it describes that type of activity that causes the controlled system to diverge further than the tolerated field of variation […]. Human error is an ambiguous expression that must not lead to a uni-causal conception of error but encourage the search for the multiple determining factors in its production. The goal of the analysis of human error will be to discover these determining factors." /17/, p.126.

"How are faults and errors defined? Basically they are defined as causes of unfulfilled purposes […] human errors can be compared with intermittent faults in an electronic system. For such faults, you will often stick to the deterministic explanation and look for external causes such as noise interference. " /18/, p.98

"If a system performs less satisfactorily than it normally does - because of a human act - the cause will very likely be identified as a human error." /19/, p.827

"We define an error as the integrated accidental causation of an accident, injury, or death, whether or not there are multiple contributions, systems, error types, or persons involved." /20/, p. 279.

"There are three elements to an action- theory- based definition of an error: (a) errors only appear in goal- oriented action; (b) an error implies non-attainment of a goal; (c) an error should have been potentially avoidable (cf. Frese & Peters, 1988; Norman, 1984; Rasmussen, 1987c, Reason, 1987b, 1990)." /21/, p.313.

"Defining error as a 'failure of planned actions to achieve their desired goal' […] /22/, p. 4 according to /23/.

"Errors represent the mental or physical activities of individuals that fail to achieve their intended outcome." /24/, p. 1.

"…error can be defined as action or inaction leading to deviation from team or organisational interventions." /25/, p. 781.

"Any action (or inaction) that potentially or actually results in negative system effects given the situation that other possibilities were available. This includes any deviation from operating procedures, good working practice or intentions. There are several benefits of this definition. First, the definition of human error is neural with regard to any question of blame. Second, an error does not need to involve any system consequences. This is in concordance with the principle that an error should be judged on the basis of the underlying processes and not the product. Third, an action or inaction can only be labelled as an error if another alternative was available. Finally, the definition accepts several different criteria or standards to which the performance can be compared, namely the standards operating procedures, good working practice or simply the actor's intentions." /26/, p. 22

"Human error is considered here as any action or failure to act by a human being in the process of his activity, which violates understood standards or acceptable boundaries of behaviour (Kotik and Yemelyanov, 1985; Miller and Swain, 1986) The notion of error is not necessarily associated with guilt, the consequences of the error or the presence or absence of intention." /27/, p. 2437.

"[…] errors as phenomena which are closely related to the correct execution of the respective action, i.e., the two are regarded as two sides of the same coin (e.g., Reason, 1979; Fromkin, 1980; Wehner & Stadler, in press). As a consequence, and in contrast to other disciplines such as engineering, psychological error research deals with both, the description and causal analysis of errors, with their phenotype and genotype (cf. Becker et al., 1994)." /28/, p. 5.

"[…] any human action that exceeds some limit of acceptability (i.e. an out- of- tolerance action) where the limits of human performance are defined by the system." /29/

"Errors are connected with goals and purposes. An individual is always aiming towards some objective and has not yet got there. As soon as he achieves one objective he turns his attention to another one thereby deliberately perpetuating or recreating a state of error […] error can be defined as a transgression of a rule." /30/, p. 727.

"Errors are, basically, defined as being human acts which are judged by somebody to deviate from some kind of reference act. This reference, however, is not stable but depends on the circumstances of the judgement. […] In consequence, the perception of an act as being an error depends on the identity of the judge and the point in time of judgement. That is the concept of ´human error´ is subjective and varies with time. In addition the definition of error appears to be changing with the nature of the work environment in question" /31/.

"...departure from acceptable or desirable practice on the part of an individual that can result in unacceptable or undesirable results" /32/, p. 538; /33/, p. 432.

"[…] human errors as instances of man- machine misfits, i.e., instances when human variability is not within the span acceptable for successful task performance. Variations in performance become human errors only in an ´unkind´ environment which does not allow immediate correction. This means that to characterize human ´errors´, one has to determine the variability of human behaviour and there acceptance limits for variation which hold for the work situation. Generally, human errors are defined in terms of faulty, external task element and data are collected correspondingly." /34/, p. 82).

"[…] any failure in a system may be seen as human error" /35/, p.10.

To organize these different understandings and perspectives on human error and human factors it is suggested to classify them according to task, action, consequences and organizational aspects:

1. Task related definitions

Omission: „failure to act at all", „what is not done", „failing to do the right thing" /16/, p. 419; /36/, p. 126; (AHRQ, 2007 according to Reason 1990, 2000)

Commission: „the correct function at the wrong time", „what is done", „doing something wrong" /16/, p. 419; /36/, p. 126; (AHRQ, 2007)

2. Action related definitions

Terms: slips, lapses, mistakes

„Errors as failure of planned actions to achieve their desired ends." /37/, p.71.

„The plan is adequate, but the action fail to go as planned." /37/, p. 71.

„The actions may conform exactly to the plan, but the plan is inadequate to achieve its intended outcome." /37/, p. 71.

3. Consequence related definitions

Violation: "deviation from safe operating practice" /22/, p. 6, "the failure to apply a good rule" /22/, p. 6 according to /38/)

Mismatch: „errors considered as occurrences of man- task mismatches" /39/, p. 53.

4. Definitions related to organizational aspects

Terms: latent failures, performance shaping factors (PSFs), general failure types

„Errors as described by Reason relates to the difference in the active or latent nature of error" /22/, p. 4

„Active errors occur at the point of contact between a human and some aspect of a larger system (eg, a human-machine interface). They are generally readily apparent (eg, pushing an incorrect button, ignoring a warning light) and almost always involve someone at the frontline. Latent errors (or latent conditions), in contrast, refer to less apparent failures of organization or design that contributed to the occurrence of errors or allowed them to cause harm" (AHRQ, 2007 according to Reason 1990, 2000)

"Unsafe acts and situations do not just occur. They are generated by mechanism acting in an organisation. …Sometimes those mechanisms result from decisions taken high in the organisation, thereby causing many unsafe acts. … These mechanisms are called General Failure Types (GFTs)." 11 GFTs were identified as follows /40/, p.151:

- hardware defects
- inappropriate design
- poor maintenance management
- poor operating procedures
- error- enforcing conditions
- poor housekeeping
- incompatible goals
- communication failures
- organizational failures
- inadequate training
- inadequate defences

Reason /38/, /37/ suggested a widely accepted model on human error which he defines "as the failure of planned actions to achieve their desired ends – without the intervention of some unforeseeable event" (p. 71). In this definition are three elements: 1.) a plan or intention including the goal and how to achieve it; 2) a sequence of actions initiated by that plan and 3.) the extent to which these actions are successful in achieving that goal.

Table 1: Summary of the principal error types according to Reason /38/

Human Failure					
Errors				Violations	
Slips		Mistakes		Misvention	Mispliance
Attentional slips of action	Lapses of memory	Rule-based mistakes	Knowledge-based mistakes		

As the following explanations of the different human failure types show most of the above mentioned terms and definitions can be subsumed under Reason's model.

- **Slips**
  The plan is adequate, but the actions fail to go as planned
- **Attentional slips of action**
  are related to observable actions and associated with attentional or perceptual failures
- **Lapses of memory**
  are more internal events and generally involve failures of memory
- **Mistakes**
  The actions conform to the plan, but the plan is inadequate to achieve the goal. The failure lies at a higher level, the mental processes go wrong
- **Rule-based mistake**
  misapplication of good mental rules or the application of bad mental rules
- **Knowledge-based mistakes**
  occur when there are no prepackaged solutions and problem solutions have to identified on line
- **Violations**
  the failure to apply a good rule
- **Misvention**
  behaviour that involves both a deviation from appropriate safety procedures and errors leading to unsafe outcome
- **Mispliance**
  behaviour that involves mistaken compliance with inappropriate or inaccurate operating procedures, leading to an unsafe outcome

2.5 Conclusions

If the different terms like human error, human failure, human factors etc should be defined it seems reasonable to order them in a hierarchic model like the one of Reason described above.

Summarizing the background for this thematic session the following **additional** terms and definitions are identified as important for integration in the glossary of the OECD Guiding Principles:

2.5.1 Terms relevant for incident investigation and documentation

1. **Error of omission**
   which are „failure to act at all“, „what is not done” and „failing to do the right thing” /16/, p. 421; /36/, p. 126; (AHRQ, 2007) can be subsumed under slips (of action)

2. **Error of commission**
   which are „the correct function at the wrong time“, „what is done” and „doing something wrong” /16/, p.421; /36/, p. 126; (AHRQ, 2007) can be subsumed under lapses (of memory)

3. **Human error**
   “In this regard, it should be recognised that humans will, on occasion, fail and the majority of accidents are in some part attributable to human error, meaning human actions or inactions which unintentionally exploit weaknesses in equipment, procedures, systems and/or organisations” (HSE /3/, p.2 in HSG48 /4/)
   Unintentional errors:
   slips/lapses are “actions that were not as planned” (unintended actions). These can occur during a familiar task e.g. omissions like forgetting to do something, which are particularly relevant to repair, maintenance, calibration or testing. These are unlikely to be eliminated by training and need to be designed out /41/.
   Mistakes are also errors, but errors of judgement or decision-making (“intended actions are wrong”) - where we do the wrong thing believing it to be right. These can appear in situations where behaviour is based on remembered rules or familiar procedures or unfamiliar situations where decisions are formed from first principles and lead to misdiagnoses or miscalculations. Training is the key to avoiding mistakes /41/.
   Intentional errors:
   Violations differ from the above in that they are intentional (but usually well-meaning) failures, such as taking a short-cut or non-compliance with procedures e.g. deliberate deviations from the rules or procedures. They are rarely wilful (e.g. sabotage) and usually result from an intention to get the job done despite the consequences. Violations may be situational, routine, exceptional or malicious.“ /3/, p. 2f

4. **Active error**
   which relates to human error: „ […] active failures are made by those at the sharp end of incident causation (e.g. control room operators, maintenance personnel, the pilot who shuts down the perfectly healthy engine in the incident description). Failures made at the sharp end generally lead to direct consequences and the one making the failure is therefore also likely to experience the consequences" /41/, p.11, according to /38/.

5. **Latent Error**
   which are mainly organizational errors*:* „Latent errors … are made at the blunt end by those whose activities are removed in both time and sharp end of incident causation (e.g. high level decision makers, designers, the CAA in the incident description). These latent failures create the conditions for active failures to be made" /41/, p.11, according to /38/.

6. **Organizational culture**
   "a pattern of basic assumptions-invented, discovered, or developed by a given group as it learns to cope with its problems of external adaptation and internal integration that has worked well enough to be considered valid and therefore to be thought to new members as the correct way to perceive, think, and feel in relation to those problems" (Schein, 1985, p.9).

7. **Qualification**
   "The existence of physical, mental, and personal qualifications for tasks with specific requirements, whereby it is essential to dispose of capabilities (physical as well as psychological) and skills (behaviour learned and trained) to react according to the requirements" /6/, p.3.

8. **Safety culture**
   Safety culture is an amalgamation of values, standards, morals and norms of acceptable behaviour. These are aimed at maintaining a self-disciplined approach to the enhancement of safety beyond legislative and regulatory requirements. Therefore, safety culture has to be inherent in the thoughts and actions of all the individuals at every level in an organization. The leadership provided by top management is crucial. Safety culture applies to conventional and personal safety as well as nuclear safety. All safety considerations are affected by common points of beliefs, attitudes, behaviour, and cultural differences, closely linked to a shared system of values and standards. (According to INSAG-4 /47/, p. 3)

9. **Safety climate**
   "the workforce's attitudes and perceptions at a given place and time. It is a snapshot of the state of safety providing an indicator of the underlying safety culture of an organisation." (PRISM, 2003, /91/, p.6)

10. **Training**
    "Organized education which is designed to increase and maintain the physical and psychological performance capabilities of human beings" /6/, p.4.

11. Work load

"The entirety of all external conditions and requirements in the working system, which could influence a person physically and/or psychologically /6/, p.4.

12. Work stress

"sum of those external conditions and demands in the work system which act to disturb a person's physiological and/or psychological state" (ISO/TC 159/SC 1/WG 1 N 88, 2006).

2.5.2 Terms relevant for sessions of this workshop

13. Alarm

"Indication requiring immediate response by the operator" for reasons of safety. "The response may be, for example, manual intervention, increased watchfulness or initiation of further investigation." (according to Namur-Worksheet NA 102 /8/, p.6).

14. Alarm flooding

"Situation in which alarms occur faster than they can be perceived and processed by the operator" according to /8/, p.6.

15. Alarm Management

"Alarm management systems support the operator in avoiding and controlling abnormal conditions" /8/, p.6.

16. Alarm Priority

"Classification of alarms according to their importance (e.g. seriousness of consequences and urgency)" /8/, p.6.

17. Alarm rate

"Number of alarms that occur per unit of time" /8/, p.6.

18. Behaviour

skill-based behaviour

"Behavior mostly related to frequent tasks. Only a small degree of conscious thinking activity is required."

rule-based behaviour

"Behaviour mostly related to less-familiar tasks, which are based on the experience and capabilities of the person in question. The behaviour is the result of comparing the information with familiar patterns or rules on a if-then-basis."

knowledge-based behaviour

"Behaviour mostly related to new tasks, whereas familiar patterns and rules cannot be applicated directly. Requires a high degree of conscious thinking" /6/, p.2.

19. Critical alarm

"Safety critical alarms are distinguishable from other operational alarms. For critical alarms, the expected operator action is documented. The state of all critical alarms is always visible. Critical alarms are tested on some plant-defined frequency." (according to HSE, 1998 /96/, p. 217)

20. Human reliability

Which refers to the absence of human errors: The capability of human beings to complete a task under given conditions within a defined period of time and within the acceptance limits. /6/.

21. Ergonomics

"The area of ergonomics with the purpose of designing working conditions adapted to human beings. The discipline which deals with the design and handling of machines as well as with working environments so that these match human capabilities and limitations" /6/, p.3.

22. Man-machine-system (MMS)

"The combinations and the total of interactions between human beings and operational means during the work" /6/, p.3.

23. Message

"Indication or report of an occurrence i.e. transition from one discrete status to another (according to VDI/VDE 3699). Note: *The term "message" or "notification" is used in the literature both as a generic and a particular term.* In this worksheet, the term is used for those messages that do not necessitate an immediate response from the operator". /8/, p.6.

24. Performance shaping factors

In modelling human performance for PRA, it is necessary to consider those factors that have the most effect on performance. …Some of these performance shaping factors (PSFs) are external to the person and some are internal. The external PSFs include the entire work environment, especially the equipment design and the written procedures or oral instructions. The internal PSFs represent the individual characteristics of the person – his skills, motivations, and the expectations that influence his performance. /42/, p.2-5

25. Safety function

"function to be implemented by an SIS, other technology safety related system or external risk, reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event

26. Safety instrumented system (SIS)

"instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements (s) (according IEC 61511-1, 2003 /7/, p. 25f)

27. Safety life cycle

"necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use

28. Task analysis

"Analytical process employed to determine the specific behaviours required of people when operating equipment or doing work (ISO 9241-5:1998). Note: The task analysis is not a risk assessment of the workplace according to legal requirements" (ISO/TC 159/SC 1/WG 1 N 88, 2006).

In addressing the different types of human error which can occur at the various stages of management and operation of a hazardous installation (e.g. design, construction, start-up, processing; handling, storage, shut-down, etc.) it seems sensible to use an empirical proofed classification like the GFT-model which covers the factors addressed in the HSE /3,12/ and HSL /10/ reports discussed above:

- hardware defects
- inappropriate design
- poor maintenance management
- poor operating procedures
- error- enforcing conditions
- poor housekeeping
- incompatible goals
- communication failures
- organizational failures
- inadequate training
- inadequate defences

Beside the analysis of the different accident-databases and explanation of existing tools and their possible improvements is given by the above mentioned HSE /3, 12/ and HSL /10/ reports. In these reports important factors contributing either as intermediate or underlying causes are identified, but also the problem that not all reports are detailed enough. For this problem it is suggested to classify both kinds of causal factors in the future. A coding scheme could be linked to the list of factors from the above mentioned reports. As tools to identify underlying causes one of the reviewed methods could be used.

2.6 Questions

1. Is a hierarchical model of terms related to human factors/error for the definition useful?
2. Are the definitions suitable/ useful in regard to event-analysis and reporting?
3. Are relevant definitions missing?
4. Are the definitions and the system for incident analysis suitable as a basis for testing and further amending in a working group to be considered for reports to MARS?

3 Thematic session 2: Assessment of Safety Cultures

Key objectives to be covered in the session

- Describe methodologies and instruments which allow to assess safety cultures as well as how to improve them;
- Define basic requirements of these methodologies/ instruments, e.g. requirements related to the dimensions/key elements to be assessed as well as structures and/or groups to be included;
- Explain the use of safety culture assessment to improve safety;
- Make recommendations on the best ways to assess safety cultures;

3.1 Introduction

The main focus in this session is the prevention and mitigation of chemical accidents, i.e. the process safety, not the prevention of occupational accidents, i.e. workplace safety. Therefore definitions of safety culture and safety climate are discussed, ways to characterize and differentiate safety culture are described and possibilities to assess or evaluate safety culture and safety climate are presented. The question how to improve safety culture is not part of this document.

The OECD *Guiding Principles* /5/ highlights the importance of safety cultures and include several recommendations concerning the different elements of a safety culture. Presently, there are no recommendations on methodologies to assess existing safety cultures and how they can be improved. The topics to be addressed under this item include: Review the existing, and as far as possible well proven, approaches to assess safety cultures; define the likely key elements of these methodologies; and make recommendations on how progress of safety cultures assessment should be addressed. Reference to the relevant sections of the *OECD Guidance on Safety Performance Indicators* /43/ should be made.

In spite of its wide diffusion and use, the term safety culture is still vague in its understanding and theoretical underpinnings - ranging from cognitive characteristics of the members of an organization to a more comprehensive notion including also behaviour not only of the members of a given organization but of all actors in the system understood in its wider sense: individual organization members, work teams, organizational features and units, extra-organizational environment, technology. A growing consensus emerges that safety culture ought to be conceived as a holistic and integrating concept. /44/. Safety culture should be seen as an aspect of the organizational culture in which safety is a critical factor in the norms, values and attidudes of every staff member. The mostly referred model in this regard is the model of Schein (1985). He defines the culture of an organization as “a pattern of basic assumptions-invented, discovered, or developed by a given group as it learns to cope with its problems of external adaptation and internal integration-that has worked well enough to be considered valid and therefore to be thought to new members as the correct way to perceive, think, and feel in relation to those problems” (p.9). With respect to the empirical approach and the question about the practical relevance can both concepts be equated.

Because there are many problems in the assessment of safety culture, but a huge body of references of safety climate tools /90/, also some links to safety climate are drawn. According to Olive, O'Connor and Mannan /56/ both phrases: safety culture and safety climate can be used to describe the underlying safety attitude of an organization. The authors argued that "safety climate generally refers to the attitude the people in the organization have towards safety. […] Culture can be viewed as the background influence on the organization, while climate is the foreground. As a result, safety climate changes more quickly and more readily than safety culture. In the aftermath of a significant accident, it is the climate of an organization, rather than the culture, that will undergo immediate modification." /56/, p. 133.

