International Journal of Performability Engineering, Vol. 10, No. 5, July 2014, pp. 487-496.

Printed in India

Human Factor Analysis Embedded in Risk Assessment of Industrial Machines: Effects on the Safety Integrity Level

MICAELA DEMICHELA[1*], ROBERTA PIRANI[2], and MARIA CHIARA LEVA[3]

[1] *SAfeR - Dipartimento di Scienza Applicata e Tecnologia, Politecnico di Torino, Corso Duca degli Abruzzi, 24 – 10129 Torino, ITALY*
[2] *Fiat Group S.p.A., Corso Settembrini, 40 – 10100 Torino, ITALY*
[3] *Aerospace Psychology Research Group – Department of Psychology, Trinity College Dublin, College Green, Dublin 2, IRELAND*

(Received on November 19, 2013, revised on May 03, May 08, and May 23,2014)

Abstract: The study consists in devising a method to account qualitatively and quantitatively for the human factor in verifying the Safety Integrity Level (SIL) assigned to machinery. Two crucial aspects have to be taken into account modelling man-machine interaction in Quantitative Risk Analysis (QRA):

1. The need to include the human interaction in the logical model of QRAs techniques;
2. The quantification of the effect of human factors.

The efforts were thus aimed at defining an improved methodological framework encompassing the integration of Human and Organisational Factors (H&OF) into safety analysis by means of quantitative risk assessment schemes.
In the end, the Integrated Dynamic Decision Analysis (IDDA) was adopted, integrated to Task Analysis. This tool allows modelling the logic of a complex system; it provides a representation of all the possible alternative states into which the system could evolve as a real logical and temporal sequence of events. The proposed model is designed with the aim of transferring the IDDA philosophy to the in-depth study of the deviations that may occur during human implementation of operational procedures and to analyse their effects on system reliability.

Keywords: *Operational SIL, Human and organisational factors, Quantitative Risk Assessment, Integrated Dynamic Decision Analysis*

1. Introduction

In the past 40 years, several research projects and programs on System Safety Engineering and Quantitative Risk Analysis offered strong evidences of the crucial role that Human and Organizational Factors (HOFs) play in major accidents. According to this increasing concern toward the relevance of HOFs in limiting safety performance of complex socio-technical systems, a considerable research effort was recently spent worldwide.
Nevertheless, many of the models and applications described in scientific literature demonstrate a very limited impact on the technical standards applied for the evaluation of safety critical equipment and procedures [1]. However regulatory requirements and standards will only be effective if design has taken into account the user's needs (usability) and reduced operating errors [2] in order to achieve expected levels of performance, *i.e.*, the standard IEC 62061 (2005) [3] contains requirements and recommendations for drafting, integrating and validating Safety-Related Electrical, electronic and programmable Control Systems (SRECS) for machinery, in relation to the significant faults to which these components could be subjected. However, no indication

* Corresponding author's email: micaela.demichela@polito.it

is provided in respect to the possible sources of malfunctions for the Safety Integrity Level (SIL) stemming from the interactions with the operators, during normal or abnormal conditions. While some aspects of human factors to be taken into account in the design of safety-related functions have been already discussed for complex hazardous installation by Kosmowski [4].

The idea of the current paper originated from a case study on a bending tool (hydraulic press): an unforeseen accident occurred, even if the press had been previously evaluated according to the above-mentioned standard. The accident was the consequence of a failure in the left button of the two-hand control safety, which caused an improper contact between the conductors of the control circuit. The analysis of the electrical circuit diagram showed that this failure allowed starting a machine cycle, the same that would have been activated if an operator had pressed the two buttons on the two-hand control safety system.

A risk analysis was carried out for the machine involved in the accident, in order to identify the lacking protective devices, and thus the priority of interventions needed to reduce the risks.

Different techniques for risk assessment have been applied to the case study and the results compared to find the more suitable procedure. In particular, two approaches have been proposed:

1. The Hazard Identification (HazId), described in Section 2, was applied for a semi-quantitative preliminary hazard assessment to identify the more critical events to be analysed more in detail through the Integrated Recursive Operability Analysis (IROA), described in Section 3.
2. The Task Analysis, as a qualitative hazard identification tool, was applied to describe the behaviour of the human-machine system; this logical model has been integrated with the analysis of the possible failures of the technical system and the final resulting model constituted the input structure for the Integrated Dynamic Decision Analysis (IDDA). IDDA allowed performing the logical and probabilistic analysis of the integrated system as detailed in Section 4.

