ECSS-Q-HB-30-03A
14 July 2015

EUROPEAN COOPERATION
ECSS
FOR SPACE STANDARDIZATION

Space product assurance

Human dependability handbook

**ECSS Secretariat
ESA-ESTEC
Requirements and Standards Division
Noordwijk, The Netherlands**

Foreword

This Handbook is one document of the series of ECSS Documents intended to be used as supporting material for ECSS Standards in space projects and applications. ECSS is a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards.

The material in this Handbook is defined in terms of description and recommendation how to organize and perform activities dealing with human dependability.

This handbook has been prepared by the ECSS-Q-HB-30-03A Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

Disclaimer

ECSS does not provide any warranty whatsoever, whether expressed, implied, or statutory, including, but not limited to, any warranty of merchantability or fitness for a particular purpose or any warranty that the contents of the item are error-free. In no respect shall ECSS incur any liability for any damages, including, but not limited to, direct, indirect, special, or consequential damages arising out of, resulting from, or in any way connected to the use of this document, whether or not based upon warranty, business agreement, tort, or otherwise; whether or not injury was sustained by persons or property or otherwise; and whether or not loss was sustained from, or arose out of, the results of, the item, or any services that may be provided by ECSS.

Published by: ESA Requirements and Standards Division
ESTEC, P.O. Box 299,
2200 AG Noordwijk
The Netherlands

Change log

ECSS-Q-HB-30-03A 14 July 2015	First issue

Table of contents

Figures

Tables

Introduction

Space systems always have “human in the loop” such as spacecraft operators in a control centre, test or maintenance staff on a ground or astronauts on board.

Human dependability complements disciplines that concern the interaction of the human element with or within a complex sociotechnical system and its constituents and processes such as human factors engineering (see ECSS-E-ST-10-11C “Human factors engineering” [1]), human systems integration [2], human performance capabilities, human-machine interaction and human-computer interaction in the space domain [3],[4].

Human dependability captures the emerging consensus and nascent effort in the space sector to systematically include the considerations of “human behaviour and performance” in the design, validation and operations of both crewed and un-crewed systems to take benefit of human capabilities and to prevent human errors. Human behaviour and performance can be influenced by various factors, also called precursors (e.g. performance shaping factors), resulting in human errors, or error mitigators, limiting the occurrence or impact of human errors. Human errors can originate from inadequate system design i.e. that ignores or does not properly account for human factor engineering and system operation. Human errors can contribute to or be part of failure or accident scenarios leading to undesirable consequences on a space mission such as loss of mission or as worst case loss of life.

In the space domain, human dependability as a discipline first surfaced during contractor study and policy work in the early 1990s in the product assurance, system safety and knowledge management domain [5],[6] and concerned principles and practices to improve the safety and dependability of space systems by focusing on human error, related design recommendations and root cause analysis [7],[8].

The standards ECSS-Q-ST-30C “Dependability”[9] and ECSS-Q-ST-40C”Safety” [10] define principles and requirements to assess and reduce safety and dependability risks and address aspects of human dependability such as human error failure tolerance and human error analysis to complement FMECA and hazard analysis. The objective of human error analysis is to identify, assess and reduce human errors involved failure scenarios and their consequences. Human error analysis can be implemented through an iterative process, with iterations being determined by the project progress through the different project phases. Human error analysis is not to be seen as the conclusion of an investigation, but rather as a starting point to ensure safety and mission operations success.

The main focus of the handbook is on human dependability associated with humans directly involved in the operations of a space system (“humans” understood here as individual human operator or astronaut or groups of humans i.e. e.g. a crew, a team or an organization including AIT (assembly, integration and test)and launch preparation). This includes and concerns especially the activities related to the planning and implementation of space system control and mission operations from launch to disposal, and can be extended to cover operations such as AIT and launch preparation.

References

[1] ECSS-E-ST-10-11C - Space engineering - Human factors engineering, 31 July 2008

[2] Booher, Harold R. (Ed.) (2003) Handbook of Human Systems Integration. New York: Wiley.

[3] NASA (2010) Human Integration Design Handbook NASA/SP-2010-3407 (Baseline). Washington, D.C.: NASA.

[4] NASA (2011) Space Flight Human-System Standard Vol. 2: Human Factors, Habitability, and Environmental Health NASA-STD-3001,Vol. 2. Washington, D.C.: NASA.

[5] Atkins, R. K. (1990) Human Dependability Requirements, Scope and Implementation at the European Space Agency. Proceedings of the Annual Reliability and Maintainability Symposium, IEEE, pp. 85-89.

[6] Meaker, T. A. (1992) Future role of ESA R&M assurance in space flight operation. Proceedings of the Annual Reliability and Maintainability Symposium, IEEE, pp. 241-242.

[7] Alenia Spazio (1994) Human Dependability Tools, Techniques and Guidelines: Human Error Avoidance Design Guidelines and Root Cause Analysis Method (SD-TUN-AI-351, -353, -351). Noordwijk: ESTEC.

[8] Cojazzi, G. (1993) Root Cause Analysis Methodologies: Selection Criteria and Preliminary Evaluation, ISEI/IE/2443/93, JRC Ispra, Italy: Institute for System Engineering and Informatics.

[9] ECSS-Q-ST-30 – Space product assurance - Dependability, 6 March 2009

[10] ECSS-Q-ST-40 – Space product assurance - Safety, 6 March 2009

1
Scope and objectives

1.1 Scope

The handbook defines the principles and processes of human dependability as integral part of system safety and dependability. The handbook focuses on human behaviour and performance during the different operation situations as for example in a control centre such as handover to routine mission operation, routine mission operation, satellite maintenance or emergency operations.

This handbook illustrates the implementation of human dependability in the system life cycle, where during any project phase there exists the need to systematically include considerations of the:

- Human element as part of the space system,
- Impact of human behaviour and performance on safety and dependability.

Within this scope, the main application areas of the handbook are to support the:

a. Development and validation of space system design during the different project phases,

b. Development, preparation and implementation of space system operations including their support such as the organisation, rules, training etc.

c. Collection of human error data and investigation of incidents or accidents involving human error.

The handbook does not address:

- Design errors: The handbook intends to support design (and therefore in this sense, addresses design errors) regarding the avoidance or mitigation of human errors during operations. However, human error during design development are not considered.
- Quantitative (e.g. probabilistic) analysis of human behaviour and performance: The handbook does not address probabilistic assessment of human errors as input to system level safety and dependability analysis and consideration of probabilistic targets, and
- Intentional malicious acts and security related issues: Dependability and safety deals with “threats to safety and mission success” in terms of failures and human non malicious errors and for the sake of completeness includes “threats to safety and mission success” in terms of malicious actions, which are addressed through security risk analysis. However by definition “human dependability” as presented in this handbook excludes the consideration of “malicious actions” and security related issues i.e. considers only “non-malicious actions” of humans.

The handbook does not directly provide information on some disciplines or subjects, which only indirectly i.e. at the level of PSFs (see section 5) interface with “human dependability”. Therefore the handbook does not provide direct support to “goals” such as:

- optimize information flux in control room during simulations and critical operations,
- manage cultural differences in a team,
- cope with negative group dynamics,

- present best practices and guidelines about team training needs and training methods,
- provide guidelines and best practices concerning planning of shifts,
- present basic theory about team motivation, and
- manage conflict of interests on a project.

1.2 Objectives

The objectives of the handbook are to support:

- Familiarization with human dependability (see section 5 "principles of human dependability"). For details and further reading see listed "references" at the end of each section of the handbook.
- Application of human dependability; (see section 6 "human dependability processes" and 7 "implementation of human dependability in system life cycle").

2 References

Due to the structure of the document, each section includes at its end the references called in it.

The Bibliography at the end of this document contains a list of recommended literature.

3 Terms, definitions and abbreviated terms

3.1 Terms from other standards

a. For the purpose of this document, the terms and definitions from ECSS-S-ST-00-01 apply

b. For the purpose of this document, the terms and definitions from ECSS-Q-ST-40 apply, in particular the following term:

   1. operator error

3.2 Terms specific to the present handbook

3.2.1 automation

design and execution of functions by the technical system that can include functions resulting from the delegation of user's tasks to the system

3.2.2 error mitigator

set of conditions and circumstances that influences in a positive way human performance and the occurrence of a human error

NOTE The conditions and circumstances are best described by the **performance shaping factors** and levels of human performance.

3.2.3 error precursor

set of conditions and circumstances that influences in a negative way human performance and the occurrence of a human error

3.2.4 human dependability

performance of the human constituent element and its influencing factors on system safety, reliability, availability and maintainability

3.2.5 human error

inappropriate or undesirable observable human behaviour with potential impact on safety, dependability or system performance

NOTE Human behaviour can be decomposed into perception, analysis, decision and action.

3.2.6 human error analysis

systematic and documented process of identification and assessment of human errors, and analysis activities supporting the reduction of human errors

3.2.7 human error reduction

elimination, or minimisation and control of existing or potential conditions for human errors

NOTE The conditions and circumstances are best described by the **performance shaping factors** and levels of human performance.

3.2.8 human error type

classification of human errors into slips, lapses or mistakes

NOTE The types of human error are described in section 6.2 on the human dependability concept.

3.2.9 level of human performance

categories of human performances resulting from human cognitive, perceptive or motor behaviour in a given situation

NOTE 1 As an example, categories of human performances can be "skill based", "rule based" and "knowledge based".

NOTE 2 The level of human performance results from the combination of the circumstances and current situation (e.g. routine situation, trained situation, novel situation) and the type of control of the human action (e.g. consciously or automatically).

3.2.10 operator-centred design

approach to human-machine system design and development that focuses, beyond the other technical aims, on making systems usable

3.2.11 performance shaping factor

specific error precursor or error mitigator that influences human performance and the likelihood of occurrence of a human error.

NOTE 1 Performance shaping factors are either error precursors or error mitigators appearing in a failure scenario and enhance or degrade human performance.

NOTE 2 Different performances shaping factors are listed in section 5 of this document.

3.2.12 resilience

ability to anticipate and adapt to the potential for “surprise and error” in complex sociotechnical systems

NOTE Resilience engineering provides a framework for understanding and addressing the context of failures i.e. as a symptom of more in-depth structural problems of a system.

3.2.13 socio-technical system

holistic view of the system including the operators, the organization in which the operator is involved and the technical system operated.

NOTE A socio-technical system is the whole structure including administration, politics, economy and cultural ingredients of an organisation or a project.

3.3 Abbreviated terms

For the purpose of this document, the following abbreviated terms apply:

Abbreviation	**Meaning**
AIT	assembly, integration and testing
FDIR	failure detection, isolation and recovery
FMEA	failure mode effect analysis
FMECA	failure mode effect and criticality analysis
HET	human error type
HFACS	Human Factors Analysis and Classification System
HMI	human-machine interface
HUDEP	human dependability
LHP	level of human performance
O&M	organizational and management
PIF	performance influencing factors
PSF	performance shaping factor
RAMS	reliability, availability, maintainability and safety
SRK	skill, rule, knowledge
VACP	visual, auditory, cognitive and psychomotor

4 Objectives of human dependability

Objectives of human dependability during the space system life cycle include:

- Definition of the role and involvement of the human in the system, for example support selection of an automation strategy, enhancement of system resilience due to operator intervention to prevent incidents or accidents;
- Definition and verification of human dependability requirements on a project such as human error tolerance as part of overall failure tolerance;
- Assessment of safety and dependability risks of a system from design to operation with respect to human behaviour and performance, and identification of their positive and negative contributions to safety and mission success;
- Identification of failure scenarios involving human errors through “human error analysis” as input to safety and dependability analysis and as basis of a “human error reduction”;
- Definition of human error reduction means to drive the definition and implementation of, for example system design and operation requirements, specifications, operation concepts, operation procedures, and operator training requirements;
- Support of the development of operation procedures for normal, emergency and other conditions with respect to human performance and behaviour;
- Collection and reporting of human error data; and
- Support of the investigation of failure scenarios involving human errors.

5 Principles of human dependability

5.1 Human dependability concept

5.1.1 Introduction

Human dependability is based on the following concept. When a human operates a system, human capabilities (skills and knowledge) are exploited. These capabilities have the potential to mitigate expected and unexpected undesired system behaviour, however they can also introduce human errors causing or contributing to failure scenarios of the system.

In a first step, for safety and dependability analysis at functional analysis level there is no need to discriminate how functions are implemented i.e. using hardware, software or humans. Indeed functional failures (loss or degradation of functions) are identified and the associated consequences with their consequence severities are determined.

However, in further steps, at lower level of safety and dependability analysis such as FMECA on the physical design the fact that the function is implemented by hardware or software is considered (see section 6). Similarly, when operations are analysed, the interaction of the human with the rest of the system is investigated.

Technical failures and human errors are inevitable in complex systems. The human performance and the technical system can be seen as functioning as a joint cognitive system [11] with three human relationships:

- Human - environment (technical system),
- Human - human (operating team), and
- Human - itself (work orientation, motivation) and the associated outcome in terms of human performance and the overall socio-technical system one.

In order to prevent or mitigate as much as possible human errors systems need to be designed taking into account human factors engineering considerations (see ECSS-E-ST-10-11C “Human factors engineering” [12]). Proper consideration of human error to achieve the design and operation of a safe and dependable system is based on analysis of human performance and acknowledges the fact that humans err.

Human error analysis addresses the systematic identification and assessment of human functions with the aim of reducing and mitigating human errors. Such human error analyses are an integral part of safety and dependability through the safety and dependability analysis process. However, human dependability analysis has to consider both positive and negative aspects of the human contribution to safety and mission success (as presented in section 5.2). The outcomes of these analyses will, on the one hand, provide recommendations for reducing and mitigating human errors and on the other hand provide recommendations to foster and encourage positive contributions.

Including in an explicit and possible systematic way both types of contributions in failure scenarios is a mean of identifying recommendations for human error prevention, removal and tolerance.

NOTE More information about human error analysis data are provided in the Annex A.

5.1.2 Failure scenario integrating human errors

Failure scenarios describe failures and human error in terms of event propagation from causes to consequences, as shown at Figure 5-1 where the upper part presents for example a human error causing an undesirable event leading to a consequence. The lower part of the Figure 5-1 describes a technical failure followed by human error which leads to an undesirable event and a consequence. Consequences are characterized by their severity.

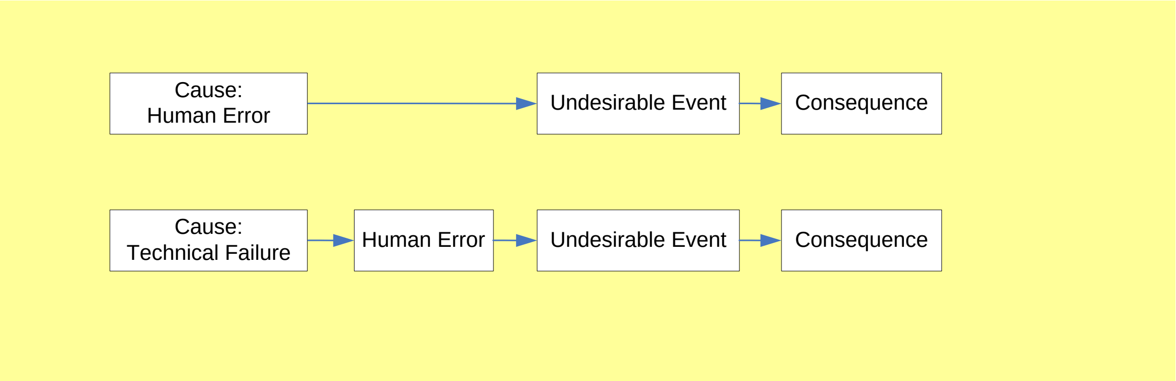


Figure 5-1: Examples of human error in failure scenarios

Space systems with human operator in the loop need to be designed having in mind strengths of the human (such as the mental capability to resolve problems in case of failures in the system) and weaknesses of the human (in particular regarding human error and reaction to technical failures in the system).

