Accident Analysis and Prevention xxx (2008) xxx–xxx

Contents lists available at ScienceDirect

Accident Analysis and Prevention

journal homepage: www.elsevier.com/locate/aap

Combining task analysis and fault tree analysis for accident and incident analysis: A case study from Bulgaria

Doytchin E. Doytchev*, Gerd Szwillus

Faculty of Computer Science, Electrical Engineering and Mathematics, University of Paderborn, 33102 Paderborn, Germany

ARTICLE INFO

Article history:
Received 20 June 2008
Accepted 12 July 2008

Keywords:
Incident analysis
Task analysis
Human error identification
Performance shaping factors
Fault tree analysis

ABSTRACT

Understanding the reasons for incident and accident occurrence is important for an organization's safety. Different methods have been developed to achieve this goal. To better understand the human behaviour in incident occurrence we propose an analysis concept that combines Fault Tree Analysis (FTA) and Task Analysis (TA). The former method identifies the root causes of an accident/incident, while the latter analyses the way people perform the tasks in their work environment and how they interact with machines or colleagues. These methods were complemented with the use of the Human Error Identification in System Tools (HEIST) methodology and the concept of Performance Shaping Factors (PSF) to deepen the insight into the error modes of an operator's behaviour. HEIST shows the external error modes that caused the human error and the factors that prompted the human to err. To show the validity of the approach, a case study at a Bulgarian Hydro power plant was carried out. An incident – the flooding of the plant's basement – was analysed by combining the afore-mentioned methods. The case study shows that Task Analysis in combination with other methods can be applied successfully to human error analysis, revealing details about erroneous actions in a realistic situation.

1. Introduction

Accidents and incidents have occurred since the invention of the first machine and the beginning of the industrial revolution. Despite the efforts of mankind to prevent or avoid them, they continue to occur, the reasons usually being complex. An accident may be based on 10 or more events that can be counted as causes (SETON, 2006). One failure may lead to another and a chain reaction may propagate through barriers and time to produce an undesired event. The most common reasons for accident/incident occurrence are failure of people, equipment, supplies, or surroundings to behave or react as expected.

The work of Hollnagel (1999), Johnson (2003), Kirwan (1994) and Petersen (1996) are of exceptional importance to understand why accidents/incidents occur and how to prevent them. Most traditional engineering accident/incident analysis techniques focus on the technical components of the system that failed. An exception is the human related HAZOP method (Redmill et al., 1999), which is focused on human error in the context of a technical system and was developed for the process and chemical industry. Today, due to the complexity of the processes carried out and the corresponding man-machine interfaces, the share of human error in accidents/incidents occurrence has increased. As reported by the Federal Aviation Administration (Clemens, 2002) "... more than seventy percent of all crashes of scheduled commercial aircraft are caused directly by 'controlled flight' into terrain." The same percentage (human-error contribution) holds for the chemical industry.

This paper is divided in 7 sections. It presents the reasons for accidents/incidents occurrence in Bulgarian industry—an aspiring EU member country.[1] Section 3 introduces the basic concepts of accidents/incidents analysis. The next chapter sketches the concepts of the proposed analysis approach, followed by the presentation of a case study. We close by presenting the results obtained from the application of the analysis approach and give some conclusions.

* Corresponding author. Tel.: +49 5251 606623; fax: +49 5251 606619.
E-mail address: doytchin@upb.de (D.E. Doytchev).

[1] Since 2007, Bulgaria is an official EU member. This paper, was first presented at the ESREL 2006 conference, before Bulgaria had joined the EU.

0001-4575/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.aap.2008.07.014

2. Safety in Bulgarian industry

2.1. Health and safety conditions of work in Bulgarian industry

Bulgaria has about 30 large potentially hazardous plants on its territory, including power plants (hydro, thermal, and nuclear), refineries, production plants (chemical, metallurgical, machine, etc.) and a shipyard (SACP, 2005). The remaining power, metallurgical and chemical plants on the territory of Bulgaria, though smaller in size or capacity in comparison, should also be considered when accounting for the total number of plants with high-risk production units. According to the analysis, made by the Executive Agency "Labour inspection" (EAGLI, 2004, 2005a,b) for provision of health and safety conditions at work in Bulgarian industry, certain progress has been made, and but problems still exit. The results, which we discuss in a short overview here, are presented jointly for the metallurgical, chemical branch of industry and the plants generating thermal and electrical energy.

2.1.1. Achievements

In all enterprises and power plants inspected by the Executive Agency, the main requirements of the Health and Safety (H&S) regulations are fulfilled: a risk assessment of the places of work and the production process is carried out, employees are provided with services by the Office of "Labour medicine" (referred to as the "Office"),[2] committees or groups responsible for conditions of safety work are established, as well as health and safety departments, or gas rescue departments. Most of the companies have implemented the ISO 9001:2000 standard. Some have even implemented an integrated environmental, quality and safety management system according to the requirements of ISO 90001:2000, 14001:20002 and OHSAS 18001. The rest are following suit. Training and educational systems for health and safety conditions of work have been established in all companies. Every newly appointed employee must undertake and pass a course dealing with H&S conditions of work, according to the specifics of his working place and profession. In general, the main process equipment is well maintained. Measurements of the parameters of the working environment are carried out annually by companies externally authorized by the Ministry of Health or by the "Office". The production output from these three sectors has increased visibly in comparison with 2003.