The results of this analysis were then compared with the requirements of the most recent technical standards.

Abbreviations:

APM: Automatic Protective Means
EI: Erroneous Intervention
EIPM: Erroneous Intervention Protective Means
ESF: Engineered Safety Features
ET: Event Tree
FT: Fault Tree
HAZID: Hazard Identification
HEP: Human Error Probability
H&OF: Human and Organisational Factors
IROA: Integrated Recursive Operability Analysis
IDDA: Integrated Dynamic Decision Analysis
MI: Missing Intervention
ROA: Recursive Operability Analysis
SIL: Safety Integrity Level
TA: Task Analysis
TE: Top Event

2. Preliminary Hazard Assessment

The core of the work was the development and application of a method able to take into account the Human and Organizational Factors, and to integrate them within the risk assessment methods proposed by the technical standards usually applied for the evaluation of safety critical equipment and procedures.
A risk assessment should systematically analyse each functional part of equipment, in each mode of operation and in all operational phases, including the human-machine interaction.

For this reason the Hazard Identification approach (HazId) [5] was initially chosen to investigate the criticalities of the analysed bending tool. The HazId analysis was used as a support for the determination of the required Safety Integrity Level - SIL of the safety functions, that have to be realized through a safety system.

The results of the HazId analysis showed that the most hazardous area of the hydraulic press is the tools area, on the front side of the machine. Adequate preventive measures should be taken to deal with these relevant hazards, as stated also by technical regulations. Furthermore, HazId analysis identified the use of the machine in manual mode cycle as one of the most critical phases. Table 1 shows an extract of the whole HazId analysis, which can be found in [6].

Risk estimation was carried out for each hazard, by determining a risk parameter, R, that can be derived from the following:

- Severity of the harm, Se
- Probability of occurrence of the harm, expressed by the Class Indicator (Cl) which is obtained adding the following indexes:
    - frequency and duration of the exposure of people to the hazard, Fr;
    - index of probability of occurrence of a hazardous event, Pr;
    - possibilities to avoid or limit the harm, Av.

The definition of the indexes above mentioned is given in the standard ISO 12100 [7].

As an example, for the crushing hazard in tools' dangerous area (ref. Table 1 – line 4.1.1) the following values have been assigned to the indexes: Se= 4 irreversible consequence: death, losing an eye or arm; Fr= 5: the frequency of exposure is < 1 h; Pr=3 and Av= 3: the operators are trained and know the criticality of the machine, but failure of the machine is not always predictable in time to be avoided; thus obtaining a Cl index of 11.

N°	Phases	Hazard deviation	Cause	Consequences	Class Indicator			Se	R
					Pr	Av	Fr		
4.	Processing cycle								
4.1	Setting tools								
4.1.1	Positioning the die suitable to the type of work involved	Contact with tool	Accidental start of the machine	Hurt, crushing, cutting, upper limb amputation	3	3	4	4	40
			Gravity fall of the slide/ram because of a failure of hydraulic system	Hurt, crushing, cutting, upper limb amputation	3	1	4	4	32
4.2.	Feeding and loading raw materials								
4.2.1	Feeding of metal sheet (by hand)	Contact with tool	Accidental start of the machine because of wrong position of the safety contact.	Hurt, crushing, cutting, upper limb amputation	3	3	5	4	44

Table 1: HazId Analysis (Extract showing the More Critical Events). Indexes: Pr, probability of occurrence; Av, possibility of limiting the harm; Fr, frequency and duration of the exposure; Se, severity; R, risk.

Once Cl has been calculated and Se assigned, it is possible to use the risk matrix from the IEC 62061 – shown in Table 2 - to assign the required SIL for the protection system.
In the matrix, grey cells indicate the target SIL for each Safety-Related Control Function (SRCF). The light grey cells indicate that measures other than SIL should be used (Other Measures – OM).