For the preparation of this section of the discussion document the following sources were analysed:

- Official documents by the OECD, IAEA, Responsible Care, ILK, and HSE
- Scientific literature from the field of psychology, human factors, organization studies

3.2 Official documents

Documents taken into account were OECD Guiding Principles for Chemical Accident Prevention, Preparedness and response /5/, OECD Guidance on Safety Performance Indicators /43/, several publications of the IAEA /45, 46, 47, 48/ as well as the Responsible Care Fundamental Features /49/, a report from HSE /50, 51/ and a statement from a German consulting commission in the nuclear field /52/.

3.2.1 General principles by the OECD

The **OECD** formulates in its Guiding Principles for Chemical Accident Prevention, Preparedness and Response /5/ general principles for safety culture addressing implementation and enhancement of safety culture:

- Establishment and promotion of corporate safety culture, reflected in a corporate Safety Policy.
  - Effective safety culture as an essential element of safety management
  - Values, attitudes and behaviour of senior management and the communication of these throughout the organisation determine the safety culture.
  - Additional a bottom-up commitment through the active application of safety policies by all employees is necessary
  - An essential element of safety culture is the belief that all accidents are preventable.
  - Comprehensive rules concerning the roles, rights and obligations of all those concerned with the assurance and maintenance of safety are necessary.
  - Safety considerations should be incorporated into: planning, design, construction and commissioning of installations; operating policies and procedures, including organisation and personnel arrangements; maintenance; temporary shutdowns; monitoring and assessment of safety; and decommissioning, closure and demolition of hazardous installations.

- Clearly-stated and visible commitment to safety in an enterprise, directed at having all employees act appropriately with regard to safety, i.e.:
  - clear and visible management interest in safety performance through personal involvement
  - good communication on safety issues among and between management and other employees
  - positive feedback concerning actions taken to increase safety
  - quick response to remedy identified faults
  - financial and career incentives for good safety performance
  - participation of employees at all levels in developing and reviewing safety management procedures
  - timely investigations of all accidents and relevant near-misses, and rapid dissemination of the findings of the investigations
- Initiative and alertness in the interest of safety should be encouraged:
  - Guard against complacency or structural/procedural shortcomings
  - "Error tolerance"; no focus on assessing blame or punishing errors, atmosphere of co-operation and openness in which employees feel comfortable about discussing errors and near-misses in order to improve learning, but nevertheless appropriate responsibility and accountability is required
  - Employees and their representatives should be provided with opportunities to participate in the development and review of procedures
- Management should take all appropriate actions to ensure that all employees are aware of their roles and responsibilities with respect to safety, and have the necessary skills, training, education, support and resources. Management should ensure that all safety procedures are disseminated, well-known and understood by all employees.
- Management and other employees should not become complacent; continuous efforts are needed to maintain safety.
- Enhancement of safety culture by management through an open attitude towards the public with respect to safety issues.

According to the safety policy the following principles are stated:

- A clear and meaningful written statement of Safety Policy agreed, promulgated and applied throughout the enterprise, reflecting the corporate safety culture, containing the overall aims and principles with respect to chemical safety
  - At the top of a hierarchy of documentation related to chemical safety at an enterprise
  - Addressing accident prevention, preparedness and response, including the elements of the safety management system
  - Protecting the safety and health of all persons involved in, or who may be affected by, the production, process, handling, use, storage, disposal or elimination of hazardous substances, as well as to safeguard the environment and property.
  - Reviewed regularly and amended, as appropriate, in light of experience gained and any relevant changes in technologies, laws and regulations.
- Consultancy with and involving of employees at all levels for the safety policy

- Independence of employees responsible for the development of corporate safety policies from production management with direct access to top management.
- Widely communication of the safety policy, the intent should be understood and appreciated by all employees
- Management and other employees should co-operate to comply with the enterprise's Safety Policy and meet its safety goals.
  - Complementary roles of management and labour
  - Employees at all levels should be motivated and educated/trained to recognise safety as a top priority and its continuing improvement
  - Labour and their representatives should co-operate with management in promoting chemical safety and should be provided with effective means to do so.
- The Safety Policy should be made accessible to the public.
- Safety programmes for all sites conforming to the enterprise's safety policy and addressing safety concerns and requirements specific to that site.
  - Responsibility for day-to-day management of safety in the hands of line management at individual installations
  - Line management should respond to proposals and suggestions of labour related to safety matters
  - Senior management should provide the necessary support to line management for safety-related decisions and actions
- Development and implementation of a safety policy should be co-ordinated and integrated with the enterprise's activities relating to other aspects of occupational safety, health and environmental protection
  - Efforts towards the integrated management of safety, health and environment (SHE) throughout the regular business operations of an enterprise
  - Safety management as an integral part of total quality management (TQM)
  - The integration of management systems for environmental, health and safety issues, and the development of enterprise-wide procedures applicable to all sites, lead to improvements in safety

In the Guidance on Safety Performance Indicators /43/, outcome indicators for the safety policy, safety goals and objectives and safety leadership were formulated:

- "Extent to which the Safety Policy has been received and understood by: employees, other persons working at the enterprise (contractors, etc.); relevant external stakeholders (suppliers, customers, potentially affected public, etc" /43/, p.30.
- "Extent to which safety goals and objectives have been achieved.
- Extent to which safety goals and objectives are reviewed and updated in relation to the established procedures." /43/, p.32.
- "Extent employees follow established procedures related to safety.
- Extent employees consider management a trusted source of information on: chemical risk at the facility; and safety related information.
- Extent management is involved in safety activities, e.g.: management visibility in daily operations …; number of meetings held periodically … with safety as a substantial item on the agenda.

- Extent suggestions and complaints from employees result in improvement in safety.
- Amount of money or other resource spent per year for safety; relative to other expenditures. …
- Correlation between amount spent on safety and the level of risk at the installation (as measured by, for example, a risk assessment).” /43/, p.34.

3.2.2 Definitions and key elements by the IAEA

Coined in the aftermath of Chernobyl as an explanatory concept for the accident by the IAEA, safety culture has now caught the imagination of virtually all hazard industries: chemical process industries, civil and military aviation or space research, railway systems, petrochemical and pharmaceutical industries, medicine. Thus, the majority of definitions, concepts and instruments still are from the nuclear filed.

In 1991 the **INSAG** /45/ defined safety culture as follows: “Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.” /45/, p.1.

In 1998 the **IAEA** /46/ continued and widened its definition to behaviour: “Safety culture is also an amalgamation of values, standards, morals and standards of acceptable behaviour. These are aimed at maintaining a self-disciplined approach to the enhancement of safety beyond legislative and regulatory requirements. Therefore, safety culture has to be inherent in the thoughts and actions of all the individuals at every level in an organization. The leadership provided by top management is crucial.” /46/, p. 3.

According to INSAG /46/ the major components of safety culture are commitments on different levels:

1. Policy level commitment:
- Statement of safety policy
- Management structures
- Resources
- Self-regulation

2. Managers’ commitment
- Definition of responsibilities
- Definition and control of safety practices
- Qualifications and training
- Rewards and sanctions
- Audit, review and comparison

3. Individuals’ commitment
- Questioning attitude
- Rigorous and prudent approach
- Communication

To provide practical and pragmatic guidelines on the development of safety culture, key issues in safety culture were defined by INSAG (/47/, p. 5ff). For the following key issues questions were derived to provide some simple diagnostic tool: Commitment to safety and to the strengthening of safety culture, use of procedures, conservative decision making, a reporting culture, challenging unsafe acts and conditions, the learning organization and underpinning issues like communication, clear priorities and organization (for the full text, see Annex II)

Safety culture is furthermore seen as a process with different levels. The efforts made to enhance safety culture can result in improved organization, analyses, anticipation and work processes. A strong safety culture can lead to more effective work and a sense of accountability among managers and employees. In promoting an improved safety culture, overall different approaches were taken: an approach emphasizing the use of behavioral sciences or the quality management system approach to enhancing safety performance.

Many features of a strong safety culture have long been recognized as 'good practices' in numerous areas of safety activities in high hazard industries. Recently there has been increased emphasis on a systematic approach to the development of an improved safety culture as well as on the contribution of behavioral sciences to developing good safety practices. Change in culture is both a 'top-down' and a 'bottom-up' approach, but consistent and visible leadership from the top is essential. "Technical specialists, human factors specialists, operating personnel and management must work together to develop a common understanding across their various functions. This is in itself a learning process and, as such, a characteristic of a good safety culture. Continuous learning and improvement processes play a central role in developing and maintaining a good safety culture." /47/, p. 4f.

There are differences in the understanding of organizations according to the concept of safety culture and to the actions necessary to influence it in a positive way. This diversity may reflect different levels of awareness of the safety impact of human behavior and attitudes even in highly technical organizations.

3.2.3 Principles by Responsible Care

The **Responsible Care Fundamental Features** /49/ state as follows:

- Formal commitment by each company to a set of guiding principles, signed by the Chief Executive Officer
- Series of codes, guidance notes and checklists to help companies fulfill their commitment
- Development of indicators against which improvements in performance can be measured
- Open communication on health, safety and environmental matters with interested parties, both inside and outside the industry
- Opportunities for companies to share views and exchange experiences on implementing Responsible Care
- Consideration of how best to encourage all member companies to commit themselves to, and participate in, Responsible Care
- Procedures for verifying that member companies have implemented the measurable or practical elements of Responsible Care

3.2.4 Elements of safety culture by the ILK (Internationale Länderkommission Kerntechnik)

A German consulting commission **ILK (Internationale Länderkommission Kerntechnik)** /52/ in the nuclear field defines the elements of safety culture in its statement on the regulator's management of the licensee self-assessment of safety culture, which exceed the number of elements stated before:

- Top management commitment to safety
- Visible leadership
- High priority to safety
- Systematic approach to safety
- Strategic business importance of safety
- Absence of safety versus production conflict
- Relationship to regulators and other external organizations
- Proactive and long term perspective
- Management of change
- Quality of documentation and procedures
- Compliance with regulations and procedures
- Sufficient and competent staff
- Proper resource allocation
- Knowledge in work science, including health and safety and man-technology-organization (MTO)
- Clear roles and responsibilities
- Clearly organized team work
- Openness and communication
- Motivation and job satisfaction
- Involvement of all employees
- Good working conditions (time, work load, stress)
- Housekeeping
- Measurement of safety performance
- Organizational Learning

In the statement also some examples for safety culture indicators are written down:
"Accountability for safety is clear

- Managers have specific safety goals to achieve
- Rewards reflect achievement
- Employees involved in safety improvements
- Team appraisals include safety achievement

Safety is learning driven

- Program exists for feeding back lessons from operating experience
- Familiarity with learning processes
- Process exists for dealing with repeated events
- Process to prevent mistakes through strengthening defense in depth
- Mistakes may be a learning opportunity

High priority to safety

- Safety resources adequate for workloads
- Safety concerns can be raised openly and safety behaviors are actively supported

- Teamwork among departments is encouraged

Clear leadership for safety

- Top managers dedicate time and efforts to improve safety
- Training in safety culture is available and used by managers
- Management/workforce interaction frequency
- Level of personal accountability for safety

Style of management

- Clear standards and expectations
- Managers reinforce expected behaviors" /52/.

The commission suggests to conduct a self-assessment each 2-3 years and after a significant organizational change.

3.2.5 Models on evaluation and classification of safety culture and safety climate

The HSE published in the Offshore Technology Report 1999/063 /90/ a summary guide to safety climate tools. The guide should serve to provide summary information on questionnaire-based tools for measuring the safety climate of organizations and to determine the most useful and necessary scales and items. In the report the following recommendations for the assessment of safety climate are given:

- Preparation is essential before launching into the use of a climate survey tool. Any tool is unlikely to work well - or may even have a negative effect - if senior management put insufficient effort into preparation, do not commit to act on findings (whatever they are) and fail to involve the entire workforce throughout the process.
- Recipients of the questionnaire need to know why the survey is being done and how the results will be used.
- It is essential that there is a rapid, but realistic, post-survey implementation plan. Some visible results need to be achieved as soon as possible after completion of the survey.
- The results of the survey need to be fed back to the surveyed group as rapidly as possible.
- Issues or areas of weakness identified by the survey need to be discussed with the respondents to clarify the details of their concerns.
- After clarification, a plan of action should be developed to address the most significant weaknesses. The plan may include behaviour modification programmes.
- During implementation of the action plan, some form of monitoring needs to be in place to check progress. The results of the monitoring programme should be fed back to the employees concerned.
- Repeat climate surveys should not be undertaken before an action plan to address weaknesses from the first survey has been implemented. (/90/, p. 11f.)

According to items and scales, the following core safety climate item sets were identified:

- Training and competence
- Job security and job satisfaction
- Pressure for production

- Communications
- Perceptions of personal involvement in health and safety
- Accidents/ incidents/ near misses
- Perception of organisational/management commitment to health & safety – general and specific
- Merits of the health and safety procedures/ instructions/ rules
- Rule breaking
- Workforce view on state of safety/ culture
- Assessment of safety levels

Furthermore, there are more sets of items, which could be included in an assessment:

- Planning for emergencies
- Maintenance
- Task allocation and human factor design
- Work pressures
- Work environment
- Individual competence, capacities, health and skills
- Procedures
- Safety priorities
- Management/structural (including decision making and team working)

According to the IAEA (1998) three stages of development of safety culture seem to emerge. The characteristics of each stage provide organizations with a basis for self-diagnosis.

Stage I: Safety based solely on rules and regulations

Safety is seen as an external requirement and not as an aspect of conduct that will help the organization to succeed. The external requirements are those of national governments, regional authorities, or regulatory bodies. “There is little awareness of behavioral and attitudinal aspects of safety performance, and no willingness to consider such issues. Safety is seen very much as a technical issue; mere compliance with rules and regulations is considered adequate. For an organization which relies predominantly on rules, the following characteristics may be observed:

- Problems are not anticipated; the organization reacts to each one as it occurs.
- Communication between departments and functions is poor.
- Departments and functions behave as semi-autonomous units and there is little collaboration and shared decision making among them.
- The decisions taken by departments and functions concentrate upon little more than the need to comply with rules.
- People who make mistakes are simply blamed for their failure to comply with the rules.
- Conflicts are not resolved; departments and functions compete with one another.
- The role of management is seen as endorsing the rules, pushing employees and expecting results.

- There is not much listening or learning inside or outside the organization, which adopts a defensive posture when criticized.
- Safety is viewed as a required nuisance.
- Regulators, customers, suppliers and contractors are treated cautiously or in an adversarial manner.
- Short term profits are seen as all-important.
- People are viewed as 'system components'— they are defined and valued solely in terms of what they do.
- There is an adversarial relationship between management and employees.
- There is little or no awareness of work or business processes.
- People are rewarded for obedience and results, regardless of long term consequences." /47/, p. 5f.

Stage II – Good safety performance becomes an organizational goal

The management perceives safety performance as important even in the absence of regulatory pressure. Although there is growing awareness of behavioral issues, this aspect is largely missing from safety management methods, which focus on technical and procedural solutions. Safety performance is dealt with in terms of targets or goals. The organization begins to question why safety performance reaches a plateau and is willing to learn from other organizations. The following characterizes the second stage:

- "The organization concentrates primarily on day to day matters. There is little in the way of strategy.
- Management encourages cross-departmental and cross-functional teams and communication.
- Senior managers function as a team and begin to co-ordinate departmental and functional decisions.
- Decisions are often centered on cost and function.
- Management's response to mistakes is to put more controls in place via procedures and retraining. There is a little less blaming.
- Conflict is disturbing and is discouraged in the name of teamwork.
- The role of management is seen as applying management techniques, such as management by objectives.
- The organization is somewhat open about learning from other companies, especially techniques and best practices.
- Safety, cost and productivity are seen as detracting from one another. Safety is thought to imply higher cost and reduced production.
- The organization's relationship with regulators, customers, suppliers and contractors is distant rather than close; there is a cautious approach where trust has to be earned.
- It is important to meet or exceed short term profit goals. People are rewarded for exceeding goals regardless of the long term results or consequences.
- The relationship between employees and management is adversarial, with little trust or respect demonstrated.
- There is growing awareness of the impact of cultural issues in the workplace. It is not understood why added controls do not yield the expected results in safety performance." /47/, p.6.

Stage III – Safety performance can always be improved

Continuous improvement is seen as important and applied to safety performance. There is a strong emphasis on soft skills as communications, training, and management style. People understand the impact of behavioral issues on safety. The level of awareness of behavioral and attitudinal issues is high, and measures are being taken to improve behavior. The stage is characterized by:

- "The organization begins to act strategically with a focus on the longer term as well as awareness of the present. It anticipates problems and deals with their causes before they happen.
- People recognize and state the need for collaboration between departments and functions. They receive management support, recognition and the resources they need for collaborative work.
- People are aware of work or business processes in the organization and help managers to manage them.
- Decisions are made in the full knowledge of their safety impact on work or business processes as well as on departments and functions.
- There is no goal conflict between safety and production performance, so that safety is not jeopardized in pursuit of production targets.
- Almost all mistakes are viewed in terms of work process variability. It is more important to understand what has happened than to find someone to blame. This understanding is used to modify the work process.
- The existence of conflict is recognized and dealt with by trying to find mutually beneficial solutions.
- Management's role is seen as coaching people to improve business performance.
- Learning from others both inside and outside the organization is valued. Time is made available and devoted to adapting such knowledge to improve business performance.
- Safety and production are seen as interdependent.
- Collaborative relationships are developed between the organization and regulators, suppliers, customers and contractors.
- Short term performance is measured and analyzed so that changes can be made which improve long term performance.
- People are respected and valued for their contribution.
- The relationship between management and employees is respectful and supportive.
- People are aware of the impact of cultural issues, and these are factors considered in key decisions.
- The organization rewards not only those who 'produce' but also those who support the work of others. People are also rewarded for improving processes as well as results." /47/, p. 7f.

For the **U.K. *HSE Offshore Technology Report 2000/049*** the Keil Centre developed a safety culture maturity model /50/, which has five developmental stages, i.e. two more as the model of the IAEA /46/. The elements differ mainly in the way that the elements of the safety culture maturity model take more the employees' perspective into account. The described elements are:

- Management commitment and visibility
- Communication
- Productivity versus safety
- Learning organization
- Safety resources
- Participation
- Shared perceptions about safety
- Trust
- Industrial relations and job satisfaction
- Training

Following assumptions are the basis of the model: “Cultural or behavioural approaches to safety improvement are their most effective when the technical and system aspects of safety are performing adequately and the majority of accidents appear due to behavioural or cultural factors.” The safety culture maturity model is therefore only of relevance to organisations that fulfil a number of specific criteria. These include:

- An adequate Safety Management System
- Technical failures are not causing the majority of accidents
- The company is compliant with health and safety law
- Safety is not driven by the avoidance of prosecution but by the desire to prevent accidents

The five stages of the model are described below and shown in figure1:

Level One: Emerging

Safety is defined in terms of technical and procedural solutions and compliance with regulations. The safety department is perceived to have primary responsibility for safety. Many accidents are seen as unavoidable and as part of the job. Most frontline staff are uninterested in safety.