2.1.2. Problems

Although risk assessment is performed in all companies of these three branches, and safety departments are established, the assessments carried out are incomplete, according to the requirements of article 3 of Ordinance N 5/11.V.1999 of the Ministry of Labour and Social Policy and Ministry of Health. In most cases during the risk assessment implementation, the specific hazards and harms, resulting from operation with hazardous chemical substances and products, are not identified. The level of safeguarding the production process and the safety of machines in manufacturing sectors of companies from the metallurgical industry in particular is neglected. In some of the enterprises, the risk assessment is based on out-of-date measurements of the working environment parameters. In most of the high-risk chemical companies, the main process equipment is more than 30 year old. Therefore, the relative share of employees working in bad conditions (combined negative influence of different parameters of the working environment like noise, dust, harmful substances, especially carcinogenic chemical substances, exceeding the threshold limits of the Ministry of Health) is still high. A general wrongdoing in metallurgical companies is that repaired equipment is set back in operation, without proving sufficiently its safe performance or guarantee the safety of its employees. Controlling compliance with health and safety at work regulations by top management is not performed strictly enough, including the implementation of duties in this area by operators and employees. Overall, there is a lack of control and demand for the development of an organization of work which ensures accident free and health secure working conditions.

The data for the metallurgical industry from the observed breaches of health and safety and labour regulation by the EA shows that 40% of them are due to lapses in organization and management of health and safety activity, 36% are due to lapses in provision of safety at work, 21% are due to problems with provision of hygiene labour conditions and 3% due to legislative issues. The percentages for the power plants, regarding the same problems, are similar.

3. Accident and incidents analysis

3.1. Purpose and definition

The purpose of accident and incident analysis is to determine their causes and the specific factors that contribute to them. The analysis gives insight into what went wrong in order to take counter-measures to avoid recurrence. During the analysis, information is collected about the workplace, the work itself, the work process, and the process technology involved.

In the literature (Blacket, 2005; Johnson, 2003) different definitions of accidents and incidents exist. There is general agreement, however, that an accident can be defined as "an undesired event or sequence of events causing injury, ill-health or property damage" (NRMC, 2006), while an incident is "an unplanned, undesired event that hinders completion of a task and may cause injury or other damage" (NRMC, 2006). Incidents can include human operator injury that results in a short absence from work, minor damage to a smaller part of the system, or failure of a component—but these events do not lead to a disruption of the system as a whole (Blacket, 2005). There are five primary accident analyses types, as defined by Stellman (1998):

- Analyses and identification of where and which types of accidents occur.
- Analyses with respect to monitoring developments in the incidence of accidents.[3]
- Analyses to prioritize initiatives that call for high degrees of risk measurement, which in turn involve calculating the frequency and seriousness of accidents.
- Analyses to determine how accidents occurred and, especially, to establish both direct and underlying causes, and
- Analyses for elucidation of special areas which have otherwise attracted attention (a sort of rediscovery or control analyses).

In the following we take a closer look on existing accident analysis techniques.

3.2. Accident analysis techniques

There are many ways to analyse an accident or an incident. Traditional analytical techniques deal mainly with the identification

[2] The Office is an external centre that provides medical and health services and examination of company's employees.

[3] This type of analysis looks at factors that affect the process operation and could lead to accident and urges for monitoring the effectiveness of preventive activities (Stellman, 1998).

Please cite this article in press as: Doytchev, D.E., Szwillus, G., Combining task analysis and fault tree analysis for accident and incident analysis: A case study from Bulgaria. Accid. Anal. Prev. (2008), doi:10.1016/j.aap.2008.07.014

of event sequences, looking for unsafe acts or conditions leading to the accident. Such techniques include the Why-because analysis, Sequence of events (domino effect), Sequential time and events plotting, Multilinear events sequencing and technique of operations review and change analysis (Blacket, 2005; Johnson, 2003). Causal analysis goes beyond identifying what happened, but looks deeper into why it happened (Johnson, 2003).

A widely used method for analysing the reasons for a past accident or incident is the Fault Tree Analysis (FTA). Fault trees show failures that have to occur or did occur to cause an undesired event. They start with a top event, describing the failure. Through a series of logic gates (such as AND and OR), displaying the various logical combinations leading to the failure, the top event is decomposed to subsidiary and basic events. The basic events are located at the bottom as the leaves of the tree. The basic events may be human errors, hardware or software failures, or environmental events (Modarres, 1993). The analysis of fault trees can be conducted in a qualitative or a quantitative manner. The aim of FTA is to find the minimal cut set—a combination of minimum basic events whose occurrence will cause the top event. Through analysis of the cut sets actions can be prioritised to prevent the top event from occurring and find weak points in the system.

3.3. Analysing the human component of an accident

As mentioned before, the percentage of human-error contribution to accidents and incidents has increased. Therefore, understanding the reasons for human error is quite important in understanding the reasons for accident/incident occurrence. "Human errors have become widely recognized as a major contributory cause of serious accidents in a wide range of industries" (Hollywell, 1996). In addition, there has been a growing appreciation that the systematic consideration of human error in the design, operation, and maintenance of highly complex systems can lead to improved safety and more efficient operation (Hollywell, 1996). Work place design, corporate and safety culture, in addition to training, competence, task complexity, stress, etc. constitute a group of factors that influence operators' behaviour. These factors are called Performance Shaping Factors (PSF) (Kim and Jung, 2003). These factors concern all work related areas (e.g. operating environment, task and operator characteristics) that exert certain influence on the operators performance. They are used in human error analysis techniques (Kirwan, 1994); in tools for identification of latent operational conditions (CCHS, 2007) and "can be cause of some failures in other complex industrial systems" (Cilingir and Mackhieh, 1998; Bellamy et al., 2008).

Hollnagel (1998) and Kirwan (1994) have listed different human error analysis techniques, including ATHEANA (A Technique for Human Error Analysis), CREAM (Cognitive Reliability and Error Analysis Method), HEART (Human Error Analysis and Reduction Technique), HEIST (Human Error Identification in System Tools), THERP (Technique for Human Error Rate Prediction) and others. The goal of these techniques is to determine the reasons for human error occurrence, the factors that influence human performance, and how likely the errors are to occur. Only in HEIST the error likelihood is not estimated.

Another methodology used for the assessment and reduction of human error, according to Embrey (2000), is the task analysis, which is less focussed towards the psychological aspects of human behaviour, but concentrates on work flow and organization.

