Advances in Social Sciences Research Journal – Vol.3, No.10
Publication Date: Oct. 25, 2016
DoI:10.14738/assrj.310.2275.
Calixto, E. (2016). The human factors in the Hybrid Risk Analysis Approach: FTA, BTA and HRA integrated approach applied to assess the influence of human error to the risk of plant shutdown. *Advances in Social Sciences Research Journal,* 3*(10)* 75-89.

The Human factors in the Hybrid Risk analysis approach: FTA, BTA and HRA integrated approach applied to assess the influence of human error to the risk of Plant shutdown

Dr. Eduardo Calixto
ECC, Germany, Ravensburge Straße 12, Ulm 89079 Germany

Abstract

The paper aim to demonstrate the importance of human error in risk analysis by applying the hybrid risk analysis, which encompasses the Fault Tree Analysis as well as the Bow Tie Analysis, including the human error probability as a result of human reliability analysis. Therefore, the brief explanation of the risk analysis such as FTA and BTA as well as different human reliability analysis, such as ASEP, SPAH-R and HEART will be presented. In order to exemplify the importance of hybrid risk analysis considering human factor, the emergency shutdown, valve (ESDV) procedure case will be demonstrated which consider the real time in response event based on dynamic simulation results. The result will show how important is to consider human factors together with risk analysis to support decisions during an operational critical event which can lead a total plant shut down.

Key words: Fault Tree Analysis, Bow Tie Analysis, Hybrid Analyis, Human reliability Analysis, ASEP, SPAH-R, HEART

Introduction

The Risk assessment has been very well applied in the last decades, enabling the improvement of risk management throughout the asset's life cycled for different industries such as Nuclear, Oil and gas, Chemical, Metallurgy, Railway, Aerospace & defence, Military and Automotive. Additionally, it has been realized the more application of different risk analysis methods not only during the project phase, but during the operational phase in order to analyse the risk when some asset concept modification takes place, asset revamp or in cases of incidents and accident. Nevertheless, the lack of human factor in risk analysis is still an issue that must be improved in order to mitigate the root cause of many risks and accident. Despite the recognized fact of human factor being the root cause of many incidents and accident, most of industries organization are not applying the human reliability analysis and including the human factor systematically in their risk assessment. Such fact may explain why major accident still happens despite of all improvement and effort implemented by different organization in different industries in the last decades.

The lack of human reliability analysis as a baseline for risk assessment can be explained for the misunderstood about the human reliability analysis approach or even for the belief that it´s not possible to predict human error. In the first case, it´s necessary more effort to train people on the human reliability concept an enable the specialist to contribute with their knowledge about human factor to enable more robust risk assessment.

A successful case of human reliability analysis application has been taking place for decades in the nuclear industry who has been developing different human reliability analysis methods and has been included such methods in their procedures to assess and mitigate risk. Even in this case, is not systematically in place the application of the hybrid risk assessment approach which consider the human error probability based on human reliability analysis as an input for different risk analysis methods.

Therefore, this paper aims to demonstrate the hybrid risk assessment approach based on different risk analysis and human reliability methods applied to a real case of plant shutdown risk assessment. The human reliability analysis, concept will be introduced as well as the different HRA methods such as the Accident Sequence Evaluation Program (ASEP), Human Error Assessment Reduction Technique (HEART), Standardized Plant Analysis, Risk Human Reliability (SPAR-H), Human Error Assessment Reduction Technique (HEART). Furthermore, the risk analysis methods such as Fault Tree analysis (FTA) and Bow Tie Anlalysis (BTA) will also be briefly explained. Finally, the case application will show the real application of hybrid risk assessment which integrate the FTA analysis with the BTA analysis concerning the results of human error probability derived from HRA.

HUMAN RELIABILITY ANALYSIS

Human reliability analysis began in the 1950s. A basic timeline is as follows:

- In 1958, Williams suggested the importance of considering human reliability in System reliability analysis (Williams, 1988).
- In 1960, reliability studies showed that some equipment failures were influenced by human actions.
- In 1972, the Institute of Electrical and Electronics Engineers (IEEE) published a report about human reliability.
- In 1975, Swain and Guttmann proposed the first human reliability approach to solving human failures in atomic reactor operations (Swain and Guttmann, 1980). The main objective of THERP (Technique for Human Error Prediction) was to understand operational sequential actions to define human error probability and prevent human failures (Spurgin, 2010).

From the 1970s on, several methodologies were proposed and published by the U.S. Nuclear Regulatory Commission (USNRC) and other industries and governmental organizations.

In general terms, human reliability methods were developed in three stages. The first stage (1970–1990) was known as the first generation of human reliability methods, and it focused on human error probabilities and human operational errors.

The second phase (1990–2005) was known as the second generation of human reliability methods, and it focused on human performance-shaping factors (PSFs) and cognitive processes. Human performance-shaping factors are internal or external and, in general, include everything that influences human performance, such as workload, stress, sociological issues, psychological issues, illness, etc.

Finally, the third phase, the third generation of human reliability methods, started in 2005 and continues today and focuses on human performance shaping factors, relations, and dependencies.

The first concept that is applied to different HRA methods and must be clarified is the human error. Basically, there are two types of human error such as:

- The Omission error, which happens when one action is not performed due to lapse or misperception. For example, in preventive incident actions, omission, error is the misperception of an alarm (and consequently not performing the actions required). In maintenance, omission, error is when equipment fails as soon as corrective maintenance is conducted due to lapse, which means some steps of corrective maintenance procedures were not performed.