Human factors engineering (see ECSS-E-ST-10-11C"Human factors engineering" [12]) deals with the specifics of human performance and how it can be improved. Ergonomics deals with the physical and physiological aspects of the system design and operations while human-computer interaction addresses presentation and interaction aspects when computers are included in the technical system.

5.1.3 Human error and error type

A human error is characterised by a type. For example: the human error event "pressing cancel button inadvertently" can be categorised as the error type "slip". Such categorization is meant to help the analyst in identifying means for preventing their occurrence or mitigating their impact depending on the objectives and levels of the analysis.

5.1.4 Error precursors and error mitigators

5.1.4.1 Overview

Human performance in complex systems is influenced by:

- Performance Shaping Factors (PSF)
- Levels of Human Performance (LHP)

The occurrence of human errors and their propagation in failure scenarios is influenced by error precursors and error mitigators as shown at Figure 5-2. Precursors and mitigators of a human error are the set of conditions and circumstances under which a human behaves and which influence the human performance. They are best described in terms of PSFs and LHPs.

The PSFs and LHPs interfere with each other. For example, the PSF "stress" might not be relevant under "nominal operational conditions" (corresponding to the operations under LHP "skill"). The stress-factor can become more significant when the "normal operational conditions" are changed to "abnormal operation with limited time availability" (corresponding to the operations under LHP "rule") and might become even more important when no rules (e.g. a contingency procedure) are defined for the specific abnormal situation (corresponding to the operations under LHP "knowledge" as the operator has to employ his/her knowledge of the domain to define an operational rule to handle the abnormal situation).

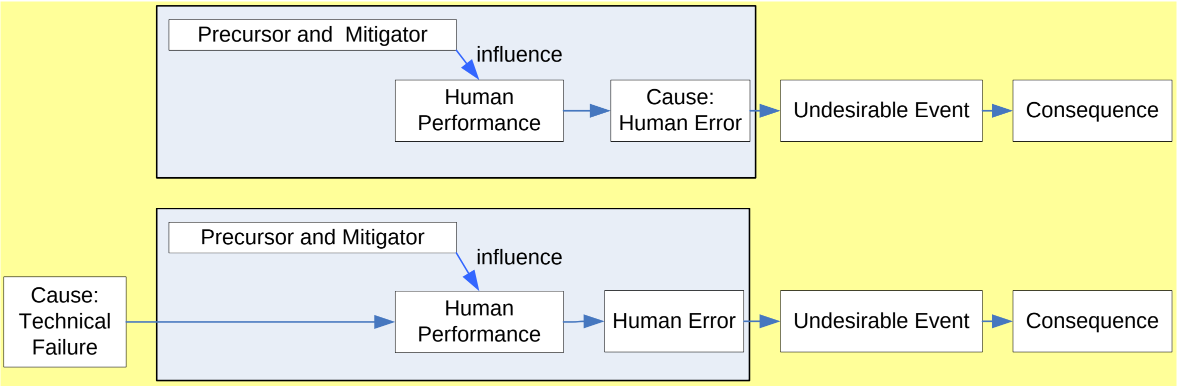


Figure 5-2: Error precursors, error mitigators and human error in failure scenarios

5.1.4.2 Performance shaping factors

Performance shaping factors (PSFs) - sometimes referred as PIF (as Performance Influencing Factors) - can affect human performance in a positive ("help performance") or negative ("hinder performance") manner. It is important to note that some of the PSFs can be considered as meta-PSFs as they influence other PSFs. This is the case, for instance, for the PSF "levels of automation" that influence vigilance, trust, complacency, … as detailed below. PSFs can be broadly grouped into two types [13]:

- **External PSFs** that are external to the operators divided in two groups: organizational and management (O&M) factors and job factors,
- **Internal PSFs** that can be part of operators' internal characteristics, also called personal factors

Another classification of PSF has been proposed in [13] dividing them in "direct" and "indirect". Identifying PSFs according to this classification is important when predicting human error.

- **Direct PSFs** Those PSFs, such as time to complete the task, that can be measured directly, whereby there is a one-to-one relationship between the magnitude of the PSF and that which is measured.
- **Indirect PSFs** Those PSFs, such as fitness for duty, that cannot be measured directly, whereby the magnitude of the PSF can only be determined multivariately or subjectively, or through other measures or PSFs.

Typical external O&M PSFs are as follows:

a. Work or customer pressures (e.g. production vs. safety)

b. Workload (e.g. allocation of work and tasks for personal)

c. Level and nature of supervision and leadership

d. Organization complexity, multi-cultural issues with other partners

e. Communication, with colleagues, supervision, contractor, other

f. Turn-over and training management

g. Manning levels

h. Clarity of roles and responsibilities

i. Working environment (e.g. noise, heat, space, lighting, ventilation, hygiene care, catering)

j. Violations of procedures and rules (e.g. widespread violations)

k. Team or crew dynamics

l. Available staffing and resources

m. Effectiveness of organisational learning (learning from experiences)

n. Safety culture (e.g. everyone breaks the rules)

Typical external job PSFs are as follows:

a. Clarity of signs, signals, instructions and other information

b. System and equipment interface (labelling, alarms, error avoidance, error tolerance)

c. Difficulty and complexity of task

d. Routine or unusual

e. Divided attention

f. Procedures inadequate or inappropriate

g. Preparation for task (e.g. permits, risk assessments, checking)

h. Time available and time pressure

i. Training and experience Tools appropriate for task

j. Usability of the operator interfaces

k. Levels of automation (meta-PSF impacting many of others such as overconfidence, complacency, vigilance)

Typical internal personal PSFs are as follows:

a. Physical capability and condition

b. Fatigue (acute from temporary situation, or chronic)

c. Vigilance

d. Complacency and over-attention

e. Trust or overconfidence and mistrust

f. Stress and morale

g. Peer pressure

h. individual behaviour and character (e.g. anti-authority, impulsiveness, invulnerability, machismo, shyness , hoarding (no sharing of) knowledge)

i. Work overload or under-load (it can be caused also by inadequate personal organization)

j. Competence to deal with circumstances (inept or too skilled)

k. Motivation vs. other priorities

l. Deviation from procedures and rules.

Organizational and Management Factors (O&M) factors are important PSFs that are more and more pointed out in human error prevention and reduction issues [14]. Carefully considering these factors contributes to safety and mission success. To highlight them is a way to involve organizations and all level of management in the process of human error reduction. The manager implication in human error prevention and reduction is crucial because decision makers are most of the time in the best position to argue and take remedial actions taking into account trade-off between finance and risks.

Symptoms on personal (e.g. operator) and management actions due to organizational issues are for example:

a. Lack of personal (e.g. operator) commitment: widespread violations of routine procedures and rules.

b. Lack of management commitment: management decisions that consistently put e.g. "production" or "cost factors" before safety, or a tendency to focussing on the short-term and being highly reactive. Postponing training due to crew resources scarcity is also a latent factor for human error.

As illustrated in Figure 5-3 showing the "Human Factors Analysis and Classification System" HFACS "organizational factors" can influence "management issues" (also referred to as "supervision") which in turn can influence "job and personal factors" (for further details see [15] or [16]).

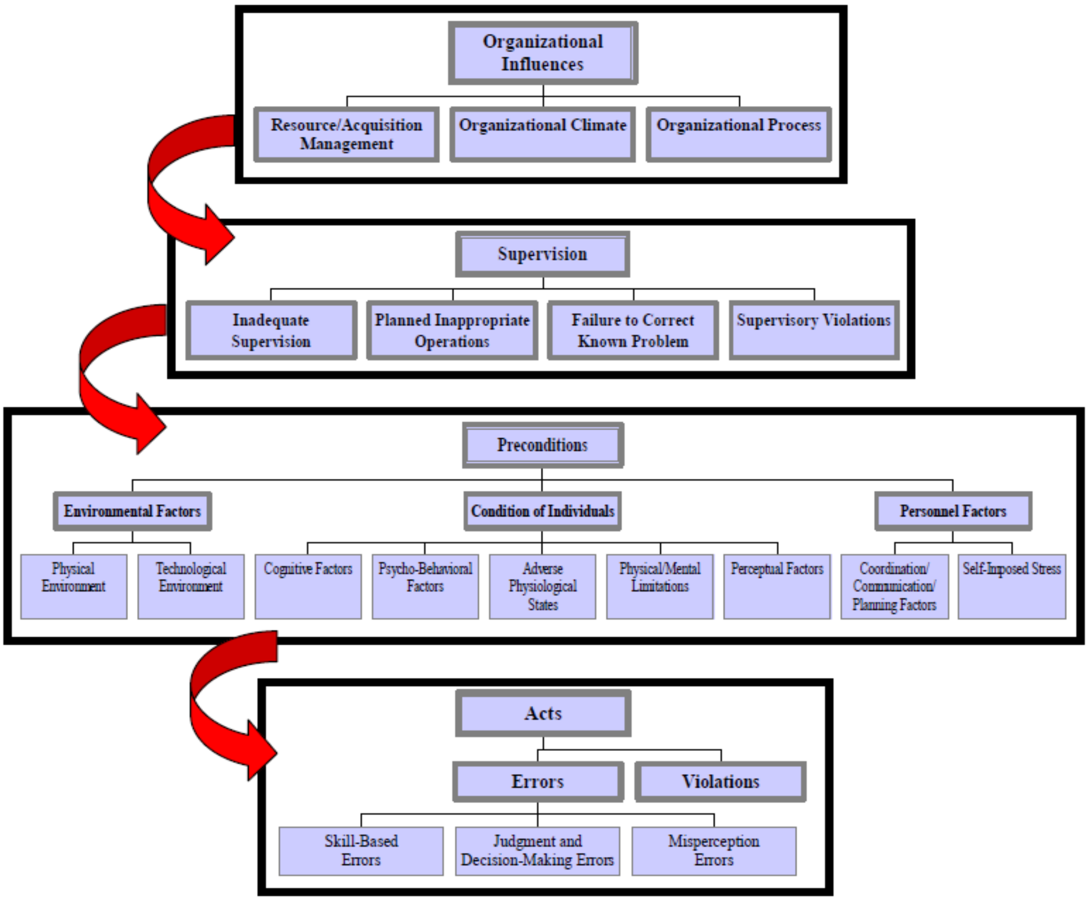


Figure 5-3: HFACS model

Decisions of upper-level management can directly have an effect on lower-level managers or supervisors practices as well as the conditions and actions of the rest of personnel. Consequently, organizational influences can result in a system failure, human error or an unsafe situation. Three categories of possible negative organizational influences can be considered:

a. Resource and acquisition management: this category refers to the management, allocation and maintenance of organizational resources (human or monetary) and equipment/facilities.

b. Organizational climate: this category refers to a broad class of organizational variables that influence worker performance and in general is the usual environment within the organization. This category is related with the Safety Culture or the definition of policies and rules.

c. Organizational process: this category refers to the formal process by which things are done in the organization and includes definition of operations and procedures and control of activities.

On the other hand, four major categories of negative management and supervisory influences can be considered, as showed in Figure 5-3:

a. Inadequate management and supervision: this category refers to those times when management results are inappropriate, improper or cannot occur at all.

b. Planned inappropriate operations: this category affects to the appropriate planning of operational schedule or selection of operators.

c. Failure to correct a known problem: this category refers to deficiencies affecting personnel, equipment, training or procedures that are "known" by the management, but yet they are allowed to continue uncorrected.

d. Management and supervisory violations: this category refers to situations when managers disregard existing rules and regulations.

Understanding these influences is useful for defining recommendations and mitigations means for "O&M factors" (like for instance those indicated in section 5.1.2) that could lead to human errors.

Performance shaping factors can change during a failure scenario and influence how a failure scenario develops. Three types of PSF modifications are considered:

a. Static Condition: PSFs remain constant across the events in a scenario,

b. Dynamic Progression: PSFs evolve across events in a scenario,

c. Dynamic Initiator: a sudden change in a scenario causes changes in the PSFs.

See Annex A for some examples of types of PSF modifications.

This HFACS process highlights Reason's principle of latent and active failures [17]. Indeed, O&M PSFs usually don't play an active role in a human error but they provide the underlying foundations for reducing or increasing human errors occurrence.

5.1.4.3 Level of human performance

5.1.4.3.1 Overview

To simplify the complex human cognitive behaviour three levels of human performance are described as proposed by Jens Rasmussen in [18]:

- Skill Based Performance (S): requires little or no cognitive effort, which is acquired by training or repetition of actions (e.g. changing gears while driving a car).
- Rule Based Performance (R): is driven by procedures or rules, which is already present in the head of the operator (e.g. considering the traffic regulation).
- Knowledge Based Performance (K): requires problem-solving and decision-making that produces new rules that are then executed as presented in rule based section (e.g. identifying a new route to avoid traffic jam).

These levels of human performance (LHPs) can be associated with specific "situations" and "control modes" as shown at Figure 5-4 (excerpt from [19]).

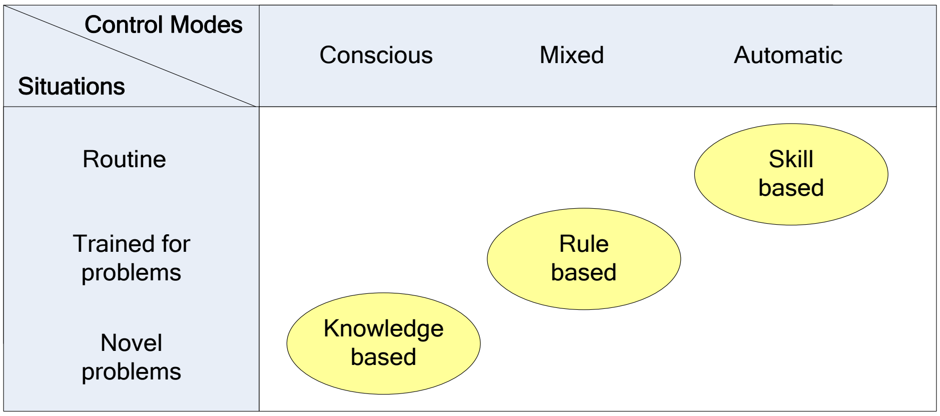


Figure 5-4: Levels of human performance

The modes to control a situation can be further characterized as follows:

a. Conscious mode:
   1. Laborious
   2. Slow and sequential
   3. Error-prone
   4. Potentially very smart

b. Automatic mode:
   1. Unconscious
   2. Fast, parallel operation
   3. Effortless
   4. Highly specialized for routine events

The control mode "mixed" can be also referred to as "subconscious".

Operators can switch from one mode to another one during the same task.

The spectrum of event situations covers:

a. Situations involving routine tasks,

b. Problem situations for which the operator is trained,

c. Situations with problems new to the operator.

5.1.4.3.2 Skill based performance

Skill Based Performance involves the ability to carry out a task using smooth, automated and highly integrated patterns. Triggered by a specific event, the skill-based processing is normally performed without conscious monitoring. During Skilled Based Performance human errors are often caused by attentional slips and/or lapses of memory.

NOTE Skill-based behaviour is characterized by a quasi-instinctive response of the operator, i.e. a close coupling between input signals and output. Skill-based behaviour occurs when an operator is well trained on a particular task, independent of the level of complexity of the task. Skill-based behaviour is characterized by a fast performance and a low number of errors. Example: "getting out of bed", "putting on a T-shirt", or "opening a door" - all of which are unconscious actions one does not need to explicitly "think about" to accomplish.