3.4. Task analysis perspective for human error

Task Analysis is the process of analysing the way people perform the tasks in their work environment and how these tasks are refined into subtasks. It is a method of describing and analysing how the operators interact both with the system itself and with other personnel in that system. It can be used to create a detailed picture of human involvement using all the information necessary for an analysis in an adequate degree of details (Kirwan, 1994). There are several variants of task analysis resulting from different purposes, as described in Brauchler and Landau (1998a,b), Callan et al. (2008). The result of a task analysis is a Task Model.

A widely used form of task analysis is the hierarchical task analysis (HTA). It involves identifying the overall goal of the task and the various sub-tasks and the conditions under which they should be carried out to achieve that goal. Through its hierarchical approach it provides a well-structured overview of the work processes even in realistically sized examples. Other analysis techniques known are the Tabular Task Analysis, Timeline analysis, Operator Action Event Trees, the GOMS-methods (Goals, Operators, Methods, and Selection Rules), Critical Action and Decision Evaluation Technique and others (Embrey, 2000). The most popular and widespread notation and tool for HTA is the Concur Task Tree Environment CTTE (Paterno et al., 2001). HTA is an easy to use method of gathering and organising information about human activities and human interaction, and enables the analyst to find safety critical tasks. It is time-consuming in case of complex tasks and requires the cooperation of experts from the application domain, knowledgeable about the task operation conditions. Today, task analysis has found application in several areas, such as the allocation of functions (to specify whether a human or machine function is needed), in interface design (in design stage of a new system or the modification of an existing system), job design (whom do we need and how do the job functions interact with the existing ones), training and procedures (what training and job aids are required), staffing and organisation (how many people are needed), and human reliability assessment (Kirwan, 1994). The application mentioned last is of importance for understanding the reasons for human error, since it includes the process of error identification, analysis and quantification. In our case, we focus on the task analysis application in the error identification part, which deals with the question of what can go/has gone wrong in a system from the human action point of view.

In our practical work we used a system developed in our group called TOMBOLA (Uhr, 2003) complemented with the graphical editor GAME (Habbe, 2005). An excerpt of the task model created during the analysis of the case study is given in Fig. 1. It shows the decomposition of the overall actions responding to the emergency situation as a task hierarchy. The tool provides a graphical interface to the user to create, open, and edit existing models, as well as perform simulations. Simulation means that the model can be executed to verify its correctness or observe how the task performance will change in the presence of certain conditions. Within the model, tasks are presented in a hierarchical manner starting from the top task (the goal) to the very low (atomic) level. For each non-atomic task a temporal relation (one of: sequential, serial, parallel, simultaneous, alternative, optional and loop) is specified, which specifies the temporal ordering of subtask execution. The temporal relations are shown in a rectangle at the bottom of the task. It may also contain the so-called auto-start and auto-stop option (denoted by the green or red circles)[4] that specify the task to be executed and stopped automatically without user interference. In

[4] In the TOMBOLA programme the auto-start and auto-stop condition appear as green and red circle. In the black and white print out, from the two circles located at the top-left angle in the rectangular, the auto-start condition is the one on the left side. The auto-stop condition is the one on the right side.

Please cite this article in press as: Doytchev, D.E., Szwillus, G., Combining task analysis and fault tree analysis for accident and incident analysis: A case study from Bulgaria. Accid. Anal. Prev. (2008), doi:10.1016/j.aap.2008.07.014

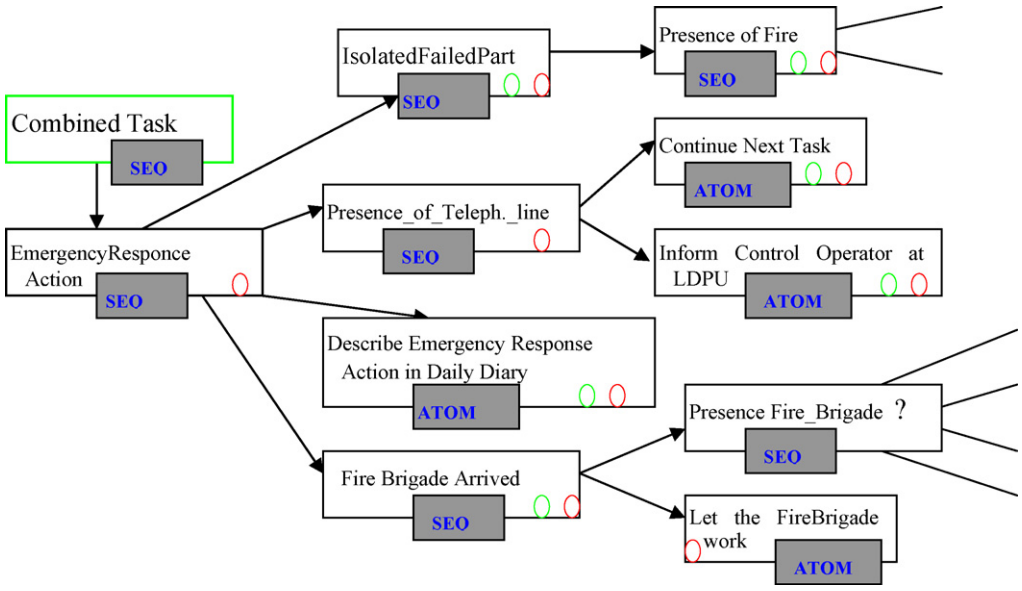

Fig. 1. Excerpt[a] of a task model developed with Tombola. [a]The figure corresponds exactly to snapshot developed with TOMBOLA, as presented in "D. Doytchev, G. Szwillus. Combining task analysis and fault tree analysis for accident and incident. . . ESREL 2006 Safety and Reliability Conference, September 2006", but Windows block graphics are used for better clarity, which the snapshot of the tool does not allow.

addition, tasks may have pre and/or post-conditions (requirements that should be fulfilled before, resp. after the task is executed). The pre-/post-conditions are "an expression involving object variables" (Uhr, 2003) and denoted with a question mark. The variables that can be specified by the user in each task can have integer, string, boolean, class types or arrays format. The variables are used by the simulator and the data model. A complete description of the TOMBOLA programme is given in Uhr (2003).