- Commission error, which happens when an action is performed incorrectly due to an incorrect quantity or quality of action or a mistake in selecting or proceeding with a sequence. For example, in preventive incident actions, commission error is selecting the wrong command or making a mistake in the sequence of actions required. Equipment degradation repair is a commission error when the repair is performed incorrectly.
- In addition to understanding the human error types it is necessary to understand the factors that influence them. There are many factors that influence human error such as human performance-shaping factors (internal or external) and human behaviour. Internal human performance-shaping factors depend on individual characteristics including:
- Psychological: related to emotional issues such as stress, overworked psyche, depression, demotivation, no concentration.
- Physiologic: related to physical issues such as health conditions, diseases.
- Such factors can be monitored to guarantee that employees will be in better physical and psychological shape to perform critical actions.External human performance-shaping factors are technological and social.
- Technological: Related to work conditions, tools, and technology, such as ergonomics, procedures, equipment.
- Social: Related to social issues in and out of the workplace, such as poor social conditions, lack of acceptance in the group.
- In order to predict the human error probability, the different HRA method can be applied. In this paper will be considered the ASEP, SPAH-R and HEART methods.

The Accident Sequence Evaluation Program (ASEP)

The Accident Sequence Evaluation Program (ASEP) approach assesses an action before an accident happens. The ASEP human reliability analysis procedure consists of a pre-accident human reliability analysis and post- accident human reliability analysis. The ASEP is an abbreviated and slightly modified version of THERP in some terms. The ASEP provides a shorter route to human reliability analysis as human error probability is predefined, requiring less training to use the tool compared to other human reliability analysis methods (Bell and Holroyd, 2009). The four procedures and two general approaches involved in this method are described as follows:

- Pre-accident tasks: Those tasks that, if performed incorrectly, could result in the unavailability of necessary systems or components to respond appropriately to an accident.
- Post-accident tasks: Those tasks that are intended to assist the plant in an abnormal event, that is, to return the plant’s systems to safe conditions.
- Even pre-accident and post-accident analysis have screening and nominal approaches that differ from less and more conservative human error probability values, respectively.

For the purpose of the paper the pre-accident task will be taking into account. Therefore, concerning the time to perform an action the figure 1 shows the probability of 60% to have a human error when the response must be carried out in less than 10 minutes.

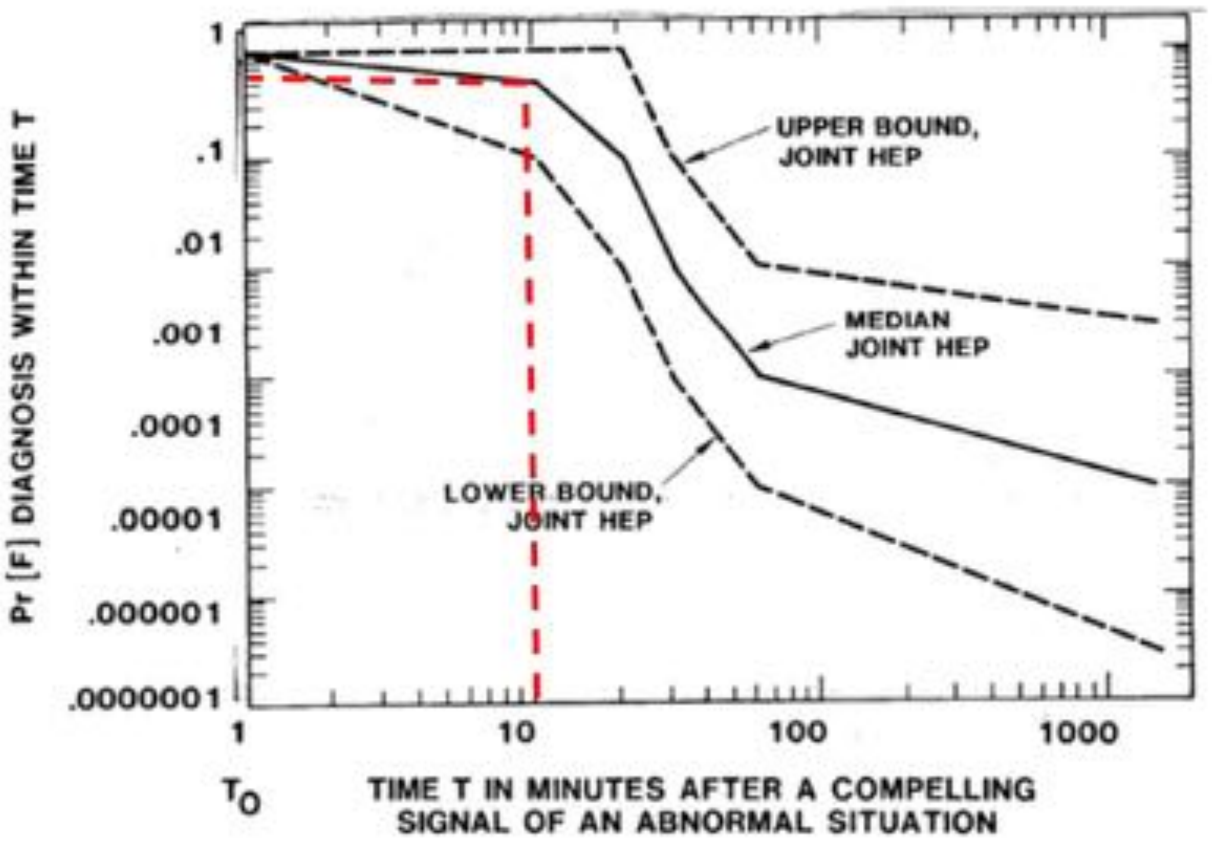

Figure 1. Nominal Diagnose Model (estimate HEPs and UCBs for diagnoses within time)