5.1.4.3.3 Rule based performance

Rule Based Performance is driven by a stored rule or procedure, which has been for example acquired through formal training, provided by other persons' know how, a 'best practice' guide or previous successful experience. The level of conscious control is intermediate between that of the knowledge and skill based behaviour. Rule-Based Errors occur when the wrong rule is chosen due to misperception of the situation or due to misapplication of the rule i.e. a rule-based human error is associated with failure to match the context and problem currently facing the operator. These rules are typically of the "if X then Y" form, can be based, for example, on past experience, and explicit instructions. Therefore during rule based performance human errors are caused by e.g. lack of attention, misapplication of good rules, and application of bad rules.

NOTE Rule-based behaviour is encountered when an operator's action is governed by a set of well-known rules, which the operator follows.

Example: "follow a procedure to repair a car". A major difference between skill-based and rule-based behaviour is in the degree of practice of rules. Since the rules need to be checked, the response of the operator is slower and more prone to errors.

5.1.4.3.4 Knowledge based performance

Knowledge Based Performance is characteristic for unfamiliar or ambiguous situations or where rules are not appropriate (e.g. making strategic decisions, and diagnosis) and applied in an almost completely conscious manner, exerting considerable mental effort to analyse the situation and to identify a solution path. The operator needs to rely on own knowledge of the system and correct interpretation of the problem situation. Errors occur from a lack of or misapplication of knowledge. Therefore during knowledge based performance human errors are e.g. caused by lack of experience or qualification, confirmation bias, and over-confidence.

NOTE If rule based behaviour does not solve a problem, human fall back on knowledge based behaviour in order to produce rules that are then applied.

5.1.4.4 Dependability of human information processing

5.1.4.4.1 General

The SRK model presented in 5.1.4.3 does not exhibit how error type relates to this classification. Figure 5-5 presents how the error types presented above can be connected to these performance levels.

Performance Level	Error Type
Skill-based level	Slips and lapses
Rule-base level	Rule based mistakes
Knowledge-based level	Knowledge-based mistakes

Figure 5-5: Basic error types

Figure 5-5 shows the relation between three basic error types and the three performance levels [19].

The assumption behind that table and the HFACS model is that human information processing is "normally" dependable but external factors can degrade or improve it. However, research in psychology has demonstrated that human information processing can embed unexpected behaviours such as confirmation biases, faulty deductive reasoning or attention tunnelling.

5.1.4.4.2 Confirmation Biases

Confirmation biases (see for instance [20]) corresponds to faulty information search or information interpretation as the new information is modified by existing beliefs or expectations in the operators' mind. For instance, the fact that a system failure occurs regularly and that the operator is used to handle it, when a different failure occur the operator will unconsciously avoid any information that is not similar to the one he is used to process and will carry on managing the new failure as he is used to do it in the usual failure.

5.1.4.4.3 Faulty Deductive Reasoning

Faulty deductive reasoning has been largely studied in particular for explaining how human have difficulties in interpreting statistics [21] as intuitive behaviours interfere with mathematical reasoning. Another common example is the selection task proposed in [22] where subjects are required to identify items to be checked to guarantee that a give rule is true. Despite the fact that the set of items is very small (4 cards in the original test) and the rule is a simple inference (if A then B) only 10% of the subjects find the correct solution.

5.1.4.4.4 Attention Tunnelling

Attention tunnelling has been identified a cause of breakdown in task management. This phenomena corresponds to allocation of attention to a channel of information by the operator for too long a time, with the consequence that other channels of information are ignored or insufficiently taken into account. Incident and accidents have been attributed to this phenomena and studies, such as the one in [23], demonstrate that additional information channels (such as head up displays) can foster the instance of the phenomena (if located close to the centre of visual scan area in a cockpit).

5.2 Human role in the system

5.2.1 Overview

The definition, development, implementation and operation of a system involves the implementation of functions by hardware, software and human. This implementation of functions involves the introduction of automation and considerations of “human versus machine” for function allocation. The goal is to distribute adequately tasks according to their characteristics. An example of automated process in space systems is FDIR (Failure-Detection, Isolation and Recovery) and an example of a human operator implemented approach is the use of contingency procedures performed by the operator.

Next sections highlight some classical roles of the human operators during space operation and some factors impacting the human performances.

5.2.2 Human contribution to safety and mission success

When analysing human behaviour and performance, it is worth remembering that in everyday practice, operators predominantly strive to, and succeed in, making operations work.

The contemporary perspective on human behaviour and performance in complex industrial systems recognises the operator’s positive contribution to the robustness and resilience of an operational system during routine, special and contingency operations [24],[25].

On an individual, team and organisational level, operators positively contribute by [26]:

- monitoring the system’s performance and responding to critical events;
- responding to regular and irregular threats and novel situations in nominal operations;
- staying aware of and anticipating potential disruptions, pressures and their consequences in the near future;
- learning from experience such as incidents.

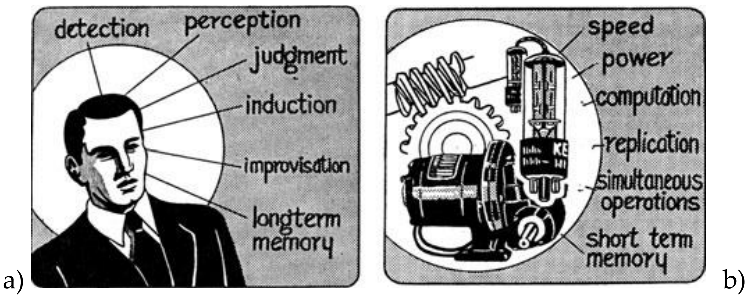
To achieve these tasks above, and in view of changing constraints and demands, operators have to adjust their practices. Particularly at the front-end of operations, this can involve modifying tasks, inserting buffers, creating workarounds and double-checks, or improvising [27].

This so-called performance variability is inevitable, normal and necessary [28]. It represents the difference between formal operating requirements ("work-as-imagined" as captured by "Flight Operations Procedures" or a "Quality Management System") and what actually happens in the operational environment ("work-as-done") [29].

Operator behaviour and performance is a product of the operational environment [30]. Understanding how actual operator practices contribute to successful normal functioning of an operational system is essential to analysing how failures unfold as for example during investigation of failures involving human error.

5.2.3 Fundamental principles driving function allocation

Operations in complex system usually involve repetitive actions that have to be performed in a systematic and reliable way. Humans and machine possess different capabilities making them more complementary than concurrent. In automated systems, function allocation between human and machine has always been a point of controversy. In the context of automation, "function allocation" means that the actor, (either being human or machine), that is best suited should be responsible of performing the function such as according to the MABA-MABA principle ("Men Are Better At" – "Machines Are Better At" depicted in Figure 5-6 [31].



MABA – MABA
Men Are Better At – Machines Are Better At

🔴	Speed	🟢
🔴	Memory	🟢
🟢	Sensing	🔴
🟢	Perceiving	🔴
🟢	Reasoning	🔴
🔴	Consistency	🟢
🔴	Computation	🟢
🔴	Power Output	🟢
🔴	Information Capacity	🟢

Figure 5-6: MABA-MABA principle

Three levels for implementing design decisions in order to include autonomous behaviours in a system can be discriminated:

- The first level (static level) consists of defining and designing the allocation at design time and to design and build the interactive system according to this allocation of functions. This is for instance the case in the automotive industry with the ABS (anti-lock braking system). This autonomous system prevents vehicles wheel from blocking while the driver is braking. Even though the autonomous system is triggered by the user, its behaviour is "hard coded" and cannot be altered.
- The second level (dynamic execution level) consists in designing and defining flexible and redundant functions as in the aeronautics domain with the auto pilot. All the functions that are available in that autonomous system (such as climbing to a certain altitude) can also be performed manually by the pilot. The decision to allocate the execution of the function to the

autonomous system remains in the hand of the user, but not letting the possibility for the user to define new procedures.

- The third level (definition and dynamic execution level) allows the user to define the behaviour of the automation and also to decide when such autonomous behaviour will be executed. Such level corresponds for instance to the definition and execution of macros in Microsoft Excel or the text styles in Microsoft Word. The third level can be found in space domain as in the context of command and control systems for satellite control rooms. Indeed, in case of malfunction the operator is required to define a procedure in charge of solving the identified problem. Such procedures are then tested and executed either in an autonomous or manual way. However, even in the case of autonomous execution some information might be required from the operator to complete the execution. Such information can be values of some parameters (presented on some display units) of the satellite or "go" or "no go" that contacted experts in the domain of the failure (e.g. propulsion, AOCS, …) have provided to the operator. One of the issues related to that problem is that the information required from the operator can be distributed amongst many displays making this activity cumbersome, time consuming or even error-prone. When difficulties occur due to difficulties of interacting with automation they are known under the term "automation surprises" [32]. Such issues have to be addressed as carefully as the ones related to user interface and interaction design.

5.2.4 Some principles driving user interfaces design

In the early days, the basic design rationale for user interfaces for control rooms was to assign one display to each component to be monitored and one physical input to each command to be sent to one component of the controlled system (see Figure 5-7 as an example). This resulted in very large command and control rooms being rather easy to design and build but rather cumbersome to operate.

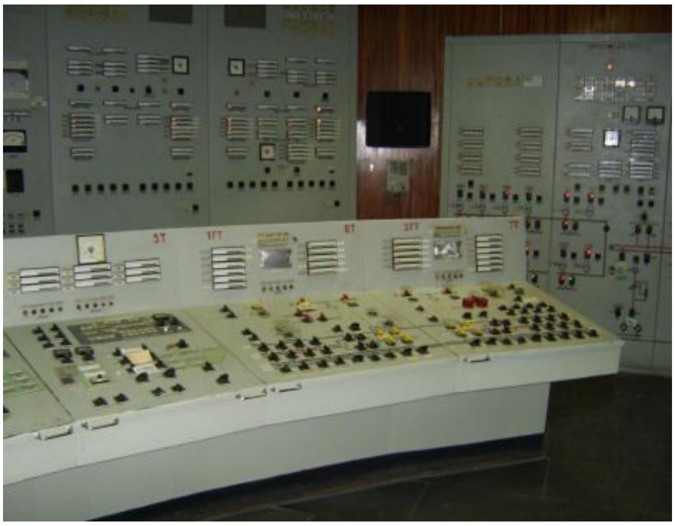


Figure 5-7: Small portion of Chernobyl nuclear power plant control room (from http://www.upandatom.net/Chernobyl.htm)

In order to overcome such constraints, design drivers for command and control systems have been targeting at concentration and integration of both displays and controls. In several domains such as control rooms (see Figure 5-8) and aviation (see Figure 5-9), such concentration was achieved by adding computing resources for concentrating data from multiple displays into a single (or sometimes several in case of large and complex systems) display unit.

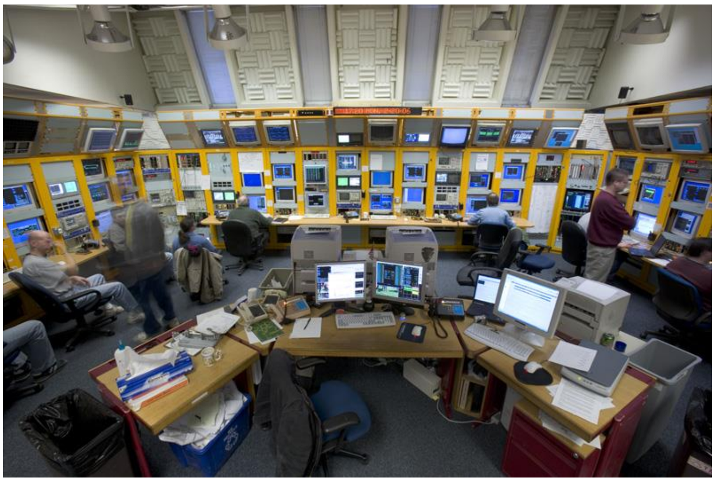


Figure 5-8: Example of a computer-based, concentrated control room (Large Hadron Collider at CERN)

In aeronautics such concentration of display is known under the notion of "glass cockpit" as computer screens were replacing previous analogic displays (such analogic displays can be seen together with the computer screen on the cockpit of a Boeing 747 as shown in Figure 5-9).

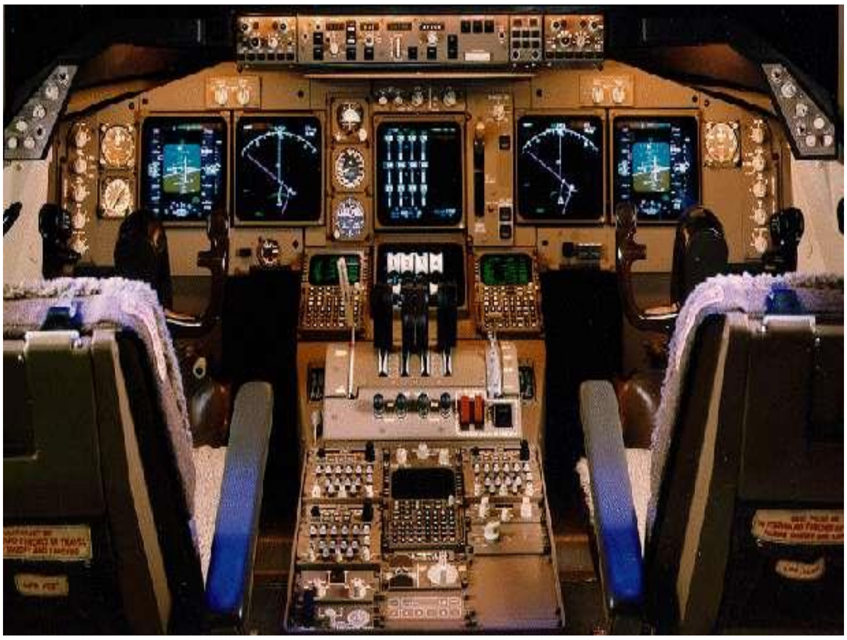


Figure 5-9. Example of a computer-based, concentrated user interface – the glass cockpit (transition to glass cockpit for the Boeing 747)

The benefits of such concentration had significant positive impact on operations, for instance, large commercial aircraft operations evolve from 3 operators to only 2. However, nowadays, operators of safety critical systems are facing more and more sources of information competing for attention which might affect their abilities to complete their tasks. Automation can reduce tasks' complexity and time consumption allowing operators to focus on other tasks. However, too much (or inadequate) automation can lead to complacency, loss of situational awareness, or skill degradation, whereas not enough automation can lead to an unmanageable, unsafe or problematic workload [33]. For instance, SESAR (Single European Sky ATM Research) programme targets at reaching higher levels of automation in aviation in order to improve safety and efficiency of "air traffic management" ATM operations.

"User centred design" approaches (as defined in [34]) support the design of user interfaces that fit the user needs and activities focussing on their usability. At design time, user needs are identified, prototypes are designed, built and evaluated with "real" users. Such iterative processes make it possible to tune and adjust the user interfaces to the user needs, and beyond that, to take into account the evolution of these needs when the new system is introduced. Such approaches are efficient for dealing with static interactive systems i.e. systems for which the use can be defined beforehand with very limited evolutions over time. However, these approaches are of little help when the interactive system has to exhibit autonomous behaviour in order to handle some tasks previously performed by the operators. Work on function allocation (see for example [35] or [36]) aims at supporting the design of automation and more precisely at identifying and assessing candidate functions to be automated.