4. The analysis approach

In the previous section, we gave a brief overview of methods and techniques for accident/incident analysis from the literature. These methods are focused either on the failure of the "hardware", i.e. a machine or a computer, or the human component. Some of the methods, such as THERP and HAZOP, are rather complex and require the involvement of several persons. On the other hand, in traditional engineering failure analysis techniques, the analysis of the contribution of human error to accident/incident occurrence is under-represented; which holds vice-versa for the human error analysis techniques, like TRACERlight (Shorrock and Kirwan, 2002).

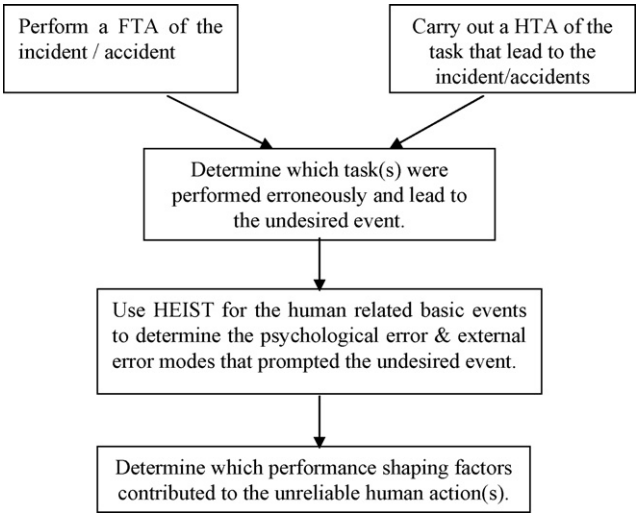

Fig. 2. Flowchart of the analysis approach.

To overcome this separation we propose an analysis approach, illustrated in Fig. 2, which combines a traditional engineering accident analysis method, namely Fault Tree Analysis, with task analysis, as a means to represent human behaviour when operating systems. Both methods use a tree structure and basic or atomic events and have been in use for a long time. The two methods have a predetermined sequence in the way elements are connected: AND-OR-gates between events for fault tree analysis, and temporal specifications such as parallelism or simultaneous performance for task analysis. For both, programming tools have been developed and can complement each other quite well. The task analysis can explicitly show where in the work process implementation the human error occurred, which is then related to the basic event in fault tree analysis. By combining the two methods, the analyst can see which tasks correspond to the failure event in the FTA.

First the FTA is implemented to establish the root-causes of the undesired event. Then task analysis is carried out. It describes the sequence of tasks that were performed and lead to the undesired event. Next a match between the human related basic event(s) from the FTA and the task(s) from the task tree corresponding to activities in the basic event(s) is established. Thus the task(s) that lead to the undesired event is/are defined. A task is defined as critical if it contributes directly to the undesired event. The match allows to see the correspondence between the two trees involved and is performed by mapping error conditions in the FTA to task nodes in the task model. We plan to support this matching step with an appropriate tool in the near future.

To deeper elicit the external error modes that prompted the errors and understand the type of errors committed by the human the Human Error Identification in Systems Tool (HEIST) method was added to the method. The reason for choosing HEIST was because "it can be used by a single assessor", though "it is more theoretical as method" (Kirwan, 1994). The method begins with an *error identification question*, related to the observable *external error modes* and the underlying *system cause/psychological error mechanism* that

Please cite this article in press as: Doytchev, D.E., Szwillus, G., Combining task analysis and fault tree analysis for accident and incident analysis: A case study from Bulgaria. Accid. Anal. Prev. (2008), doi:10.1016/j.aap.2008.07.014

Table 1
Excerpt from the Human Error Identification in System Tools (HEIST) method.

Code	Error identification prompt	External error mode	System cause/psychological error—mechanism	Error-reduction guidelines
PEP1	Could the operator carry out the task inadequately?	Error of quality; or wrong action; or omission of action	Manual variability prompting; random fluctuation; misprompting; misperception; memory failure	Training; ergonomic design of equipment; ergonomic procedures; accurate and timely feedback; error recovery potential; supervision
EVO1	Could the team/supervisor/operator omit key parameters in the evaluation process (i.e. fail to check them)?	Error of quality (inadequate evaluation), wrong action	Failure to consider side effects; inadequate mental model; bounded rationally	Procedural evaluation aids; team training; function-based displays and procedures
OP2	Could the operator forget one or more items in the procedures)?	Action omitted or performed either to early or to late; or wrong act performed	Forget isolated act; slip of memory: place-losing error	Ensure an ergonomic procedure design; utilize tick-off sheets, place keeping aid, etc. team training to emphasis the checking by other team member(s)
IDO3	Will it be clear who must respond?	Action omitted or performed too late	Crew-coordination failure	Training and task allocation among crew; team training
IDO4	Could information collected fail to be transmitted effectively across shift-handover boundaries?	Failed to act; or wrong action performed; or action performed either too late or too early; or an error quality	Crew-coordination failure	Robust shift-hand-over procedures; training; team training across shift boundaries; robust data recording system
IDP2	Could the operator fail to follow the procedure entirely?	Action omitted or wrong action performed	Rule-violation; risk recognition failure; production-safety conflicts; safety-culture deficiency	Training in use of procedures; operator involvement in the development and verification of procedures

prompt the error. The method has a table format and ends with *error reduction guidelines*. A *code* is associated with each error identification question. The error identification prompt is based on a set of performance shaping factors. An excerpt of the HEIST method is shown in Table 1. The code, the error identification prompt, etc. are predefined by the method.