Human Error Assessment Reduction Technique (HEART)

In 1985, the Human Error Assessment Reduction Technique (HEART) was presented for Williams and after 3 years described in detail. Thus, in general, this methodology is applied to analysing human tasks with defined values for human error probability (nominal human reliability) related to activities and for contexts where each activity is involved. Based on such values the final human error probability formula for activities and error- producing conditions are calculated. The general application steps are as follows:

1. Define the activity.
2. Define the corresponding generic task and define the nominal human unreliability.
3. Define the error-producing condition related to the activity.
4. Assess the rate of the error-producing condition.
5. Calculate the final human error probability.

To calculate the final human error probability this equation is applied:

$$Final\ HEP = GEP \times \prod R(i) \times (Wi - 1) + 1$$

Where:

GEP=Generic Error probability (is defined in generic task table 5-4)

R(i)=Value of context task (based on generic context task table 5-5 values)

W(i)=Weigh for each context task defined for specialist opinion.

To define final human error probability the first step is to define the task that is best defined in Table 1. Thus, nominal human unreliability is chosen from the proposal range values on the right.

	Generic Tasks	Nominal Human Unreliability	
A	Totally unfamiliar, performed at speed with no real idea of likely consequences.	0,55	(0,35-0,97)
B	Shift or restore system to a new or original state on a single attempt without supervision or procedures.	0,26	(0,14-0,42)
C	Complex task requiring high level of comprehention and skill.	0,16	(0,12-0,28)
D	Fairly simple task performed rapidly or given scant attention.	0,09	(0,06-0,13)
E	Routine, highly practised, rapid task involving relatively low level of skill	0,02	(0,07-0,045)
F	Restore or shift a system to original or new state following procedures with some checking.	0,003	(0,0008-0,007)
G	Completely familiar, well-designed, highly practised, routine task ocurring several times per day, performed to highest possibe standards by highly motivated, highlytrained and experienced personnel, with time to correct potential error, but without the benefit of significant job aid.	0,0004	(0,00008-0,009)
H	Respond correctly to system command even when there is an augments or automated supervisory system providing accurate interpratation of system state	0,00002	(0,000006-0,009) 5th-95th percentible bound

Table 1 Generic Tasks and Nominal Human Unreliability Source – Willians, 1988.

Standardized Plant Analysis Risk Human Reliability (SPAR-H)

In support of the Accident Sequence Precursor Program (ASP), the U.S. Nuclear Regulatory Commission

(NRC), in conjunction with the Idaho National Laboratory (INL), in 1994 developed the Accident Sequence Precursor Standardized Plant Analysis Risk Retain Human Reliability (ASP/SPAR) model for the human reliability analysis method, which was used in the development of nuclear power plant (NPP) models. Based on experience gained in field testing, this method was updated in 1999 and renamed SPAR-H, for Standardized Plant Analysis Risk-Human Reliability method (NUREG/CR-6883).

The main objective is to define human error probability based on human performance factors influence. Such methodology requires a specialist opinion to define the human factors influence based on performance-shaping factor values. The performance factors include human error probability as shown in the following equation.Equation 1

$$HEP = \frac{NHEP \cdot PSF_{composite}}{NHEP \cdot \left(PSF_{composite} - 1\right) + 1}$$

Such a method establishes the value of human error probability of omission error (0.01) and commission error (0.001). The SPAR-H method is based on eight performance-shaping factors (Boring and Gertman, 2005) that encap- sulate the majority of the contributors to human error. These eight perfor- mance-shaping factors are as follows: available time to complete task, stress and stressors, experience and training, task complexity, ergonomics, the quality of any procedures in use, fitness for duty, and work processes. Each performanceshaping factor feature is listed with different levels and associated multipliers. For example, the presence of extremely high stress would receive a higher multiplier than moderate stress. Table 5-11 shows the performance-shaping factor values used to define the performance-shaping factor composite.

The SPAR-H method is straightforward, easy to apply, and is based on human performance and results from human performance studies available in the behavioural sciences literature (NUREG/CR-6883).

The main question concerning human factors in the SPAR-H method is the relation between such human factors and how they influence human reliability. The relation between performance-shaping factors can be represented as shown in Figure 5-16.

To illustrate the SPAR-H method an example of human error in the startup of a compressor in a propylene plant, which shows that a supply energy breakdown caused the propylene plant shutdown. One of the most complex pieces of equipment to start up is a compressor, and in this case, the compressor was new and the operators and maintenance team were not familiar with the startup steps and relied on a general procedure. In addition, whenever there is a propylene plant shutdown there's a high stress level to get the plant started again so as not to experience an additional loss of production. Based on the compressor startup scenario information, Table 512 shows the classification for human performance-shaping factors.

