HUMAN ERROR PROBABILITY ASSESSMENT FOR FUNCTIONAL CONTROL GROUPS IN THE PROCESS INDUSTRY

Martin VISSER
Peter A. WIERINGA

Man-Machine Systems and Control. Faculty of Design, Engineering and Production, Delft University of Technology, Mekelweg 2, 2628 CD Delft, The Netherlands.
P.A.Wieringa@wbmt.tudelft.nl

ABSTRACT

This paper describes a methodology to use Human Error Probabilities (HEP) and design to create robust complex systems. If a Human Reliability Assessment (HRA) is performed, than this is done mostly after the detailed design phase is finished. The presented method helps to understand the influence of Human Error (HE) in an earlier design phase, e.g. at the functional analysis level.

The method consists of several steps. First alternative configurations of functional control groups with different complexities are developed. For each configuration, a fault tree is developed to find the initiating events (failures of equipment) which lead to a chosen top event. This top event is an undesired event such as an overflowing tank. The initiating events are used to create event trees (ET) with special emphasis on operator actions, such as monitoring the process and fault diagnosis. A diagnosis diagram simulates the fault diagnosis process to identify the initiating failures. The probability of a top event due to human error can then be found, by using HEP-factors and by normalising the failure probabilities of the equipment. The methodology is demonstrated by two examples of functional control groups with two different levels of complexity.

The results of the example configurations indicate that: The Basic Human Error Probability (BHEP) of a top event decreases with increasing task complexity (measure for task complexity: maximum number of consecutive alarm points in a configuration. In this paper, the configurations have maximal one to four alarm points). In a very simple system, too few recovery paths exist.

This does not imply that the more alarm points the lower the BHEP. The HEP for missing consecutive alarms above 10 are not available. It is plausible that an adverse effect of the number of alarms on the BHEP can be seen for large alarm sequences. This suggests that there exist a minimum BHEP for a certain number of alarm points.

KEYWORDS

Complexity, design, reliability.

INTRODUCTION

Human error is extremely commonplace, with almost everyone committing at least some errors every day.[1]-[2] Most errors are recoverable having none or relatively small impact on our lives. However, in complex systems this may not be the case. It is very important to design a system that is robust to human errors under all circumstances.

The increase in complexity of industrial processes makes the design of large industrial systems more difficult.[3]-[4] Another reason is the necessity for human centred automation. In addition, little is known about the details of the system during the first phases of the design process. Furthermore, the MMI[5]-[8] (Man-Machine Interface) will not be known in this phase. The designer has little or no information about the human actions and the associated HEPs (Human Error Probabilities), displayed in table 1. Thus a HRA (Human reliability assessment)[2] will be difficult to perform in this phase. Only global, time independent errors may be determined, e.g. wrong reading of data and not following the procedures.[2] Furthermore, the actions of all the human operators should be considered: the control room operators, supervisors, fieldworkers, etc.

Table 1 : Levels undertaken when designing a system.

Design phase	Level	
Concept	Goals	↑
↓	Functions	
	Tasks	
	Jobs	
	Means	
Detailed design	Actions	HEP

METHODOLOGY

Elementary modules, further called Functional Control Groups (FCGs), with their Human Error Probability (HEP) will be identified. Such a FCG covers a part of the process and performs one of the many functions, which are necessary to accomplish the overall goal of the system. Some examples of the FCGs are:

- Level control.
- Steam provision.
- Temperature control.
- Flow control.
- Position control.
- Pressure control.

Due to the absence of a detailed layout of the MMI and of the operator tasks in the early design stage, a minimum of alarms, controls and indicators for each FCG will be defined.

In this paper, we assume that the error probabilities of the human actions may be obtained using the THERP (Technique for Human Error Rate Prediction)-handbook of Swain & Guttmann[9]. Although some of the values are derived for nuclear systems and not for the process industry.

The following methodology has been developed to determine the HEP of a functional control group (figure 1):

(1) Functional control group analysis. —
(2) Generate alternative configurations.
(3) Perform Human reliability assessment: This means determining:
   (i) Tasks.
   (ii) Top event(s).
   (iii) Initiating events.
   (iv) Operator-action event tree.
   (v) Human operator diagnosis diagram.
(4) HEP for a FCG.

A CLOSER LOOK AT THE STEPS OF THE METHODOLOGY

In this paragraph, the steps of the methodology are briefly described using an example FCG.