5.2.5 Automated processes and operator tasks in space systems

This section proposes as a matter of illustration typical examples of space systems functions implemented either as operators tasks or automated processes, that is FDIR, automated telecommanding, automated checks, and manual instructions.

FDIR (Failure-Detection, -Isolation and Recovery): FDIR is the automated part of the management of failures occurring or manifested during the exploitation of space systems and comprises:

- Detection: detection of failure (i.e. "something wrong happens")
- Isolation: involves both "physical isolation" (prevent propagation and further damage), and "logical isolation" (identification of which part, element, equipment etc. is concerned), and
- Recovery: switch to the best possible acceptable mode and configuration e.g.,
  - Automated Safety modes of on-board (subsystems): all or part of the space system is put and maintained in a degraded mode where survival and safety are preserved to the maximum possible extent but the mission is interrupted, waiting for further investigation and actions from operators,
  - Automated switching of redundant components on-board or on ground: automated switching to a redundancy is performed to increase the system stability, availability and performance and avoid subsequent failures from the same cause.

NOTE FDIR is very important to consider in the context of human dependability because:

- the definition of FDIR as an automated process must take into consideration the principles underlying the allocation between automated processes and operator tasks, as addressed in this handbook:
- FDIR deals with failures, including possibly any anomaly due to human errors (i.e., FDIR will or can react, on purpose or not, to failures involving human errors, and interact with further operator understanding and actions),
- FDIR must always be followed by additional investigation and actions from the operators.

Automated Telecommanding: is the process of commanding a spacecraft without operator involvement (partially or fully automated) and includes:

- Routine tasks (on-board and ground system)
- Routine checks (on-board and ground system)
- Common mission related tasks

Automated checks: Automated checks on ground to e.g. pre-process telemetry and provide the operators with information to support the operator tasks to identify anomaly/irregularity (if the detection mechanisms initiates the FDIR it is considered part of FDIR) is an automated process and includes:

- Periodic continuous function monitoring of all mission related telemetry
- Classification with different gradation to assess the relevance of the scenario
- Only visualization of relevant and important information (events warnings and alarms) to keep the attention of the Operator.

Manual instructions: Instructions for the operator to perform operator related tasks include:

- Console procedures
- Contingency procedures
- Fall back concepts/options
- All ongoing i.e. active and valid procedures are reviewed and revised.

Long-term/ mission trend analysis by the operator (e.g. Monitor system performance and degradation)

5.3 References

[11] Woods D.D. (1986): Cognitive technologies: The design of joint human-machine cognitive systems. AI Mag. 6, 4 (January 1986), 86-92

[12] ECSS-E-ST-10-11C – Space Engineering, Human Factors Engineering, 6 March 2009

[13] Boring R. L., Griffith C. D. and Joe J.C. (2007): "The Measure of Human Error: Direct and Indirect Performance Shaping Factors," The 8th IEEE Conference on Human Factors and Power Plants and 13th Conference on Human Performance, Root Cause and Trending (IEEE HFPP and HPRCT), August 2007.)

[14] Reason, J. (1997): Managing the Risks of Organizational Accidents. Ashgate, Farnham

[15] Thompson, W.T., Tvaryanas, A.P., Constable, S.H. (2005): U.S. Military Unmanned Aerial Vehicle Mishaps: Assessment of the Role of Human Factors Using Human Factors Analysis and Classification System (HFACS), HSW-PE-BR-TR-2005-0001. Brooks City-Base, TX: United States Air Force.

[16] RSSB (2008): Understanding Human Factors: A Guide for the Railway Industry. London: Rail Safety and Standards Board.

[17] Reason (1990): Human Error. Cambridge: Cambridge University Press

[18] Rasmussen J. (1983): Skill, Rules, Knowledge: Signals, Signs and Symbols and Other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man and Cybernetics (SMC-13)3:257-266, 1983]:

[19] Reason R. (2008): Reason. The human contribution: unsafe acts, accidents and heroic recoveries. Ashgate 2008 - p. 13

[20] Nickerson R.S. (1998): Confirmation Bias: A Ubiquitous Phenomenon in Many Guise. Review of general psychology, Vol. 2, n°2, 175-220,

[21] Garfield J. and Ahlgren A. (1988): Difficulties in Learning Basic Concepts in Probability and Statistics: Implications for Research. Journal for Research in Mathematics Education, Vol. 19, n°1, pp 44-63, 1988

[22] Wason, P. C. (1966): "Reasoning". In Foss, B. M. New horizons in psychology. Harmondsworth: Penguin

[23] Wickens C. and Alexander A. (2009): Attentional Tunneling and Task Management in Synthetic Vision Displays. International journal of aviation psychology, vol. 19, n°2, 182-199, 2009

[24] Woods D. D., Dekker S., Cook R., Johannesen L., Sarter, N. (2010): Behind Human Error. 2nd Edition. Burlington: Ashgate.

[25] Dekker S. (2005): Ten Questions About Human Error: A New View of Human Factors and System Safety. New York: CRC Press.

[26] Hollnagel E. Nemeth C. P., Dekker S. (Eds.) (2008): Remaining Sensitive to the Possibility of Failure. Resilience Engineering Perspectives, Vol. 1. Burlington: Ashgate.

[27] Dekker, S. (2002): The re-invention of human error. Technical Report 2002-01, Lund: Lunch University School of Aviation, pp. 12-13.

[28] Hollnagel, E. (2003): Extending the Scope of the Human Factor. In: Hollnagel, E. (Ed.) Safer Complex Industrial Environments: A Human Factors Approach. New York: CRC Press, pp. 37-59, here p. 54.

[29] McDonald N. (2006): Organisational Resilience and Industrial Risk. In: Hollnagel, E. et al. (Eds.) Resilience Engineering: Concepts and Precepts. Burlington: Ashgate, pp. 155-180.

[30] Leveson, Nancy G. (2011): Engineering a Safer World: Systems Thinking Applied to Safety. Cambridge, MA: MIT Press, p. 47.

[31] Fitts P.M. (ed) (1951): Human engineering for an effective air navigation and traffic control system. Washington, DC: National Research Council.

[32] Palmer E. (1995) "Oops, it didn't arm." - A Case Study of Two Automation Surprises. 8th International Symposium on Aviation Psychology, Ohio State University, (1995).

[33] Parasuraman R.; Sheridan T.B.; Wickens C.D. "A model for types and levels of human interaction with automation" IEEE Trans. on Systems, Man and Cybernetics, Part A: Systems and Humans, , vol.30, no.3, pp. 286-297, May 2000.

[34] Norman D., Draper S. (eds.) (1986): User Centered System Design: New Perspectives on Human-Computer Interaction. Hillsdale, NJ, Lawrence Erlbaum Associates

[35] Harrison M., Johnson P., and Wright P. (2002): Automating functions in multi-agent control systems: supporting the decision process. In Redmill, F and Anderson, T. editors, Proceedings of the Tenth safety-critical system symposium, Southampton. Springer. pp. 93-106.

[36] Boy G. (1998): Cognitive Function Analysis for Human-Centered Automation of Safety-Critical Systems. Proc. of ACM SIGCHI conference on Human Factors for Computing Systems 1998: 265-272

6 Human dependability processes

6.1 General

The implementation of human dependability on a project is supported by human dependability processes, which address the human-in-the-loop (such as operators, maintainers or astronauts) at any level of the system design and operation regime.

As part of human dependability activities, FMECA, "hazard analysis", "fault tree analysis" (as defined in ECSS documents) and "human error analysis" (as defined in this handbook) are integrated within the system safety and dependability programs.

Human dependability is supported by processes based on different and complementary approaches to deal with human errors such as:

- Analysis of single consequences caused by a single cause ("root cause analysis").
- Analysis of multiple consequences caused by a single cause (FMECA, "event tree analysis").
- Analysis of the multiple causes that lead to a single consequence ("fault tree analysis").
- Analysis of multiple consequences caused by multiple causes ("hazard analysis", HAZOP).

The deterministic analysis methods mentioned above address a limited number of identified postulated or known events (causes or consequences) and to a limited extent to capture the dynamic evolution of events in a system.

In addition to the above deterministic methods probabilistic methods such as "probabilistic risk assessment" PRA and reliability analysis that include considerations of the likelihood of human errors (e.g. "technique for human error rate prediction" THERP [37], "time-reliability correlation" TRC [38], "cognitive reliability and error analysis model" CREAM [39]) exist but are not considered here (see scope of handbook).

Understanding the role of humans in the system i.e. in system operation is important to assess the possibility of humans errors and to establish the appropriate level of automation. Consequently, the results of "task analysis" and the design of the "human machine interface" HMI are inputs to define human error scenarios in "human error analysis". Alternatively, the results of "human error analysis" influence the assignment and definition of human tasks and impact the design of the "human machine interface" HMI in the system.

"Accident investigation" provides another complementary view of human errors as causal elements of accidents. For example, "systems-theoretic accident model and processes" STAMP [40],[41] is an analytical method based on systems theory, which allows more complex relationships between events to be considered (e.g. feedback and other indirect relationships) and also provides a way to look more deeply at why the events occurred. Accident models based on systems theory consider accidents as the result of flawed processes involving interactions among system components and usually do not specify single causal variables or factors i.e. accidents are not conceived as resulting from component failures, but from inadequate control or enforcement of safety related constraints on the design, development, and operation of the system.

The collection and analysis of human error data allows to gain insight into the root causes of incidents or accidents and are subject of "Human error reporting" and "Human error investigation".

This handbook does not shortlist or promote the use of specific processes other than the following as defined in ECSS standards and in this handbook:

- FMECA (see ECSS-Q-ST-30-02 "Failure modes, effects (and criticality) analysis"[42]),
- "Hazard analysis" (see ECSS-Q-ST-40-02 "Hazard analysis"[43]),
- "Fault tree analysis" (see ECSS-Q-ST-40-12 "Fault tree analysis"[44]), and
- "Human error analysis" (see section 6.2).

FMECA, hazard analysis and fault tree analysis allow to integrate human error events into failure scenarios and to describe failures and human error in terms of event propagation from causes to consequences according to the principles defined in section 5.1.2 but without detailed assessment of failure scenarios with human error events down to the level of error precursors and mitigators.

Human error analysis allows the detailed assessment of failure scenarios with human error events down to the level of error precursors and mitigators (see section 6.2).

The process of "Human error reporting and investigation" complements human error analysis (see section 6.3).

These processes selected for supporting human dependability allow to:

- use a common classification scheme where events, causes and consequences are described consistently.
- model the human role in the system.
- model interactive complexity failures by considering the interaction between the different components of the system and the unpredictability of some failure scenarios.
- consider the influence of internal PSFs and external PSFs (O &M factors).
- consider human error analysis as part of and to complement FMECA, hazard analysis and fault tree analysis fully integrated in the safety and dependability life cycle (from design to operation).
- collect human error data.
- investigate failures, incidents or accidents involving human error.

6.2 Human error analysis

6.2.1 Objectives of human error analysis

The general objective of human error analysis is to support the implementation of human dependability in line with the "objectives of human dependability" (see section 4).

The specific objectives of human error analysis with respect to a project specific application are determined under Step 1 of the human error analysis process "Define Analysis Objective and Scope"(see section 6.2.3) and can include:

- Show compliance with safety and dependability requirements e.g. failure tolerance requirements with respect to human error,
- Support to minimize single point failures involving human error,
- Support investigation of failure scenarios involving human errors.

6.2.2 Principles of human error analysis

6.2.2.1 Human error identification and assessment

Human error analysis includes the systematic identification and assessment of human error.

Human error identification comprises the determination of undesirable scenarios involving human error and includes identification of associated error types, precursors, mitigators and reduction measures of human error, technical failures, effects, the consequence and observable symptoms of undesirable events.

Human error assessment includes determination of the severity of consequences of failure scenarios involving human errors.

Human error identification and assessment are the basis for human error reduction and mitigation. Mitigation is considered as part of general system design and not explicitly addressed further in this handbook. Human error reduction is addressed in next section 6.2.2.2.

6.2.2.2 Human error reduction

Human error analysis includes the reduction of human errors after human error identification and assessment have been performed.

Human error reduction is achieved by either elimination of existing or potential conditions for human errors or by minimisation and control of these conditions as shown at Figure 6-1 of human error reductions measures. Human error reduction is achieved by addressing external PSFs and internal PSFs such as O&M factors. Reduction means are derived from the understanding of the PSFs such as O&M conditions and the particular factors resulting from these conditions.

NOTE 1 Human errors can be reduced as part of the overall hazard and failure reduction process commensurate with ECSS-Q-ST-40C [45], ECSS-Q-ST-40-02C [43], ECSS-Q-ST-30C [46] and ECSS-Q-ST-30-02C [42].

NOTE 2 Reduction can be achieved at the level of error precursors and mitigators. Example: reduce stress, introduce two step command, improve operation procedure, improve man-machine interface, and improve training.

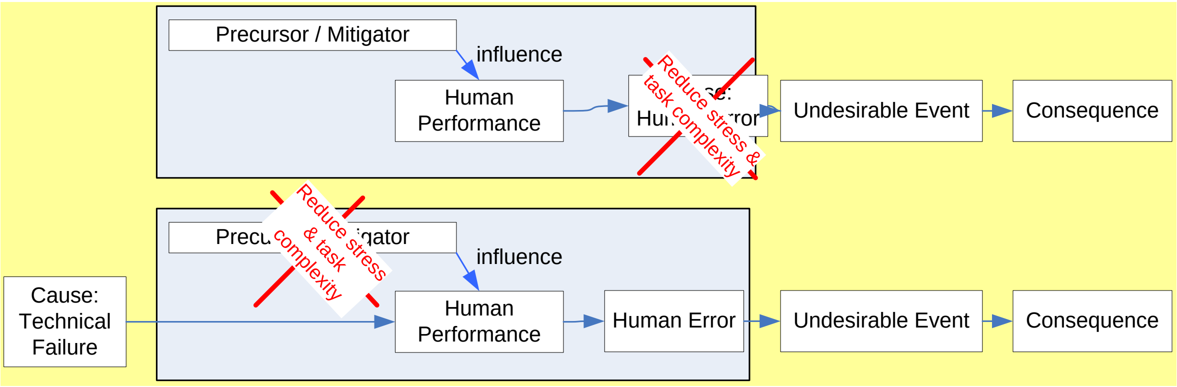


Figure 6-1: Human error reduction examples

Example: O&M factors related human error reduction measures include:

a. Work or customer pressures: this factor is the consequence of the influence of a negative organizational safety culture (e.g. cost and schedule versus safety): definition and implementation of an appropriate and positive safety culture characterised by e.g. communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures.

b. Workload: this factor is often evocated due to planning pressure (e.g. launch date is a drastic constraint and operational teams have often late deliveries to prepare operations). Workload can create motivation and can have a positive influence human performance, but too much workload for a long time can create stress and reduce performance. Managers have to take care of workload and be aware of long workload duration. Listening to teams complaints (i.e.: via reporting including human issues) and stress detectors (as signs of nervousness, irritability, tiredness) can anticipate human defection as demotivation or "burn-out" that can affect the team performance and mission success.

c. Level and nature of supervision and leadership: this factor addresses the influence of management style (e.g. delegation versus authoritarian) of superiors on individuals and their performance.

d. Organization complexity: this factor includes the implications of organisational structures and their complexity and include multi-cultural issues i.e. with European or international cooperation in space programs, the complexity of organization increases.

e. Communication: this factor deals with the influence of the communication style and consequence of communication errors.

f. Turn-over and training management: this factor is associated with developing and maintaining skills and qualification levels.

g. Clarity of roles and responsibilities: this factor is associated with the definition and implementation of team structures and team members "job-descriptions".

h. Working environment: this factor deals with the effects of e.g. noise, heat, space, lighting, ventilation, hygiene care, catering. An ergonomics expert can help on layout of a control centre or an integration room. Collegial complaints about working environment can be addressed to management.

i. Effectiveness of organizational learning from experience: this factor deals with sharing projects lessons learnt (e.g.: human error caused by an unexpected parameterization of an excel sheet update: a decimal value entered with a dot instead of a comma was accepted by monitoring and command on ground software and induced an on-board reconfiguration – warn other projects and check if such a problem can occur).