Table 2: PSF values
Source – NUREG, CR-6883

PSFs	PSF Level	Multiplier for Ation
Available time	Inadequate Time Time Available » Time required Nominal time Time Available ^{3} 5x Time required Time Available ^{3} 50x Time required Insufficient information	P(f)=1 10 1 0.1 0.01 1
Stress	Estreme High Nominal Insufficient information	5 2 1 1
Complexity	Highly complex Moderatey complex Nominal Insufficient information	5 2 11

Experience/ Training	Low
	Nominal
	High
	Insufficient information
		3
		1
		0.5 1

Procedures	Not Availble Incomplete Available, but poor Nominal Insufficient information	50 20 5 1 1

Ergonomics	Missing /Misleading
	Poor
	Nominal
	Good
	Insufficient information
		50
		10 1
		0.5
		1

Fitness for dutty	Unfit Degrate fitness Nominal Insufficient information	P(f)=1 5 1 1
Work proess	Poor Nominal Good Insufficient information	5 1 0,5 1

Risk analysis (FTA and BTA)

Risk Analysis and Management started around middle of twenty centuries in different industries with different approaches like:

- In 1960's - Aerospace Industry with Quantitative Risk Assessment methods, Nuclear Industry with Probabilistic Risk Assessment approach,
- In 1970's - Chemic Industry with Quantitative Risk Assessment and Seveso directive
- In 1980's - Oil and Gas Industry with Quantitative Risk Assessment and Safety Case,

By definition, the risk is the combination of an event of hazard and its consequence. In order to analyse and evaluate the risk, the qualitative and quantitative approach can be performed. In this paper the Bow Tie Analysis and the FTA analysis will be taking into account to provide the hybrid risk analysis we will also consider HRA.

Fault Tree Analysis (FTA)

FTA has been used since 1961, and the first application was conducted to assess a missile control system. FTA is a quantitative risk analysis method that defines event combinations that trigger top events. In FTA the first step is to define top events and then the main event (intermediary and basic) and logic gates that are necessary to calculate the top event probability. Thus, top events are usually accidents or equipment failures, and from top event down to basic events the combination of events is depicted. To calculate the top event probability based on intermediary and basic event combinations Boolean logic is needed. The fault tree is built up based on a different gate combination such as: or, and, priority and, exclusive or, stand by, undeveloped. The objective of this paper is not to have a full description of the FTA, which has already been described in several other papers. In fact, the main objective is to build up an FTA together with other methods such as BTA and HRA. An example of FTA is demonstrated in figure 2 which the event gate or combine the two other events called omission error (A)and commission error (B). The basis for the calculation for this FTA is simply described by equations: $P(A) \cup P(B) = P(A) + P(B) - (P(A) \times P(B)$.

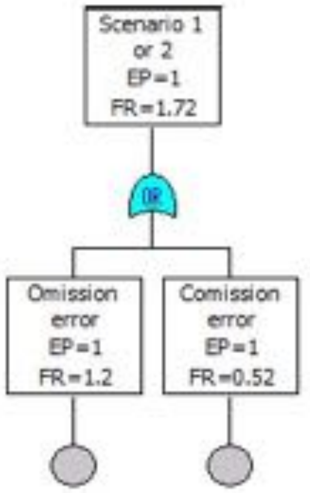

Figure 2 FTA for Omission or Commission error

Bow Tie Analysis (BTA)

Bow tie analysis is the newest quantitative risk analysis and has been in use since the 1970s. It has been incorporated by the Shell Oil Company into the hazards management at the beginning of 1990.

The bow tie analysis includes FTA, ETA, and LOPA concepts and allows reliability engineers to assess all combinations of events from incident causes to incident consequences for the layers of protection that prevent accidents and mitigate consequences. Such methodology can be used to assess different types of problems, but in safety terms, this type of analysis is used to assess and support accident analysis, process hazards, and perform risk management.

An example of bow tie analysis is an incident of pipeline methane leakage ass shown in Figure 6-48. On the left side of the bow tie all elements as follows:

- Potential causes (corrosion, pipeline disruption and flood, natural disaster)
- Control measures (PM & inspection, reliability specification, security, and storm forecast)
- Loss of control (pipeline methane leakage)
- Recovery measures (emergency response)
- Consequences (toxic gas release, jet fire, explosion, and fireball)

Whether pipeline methane leakage occur the different consequences such as Toxic gas release, Jet fire, Explosion and fireball may occur. Some actions such as Emergency response and the layers of protection might mitigate such accident consequence. These layers of protection can also be represented in the Bow Tie analysis as a control or recovery actions as shows figure 3.

The control measures that must take place to avoid corrosion are pipeline reliability specifications and inspection and preventive maintenance. Considering that the pipeline disruption is caused by sabotage, the security control must be implemented. In case of seismic events, the storm forecast must be implemented to predict the possible rain storms.