(1) Functional control group analysis:

In this step, identification of FCGs (Functional Control Groups) will be done. Definition of the physical boundary of a FCG is an important issue here and includes the definition of input, output signals and disturbances.

(2) Generate alternative configurations:

For each FCG, different configurations with increasing complexity will be generated. Environmental, safety and reliability demands affect the choice for specific components. The complexity of the FCGs is affected by the use of different configurations and by the type of components used. For instance, the choice of a pump driven by a steam turbine instead of a motor-driven pump will affect the complexity. In this step the alarms, controls and indicators (MMI) will also be defined using a minimum of necessary elements.

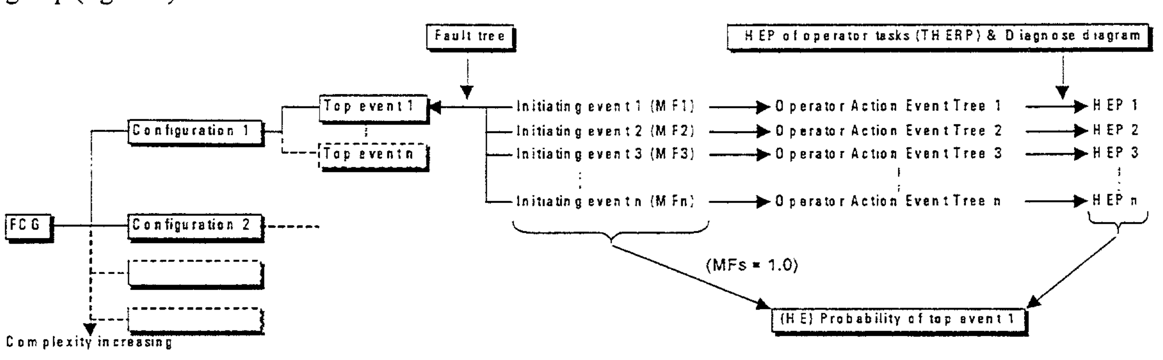

Figure. 1 : Approach to determine the HEP of the functional control groups.

The definition of complexity for the configurations is important. A good definition of system complexity doesn't really exist (Stassen[4]). Since we are concentrating on the control room operator actions, it is better to focus at the Task Demand Load (TDL)[10]-[12]. The TDL is inherent to a task and independent of the human. The MMI has a strong influence on the TDL.[13] The task complexity (during fault diagnosis) will be used as a measure for the complexity of a configuration and is based on the maximum number of consecutive alarms after an initiating event. The more consecutive alarm points, the more complex a system will be. Physical robustness of a system will reduce the interaction, and will induce fewer alarms.

Example configuration of LLC:

The P&I diagram of the low complexity LLC is presented in figure 2. It consists of a tank, a not controllable pump, a control valve and a level controller. The liquid could be water or another substance (not volatile). The following notation (ISO 3511) in the P&I diagrams is used for a measured property; F: Flow; L: Level; S: Speed; G: Position. For an instrument function the following notation is used; I: Indicating; C: Controlling; A: Alarming.

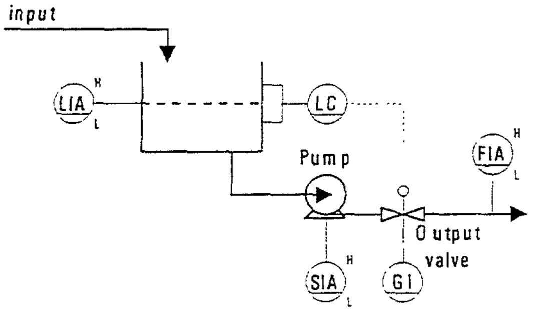

Figure 2 : LLC with low task complexity.

(3) Human reliability assessment[2]:

In summary, the following have to be determined:

(i) Tasks.

The definition of the operator tasks for each configuration will be done.

(ii) Top event(s).

The most important top events for the FCGs will be determined. These are the events with a high impact on safety or production.

The top event of the example FCG, LLC, could be an overflow of the tank.

(iii) Initiating events.

The identification of initiating events. Each FCG may have several initiating events leading to the same top event. For each top event, a fault tree is developed to determine the initiating events (top-down approach). These events can have their origin within a functional control group or outside a group. The latter initiating event can be considered as disturbances.

