CHEMICAL ENGINEERING TRANSACTIONS

VOL. 33, 2013

A publication of
AIDIC
The Italian Association
of Chemical Engineering
www.aidic.it/cet

Guest Editors: Enrico Zio, Piero Baraldi
Copyright © 2013, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-24-2; **ISSN** 1974-9791

DOI: 10.3303/CET1333076

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

Micaela Demichela[a*], Roberta Pirani[b]

[a] SAfeR - Dipartimento di Scienza Applicata e Tecnologia, Politecnico di Torino, Corso Duca degli Abruzzi, 24 – 10129 Torino, Italia
[b] Fiat Group Atomobiles S.p.A., Corso Settembrini, 40 – 10100 Torino, Italia
micaela.demichela@polito.it

The study proposed in this paper consists of devising a method to account qualitatively and quantitatively for the human factor in verifying the Integrity Level of Safety system (SIL) assigned to the machinery. It is called "operational SIL", which may differ from the design SIL, due to the impact of human and organizational factors (H&OF) in the operational phase. There are two crucial aspects related to modelling man-machine interaction in Quantitative Risk Analysis (QRA) context:

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

During the study an Operability Analysis, which is usually known with the acronym HAZOP (Hazard and Operability studies) was initially used to support the assessment, but with some added features that enable one to accommodate systematically H&OF into the process called Integrated Recursive Operability Analysis framework (IROA). This first attempt to apply IROA methodology showed that this type of analysis highlights the position where in depth human factor analysis must be carried out.

Once the point is identified in which the human erroneous action may occur it will be necessary to include the study of human factors and the assessment human error probability (HEP).

Our efforts are aimed at defining an improved methodological framework encompassing the integration of H&OF into safety analysis by means of quantitative risk assessment schemes.

In order to do that the adopted tool is the Integrated Dynamic Decision Analysis (IDDA). 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 precisely with the aim of transferring the IDDA philosophy to the in-depth study of the deviations which may occur during human implementation of operational procedures.

IDDA developed on the basis of a Task Analysis (TA) could allow to obtain a detailed quantitative analysis of human factors directly during the same risk assessment.

Starting from the analysis of a technological system through IDDA it is possible to integrate in the logical model a task analysis describing where and why the operator can cheat or by-pass the safety system thus including in the assessment explicitly the human factors that allow evaluating the operational SIL.

1. Introduction

Several research projects and programs on system safety engineering and Quantitative Risk Analysis in the last 40 years offered very 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, considerable research effort has been spent worldwide in the last couple of decades.

Nevertheless, many of the models and applications described in scientific literature demonstrate very limited impact on the technical standards applied for evaluation of safety critical equipment and procedures (Trucco and Leva, 2007). However regulatory requirements and standards will only be acceptable if design

Please cite this article as: Demichela M., Pirani R., 2013, Human factor analysis embedded in risk assessment of industrial machines: effects on the safety integrity level, Chemical Engineering Transactions, 33, 451-456 DOI: 10.3303/CET1333076

has taken into account the user’s needs (usability) and reduced operating errors (Fadier and De la Garza, 2007) in order to achieve expected levels of performance.

The standard IEC 62061 (2005) for instance 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 they are expected to be prone to. However no indication is provided in respect to the possible sources of malfunctions for the Safety Integrity Level (SIL) to be evaluated stemming from the interactions with the operators, during normal or abnormal conditions.

The idea of the current work in fact originated from a case study on a press previously evaluated according to the above standard where an unforeseen accident occurred. 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. Analysis of the electrical circuit diagram showed that this failure was enough to start a machine cycle: it was as if the operator had pressed the two buttons on the two-hand control safety.

To the machine involved in the accident a risk analysis technique has been applied in order to identify the lacking protective means and thus priority of interventions to reduce risks. The results of this analysis have been compared with the requirements of the recent technical standards.

2. Preliminary hazard assessment

The core of the work was the development and application of a method to consider human and organizational factors to be integrated with the assessment methods proposed by technical standards applied for evaluation of safety critical equipment and procedures.

A risk assessment should include a look at each functional part in turn, making sure that every mode of operation and all phases of use are properly considered, including the human-machine interaction in relation to the identified functions or functional parts. For this reason the Hazard Identification approach (HazID) was chosen to investigate the criticalities of the bending tool. The HazId analysis was used as a support for the determination of the required safety integrity level (SIL) of the safety-related functions that must be realized by a safety-related system.

HazId analysis results showed that the more hazardous area in hydraulic presses is the tools area on the front side of the machine and preventive measures have to be taken to deal with the relevant hazards, as stated also by technical regulations. One of the most critical phases revealed by the analysis is the use of the machine in manual mode cycle (Fig.1).

Risk estimation was carried out for each hazard by determining risk parameters that should be derived from the following:

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

The original machinery was not equipped with protection systems, thus from the preliminary hazard analysis it was chosen to apply light curtains protective devices and a more reliable command activation with SIL 3.

The more critical events identified through HazId were further analysed.