Level Two: Managing

The organization's accident rate is average for its industrial sector but they tend to have more serious accidents than average. Management time and effort is put into accident prevention. Safety is defined in terms of adherence to rules and procedures and engineering controls. Accidents are seen as preventable. Managers perceive that the majority of accidents are solely caused by the unsafe behavior of front-line staff. Safety performance is measured in terms of lagging indicators such as LTI and safety incentives are based on reduced LTI rates.

Level Three: Involving

Accident rates are relatively low, but they have reached a plateau. The organization is convinced that the involvement of the frontline employee in health and safety is critical, if future improvements are going to be achieved. Managers recognize that a wide range of factors cause accidents and the root causes often originate from management decisions. A significant proportion of frontline employees are willing to work with management to improve health and safety. The majority of staff accepts

personal responsibility for their own health and safety. Safety performance is actively monitored and the data is used effectively.

Level Four: Cooperating

The majority of staff in the organization is convinced that health and safety is important from both a moral and economic point of view. Managers and frontline staff recognize that a wide range of factors cause accidents and the root causes are likely to come back to management decisions. Frontline staff accept personal responsibility for their own and others health and safety. The organization puts significant effort into proactive measures to prevent accidents. Safety performance is actively monitored using all data available. Non-work accidents are also monitored and a healthy lifestyle is promoted.

Level Five Continuous improvement

The prevention of all injuries or harm to employees (both at work and at home) is a core company value. The organization has had a sustained period (years) without a recordable accident or high potential incident, but there is no feeling of complacency. They live with the paranoia that their next accident is just around the corner. The organization uses a range of indicators to monitor performance but it is not performance-driven, as it has confidence in its safety processes. The organization is constantly striving to be better and find better ways of improving hazard control mechanisms. All employees share the belief that health and safety is a critical aspect of their job and accept that the prevention of non-work injuries is important. The company invests considerable effort in promoting health and safety at home. /50/.

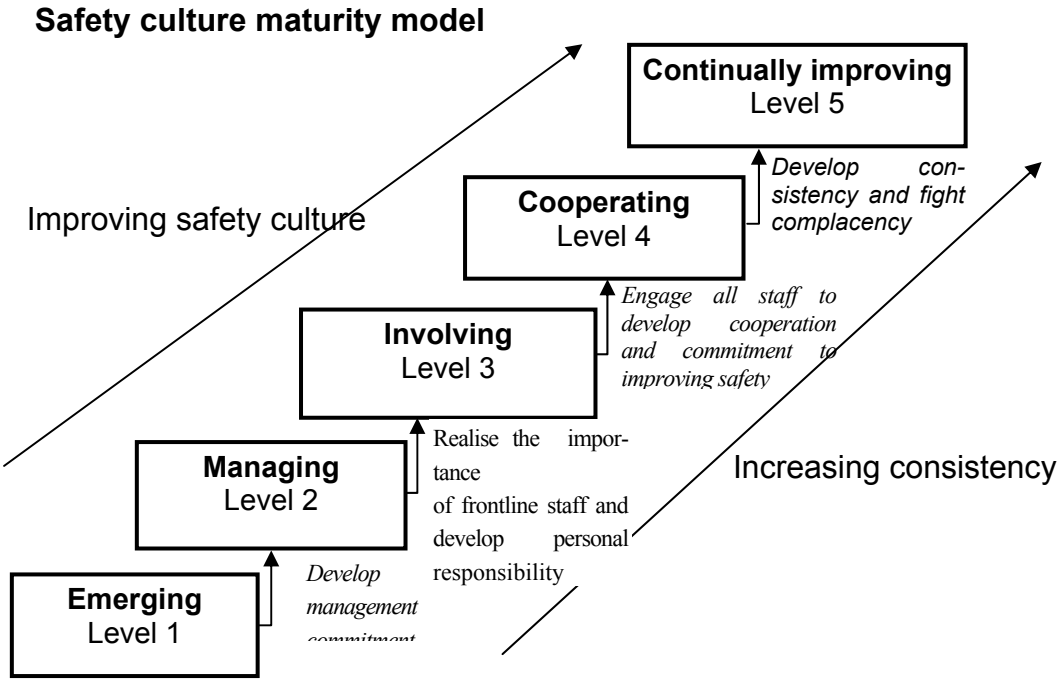


Figure 1: Safety Culture maturity model. *HSE Offshore Technology Report 2000/049.*

In: “A review of safety culture and safety climate literature for the development of the safety culture inspection toolkit” /51/ key indicators for the rail industry (HMRI) were recommended: leadership, two-way communication, employee involvement, learning culture and attitude towards blame

5

3.3 Scientific literature from the field of psychology, human factors, organization studies

There is a huge body on literature on safety culture, safety climate and its assessment. The following selection is based on either process industry specific references or on literature which exceed the official documents.

Because safety-management is not enough Kadri and Jones /53/ propose an approach that will help organizations to self-assess the state of the process safety culture in their organizations. Safety culture improvement can be reached by creation of awareness about safety culture themes, by adaptation of process safety culture themes to company experience, by use of suggested indicators to identify specific areas of improvement, by development of a strategic improvement plan to strengthen and sustain the safety culture process. There assessment is mainly vice versa, i.e. they propose indicators that show a decrease in safety culture:

"Indicators that you are not maintaining a sense of vulnerability

- You assume your safety systems are good enough
- You treat critical alarms as operating indicators
- You allow backlogs in preventative maintenance of critical equipment
- Lessons from related industry disasters are not routinely discussed at all levels in the organization
- Actions are not taken where similar deficiencies have been identified

Indicators that you are allowing normalization of deviance

- You allow systems to operate outside design safe operating limits without detailed risk assessment
- You allow deviations from established procedures without management of change (MOC) review and approval
- Wilful, conscious violation of an established procedure is tolerated without evaluating the consequences for the persons involved
- Staff cannot be counted on to strictly follow procedures when supervision is not around to monitor compliance

Indicators that appropriate and timely hazard/risk assessment are not being done

- Availability of experienced resources for risk assessment is limited
- The recommendations from risk assessment are not meaningful
- The recommendations from risk assessment are not implemented in a timely manner
- The actions taken differ from the intent of the original recommendations
- Bases for rejecting risk assessment recommendations are mostly subjective judgment or based on previous experience and observation

Indicators that safety role is not independent and unassailable

- People monitoring safety-related decisions are not sufficient technically qualified and independent
- Key process safety management positions have been downgraded over time
- Recommendations for safety improvements are resisted on the grounds of costs or schedule impact
- No system in place to ensure an independent review of major safety-related problems

- Audits conducted by people not technically competent and are regarded as negative or punitive

Indicators that open and frank communication at all levels is not happening

- The bearer of “bad news” is viewed as “not a team player”
- Safety related questioning “rewarded” by requiring the suggestor proves that he/she is correct
- Critical safety-related news that circumvents official channels is not welcomed
- Communication become altered, with the message softened, as they move up through the management chain
- Employees cannot speak freely to anyone else about their honest safety concerns, without fear of career reprisals” (p. 19)

Wilpert et al. /54/ introduce key elements for safety culture, which show clearly an organizational psychology perspective:

- Commitment on all levels of the organisation from the whole staff
- Questioning attitude
- Systemic thinking
- Role model of managers and supervisors
- Professional identity
- Treatment of errors (failure culture)
- Implicite norms

The hitherto most encompassing description and discussion of different models and analytic instruments to study safety culture has been collated by Wilpert et al., /55/ which covers altogether 20 different approaches. They differ in terms of depth of analysis, psychometric quality criteria such as reliability, objectivity and validity as well as in terms of economy of use and manageability. However, a basic difference may be highlighted with reference to a difference in general conduct of the analysis, namely whether it is conducted by external experts from outside the studied organization or whether the analysis is pursued as a self-assessment by staff members of the organization itself.

External investigations usually utilize competent outsiders who conduct a safety audit, use questionnaires and interview guidelines, study the safety related features through observation and document analysis. The advantage of outsider investigations lies mainly in their characteristic of introducing perspectives into the analysis which are guided by experience from other contexts than those of the focal organization. But such analyses are likely to remain in the realm of attitudes, climate and directly observable phenomena. Deeper layers of the organizational culture will be less approachable.

Self-assessments, in contrast, are conducted by internal qualified staff members who are thoroughly familiar with their own organization. Self-assessments can easily and economically be carried out and have an immediate educational effect in the sense that once problems of safety culture are identified they may be discussed and intervention solutions can be developed and implemented. On the other hand, a disadvantage of self-assessment may be the danger of analysts remaining focused on as-

pects in the organization which have no taboo, are acceptable to management and staff, and are easily optimized. In consequence, self-assessment and external assessment are techniques which are not mutually exclusive but complementary. The research of the Berlin based Research Center System Safety has so far mainly focused on self-assessments in developing a screening technique for safety culture which will be presented below.

Functional aspects are considered all those features of high hazard organizations which need to be present in the organization in order to make it viable such as leadership, group norms, control, rules, procedures. Structural parts are elements of the organizational build-up such as organizational level, including the most important links to external institutions and organizations such as regulators or other reference organizations.

The authors distinguished five relevant system levels: *technology* (e.g. hardware); *individual* (e.g. personal behavior, cognitive competence); *group level* (e.g. group dynamics); *organization* (e.g. leadership/control); *environment* (e.g. media/public).

Based on prototypical organizational features of nuclear power plants the following structural elements were identified: regulation, utility, plant management, managers, plant personnel categories (operational staff, maintenance, systems technology, supervision, accounting, logistics, general staff), external staff.

The allocation of functional factors resulted in the following clustering:

individual level: cognitive competence, rule compliance, qualification, risk perception, attitudes/motivation, physiological influences, commitment to safety, behavior;

group level: communication, group dynamics, leadership/control, social norms;

organizational level*:* basic assumption of the organization, goals and visions, planning, resources, process management and process evaluation, organizational learning, training, information and documentation, incentive systems;

technology (hardware, software, ergonomics).

These structural and functional dimensions provided the basis for the development of a self-assessment screening methodology of safety culture and suggested conceptualizations for the introduction and maintenance of a sustained safety culture in nuclear plants /55/.

Another new dimension or element was introduced by Olive et al. /56/, i.e. resilience and flexibility: “A strong safety culture is characterized by several traits: a definite *commitment* to the improvement of safety behaviors and attitudes at all organizational levels; an organizational structure and atmosphere that promotes open and clear *communication* in which people feel free from intimidation or retribution in raising issues; a propensity for *resilience and flexibility* to adapt effectively and safely to new situations; a prevailing attitude of constant *vigilance.”* /56/, p. 139.

Lardner (2003, /91/) stated, that “since safety culture is associated with occupational accidents then organizations that have a lower accident rate than similar organiza-

tions are also likely to have a positive safety culture" (p. 13). The following features characterize low accident organizations:

- Frequent, less formal communication about safety at all levels
- Good organizational learning
- Strong focus on safety by all
- Strongly committed senior management
- Democratic and co-operative leadership style
- High quality training, including safety training
- Good working conditions and housekeeping
- High job satisfaction
- Good industrial relations
- Selection and retention of employees who work steadily and safely

According Lardner /91/ there are some features associated with a positive safety culture which originate from several safety climate surveys:

1. **Hardware:** good plant design, working conditions and housekeeping; perception of low risk due to confidence in engineered systems
2. **Management systems:** confidence in safety rules, procedures and measures; satisfaction with training; safety prioritised over profits and production; good organizational learning; good job communication
3. **People:** high level of employee participation in safety; trust in workforce to manage risk; high level of management safety concern, involvement and commitment
4. **Behaviour:** acceptance of personal responsibilities for safety; frequent informal safety communication; willingness to speak up about safety; a cautious approach to risk
5. **Organizational climate factors:** low levels of job stress; high levels of job satisfaction

The U.S. Chemical Safety and Hazard Investigation Board summarizes in its report /92/ on the refinery explosion and fire in Texas City, that "safety management systems are necessary for prevention, but that much more is needed to prevent major accidents. Effective organizational practices, such as encouraging that incidents be reported and allocating adequate resources for safe operations, are required to make safety systems work successfully" (/92/, p. 139). One of the identified cultural causes were, that BP Group and Texas city managers were working to make safety changes prior to the accident, "but the focus was largely on personal rather than process safety. As personal injury statistic improved, the BP group executives stated that they thought safety performance was headed in the right direction" (/92, p. 139f.). But personal injury rates are not a measure of process safety.

3.4 Conclusion

There is a huge body on documents on safety culture mainly from the nuclear field. In these documents a common agreement can be found on some points like "what is safety culture?", but also open questions and blind spots.

Although there are some differences, the key elements of safety culture are very similar like commitment, learning organization, communication. Still missing are agreed key elements for the chemical industry.

There are many different instruments for assessment, but it is still unclear which levels have to be assessed, norms, values or even underlying beliefs and how to treat observable behaviour and artefacts. The cited indicators are not simple to assess or to measure and there is no validated instrument for the chemical industry.

Furthermore there is no common understanding of whom to integrate only the operators, managers, top-management or even groups outside the organization. From the literature it can be derived that assessments should be repeated regularly and after significant changes, but it is not clear yet, whether these assessments should be self-assessments by the industry or assessments by regulators.

Thus, the workshop should be a platform to define basic requirements of methodologies/ instruments, e.g. requirements related to the dimensions/key elements to be assessed as well as structures and/or groups to be included.

The key elements of safety culture according to OECD and the other cited literature should be:

- Establishment and promotion of corporate safety culture, reflected in a corporate Safety Policy.
- Clearly-stated and visible commitment to safety in an enterprise
- Initiative and alertness in the interest of safety should be encouraged
- Management should take all appropriate actions to ensure that all employees are aware of their roles and responsibilities with respect to safety, and have the necessary skills, training, education, support and resources. Management should ensure that all safety procedures are disseminated, well-known and understood by all employees.
- Management and other employees should not become complacent; continuous efforts are needed to maintain safety.
- Enhancement of safety culture by management through an open attitude towards the public with respect to safety issues.
- A clear and meaningful written statement of Safety Policy agreed, promulgated and applied throughout the enterprise, reflecting the corporate safety culture, containing the overall aims and principles with respect to chemical safety
- Consultancy with and involving of employees at all levels for the safety policy
- Independence of employees responsible for the development of corporate safety policies from production management with direct access to top management.
- Widely communication of the safety policy, the intent should be understood and appreciated by all employees
- Management and other employees should co-operate to comply with the enterprise's Safety Policy and meet its safety goals.
- The Safety Policy should be made accessible to the public.
- Safety programmes for all sites conforming to the enterprise's safety policy and addressing safety concerns and requirements specific to that site.

- Development and implementation of a safety policy should be co-ordinated and integrated with the enterprise's activities relating to other aspects of occupational safety, health and environmental protection
- Good organizational learning
- Questioning attitude
- Systemic thinking
- Role model of managers and supervisors, leadership
- Professional identity
- Treatment of errors (failure culture)
- Implicite norms
- Motivation and job satisfaction

In the evaluation of safety culture the above key elements should be assessed. As a first approach the following assessment levels /55/ with the corresponding factors could serve:

1. **Individual level**
   - cognitive competence
   - rule compliance
   - qualification
   - risk perception
   - attitudes/motivation
   - physiological influences
   - commitment to safety
   - behavior
2. **Group level**
   - communication
   - group dynamics
   - leadership/control
   - social norms
3. **Organizational level:**
   - basic assumption of the organization
   - goals and visions
   - planning
   - resources
   - process management and process evaluation
   - organizational learning
   - training
   - information and documentation
   - incentive systems
4. **Technology**
   - hardware
   - software
   - ergonomics

Groups to be included in the assessment of safety culture should be:

1. Top level management
2. Management
3. Operators
4. Maintenance personnel – crafts technicians
5. Contractors
6. External stakeholders
7. (Regulatory bodies)

Safety climate as a first approach to safety culture could be assessed by questionnaire with the above mentioned content, but for safety culture assessment a more holistic approach is needed, i.e. questionnaires should be completed by observations, document analysis and interviews or group-feedback-analyses.

3.5 Questions

1. What problems/issues are related to the different instruments/methodologies?
2. What kind of regulatory and legal restrictions to safety culture are known and how could they be minimized?
3. Are there coherences between the three level model and the five level model?
4. What alternatives exist in regard to the recommended indicators?
5. Are the key elements for the evaluation of the safety culture complete and well defined?
6. Should process safety be aggregated with other aspects in the evaluation of Safety culture?
7. Have regular surveys on safety climate to be regarded as best practice?
8. Should there be some kind of standardisation of these surveys to allow benchmarking of enterprises?
9. Should more guidance on the improvement of safety culture be provided?
10. Should the results of survey on safety culture be presented in the Sustainability Reports of enterprises?

4 Thematic session 3: Appropriate Human Factors competence

Key objectives to be covered in the session

- Identify the different types of responsibility in organisations requiring different competences in safety related human factors issues;
- Define the competences required with respect to these different responsibilities;
- Discuss the roles applicable to the industry
- Make recommendations to identify the training needs and develop training programmes;

4.1 Introduction

The various management and staff levels in organisations (industries, authorities, expert organisations/consultants) have different responsibilities which require specific competences in human factors issues. The personnel involved in the safety tasks is usually technically competent and well trained to the safety issues, but has generally no specific knowledge of the social safety dimension and its human factors competences are often less developed. The workshop will make recommendations on appropriate human factors competences taking into account the types of responsibilities and the different management and staff levels. Such recommendations may help set up adequate training programmes on human factors in the chemical industry aiming at reducing the number of accidents and mitigating their consequences.

Because this is a relatively new field only a few sources from the nuclear industry and aviation could be taken into account.

4.2 Types of responsibilities

The IAEA /48/ identified the following relevant four actors with related areas of competency:

Table 2: Relevant actors and areas of competency for the framework for education and training in nuclear safety

Relevant actors	**Areas of competency**
Regulatory body staff	Regulatory control
Technical support organizations	Siting & Design of NPPs
Operators and utility staff	Operation of NPPs
Research organizations and educators	Research reactor design, operation & utilization

The EU regulates in their Commission Regulation (EC) No 2042/2003 of 20 November 2003 /57/ on "the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organizations and personnel involved in these tasks" the training needs for maintenance personnel.

Line Maintenance Certifying Mechanic (Cat. A)
Category A authorisation entitles the holder to issue Certificates of Release to Service after simple scheduled maintenance work and after repairing simple defects within the scope of the authorisation. The issuing of Certificates of Release to Service is restricted to work which the holder of the authorisation has personally carried out.