6.2.2.3 Human error analysis requirements, applicability and interfaces

6.2.2.3.1 Human error analysis requirements

Human error analysis requirements in ECSS safety standards

In ECSS-Q-ST-40C the following requirements are defined with respect to analysing human errors:

a. Human Error Analysis in the requirements 7.5.4.6a, b, and c of ECSS-Q-ST-40C [45]:

a. Whenever safety analyses identify operator errors as a cause of catastrophic or critical hazards, a dedicated analysis shall be carried out.

> b. *The human error analysis shall be used to support the safety analysis for the identification of human operator error modes and their effects and for the definition of adequate countermeasures to prevent or control human operator errors.*
>
> c. *The human error analysis shall be developed from the early phases of the project onwards in order to define recommendations for the hardware and software design, procedure development and training preparation programme.*

b. Failure tolerance requirements explicitly address human errors in requirements 6.4.2.1b and c, of ECSS-Q-ST-40C:

> b. *No single system failure or single operator error shall have critical or catastrophic consequences.*
>
> c. *No combination of two independent system failures or operator errors shall have catastrophic consequences.*

Human error analysis aspects in ECSS dependability standards

In ECSS-Q-ST-30C [46] and ECSS-Q-ST-30-02C [42] the following aspects are defined with respect to analysing human errors:

- Identification of human factors in the technical specifications and how they influence dependability.
- Dependability engineers support to the review of the operations manual and procedures for consistency with dependability analyses.
- Verification that dispositions to minimize failures due to human errors are included in the procedures.
- Analysis of Hardware, Software and Human Functions.
- FMEA to support also the verification of safety analyses, maintainability analysis, tests, maintenance planning and Human Interfaces.
- During phase C/D review of operational procedures to evaluate human reliability problems related to HMI.
- Human Errors are analysed, as needed, with process FMECA or with a functional FMEA.

6.2.2.3.2 Human error analysis applicability

Human error analysis is applicable for:

- Functions implemented involving human operators (e.g. to include maintenance) and aspects of the design and operation where human error failure tolerance requirements are applicable,
- Design and operation involving human operators regarding failure scenarios involving human errors leading to defined consequences,
- Support to the development of operation procedures (e.g. testing, ground handling, control room, contingency procedures, maintenance procedures, training and simulation, and hazardous commands management).

6.2.2.3.3 Human error analysis interfaces

Human error analysis interfaces with:

a. Hazard analysis, fault tree analysis and FMECA with consideration of human error events: the objective is to identify operational scenarios leading to system level consequences of high severity or selected and defined “feared events” and which are therefore classified as e.g. “hazardous” or “critical”. This analysis focuses on driving the design and operation and involves the principles of hazard analysis according to ECSS-Q-ST-40-02C [43] and FMECA according to ECSS-Q-ST-30-02C [42].

b. Common cause analysis: the objective is to identify multiple failures including human errors, which result from common-cause failures and represent single failures for determining failure tolerance.

c. Task analysis: the objective is to identify and analyse tasks within an operation scenario. The tasks are based on e.g. the operational and maintenance procedures. This analysis aims at determining the specific behaviours required from the human performance in a system. It involves e.g. determining the detailed performance required of the human and equipment and the effects of environmental conditions and malfunctions. Within each task to be performed by the human, behavioural steps are analyzed in terms of:

   1. the sensory signals and related perceptions,

   2. information processing, decision-making, memory storage, and other mental processes, and

   3. the required responses.

d. Staffing and qualifications analysis: human error analysis can be input to staffing and qualifications analysis in order to support the determination of how tasks are assigned to operators or maintainers and what overall staffing levels and training are required (Operator Task Analysis and Maintenance Task Analysis).

It is stressed that within functional FMECA and hazard analysis the criticality of system functions is identified in relation to the consequences of functional failures. The result of this type and of this level of safety and dependability analysis of a system is input to decisions on the design implementation of functions using hardware, software and the human.

Human error analysis interfaces with human factors engineering (see ECSS-E-ST-10-11C [47]) at the level of performance shaping factors and human-machine interface.

6.2.2.4 Documentation of human error analysis

Human error analysis is documented to ensure that all associated decisions including main rationales and assumptions are traceable and defensible.

Every step and result of the analysis process is documented in a self-standing analysis report or as part of a safety and dependability analysis report e.g. in a dedicated section.

Annex B of this handbook provides an example of a human error analysis form.

6.2.2.5 Verification, follow up and implementation of human error analysis results

Human error analysis results in terms of recommendations for changes to the design and operation regime i.e. human error reduction actions are implemented, their implementation is verified and followed up as part of overall safety and dependability assurance. This includes for example identifying and following up single point failures involving human error as single point failures or critical items, highlighting non-compliances to failure tolerance requirements of failure scenarios involving human errors.

6.2.3 Human error analysis process

6.2.3.1 Overview

The human error analysis process comprises the steps and tasks necessary to identify, assess and reduce human errors. The steps, which might be iterated during the project evolution - as indicated in Figure 6-2 - are:

a. Step 1: Define Analysis Objective and Scope

Define the objectives, scope and depth of human error analysis, identify applicable requirements and interfacing analyses.

b. Step 2: Perform Analysis - Identify and Assess Human Errors

Identify failure scenarios involving human error i.e. identify human errors, types and effects, undesirable events and consequences, severities and observable symptoms). For a more detailed analysis identify the error precursors and mitigators in addition.

c. Step 3: Use Analysis Results – Reduce Human Errors

Identify human error reduction means, prioritize, implement, verify and track human error reductions.

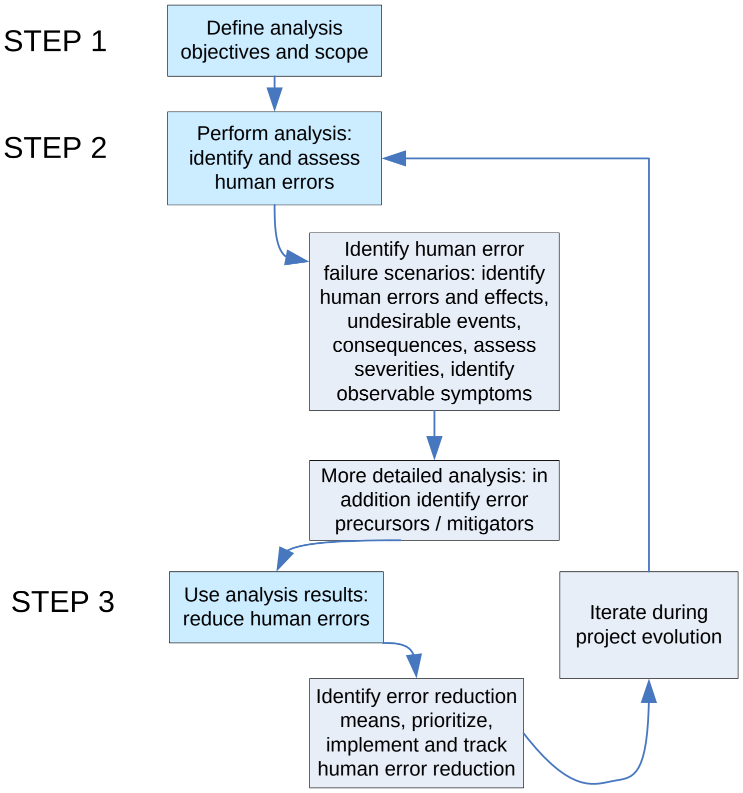

STEP 1
Define analysis objectives and scope
STEP 2
Perform analysis: identify and assess human errors
Identify human error failure scenarios: identify human errors and effects, undesirable events, consequences, assess severities, identify observable symptoms
More detailed analysis: in addition identify error precursors / mitigators
STEP 3
Use analysis results: reduce human errors
Iterate during project evolution
Identify error reduction means, prioritize, implement and track human error reduction

Figure 6-2: Human error analysis and reduction process

6.2.3.2 Steps of human error analysis

6.2.3.2.1 Step 1: "Define Analysis Objective and Scope"

Tasks

Human error analysis is implemented based on single or multiple, i.e. iterative, application of the analysis process. The tasks associated with the individual steps of the analysis process vary according to the scope and objectives specified for the analysis. The scope and objectives of the analysis depend on the type and phase of the project. The results of human error analysis can be input to safety and dependability and drive the system design and operation definition, project reviews and project decisions during the evolution and operation of the system.

a. Task 1-1: Define the human error analysis objectives, scope and depth:

   1. Define the purpose and expected outcome of the analysis, the expected outcome of the analysis varies with the project phase.

      Example: provide input i.e. support safety and dependability analysis for project phase C/D, categorise human errors and define human error reduction means.

   2. Define the design and operational baseline subject to analysis and its boundaries.

      Example: design concept of a control room, spacecraft operation procedure, maintenance procedure.

   3. Define the analysis effort and depth, the implementation of the analysis process might consist of a number of "analysis cycles" over the project's duration, human error analysis can be performed at various levels of depth.

      Example: detailed analysis with identification of failure scenarios involving human operator errors and identification of error precursors and mitigators for tasks in an operation procedure.

b. Task 1-2: Identify applicable requirements and interfacing analyses:

   1. Identify applicable requirements

      Example: human error failure tolerance as part of overall failure tolerance requirements i.e. "*No single system failure or single operator error shall have critical or catastrophic consequences*", consequence severity scheme to categorise human error failure scenarios, customer requirements.

   2. Identify interfacing analysis and identify relevant input data for the analysis

      Example: task analysis, operation hazard analysis, FMECA with scenarios involving human operator.

c. Task 1-3: Define the way to document the analysis results (see section 6.2.2.4 and the example of a human error analysis worksheet in Annex B).

Outputs

Outputs of the Step 1 include:

- Analysis objectives and scope
- Analysis baseline
- Analysis depth
- Applicable requirements
- Interfacing analyses
- Documentation format

6.2.3.2.2 Step 2: “Identify and Assess Human Errors”

Tasks

The identification and assessment of human errors is based on answering the questions “Where are human involved, what can go wrong and what are the consequences?” and “How critical are the human errors?”.

a. Task 2-1: Identify human tasks e.g. using task analysis, flight operation procedures as input.

b. Task 2-2: Identify failure scenarios involving human errors, according to the objectives, scope and depth of the human error analysis:

1. Identify human errors: analyse the operation scenarios, procedure steps or tasks under consideration and identify human error events or - if applicable - combinations of technical failures and human errors. Identify the human error types.

   NOTE 1 Human error can initiate a failure scenario i.e. be the cause of a failure scenario – example: operator error such as operator sends wrong command

   NOTE 2 Human error can also occur after a failure – example: operator error when dealing with a failure situation.

   NOTE 3 The level of failure tolerance can determine the necessity to consider single human error, the combination of two human errors or of human error and a technical failure - example: single failure tolerance or double failure tolerance.

2. Identify the effects of human errors: identify the undesirable events and consequences implied by the human error events. Eventually identify observable symptoms of the effects and undesirable events.

   NOTE 1 The consequence is the final effect, usually at system level - example: an operator error leads to a spacecraft failure and consequently loss of mission, a spacecraft failure followed by an operator error leads to loss of life.

   NOTE 2 The observable symptom is the “visual effect” of an undesirable event - example: smoke in case of a fire.

3. In case of a detailed human error analysis (commensurate with defined scope of analysis): for each human error identify the error precursors and mitigators i.e. analyse the conditions for each human error, identify the relevant performance level and the performance shaping factors.

   NOTE 1 The human performance levels and the performance shaping factors describe the operation situation during a failure scenario – example: routine operation in night shift combined with tiredness: operator presses wrong button.

   NOTE 2 Information in section 5.1 (and Annex A) can be used as input. Other analyses and data from human error data collection and reporting can be used as further input.

c. Task 2-3: Assess human errors:

1. Identify and rank the consequence severities of the failure scenarios involving human error by applying the applicable severity categorization scheme.

   NOTE The consequence severity measures the gravity of the final effect of a human error - example: an operator error scenario leading to loss of mission has severity "critical", the scenario spacecraft failure followed by operator error leading to loss of life is "catastrophic".

Outputs

Outputs of the Step 2 include:

- Failure scenarios involving human error
- Human error events and error types
- Effects, consequences and observable symptoms
- Error precursors and mitigators and performance shaping factors
- Severities
- Ranking

6.2.3.2.3 Step 3: "Reduce Human Errors"

Tasks

Human error reduction is based on answering the question "What can be done to improve?".

a. Task 3-1: Identify human error reduction means.

1. Indicate existing or identify new recommended error reduction means commensurate with the level of analysis.

NOTE 1 Human error reduction can be implemented by elimination or minimization and control of the existing or potential conditions for human errors - example: improve human-machine-interface, reduce night shift duration and introduce or improve training.

NOTE 2 Human error reduction can be implemented by replacing the human in the loop or introduction of human error tolerance - example: operator involvement is substituted by introduction of software based device (automatism), introduction of two-step commands such as. arm and fire to control single point failure as for example operator error - "operator sends wrong command leads to loss of mission".

NOTE 3 Human error reduction can be achieved at the level of performance shaping factors – example: reduce night shift duration.

b. Task 3-2: Prioritize, implement, verify and track human error reduction.

1. Use the classification of human error scenarios to prioritize and implement the recommendations and actions.

2. Identify verification means for the implementation (such as review of improved procedure, and check training certificate). Subject human error reduction to verification, tracking and close-out.

The implementation, verification, follow up and close out of recommendations and actions can be part of overall safety and dependability work – example: as part of the RAMS Recommendations Log.

Outputs

Outputs of the Step 3 include:

- Human error reduction means
- Human error reduction implementation
- Verification, tracking, follow up and close out

6.2.3.3 Iteration of human error analysis during project evolution

Commensurate with the objectives of human dependability during the project evolution human error analysis is performed in an iterative way during the project evolution with various analysis objectives and depths as indicated in Figure 6-3. Human error analysis activities differ according to the type of project and required effort, such as e.g. an analysis of a maintenance procedure at sub supplier level, of a control room design and operation of a human or unmanned mission as input to system safety and dependability efforts at supplier level.