Severity (Se)	Class Indicator (Cl)				
	3-4	5-7-	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Table 2: Risk Matrix for the SIL Assignment

The white cells indicate that the hazard is properly treated and the piece of equipment complies with the requirement of the Machinery Directive.
For the example above described, for a Class indicator of 11 and a Severity of 4, the target SIL should be 3.

The only protection system of the hydraulic press involved in the accident was the two-hand control system; thus, in order to prevent and/or protect the equipment from the critical events identified through the HazId analysis, it was proposed to apply light curtains safety devices and a more reliable command activation.
Once the protection system has been defined, the more critical events identified through the HazId were further analysed.

The choice of suitable deviations, based on the operator's behaviour during the use of the machine, is fundamental for the correctness of the analysis: indeed for the application of the integrated method, it is necessary to understand what are the actions of the operator able to compromise the intervention of the SRECS. This can be achieved analysing: what could happen with an improper maintenance, in which way an operator could by-pass the safety devices or what could happen if he fails in setting up the system.

In order to identify improper human behaviours, a study carried out by different institutions for statutory accident insurance and prevention was used as a support.
Institutions for statutory accident insurance and prevention (Germany and Switzerland) made a survey on a sample of 1605 workers between the years 1996 and 2000, investigating the tampering of the machinery safety devices and its causes.

The study describes the usual way to by-pass the safety devices for each type of protection system: manipulation of electro-mechanical devices by bridging, fixed guarding tampering or removing, manipulation of optoelectronic protection devices by repositioning, *etc*.

The investigation revealed that operators can usually by-pass the safety devices for the following reasons: comfort, time gain, simplification of the work and achievement pressure. This survey demonstrated once again how important it is to take into account the HOF issues starting from the design stage of the SRECS.

3. Integrated Recursive Operability Analysis (IROA)

For each critical event identified through HazId analysis, the Integrated Recursive Operability Analysis - IROA [8] was applied to take into account both Human and Organizational Factors, evaluating how workers could by-pass the safety devices. Since the method allows to directly extracting the logic trees from the analysis table for quantification purposes, it was used to calculate the "operational SIL" and to compare it with the assigned SIL, according to safety standards.
In the IROA scheme the Top Event - TE occurs if, and only if, there is an ineffective intervention of protective means. This kind of approach permitted to analyse the shortcomings descending from erroneous human interventions, but also to take into account the dynamic process of recovery, in which human intervention plays a key role. There is a real interpenetration and collaboration between technology and humans, making the system much safer.

In the IROA methodological frame, the trade-off between an optimal human–technology system and a bad one is modelled by attributing the ineffective intervention of protective devices due to the following two main causes: missing intervention of protective means and human failure.
Furthermore, the human inability to "recover" has to be taken into account in two different cases:

- if the alarm system fails or the operator fails to detect it or misread / misjudge the signal, or
- if the plant is left without Engineered Safety Features - ESFs, as a consequence of their by-passing.

In both cases, an Erroneous or Ineffective Recovery Intervention can be considered, and if it occurs, it will bring up directly to the ineffective intervention of protective devices, *i.e.*, fail to stop the wrong action.
In Table 3, an extract of the IROA is shown in relation to crushing hazard in the tools dangerous area of the hydraulic press, during the setting tools phase. The worst case of

accident can be the limb amputation due to the contact with tools, in case the automatic protective devices fail and the operator fails the recovery intervention.

Deviation	Causes	Cons eq.	Automatic Protective Means (APM)	Warning / Alarms	APM and/or alarm bypass	Erroneous or Ineffective recovery intervention	Missing Intervention of EIPM	TE
1. Accidental starting of the machine	4. Faulty contact …	Contact with tools	MI Light barrier		Light barrier	Erroneous repositioning of light barrier, no appropriate safety distance		1
			4. Faulty contactor of two-hand control devices, all the contacts remain in the energized position					
			*A third person operates the command without noticing a colleague who has his hands in the machine			Erroneous manual reset of the safety system		
			Erroneous setting of the selector switches key operated					
			Restore electricity supply after a break					

Table 3: IROA Framework for Setting Tool Phase (Extract) – TE1 Limb Amputation

As for the traditional Recursive Operability Analysis - ROA [9] [10], also the IROA was built to allow the direct extraction of the logic trees from the table of the analysis, for quantification purposes.