Maintenance Certifying Technician/Mechanical (Cat. B1)
Category B1 authorisation entitles the holder to issue Certificates of Release to Service after maintenance work, including work on the airframe, the engines and mechanical and electrical systems. The authorisation also includes the replacement of quickly replaceable avionic units for which a simple check – usually on board – is required to verify their integrity for further operation. Category B1 authorisation automatically entitles the holder to issue Category A Certificates of Release to Service.

Maintenance Certifying Technician/Avionic (Cat. B2)
Category B2 authorisation entitles the holder to issue Certificates of Release to Service after maintenance work on the avionic and electrical systems. Category B2 certifying staff can qualify for authorisation to issue Category A Certificates of Release to Service.

Base Maintenance Certifying Engineer (Cat. C)
Category C authorisation entitles the holder to issue Certificates of Release to service after maintenance work. The authorisation applies to aircraft in their entirety, including all systems.

The classifications from both industries have some relevance for the chemical industry, but are not simply transferable. For the chemical industry the following groups seem to be relevant according to human factors competency:

- Regulatory body staff
- Management
- Safety personnel
- Operators

4.3 Identified human factors competency

In their proposed framework for education and training in nuclear safety the IAEA identified four categories of competence and related training contents:

Regulatory control of NPPs

- Authorization process
- Review and assessment
- Inspection and enforcement
- Development of regulation and guides

- Regulatory effectiveness

Safety Assessment of NPPs

- Accident analysis methods
- Probabilistic safety assessment
- Accident management
- Ageing management
- Safety assessment of modifications

Operational safety of NPPs

- Safety culture and management of safety
- NPP operator regulator interface
- Operational experience and feedback
- Operational practices

Safety of research reactors

- Regulatory aspects and safety documentation
- Safety analysis
- Safety in operation and utilization
- Management of ageing
- Safe shutdown and decommissioning

Concerning the competence of staff members in the aeronautical field, the EU states: "The organisation shall establish and control the competence of personnel involved in any maintenance, management and/or quality audits in accordance with a procedure and to a standard agreed by the competent authority. In addition to the necessary expertise related to the job function, competence must include an understanding of the application of human factors and human performance issues appropriate to that person's function in the organisation. "Human factors" means principles which apply to aeronautical design, certification, training, operations and maintenance and which seek safe interface between the human and other system components by proper consideration of human performance. "Human performance" means human capabilities and limitations which have an impact on the safety and efficiency of aeronautical operations. … The organisation shall establish procedures agreed by the competent authority taking into account human factors and human performance to ensure good maintenance practices and compliance with this Part which shall include a clear work order or contract such that aircraft and components may be released to service in accordance with 145.A.50. " /57/.

It is regulated that basic knowledge for categories A, B1 and B2 are indicated by the allocation of knowledge levels indicators (1, 2 or 3) against each applicable subject. Category C applicants must meet either the category B1 or the category B2 basic knowledge levels. The knowledge level indicators are defined as follows:

Level 1

A familiarisation with the principal elements of the subject.

Objectives: The applicant should be familiar with the basic elements of the subject. The applicant should be able to give a simple description of the whole subject, using common words and examples. The applicant should be able to use typical terms.

Level 2

A general knowledge of the theoretical and practical aspects of the subject. An ability to apply that knowledge.

Objectives: The applicant should be able to understand the theoretical fundamentals of the subject. The applicant should be able to give a general description of the subject using, as appropriate, typical examples. The applicant should be able to use mathematical formulae in conjunction with physical laws describing the subject. The applicant should be able to read and understand sketches, drawings and schematics describing the subject. The applicant should be able to apply his knowledge in a practical manner using detailed procedures.

Level 3

A detailed knowledge of the theoretical and practical aspects of the subject. A capacity to combine and apply the separate elements of knowledge in a logical and comprehensive manner.

Objectives: The applicant should know the theory of the subject and interrelationships with other subjects. The applicant should be able to give a detailed description of the subject using theoretical fundamentals and specific examples. The applicant should understand and be able to use mathematical formulae related to the subject. The applicant should be able to read, understand and prepare sketches, simple drawings and schematics describing the subject. The applicant should be able to apply his knowledge in a practical manner using manufacturer's instructions. The applicant should be able to interpret results from various sources and measurements and apply corrective action where appropriate.

The training shall be conducted in modules; module 9 is on human factors and has the following contents:

1. **General**: Necessity to take human factors into account, incidents caused by human factors / human errors, Murphy's law
2. **Human performance and restrictions**: seeing, listening, information processing, attention and perception, memory
3. **Social psychology**: responsibility of individuals and groups, motivation and de-motivation, group pressure, "cultural" issues, teamwork, management, supervision /control and leadership
4. **Performance shaping factors**: fitness / health, stress: work and home related, time pressure and schedule, work load, fatigue, Shift work, alcohol, medicaments, drug abuse
5. **(Workplace) Environment**: noise and exhaust, illumination, climate and temperature, movement and vibration, work surrounding
6. **Tasks**: physical work, routine tasks, visual tests, complex systems
7. **Communication**: within the team and between teams, work minutes and records, "be in the loop" / situation awareness, actuality, information processing
8. **Human error**: models and theories on errors, error modes during maintenance, consequences of errors (i.e. accidents and incidents), prevention of and treatment / coping with errors
9. **Hazards at the workplace**: perception and prevention of hazards, emergency treatment

4.4 Conclusion

For the chemical industry nearly all topics are relevant. Additionally should be added:

10. Ergonomics: knowledge of man-mchine-interfaces, design
11. Human Resource Management: recruiting and training, dealing with performance issues, motivation
12. Crisis Management: forecasting potential crises and planning how how to deal with them, identifying the real nature of a current crisis, intervening to minimize damage, risk communication

The following qualifications may be recommended:

Table 3: Appropriate Human Factors Competence

	Knowledge level					
Training content	**Regulatory body staff**		**Management**			
	Regulation	**Enforcement**	**Operational management**	**Strategic management**	**Safety personnel**	**Operators**
General	2	2	2	2	3	2
Human performance and restrictions	1	2	2	1	3	2
Human resource management	1	2	2	1	3	1
Ergonomics	1	2	2	1	3	1
Social psychology	2	2	2	2	3	2
Performance shaping factors	1	2	2	1	3	2
Workplace Environment	1	2	2	1	3	2
Tasks	1	2	2	1	3	2
Communication	1	2	2	2	3	2
Human error	1	2	2	1	3	2
Hazards at the workplace	1	2	2	1	3	3
Crisis Management	2	3	3	1	3	2

In the discussion it should become clear whether the above mentioned responsibilities requiring different competences in safety related human factors issues are those which are relevant to the chemical industry. Training needs and training programmes should be addressed as well.

4.5 Questions

1. Are the above mentioned groups of responsibilities those which are relevant?
2. Are the mentioned competencies those which are relevant?
3. Are there missing competencies?
4. Are the knowledge levels sense-making for the above mentioned groups?

5 Thematic session 4: Interfaces between Safety Systems and Operators

Key objectives to be covered in the session

- Discuss how operator tasks in abnormal situations are identified and assessed when designing automatic safety systems: interlock, cut-off, shut-off, instrumented safety systems according to the IEC 61511 /7, 58, 59/ standard;
- Consider how the human skills are taken into consideration in this process;
- Describe how to prevent process alteration by operator activities to prevent automatic shut-offs causing out of design situations causing major accidents although an automatic safety system is installed;
- Make recommendation on interfaces between safety systems and operators;

5.1 Introduction

The design and reliability of safety systems (i.e. interlock-, shut-off-, cut-off-systems, safety instrumented systems and **not** control systems) and their interaction with the operators play a key role in making incidents become (major) accidents. Less attention has been paid to the fact that the interface between man and process is different in "abnormal situations" as compared with normal operation conditions, and affects the overall success. In abnormal situations the successful operation of safety systems has a very high priority and the prevention of major accidents will also depend on the quality of the interface between the safety systems and the operator. This session will discuss the strategies for developing 'efficient' interfaces between safety systems and operators based on the human factors knowledge.

For the preparation of this section of the discussion document the following sources were analysed:

- Regulations and technical standards
- Scientific literature from the field of psychology and human factors

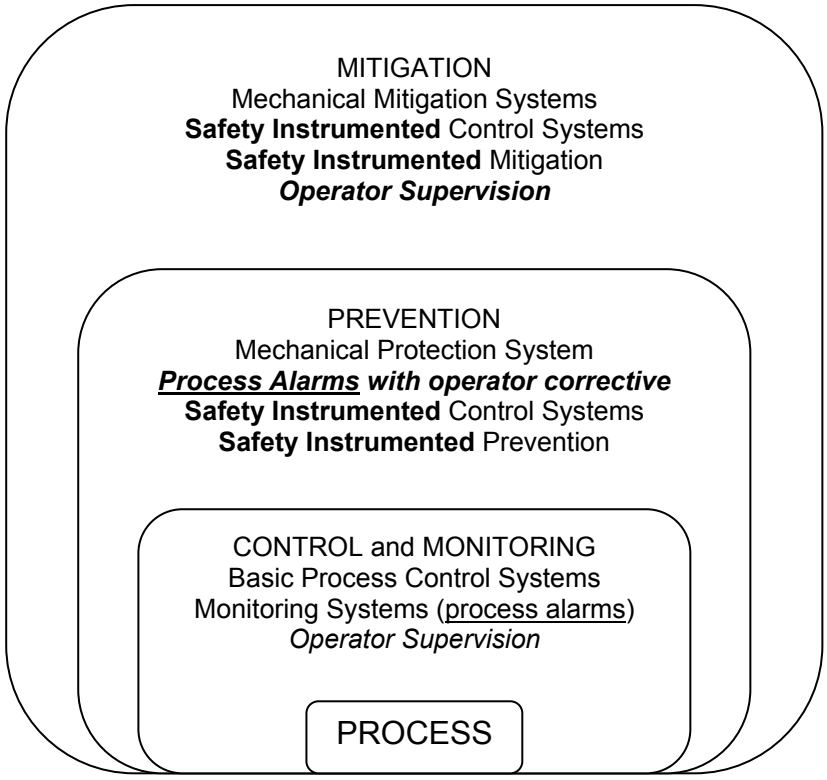
5.2 Regulations and technical standards (IEC 61511, VDI/VDE 2180, NE 31)

The Seveso II directive /60/ is aimed at the prevention of major accidents and at the restriction of accident consequences for people and environment.

Article 9 of the Seveso II /60/ directive, concerning the safety report requires that in this document it is demonstrated that adequate safety and reliability have been incorporated into the design, construction, operation and maintenance of all plant and equipment.

IEC/EN61511/ /7, 58, 59/ transfers the concept of functional safety of the standard /EN61508/ /61/ specifically to the process industry sector. A safety instrumented system (SIS) encompasses all necessary components and subsystems – from sensor to

actuator – for the performance of the safety instrumented function and integrates explicitly operating staff.
According to IEC 61511 the protection layer approach distinguishes three layers with different safety relevant functions of the operators:



From: IEC 61511 9.4 Requirements on the basic process control system as a protection layer

First (inner) level is the control and monitoring system.
The control and monitoring shall ensure the optimal and safe conditions of the process. Any failure of this layer shall not cause a major accident. As the figure shows the operators have two functions in this inner layer:
a) Process control
These means that the operators shall react skill- or rule-based on alarms from control or monitoring systems for the optimisation of the process conditions. Any failure shall not cause a major accident.
b) Supervision
The operator shall rule- or knowledge-based supervise the process i.e. correct the process conditions in abnormal situation with less or no suitable instrumentation.

The second (middle) level is the prevention system.
The figure shows only one operator function but in reality there are the same two functions, because the IEC 61511 considers low and high automated safety systems.
a) The operator is part of the safety function
This is relevant, if the safety systems of a plant are less automated, i.e. there may be only a sensor-transmitter-alarm system and it is the function of the operator to be transmitters and actor.

b) The Safety System is completely automated
This means that all possible major accidents are prevented by complete automated systems including the complete sensor-transmitter-actor chain. As a consequence only the supervision function is left for the operator.
The consequence is that there are (at least) **two types of alarms** with very different relevance for the prevention of major accidents:

1. Alarms to ensure optimal process conditions (Messages according to NAMUR) and safe process conditions
2. Alarms to prevent major accidents (i.e. critical Alarms).

This difference has to be regarded in debates on man-machine-interfaces especially the human centred alarm management.

In the frame of a defined safety-lifecycle-process (SLC) the standard requires a hazard and risk analysis (phase 1), to be able to derive the specification and the design of safety instrumented systems (phase 2…4). Other lifecycle-phases define assembly, validation, putting into operation, operation, maintenance and management of change (phases 5…7) and shut-down (phase 8). According to IEC 61511-1" each phase of the safety life cycle shall be defined in terms of its inputs, outputs and verification activities" p.35. For the phases of the SLC "safety planning shall take place to define the criteria, techniques, measures and procedures to: ensure that the SIS safety requirements are achieved for all relevant modes of the process […]; ensure proper installation and commissioning of the safety instrumented system; ensure the safety integrity of the safety instrumented functions after installation; maintain the safety integrity during operation (for example, proof testing, failure analysis); manage the process hazards during maintenance activities on the safety instrumented system" p.37. The safety life-cycle model used in IEC 61511 is shown in the figure below:

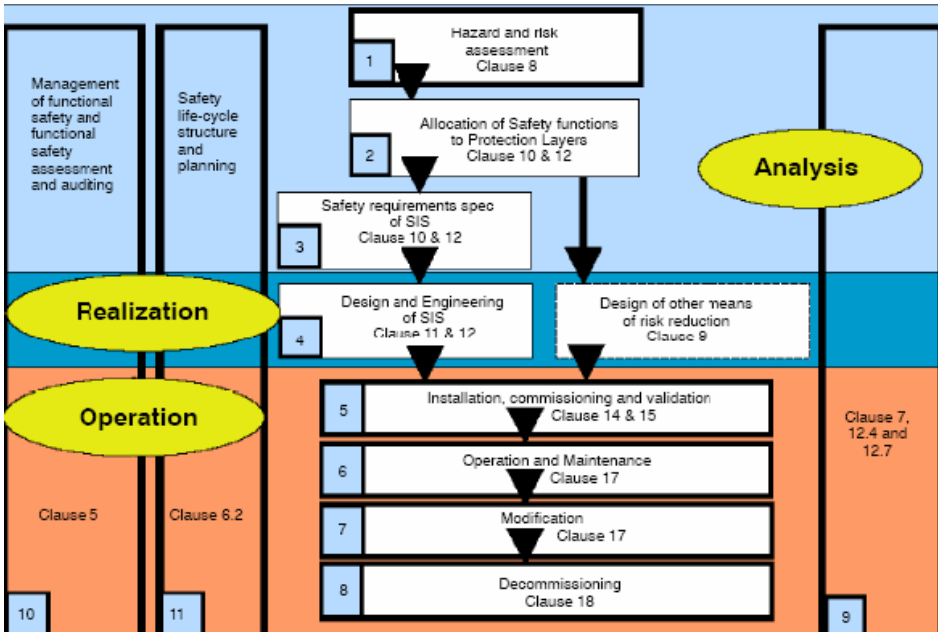


Figure 2: The safety life-cycle model /7/

This document also covers the analysis, realization, and operation phases. It emphasizes the continuous functions of planning, management, assessment, and verification, which support the sequential components of life cycle structure.

The essential details of analyzing, designing, verifying, and documenting are discussed and defined in all safety standards. It is important for an organization to devote extra care to the essential Safety Life Cycle so as to ensure that the desired safety level is achieved.

The whole process of design, realization and maintenance of functional safety has to be organized with a safety management system. There are requirements for the safety related integration of human factors aspects covering the whole lifecycle:

Table 4: Human Factors requirements

paragraph in /EN61511-2/	HF-requirements
11 Design of SIS[7]	➢ Human performance of operation and maintenance personnel as well as management is taken into account related to safety (man-machine-interface -MMI) ➢ Qualitative and quantitative analysis of human reliability ➢ Examples of human errors as safety threats: o Latent design errors o Errors during operation o Errors during maintenance o Errors during testing or interpretation of system state o Inadequate reaction in emergency case
11.7 Interfaces	➢ If an operators' action is part of the safety instrumented function all requirements for the commission of the action have to be treated as part of the safety instrumented function ➢ Ergonomic requirements for interfaces: o Highlighting of safety instrumented elements vs operation related instruments o Frequencies of display update during emergencies o Colours, flashing lights and a clear data structure should support the operator and prevent confusion o Messages should be clear, to the point and unambiguous
12.1 Requirement for the safety life cycle of software	Requirements fort the ergonomic design of the software
13 Factory acceptance test	Participation of operating staff in the factory acceptance test

These ergonomic requirements reflect only a part of the safety management system. Not treated are important features like training and maintenance of knowledge and skills of operating personnel, integration of contractors, the influence of management, organizational structure, and motivation as part of the safety culture. Additional references have to be taken into account:

[7] SIS- Safety Instrumented System, sicherheitstechnisches System (Schutzsystem)

Safety instrumented systems – programmable electronic system (VDI/VDE 2180 -1 /62/, p.10f)

- Prevention oriented: Prevention of non-tolerable states of the system
- Mitigation oriented: prevention of harm for people and environment.

The tasks of the safety instrumented systems are

- to monitor a safety relevant process parameter with respect to the admissible range of that process parameter

and in case of non conformity

- to release a trip

or

- to alert the permanently present operating crew by an alarm signal to perform necessary and already well defined counter measures.

Requirements for safety instrumented systems

1. Check, whether other direct impacting installation could be more adequate or more efficient like inherent safe design or protection / redundancy (mechanical or constructive)
2. Necessary risk-reduction

Namur Recommendation 31 /63/

“Contrary to the tasks of basic process control systems the task of a safety instrumented system is exclusively limited to avoid that the process parameter will reach the non-admissible error range. In case of non existence of the safety instrumented system a hazardous event is possible leading to personnel injury, significant hazard to the environment or a "serious hazard" according to the German legal regulation for incidents in industrial activities”

The functions of a safety instrumented system always should override functions of basic process control systems and monitoring systems. The initialization of the functions of a safety instrumented system occurs seldom, because of the low probability of the hazardous event and because of the measures of the different protection layers. Common components, i.e. components used by the safety system as well as other systems, have to be specified according to the requirements of the safety instrumented systems which are summarized in the annex.

To operate a safety instrumented systems of class A **organisational** measures are required:

- Permanent monitoring by plant operators and instrument technicians
- Inspection (functional testing)
- Maintenance
- Repair

German working group on Human Factors of the Störfall-Kommission /64/
Loccum workshop results:

1. Pure technical measures for maintenance and enhancement of the safety of complex systems reached their limits (ironies of automation), only the joined integration of the technical, human and organizational components – taken their strengths and weaknesses into account - guarantees reliability and safety.
2. System development and –design have to take an approach committed to defined safety goals as integrated parts, overcoming of the technical and economic design approach by "obligation of results"-policy (socio-technical enlargement, precautious philosophy of safety – integration of HF-aspects). Integrative und human-centred design have to follow latest standards in an interdisciplinary perspective.
3. "A consequent human factors oriented approach in design and for safety enhancement needs methods and tools", for design (allocation of function between man-machine, ergonomic aspects, control, safety instrumented and alarm systems, procedures, risk analysis, event analysis, human resource and organizational change programmes, training and education)."