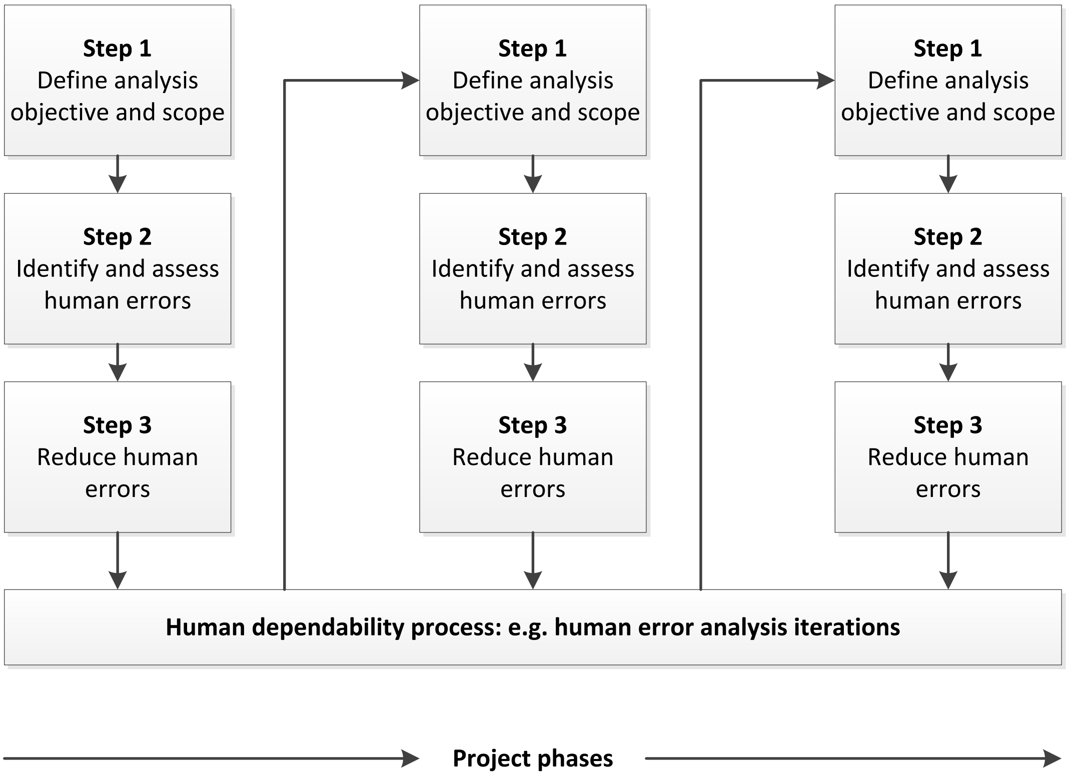

Step 1
Define analysis objective and scope
Step 2
Identify and assess human errors
Step 3
Reduce human errors
Step 1
Define analysis objective and scope
Step 2
Identify and assess human errors
Step 3
Reduce human errors
Step 1
Define analysis objective and scope
Step 2
Identify and assess human errors
Step 3
Reduce human errors
Human dependability process: e.g. human error analysis iterations
Project phases

Figure 6-3: Human error analysis iteration

6.3 Human error reporting and investigation

6.3.1 Objectives of human error reporting and investigation

The prime objectives of human error reporting and human error investigation are to:

- collect human error data as input for human error analyses and as prerequisite for safety and dependability enhancement on projects through human error reduction,
- identify and analyse root causes of incidents or accidents involving human error.

6.3.2 Principles of human error reporting and investigation

The use of insight from incident and accident data is of paramount importance, even if data is limited in scope or depth [48]. The principle to be applied is *"human error should not be the conclusion of an investigation, but the starting point"* [49]. The central question concerns the underlying organisational conditions that error observations are symptomatic of [50].

The accumulation of incident data is supported by an open reporting culture that commends or even rewards operators for reporting errors and near misses [48]. "*Stories of failure*" represent invaluable foresight tools [48] when they allow for the recognition of individual responsibility and organisational learning.

Human dependability is enhanced by tracking human errors together with system anomalies in operations including AIT, operation preparation (e.g. simulation campaign) and reporting the occurrence of failures through a dedicated process at organisation level. Collection of human error data represents mandatory input for human error analysis.

Data collection i.e. creation of a data base on human errors helps to record experience gained over the system life cycle on error pre-cursors, such as performance shaping factors or the level of human performance. The tracing of human errors aims at eliminating precursors in future operations and will not only result in improving services, but also at improving the working environment of the employees.

The definition of a human error reporting system includes the consideration of:

- Confidentiality i.e. incidents involving an operator error are handled as confidential unless they are being anonymised. Confidentiality contributes to a climate of "goodwill", ensures candour of the individual or group reporting the incident and therefore ensures meaningful data for later analysis.
- Incentives or rewards for incident reporting.
- Demonstration of usefulness of human error reporting for the team itself.
- Review of reported incidents to ensure completeness, correct classification and comprehensibility.
- Creation of classifications of human error types to allow further data analysis and a global approach to manage human error across projects or organisations e.g. if many errors (locally or in different control centres) have the same type, common enhancements can be defined (e.g. training, working environment).
- Trend analysis based on the identification of duplicated or related incidents.
- Reporting of synthesis of major human errors and human errors statistics to management (e.g. annually or bi-annually).

The principles of human error analysis can be used for the investigation of failures involving human error during spacecraft operation.

In order to gather data for analysis or investigation of incidents, it will be either essential or helpful to conduct interviews with human operators. Their observations and experiences can offer unique insights unobtainable from other sources, or confirm and enhance existing available information.

Interview guidelines for formal incident investigation [51] provide useful direction for conversations about operator performance and the nature of their work in different phases of the system life cycle.

There are three main groups of interviewees:

- Operators: the individual(s) who are, or initially appear to be, directly involved in an incident, e.g. a controller, engineer or manager;
- Observers: in the on-site or nearby an operational environment not directly involved in an incident or event;
- Those familiar with critical system elements: equipment designers, instructors, procedures specialists, managers and supervisors.

Questions that the interviewees can be asked are detailed in the Annex C

In case of an incident, especially operator interviews should be conducted as soon as possible in a neutral, distraction-free environment or in the operational setting, mock-up or simulator to facilitate or enhance recall. Necessary reference material should be at hand (i.e. procedures, technical diagrams or photographs).

Administrative concerns, such as recording and storage of data are not covered here. They will be determined by the type and extent of the investigation and subject to organisation-specific practices and constraints.

6.3.3 Human error reporting and investigation process

6.3.3.1 Overview

The human error reporting and investigation process comprises the steps and tasks necessary to report and investigate human errors. The steps are:

a. Step 1: Report Errors

   Log, classify and review incidents during operations.

b. Step 2: Investigate Errors

   In case human errors are involved in the incidents, identify cause and reduce human errors.

The process of human error reporting and investigation is depicted in Figure 6-4.

6.3.3.2 Steps of human error reporting and investigation

6.3.3.2.1 Step 1: "Report Errors"

Tasks

Task 1-1: Establish a system to log incidents during operations on a project.

Task 1-2: Log incidents.

Task 1-3: Review logs for their completeness and comprehensibility.

Task 1-4: Identify criticality and urgency and classify logs.

Task 1-5: Establish anomaly review board: review incidents and define classification of incidents.

In case of human error involved in the incidents proceed with Step 2.

Outputs

Outputs of the Step 1 are:

- List and classification of incidents

6.3.3.2.2 Step 2: "Investigate Errors"

Tasks

Task 2-1: Use the principles of human error analysis (see section 6.2) to identify the error precursors which have contributed to the human error and to identify and implement human error reduction.

Task 2-2: Verify the implementation of human error reduction.

Outputs

Outputs of the Step 2 are:

– Investigation report

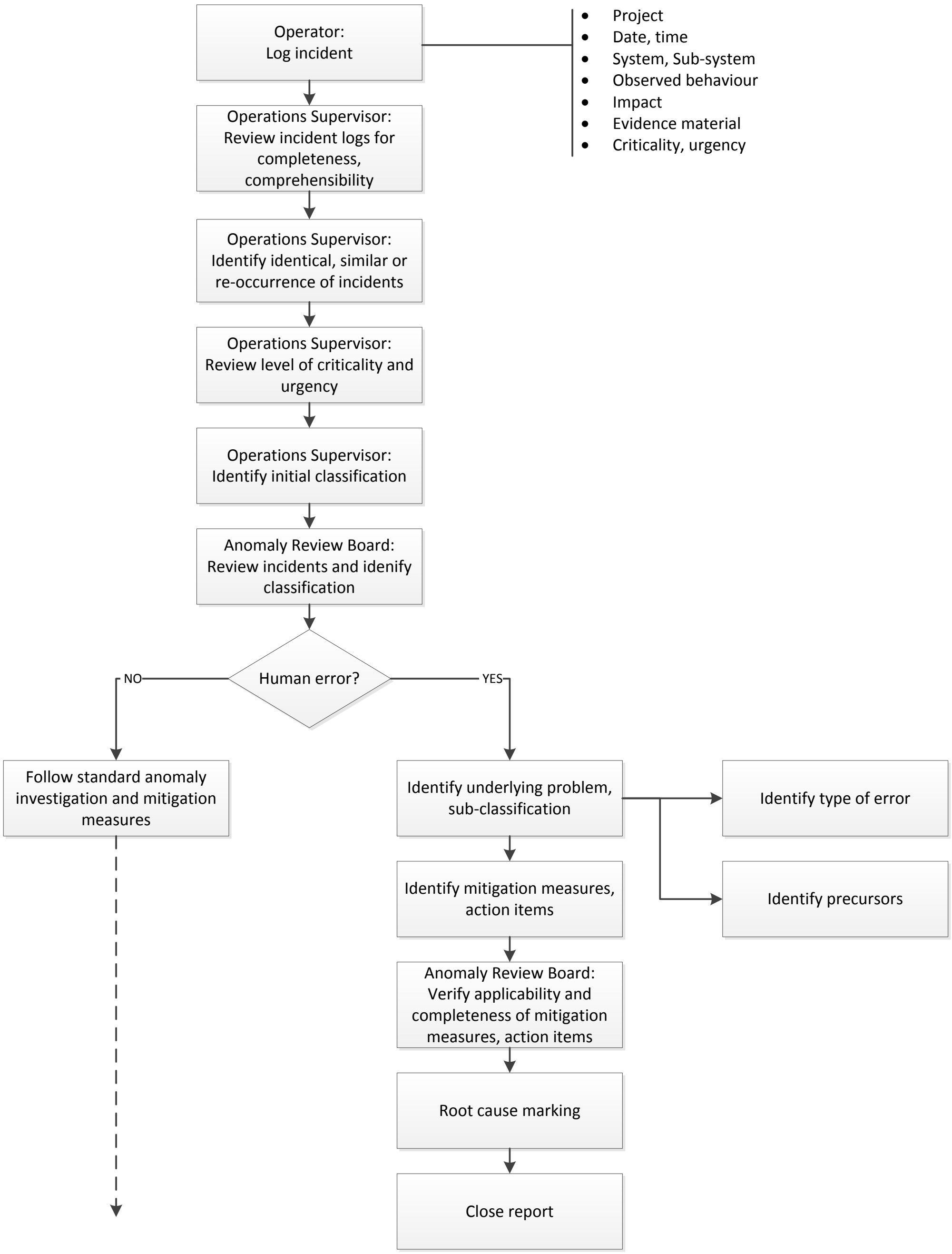

Operator:
Log incident
Project
Date, time
System, Sub-system
Observed behaviour
Impact
Evidence material
Criticality, urgency
Operations Supervisor:
Review incident logs for completeness, comprehensibility
Operations Supervisor:
Identify identical, similar or re-occurrence of incidents
Operations Supervisor:
Review level of criticality and urgency
Operations Supervisor:
Identify initial classification
Anomaly Review Board:
Review incidents and idenify classification
Human error?
NO
YES
Follow standard anomaly investigation and mitigation measures
Identify underlying problem, sub-classification
Identify type of error
Identify precursors
Identify mitigation measures, action items
Anomaly Review Board:
Verify applicability and completeness of mitigation measures, action items
Root cause marking
Close report

Figure 6-4: Human error reporting and investigation process

6.4 References

[37] Swain A.D. and Guttman H.E. (1983): Handbook of human reliability analysis with emphasis on nuclear power plan applications (NUREG CR-1278). Washington, DC: NCR.

[38] Hall R.E., Fragola J. and Wreathall J., (1982): Post event human decision errors: Operator action tree / time reliability correlation (NUREG/CR-3010). Washington, DC: US Nuclear Regulatory commission.

[39] Hollnagel E. (1998): Cognitive Reliability and Error Analysis Method: CREAM. Oxford, UK: Elsevier Science, Inc. 1998. ISBN 0-08042-848-7.

[40] Leveson. N.G. (2004): A Systems-Theoretic Approach to Safety in Software-Intensive Systems, IEEE Transactions on Dependable and Secure Computing 1 (1), pp. 66,86

[41] Nakao H., Katahira M., Miyamoto Y. and Leveson N. (2012): Safety Guided Design of Crew Return Vehicle in Concept Design Phase Using STAMP/STPA, Proceedings of the 5th IAASS Conference A Safer Space for Safer World by Ouwehand, L. ISBN:978-92-9092-263-6, Noordwijk, Netherlands: European Space Agency, 2012

[42] ECSS-Q-ST-30-02C – Space Product Assurance, Failures modes, effects (and criticality) analysis, 6 March 2009

[43] ECSS-Q-ST-40-02C – Space Product Assurance, Hazard Analysis, 15 November 2008

[44] ECSS-Q-ST-40-12C – Space Product Assurance, Fault tree analysis – Adoption notice ECSS/IEC 61025, 31 July 2008

[45] ECSS-Q-ST-40C – Space Product Assurance, Safety , 6 March 2009

[46] ECSS-Q-ST-30C – Space Product Assurance, Dependability, 6 March 2009

[47] ECSS-E-ST-10-11C – Space Engineering, Human Factors Engineering, 6 March 2009

[48] Dekker S. (2012): Just Culture: Balancing Safety and Accountability, 2nd Ed. Burlington: Ashgate.

[49] Dekker S. (2006): The Field Guide to Understanding Human Error. Burlington: Ashgate.

[50] Hollnagel E. (2003): Safer Complex Industrial Environments: A Human Factors Approach. New York: CRC Press, 37-59.

[51] Strauch, B. (2004): Investigating Human Error: Incidents, Accidents, and Complex Systems. Farnham: Ashgate.

7 Implementation of human dependability in system life cycle

7.1 General

Human dependability is an integral part of the overall engineering and safety, dependability and product assurance processes implemented during the system life cycle (commensurate with ECSS-E-ST-10C [52], ECSS-M-ST-10C [53], ECSS-Q-ST-30C [54] and ECSS-Q-ST-40C [55]).

The implementation of human dependability during the system life cycle implies different human dependability objectives and activities in the different project phases such as the definition of human dependability requirements, application of human error analysis or human error data collection and investigation as illustrated in Figure 7-1.

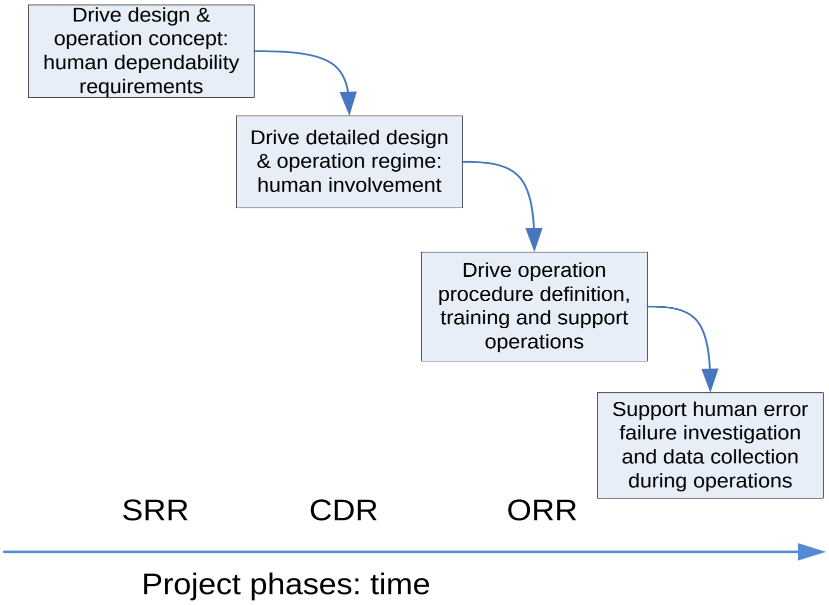

Drive design & operation concept: human dependability requirements
Drive detailed design & operation regime: human involvement
Drive operation procedure definition, training and support operations
Support human error failure investigation and data collection during operations
SRR
CDR
ORR
Project phases: time

Figure 7-1: Human dependability in system life cycle

The human dependability applications vary from project phase to project phase. The individual elements of the process within project phases vary depending on the type of project.

