CHEMICAL ENGINEERING TRANSACTIONS Volume 19, 2010
Editor Simberto Senni Buratti
 ISBN 978-88-95608-11-2 ISSN 1974-9791
DOI: 10.3303/CET1019035

Human Factor in Functional Safety

Pasquale Fanelli
Invensys Systems Italia S.p.A.
v. Carducci, 125 20099 Sesto S.G. (MI)
pasquale. fanelli @invensys.com

1. Introduction

The European Norm EN 61508 "Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-related Systems" states that although a person can form part of a safety-related system, human factor requirements related to the design of E/E/PE safety-related systems (SIS) are not considered in detail in the norm itself.
The term 'human factor' in EN 61508 throughout the lifecycle process refers to operation and maintenance, rather than any human involvement in design, engineering, implementing and delivering E/E/PE safety instrumented systems (SIS).
Nevertheless the European Norm EN 61508, issued in 2001 by CENELEC, defines the human error as "human action or inaction that can produce an unintended result".
The European Norm EN 61511 "Functional Safety: Safety Instrumented Systems for the Process Industry", issued in 2004 by CENELEC and by ANSI/ISA as S84.00.01-2004 (IEC-61511 mod.), states that the design of a safety instrumented function (SIF) shall take into account human factors as well.
The paper introduces a thorough examination of the human factor in functional safety with reference both to EN 61508 and EN 61511, with the main purpose of taking in due consideration the adequacy of operations and maintenance staff in the SIL analysis.
The SIL Analysis is executed to comply with the requirements of SIS safety life-cycle (ref. to EN 61511 clause 9) by individually assigning an SIL to every SIF actuated by the SIS.
The SIL assigned to every SIF is the measure of the risk reduction target allocated to the SIF itself, but this target can be severely jeopardized by an inadequate assessment of human factor.
The paper finally provides general guidelines on human factor adequacy assessment.

2. Human factor according to EN 61508

The term 'human factor' according to EN 61508[1] throughout the lifecycle process refers to operation and maintenance, rather than any human involvement in design,

[1] transposed in Italy as CEI EN 61508

Please cite this article as: Fanelli P. and Fanelli P., (2010), Human factor in functional safety, Chemical Engineering Transactions, 19, 213-218 DOI: 10.3303/CET1019035

engineering, implementing and delivering Electric/Electronic/Programmable Electronic (E/E/PE) safety instrumented systems (SIS).
Nevertheless the European Norm EN 61508, by defining the human error as "human action or inaction that can produce an unintended result", states the following:

- the types of accident-initiating events that need to be considered and specified include the human error;
- the hazards and hazardous hazardous events of the equipment under control (EUC) and relevant control system shall be determined under all reasonably foreseeable circumstances including all relevant human factor issues, such as;:
  - insufficient training
  - inadequate skills
  - work overload/underload
  - inadequate resources
  - inadequate procedures
  - inadequate labelling
  - inadequate communications
  - uneasy equipment operability
  - not visible/heard displays/controls
  - confusing displays/controls
  - not accessible/usable displays/controls
  - environmental condition issues
  - others;
- the hazard and risk analysis will comprise the human factors and any credit taken for human intervention shall be detailed.

3. Human factor according to EN 61511

The European Norm EN 61511[2] "Functional Safety: Safety Instrumented Systems for the Process Industry", issued in 2004 by CENELEC and by ANSI/ISA as S84.00.01-2004 (IEC-61511 mod.), developed as EN 61508 implementation for process sectors, such as oil & gas, refining, chemical, pulp & paper, non-nuclear power generation, states the following:

- the design of a safety instrumented function (SIF) takes into account human factors;
- the assessment of process risk should include associated human factor issues;
- a protection layer is any independent mechanism that reduces risk by control, prevention or mitigation, including an administrative procedure such as an emergency plan. The independent protection layer responses may be automated or initiated by human actions;
- when a human action is a part of an SIS used to implement one or more SIFs, the availability and reliability of the operator action must be specified in the safety requirements specification (SRS) and included in the performance calculations for the SIS;

---

[2] transposed in Italy as CEI EN 61511

- the hazard and risk assessment shall result in a detailed description of any credit taken for operational constraints or human intervention;
- the SRS shall specify any action necessary to achieve or maintain a safe state in the event of fault(s) being detected in the SIS. Any such action shall be determined taking account of all relevant human factors;
- requirements for operability, maintainability and testability shall be addressed during the design of the SIS to facilitate implementation of human factor requirements in the design.