Conclusions:

1. „System design for man-machine-interfaces should challenge the strengths of the human and compensate his weakness" (technology as compensation for human weaknesses is necessary in high-hazard industries, but technology in its recent shape restricts the strengths of the human operator (solution finding, routine, monotony)
2. „System design should ensure that the operator will be able to improve the safety actively during unforeseen events" (goal of enhancement and enlargement of competency, necessity of integration of system design and encompassing operator training)

5.3 Literature research

„We define automation as the execution by a machine agent (usually a computer) of a function that was previously carried out by a human." /65/, p. 231.

„Automation is any sensing, detection, information-processing, decision-making, or control action that could be performed by humans but is actually performed by machine." /66/.

In their framework for automation Parasuraman et al. /67/ discuss the questions at which stage of the information processing automation comes into play: sensory processing, perception /working memory, decision making or response selection, and on which level automation is realized (high vs. low). For the decision stage only a low automation level seems to be working.

According to Endsley and Kiris /68/ there are five stages of automation with the following roles (figure 2).

Level of Automation		Roles: Human	Roles: System
None	1	Decide, Act	———
Decision Support	2	Decide, Act	Suggest
Consensual AI	3	Concur	Decide, Act
Monitored AI	4	Veto	Decide, Act
Full Automation	5	———	Decide, Act

Figure 2: Levels of automation (Endsley & Kiris /68/)

Sheridan /69/ discusses the following eight automation levels:

1. Computer offers no assistance: the human must do it all
2. Computer suggests alternative ways to do the task
3. Computer suggest one decision alternative *and*
4. ... executes it if the human approves
5. ... allows the human a restricted time to veto before automatic execution
6. ... executes automatically, then necessarily informs the human
7. ... executes automatically, then informs the human only if asked for
8. Computer selects, acts and ignores the human

Allocation of function in MMI

A typical solution is to say: allocate functions to the human for the tasks best suited to the human, allocating to the automation the task best suited to it. This is easy to say, but not so easy to do.

The ISO/TC 159/SC 1/WG 1 N 88 (2006) defines allocation of functions as “process of deciding how system functions shall be implemented, by humans, by equipment and/or hardware and/or software” and task allocation as “distribution of work tasks or work task elements between operators and systems”.

Criteria for the allocation of functions from a psychological perspective are:

- Complete tasks for operators /70/.
- Degrees of freedom for work conduction and decision – loose coupling (time and content) to technology /71/
- Use of existing qualifications – transparency of processes
- Ability to learn from experience

Criteria for man-machine-interface-design

1. Cost-centred approaches

- Task are automated or left for the operator if the chosen solution is more economic
- Minimization of costs of „human“ / technology
- Economic perspective

2. Technology-centred approaches

- All tasks which can be automated are automated
- Reduction of the risk-factor „operator“
- Reduction to non-automation tasks (*left-over principle /72/)*
- *Engineering perspective*

3. Skill-centred approaches

- Allocation of function according to relevant performance strengths
- Optimization of performance (speed, precision)
- MABA-MABA-list (men are better at- machines are better at)
- Kompensationsgedanke (*compensatory principle /72/)*

4. Human-centred approaches

- Operator and technology are a co-operative system which performance should be optimized
- Operator and technology are complementary not compensatory,
- Automated systems as „team-partner“ /73/ Optimization of system reliability /74/

These approaches are mainly focused on the direct interface and do not take interfaces to other operators, to the organisation or to the environment into account.

Research results for problems caused by automation

- One of the problems is the so called out-of-the-loop-unfamiliarity (OOTLUF) phenomenon which restricts the effectiveness of vigilance in observation and control and can lead to a loss of skills or to a loss of situation awareness /75/; /67/; /76/:
- Loss of skills is higher for cognitive skills than for routine psycho-motoric skills, and can be reduced by regular training without automation
- Loss of situation awareness because of missing feedback, over-trust in automation or missing system knowlegde: *„Situation awareness is formally defined as perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future“ /77/.*

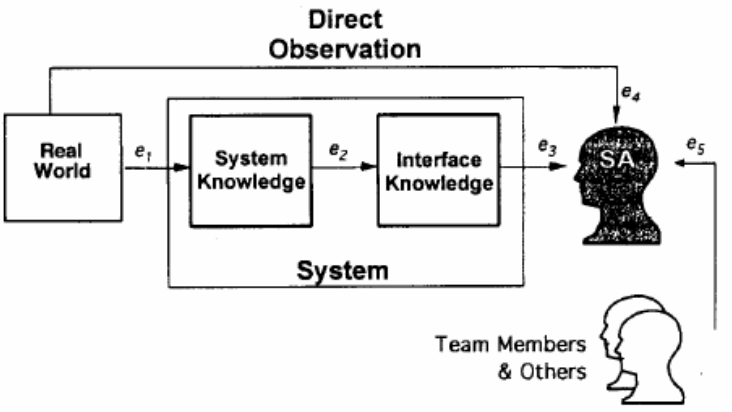


Figure 3: Information sources for situation awareness /77/

Correspondence between the level of automation and OOTLUF /78/ is not necessary. The way of implementation seems to be important, i.e. system transparency (information and feedback for perception, understanding and forecast of system state). The suggested solution is flexible automation, i.e. no static allocation, flexible change depending on defined criteria.

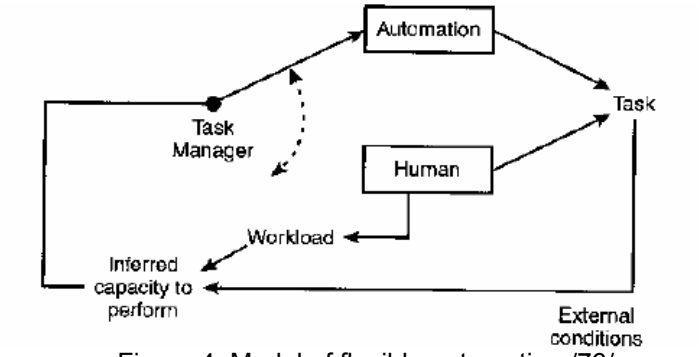


Figure 4: Model of flexible automation /76/

5.4 Conclusion

According to the standards on safety instrumented systems four different types of man-machine-interaction can be distinguished:

1. Human impact on safety instrumented systems during the whole lifecycle by design, maintenance, operation, quality management and supervision and control – like the four-eye-principle (independent checks)
2. Man-machine-interaction by monitoring of the safety instrumented system and response to faults.
3. Human impact via humans conceptualized as being “part of the safety instrumented system”, as being part of the safety function – either functioning as signal detection / information processing part or the actor part
4. Human impact by bypassing the safety instrumented system – planned or allowed- by manual operation

If the operator is part of the safety function:

1. a task analysis should be completed and there should be rules for emergencies;
2. the maximal credit for risk reduction by use of the operator in the safety function should be adjusted to IEC 61511 /7/

It seems obvious that in the standards the operator is treated as a part of the safety function as discussed above, but that only a very few recommendations and requirements according to his potential impact are given, e.g. according to education, tasks and task design, training and necessary competence etc. It seems necessary to formulate requirements to proof the safety function of the man-machine-interface.

There is still a need to emphasise the four different types of human influence on the safety instrumented system as described above more explicitly in the standards and regulations. Furthermore there is a need to include the results of the research into existing regulation, especially the need for task-analysis, for ergonomic requirements, for education and training as well as safety culture improvements which have to be formulated and taken into account.

5.5 Questions

The discussion should cover topics like:

1. Are the four different types of Man-Machine-Interaction according to IEC 61511 well described?
2. How operator tasks in abnormal situations should be identified and assessed is the operator is part of the safety function?
3. How to consider human skills in this process?
4. Does it make sense to limit the credit to be taken from the operator as a part of the safety function by 10 as maximum achievable risk reduction?
5. How to inhibit process alteration by operator activities to prevent automatic shut-offs causing out of design situations causing major accidents although an automatic safety system is installed?

6 Thematic session 5: Human Factors in alarm management

Key objectives to be covered in the session

- Explain considerations on how to take human factors into account in designing new alarm systems;
- Explain ways of evaluating and improving existing alarm systems of installations;
- Make recommendations on the sufficient support of the operator handling flood, suppression, prioritisation etc.

6.1 Introduction

According to the IEC 61511 there are messages and two types of alarms:

Monitoring System -	Messages
Control system –	**Alarms**
Safety System –	**Critical alarms** – operator action for prevention of major accidents
	SIS - **Alarms** – operator supervision of the SIS

Parallel to the safety system exists the alarm system (i.e. alarms of the control and safety systems) and its interface with the operators involved in "abnormal situations". Design, modifications to, and maintenance of alarm systems should take human weaknesses into account as well as the 'natural' ability of operators to successfully control the course of events in abnormal situations and avoid a (major) accident. The aim of this session is to make recommendations on suitable alarm management.

For the preparation of this section of the discussion document the following sources were analysed:

- Regulations and technical standards
- Scientific literature

6.2 Regulation and technical standards

For the discussion of human factors in alarm management the following official documents seems to be relevant:

- HSE information sheet No 6: better alarm handling /79/
- HSE Human Factors Briefing Note No 9: Alarm Handling /80/
- Namur Worksheet 102: Alarm management /8/
- EEMUA Publication No 191: Alarm systems – a guide to design, management and procurement /81/

HSE concludes in the information sheet No 6 /79/ that a better alarm handling can have a significant effect on the safety, because it leads to a tighter quality control, improved fault diagnosis and more effective plant management by operators. For the diagnosis of problems related to alarms the following questions are suggested:

- How many alarms are there?
- Are all necessary, requiring operator action? (Process status indicators should not be designated as alarms)
- How many alarms occur during normal operation?
- How many occur during a plant upset?
- How many standing alarms are there?
- Are operators overwhelmed by alarm “floods”?
- Are there nuisance alarms, e.g. large numbers of alarms acknowledged in quick succession, or are audible alarm regularly turned off?
- Is alarm prioritisation helpful for operators?
- Do operators know what to do with each alarm?
- Are there control room displays well laid out and easy to understand?
- Is clear help available, written or on-screen?
- How easy is it to ‘navigate’ around the alarm pages?
- Are the terms used on screen the same as the terms the operators use?
- Have there been any critical incidents or near misses where operators missed alarms or made the wrong response?
- Is there a written policy/strategy on alarms?
- Is there a company standard on alarms?
- Is there a structured process for adding new alarms or modifying existing ones? (There is a tendency for hazard and operability studies (HAZOPs) to generate actions which result in a lot of ‘quick fix’ alarms being installed)
- How many new alarms did your last HAZOP produce and how were they justified?
- Can operators notice the alarms and correspond correctly to them? Was the impact on the overall alarm burden on operators considered?

The following recommendation and references are given:

The long-term average alarm rate during normal operation should be no more than one in every ten minutes; and no more than ten displayed in the first ten minutes following a major plant upset (EEMUA guide /81/, p. 37). For an effective alarm prioritisation it is necessary to define rules and apply them consistently to each alarm, to use about three priorities, to base priorities on the potential consequences if operators fail to respond. The proportion of prioritisation should be 5% high priority, 15% medium and 80% low (/81/, p.65). According to operator reliability it is required that there are a very obvious display of the specific alarm, few false alarms, low operator workload, a simple well-defined operator response, well trained operators and a testing of the effectiveness of operators’ responses. An effective alarm system should alert, inform and guide operators, allowing them to diagnose problems, prevent unnecessary emergency shutdown, only display useful and relevant alarms, be ergonomically designed and allow enough time for the operator to respond as well as defined responses for each alarm.

In HSE Human Factors Briefing Note No 9 /80/ the following problems and solutions are presented:

Table 5: Alarm handling (/80/, p.3)

PROBLEM	POSSIBLE SOLUTIONS
DESIGN	
Masking - alarm sound is not heard above typical noise levels; alarm drowns out communications - lit up alarm cannot be seen above typical lighting levels	Raise alarm volume to 10dB(A) above other workplace noise; allow operators to lower the volume of alarms once they've sounded. Make alarm bright enough for all expected conditions; use colour to highlight the alarm; accompany visual alarm with a sound
Flooding - more alarms than the operators can deal with are presented at once	System should be designed to filter out or suppress unnecessary alarms and to present alarms in priority order; operators may need clear procedures and training on how to prioritise their actions
Difficult to tell one alarm from another - sounds or lights are very similar	Use 'coding' (e.g. different sounds; pulsing of sounds; different colours; flashing) to show importance of alarms and group by the safety function to which they relate
Nuisance alarms - false alarms, 'fleeting' or standing alarms	Change set points, hysteresis or dead bands to make the system less sensitive to short duration unimportant fluctuations. When alarms are expected (e.g. during testing and maintenance) and these cannot be overridden, use tags to indicate they are being tested
ORGANISATION / PROCEDURES	
Operators do not have enough time after the alarm commences to take the right action	Set the alarm levels to show the progress of an alarm situation e.g. a tank overfill alarm sounds at 'high' level then again at 'high high' level
Alarms are missed because the area where they appear is not constantly manned	Install 'repeater' alarms in several places; enforce manning of key operating areas
Operators experience other problems with alarms such as irrelevant and unimportant information being given or poor alarm names being used	Include operators in making suggestions about alarm problems and in suggesting solutions; check solutions against recommended guidance (see references)
Alarms are produced when a warning signal would do (alarm is attached to an event that is safety critical)	Alarms are designed against a risk assessment that identifies what plant conditions should produce an alarm
Alarms are in place because it's too difficult to automate the process - puts the responsibility on the operator to act	Design alarms according to good practice principles (see references) - beware not to overload the operator

In the Namur Worksheet 102 /8/ the purpose is to set out a procedure for designing alarm management within a process control system with the following characteristics:

- “Demand for action depending on process status
- Support for appropriate assessment of situations and operator intervention
- Easy recognition, transparency and consistency of messages and alarms
- Number and frequency of alarm and message signals kept to a minimum
- Low burden on operator when alarms or messages come up
- Documentation and evaluation tools” /8/, p.5

An alarm should have the following characteristics /8/; /81/: relevant, unique, timely, prioritized, understandable, diagnostic, advisory, focusing. Because of physiological

and mental characteristics human beings are capable of differentiating between relative signals (shades of colours, sounds) and distinguish one from another, but do not show the same skills for absolute signals (specific colours, specific pitch of sounds, flash frequency), which reduces the variety of those that can be used (e.g. no more than 5-9 colours, 2 different flash rates, see also VDI 3699 /82, 83/, IEC 73 /84/, DIN 2403 /85/). The provision of pre-processed information (meta-characters) has a positive effect on fast recognition and association.

Methods for alarm processing are: alarm grouping, filtering when generating alarms, first-event signal, and alarm suppression. It is suggested that the prioritization follows the criteria of a) consequence and b) time available for action. Prioritization should be colour-coded. The following prioritization matrix is suggested:

Priority

Priority

Seriousness			
Response time	Shutdown	Loss of product quality	Delay in production
< 5 min	High	Medium	Low
5-20 min	Medium	Low	Low
> 20 min	Low	Low	Low

Figure 5: Prioritization matrix /8/, p. 12

In this prioritization matrix two implicit assumptions are covered: a) seriousness could be a major accident or an environmental damage and b) all systems with alarms have more or less automated shutdowns.

Prioritizations can be reached by volume for audible signals or by pulsation frequency and by colour or flash frequency for visible signals.

Types of visualization for alarms are:

- Alarm diagram for the area
- Alarm visualization via alarm list
- Alarms in process displays
- First event indication warning system

For a continuous improvement process, i.e. optimization, updating and organization of the alarm management the following functions are required:

- “Performance monitor for analysing the

  - Number of alarm per alarm type, alarm signal, alarm source and unit type
  - Number of process alarms of one alarm source per time unit, “wobby” alarms, permanent alarms
  - Duration of alarm status
  - Evolution of active alarm signals from one alarm source (alarm chains), evolution over duration of active/unacknowledged signal separated into time units
  - Incidence of active/unacknowledged alarm signal times
  - Duration of alarm acknowledgement
  - Number of alarms that have returned unacknowledged
  - Alarm resulting from operator intervention
  - Operator intervention as a result of process alarm and following acknowledgement
- Audit trail for alarms, limit value warnings and suppressed alarms
- Access and authorization” /8/, p. 19

A careful documentation of important features as prioritization, grouping and situation-related alarm suppression is required.

In the EEMUA guide /81/ recommendations for alarm systems design activities are given:

- **Risk assessment** (development of a plant safety case, identification of the safety role of the operator, risk assessment to identify alarms to protect against safety, environmental or economic risks, review to identify alarms providing significant risk reduction)
- **Ergonomics** (identification of number of operators and their roles, overall design of operator interface, design of alarm interface)
- **Design of individual alarms** (review of proposed alarms not deriving from risk assessment, identification of alarms with special integrity or display requirements, completion of data from for each alarm, production of alarm response procedures, design of plant alarm sensors, design of hardware for conditioning individual alarm signals, installation of plant alarm sensors and signal conditioning)
- **Design integration** (rationalization of lists of proposed alarms, review of overall system design to meet key design principles, identification of required alarm processing functionality)
- **Alarm system configuration** (installation of alarm system hardware, configuration of alarm system hardware/software facilities, construction of alarm information database, configuration of hardware/software for individual alarms, configuration of alarm combination logic)
- **Testing and commissioning** (testing of alarm system facilities, testing of alarm sensors and signal conditioning, testing of individual alarm hardware/software configurations, evaluation of overall ergonomic acceptability, measurement of alarm system performance, determination of ongoing testing needs, optimization of operational performance)

Furthermore, elements of user-centred design are described, because the complete interface should be designed reflecting best ergonomic practices as an integrated and usable system: design review, task analysis, operator involvement, early ergonomics evaluation, on-going monitoring.

According to EEMUA /81/ attributes of a good alarm message are the following:

- Clearly identifies the condition that has occurred
- Uses terms that the operator is familiar with
- Uses consistent abbreviations from a standard site dictionary of abbreviations
- Has a consistent message structure
- Does not rely on the learning of tag names or numbers
- Has been checked for usability during actual plant operation

6.3 Scientific literature

The evaluation of the scientific literature yields only a few additional items. Smith et al. /86/ describe a gap in safety management systems according to alarm handling: no clear identification of safety related alarm, too many top priority alarms, no site alarm policy or philosophy, no records of assessing operator competence, no performance specifications for alarm procurement. Dunn and Sands /87/ identify nuisance alarms, stale alarms, flood of alarms and lack of clarity of alarms as problems related to alarm systems. They present an alarm management lifecycle: philosophy, identification, rationalization, design, implementation and training, operation, performance monitoring, maintenance, assessment, management of change with three loops for maintaining and improving: monitoring and maintenance loop, monitoring and management of change loop, assessment loop.