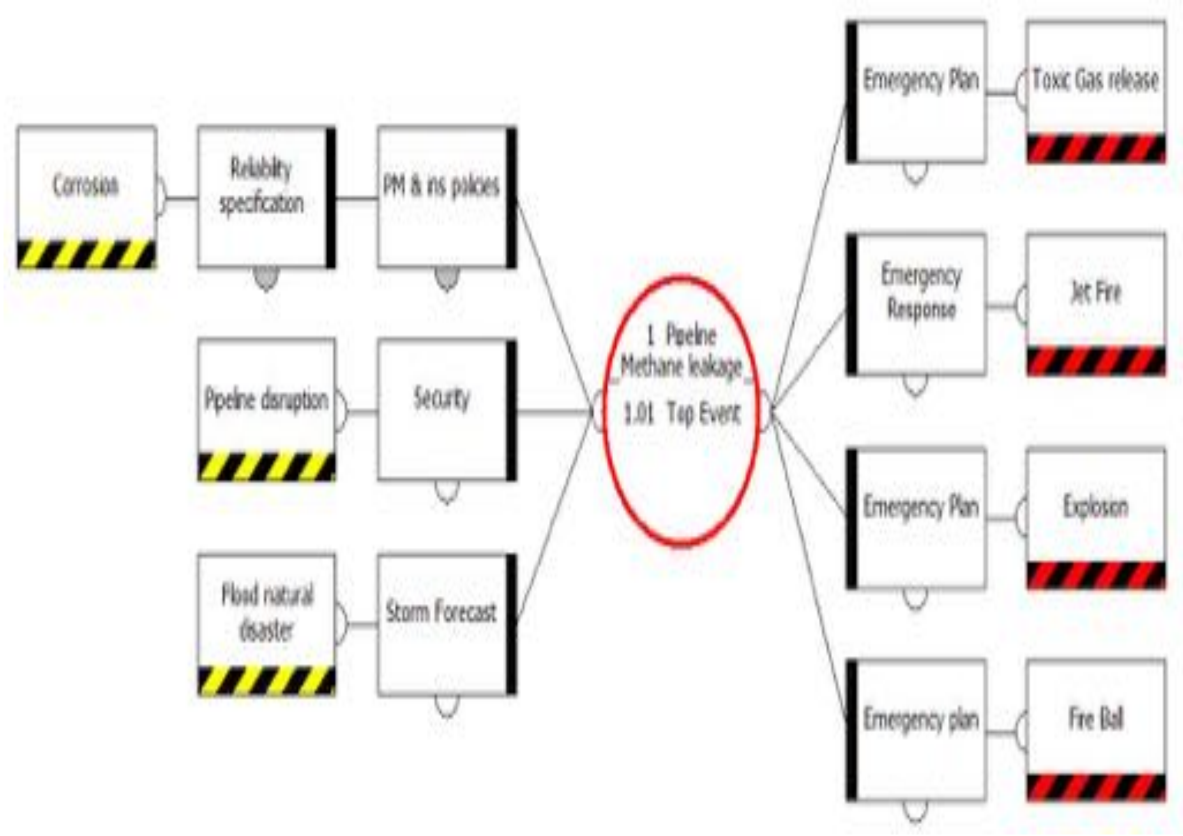

Figure 3: Bow Tie Analysis: Pipeline Methane Leakage (control and recovery measures)
Source; Calixto Eduardo, 2016

A HYBRID RISK APPROACH APPLIED TO PLANT SHUTDOWN ASSESSMENT CASE

The purpose of this case study is to demonstrate the Hybrid risk analysis, including Human reliability analysis, Bow Tie and Fault tree analysis. Therefore, the case study focuses on shutdown caused by the spurious closure of an ESDV on a transfer line leading to zero flow through that line. The purpose of the case study is to determine whether there is smooth operation following the trip of a single CRM line and identify any consequential process trips figure 4 shows that when ESDVcloses, the mass flow through the East Transfer Line drops to zero. The total mass export rate also falls, before recovering to a flow rate of around 530,000 kg/h, which is lower than the initial total export flow of around 690,000 kg/h.

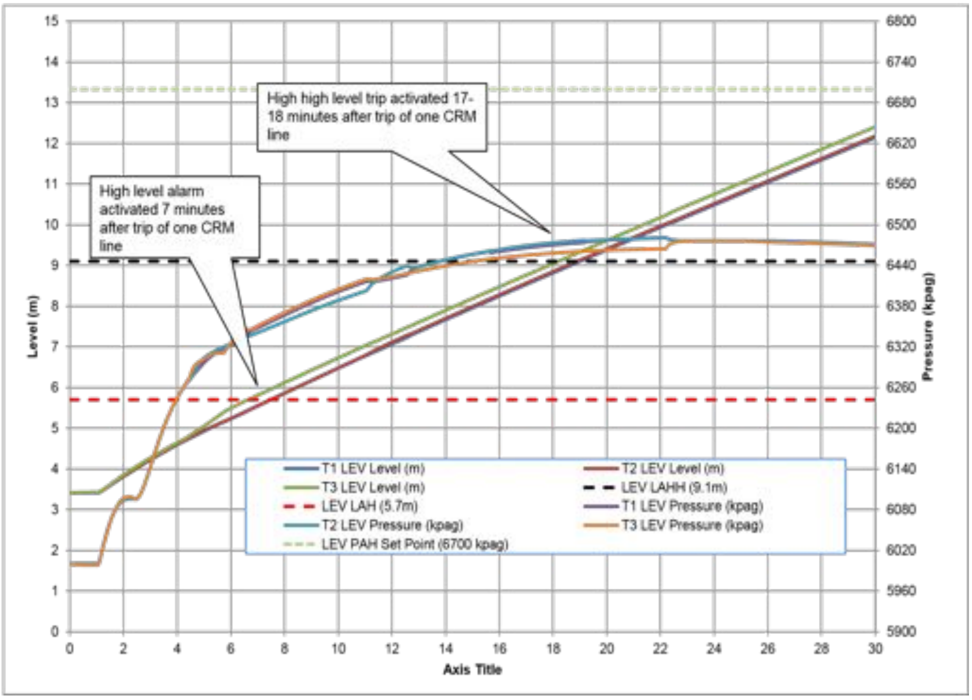

Figure 4: CRM Transfer Line Flow and Pressure

The figure above is a result of dynamic simulation result which consider the sequence of events below. At:

T = 0 min, Initial Conditions as above;
T = 1 min, ESDV at Transfer Line inlet close with a closure time of 12 seconds.
T = 17 min, Liquid level in the 3 LEVs will reach the LZHH trip set point with a single flow line operating. The trip actions were not simulated as part of this run.
T = 30 min, Simulation ends.