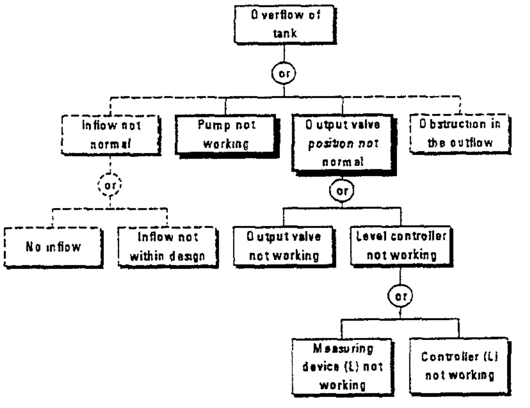

Figure 3 : System fault tree for low complexity LLC.

Example FCG, LLC:

Figure 3 displays the fault tree for the low complexity LLC. In figure 3, the initiating events caused by components outside a FCG are displayed with dashed lines. They will not be treated further here. The term device "X" "not working" in the figure refers to a mechanical failure (device "X" "defect") or to a human operator error.

(iv) Operator-action event tree (OAET)[2].

Derivation of event trees for the initiating events caused by a mechanical failure (MF) of the components of a FCG. The Operator Action Event Tree (OAET) describes the consecutive actions or lack of actions taken by the operator. Each operator action consists of detection followed by a fault diagnosis. This set of actions is referred to as phases. The event trees will be derived only with the information available for a FCG, because the contents of the process before or after a FCG are not known.

System dynamics determine the time between each alarm and thus the possibility of the operator reacting to one or more alarms at the time. The system dynamics are not known in this phase of design and are not taken into account. In addition, the event dynamics itself are not known, e.g. a defect pump may stop completely or may continue at a low rotation speed. Consequently, all the alarms and the reactions in the event tree are considered separately regardless their dynamics.

Example FCG, LLC:

Figure 4 displays the Operator Action Event Tree for the initiating event "pump defect" of the fault tree displayed in figure 3.
This OAET of the initiating event "pump defect" has three phases. After not detecting the first alarm or after an unsuccessful fault diagnosis in phase A, the operator may detect a second alarm in phase B. If the operator performs a successful fault diagnosis in phase B, full recovery of the situation occurs. If the operator does not detect the second alarm or performs the fault diagnosis unsuccessfully in phase B, than a recovery path in phase C exists. This pattern of phases is applied in all the event trees.

Note that the operator can make several time independent errors while performing the task "human operator detects an alarm low (or high)" (Detection Error Probability DEP1 to DEP3 in the event tree):

(1) Missing an alarm.

- Due to not attending.
- Due to assuming a false alarm.

(2) Selecting a wrong mimic and thus assuming it is a false alarm.

(3) Detecting wrong alarm high (low) instead of low (high).

The Fault detection error probabilities (FDEPs) are determined in the next step with a diagnose diagram.

(v) Human operator diagnosis diagram.

Diagnosis diagrams are developed to describe the fault diagnosis. After the human operator detects an alarm, several steps will be followed to diagnose the initiating event. These steps are part of an (assumed) procedure and are described in the diagnosis diagrams.

Although an operator, after detecting an alarm, would first start with checking the indicator associated with the detected alarm, we assume that the operator always starts at the top of the diagnosis diagram after detecting an alarm. The advantage of this approach is that in every phase and event tree the same diagnosis diagram can be applied to derive the HEP for the fault diagnosis. The disadvantage is that the BHEP may be too high because of the "summation" of the probabilities due to the "or functions" in the diagnosis diagrams.

Example FCG, LLC:

Figure 5 displays the diagnosis diagram for the LLC. The triangular tags labelled "A" in the diagnosis diagrams refer to figure 6.