The choice of suitable deviations based on operator’s behaviour during the use of the machine was fundamental for the correctness of the analysis. For the application of the method it was important to understand what the operator can do on SRECS in order that the system does not react. This can be achieved studying what could happen with an improper maintenance, in which way human being may by-pass the safety devices or what happen if he fails in setting up the system. It was also necessary to determine whether the operator acted in the condition of ordinary use of the machine or during maintenance.

In order to identify improper human behaviour, a study carried out by different institutions for statutory accident insurance and prevention was used as a support.

The investigation revealed that the reasons why the operator by-pass the safety devices are due to comfort, time gain, simplification of the work and achievement pressure, emphasizing once again how important it is to take account of certain problems already at the design stage of SRECS.

The safety systems by-pass modes can be summarized in the manipulation of two hand control to gain time and work quicker and in the manipulation by repositioning of Optoelectronic protection devices to simplify the work, to relief of certain modes of operating and caused by lack of concern.

N°	Phases	Hazard Deviation	Cause	Consequences	(Cl)			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

Figure 1. HazId analysis (extract showing the more critical events).

3. Integrated Recursive Operability Analysis (IROA)

For each critical event identified through HazId analysis in a specific scenario, as material load or tool change phase, we applied IROA (Colombo and Demichela, 2008) to take into account human and organizational factors and the way in which workers could by-pass the safety devices to calculate “operational SIL” and compare it with assigned and verified SIL according to safety standard.

In the IROA scheme the Top Event (TE) occurs if, and only if, there is an ineffective intervention of protective means. This definition allows for the accounting of 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. The failure occurs actually only when the intervention of both the automatic protective means (APM) and humans fail.

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 means to the following two main causes: MI of protective means and human failure.

In the IROA concept, the human failure 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 another form of indication (misreading, misjudging, etc.), or
- if the plant is left without Engineered Safety Features (ESFs), due to their by-passing.

In both cases, a missing or ineffective intervention of Erroneous Intervention of Protective Means (EIPM) can be considered, and if its missing or ineffective intervention occurs, it will bring up directly to the ineffective intervention of protective means, i.e., fail to stop the wrong action.

We present an extract related to crushing hazard in tools’ dangerous area during the setting tools phase (Fig.2).

From the analysis the worst case of accident is limb amputation if the automatic protective means fails and if the operator fails the recovery intervention. As for as the traditional ROA, also the IROA was built to allow the direct extraction from the table of the logic trees for quantification purposes (Demichela and Piccinini, 2004; Piccinini and Demichela, 2008).

Once the point is identified in which the human erroneous action may occur it will be necessary to engage the study of human factors to understand how and why the human action fails in order to compute the human error probability (HEP).

Deviation	Causes	Conseq.	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 Erroneous manual reset of the safety system		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 setting of the selector switches key operated

Restore electricity supply after a break

Figure 2. IROA framework for setting tool phase (extract) – TE1 Limb amputation

4. The final proposed approach

In order to do that through a single analysis, a powerful tool is the Integrated Dynamic Decision Analysis – IDDA (Demichela and Piccinini, 2003; Demichela and Piccinini, 2008; Turja and Demichela, 2011). 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.
IDDA integrated with Task Analysis – TA (Kirwan and Ainsworth, 1992; Embrey, 2000) could allow to obtain a detailed quantitative analysis of human factors during the risk assessment.
The proposed model is designed precisely with the aim of transferring the I.D.D.A. philosophy to the in-depth study of the deviations which may occur during human implementation of operational procedures.
The large database based on real data, coupled with the fact that the THERP is strongly oriented to engineering analysis of human errors, led to chose this method (Kirwan, 1996; Kirwan, 1997).
Once identified the machine's behavior and the possible malfunction in which this can fall, with relatives influence for the operator, it was necessary to develop a detailed analysis of procedure to be performed, identifying all possible operator's error and omission.
A good task analysis was important requirement for the implementation of input file in I.D.D.A. software.
The new embedded methodology was applied to the full procedure for the use of a press, including setting of the equipment, functional check and processing material during normal use of the machine.
For a good and complete task analysis a template developed and tested on a case study related to a Gas Insulated Switchgear was implemented (Demichela and Pirani, 2011).

Table 1: Template related to procedure using of Hydraulic press

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

Once task analysis has been developped the second step was to prepare the Input File finalized to run the I.D.D.A. program. The task analysis related to use of press has been described with I.D.D.A.'s syntax:

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 the event tree.
2. Construction of a 'reticulum' indicating the addresses (subsequent level) to be visit 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 required to identify the likelihood related to failure mode of different elements like electrical components, human error, implemented in each level of source file; for this reason these values have been obtained from different sources. Failure rate of electrical device were provided by reliability data of the manufacturer or calculated trough the theory of technical standard EN IEC 62061.

The probability of occurrence of injury associated with failure of the barrier or with by-pass of the device in this way was calculated extracting 3072 relevant constituents. Each probability of these constituents has been calculated and added together to obtain cumulative probability.