Since the *error identification questions* are based on performance factors, the factors that influence an operator's behaviour "pushing" him to err are considered (i.e. taken into account as contributing reasons for unsafe behaviour). Factors, like stress and task complexity in addition to task load (Hohlfeld et al., 2004) have a negative influence on operators' performance. Finding ways to decrease the influence of adverse PSFs can ultimately lead to increase in reliability of operator's performance. In Bellamy's et al. (2008) analysis of 8 chemical accidents, using a taxonomy of 850 factors, the factors selection and training, workload, competence, expertise, skills, peoples' capacity have contributed to undesired occurrences in more than 60% of the cases. The selected PSFs for our study were compiled from the set of factors given in HEIST—time, interface, training/experience, procedures, task organisation and task complexity, and the environmental stress and level of burden factors (Clemens, 2002).

The External error modes (Kirwan, 1994) classify the external and observable manifestation of the actual or potential error, based on logical outcomes of erroneous actions, in terms of timing, sequence, selection, quality, etc. Thus they provide information on the type of error committed, such as whether an action came too early, too late, or was omitted completely. The "system cause/psychological error mechanism" is an indication of the cognitive and/or co-ordination failure that lead to the erroneous action. Only in some instances the technical failure is included. The "psychological error" of operators' behaviour and the factors influencing his behaviour, i.e. performance shaping factors, explain the reasons that lead to the erroneous task implementation.

The error questions are applied to the basic events in the fault tree, which correspond to the critical tasks, to further determine the underlying causes of human error that initiated the incident/accident. The question points directly to the system cause/psychological error, which are then added as sub-events to the human basic events in the fault tree.

After the psychological error mechanism and the PSFs are determined, the error reduction guidelines from HEIST can be applied for recommending improvement actions. In the process, a set of error reduction guidelines is given for each system cause/psychological error determined trough using the error identification question.

Similar analysis procedures have been developed by Sheue-Ling et al. (2000), Hollywell (1996) and Kim and Jung (2002). The Humane Error Criticality Analysis (HECA) proposed by the first author consists of the construction of a human reliability analysis event tree, human error probability (HEP) estimation, and a HECA worksheet analysis. In Hollywell (1996) the framework for incorporating human dependency failures in risk assessment is based on more theoretical examples with a simplified task analysis structure and the PSFs are not explicitly specified. The human and hardware failures are represented by fault tree analysis and the task analysis tree is analogous to the FTA.

As within the HECA method (Sheue-Ling et al., 2000) we use FTA, and the psychological error mechanisms leading to the incident are shown. Compared to Hollywell (1996), our approach includes explicitly the relevant PSF; in addition, the task analysis is showing which task actually failed. In the work of Kim and Jung (2002), the assessment of the human error potential differs in the classification we used; also they have not used FTA.

5. Case study

In September 2005, two Hydro Power Plants (HPPs) located in the South-West and Central-West part of Bulgaria were visited by

Please cite this article in press as: Doytchev, D.E., Szwillus, G., Combining task analysis and fault tree analysis for accident and incident analysis: A case study from Bulgaria. Accid. Anal. Prev. (2008), doi:10.1016/j.aap.2008.07.014

one of the authors. Considering the problems in health and safety in the Bulgarian industry mentioned in Section 2, the purpose of the visit was to identify and analyse the type of human errors committed by the operators of both plants, the type of accidents/incidents that have occurred, and their influence on the plant safety operation. Also, we wanted to demonstrate the validity of our approach proposed for accident analysis.

We looked closer into an incident – a flooding of the plant basement in conjunction with a maintenance task – that had happened in a water turbine unit of the HPP. A water turbine unit in a HPP consists of a water inlet, nozzles, shutters, a rotor, a power generator, transmitters, a water outlet and other sub-units. The water outlet is situated in the bottom floor of a HPP.

Interviews with the shop floor operators and managers of the two HPP groups owned by the private company[5], as well as with the safety-engineer of the company, were conducted. Observation of the working environment was made. The authors got acquainted with the operational and safety procedures of the plants. The flooding incident mentioned above was analysed by applying the analysis approach proposed in Section 4. The basement is the place where the water outlet is situated and parts of the process are carried out. The reasons that lead to the flooding were that the water shutter was left closed, the scheduled maintenance activities of one of the turbines took too long, and the complete review of the scheme after maintenance completion was forgotten. Due to a human's error (duty registry N: 39 & 40 filled in incorrectly by power electrical technician instead of by shift operator), one of the components of the operational scheme was not reported in one of the duty diaries during the maintenance activities. This lead to information loss, about the water shutter state at the end of the maintenance period. Fault tree analysis was used to analyse the reasons for the flooding and task analysis was used to analyse the critical steps in the task implementation during the turbine maintenance operation preceding the flooding incident. The psychological error mechanisms were added to the fault tree analysis to account for the human-error contribution. The TOMBOLA task modelling programme (Uhr, 2003) was used to model the task analysis.

6. Results

From the interviews and the operational safety procedures of the plants, information about the activities and potential hazards for operators as well as reasons for committing human error was gathered. In Table 2 both the activities involved and potential hazards are summarized. Fig. 3 shows the fault tree analysis of the flooding incident. The figure shows that closing the water shutter, was not reported in the duty diary, as would have been required by company instructions. Also, the complete review of the operational scheme was skipped by the Duty Chief after the maintenance work was carried out. In addition, the maintenance activities took too long. These events lead to the situation "water shutter left closed". The left closed water shutter and the start of the turbine triggered the flooding. The "closed water shutter not reported. . .", and "OS scheme review by Duty chief. . ." were the human error causes that initiated the incident. In a traditional fault tree analysis the human error causes, would have corresponded to basic events in the diagram. Fig. 4 shows the task model of the turbine maintenance activities as created with TOMBOLA. In the model a check option is included, which requires the verification of the correct fill-up of the duty registry to ensure that nothing is forgotten to be reported.

A similar check is performed for the scheme restoration, and at the end of the turbine reparation. In reality, these two checks were omitted. The task model starts with the initiation of turbine maintenance by the plant operators for a given period. Next the reparation activity begins, starting with the assignment of the duty chief, the executors, etc.; the model continues with activities to make the place of reparation safe, including the closing of the water shutter. The model ends with inspection of the working place, the review of the process operational scheme, and finally with setting the water turbine back in operation. The marked tasks in Fig. 4 show the correspondence between the fault tree and task model. After performing the fault tree analysis and task analysis the task(s)

Table 2
Summary of task and potential hazards for operators.