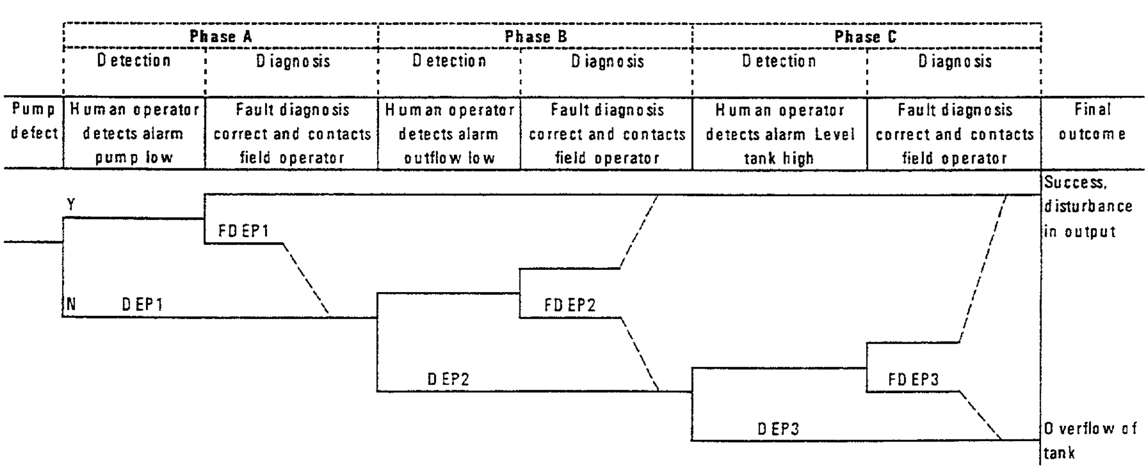

Figure 4 : Event tree for low complexity LLC starting with initiating event "pump defect".

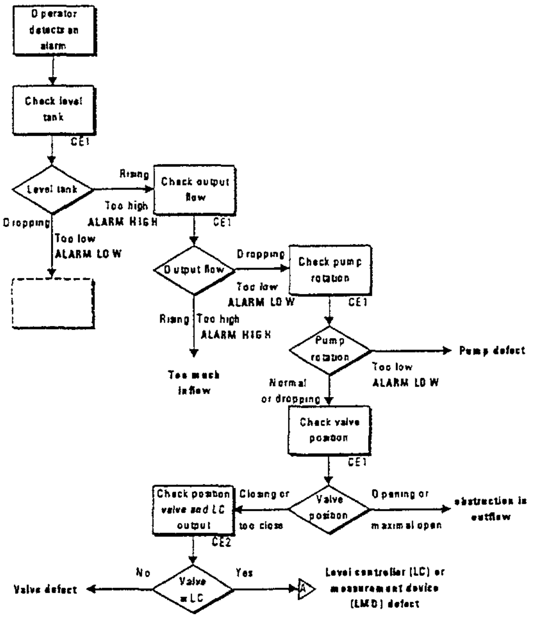

Figure 5 : Diagnosis diagram for the low complexity LLC.

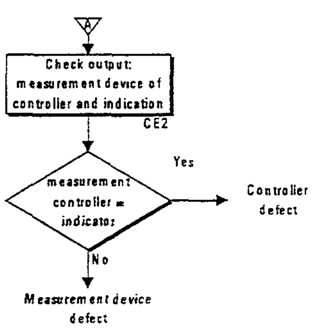

Figure 6 : Diagnosis diagram to decide between a defect controller or measurement device.

The status of a component checked by an operator is dependent on the time passed after the initiating event happened. Thus, the text at a decision point of the diagnosis diagrams refers to a trend or a threshold for a component or process state variable. This is demonstrated in an example for the initiating event "pump defect" for the low complexity configuration LLC:

Phase A: The human operator detects the alarm "pump low". The operator starts than with the fault diagnosis (figure 5 at the top). The success path through the diagnosis diagram to detect that the pump is defect:

(1) "Check level tank". The operator detects a not normal value and decides that the level is "rising" in the decision point.

(2) "Check output flow". The operator detects a not normal value and decides that the output flow is "dropping" in the decision point.

(3) "Check pump rotation". The operator detects a too low value and decides that the pump rotation is "too low, alarm low" in the decision point.

Phase B: The operator detects the alarm "output flow low". The operator starts again with the fault diagnosis (figure 5 at the top). Only point (2) is different in this phase: The operator "checks the output flow" and detects a too low value and decides that the output flow is "too low, alarm low" in the decision point.

Phase C: The operator detects the alarm "level tank high". The operator detects now a too high value (alarm high) for the "level in the tank" for point (1).

Note that the Check Errors CE1 to CE3 in the diagnosis diagrams are the probabilities of a human operator making an error while checking an indicator. These probabilities consist of more than one human error. The human errors for an operator performing the task "check the status of an indicator" (CE1) are:

- Selecting wrong mimic.
- Check reading error.

The human errors for an operator performing the task "check the status of indicator 1 and 2" (CE2) are:

- First indicator: selecting wrong mimic.
- First indicator: check reading error.
- Second indicator: selecting wrong mimic.
- Second indicator: check reading error.

(v) <u>HEP for a top event of a configuration</u>:

Calculation of the HEP for a top event by inserting the HEPs into the event and fault trees. A Mechanical Failure rate of one is assumed for all the initiating mechanical failures in this step.