This probability can be associated to the probability of dangerous failure expressed in the technical standard.

Once obtained the cumulative probability, it was necessary to translate it into a numerical index to apply the matrix of technical standard EN IEC 62061, thereby carrying out the assignment of the level of integrity required e.g. for the light barrier.

To justify the choice of the category in which the probability of occurrence of injury falls we have used the guidelines provided by the U.S. Military Standard MIL-STD-882 (1993).

From the application of matrix we obtained a SIL 2 for the light barrier. This means that the architecture of the device has to ensure at least the level 2 of availability.

To verify that the Safety-related Electrical Control System satisfies a Safety Integrity Level equal to three it was built a new source file that takes into account only the light barrier, evaluating all the ways it can fail or be by-passed by the operator.

At this point it is possible to verify if the cumulative probability falls in the interval of probability conservatively related to SIL 3; if it is included in that interval it satisfies the requirement previously requested (Table 2).

Table 2: Correspondence between SIL and probability of dangerous failure

SIL	PFH
3	≥ 10^{-9} to < 10^{-7}
2	≥ 10^{-7} to < 10^{-6}
1	≥ 10^{-6} to < 10^{-5}

We verified that cumulative probability falls in the range ≥ 10-9 to < 10-7 ensuring a Safety Integrity Level higher than that assigned.

5. Conclusions

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 security functions.

Incorporating human factors (HFs) into safety analyses is rather difficult and complex exercise. For the work purpose we needed of a methodological framework which could ease the way in which safety analysis may account for human an organizational factors (H&OF) since the early stages of the analysis.

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 new value calculated with the new methodological approach is not directly comparable with the value obtained by purely qualitative 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 much 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 this different result.

On the whole this study shows that more exhaustive evaluation is necessary and that the interface between the operator and the equipment cannot be neglected.

To take into account this conclusion and to comply with the previous analyzed technical standard it is necessary to assess the human factors trough a detailed task analysis. This tool has to describe every elementary action that the operator performs. For each action the analyst identifies the possible error of commission or of omission that the operator is likely to commit.

Once identified the correct sequence of tasks and the likely failure modes, the analyst is able to implement the source file to apply the Integrated Dynamic Decision Analysis (IDDA).

If the SIL calculated in the last step corresponds with the one previously assigned, the SRECS will be considered reliable also in case of a hypothetical wrong behaviour of the operator and the goal will be reached.

References

Colombo S., Demichela M., 2008, The systematic integration of human factors into safety analyses: An integrated engineering approach, Reliability Engineering & System Safety, 93 (12), 1911-1921

Demichela M., Piccinini N., 2003, Integrated dynamic decision analysis (IDDA) a new approach for risk analysis, AIDIC Conference Series, 6, 93-100

Demichela M., Piccinini N., 2004, Integrated Dynamic Decision Analysis (IDDA): an Advanced Tool for Risk Analysis, PSAM 7, International Conference on Probabilistic Safety Assessment and Management, 2004.

Demichela, M., Piccinini, N., 2004, Risk-based design of a regenerative thermal oxidizer, Industrial and Engineering Chemistry Research, 43 (18), 5838-5845

Demichela M., Piccinini N., 2008, Integrated Dynamic Decision Analysis: a method for PSA in dynamic process system, In: CISAP 3, Roma, 11-14 maggio 2008, 249-256

Demichela M., Pirani R., 201, Human Factor Effects on the Safety Integrity Level Assigned to Safety-Related Electrical Control System in the Operational Phase. In: 19th AR2TS Advances in Risk and Reliability Technology Symposium, Stratford upon Avon (UK), 12th-14th April 2011, 28-40

Embrey D., 2000, Task Analysis Techniques, Human Reliability Associates Ltd.

Fadier E., De la Garza C., 2007, Towards a proactive safety approach in the design process: the case of printing machinery, Safety Science, 45, 199-229

Kirwan B., Ainsworth L., 1992, A guide to task analysis, Taylor & Francis.

Kirwan, B., 1996, The validation of three human reliability quantification techniques - THERP, HEART, JHEDI: Part I -- technique descriptions and validation issues, Applied Ergonomics, 27(6), 359-373.

Kirwan, B., 1997, The validation of three human reliability quantification techniques - THERP, HEART, JHEDI: Part II - Results of validation exercise, Applied Ergonomics, 28(1), 17-25

IEC 61062:2005, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems. International Electrotechnical Commission.

MIL-STD-882, System Safety Program Requirements, 1993.

Piccinini, N., Demichela, M., 2008, Risk based decision-making in plant design, Canadian Journal of Chemical Engineering, 86 (3), 316-322

Turja, A., Demichela, M., 2011, Risk based design of allyl chloride production plant, Chemical Engineering Transactions, 24, 1087-1092

Trucco P., Leva M.C., 2007, A Probabilistic Cognitive Simulator for HRA studies (PROCOS), Reliability Engineering and System Safety, 92, 1117-1130