Task	Hazards
• Starting-up and shutting-down of turbine and generator and connected process components	• Falling under electric. current/voltage load during task implementation and equipment inspection
• Carrying out operational switches and manipulation	• Strikes from solid flying objects from collapse of isolating material and valve pipes
• Eliminating failures and carrying out repairmen activities.	• Foot/step electricity
• Replacement of electric protectors	• Gas suffocation due to ignition of isolation
• Checking gas relays	• Reverse voltage load from transformers measuring voltage
• Working with voltage up to 1000 V	• Burn-out from electric arch
• Carrying out of duties[a]	• Black-out during equipment inspection • Bites from snakes, wasps, etc.

[a] Borrowed from the Military meaning of the word Duty and defined in "Regulation on safety at work in electrical systems at electrical power plants and thermal power plants and on the electricity network" (DOE, 2004 SG N: 72/19.08.2004).

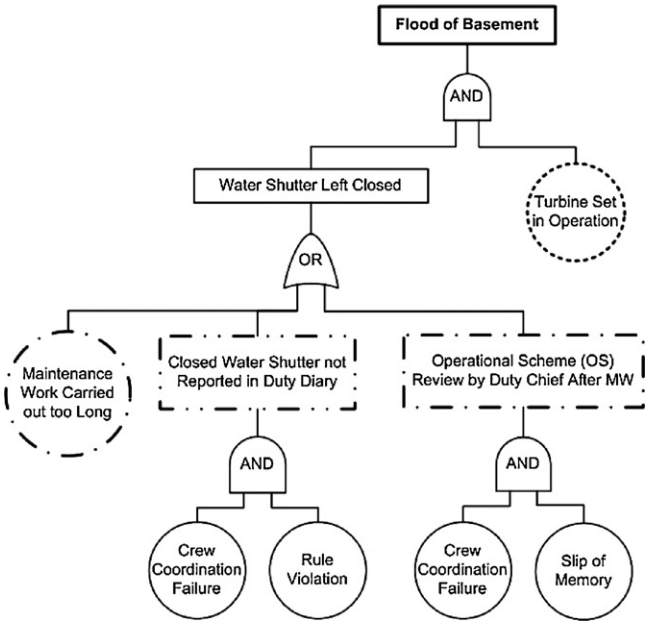

Fig. 3. Fault tree analysis of the water flooding incident.

[5] Because of confidential agreement with the company, neither the name of the company and HPPs nor the content of the procedures obtained is disclosed equipment is located.

Please cite this article in press as: Doytchev, D.E., Szwillus, G., Combining task analysis and fault tree analysis for accident and incident analysis: A case study from Bulgaria. Accid. Anal. Prev. (2008), doi:10.1016/j.aap.2008.07.014