7.2 Human dependability activities in project phases

7.2.1 Overview

This section provides information on and examples of typical human dependability activities in different project phases. After subjection to tailoring these data can be used as input to the generation of the "product assurance and safety plan" of a specific space project.

For each project phase some typical objectives, inputs, tasks, outputs and milestone are indicated as overall guidance and are subject to be tailored when producing a specific "product assurance and safety plan".

The main phase objectives and human factors engineering objectives (ECSS-E-ST-10-11C [56]) are reflected in the human dependability objectives and tasks.

In the text below human dependability is referred to as HUDEP.

7.2.2 Phase A: Feasibility

Objectives:

- Define HUDEP input to system and operation concept
- Support high level trades including high level HUDEP aspects
- Determine and make aware of HUDEP approach
- Pre-schedule HUDEP activities and data submission during the overall project plan
- Plan HUDEP tasks for next phase

Inputs:

- Mission Definition from phase 0

Task:

- Perform preliminary safety and dependability analysis (preliminary hazard analysis and functional FMECA) and preliminary HUDEP assessment to contribute to:
  - determine the optimal level of automation
  - define potential human roles in system

Outputs:

- HUDEP Plan for phase B (included in RAMS Plan or RAMS part of PA Plan)
- Technical specifications, including:
  - functional high-level human in the loop requirements
  - functions to be added to cover operations' needs
  - system timeline
  - user and organisational requirements
  - HMI requirements
  - human error failure tolerance requirements
- Preliminary safety and dependability analysis with HUDEP assessment results, identifying for the defined system-concept:
  - contribution to system functional analysis as result of HUDEP assessment
  - preliminary training approach

  - o scenarios involving human error (including critical failure scenarios and potential hazardous conditions)
  - o list of HUDEP critical elements and operations and operator involved functions and HMIs
  - o HUDEP recommendations for human error and hazard reduction
- – HUDEP contribution to Statement of Work

Milestone:

- – Preliminary requirement review (PRR)

7.2.3 Phase B: Preliminary Definition

Objectives:

- – Elaborate preliminary design definition with HUDEP input
- – Develop final technical system specification including HUDEP requirements
- – Complete safety and dependability analysis with HUDEP aspects
- – Make aware of potential non-compliances to HUDEP requirements and provide potential solutions

Inputs:

- – Preliminary safety and dependability analysis with preliminary human failure scenarios
- – Preliminary task analysis
- – Preliminary system technical specification
- – Approved system functional specification
- – Statement of work
- – All previous inputs and outputs

Tasks:

- – Perform human error analysis to complement safety and dependability analysis
- – Transfer HUDEP related requirements to supplier level for sub-systems or equipment
- – Analyse, review, plan and drive HUDEP activities on supplier level
- – Complete HUDEP assessment of system design and specification and task analysis, contribute to:
  - o Specify users and organizational requirements
  - o Define human roles and responsibilities
  - o Determine how tasks should be assigned to operators and maintainers and what overall staffing levels and training are required.
  - o Identify operational constrains
  - o Define operators qualification criteria
  - o Design human machine interfaces
  - o Define training approach
  - o Identify emergency, warning, and caution situations
  - o Define system user manuals

Outputs:

- HUDEP Plan for phase C (included in RAMS Plan or RAMS part of PA Plan)
- Human Error Analysis report, including:
  - HUDEP requirements verification tracking log
  - action tracking log for open points
- Update technical specification at system and supplier level, including:
  - functional high-level human in the loop requirements, identifying functions that need to be added to the system functional analysis because of the operations' needs
  - timeline
  - user and organisational requirements
  - HMI
  - human error failure tolerance requirements
- HUDEP contribution to preliminary design definition, including:
  - preliminary user manual
  - training models and approach
  - updated failure scenarios involving human error (including critical failure scenarios and potential hazardous conditions for the operations)
  - updated list of HUDEP critical elements, operations, operator involved functions and HMIs
  - updated HUDEP recommendations for human error and hazard reduction
  - contribution to verification planning (verification of HUDEP requirements)

Milestone:

- System Requirements Review (SRR)
- Preliminary Design Review (PDR)

7.2.4 Phase C: Detailed Definition

Objectives:

- Refine HUDEP relevant analyses reports
- Check the closure of open actions, recommendations from Phase B
- Determine if non-compliance of HUDEP requirements, identified in Phase B, are solved
- Clarify if new non-compliance of HUDEP requirements are identified and provide solutions
- Delivery updated HUDEP report and provision of recommendations

Inputs:

- Safety and dependability analysis
- Task analysis
- Human error analysis
- Preliminary system user Manual
- System Technical Specification (TS) including the operational requirements
- System design definition
- List of anomalies, waivers and non-compliance of requirements
- All previous inputs and outputs

Tasks:

- Performed detailed Human Error Analysis:
  - Collect Human Error Data
  - Update identification of Human failure scenarios: Human Error Types, error causes, performance shaping factors and consequences
- Analyse, review, plan and drive HUDEP activities on supplier level
- Review and approve hazardous and HUDEP critical operational procedures
- Review anomalies, waivers changes under HUDEP aspects
- Update HUDEP requirements if necessary
- Complete HUDEP assessment of system design and specification and task analysis, contribute to:
  - Consolidate operational scenarios (confirm the compatibility between them and the operational requirements and functional design)
  - Consolidate timeline and define operator workload requirements
  - Define system operation manual

Outputs:

- Human Error Analysis report, including:
  - HUDEP requirements verification tracking log
  - action tracking log for open points
- Update technical specification at system and supplier level (if needed)
- HUDEP contribution to design and operations and maintenance definition, including:
  - system operation manual
  - training models and approach
  - updated failure scenarios involving human error (including critical failure scenarios and potential hazardous conditions for the operations)
  - updated list of HUDEP critical elements, operations, operator involved functions and HMIs
  - updated HUDEP recommendations for human error and hazard reduction

Milestone:

- Critical Design Review (CDR)

7.2.5 Phase D: Qualification and Production

Objectives:

- Re-assess HUDEP relevant analyses reports
- Check the closure of open HUDEP actions, recommendations from Phase C
- Determine if non-compliance of HUDEP requirements, identified in Phase C, are solved
- Clarify if new non-compliance of HUDEP requirements are identified and provide solutions
- Delivery updated HUDEP report and provision of recommendations
- Prepare project specific HUDEP lessons learnt report
- Demonstrate that the system is ready for operation from a HUDEP point of view

Inputs:

- Safety and dependability analysis
- Task Analysis
- Human error analysis
- System operation manual
- System design definition
- List of anomalies, waivers and non-compliance of requirements
- All previous inputs and outputs

Tasks:

- Update Human Error Analysis with regard to design changes decided after the critical design review (CDR) and according to test results
- Support writing of operational procedures for nominal and contingency operations to be included in the system operation manual
- Review and approve hazardous and HUDEP critical operational procedures
- Analyse, review and drive HUDEP activities on supplier level
- Review anomalies, waivers changes under HUDEP aspects
- HUDEP re-assessment of system design and specification with regard to design changes decided after the critical design review (CDR) and according to test results
- HUDEP re-assessment of Phase C operation concept
- Complete HUDEP assessment of the system specification and design
- Ensure that project requirement documentation complies with HUDEP requirements
- Ensure that project implementation and verification program covers HUDEP related human error and hazard reduction verification activities (on system and on-supplier level)

Outputs:

- Updated human error analysis report
- HUDEP "lessons-learnt" data
- HUDEP contribution to design and operations and maintenance update including:
  - system operation manual
  - installation manual
  - updated human failure scenarios (including critical failure scenarios and potential hazardous conditions for the operations)
  - updated list of HUDEP critical elements, operations, operator involved functions, HMIs
  - updated HUDEP recommendations for human error and hazard reduction

Milestones:

- Qualification Review (QR)
- Acceptance Review (AR)
- Operational Readiness Review (ORR)
- Flight Acceptance Review (FAR)

7.2.6 Phases: E Operations/Utilization and F Disposal

Objectives:

- Assess existing operations baseline versus HUDEP
- Assess anomalies with respect to HUDEP aspects
- Support human error failure investigation and data collection during operations
- Collect human error data and elaborate HUDEP lessons learnt

Inputs:

- Safety and dependability analysis
- Human error analysis
- Qualification reports
- System operation manual
- Technical description of the system from phase C/D
- List of anomalies, waivers and non-compliance of requirements
- All previous inputs and outputs

Tasks:

- Evaluate design and operational changes for impact to HUDEP
- Collect human error data during operation
- Support review of operational procedures for both, nominal and contingency operations included in the system operation manual from a HUDEP perspective
- Support investigation of operational anomalies and trends regarding human error
- Support to prepare disposal phase plan for HUDEP aspects
- Contribute to disposal plan (for phase F) - if applicable: perform HUDEP assessment for disposal operations (if project foresees a disposal phase HUDEP to cover this from Phase A on)

Outputs:

- Update Human Error Analysis report, including:
  - Anomalies assessment
  - Action tracking log for open points
- Human error data
- HUDEP "lessons-learnt" data
- HUDEP contribution to Design, Operations and Maintenance update including (if needed):
  - system operation manual
  - installation manual
  - updated human failure scenarios (including critical failure scenarios and potential hazardous conditions for the operations)
  - updated list of HUDEP critical elements, operations, operator involved functions and HMIs
  - updated HUDEP recommendations for human error and hazard reduction

Milestones:

- End of Life Cycle
- Disposal Plan Review

7.3 References

[52] ECSS-E-ST-10C – Space Engineering - System engineering general requirements,6 March 2009

[53] ECSS-M-ST-10C Rev.1 – Space management - Project planning and implementation, 6 March 2009

[54] ECSS-Q-ST-30C – Space product assurance - Dependability, 6 March 2009

[55] ECSS-Q-ST-40C – Space product assurance - Safety, 6 March 2009

[56] ECSS-E-ST-10-11C – Space engineering - Human factors engineering, 31 July 2008

Annex A (informative) Human error analysis data - examples

A.1 Overview

The following information is limited to the use and understanding of this handbook and might be used differently in other documents or environments. The information provided in this Annex A can be regarded as examples of human error analysis data that can be used for supporting the identification of failure scenarios involving human error.

A.2 Examples of the Evolution of PSFs

Table A-1 provides examples of the three types of modifications to PSFs that can occur throughout a particular scenario.

Table A-1: SPAR_H PSF modelling considerations for MIDAS [57]

PSFs	Considerations for Static Condition[1]	Considerations for Dynamic Progression[2]	Considerations for Dynamic Initiator[3]	Considerations for VACP Model [4]
Available Time	Can be set initially for scenario if there are time limits in place.	As scenario progresses, available time is diminishing unless actions are taken that effectively buy time to successfully complete required actions in the scenario.	Situational changes (e.g., sudden hardware failure) can diminish available time.	Inadequate time can lower overload threshold for VACP activities by requiring more rapid sequencing of information and actions. It is assumed that a generous allotment of time does not significantly increase the overload threshold for VACP activities beyond the default threshold found for adequate time.
Stress/Stressors	Can be set initially for scenario. In most cases, stress/stressors assumed to be nominal at the outset of a scenario.	In the presence of stress, it is assumed that the outcome of tasks can affect the severity and continuance of stress. Successful actions and recovery can serve to decrease stress gradually, while unsuccessful actions and errors can increase stress over successive actions.	Situational changes (e.g., sudden hardware failure), environmental changes (e.g., excessive heat), and psychological factors (e.g., sudden adverse event that negatively impacts state of mind) can increase stress.	Stress and stressors lower the overload threshold for all VACP activities. Sustained high VACP levels can induce stress.

PSFs	Considerations for Static Condition[1]	Considerations for Dynamic Progression[2]	Considerations for Dynamic Initiator[3]	Considerations for VACP Model [4]
Complexity	Can be set initially for scenario or sequence of events within a scenario.	Complexity can vary from task to task. Successful actions and recovery can decrease subsequent task complexity, while unsuccessful actions and errors can increase subsequent complexity and recovery.	Situational changes (e.g., sudden hardware failure) can increase task complexity.	Task complexity can lower overload threshold for visual, auditory and especially cognitive activities.
Experience/ Training	Can be set initially for scenario, as individual's experience and training, not vary throughout scenario.	Unlikely to change throughout the scenario, although can change if task switches to less familiar or more familiar domain.	Situational changes (e.g., sudden hardware failure) can move individual into a less trained and experienced domain	Low experience can lower the overload threshold for VACP activities, while high experience can increase the overload threshold for VACP activities.
Procedures	Overall quality of procedures can be set globally at the initiation of the scenario.	Assuming screened and edited procedures of at least nominal quality, deviations in quality of procedure (e.g., omitted step) are task specific and vary from task to task.	Situational changes can introduce cases for which the procedures are deficient.	Assumed nominal overload threshold for VACP activities. Simultaneous utilization of several procedures with elevate visual and cognitive activity levels. Multiple annunciators requiring separate procedural response can elevate visual, auditory, and cognitive activity levels.
Ergonomics/ HMI	Overall quality of ergonomics can be set globally at the initiation of the scenario.	Poor ergonomics or HMI can appear in specific tasks.	Situational changes (e.g., sudden hardware failure including instrumentation failure) can reduce the quality of the ergonomics of HMI.	Poor ergonomics can especially elevate the level of psychomotor activity requiring greater physical effort by the individual. Poor HMI can elevate the visual, auditory or cognitive activity levels.

PSFs	Considerations for Static Condition[1]	Considerations for Dynamic Progression[2]	Considerations for Dynamic Initiator[3]	Considerations for VACP Model [4]
Fitness for Duty	Individual brings fitness for duty to work environment; can in most cases be set and kept static at initiation of scenario.	Long duration scenarios can degrade fitness for duty through fatigue. Environmental conditions (e.g. excessive heat) can degrade fitness for duty.	Sudden change in the environment (e.g., radioactive release), physical injury, or psychological shock can be introduced to significantly degrade fitness for duty.	Degraded psychological state can lower overload threshold for visual, auditory and cognitive activities. Degraded physical state can lower overload threshold for psychomotor activity.
Work Processes	Work processes represent precipitating circumstances that are unlikely to change across the scenario and can be set at the initiation of the scenario.	Unlikely to change through the scenario unless new individuals are introduced into the scenario with different work processes.	Sudden introduction of novel individuals or novel punitive consequences to actions can result in poor work processes	Work processes – particularly communication – are likely manifest in the visual and auditory activities. Poor work processes can lower overload threshold for these activities.

NOTE:

1:Static Condition – PSFs remain constant across the events in a scenario [57]

2: Dynamic Progression – PSFs evolve across events in a scenario [57]

3: Dynamic Initiator A sudden change in the scenario causes changes in the PSFs [57]

4: VACP Model : Visual, Auditory, Cognitive and Psychomotor Model [58]

SPAR-H is explained in [59].

MIDAS: Man-Machine Integration Design and Analysis System is explained in [60]

A.3 Examples of Human Error Scenario Data

Examples of events for human errors can be found in the CFDA Project web-page:

http://www.cfda.info/.