Human reliability: SPAR-H and ASEP application

The human reliability analysis qualifies the human intervention in terms of the probability of the operator making an error and consequently, leading to a total plant shut down. This paragraph effectively calculates the frequency of total shutdowns incurred as a result of this scenario when relying on a specific operator action.

The error is effectively the operator either:

- Completely missing the first-out alarm that came up, i.e. the high pressure at the inlet of the CRM, i.e. an omission error or
- Recognizing the alarm, but not performing the correct action as per the procedure, i.e. commission error.

Note that for the former omission, error it takes a single operator, i.e. the control room operator to miss the alarm.

In addition, the later commission error, it involves both the control room and the field operator. The scenario is as follows:

It is expected that by time t = 14min (10 min from the first alarm) operator should be able to understand the issue and the route cause. At that time he has, however, been receiving continuous alarms since the incident that may impede his judgement (distractions) or enhance his judgement. He is expected to receive at least 5 alarms during that period, i.e. the 2 high pressure CRM alarms and the 3 high level LEV alarms. General standards allow operator 10 minutes to react to an alarm. So, by this moment he will try to contact the field operator to fix the problem and open the valve.

The field operator, if he is close to the valve he can try to open it locally. If the valve does not open he will call back into the control room operator to explain the issue. It is assumed here that the valve cannot open or reset from the control room being a shutdown valve. It can only open or reset from the field.

If the field operator happens to be away from the valve, it is impossible to react to any instructions within 10min.

The control room operator has to co-ordinate the actions of the field operator with his decision to trip or not the single Train following the procedure. If the time since the alarm approaches 10min then he needs to trip the Train.

Tripping the train involves pressing two physical ESD pushbutton that is located very close to the operator console. One for the LEP/LEV trains and one for the production train. The commission error in steps (a) – (c) can be one of the following:

- Control room operator forgetting that he needs to act within 10min, i.e. neglecting the procedure.
- The control room operator does recognize the alarm, but long after it occurred, say 5min. He does not realize that the time to act is less than 10min, i.e. only 5min because the alarm activated long before he acknowledged it.
- The field operator starts talking to control room operator about other issues diverting his attention.
- Another incident happens that also diverts the attention of the control room operator.
- The control room operator does everything right, but presses the wrong ESD push-button and either does not trip any train or he trips the whole plant.

The computation of the probability of human error is as follows:

- Omission error Probability

The omission, error probability is computed using the ASEP method (Appendix A). Error! Reference source not found.3 suggests that a 10 min response time leads to a 60% failure rate. The same result can be obtained by using method SPAR-H., NHEP = 0.13 for a simple task performed rapidly (Task type: D) which is the recognition of the alarm and the action to trip one train in 10min. The NHEP is 0.13, i.e. the upper bound of category D. The task is not complex (pressing a single physical pushbutton), there is no reason to suggest that procedures, training and ergonomics are not in place for such an activity. The available time is, however, the same as the required time if in the 10min we include the diagnosis. High stress is not considered, because prior to the CRM blockage it is assumed that there has not been any other incident. Otherwise, a double jeopardy case arises. Hence, the PSF composite value is 1. As a result, based on the equation (17) the HEP = 0.6 which is the same as the value of 0.6 predicted by the ASEP method.

SPAH-R : Commission error Probability

There are clearly two potential errors here, one for the field and one for the control room operator.

The rate of failure of the commission error is computed based on the SPAR-H method. The PFS values considered for the field operator error probability are shown in table 2 along with the justification. The PFS composite is predicted as shown in equation below:

PFScomposite = PFS (available time) x PFS (Stress) x PFS (complexity) x PFS (Experience/Training) x PFS

(Procedures) x PFS (Ergonomics) x PFS (Fitness for duty) x PFS (Work process) PFScomposite = 1 x 2 x 1 x 1 x 1 x 1 x 1 x 1=2 (2)

For the control room operator error, Error! Reference source not found. illustrates the PSF. The PFS composite predicted is:

PFScomposite = PFS (available time) x PFS (Stress) x PFS (complexity) x PFS (Experience/Training) x PFS
(Procedures) x PFS (Ergonomics) x PFS (Fitness for duty) x PFS (Work process)

PFScomposite = 10 x 5 x 1 x 1 x 1 x 1 x 1 x 1=50

The next step is to calculate the HEP. In order to calculate the human error probability it's necessary to define the nominal human error probability. Based on current SPAR-H procedures, the NHEP for commission error is 0.001. In fact, this value defined by the standard is very low and will not reflect the human error during early life phase. In case of operational phase, such value can be applied to predict the HEP. In order to define the NHEP for early life phase, will be applied based on Human error assessment reduction technique.

Based on HEART nominal human error definition, table 1, the respective task and human probability error are:

- Field Operator Action - task B – NHEP = 0.14
- Control room operator Action (commission error) - task F – NHEP = 0.007

Thus, the field operator and control room operator commission error human probability are:

Field Operator Action error:

$$\mathrm{HEP} = \frac{0.14\times 2}{0.14\times(2-1)+1} = 0.25 = 25\%$$

Control room operator action (after field operator fails to recover)

$$\mathrm{HEP} = \frac{0.007\times 100}{0.007\times(100-1)+1} = 0.26 = 26\%$$

The decision of whether to trip one Train and performing it correctly is contingent on the control room operator. As a result, it is highly unlikely that the Field Operator error will influence the decision making of the control room. As a result, for the frequency of shutdowns only the control room operator (6) unreliability will be considered.