Once the point in which the human erroneous action may occur is identified, in order to compute the human error probability - HEP, it is necessary to perform an in-depth analysis of the human factors, to understand how and why the human action can fail.

4. The Proposed Approach

Despite the analysis can be carried on effectively with the above-described methodologies, the need for an integrated tool arose during the study, in order to avoid study fragmentation and the loss of relevant information. The Integrated Dynamic Decision Analysis – IDDA was proposed to overcome this issue [11] [12] [13] [14]. This tool allows modelling the logic of a complex system; it provides a representation of all the possible alternative states into which the system could evolve, as a real logical and temporal sequence of events.

In particular, the Task Analysis – TA [15] [16] was used as a starting point for the input logical model to IDDA, allowing to obtain a detailed qualitative and quantitative analysis of human factors during the risk assessment.

4.1 Logical-Probabilistic Model

Once the machine's behaviour and its possible malfunction has been described, the TA allows developing a detailed analysis of the operational procedure to be carried on, identifying all possible operator's error and omission or recovery interventions.

The described approach was applied to the full procedure for the use of a press, including setting of the equipment, functional check and processing material during the normal use of the machine.

For a systematic and complete task analysis, a template developed and tested on a case study related to a Gas Insulated Switchgear, was implemented [17]. Table 4 shows an extract of the performed TA.

Id.	Man-Machine function	Link to	Failure mode	Causes	Consequences
1	Work on the press (only one operator)		-		
1.1	Setting of the equipment	1.1.2	Operation by two instead of one person	Wrong operation mode	Increase probability of injury for the operator
1.1.2	Check area is clear of tools	If clear 1.1.4, if not clear 1.1.3	Omission (operator doesn't check), some operator left some tool in dangerous zone	Omitting a step or important instruction from a formal or ad hoc procedure, lack of concern	Increase probability of injury for the operator

Table 4: Template Related to Procedure using of Hydraulic Press

Once TA has been developed, the Input File (logical-probabilistic model) for IDDA was prepared through the following steps:

1. Identification of the events related to the operation of the system itself and construction of a list of levels, with questions and affirmations, which represents the elementary matter of the logical model (and also the nodes in an event tree).
2. Construction of a 'reticulum' indicating the addresses (subsequent level) to be visited after each response in each level, and a comment string that allows the user to read the logical development of a sequence.
3. Association to each of the levels of a probability, which represents the expectation degree of the failure or unwanted event and of an uncertainty ratio, which represents the distribution.
4. Definition of all the constraints, which can modify run time the model, fitting it to the current knowledge status, this fulfilling to the need to relate the probability of success or failure of different actions.

The quantitative analysis requires identifying the likelihood related to failure mode of different elements - electrical and mechanical components as human factors. Failure rate of electrical devices were provided by the manufacturer or were calculated trough the simplified approach of the technical standard EN IEC 62061. Human factor quantification was based on the Technique for Human Error Rate Prediction – THERP, due to its large database based on real data, coupled with the fact that the THERP is strongly oriented to engineering analysis of human errors [18] [19].

4.2 SIL Allocation

The software tool combines the answers to the analyst's questions exposed in the input file in all the possible ways, in order to develop all the possible alternative events that may take place in the system (constituents). These are represented as sequence of events that show, step by step, the paths chosen and the probabilities of occurrence assigned. The probability of occurrence of an injury associated with failure of the barrier or with by-pass of the device was calculated extracting 3072 relevant constituents. Their probabilities have been combined in the cumulative probability of the TE.

This probability can be associated to the probability of dangerous failure expressed in the technical standard, through the guidelines provided by the U.S. Military Standard MIL-STD-882 (1993) [20].

A probability index is thus obtained that can be used in the matrix of the technical standard EN IEC 62061 to attain the assignment of the level of integrity required for the protective system; *e.g.*, a SIL 3 requirements was obtained for the light barrier. This means that the architecture of the device has to ensure a probability of dangerous failure within 10^{-7} and 10^{-6}.

4.3 SIL Verification

To verify that the Safety-related Electrical Control System satisfies a SIL of 3, a new input file was built taking into account each single safety function, evaluating all the ways it can fail, be recovered or be by-passed by the operator.