Honeywell /88/ identifies another problem: the fact that alarms actually are single-dimension representations of what are often multi-dimensional problems.

Nimmo /89/ suggests two types of assessments for alarm management: a physical assessment of performance in a range of scenarios and a ladder assessment of the management and cultural attributes underlying the control of operations, including individual factors (situation awareness, teamwork, alertness and fatigue, training and development, roles and responsibilities, willingness to act) and organizational factors (management of operating procedures, management of change, continuous improvement of control room safety, management of safety)

6.4 Conclusion

In this session recommendations on the consideration of the results of EEMUA /81/ and NAMUR /8/ in the OECD Guiding Principles /5/ should be presented and discussed, concerning relevant recommendations as well as taking into account ergonomic requirements.

According to EEMUA /81/ four core principles should be regarded:

- **Usability**: Alarm systems should be designed to meet user needs and operate within the user's capabilities.
- **Safety**: The contribution of the alarm system to protecting the safety of people, the environment and the plant should be clearly identified.
- **Performance monitoring**: The performance of the alarm system should be assessed during design and commissioning to ensure that it is usable and effective under all operating conditions. Regular auditing should be continued throughout plant life to confirm that good performance is maintained.
- **Investment in engineering:** Alarm Systems should be engineered to suitably high standards. When new alarm systems are developed (or existing systems are modified), the design should follow a structured methodology in which every alarm is justified and properly engineered.

Furthermore shall alarm systems help the operator:

- to correct potentially dangerous situations before the Emergency Shutdown System (ESD) is forced to intervene
- to recognise and act to avoid hazardous situations
- to prevent major accidents or limit its consequences.

Alarm Management should include:

1. Design of alarm systems, including risk assessment, structuring of alarms (prioritisation), reliability evaluation and evaluation of the consideration of ergonomic requirements
2. Documentation, validation, testing of the alarm system
3. Monitoring, verification, performance measurement and improvement programme
4. Management of change and decommissioning

1. Alarm Systems Design

Principles for alarm systems design are:

- The purpose of an alarm system is to direct the operators attention towards plant conditions requiring timely assessment or action.
- Each alarm should alert, inform and guide.
- Every alarm presented to the operator should be useful and relevant to the operator.
- Every alarm should have a defined response.
- Adequate time should be allowed for the operator to carry out his defined response.
- The alarm system should be explicitly designed to take account of human limitations.
- Every alarm should be justified, properly engineered and be consistent with the overall alarm philosophy and the plant risk assessment.
- The design of each alarm should follow a systematic structured procedure in which design decisions are documented.
- Stand alone systems can provide good reliability and can be designed so that critical alarms are very obvious and easy to recognise.

- The process control system should support the assessment of complex situations like more than one alarm is raised or failures of the emergency shut of systems or the alarm system.
- Alarm systems should be designed so that failures are made obvious to the operator. The operational implications of potential failures should be assessed, and considerations should be given to the need for operator procedures to cover them.
- Alarm list displays should be designed such that repeating alarms do not cause them to become unusable.
- An integrated design should be developed for all audible alarms in the control room. Human physiological performance factors muse be borne in mind.
- The colours and visualization standards must be used consistently throughout the alarm system

A fundamental issue when designing each alarm is to consider how important it is and how reliable it should be. To do this it is necessary to go through some form of qualitative and quantitative risk assessment.

The Principles for risk assessment are:

- Risk reduction should start with the initial plant design by selecting processes and plant configurations which have appropriate inherent safety.
- The design of alarm systems should involve a consideration of the risks of injury to people and damage to the environment, and a decision about which risks the alarms are intended to reduce.
- Even on highly automated plants with extensive automatic protection systems there almost certainly will be potential fault scenarios that require operator intervention. These scenarios should be identified and it should be determined whether and how the alarm system will support the operator in carrying out this corrective action.
- There is a limit to the amount of risk reduction which can be achieved using (critical) alarms even when the equipment is of the highest integrity.
- If an alarm system is not suitable for implementation and significant risk reduction is needed, then this should be obtained by alternative means (e.g. installing additional technology or process modification).

Alarm processing should support the operator by compressing information and giving interpretation support. It includes alarm grouping, filtering when generating alarms, first event signals and alarm suppression.

The Principles for structuring of alarm systems are:

- Availability of written rules on how priorities should be assigned. These should be applied consistently to all alarms in all systems used by the operator.
- In every alarm system the operator should not be overloaded with alarms presented by the chosen display arrangement – either in normal operation, start-up, changing process conditions or shut-down.
- It is usually appropriate to prioritise alarms according to two factors: the severity of the consequences that the operator could prevent by taking the corrective ac-

tion associated with the alarm and the time available compared with the time required for the corrective action to be performed to have the desired effect.

- Experience has shown that the use of priority bands within any one type of display is ergonomically effective for the normal presentation of alarms. Definitions of alarm priority should be consistent across systems
- Displays should be designed to assist the operator information so that the operator can easily access all key information even if the alarm system does become overloaded.
- In case of alarm overload the operator may be able to: select the alarm list display to show only high priority alarms and ignore all medium and low priority alarms or ignore all alarms on the process control system and only look at alarms on the stand-alone system.
- There are two parallel approaches that the designer should take to reduce the problems of alarm overload: Eliminate the alarm overload or improve the management of alarm overloads. Steps should be taken to ensure that the operator performs as effectively as possible during any overload incident that do occur nevertheless.

2. Documentation, validation, testing of the alarm system

For all credible accident scenarios the designer should demonstrate that the total number of alarms and their maximum rate of presentation does not overload the operator. The following points should be regarded:

- Each and every alarm should be covered by a written (or on screen) alarm response procedure which should assist the operator in identifying and carrying out the necessary response. Many alarms may have a very similar response and may be covered by a general procedure. However, for critical alarms an individual procedure per alarm is generally justified.
- All alarm settings should be systematically determined and documented during design, commissioning and operation. All changes should be documented with reasons.
- A strategy should be developed for the validation and testing of alarm systems. Validation and testing shall be carried out where an alarm is critical. There should be written procedures. The procedures should specify realistic tolerances on the point at which an alarm should become active.

3. Monitoring, verification, performance measurement and improvement programme

Alarm management is not a one-off exercise. It needs to be evaluated continuously or at reasonable intervals. Alarm systems performance should be regularly checked especially to ensure that alarm overload is not occurring.

- Measurement of the performance of an alarm system can be used: as performance targets for the acceptability of a new alarm system, to assess the adequacy of an existing alarm system, as management tools for assessing the effectiveness of an on-going improvement programme, to identify specific nuisance alarms.
- Usability benchmarks may help in the assessment of whether the operator will find the alarm system easy to work with.

- A review programme should be set up to identify spurious or badly designed alarms and to re-engineer them. The review should ultimately cover every alarm in the system.
- A powerful tool for achieving alarm system improvement is to assign the task to specific teams. The operators and supervisors should be involved deeply in any programme to improve alarm systems.
- Performance should be audited, overload incidents should be identified and steps should be taken to minimise their frequency.

4. .**Management of change and decommissioning**

There should be defined procedures to control changes to the alarm system including decommissioning of parts of it. Thus all proposed changes should be fully analysed, their consequences should be determined, and agreed changes should be recorded with reasons.

6.5 Questions

1. Is the overall structure of the proposed recommendations suitable?
2. Are relevant chapters or overall subjects missing?
3. Are general modifications due to existing legislation, standards or practices required?
4. Are relevant recommendations e.g. of Namur, EEMUA etc. missing?
5. Are modifications of significant relevance of the proposed recommendations required?
6. What are the barriers and further problems related to alarm management?
7. What are the barriers and further problems to consider beside technical and information processing factors those which are more “soft” like teamwork and organizational factors?
8. How can the numbers according to human perception and progressing reported in Namur or EEMUA be validated?

7 References

/1/ Working Group on Chemical Accidents (2006). PREPARATION OF A WORKSHOP ON HUMAN FACTOR IN CHEMICAL ACCIDENTS AND INCIDENTS. ENV/JM/ACC(2006)5. Proceeding at the 16th Meeting of the Working Group on Chemical Accidents, to be held on 19-20 October 2006 in Varese, Italy.

/2/ Uth, H.-J., & Wiese, N. (2004). Central collecting and evaluating of major accidents and near- miss- events in the Federal Republic of Germany- results, experiences, perspectives. Journal of Hazardous Materials, 111, 139-145.

/3/ HSE (2005). Inspectors Toolkit: Human factor in the management of major accident hazards. Available under: http://213.212.77.20/humanfactors/comah/toolkitintro.pdf [19.12.2006].

/4/ Health and Safety Executive (1999). HSG48. Reducing error and influencing behaviour. London: HMSO

/5/ OECD (2003). Guiding Principles for Chemical Accident Prevention, Preparedness and Response. Available under: http://www.oecd.org/dataoecd/10/37/2789820.pdf [23.06.2003].

/6/ VDI 4006-1. Human reliability - Ergonomic requirements and methods of assessment, November, 2002.

/7/ IEC 61511-1. Functional safety- Safety instrumented systems for the process industry sector- Part 1: Framework, definitions, system, hardware and software requirements, January 2003.

/8/ Namur- Worksheet NA 102. Alarm Management. AK 2.9, Dezember 2005.

/9/ VDI 4006-2. Human reliability - Methods for quantitative assessment of human reliability, February 2003.

/10/ HSL Report: Bell, J. & Healey, N. (2006). The causes of major hazard incidents and how to improve risk control and health and safety management: a review of the existing literature. Health & Safety Laboratory. HSL/2006/117.

/11/ Lee, T. (1998). Assessment of safety culture at a nuclear reprocessing plant. Work & Stress, 12 (3), 217-237.

/12/ HSE (1996). The contribution of attitudinal and management factors to risk in chemical industry. HSE Contract Research Report No. 81/1996. Available under: http://www.hse.gov.uk/research/crr_pdf/1996/CRR96081.pdf [11.01.2007].

/13/ Fahlbruch, B. (2000). Vom Unfall zu den Ursachen: Empirische Bewertung von Analyseverfahren. Berlin: Mensch & Buch Verlag.

/14/ Hollnagel, E. (2005). The Elusiveness of "Human Error". Available under: http://www.ida.liu.se/~eriho/HumanError_M.htm [28.11.2006].

/15/ Amalberti, R. (2001). The Paradoxes of almost totally safe transportation systems. Safety Science, 37, 109- 126.

/16/ Lourens, P. F. (1989). Error analysis and application in transportation systems. Accident Analysis & Prevention, 21(5), 419-426.

/17/ Leplat, J. (1986). Human errors in new technologies: Methods of analysis. In H. Raum & W. Hacker (Eds.), Optimierung geistiger Arbeitstätigkeiten. Referate des V. Dresdner Symposiums zur Arbeits- und Ingenieurspsychologie.

/18/ Rasmussen, J. (1980). What can be learned from human error reports? In K. D. Duncan, M. M. Gruneberg, & D. Walls (Eds.), Changes in Working Life (pp. 97-113). Chichester: Wiley.

/19/ Rauterberg, M. (1996). Why and What can we learn from human errors?. In A. F. Özok & G. Salvendy (Eds.), Advances in Applied Ergonomics. Proceedings of the 1st International Conference on Applied Psychology, ICAE `96, Istanbul, May 21.24, 1996 (pp. 827-830). Istanbul, West Lafayette: USA Publishing.

/20/ Duffey, R. B. & Saull, J. W. (2003). Errors in Technological Systems. Human factors and Ergonomics in Manufacturing, 13(4), 279-291.

/21/ Zapf, D., Brodbeck, F. C., Frese, M., Peters, H., & Prümper, J. (1992). Errors in working with office computers: A first validation of a taxonomy for observed errors in a field setting. International Journal of Human-Computer Interaction, 4(4), 311-339.

/22/ Shaban, R. Z., Wyatt Smith, C.M., Joy Cumming, J. (2004). Uncertainty, Error and Risk in Human Clinical Judgement: Introductory Theoretical Frameworks in Paramedic Practice. Journal of Emergency Primary Health Care (JEPHC), 2, Issue 1-2.

/23/ Reason, J. (2001). Understanding adverts events: the human factor. In: C. Vincent (Eds.), Clinical Risk Management. London: British Medical Journal Books.

/24/ Shappell, S. A., Wiegmann, D.A. (2003). Human Error and General Aviation Accidents: A Comprehensive, Fine- Grained Analyses Using HFACS. Available under: http://www.hf.faa.gov/docs/508/docs/gaFY04HFACSrpt.pdf [28.11.2006].

/25/ Helmreich, R. L. (2000). On error management: lessons from aviation. Available under: http://bmj.com/cgi/content/full/320/7237/781#BIBL [07.01.2005].

/26/ Bove, T. (2002). Development and Validition of a Human Error Management Taxonomy in Air Traffic Control. Doctoral Dissertation at University of Roskilde.

/27/ Yemelyanov, A. M. (2004). Toward a System Approach to Human Error Investigation. Proceedings of the Human factors and Ergonomics Society 48th Annual Meeting. Denver, CO: 20- 24 September 2004, pp. 2436- 2440.

/28/ Klumb, P. L. (1994). Attention, action, absent-minded aberrations: A behaviour-economic approach. Doctoral Dissertation at Technische Universität Berlin.

/29/ Lorenzo, D. K. (1990). A Manager's Guide to Reducing Human Errors. Washington, DC: Chemical Manufactures Association, Inc.

/30/ Singleton, W. T. (1973). Theoretical approaches to human error. Ergonomics, 16(6), 727-737.

/31/ Rasmussen, J. (1993). Perspective on the concept of human error. Paper presented at Society for Technology in Anesthesia Conference "Human Performance and Anasthesia Technology", New Orleans, February 1993.

/32/ More, D. A. (2003). A Simplified Risk- Based Approach For Analyzing Human factors. In Hazards XVII- Process safety- Fulfilling our responsibilities, Symposium Series No. 149 (pp. 537- 548). Rugby, UK: IChemE.

/33/ Abu- Khader, M. M. (2004). Impact Of Human Behaviour On Process Safety Management In Developing Countries. In Proceedings of the Trans ICemE, Part B, Process Safety and Environmental Protection, 82 (B6), 431-437.

/34/ Leplat, J., & Rasmussen, J. (1984). Analysis of human errors in industrial incidents and accidents for improvement of work safety. Accident Analysis & Prevention, 16(2), 77-88.

/35/ ICNPO- Conferenence Report. (1994). First International Conference on HF-Research in Nuclear Power Operations (ICNPO). 31 Oktober bis 2 November, Berlin.

/36/ Singleton, W. T. (1972). Techniques for determining the causes of error. Applied Ergonomics, 3(3), 126-131.

/37/ Reason, J. (1997). Managing the risks of organizational accidents. Aldershot: Ashgate.

/38/ Reason, J. (1990). *Human error.* Cambridge: Cambridge University Press.

/39/ Rasmussen, J. (1987). Approaches to the Control of the Effects of Human Error on chemical plant safety. Roskilde: Riso National Laboratory.

/40/ Groeneweg, J. (1992). Controlling the controllable. The management of safety. Leiden: DSWO Press.

/41/ van Vuuren, W. (1998). Organisational failure: An explonatory study in the steel industry and the medical domain (pp. 1-149). Eindhoven: Eindhoven University of Technology - Proefschrift 1998.

/42/ Swain, A.D., Guttman H.E. (1983). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final report. (NUREG/CR-1278). Washington DC: U.S. Nuclear Regulatory Commission.

/43/ OECD (2003). OECD Guidance on Safety Performance Indicators. Available under: http://www.oecd.org/dataoecd/60/39/21568440.pdf [11.01.2007].

/44/ Wilpert, B., & Fahlbruch, B. (2004). Safety culture: Analysis and intervention. In C. Spitzer, U. Schmocker, & V. N. Dang (Eds.), Probabilistic safety assessment and management (Vol. 2, pp. 843-849). London: Springer.

/45/ INSAG. (1991). Safety culture. Vienna: International Atomic Energy Agency (Safety Series No. 75-INSAG-4).

/46/ IAEA. (1998). Safety culture self-assessment. Report of a technical committee meeting, June 1998.

/47/ INSAG - International Safety Advisory Group (1998). Developing safety culture in nuclear activities: Practical suggestions to assist progress. Safety Reports Series No. 11. Vienna: IAEA.

/48/ IAEA. (2001). The operating organization for nuclear power plants: safety guide. Vienna: International Atomic Energy Agency (IAEA).

/49/ Responsible Care (n.d.). Available under: http://www.cefic.be/Files/Publications/rcreport2004.pdf [11.01.2007].

/50/ The Keil Centre (2001). Safety Culture maturity model. HSE Offshore Technology Report 2000/049.

/51/ A review of safety culture and safety climate literature for the development of the safety culture inspection toolkit. Human Engineering 2005. HSE CRR 367. Key indicators from the safety culture inspection toolkit for the rail industry (HMRI): leadership, two-way communication, employee involvement, learning culture and attitude towards blame.

/52/ Internationale Länderkommission Kerntechnik (2005). ILK-Stellungnahme zum Umgang der Aufsichtsbehörde mit den von den Betreibern durchgeführten Selbstbewertungen der Sicherheitskultur. atw 2005/5, p.317-322.

/53/ Kadri, S.H. & Jones, D.W. (2006). Nuturing a strong process safety culture. Process Safety Progress, 25/1, 16-20.

/54/ Wilpert, B., Maimer, H. & Loroff, C. (2000). Einfluß des Menschen auf die Sicherheit von Kernkraftwerken - Bewertung der Zuverlässigkeit einer computergestützten Ereignisanalyse (CEA) in der Kernindustrie. Endbericht. TU Berlin.

/55/ Wilpert, B. & Fahlbruch, B. (2003). Final Report on the Advanced Research and Training Seminar (ARTS) on Work-Place Safety, System Safety and Psychology, Singapore, July 13-15, 2002. International Journal of Psychology, 38 (2), 113-118.

/56/ Olive, C., O'Connor, M. & Mannan, M.S. (2006). Relationship of safety culture and process safety. Journal of Hazardous Materials, 130, 133-140.

/57/ Commission Regulation (EC) No 2042/2003 of 20 November 2003 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks (Text with EEA relevance). Official Journal L 315 , 28/11/2003 P. 0001 – 0165.

/58/ IEC/EN 61511- 2. Functional safety- Safety instrumented systems for the process industry sector- Part 2: Guidelines for the application of IEC 61511- 1, July 2003.

/59/ IEC/EN 61511- 3. Functional safety- Safety instrumented systems for the process industry sector- Part 3: Guidance for the determination of the required safety integrity levels, March 2003.

/60/ Richtlinie 96/82/EG des Rates vom 9. Dezember 1996 zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen ("Seveso II- Richtlinie") . Available under: http://europa.eu.int/comm/environment/seveso/ and http://mahbsrv.jrc.it.

