Human Error Probability Estimation for Process Risk Assessment with emphasis on Control Room Operations

Claudio Nespoli, Sabatino Ditali
Loss Prevention and Environment Department, Snamprogetti Centre of Excellence,
Business-Unit Onshore, Saipem SpA
San Donato Milanese (MI), Italy

To assess operator errors contribution to major accidents likelihood, an estimation of human errors probabilities during a credible process emergency is necessary.
In this paper, the human error probability (HEP) is the likelihood of failure to perform a corrective task in Control Room in order to prevent the hazardous event. Since human performance in diagnosing emergency situations is strongly dependent of the available time for performing correctly the requested actions, the estimations were performed for different cases, corresponding to different capabilities of the process plant to cope with the upset without loss of containment over a specified interval of time. The quantification was made by the means of THERP and HEARTH. As a result of the study it is evident that Human Factors Engineering as well as process risk assessment comprising the quantification of human error contribution should include a study of the process physics and the determination of the operators mental burden in case of credible emergency situations Independent shut-down logics should be taken into consideration in case of very quick and credible accidental sequences. Credit on the human safety barrier can be assigned only if the plant equipment is able to withstand upsets without losing equipment mechanical integrities. Although THERP is not a very recent method, it is still helpful due to its comprehensive estimation procedure and reproducibility. HEARTH is useful for quick human reliability estimations and when a specific approach is missing for the specific case study (i.e. field different to alarms handling).

1. Work organization assumptions

The usual work organization foresees one control room operator to monitor a unit and a shift manager supervisor or his assistant always present nearby. The control room is always manned, usually with more than two operators. It is assumed that when an operator is faced with dealing with an emergency, he is supported by another operator and the shift supervisor. Their support comes into play with different timings. It is assumed that final actions in the control room are straightforward because of good ergonomics. It is widely accepted that mean HEP for a generic action (i.e. button switch) is much lower than the mean HEP for diagnose an emergency. Critical alarms are those related to an existing safe concern. Non-critical alarms can have safety implications but only as causes and not as a result. There is an appropriate prioritization

of alarm annunciators that makes critical-alarms the more noticeable. If critical and non-critical alarms take place together, the critical alarm makes the others not detectable, but at the same time it is assured the detection of the critical one.

2. Cognitive assumptions

Human reliability methods in use in nuclear power plants are suitable for the assessment of human performance in process plants applications: this means the trend of the human diagnose error probability curve over the time is the same. Particularly, it depends on the complexity of the task but process control logics and instruments are basically the same. In addition, it depends on the familiarity of the potential error maker with the specific matter thus similar operators training standards are assumed. The only possible operator error considered is the omission-type error, that is, the operator error is the omission of the subtask or the whole task and not the substitution of the requested subtask with another unwanted action on the system. There is an exhaustive operating manual: procedures are previously established and in case of need the manual is accessible. It is assumed that subtasks are independent of each other, that is, an error in a previous subtask does not increase the probability of human error in the subsequent. Time perceived by the operator as the available time to intervene is the actual available time before the critical event: this means the operator does not overrate or underestimate the gravity of the emergency. Both overrating and underestimation bring about an increment of human error probabilities. Single process component failure is not a very rare event. Multiple process component failures are a rare event but operators are well trained for medalling with them. The human role in case of critical alarm triggering is associated with high emotive stress level because: the event is very rare, dealing with the emergency is an urgent matter (time available before the major event can be little), there is an important conflict of interest: shut-down a unit or worse an entire installation could bring about great economic losses, unjustified if there is an alternative. Ultimate safety emergency requiring manual emergency shut-down, in case of automatic emergency shut-down failure, is a very rare event.

3. Case studies and characteristic time definitions

Let’s consider a simple surge drum provided with two control loops. The first one controls the pressure acting on the nitrogen blanketing, while the second controls the liquid level acting on the liquid feed valve. The surge drum assures constant liquid flow rate downstream by the means of reciprocating pumps. Two critical alarms are installed on the system: one of them for high and low pressure and the other for high and low level. These alarms are directly associated with the main control loops and there are not safety independent logics prompting safety shut-downs (case A). Thus, variable deviations activating the alarms must not be very large to give time for human intervention. A safer solution is to provide a safety interlock on very high pressure or level values (case B).