Analysing the source file five constituents have been obtained. Being interested in the Top Event: "Light barrier is not available", a cumulative probability of 5.5×10^{-8} was found. This probability falls in the range within 10^{-9} and 10^{-7} ensuring a Safety Integrity Level – SIL 3 as requested.

5. Conclusion

This case study has shown that the performance of a safety instrumented system in the operational phase is influenced by many factors; not only by the system design and the related testing and maintenance strategies, but also by the operating conditions in the wider socio-technical system.

For this reason it is important to account for the human factor in assigning integrity levels of safety systems (SIL) to the identified safety functions.
Incorporating human factors (HFs) into safety analyses is rather difficult and complex exercise.

The use of the IDDA framework associated with Task Analysis was proposed and in the logical-probabilistic model the following element of innovation has been considered:

- It was explicitly cantered on the effects of abnormal and normal condition raising from human interactions;
- It included a critical incorporation of all useful elements of latest advances in Human Reliability Analysis methods and an explicit focus on the capability to lead in the direction of a design improvement solution and the prioritization of interventions.

The operational SIL calculated with the proposed approach is not directly comparable with the value obtained through the semi-quantitative risk analysis suggested by the technical standard EN IEC 62061. It is clear however that the Integrated Dynamic Decision Analysis allows a construction of the problem more detailed and accurate, allowing to take into consideration also the important aspect related to man-machine interface.

However, the probability of dangerous failure (PDF) calculated trough IDDA results significantly higher than the probability tied exclusively to the device architecture. By the way, the operational SIL and the SIL calculated in the previous way are the same because the range of probability in which this falls is too wide to appreciate the different results.
This study shows that more exhaustive evaluation is necessary and that the interface between the operator and the equipment cannot be neglected. Thus the integration between IDDA and Task Analysis was proposed.

If the SIL calculated in the SIL verification corresponds with the one previously assigned, both with the integrated system and with the standard's system, the SRECS will

be considered reliable also in case of a hypothetical wrong behaviour of the operator and the goal will be reached.

References

[1] Trucco, P., and M.C. Leva. *A Probabilistic Cognitive Simulator for HRA Studies (PROCOS)*. Reliability Engineering and System Safety, August 2007; 92 (8), 1117-1130.

[2] Fadier, E., and C. De la Garza C. *Towards a Proactive Safety Approach in the Design Process: the Case of Printing Machinery*. Safety Science, January – February 2007; 45 (1-2), 199-229.

[3] IEC 61062:2005, Safety of Machinery – Functional Safety of Safety-related Electrical, Electronic and Programmable Electronic Control Systems. International Electrotechnical Commission.

[4] Kosmowski, K.T. *Functional Safety Analysis including Human Factors*. International Journal of Performability Engineering. 2011: 7(1), 61-76

[5] Smith, D. J. *Reliability, Maintainability and Risk (Eighth Edition)*. Butterworth-Heinemann, Oxford, 2011; 423-425.

[6] Pirani, R.S. *La valutazione del livello di integrità dei sistemi di protezione delle macchine, dall'analisi dei rischi ai dati affidabilistici*. Ph.D. thesis, Politecnico di Torino, DISPEA – Sistemi di Produzione ed Economia dell'Azienda, 2012.

[7] ISO 12100:2010, *Safety of Machinery -- General Principles for Design -- Risk Assessment and Risk Reduction*. International Organization for Standardization.

[8] Colombo, S., and M. Demichela. *The Systematic Integration of Human Factors into Safety Analyses: An Integrated Engineering Approach*. Reliability Engineering & System Safety, December 2008; 93 (12), 1911-1921.

[9] Demichela, M., and N. Piccinini. *Risk-based Design of a Regenerative Thermal Oxidizer*. Industrial and Engineering Chemistry Research, 2004; 43 (18), 5838-5845.

[10] Piccinini, N., and M. Demichela. *Risk Based Decision-making in Plant De*sign. Canadian Journal of Chemical Engineering, 2008; 86 (3), 316-322.

[11] Demichela, M., and G. Camuncoli. *Risk based Decision Making. Discussion on Two Methodological Milestones*. Journal of Loss Prevention in the Process Industry, 2014; 28, 101-108.