/61/ IEC/EN 61508 (2002). International Standard 61508 Functional Safety: Safety-Related System. Geneva, International Electrotechnical Commission.

/62/ VDI/VDE 2180- 1. Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (Entwurf), Oktober 2005.

/63/ NE 031. Anlagensicherung mit Mitteln der Prozessleittechnik. AK 4.5, Juli 2006.

/64/ IFSN- Interdisziplinäre Forschungsgruppe für soziale Nachhaltigkeit (2002). Projekt: Wissenschaftliche Beteiligung sowie Informationsdarstellung zu dem Vorhaben „Human Factors", Abschlussbericht. Verfügbar unter: http://www.sfk-taa.de/berichte_reports/andere_dokumente/abschlussbericht_uni_oldenburg.pdf [Stand: 11.01. 2007].

/65/ Parasuraman, R. & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. Human factors, 39, 230-253.

/66/ Moray, N., Inagaki, T., & Itoh, M. (2000). Adaptive Automation, Trust, and Self-Confidence in Fault Management of Time-Critical Tasks. Journal of Experimental Psychology: Applied, 6(1), 44-58.

/67/ Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A Model for Types and Levels of Human Interaction with Automation. IEEE Transactions on Systems,Man, and Cybernetics, 30(3), 286-297.

/68/ Endsley, M., & Kiris, E. (1995). The out-of-the-loop performance problem and level of control in automation. Human factors, 37(2), 381-394.

/69/ Sheridan, T.B. (2000). Function allocation: algorithm, alchemy or apostasy? International Journal of Human-Computer Studies, 52, 203-216.

/70/ Ulich, E. (2001). Arbeitspsychologie (4. Aufl.). Zürich: Verlag der Fachvereine; Stuttgart: Poeschel.

/71/ Grote, G., Weik, S., Wäfler, T., Zölch, M. & Ryser, C. (1999). KOMPASS (Komplementäre Analyse und Gestaltung von Produktionsaufgaben in sozio-technischen Systemen). In: H. Dunckel (Hrsg.), Handbuch psychologischer Arbeitsanalyseverfahren. Zürich: vdf.

/72/ Hollnagel E., Bye, A. (2000): Principles for Modelling Function Allocation. In International Journal of Human-Computer Studies, 52 (2), p. 253-265.

/73/ Christoffersen, K., & Woods, D. D. (2002). How to make automated systems team players. Advances in Human Performance and Cognitive Engineering Research, 2, 1-12.

/74/ Gisa, H. G. & Timpe K.-P. (2000). Technisches Versagen und menschliche Zuverlässigkeit. Bewertung der Verlässlichkeit in Mensch- Maschine- Systemen. In K.-P. Timpe, T. Jürgensohn & H. Kolrep (Hrsg), Mensch-Maschine-Systemsicherheit (S. 63-106). Düsseldorf: Symposium Publishing.

/75/ Manzey, D. (2005). Arbeit in Mensch- Maschine Systemen 1-2. Vorlesung an der TU-Berlin. Available under: http://www.gp.tu-berlin.de/AOPsychologie/Studium/material/ws0506m/A&O_I_10_1.pdf [11.01.2007].

/76/ Wickens, C. D., & Hollands, J. G. (2000). Engineering psychology and human performance (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

/77/ Endsley, M. (1996). Automation and situation awareness. In: Parasuraman, R. & Mouloua, M. (eds.), Automation and human performance. Theory and applications. Mahwah: Erlbaum.

/78/ Lorenz, B., Di Nocera, F., Röttger, S., & Parasuraman, R. (2002). Automated fault management during simulated space flight. Aviation, Space, and Environmental Medicine, 73, 886-897.

/79/ HSE (2000). Better Alarm Handling. HSE Information Sheet- Chemical Sheet No. 6. March, 2000.

/80/ HSE (n.d.). Alarm handling. HSE information Sheet- Chemical Sheet No. 9. Available under: http://www.hse.gov.uk/humanfactors/comah/09alarms.pdf [11.01.2007].

/81/ EEMUA (1999). Alarm Systems: A Guide to Design, Management and Procedurement. EEMUA Publication No 191. The Engineering Equipment and Materials Users Association: London.

/82/ VDI/VDE 3699- 1. Prozessführung mit Bildschirmen – Begriffe, Mai 2005.

/83/ VDI/VDE 3699- 2. Prozessführung mit Bildschirmen – Grundlagen, Mai 2005.

/84/ IEC 73 (1990). Colours of pushbuttons and their meanings. NY: International Electrotechnical Commission.

/85/ DIN 2403. Kennzeichnung von Rohrleitungen nach dem Durchlflußstoff, März 1984.

/86/ Smith, W. H., Howard, C. R., & Foord, A. G. (2003). Alarms Management – Priority, Floods, Tears or Gain?. Available under: http://www.4-sightconsulting.co.uk/Current_Papers/Alarms_Management/alarmsmanagement.html [13.03.2003]

/87/ Dunn, D. G. & Sands, N. P. (2003). ISA-SP18- Alarm systems Managament and design guide. Available under: http://www.equistar.com/TechLit/Tech%20Topics/Equistar%20Industry%20Papers/Alarm_Systems_Management.pdf. [11.01.2007]

/88/ Honeywell (2006). Alarm Management. Available under: http://hpsweb.honeywell.com/Cultures/en-US/Products/ControlApplications/AlarmManagement/default.htm [11.01.2007].

/89/ Nimmo, I. (2002). It's time to consider Human factors in Alarm Management. Available under: http://www.mycontrolroom.com/sitedata/articles/archive/Human%20Factors%20in%20Alarm%20Management.pdf [11.01.2007].

/90/ MaTSU (1999). Summary guide to safety climate tools. HSE Offshore Technology Report 1999/063. Available under: http://www.hse.gov.uk/RESEARCH/otopdf/1999/oto99063.pdf [13.04.2007].

/91/ Lardner, R. (2003). Safety Culture Application Guide. PRISM FG1. The Keil Centre.

/92/ U.S. Chemical Safety and Hazard Investigation Board (2007). Investigation report. Refinery explosion and fire. Report No.2005-04-I-TX.

/93/ HSE (2004). Core topic 2: HF in accident investigation. Available under: http://www.hse.gov.uk/humanfactors/comah/core2.pdf [13.04.2007]

/94/ HSE (2005). Inspectors toolkit (Draft). Human factors in the management of major accident hazards. Available under: http://213.212.77.20/humanfactors/comah/toolkit.pdf [13.04.2007]

/95/ HSE (2000). Major incident investigation report- BP Grangemouth Scotland: 29th May - 10th June 2000 a public report prepared by the HSE on behalf of competent authority. Available under: http://www.hse.gov.uk/comah/bpgrange/glossary.htm [13.04.2007]

/96/ HSE (1998). Management of alarm systems. Available under: http://www.hse.gov.uk/research/crr_pdf/1998/CRR98166.pdf [13.04.2007]

/97/ Parliamentary Office of Science and Technology (2001). Managing human error. postnote, 156, p. 1-8.

/98/ HSE (n.d.). Humans and risk. HSE Human Factors Briefing Note No. 3. Available under: http://www.hse.gov.uk/humanfactors/comah/03humansrisk.pdf [13.04.2007]

/99/ ISO/TC 159 (2006). Terminology. Unpublished paper

8 Annex I

Table 6: Descriptions of “Cause Human” in the MARS database

MARS Database		
Cause Human		
No.	**Description**	**Frequency**
1	**accidental** inversion	1
2	**act** of negligence	2
3	**arson** (sabotage action), inadequate safeguarding	1
4	**checking** erroneously	1
5	**confusion**	1
6	**control** error, failure to control	1
7	**defective** information system	1
8	defective work permit system	1
9	**disregard** of the risk	1
10	**erroneous** manoeuvring	1
11	erroneous mixture	1
12	erroneous operation	1
13	**external** manipulation	1
14	**failure** of supervision	1
15	failures were not noticed	1
16	**forgotte**n, human error of omission	2
17	**handling** error	1
18	**hazards** underestimated	1
19	**human** error during repair / maintenance	3
20	**inadequate** maintenance works	1
21	inadequate operation procedures	2
22	inadequate plant design	3
23	inadequate procedures	1
24	inadequate process analysis	1
25	Inadequate safety education of operators	1
26	inadequate training/instruction	1
27	**inappropriate** action	1
28	inappropriate design of plant/equipment/system	1
29	**incorrect** operation	1
30	**ineffective** control	1
31	**instruction** wasn't followed by the operator	1
32	instructions have not been respected	1
33	**insufficient** maintenance procedures	1
34	insufficient operational procedures	4
35	insufficient testing/inspection procedures	1
36	insufficient training	3
37	**interchange**	1

5

MARS Database		
Cause Human		
No	**Description**	**Frequency**
38	**lack** of coordination	1
39	lack of maintenance	1
40	**loose** of control	1
41	**loss** of operational process control	1
42	**malicious** act	1
43	**mistake** (of the operator)	4
44	**misunderstanding**	1
45	**not** completely degasified	1
46	not fastened	1
47	not informed	1
48	**operation** against regulations	1
49	operator error	10
50	operator's mistake during demolition of installation	1
51	**over**-charge	1
52	overfilling	1
53	overpressurization	1
54	**procedures** were not fully applied	1
55	**safety** procedures were not suitable	1
56	**storage** mistakes	1
57	**terroristic** action (sabotage).	2
58	**too** long delay in reacting	1
59	**untimely** (wrongly) opened	1
60	**violation** of procedures	1
61	**wrong** connection	1
62	wrong handling / (manipulation)	4
63	wrong inertization	1
64	wrong loading	1
65	wrong manipulation	1
66	wrong mixing operation	1
67	wrong performance of a venting operation	1
68	wrong removal	1
69	wrongly operated	1
70	wrongly set rupture pressure	1
71	wrongly shut	1
72	wrongly supplied	1
	Sum	100

Table 7: NRC Coding Scheme

Categories	Areas	Details
T Training	**T1** Initial **T2** Continuing/requalification **T3** On-the-job training	**100** Training LTA **101** Training process problem **102** Individual knowledge LTA
	T4 Simulator training	**103** Simulator training LTA
P Procedures and Reference Documents	**P1** General operating **P2** Abnormal/off normal/alarm condition **P3** Emergency (EOPs & ERPs) **P4** Reactivity control **P5** Maintenance/modification **P6** Surveillance/calibration/test **P7** Chemical/ radiochemical **P8** Refueling **P9** Administrative **P10** Licensing Documents **P11** Special **P12** Other	**110** No procedure/reference documents **111** Procedure/reference document technical content LTA **112** Procedure/reference document contains human factors deficiencies **113** Procedure/reference document development and maintenance LTA
F Fitness for Duty	**F1** Drugs **F2** Alcohol **F3** Mental/emotional **F4** Fatigue **F5** Unknown/other	**120** Testing LTA **121** Assessment LTA **122** Behavioral observation LTA **123** Self-declaration LTA **124** Training missing/LTA **125** Work hour control **126** Task design/work environment **127** Circadian factors/individual differences **128** Non-compliance **129** Impairment
O Oversight	**O1** Oversight	**130** Inadequate supervision/ command and control **131** Management expectations or directions LTA
R Problem Identification and Resolution R1 Problem	**R1** Problem identification	**140** Problem not completely or accurately identified **141** Problem not properly classified or prioritized **142** Operating experience (OE) review LTA **143** Tracking/trending LTA **144** Audit/self-assessment/effectiveness review LTA
	R2 Problem evaluation	**145** Causal development LTA **146** Evaluation LTA
	R3 Problem resolution	**147** Individual corrective action LTA **148** Action not yet started or untimely **149** No action planned
	R4 Corrective action program	**150** Programmatic deficiency
	R5 Safety conscious work environment	**151** Willingness to raise concerns LTA **152** Preventing and detecting retaliation LTA
C Communication	**C1** Oral **C2** Written	**160** No communication/information not communicated **161** Communication LTA **162** Communication equipment LTA

H Human - System Interface (HSI) and Environment	**H1** HSI components/equipment	**170** HSI or availability/quality LTA
	H2 Simulator	**171** Simulator fidelity LTA **172** Simulator use LTA
	H3 Physical work environment	**173** Physical conditions LTA
W Work Planning and Practices	**W1** Work planning and coordination	**180** Scheduling and planning LTA **181** Inadequate staffing/task allocation **182** Work package quality LTA **183** Pre-job activities LTA **184** Tag outs LTA
	W2 Work practices	**185** Procedural adherence LTA **186** Failure to take action/meet requirements **187** Action implementation LTA **188** Work practice or craft skill LTA **189** Recognition of adverse condition/questioning attitude LTA **190** Failure to stop work/non-conservative decision making **191** Team interactions LTA **192** Work untimely **193** Non-conservative action **194** Housekeeping LTA **195** Logkeeping or log review LTA **196** Independent verification/plant tours LTA
	W3 Awareness/ attention	**197** Self-check LTA **198** Worker distracted/interrupted

Examples of CSB reports of accidents with human contribution:

1. Fire at Formosa Plastics Corporation, Point Comfort, Texas, October 6, 2005

- A worker driving a fork truck towing a trailer under a pipe rack backed into an opening between two columns to turn around.
- When the worker drove forward, the trailer caught on a valve protruding from a strainer in a propylene piping system.
- The trailer pulled the valve and associated pipe out of the strainer, leaving a 1.9-inch diameter opening.
- Pressurized liquid propylene (216 psig) rapidly escaped through the opening and partially vaporized creating both a pool of propylene liquid and a rapidly expanding vapor cloud.
- Control room operators saw the vapour cloud on a closed circuit television and began to shut down the unit.
- Outside operators tried unsuccessfully to reach and close manual valves that could stop the release.
- The vapor cloud ignited.
- A large pool fire burned under the pipe rack and the side of an elevated structure that supported a number of vessels, heat exchangers, and relief valves.
- The fire was extinguished about five days after the start of the incident.

2. Kaltech Industries Group, Inc. Borough of Manhattan, New York April 25, 2002

A chemical reaction caused an explosion when the [nitric] acid was combined with lacquer thinner from another container.

Root Causes:

- There was no compiled list of hazardous chemicals present in the facility.
- Containers of wastes and certain chemicals onsite were not labeled.
- Employees received no formal training on the hazards of specific chemicals in the workplace.
- Material safety data sheets were unavailable to the workforce.
- Waste materials were mixed without being identified or characterized, and no effort was made to determine compatibility among materials.
- Employees received no formal training on proper hazardous waste management practices.

3. West Pharmaceutical Services Dust Explosion and Fire Kinston, NC, January 29, 2003

Root Causes:

- West Pharmaceutical Services, Inc., did not perform an adequate engineering assessment of the use of powdered zinc stearate and polyethylene as antitack agents in the rubber batchoff process.
- The company's engineering management systems did not ensure that relevant industrial fire safety standards were consulted.
- The company's management systems for reviewing MSDSs did not identify combustible dust hazards.
- The hazard communication program at the Kinston facility did not identify combustible dust hazards or make the workforce aware of such.

9 ANNEX II

INSAG key issues in safety culture (/47/, p. 5ff)

Commitment: "Commitment to safety and to the strengthening of safety culture at the top of an organization is the first and vital ingredient in achieving excellent safety performance. This means that safety (and particularly nuclear safety) is put clearly and unequivocally in first place in requirements from the top of the organization, and there is absolute clarity about the organization's safety philosophy. However, true commitment to the enhancement of safety means more than writing a policy statement and mentioning the importance of safety in speeches by senior staff. Although these are vital steps, most people are adept at spotting mismatches between fine words and reality. Commitment means not only providing leadership but also developing, in partnership with staff and their representatives, the means of translating the safety goals of the organization into day to day reality. This latter step provides the visible evidence that aspirations are really held. It means genuinely devoting time and resources to safety and requires that senior managers are trained and, in particular, have the necessary competence in matters relating to nuclear safety" /47/, p.5.

Use of procedures: "Management systems require clearly written procedures that are fit for their purpose to control all aspects of nuclear and radiological safety. However, there is a great difference between having excellent procedures on paper and having procedures that are understood and applied consistently and conscientiously by all staff. There is a need for balance in the number and extent of procedures. They should identify and address the main risks and be intelligible and of relevance to those who will use them. In particular, the rules and procedures, reinforced by training, need to bring out clearly to the workforce the reasons for particular requirements, since only then will the procedures pass the test of relevance required by the operator if he or she is to be fully committed to their use. In other words, it is essential that employees' perceptions of risk are such that the requirements placed upon them are seen to be necessary and relevant. If procedures are not valued, shortcuts or 'workarounds' will begin to be practised. This could lead to further degradation of safety standards, since working around a requirement which is not a prime safety requirement can quickly lead to a culture in which even vital and fundamental safety procedures are no longer viewed as sacrosanct. The important conclusion from this is that simple intelligible procedures should be in place for work which needs to be controlled. These procedures ought to be in a form that can be used directly at the place of work." /47/, p.6.

Conservative decision making: "INSAG-4 [1] referred to a questioning attitude and a rigorous and prudent approach. Well tested systems relying on defence in depth and supported by procedural requirements will protect employees and the public from radiation hazards. It is easy, therefore, for the workforce to develop the attitude that safe conditions are provided for them by others, and that events at other plants are exceptional and isolated and could not occur at their plant. It is therefore essential that everyone connected with nuclear safety be constantly reminded of the potential consequences of failing to give safety absolute priority. Most incidents and accidents in the nuclear industry have occurred because someone has failed to take the relevant precautions or has failed to consider or question in a conservative way decisions that they have made or the steps which were taken to implement them. In practice, it is important that there should be a requirement for each individual or team to stop

and review safety before starting a piece of work or beginning to carry out a procedure. Various techniques have been developed, including the STAR (stop, think, act, review) principle. They all have one feature in common: the need to be conservative in safety related matters by staff checking their understanding of a situation (and if necessary seeking more information or advice) and by assuming that the worst could happen. To take a conservative course of action is not always easy, particularly when there are operational pressures, and this is when an organization's priorities have to be clear and genuinely accepted. To develop and reinforce this culture, employees should be praised if they stop work or do not approve modifications because there is a reasonable doubt about the safety implications." /47/, p.7.

A reporting culture: "Failures and 'near misses' are considered by organizations with good safety cultures as lessons which can be used to avoid more serious events. There is thus a strong drive to ensure that all events which have the potential to be instructive are reported and investigated to discover the root causes, and that timely feedback is given on the findings and remedial actions, both to the work groups involved and to others in the organization or industry who might experience the same problem. This 'horizontal' communication is particularly important. Near misses are also very important because they usually present a greater variety and volume of information for learning. To achieve this, all employees need to be encouraged to report even minor concerns. This raises the important question of 'blame free' reporting. If employees are to report near misses, they must believe that these reports are valued and that they and their colleagues will not be penalized or disciplined as a result of coming forward to make them. There will, of course, be situations in which some action needs to be taken in relation to an individual as a result of an incident. One example would be a willful act; another, the deliberate contravention of a procedure which is known to be workable, intelligible and correct. Sometimes retraining may be necessary. A more difficult issue arises when a conscientious worker makes repeated mistakes which cannot be corrected by coaching and retraining. However, in a good reporting culture, it is accepted that it is the failure to report any issue that may adversely affect safety which is unacceptable. A good reporting culture will be regarded by staff as 'just' and will be built on an atmosphere of trust. This open and responsive approach to reporting and following up also has implications for regulators. For example, they may become aware of a greater number of 'failures' reported by the operating organization as such a system is developed and may be tempted to take action as a result. It is vital that a balanced view be taken, however, since overreaction could stifle developments which in the longer term will lead to real and sustainable enhancements in safety." /47/, p.8.