A credible accidental sequence could begin with the spurious opening of the liquid feed valve and concomitant alarm on high flow-rate. The operator tries to remotely control the feed flow but he can not due the nature of the failure. He tries, as a second attempt, to close a gate valve. The level increases till the critical alarm triggers. The first HEP estimated is the probability of omission of the gate valve closure in the time between the first component failure and the first critical alarm (1^{st} HEP). Nitrogen control loop fails and the pressure goes up. Level increase has a further negative effect on the increasing internal pressure. The second HEP estimated is the omission of both stopping drum feeds and activating the manual shut-down in the time interval between the first critical alarm and the top-event (2^{nd} HEP). In case of pressure safety relief failure, overhead drum nozzle could be projected with potential domino effect or harm to workers. If automatic shut-down devices are employed (case B), a third error probability can be estimated for the omission of the requested manual shut-down following automatic shut-down failure.
Some assumptions are listed hereafter:

a) Human errors in the shut-down and start-up sequences are not in the scope of this paper;

b) After the main process variable being monitored has exceeded the first limit (operating limit), there is no sense in operating a manual shut-down. The potential reduction in top-event frequency would be too penalising in terms of production losses. Indeed automatic shut-down means should be employed only when the deviation of the process variable is very large and the situation is close to the loss of containment. Moreover considerations about criticality of shut-down and start-up procedures are still valid. The operator tries to cope with the situation as from operating manual. The manual guidelines come from balancing economic and production enhancement with risk reduction management;

c) Indications of process variables are always coupled with alarms if there is a minimum safety concern about the equipment involved;

Since human performance is strongly affected by the available time for performing correctly the requested actions, the estimations were performed for different cases, corresponding to different capabilities of the process plant to withstand the upset without equipment mechanical breakdowns over a specified interval of time. The categories are defined in table 1.

Table 1 Typical model times for different process plant response

Process plant reaction versus subtask HEPs	Very slow (min)	Slow (min)	Intermediate (min)	Fast (min)	Very fast (min)
1^{st} HEP (A&B)	50	30	10	5	< 1
2^{nd} HEP (A)	105	63	22	11	< 1
2^{nd} HEP (B)	100	60	20	10	< 1
3^{rd} HEP(B)	5	3	2	1	< 1

HEP calculation does not vary from case A to case B. In the following only case B will be addressed.

4. Human Reliability Methods employment

The choice of the proper HEP estimation methods was made on the basis of high level of accuracy and reproducibility. THERP and HEARTH have been widely used, studied and validated over the last decades [1,2]. According to THERP method, there exist three types of task: routine, ruled-based and knowledge-based tasks. Knowledge based tasks require actions planning because the problem to solve is almost new or only partially similar to previous. Ruled-based tasks require selection of the correct procedure to apply (diagnose), attention and capability to follow pre-establish path without omissions. Routine tasks require minimal attention because they have been performed so many times that the operator is capable to solve the task mechanically. THERP method provides users with time reliability curves to be selected on the base of the aforementioned task categorization [3]. HEARTH quantification method requires the human reliability analyst to select the proper generic HEP among various pre-established task categories, then this probability has to be multiplied by factors to take into account error producing specific conditions of the case study [4]. The analyst is given the maximum multipliers values and is requested to quantify the needed multiplier between the unity and the maximum values. The error producing conditions, which can be applied, are:

- high emotive stress level,
- time shortage,
- unfamiliarity with the task (rarity of the occurrence) and,
- Interest conflict.

While THERP provides users with guidelines for reducing the estimated HEP in order to take account of positively influencing conditions, HEARTH does not consider factors enhancing human performances (i.e. long time available for the intervention).

The following assumptions were made in order to apply THERP and HEARTH methodologies:

1. Single process component failures are not a very rare event. Recognising a single failure event can, on a conservative side, be regarded as rule-based task. Multiple process component failures are a rare event but operators are well versed therefore the diagnose is ruled-based, save the case of a needed manual shut-down that is assumed to be a knowledge-based task;

2. Shift supervisor diagnose is a knowledge based task. Shift manager deals with the emergency in a manner different to the operator strategy. If the shift-manager followed the same rule-based method, he would useless because he could be wrong as the operator. In terms of method's employment there would be almost a complete dependency. In case of operator error also shift manager would be possibly wrong. Indeed a shift supervisor is the one called to employ his expertise to solve specific problems, which the operator alone has failed to deal with;

3. Deciding whether to activate a manual shut-down or not is a tricky problem because many considerations are to be made in order to select the correct way of actions.