4. Human Factor

According to EN 61508 the hazards and risks are generated by the equipment under control (EUC), by malfunctions of the EUC control system, by human error or by other reasonably foreseeable events. By taking into account any human recovery or procedural controls, the risk can be finally assessed. From the assessment of risk of hazardous event it is viable the determination of the level of risk reduction required to achieve the target level of safety.
The human factor can, therefore, be considered, as follows:

- any potential operational errors are included as initiating or contributory events in the process hazard and risk analysis;
- operational recovery actions, such as 'human safety functions' are included as assumptions in estimating the EUC baseline risk level;
- effort is required in ensuring that operations and maintenance procedures are defined up front and then implemented with full adequacy factor;
- determination of the safety integrity level (SIL) for an SIF requires careful consideration of not only of the direct risk reduction function it is providing, but also the risk reduction function implemented by the interacting operational staff;
- having determined the SIF SIL the human factor impact on operation and maintenance results greater for higher SIL;
- determining all hazards and hazardous events shall include consideration of all human factor issues and shall give particular attention to abnormal or infrequent modes of operation;
- the availability of skills and resources for operation and maintenance, and the operating environment may be critical to achieving the required functional safety in actual operation. The management of functional safety (FSM) system to be established according to EN 61511-1 clause 5 it's compulsory to claim an SIS conformity to EN-61511 itself. Roles and responsibilities (R&R) of all the personnel involved at any title in the functional safety life-cycle activities shall be clearly stated;
- in the frame of a FSM system a Personnel Competency Assessment task shall be executed and periodically repeated on all the personnel involved in the functional safety life-cycle activities;
- as part of Safety Management System (SMS) the incidents and near-misses recording shall report any human error involving a 'human safety function' (e.g.

missed or incorrect operator action following a high priority alarm) and the identification of the human factor(s) determining the human error itself;
- perform qualitative human reliability assessment aimed to identify the possible forms of human error that could generate a demand upon the SIS or may cause a human fault recovery action to fail. Operating tasks are examined to identify possible failure modes, hazards and consequences. The output of human reliability assessment may be in the form of training, procedures or operator-oriented design requirements;
- perform quantitative human reliability assessment should a probabilistic approach be taken to assessing risk reduction requirements;
- perform violation analysis to assess any potential for misuse and abuse (deliberate deviations from the rules, procedures, instructions and regulations drawn up for the safe or efficient operation and maintenance of plant or equipment). For any set of human factors determining possible types of violations a checking mechanism shall be provided.

5. Human Factor Assessment

The Human Factor shall find a high consideration and focus in FSM systems to reduce the risk to safety, environment and asset losses. To this purpose Human Factor Best Practices shall be set up and relevant benchmarking is required to every Project and Organization involved in a safety life-cycle.
According to "Human Factors Assessment Model Validation Study" issued by UK HSE in 2004, Projects and Organizations through the Human Factor Assessment Methodology (HFAM) are in the position to benchmark themselves against what might be considered Best Practice in Human Factors. The proposed HFAM application is hereinafter examined in detail.
Twenty-one Human Factor Elements (HFE) are identified to execute an HFA, where each HFE has a basic points assignment:

Elements aligned to "Policy":

1.	Recognition	10p

Elements aligned to "Organizing":

2.	Clear Responsibility	2p
3.	Contractors	1p
4.	User Involvement	10p
5.	Competence	2p

Elements aligned to "Planning & Implementation":