A.4 References

[57] Boring R.L. (2006): Modeling Human Reliability analysis Using MIDAS. International Workshop on Future control Station Designs and Human Performance issues in Nuclear Power Plants. Idaho National Laboratory

[58] Wickens C. (1984): Engineering Psychology and Human Performance, Harper Collins, 1984

[59] Gertman D., Blackman H., Marble J., Byers J. and Smith C. (2005):The SPAR-H Human Reliability Analysis Method, NUREG/CR-6883, US Nuclear Regulatory Commission.

[60] Hart G., Dahn D., Atencio A. and Dalal K.M. (2001): "Evaluation and application of MIDAS v2.0," Proceedings of the 2001 Aerospace Congress, Paper 2001-01-2648

Annex B (informative) Human error analysis documentation

An example of an analysis form sheet to document the results of human error analysis is given in Table B-1. Instructions to complete the form sheet by filling the data fields are provided below.

1. “Operation”:

   Define reference and title of operation i.e. operation scenario, procedure, step and task including e.g. time available and required to perform task, …, identify source e.g. mission operation concept document.

2. “Failure Scenario involving Human Error”

   (a) Identify the human error including error type (or if applicable combination of failure and human error or combination of human errors),

   (b) Identify effect and resulting undesirable event,

   (c) Identify the consequence.

3. “Severity and Requirements”

   Identify consequence severity according to severity scheme (e.g. catastrophic, critical, …) and applicable requirements (e.g. failure tolerance, indicate safety relevance, priority,…)

4. “Error Precursor and Mitigator and Reduction Measures”

   If commensurate with scope identify error precursors, mitigators and reduction measures and performance shaping factors and human error level.

5. “Observable Symptom”

   Identify observable symptoms of failure scenario (i.e. e.g. of effect).

6. “Links and Interface”

   Identify links to other analysis, documents or domain (e.g. FMECA, hazard analysis, …).

7. “Human Error Reduction Recommendations”

   Identify recommendations for human error reduction measures: either indicate existing and/or recommend new measures.

8. “Implementation, Verification, Status, Remarks”

   Identify the implementation status, verification means and verification status, and remarks.

Table B-1: Example of an "Human Error Analysis Form sheet"

HUMAN ERROR ANALYSIS										Page
Document Reference:		Issue:					Prepared by:			
Project:		Operation:		Ref.:			Approved by:			
Ref.:	**1. Operation**	**2. Failure scenario involving human errors**			**3. Severity & Requirements**	**4. Precursor, Mitigator & Reduction measure: PSFs**	**5. Observable Symptom**	**6. Links & Interface**	**7. Error Reduction Recommend ation**	**8. Implementation, Verification, Status, Remarks**
	Step & Task	Cause & Human Error	Effect & Undesirable Event	Consequence						
S1.1	Selection of file	Slip: operator selects wrong file	Wrong file sent to spacecraft leading to safe mode	Service interruption	3	Routine, night shift	Flag	Task analysis	Peer review of files	Now part of normal practice, procedure reviewed, closed

Annex C (informative) Human error analysis example questions

C.1 Examples of questions to support a risk analysis on anomalies and human error during operations

Potential severity [61]:

- What are the risks if the anomaly occurs during a critical phase ?
- What is the potential severity of the anomaly ?
- Will there be an impact on people or on facilities ?

To evaluate criticality [61] :

- Will the anomaly block the operations ?
- What is the impact if the degradation becomes more marked ?
- What is the impact on other similar operations ?
- Criticality of potential previous events or precursors ?

For the intervention [61]: (evaluate the potential error risk on this new intervention)

- Is a procedure available ?
- Is this intervention common for the operators ?
- Does it need specific practices: e.g. use of not well-known equipment or of new technology device ?
- Does it need specific organisation ?
- Does it need unusual working postures ?
- Are working conditions usual (e.g. noise, night operations, etc...) ?
- Is the intervention compliant w.r.t. time of rest ?
- What kind of validation is needed at the end of the intervention: correct running test, non-regression ?
- Efficiency and harmlessness of the intervention ? Quality engineers need to be involved.

Intervention environment or framework [61]:

- Impact on the system ?
- Impact on equivalent hardware ?
- Risk of impact in the anomaly area during the intervention ?

Impact on facilities qualification ? (the anomaly and its correction does not jeopardise facilities or ground support equipment (GSE) qualification) [61]:

- Is the configuration modified (e.g. HW, SW, operational conditions) ?
- Is a device replaced by a different one ?
- Is there a geometrical modification ?
- Are plans available ?
- Is the process modified (e.g. pressure, temperature, voltage …) ?

Incident Analysis [61]

- Operators:
  - Actions and decisions before or during an event, their approximate time, outcome and consequences;
  - Information on task, duties and responsibilities in general and during the event, workload, extent to which novel situations are encountered and how they are responded to;
  - General and task-specific practices and procedures, differences between intent and actual practice;
  - Personal information such as shift pattern, i.e. overall health or sleep schedule if applicable.
- Observers:
  - Which details of the event caught their attention, and when;
  - Their location/ position and what they heard, saw, felt etc.;
  - Operator and own actions.
- Those familiar with system elements:
  - Operator training and work history;
  - Training programme history and description;
  - General and specific policies and practices.

Specifically, the interviewer can chose to focus on what should have happened in the everyday routine case, in order to develop an understanding of why this did not happen in the case of a failure [62]. Possible questions and prompts include (from [63]):

- When do you typically start the activity?
- Do you ever adjust or customize the activity to the situation? How?
- What do you do if something unexpected happens (interruption, new urgent task, unexpected change of conditions, unavailability of resources, something that goes wrong)?
- How stable are the working conditions? Does your work require improvisation?
- How predictable is the work situation and the working conditions?
- Is there something that you often have to tolerate or get used to during everyday work?
- What preconditions for your work are usually fulfilled?
- Are there any factors which you and all who participate in an activity take for granted during work?
- How do you prepare for your work (e.g., reading documents, talking to colleagues, refreshing instructions)?
- What resources do you need (equipment, service features, information)? Do you usually assume that they will be available when needed?
- What do you do in case of time pressure, missing information or when certain people are unavailable?
- Is there a ‘better’ or ‘best way’ to do this activity?

C.2 References

[61] Strauch, B. (2004) Investigating Human Error: Incidents, Accidents, and Complex Systems. Farnham: Ashgate.

[62] Hollnagel, E. (2012) FRAM: the Functional Resonance Analysis Method – Modelling Complex Socio-technical Systems. Farnham: Ashgate, p. 34.

[63] Hollnagel, E. (2014) The Functional Resonance Analysis Method: Finding what goes right. Online: http://functionalresonance.com/how-to-build-a-fram-model/finding-what-goes-right.html (Accessed 20 March 2014)

Annex D (informative) Human dependability in various domains

D.1 Human dependability in industrial sectors

Human dependability is a discipline of importance for all industrial sectors. This section provides a high level overview of industrial domains concerned with human dependability. Some few examples with emphasis on operational aspects and examples of references are listed.

Relevant insights on human dependability experiences, developments and practices can be derived from domains comparable to the space domain such as safety critical industrial systems or infrastructures, "high reliability organisations" or the space sector itself. They can apply to aspects both at the "sharp end" and "blunt end", including planning, decision making, failure and recovery, and overarching aspects such as standards, regulations, and guidelines.

The following collection outlines domains relevant particularly to the ground segment in space operations, i.e. where a human is situated in the loop of controlling a complex system, network, process or asset. While many settings in the domains include either "local control centres" CCs or "central control rooms" CCRs, they can feature different:

- Control centre design paradigms (architecture, HMIs);
- Types of interaction with the system to be controlled (e.g. direct, remote, time delay, environment hazardous to operator);
- Types of system or asset to be controlled (e.g. hazardous material versus valuable asset)
- Degrees of cost of failure (e.g. loss of asset versus loss of life; individual operator risks versus global safety risk); or
- Sectors (commercial, governmental, science, military, public).

For each domain, generic types of "environments", concrete examples and examples of a reference to a document i.e. providing e.g. an approach, case study or review are provided in Table D-1.

Table D-1: Examples of Comparable External Domains

DOMAIN	GENERIC ENVIRONMENT	EXAMPLE	DOCUMENT
SPACE	• Ground station network control; • Launch sites: Human-In-The-Loop (HITL) • Isolation chambers and space simulators; • Assembly and integration cleanrooms.	ESTRACK Control Centre	NASA HRA Methods [64]
DEFENSE and SECURITY	• Nuclear submarines, Flight deck/cockpit; • Unmanned Aerial Vehicles (UAVs); • Guided Weapons Systems; missile silos; • Nuclear, biological, chemical (NBC) weapons research facilities; • Central or distributed command and control settings; • Intelligence analysis; • Metropolitan police and security control; • High security prisons; • Remote ordnance disposal.	HMS Astute	UAV Mishaps Human Factors Analysis [65]
TRANSPORT and INFRASTRUCTURE	• Air Traffic Management (ATM), Flight deck/cockpit; • Railway (rapid transit, cargo), mass transit authorities (e.g. in metropolitan areas); • Tunnels and channels; • Marine vessel traffic service (VTS); • Construction/demolition projects in civil engineering (e.g. crane operation, tunnelling, controlled demolition).	VTS Houston Texas	Railway Human Factors Guide [66]
ENERGY and UTILITIES	• Nuclear Power Plants; • Chemical Processing Plants (CPPs) and refineries, steel production; • Power plants (incl. fossil fuel and waste incineration); • Grid regulation and power distribution; • Hydro power, reservoirs and dams, water purification sewage networks; • Exploitation and extraction (on/off-shore), mining oil and gas, off-shore wind parks; • Decommissioning of plants.	Tricastin Nuclear Power Centre	Safety Culture Assessment [67]

DOMAIN	GENERIC ENVIRONMENT	EXAMPLE	DOCUMENT
SCIENCE and ENGINEERING	• Science reactors (nuclear, biological, chemical); • Heavy ion research/ particle accelerators; • Tokamaks, laser research facilities, neutrino observatories; • Robotic deep sea exploration/ submersible manipulators; • Wind tunnels and ballistic range complexes.	Super-Kamioka Neutrino Detection Experiment	CERN Safety Guide [68]
LIFE SCIENCES and MEDICAL	• High security laboratories and pathogen units (Biosafety Level 4), e.g. contamination control; • Human centrifuge, chamber studies; • Telemedicine, infection control and pandemic response; • Surgery, anaesthesiology, robotic surgery; • Intensive care units (ICU), epilepsy monitoring units (EMU).	Centres for Disease Control and Prevention	Laboratory Biosafety Manual [69]
OTHER	• Emergency response, coordination or rescue control centres (RCCs); • Industrial production and manufacturing including robotic assembly; TV and radio studios, polling and election centres; • Crowd control and facility management (e.g. themes parks, sports arenas); • High security facilities (e.g. data centres, large archives, distribution and retrieval systems).	Inmarsat Maritime Rescue Control Centres	Industrial Robotics Safety Guidelines [70]

D.2 References

[64] Chandler, F.T., Chang, J.Y.H., Mosleh, A., Marble, J., Boring, R.L., Gertman, D. I. (2006) Human Reliability Analysis Methods: Selection Guidance for NASA. Washington, D.C.: NASA.

[65] Thompson, W.T., Tvaryanas, A.P., Constable, S.H. (2005) U.S. Military Unmanned Aerial Vehicle Mishaps: Assessment of the Role of Human Factors Using Human Factors Analysis and Classification System (HFACS), HSW-PE-BR-TR-2005-0001. Brooks City-Base, TX: United States Air Force.

[66] RSSB (2008) Understanding Human Factors: A Guide for the Railway Industry. London: Rail Safety and Standards Board.

[67] IAEA (2002) Self-assessment of safety culture in nuclear installations: Highlights and good practices, IAEA-TECDOC-1321. Vienna: IAEA.

[68] CERN (2005) Safety Guide for Experiments at CERN. Geneva: European Organization for Nuclear Research.

[69] WHO (2004) Laboratory biosafety manual, 3rd Ed. Geneva: World Health Organisation.

[70] OSHA (1987) Guidelines For Robotics Safety, STD 01-12-002. Washington, D.C.: Occupational of Safety and Health Administration.

Bibliography

ECSS-S-ST-00-01C ECSS - Glossary of terms

NUREG/CR-6883,2005 The SPAR-H Human Reliability Analysis Method

NUREG/CR-1278 Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (THERP) Final Report, Sandia National Laboratories, 1983

Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. In IEEE Trans. on Dependable and Secure Computing, vol.1, no.1, pp. 11- 33, Jan.-March 2004

Atkins R.K. Human Error Requirements, Scope and Implementation at the European Space Agency - 1990 Proceedings Annual Reliability and Maintainability Symposium

Boring R. Human Reliability Analysis Methods for Space Safety - Idaho National Laboratory- Dec. 7, 2005

Carnino A. et al Man and Risks, Marcel Dekker, 1990 (ISBN-0-08247-8379-4)

Carver L., Turoff M. Human-computer interaction: the human and computer as a team in emergency management information systems. Commun. ACM 50(3): 33-38 (2007)

Chandler, F., Heard, I. A., Presley, M., Burg, A., Mongan, P. NASA Human Error Analysis. Washington, D.C.: NASA, 2010

Chen F., Choi E.H.C., Ruiz N., Shi Yu, and Taib R. User interface design and evaluation for control room. In Proceedings of the 17th Australian conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future (OZCHI '05), 1-4, 2005

ISO 11064-1, 2000 (1st Edition), Geneva: ISO. Ergonomic design of control centres – Part 1: Principles for the design of control centres.

Kontogiannis T. Adapting plans in progress in distributed supervisory work: aspects of complexity, coupling, and control. Cogn. Technol. Work 12, 2 (June 2010), 103-118, 2010

Liu F., Zuo M. and Zhang P. Human-Machine Function Allocation In Information Systems: A Comprehensive Approach. Proceedings of The 15th Pacific Asia Conference on Information Systems (PACIS 2011), Brisbane, Australia, July 2011.

Martinie C., Navarre D., Palanque P. A multi-formalism approach for model-based dynamic distribution of user interfaces of critical interactive systems. Int. J. Hum.-Comput. Stud. 72(1): 77-99 (2014)

Norman D. The design of everyday things. Cambridge, MA: MIT Press 1998

Rohn J. Petersen, William W. Banks, and David I. Gertman. Performance-based evaluation of graphic displays for nuclear power plant control rooms. In Proceedings of the 1982 conference on Human factors in computing systems (CHI '82). ACM, New York, NY, USA, 182-189.

Polet P., Vanderhaegen F. and Wieringa P. Theory of safety related violation of system barriers. Cognition Technology and Work, 4, 3, 171-179. 2002.

Preyssl C. Dependability and Safety and the European Space Agency: Organisation Overview and Recent Study Initiatives. IEEE, 519-521,2009

Seminara J. L., Gonzalez, W. R., and Parsons, S. O. Human factor review of nuclear power plant control room design (NP-309). Palo Alto, CA: Electric Power Research Institute. (1977).

Stanton N. A., Salmon P., Jenkins D., Walker, G. Human Factors in the Design and Evaluation of Central Control Room Operations. Boca Raton, FL: CRC Press. (2010)

Vanderdonckt, J. Distributed User Interfaces: How to Distribute User Interface Elements across Users, Platforms, and Environments. In Proceedings of XIth Congreso Internacional de Interacción Persona-Ordenador Interacción'2010 (Valencia, 7-10 September 2010), J.L. Garrido, F. Paterno, J. Panach, K. Benghazi, N. Aquino (Eds.), AIPO, Valencia, 2010, pp. 3-14, Keynote address

Wegner D. Considering of overall 'Human Dependability' in Project Management and Engineering (abstract only). Proceedings of the 1st Human Dependability Workshop (HUDEP), September 2009.