5. Results Discussion

Table 2 THERP results (taking into account other crew members and shift manager)

Plant reaction responses versus subtask HEPs	Very slow (min)	Slow (min)	Intermediate (min)	Fast (min)	Very fast (min)
1st HEP	0.0005	0.001	0.1	0.5	1
2nd HEP	0.0001	0.0001	0.01	0.1	1
3rd HEP	0.5	≈ 1	≈ 1	≈ 1	1
Task HEP	≈ 0	≈ 0	**0.001**	**0.05**	**1**

Table 3 HEARTH results (taking into account shift manager support)

Plant reaction responses versus subtask HEPs	Very slow (min)	Slow (min)	Intermediate (min)	Fast (min)	Very fast (min)
1st HEP	0.07	0.07	0.3	0.77	0.77
2nd HEP	0.01	0.01	0.04	0.16	0.77
3rd HEP	≈ 1	≈ 1	≈ 1	≈ 1	≈ 1
Task HEP	**≈ 0.001**	**≈ 0.001**	**≈ 0.01**	**≈ 0.1**	**≈ 0.6**

If the alarm/indication requires interpretation of a specific pattern of symptoms, then the HEP can be high. On the contrary, if the alarm is self-explanatory, that is the corrective remedy is almost suggested by the alarm, then diagnose HEP is quite low (indeed the current consol devices give support for troubleshooting component failures on the base of the operating manual). In case of automatic shut-down failure, if a safety culture establishes the must for the operator of activating the shut-down key and the operator is given sufficient time it is possible to decrease significantly the loss of containment frequency. Independent shut-down logics should be taken into consideration in case of very quick and credible accidental sequences. Credit on the human safety barrier can be assigned only if the process plant is able to withstand upsets without losing equipment mechanical integrities. Numerical results from the two methods are in substantial agreement, however since the differences are due to the analyst it is recommended to relate on THERP output. For the task complexity along with available time are the most performance influencing factors, prior to applying this paper numerical results it is advisable to assure that very tricky diagnoses are not being addressed. This would imply that only knowledge based tasks are applicable. In the case of very tricky diagnose problems it is suggested to use ASEP, a very conservative screening method derived from THERP, together with the knowledge based time reliability curve [5]. HEARTH estimations for a very fast accidental sequence are limited by the maximum error-producing conditions multipliers. As HEARTH manual prescribes, it is analyst's duty to

modify the results if deemed necessary. THERP is a time-consuming method and requires practise. Human reliability curves and detailed guidelines on their use account for a good reproducibility of the results. Conversely, analyst subjective judgement makes HEARTH dependent of the user expertise with consequent high potential for biases. However, HEARTH rationale is simple and quick to apply. Moreover, the wide task categorization makes HEARTH useful in non-process scopes as well.

6. Conclusions

Human factors engineering as well as process risk assessment comprising the quantification of human error contribution should include a study of the process physics and the determination of the operators' mental burden in case of credible emergency situations. Independent shut-down logics should be taken into consideration in case of very quick and credible accidental sequences. Credit on the human safety barrier can be assigned only if the process plant is able to withstand upsets without losing equipment mechanical integrities. Although THERP is not a very recent method, it proved to be still valid because of its comprehensive estimation procedure and reproducibility. Prior to using THERP, it could advisable to try a simplified version, ASEP, which is valid as a screening tool. ASEP is very conservative and its output is validated. On one hand, HEARTH is useful for quick human reliability estimations and when a specific approach is missing for the specific case study (i.e. field different to alarms handling). On the other hand, it requires analyst subjective contribution to the estimation therefore for this paper case study analysis, THERP is more suitable.

References

[1] Kirwan, B. (1996). The validation of three human reliability quantification techniques, THERP, HEARTH and JHEDI: Part I technique descriptions and validation issues. *Applied ergonomics, 28 (6), 359-373;*

[2] Kirwan, B., Kennedy, R., Taylor-Adams, S. and Lambert, B. (1997). The validation of three human reliability quantification techniques, THERP, HEARTH and JHEDI: Part II results of validation exercise. *Applied ergonomics, 28 (1), 17-25;*

[3] William, J.C. (1992). A User Manual for the HEARTH Human Reliability Assessment Method. Prepared for Nuclear Electric plc. (C2547-1.001).

[4] Swain, A.D., & Guttmann, H.E. (1983). Handbook of Human Reliability Analysis with emphasis on Nuclear Power Plant Applications, NUREG/CE-1278. Washington, DC: US Nuclear Regulatory Commission;

[5] Swain, A.D. (1987). Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CE-4772. Washington, DC: US Nuclear Regulatory Commission.