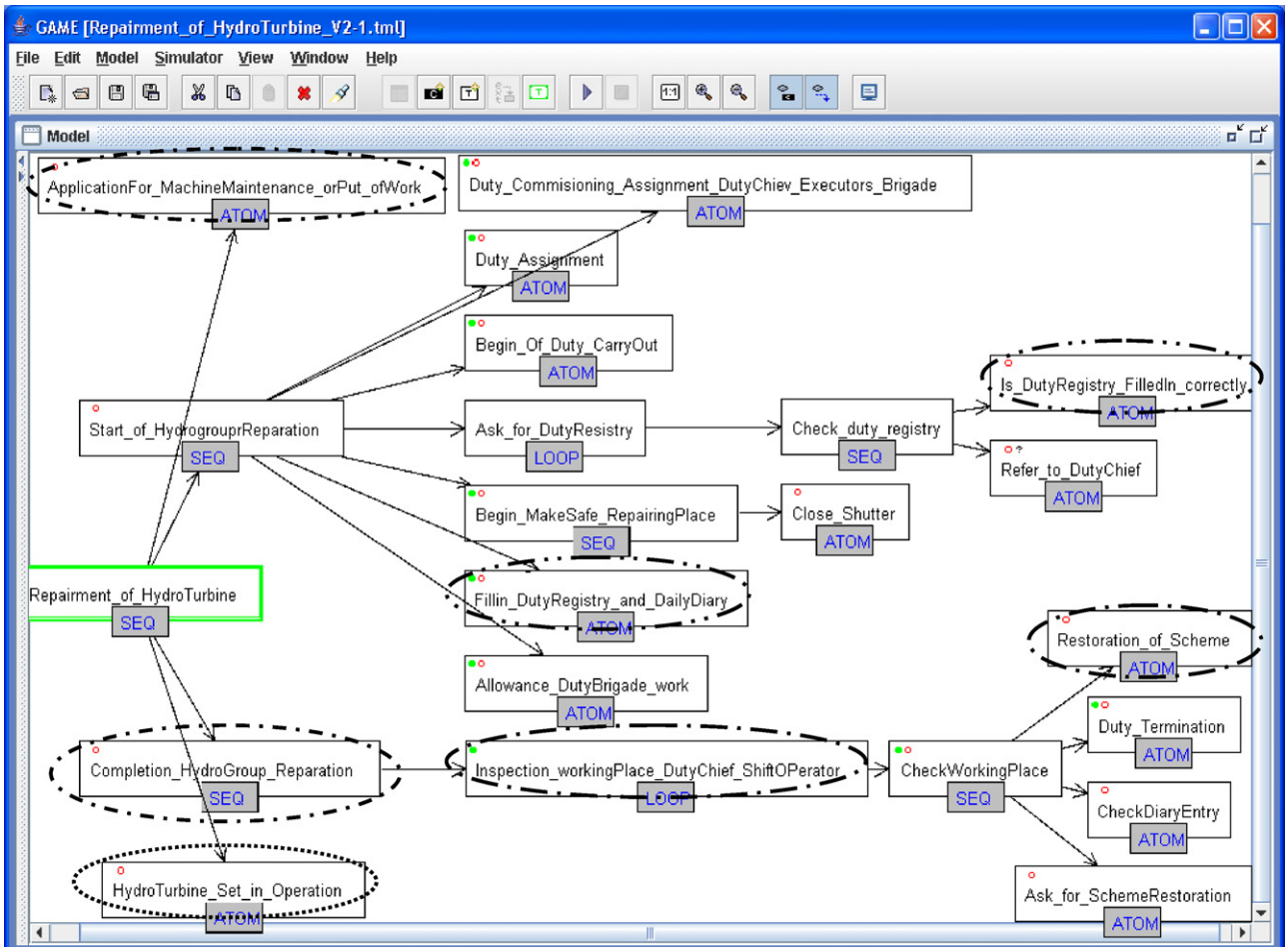

Fig. 4. Task analysis of the hydro turbine reparation activity.

carried out erroneously and ultimately leading to the undesired event, were determined. The events and activities in the two figures marked with dashed lines show the relation between the two diagrams. The critical tasks that lead to the flood are "Fill in duty registry and Daily diary" and "Inspection of working place by Duty chief or Shift operator"—Fig. 4.

As the example shows, the combination of fault tree analysis and task analysis permits to see the link between the fault event and the operators' tasks. This is important, because it shows the erroneous human actions that lead to the incident in the FTA.

To understand the reasons for human error, the human error basic events marked with dotted lines in the OR gate of the FTA (Fig. 3) were analysed by applying the HEIST method. This method enables the psychological causes for the faults to be seen.

In applying HEIST, we used the error prompt questions in the passive form to determine the exact psychological errors prompting the erroneous human behaviour. For example "Could it be that the operator forgot to transmit effectively across shift-handover boundaries?" This question corresponds to code IDO4 and "Crew coordination failure" system cause, as shown in Table 1. The external error modes and possible error reduction guidelines are also given in the table. In this way the system cause/psychological error-mechanism for the event "closed water shutter not reported in the duty diary" were determined as crew coordination failure and rule violation. In a similar manner the system causes/psychological error mechanisms for the incomplete operational scheme review were determined. The psychological error mechanisms for both human related events are given in Fig. 3. After adding the system causes/psychological error mechanisms to the "closed water shutter not reported. . .", and "OS scheme review by Duty chief. . ." events, the latest were transformed into intermediate events.

The external error modes that correspond to the system cause/psychological error mechanism are: wrong action, error of quality, action omitted, which fall into the global external error modes categories Error of omission, Error of Commission, Extraneous act. The complete list of error modes is given in Kirwan (1994).

In addition to the above mentioned incident, breaches of the safety regulations were also observed. Examples in this respect are:

- breaches of the regulation for starting of equipment working under high voltage;
- not wearing safety helmets;
- not wearing safety gloves or boots now and then.

The performance shaping factors influencing operators' behaviour were determined and classified according to their significance. They are presented in Table 3. The classification is based on the outcomes from the PSF related error identification prompts and the knowledge of the company's safety engineer about the production process. The most important PSFs are Training/Experience, Procedures and Task Complexity, because they are directly related to the flooding incident. Their significance coincides with Belamy's (2006) findings. On the other hand, the ergonomic related PSF have little importance. The training of the HPP operators is good and some of them have more than 10

Please cite this article in press as: Doytchev, D.E., Szwillus, G., Combining task analysis and fault tree analysis for accident and incident analysis: A case study from Bulgaria. Accid. Anal. Prev. (2008), doi:10.1016/j.aap.2008.07.014

Table 3
Type of performing shaping factors and their influence.

Type of PSF	Level of influence on operators
• Training/experience/competence	• Significant
• Procedures	• Significant
• Task complexity	• Significant
• Task organisation	• High
• Type of work load	• Moderate to high
• Stress	• Moderate to high (in Em.Sit)
• Noise and noise level	• Moderate to low
• Lightning	• Insignificant
• Shift duration	• Insignificant
• Ambient work climate (temp., moist., etc.)	• Insignificant

Em.Sit—Emergency situations.

years of experience. However, the tasks to be carried out at the plants are very complex sometimes and require the co-ordination of externally contracted companies, working e.g. on the electric wires between the stations of the group. These factors combined with the specific work load and the necessity to quickly repair a failed part now and then, influence utmost operators behaviour and increase the possibility to commit an error, which was the case in the investigated flooding. The factors time and interface have no influence on operator's performance and therefore are not included in the table.

The influence of human errors on plant safety operation, including human health, could be classified as less serious to grave depending on the outcome for each case.

7. Conclusions

A first application of the analysis approach for accident/incident analysis was successfully demonstrated. The approach consists of a combination of the fault tree analysis, a task analysis method and a human error analysis method, coupled with the factors influencing operators' performance.

As seen from the case study, task analysis permits to find out, which activities are candidates for being omitted during task implementation, and where checks could be added to safeguard against this task skip. Task analysis also permits to see where in the work process implementation the human error basic event, as used in fault tree analysis, occurred. By using HEIST, the types of human psychological errors could be systematically observed. HEIST is applicable to cases whenever there is an erroneous human action involved in incidents/accidents occurrence.

Last but not least, an insight of the type and reasons for incidents, including human errors in Bulgarian companies in the field of power generation was gained. Some of the observed errors resemble the general safety related errors and problems in Bulgarian industry, as mentioned in Section 2.

Acknowledgement

This paper would have not been possible without the financial aid of the EU Commission funding, ADVISES project, contract N: HPRN-CT-2002-00288, which help is highly acknowledged.