6.	Risk Screening	2p
7.	Exposure to Hazards	1p
8.	Human Factors Planning	2p
9.	Understanding the Operational Context	2p
10.	Recognition of Established Work Patterns	1p
11.	Assumptions & Constraints	1p
12.	Operator Characteristics	1p

13.	Manning & Roles	1p
14.	Operational Tasks	1p
15.	Maintenance Tasks	1p
16.	Training Needs	1p

Elements aligned to "Measuring Performance":

17.	Human Requirements	2p
18.	Human Factors Design Review	1p
19.	Operability Validation	10p

Elements aligned to Auditing & Reviewing Performance:

20.	Learning from Experience	10p
21.	Operational Feedback	2p
	Basic Points Total	**64p**

According to Human Factors Assessment (HFA) Model Validation Study basic points are assigned to each HFE (1p, 2p, 10p) and three factors (assessment ratings) are assigned to each HFE according to the independent assessor judgment:

HFA Rating Factors

HFE "not satisfied"	HFA Rating Factor = 1
HFE "unsure"	HFA Rating Factor = 2
HFE "satisfied"	HFA Rating Factor = 3

e.g.

Recognition (10p)

The Organization recognizes that design projects need to consider the role of the human in operating or maintaining equipment or facilities or the impact of the equipment on the operators and maintainers. As an example of possible evidence: Human Factors/Ergonomics recognized as a technical area in the Project.

Independent assessor judgment:

HFE "satisfied" corresponding to HFA Rating Factor = 3.

Recognition Score: 10 basic points x 3 = 30 p

By independent assessing judgement the HFA Total Score is calculated for each HFE.
The HFA Score % is worked out as follows:
HFA Score % = HFA Total Score/192*100
where:
HFA max. achievable score = 64p (Basic Points Total) x 3 (HFA max Rating Factor) = 192 p
finally according to the HFA Score % a human factor assessment is given according to the following ranking

HFA Score %	
"Best Practice in Human Factors"	> 90%
"Good Practice in Human Factors, towards Best Practice"	> 75%
"Good Practice in Human Factors"	> 65%
"Good Practice in Human Factors Partially Followed"	> 45%
"Good Practice in Human Factors Not Followed"	< 45%

6. Conclusion

Besides pros and cons of each human error assessment technique, even the more rigorous are not fully exempt from controversial and inconsistent results, any effort since the early project phases shall be devoted to:

- identify by extended HazOp the operational tasks potentially determining a main deviation cause or enabling an initiating event, and the emergency procedures posted as operator response to hazardous event;
- analyze the operational tasks and the emergency procedures to identify the more likely human errors and latent weaknesses, the human error recovery actions, the main performance shaping factors, meant as the factors that affect the human behaviour, and the associated particularly relevant conditions for control room and local actions;
- assess the operational tasks execution frequency;
- quantify the failure frequency of the operational tasks and emergency procedures;
- establish for each of the operational tasks and emergency procedures a model for virtual dynamic training in the frame of Process Safety Training Program.

The identified human error scenarios can be virtually recreated by modeling operational tasks and emergency procedures, different error recovery scenarios and variable error recovery timing. The practice of "learning from mistakes" is one of the recognized HFEs (see above HFE "Learning from experience") and whenever based on personal experience gained on conventional OTS (Operator Training Simulator) and VR (Virtual Reality) OTS, designed to train respectively control room operators and field operators, it yields an improved operator response quality, a reduced operator response anxiety, an enhanced operator response effectiveness.

What above it's fully applicable to maintenance & testing tasks as well with a potential direct and indirect impact on safety and risk reduction.

References

EN 61508 "Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-related Systems"

EN 61511 "Functional Safety: Safety Instrumented Systems for the Process Industry"

HSE "Proposed framework for addressing Human Factors in IEC 61508"

HSE "Human Factors Assessment Model Validation Study"