Bow Tie Case study application

The next step is to calculate the frequency of shutdowns due to this upset scenario, i.e. CRM inlet valve closure, while accounting for the human reliability. The BTA will be applied in this Safety instrumented function risk analysis. The main objective predicts the frequency of plant shutdown/ year considering the human error of operator and control room operator in different recovery action scenarios.

The frequency of ESDV valve failure considers as 1 per year based on the company database. The failure rate of a single component is significantly lower than that in the order of 1 failure per 100 or even 104 years depending on the SIL level. However, when considering the combination of components and also the chance of a human error, this rate can indeed be close to one failure per year. Note there are two identical trains, hence two of the CRM valves can fail to close. Such frequency can also be calculated based on real failure historical data. Consequently, once such data are available a lifetime data analysis is required. Combining the valve failure rate and the operator reliability calculations is shown in figure 5 and 6.

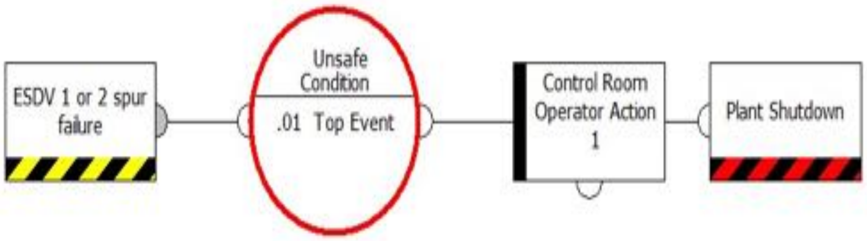

Figure 5: Scenario 1 – Detection mistake (omission error)

F (System Shut Down) = F (ESDV Train 1 or Train 2 Fails) x P (Control Room Operator action Fails) = 2 x 0.6 = 1.2 Plant Shutdown/ year (7)

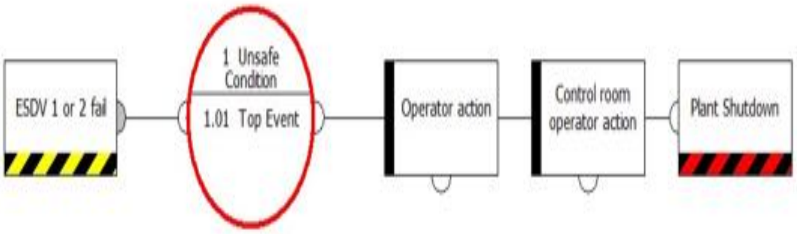

Figure 6: Scenario 2 – Field Operator not recovering and control room operator recovery action not successful

F (System Shut Down) = F (ESDV 1 or 2 Fails) x P (Field Operator action Fails) x P (Control Room Operator action Fails)
= 2 x 1 x 0.26 = 0.52 Plant Shutdown/ year (8)

As the field operator action is a failure (did not manage to open the valve), it is considered as 1 the contribution to the event failure rate. The omission, error is independent of the commission error. Hence, the combination of the two needs to be considered to calculate the total failure rate that will be demonstrated on the next item.

Hybrid method case application

The complete Hybrid diagram, which encompasses both FTA and Bow tie is represented in figure 7. This implies around 1 shutdown every year due to CRM valve failure that occurs once a year. However, given that there are 2 CRM lines and hence valves, the chance of any of them failing is once every year, i.e. twice a year. The operator contribution manages to reduce the impact of the plant shutdown to once every year, i.e. a 2-fold improvement. However, if the valve failure rate changes, the operator performance are expected to change. More frequent valve failure will render the operator more familiar with the procedure that will minimize the error. While a rare valve failure, may catch the operator unprepared and oblivious of the procedure he has to follow if the adverse event occurs.

From this analysis, it can be deduced that an automated system is required in order to prevent the plant-wide trip following the CRM inlet valve inadvertent closure. Relying on the operator will not reduce the shutdown rate significantly. The automated system can take a combination of measurements and with a time delay send a signal to trip Train 1 LEV/LEP and Train 1 of the gas production side (ISV, HP Separator etc.). The logic recommended is:

If Pressure at CRM measured by PZT-109A/B/C (receiver B) inlet is high (above alarm of 7500 KPag) and the CRM ESDV-094 or 078 (Receiver B) are closed then after a delay of 10min trip Train 1. The pressure transmitter is already wired in the ESD, while it has to be ensured that the ESDV valves limit switches are also wired to the ESD.