References

Bellamy, L.J., Geyer, T.A.W., Wilkinson, J., 2008. Development of a functional model which integrates human factors, safety management systems and wider organisational issues. Safety Science 46 (3), 461–492.
Blacket, C., 2005. Combining accident analysis techniques for organizational safety. Ph.D. Thesis. School of Computer Science and Informatics National University of Ireland.
Brauchler, R., Landau, K., 1998a. Task analysis. Part I – Guidelines for the practitioner. International Journal of Industrial Ergonomics 22 (1–2), 3–11.
Brauchler, R., Landau, K., 1998b. Task analysis. Part II – The scientific basis (knowledge base for the guide). International Journal of Industrial Ergonomics 22 (1–2), 13–35.
Callan, K., Siemieniuch, C., Sinclair, M., Rognin, L., Kirwan, B., Gordon, R., 2008. Review of Task Analysis Techniques for use with Human Error Assessment Techniques within the ATC Domain www.eurocontrol.int/eec/public/standard_page/safety_doc_task_analysis_and_atm.html, last accessed, March 2008.
Clemens, P.E., 2002. Human Factors and Operators Error, Second Edition. JE Sverdrup.
Cilingir, C., Mackhieh, A., 1998. Effects of performance shaping factors on human error. International Journal of Industrial Ergonomics 22, 285–292.
Contra Costa Health Service (CCHS), 2007. http://www.cchealth.org/groups/hazmat/pdf/iso/sect_b_ch_3.pdf, last accessed 2007.
Embrey, D., 2000. Task Analysis Techniques. Human Reliability Associates Ltd. www.humanreliability.com, last accessed 2006.
Executive Agency General Labour Inspectorate (EAGLI), 2004. Analysis of the results of the national campaign for setting of labour conditions in the chemical enterprises and units with high professional risk in compliance with the Health and Safety Conditions at Work Act (HSCW). To be found on http://git.mlsp.government.bg/.
Executive Agency General Labour Inspectorate (EAGLI), 2005a. Analysis of the results of the national survey for provision of health and safety conditions at work in the main risk enterprises of the metallurgical industry. To be found on http://git.mlsp.government.bg/.
Executive Agency General Labour Inspectorate (EAGLI), 2005b. Analysis of the results of the carried out national campaign "Control of implementations of obligations for provision of HSCW" in the enterprises for production of thermal and electric energy. To be found on http://git.mlsp.government.bg/.
Habbe, Ch., 2005. GAME: A graphical editor for task models (In German: GAME: Ein grafischer Editor für Aufgabenmodelle - Konzeption und Implementierung), University of Paderborn, Institute of Computer Science, Diploma Thesis, January 2005.
Hohlfeld, A., Fukuda, R., Neuper, S., Sangals, J., Sommer, W., Sträter, O., 2004. Task load effect on language processing: experimental approach. In: Dietrich, R., Childress, T.M. (Eds.), Group Interaction in High Risk Environments. Ashgate Publisher, pp. 207–240.
Hollnagel, E., 1998. Cognitive Reliability and Error Analysis. Elsevier.
Hollnagel, E., 1999. Accident analysis and barrier functions. IFE (N), Version 1.0. Available at: www.it.uu.se/research/project/train/papers/AccidentAnalysis.pdf.
Hollywell, P.D., 1996. Incorporating human dependent failures in risk assessments to improve estimates of actual risk. Safety Science 22 (1–3), 177–194.
Johnson, C., 2003. Failure in Safety Critical Systems: A Handbook of Incident and Accident Reporting Glasgow University Press.
Kim, J.W., Jung, W.D., 2003. A taxonomy of performance influencing factors for human reliability analysis of emergency tasks. Journal of Loss Prevention in the Process Industries 16 (6), 479–495.
Kim, J.W., Jung, W.D., 2002. An integrated framework to the predictive error analysis in emergency situation. Journal of Loss Prevention in the Process Industries 15 (2), 97–104.
Kirwan, B., 1994. A Guide to Practical Human Reliability Assessment. Taylor & Francis Press, Boca Raton.
Modarres, M., 1993. What Every Engineer Should Know About: Reliability and Risk Analysis. Marcel Dekker (publ.), New York, USA.
Non-profit Risk Management Centre (NRMC). Last access 2006. http://nonprofitrisk.org/ws/c2/acc-inc-nm.htm.
Paterno, F., Mori, G., Galiberti, R., 2001. CTTE: an environment for analysis and development of task models of cooperative applications. In: CHI '01 Extended Abstracts on Human Factors in Computing Systems, pp. 21–22.
Petersen, D., 1996. Human Error Reduction and Safety Management, 3rd edition. Van Nostrand Reinhold, New York.
Redmill, F., Chudleigh, M., Catmur, J., 1999. System Safety:HAZOP and Software HAZOP. John Wileys & Sons, Chichester.
SETON, 2006. www.seton.com/seton/internalHtmlAction.do?relpath=/pages/content/en_US/setonalerts/articles/0402/0402_accident_investigation.jsp. Last visited 2006.
Sheue-Ling, H., Fan-Jang, Y., Yu-Hao, H., Jinn-Sing, L., 2000. Application of human error criticality analysis for improving the initiator assembly process. International Journal of Industrial Ergonomics 26 (1), 87–99.
Shorrock, S.T., Kirwan, B., 2002. Development and application of a human error identification tool for air traffic control. Applied Ergonomics 33 (4), 319–336.
State Agency for Civil Protection (SACP), 2005. http://www.cp.government.bg/about.php?a=34. Last access 2005.
Stellman, J.M., 1998. Encyclopedia of Occupational Health and Safety, vol. 2., Fourth edition International Labour Organisation.
Uhr, H., 2003. TOMBOLA: simulation and user-specific presentation of executable task models, paper. In: Human-Computer Interaction: Theory and Practice (Part I), Proceedings of HCI International 2003, Crete, Greece, Lawrence Erlbaum Associates, pp. 263–267.

Please cite this article in press as: Doytchev, D.E., Szwillus, G., Combining task analysis and fault tree analysis for accident and incident analysis: A case study from Bulgaria. Accid. Anal. Prev. (2008), doi:10.1016/j.aap.2008.07.014