[12] Demichela, M., and N. Piccinini N. *Integrated Dynamic Decision Analysis (IDDA): an Advanced Tool for Risk Analysis*. PSAM 7, International Conference on Probabilistic Safety Assessment and Management, Berlin, Germany, June 14 - 18, 2004; 2956-2961.

[13] Demichela, M., and N. Piccinini, *Integrated Dynamic Decision Analysis: a Method for PSA in Dynamic Process System*, CISAP 3, Rome, Italy, May 11-14, 2008; 249-256.

[14] Turja, A., and M. Demichela, *Risk Based Design of Allyl Chloride Production Plant*. ICheaP-10 The 10th International Conference on Chemical & Process Engineering, Florence, Italy, May 8-11, 2011; 1087-1092.

[15] Kirwan, B., and L. Ainsworth. *A Guide to Task Analysis*. Taylor & Francis Group, 1992.

[16] Embrey, D. *Task Analysis Techniques*, Human Reliability Associates Ltd, NW England. 2000.

[17] Demichela, M., and R. Pirani. *Human Factor Effects on the Safety Integrity Level Assigned to Safety-Related Electrical Control System in the Operational Phase*. 19th AR2TS Advances in Risk and Reliability Technology Symposium, Stratford upon Avon, UK, April 12-14, 2011; 28-40.

[18] Kirwan, B. *The Validation of Three Human Reliability Quantification Techniques - THERP, HEART, JHEDI: Part I - Technique Descriptions and Validation Issues*. Applied Ergonomics, December 1996; 27(6), 359-373.

[19] Kirwan, B. *The Validation of Three Human Reliability Quantification Techniques - THERP, HEART, JHEDI: Part II - Results of Validation Exercise*. Applied Ergonomics, January 1997, 28(1), 17-25.

[20] MIL-STD-882, *System Safety Program Requirements*, 1993.

Micaela Demichela is a Chemical Engineer and obtained her Ph.D. degree in Chemical Engineering in 2002 from Politecnico di Torino. Since 2006, she has been working as assistant professor at the Department of Applied Science and Technology of the Politecnico di Torino, developing her research activity not only at the Department, but also among chemical and petrochemical companies and foreign research centers. The research activity is related to several aspects of the safety in process industry: in particular, the chosen approach consisted of the integration of the deterministic modelling of the process, with the actual characteristics of the considered plant, in order to obtain a reliable assessment of the safety condition in a productive line. Since 2006 she is in charge of different safety related course for engineers, both at bachelor and Ph.D. level.
Since 2007, Micaela has been the Scientific Coordinator of several projects both national and at European level in the process safety field.
From September 2007 on Micaela is a member of the Editorial Board of the Journal of Loss Prevention in the Process Industry.

Roberta Pirani is working from October 2011 as Security Manager among the Fiat Powertrain Technology spa, dealing with the plants of Turin, Italy. She took her MSc in Environmental Engineering at the Politecnico di Torino (2004), and then she received a research grant for the TEMPUS European Project "Toshi", related to the development of training courses for workers' health and safety in high risk workplaces (2008-2009).
From 2009 to 2011, she attended at the Politecnico di Torino the Ph.D. Program in Metrology: Measuring Science and Technique, and obtained the Ph.D. degree in December 2011. In the meantime, she also attended the High specializing course in Safety Engineering and Risk Analysis.

Chiara Leva obtained in March 2007 a Ph.D. degree in Economic, Management and Industrial Engineering at the Politecnico di Milano, Milan - Italy. In June 2007, Chiara was nominated as Research Fellow in the Aerospace Research Group, School of Psychology in Trinity College Dublin. In April 2008 she was employed as a Contract Lecturer: for the course of "Human Factors" in the School of Psychology for the academic year 2008-2009, and in parallel she was also assigned the role of Contract Lecturer: in the Dublin Institute of Technology Dublin, Ireland for the courses of "Environmental Health Risk" and "Occupational Health and Safety" in the Faculty of Tourism and Food for the academic year 2008-2009. She also received a Master degree in Environmental Health and Safety Management in September 2009 from the Dublin Institute of Technology, Ireland. At the moment she is also working on various EU funded project focused on Human Factors and Safety Management applications.