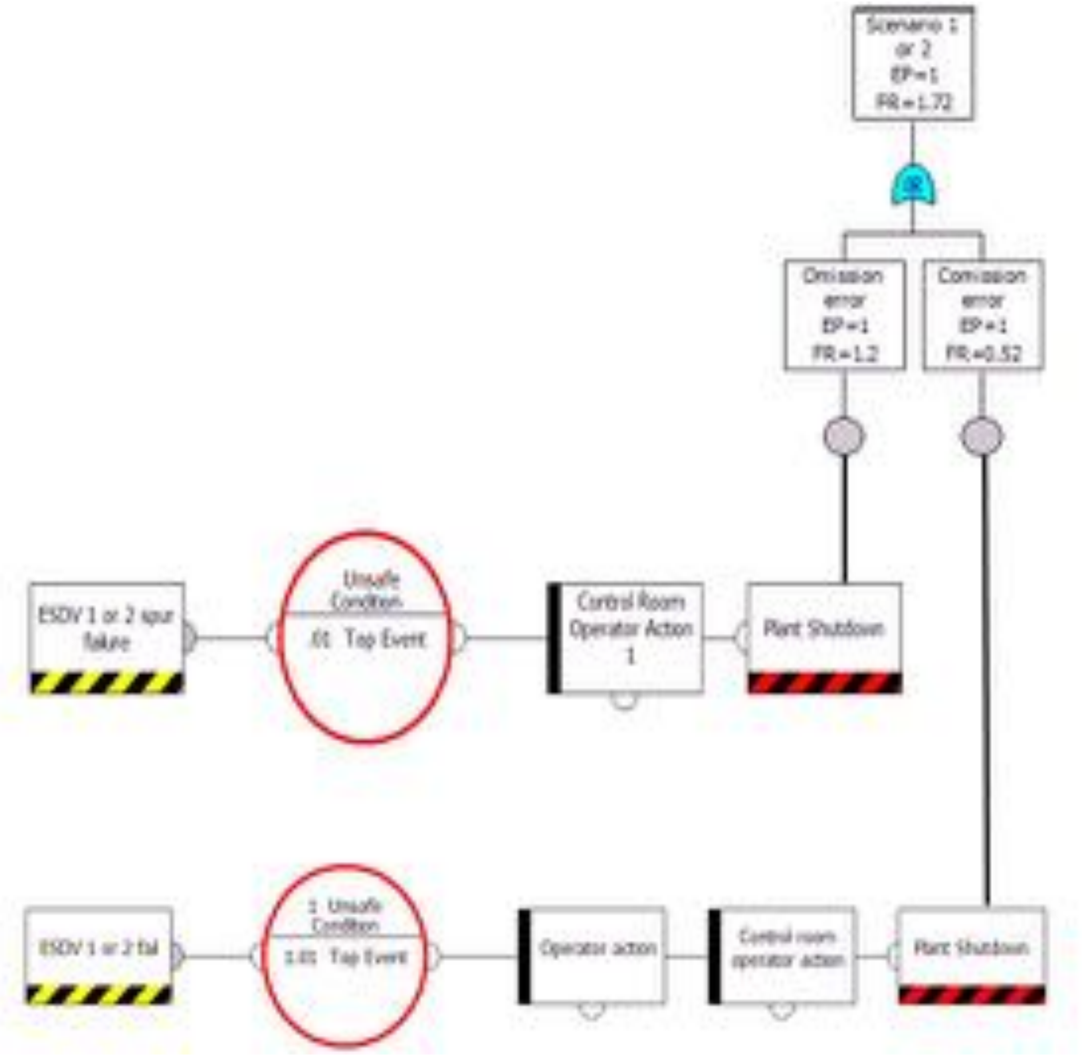

Figure 7 Complete Hybrid model Diagram

CONCLUSIONS

The paper has demonstrated the importance of human error in risk analysis by applying the hybrid risk analysis, which encompasses the Fault Tree Analysis as well as the Bow Tie Analysis, including the human error probability as a result of human reliability analysis. Therefore, the hybrid analysis was applied to the emergency shutdown, valve (ESDV) procedure case concerning the real time in response event based on dynamic simulation results. The final result shown how important is to consider human factors together with risk analysis to support decisions during an operational critical event which can lead a total plant shut down.

Based on the sensitivity analysis to avoid cascade trips on all CPF trains following a CRM line inlet blockage it is recommended to:

- Reduce the high pressure alarm setting at the inlet to the CRM from 7800 KPag to 6200 KPag in the LP mode to alert the operator early about the CRM blockage. Otherwise, the response time becomes closer to the available time increasing 10 fold the probability of operator failure.
- Make sure the operating instruction is such that if a high pressure alarm at the inlet of the CRMs is triggered to check if there is a blockage in the CRM lines. If the blockage is confirmed and cannot be recovered, i.e. unblock or re-open failed valve, he has 20min from the alarm activation to trip one of the trains in order to prevent multiple train trips.
- Implementing recommendations 1 & 2 there is a 0.332 frequency of total plant shutdown following the upset, provided the single ESDV valve has a combined failure rate of 1 per year.

The hybrid risk analysis allows to perform a complete assessment which encompasses equipments failures or incident events together with human error. The next step is to consider the dependency on time event when BTA and FTA is performed in order to mitigate the risk over time.

Bibliography

Calixto, E., 2015. Safety Science: Methods to Prevent Incidents and Worker Health Damage at the Workplace. DOI: 10.2174/97816080595221150101. eISBN: 978-1-60805-952-2, 2015. ISBN: 978-1-60805-953-9.bethamebook.

Calixto E, Brito Gilson Alves Lima2, Firmino Paulo Renato Alves 3 Comparing SLIM, SPAR-H and Bayesian Network Methodologies.Open Journal of Safety Science and Technology, 2013, 3, 31-41 doi:10.4236/ojsst.2013.32004 Published Online June 2013 (http://www.scirp.org/journal/ojsst).

Ericson, C., 1999. Fault tree analysis-A history. 17th International System Safety Conference, EUA, Orlando, FL.

SWAIN, A D.Accident Sequence Evaluation Program Human Reliability Analysis Procedure. NUREG/CR4772.February 1987.

Swain A. D. and H. E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, draft, NUREG/CR-1278,October 1980.

NUREG/CR 4772

NUREG/CR-6883,INL/EXT-05-00509.