Challenging unsafe acts and conditions: "Nearly all events, ranging from industrial and radiological accidents, incidents and near misses to failures affecting nuclear safety, start with an unintentionally unsafe act or an unacceptable plant condition or process. These have often been latent and have gone undetected or been treated as 'custom and practice' and therefore been ignored. Then, in combination with another challenge to the system, a further more significant failure occurs. Minimizing existing latent shortcomings in working practices or plant conditions is therefore vital in avoiding more serious events. Minimizing latent shortcomings requires knowledge on the part of plant employees and contractors about why specific safety systems and requirements are in place, and about the importance of each item of plant in contributing to safety. Not only should they be suitably qualified and experienced for their particular areas of specialization, but they must be encouraged to challenge potentially unsafe practices and identify deficiencies wherever and whenever they en-

counter them. In addition to knowledge about the safety significance of plant, systems and procedures, they must be helped to develop the confidence to challenge others if they observe shortcomings in safety performance. This needs to be done in a constructive way and combined with praise for good safety performance. Regulators, also, should be aware of why safety systems and requirements defined by plant management are in place, and why they are important. Regulators must also be particularly careful to ensure regulatory actions taken to correct deficiencies do not impede continued improvements in safety culture. For example, employees must still 'own' their procedures and the procedures must continue to be seen by employees as being fit for their purpose. Failure to challenge, particularly by managers and supervisors, not only fails to eliminate the particular shortcoming in performance which has been observed, but also creates a culture in which failures, oversights and shortcuts become the norm. This is well captured by the phrase 'to tolerate is to validate'." /47/, p.9.

The learning organization: "If an organization stops searching for improvements and new ideas by means of benchmarking and seeking out best practice, there is a danger that it will slip backwards. A learning organization is able to tap into the ideas, energy and concerns of those at all levels in the organization. Enhancements in safety are sustained by ensuring that the benefits obtained from improvements are widely recognized by individuals and teams, and this in turn leads to even greater commitment and identification with the process of improving safety culture. Ideally, all employees are involved in proactively contributing ideas for improvement, and are encouraged to become aware of what world class performance in terms of safety means in their jobs. They contribute not because they are *told* to do so but because they *want* to do so. To do this, staff need to be given the opportunity to compare how they do things with how other workers do, so that they are aware of what constitutes excellence in their field of work. To generate a sense of achievement, they need to be enabled themselves to carry out, wherever it is safe and sensible for them to do so, the improvements which they have identified, and to do so with the evident encouragement and the full backing of management. It is necessary to provide mechanisms to enable experience and ideas to be transferred within the organization. It is also necessary to have formal systems for monitoring and providing feedback to management so that they know the effectiveness of the improvements that have been carried out and for ensuring that the organization retains 'corporate memory' of why and how improvements have been made. Although employees often concentrate initially on industrial safety and issues relating to plant conditions, involvement in and commitment to the improvement process is likely to lead to a wider appreciation of issues of nuclear safety and environmental issues, and to have broader benefits for the business in promoting a culture of active involvement and teamwork. Schemes which encourage staff to provide ideas for improvement are valuable. Sometimes they can lead to either a team being rewarded or donations being made to good causes. However, experience shows that such schemes tend to lose momentum and to become less effective with time. More sustainable approaches involve encouraging staff to work as teams and continually to seek improvements by identifying prioritized actions to enhance safety in their own work areas." /47/, p.10.

Underpinning issues: communication, clear priorities and organization: "In addition to the specific issues discussed earlier, there are three prerequisites which underpin all of these questions. The first is that of establishing good communication about safety issues. This involves the three elements of communication: transmission, reception and verification. Various methods can be valuable, from oral team briefings to dedicated written safety communications, but there is little doubt that

face to face communication, achieved with high visibility of managers and supervisors at the place of work, has the greatest effect. It is sometimes found that, even when managers are able to provide evidence that they have transmitted a message concerning safety, it is the perception of employees that they have not received adequate information or that they do not recognize its significance to them. This means that the form of transmission is inappropriate, that there is insufficient clarity or that the message is not being welcomed by those receiving it. It is thus important to check that messages not only have been sent but also have been received and understood, and are being acted upon. It is also important to ensure that communication with regulatory bodies is carried out using the same principles. The second issue is that of ensuring that a sense of reality is retained about what can be achieved and on what timescales. Many programmes of safety enhancement have faltered because of a failure to deliver agreed objectives. The key prerequisite here seems to be one of prioritization. Providing 'wish lists' of improvements, which are not delivered or are only partly implemented because clear priorities have not been agreed, not only fails to deliver real improvement but also encourages cynicism and a feeling of initiative overload, and ultimately results in a loss of momentum in the process of safety enhancement. In discussions with staff and contractors, it is important that realistic objectives and timescales are set, and that efforts to achieve these are then properly resourced. Plans for enhancement or improvement need to be prioritized, with feedback to regulatory bodies and employees on why certain activities have been selected for implementation while others have not been given the same priority. One important way of signaling intent and providing a vehicle for change is the deployment of a plan to improve safety. To be effective this must be prioritized, reflect any changes in priority (i.e. be a living document) and, very importantly, be developed and widely shared with the workforce. It is also vital that such a plan should identify measures of success and be clear about timescales and accountabilities. The third underlying issue is that of achieving and maintaining clarity about the organizational structure and accountability for what is to be done. People need to know what their task is in the organization, and how their skills and knowledge are to be used in achieving and maintaining its goals. All team members need to know and respect the inputs expected of the other members, and of those, such as contractors, who are working alongside them. This is particularly important in periods of rapid organizational change." /47/, p.11ff.

10 ANNEX III

10.1 Namur Empfehlung (Namur recommendation) 31 – Most Relevant Recommendations

Requirements for safety instrumented systems

In particular definitions have to be made for (NE 31):

- Safety objective
- Function of the safety instrumented system
- Conceptual process design (Principle)
- Nature and frequency of the scheduled functional testing
- Other organizational measures (for instance scheduled maintenance)

The necessary risk reduction to meet the tolerable risk level and the safety related availability of the safety instrumented system have to be taken into consideration when defining the safety instrumented system.

"Basic requirements:
The safety instrumented system class A has to be designed and operated in such a way that in case of one covert fault assumed to be probably to occur within the protective equipment the scope of protection is still achieved."

The safety related availability has to be selected in such a way that even in case of a covert fault the risk (R) to be covered is reduced below the risk limit (RI) down to the remaining risk (Rr).
The safety related availability of protective systems depends on

- the failure rate due to covert faults,
- average time for detection and eliminating covert faults,
- degree of redundancy of the safety instrumented system

Fundamentals:

- Proven and reliable equipment and installation techniques have to be selected, the safety instrumented system has to be simple and clear. The effects of faults (for instance consecutive faults within the safety instrumented system) have to be limited as much as possible by suitable fault suppression barriers
- Harmful influences by environment and by the product such as: Vibration, mechanical impact or stress, temperature influence, corrosion, contamination, fouling, electromagnetic influence have to be taken into account.
- The principle of normally closed contacts has to be applied as often as possible and one has to make use of the fail safe properties of the equipment (for instance final control elements with fail safe position by means of a spring)
- If safety instrumented systems share equipment with Basic process control systems and monitoring systems the following criteria have to be applied: the protective function overrides all other functions, the design of this equipment should be governed by the rules for the design of safety instrumented systems, in accordance with the safety problem the measurement of the safety related process value, the signal treatment and the actuation of the protective function has to be accurate and fast enough.

- The measuring range for the safety related process value has to be selected in such a way that it provides a sufficient resolution. The limit values should be so distant from the end of the range that in case of erroneous measurements within the tolerable limits a reliable resolution can be guarantied.
- The correct adjustment of the limit values has to be protected against involuntary manipulation.
- Any automatic restart after a reaction of the safety instrumented system should normally be blocked.
- All essential components of the safety instrumented system should be accordingly tagged in the documentation, in the field, in the switchgear room and in the control room, in order to draw attention to its special service, whenever an intervention in the plant is necessary.

Functional testing is required to detect covert faults. The check procedure must contain indications of the specified status and reactions of the safety instrumented system as well as a description of the features and functions to be checked. In particular indications of limit values, ranges and other specified characteristics like travel time of valves, delay times for initiating signals or similar features which are essential to fulfil the protection task, belong to this content. The sequence of checks to be performed shall be described in a manner easily understandable to the checking personnel. The check procedure has to be agreed upon between the plant management and the specialists of the instrument department. The limit values have to be provided to the instrument department the plant management in written form.

The frequency of functional testing procedures shall be determined in the general safety review. Due to the difference in availability it may be necessary to check parts of the system more frequently than others. If no comparable experience is available, the check frequency has to be set appropriately high. If a sufficient safety related availability results from the checks, the check frequency can be decreased over the time the plant is operating. As a minimum in analogy to prevailing and pertaining technical rules a check of the total safety instrumented system from sensor to actuator has to be performed once a year (Source: AD-Merkblatt A6, TRbF).

A check has also to be performed after a longer shut-off of the plant and after any repair of the safety instrumented system. Any measures of inspection, maintenance and repair of safety instrumented systems must be documented (see also § 2 (2) of German legal regulation for incidents in industrial activities). Particularly functional testing must be documented with the following information as a minimum:

- Name of the object which has been checked
- Result of check and details of repair if any
- Date of the check Signature of the person who carried out the check
- Signature of the plant operator

10.2 IEC/EN/DIN 61511 - Required Consideration of Human Factors

Contents and requirements of IEC 61511 with respect to Operator action, consideration of HF and HF-SIS-interfaces

IEC 61511 consists of the following parts, under the general title “Functional safety: Safety Instrumented Systems for the process industry sector”:

- Part 1: Framework, definitions, system, hardware and software requirements
- Part 2: Guidelines in the application of IEC 61511-1
- Part 3: Guidance for the determination of the required safety integrity levels

IEC 61511-1

1 Scope

...In particular this standard

...

w) requires that the design of a safety instrumented function takes into account human factors;

x) does not place any direct requirements on the individual operator or maintenance person.

3.2.72 safety instrumented system (SIS)

NOTE 5: When a human action is a part of an SIS, the availability and reliability of the operator action must be specified in the SRS and included in the performance calculations for the SIS. See IEC 61511-2 for guidance on how to include operator availability and reliability in SIL calculations.

5.2.2.2 Competence of persons

As a minimum, the following items should be addressed when considering the competence of persons, departments, organizations or other units involved in safety life-cycle activities:

a) engineering knowledge, training and experience appropriate to the process application;

b) engineering knowledge, training and experience appropriate to the applicable technology used (e.g., electrical, electronic or programmable electronic);

c) engineering knowledge, training and experience appropriate to the sensors and final elements ;

d) safety engineering knowledge (e.g., process safety analysis);

e) knowledge of the legal and safety regulatory requirements;

f) adequate management and leadership skills appropriate to their role in safety life-cycle activities;

g) understanding of the potential consequence of an event;

h) the safety integrity level of the safety instrumented functions;

i) the novelty and complexity of the application and the technology.

11.3 Requirements for system behaviour on detection of a fault

Where the above actions depend on an operator taking specific actions in response to an alarm (e.g., opening or closing a valve), then the alarm shall be considered part of the safety instrumented system (i.e., independent of the BPCS).

Where the above actions depend on an operator notifying maintenance to repair a faulty system in response to diagnostic alarm, this diagnostic alarm may be a part of the BPCS but shall be subject to appropriate proof testing and management of change along with the rest of the SIS.

NOTE: The specified action (fault reaction) required to achieve or maintain a safe state should be specified in the safety requirements (see 10.3). It may consist, for example, of the safe shut-down of the process, or of that part of the process which relies, for risk reduction, on the faulty subsystem or other specified mitigation planning.

11.7.1 Operator interface requirements

11.7.1.1

Where the SIS operator interface is via the BPCS operator interface account shall be taken of credible failures that may occur in the BPCS operator interface.

11.7.1.2

The design of the SIS shall minimize the need for operator selection of options and the need to bypass the system while the unit is running. If the design does require the use of operator actions, the design should include facilities to protect against operator error.

NOTE If the operator has to select a particular option, there should be a repeat confirmation step.

11.7.1.3

Bypass switches shall be protected by key locks or passwords to prevent unauthorized use.

11.7.1.4

The SIS status information that is critical to maintaining the SIL shall be available as part of the operator interface. This information may include:

- where the process is in its sequence;
- indication that SIS protective action has occurred;
- indication that a protective function is bypassed;
- indication that automatic action(s) such as degradation of voting and/or fault handling has occurred;
- status of sensors and final control elements;
- the loss of energy where that energy loss impacts safety;
- the results of diagnostics;
- failure of environmental conditioning equipment which is necessary to support the SIS.

11.7.1.5

The SIS operator interface design shall be such as to prevent changes to SIS application software. Where safety information needs to be transmitted from the BPCS to the SIS then systems should be used which can selectively allow writing from the BPCS to specific SIS variables. Equipment or procedures should be applied to confirm the proper selection has been transmitted and received by the SIS and does not compromise the safety functionality of the SIS.

NOTE 1 If the options or bypasses are selected in the BPCS and downloaded to the SIS then failures in the BPCS may interfere with the ability of the SIS to function on demand. If this can occur then the BPCS will become safety related.

NOTE 2 In batch processes a SIS may be used to select different set points or logic functions depending on the recipe being used. In these cases the operator interface may be used to make the required selection.

NOTE 3: Provision of incorrect information from the BPCS to the SIS shall not compromise safety.

IEC 61511-2

8.2.1 Requirements for hazard and risk analysis (guidance to IEC 61511-1 only)

When considering the frequency of demands it may be necessary in some complex cases to undertake a fault tree analysis. This is often necessary where severe consequences only result from simultaneous failure of more than one event (e.g., where relief headers are not designed for worst case relief from all sources). Judgement will need to be made on when operator errors are to be included in the list of events that can cause the hazard and the frequency to be used for such events. Operator error as a demand can often be excluded if the action is subject to permit procedures or lock-off facilities are provided to prevent inadvertent action. Care is also needed where credit is taken for reduction in demand frequency due to operator action. The credit that can be taken will need to be limited by human factors issues such as how quickly action needs to be taken and the complexity of the tasks involved. Where an operator, as a result of an alarm, takes action and the risk reduction claimed is greater than a factor of 10 then the overall system will need to be designed according to IEC 61511-1. The system that undertakes the safety function would then comprise the sensor detecting the hazardous condition, the alarm presentation, the human response and the equipment used by the operator to terminate any hazard. It should be noted that a risk reduction of up to a factor of 10 might be claimed without the need to comply with IEC 61511. Where such claims are made the human factors issues will need to be carefully considered. Any claims for risk reduction from an alarm should be supported by documented description of the necessary response for the alarm and that there is sufficient time for the operator to take the corrective action and assurance that the operator will be trained to take the preventive actions.

11.2.6 Responsibility and influence of operators

The operators, maintenance staff, supervisors and managers all have roles in safe plant operation. However, humans can make errors or be unable to perform a task, just as instruments and equipment are subject to malfunction or failure.

Human performance is therefore a system design element. The human machine interface (HMI) is particularly important in communicating the status of the SIS to operating and maintenance personnel.

Human Reliability Analysis (HRA) identifies conditions that cause people to err and provides estimates of error rates based on past statistics and behavioural studies. Some examples of human error contributing to chemical process safety risk include:
Undetected errors in design;

Errors in operations (e.g., wrong set point);

Improper maintenance (e.g., replacing a valve with one having the incorrect failure action);

Errors in calibrating, testing or interpreting output from control systems;

Failure to respond properly to an emergency.

11.7.1 Operator interface requirements (guidance to IEC 61511-1 only)

The operator interfaces used to communicate information between the operator and the SIS may include:

- Video displays;
- Panels containing lamps, push buttons, and switches;
- Annunciator (visual and audible);
- Printers (should not be the sole method of communication);
- Any combination of these.

a) Video displays

BPCS video displays may share SIS and BPCS functions provided the displayed data is for information only. Safety critical information is additionally displayed via the SIS (e.g., if the operator is part of the safety function).
When operator action is needed during emergency conditions, the update and refresh rates of the operator display should be carried out in accordance with the safety requirements specification.
Video displays relating to the SIS should be clearly identified as such, avoiding ambiguity or potential for operator confusion in an emergency situation.
The BPCS operator interface may be used to provide automatic event logging of safety instrumented functions and BPCS alarming functions.
Conditions to be logged might include the following:
SIS events (such as trip and pre-trip occurrences);
Whenever the SIS is accessed for program changes;
Diagnostics (e.g. discrepancies, etc.).
It is important that the operator be alerted to the bypass of any portion of the SIS via an alarm and / or operating procedure. For example, bypassing the final element in a SIS (e.g., shutoff valve) could be detected via limit switches on the bypass valve that

turn on an alarm on the panel board or by installing seals or mechanical locks on the bypass valve that are managed via operating procedures. It is generally suggested to keep these bypass alarms separate from the BPCS.

b) Panels

Panels should be located to give operators easy access.
Panels should be arranged to ensure that the layout of the push buttons, lamps, gauges, and other information is not confusing to the operator. Shutdown switches for different process units or equipment, which look the same and are grouped together, may result in the wrong equipment being shut down by an operator under stress in an emergency situation. The shutdown switches should be physically separated and their function labelled. Means should be provided to test all lamps.

c) Printers and Logging

Printers connected to the SIS should not compromise the safety instrumented function if the printer fails, is turned off, is disconnected, runs out of paper or behaves abnormally.

Printers are useful to document first up, Sequence of Events (SOE) information, diagnostics, and other events and alarms, with time and date stamping and identification by tag number. Report formatting utilities should be provided.

If printing is a buffered function (information is stored, then printed on demand or on a timed schedule), then the buffer should be sized so that information is not lost, and under no circumstances should SIS functionality be compromised due to filled buffer memory space.

The operator should be given enough information on one display to rapidly convey critical information. Display consistency is important and the methods, alarm conventions and display components used should be consistent with the BPCS displays.

Display layout is also important. Layouts with a large amount of information on one display should be avoided since they may lead to operators misreading data and taking wrong actions. Colours, flashing indicators, and judicious data spacing should be used to guide the operator to important information so as to reduce the possibility of confusion. Messages should be clear, concise and unambiguous.

The display should be designed such that data can be recognized by operators who may be colour blind. For example, conditions shown by red or green colours could also be shown by filled or unfilled graphics.