The Basic Human Error Probabilities (BHEPs) for the event and diagnose diagrams will be determined. We assume that the required time for the operators to perform fault diagnosis is 30 minutes. This is what is often used for a Nuclear Power Plant (NPP). In the process industry there is not such time defined. The situation where the operator has 30 minutes to perform a fault diagnosis simulates a normal condition. The minimum time within which we assume a human operator has to perform a fault diagnosis is set to 5 minutes and represents a situation under stress. The BHEP will be determined for both conditions. The handbook of Swain & Guttmann[9] is used to obtain the BHEPs.

DISCUSSION

In this paper, we focussed on two different levels of complexity for a FCG. The complexity was defined using the maximum number of consecutive alarm points after an initiating event. Note that, using this definition, an increase in the number of components does not always imply an increase in the task complexity.

The function of a FGC determines the choice of the top vent. In this paper, the LLC performs a buffering function; thus, the top event is "overflow of tank". For instance, the top event would be different for a LLC that provides cooling water: "no outflow".

The initiating events can have a human or system origin. The human initiating events, e.g. an error of commission, require a more detailed knowledge of the whole process and the working conditions, which are not known at the preliminary stage of design. Thus, in this survey only mechanical failures are considered. In addition, the initiating events, like a ruptured or blocked pipe (a defect non-return valve) are not treated in this paper.

The event trees are much more extensive than normally in a HRA, because every alarm that the operator does not detect has a possible recovery path. Such recover paths are realistic compared to the actions performed by an operator in the control room. For instance, it is possible that an operator realises due to a second alarm, that the first fault diagnosis was incorrect. This is only realistic for a small number of alarms; a twentieth consecutive alarm provides very little information to the operator. Note that the probability of recovery (by detecting a consecutive alarm) becomes less according to THERP table 20-23.

Diagnosis diagrams are flowchart procedures and are used to determine the probability for not achieving the top goal in a FCG. The operator has several options at various points in the procedure (here, all two options). Furthermore, the procedures are symptom-based which enables the operator to act in a developing event according to what symptoms are present.[2]

We assumed that the operator always starts at the top of the diagnosis diagram after detecting an alarm. Another approach is to start at the "check box" in the diagnosis diagram associated with the detected alarm. This does not make a difference, because the order of the boxes in the diagnosis diagrams is interchangeable (or-functions).

A refinement can be done in the diagnosis diagrams:

(1) Starting at the top of the diagram for an alarm point on a "process variable" (indirect alarm).

(2) Starting at the check box associated with the detected alarm for an alarm point on a "component" (direct alarm).

The operator only checks the indicator associated with an alarm point on a "component" (direct alarm), thus starting at the top of the diagnosis diagram is than not realistic. For example, the pump in the low complexity LLC (figure 2) has a direct alarm point. If the operator detects the pump alarm, the operator checks the rotation indicator of the pump and concludes, that the pump is defect without checking the indicator of the outflow and the level in the tank. The operator must check other indicators, in case of an alarm point on a "process variable" (indirect alarm: e.g. alarm outflow, figure 2), to perform a successful fault diagnosis, because there are more components that can cause this disturbance.

It is possible that the operator selects a wrong procedure (diagnose diagram) while performing a fault diagnosis. This is not taken into account, because there is a high probability of recovery. There is also the probability that the operator performs an error: namely skipping a procedure step (diagnose diagram step). This is a very small error (BHEP=0.001) according to THERP[9] table T20-7 item (1) and will not be taken in account in this paper. In addition, it is assumed that the HE of not contacting the field operator is zero. Following emergency operating procedures are considered in more detail by Macwan et al.[15]

THERP suggests a much higher BHEP for a human operator performing fault diagnosis under stress (5 minutes) than was obtained using the diagnosis diagrams (table 2). This can be explained as follows. First, the modifying factor of five, that we assumed to obtain a situation with stress with, could be too small. Secondly and more likely, the diagnosis diagrams are dependent on the complexity of the system. The configurations in this paper are small (unlike THERP) and thus one can expect a smaller BHEP for fault diagnosis under stress. For instance, in case of the normal condition (30 minutes), the operator has enough time to perform a successful fault diagnosis for a small as well as for a more complex system. Thus, the BHEP will be the same for both systems. This is not the case for the condition under stress (5 minutes). The probability for the operator to make an error will be higher for the higher complexity system than with a small system (with only 5 minutes to perform a fault diagnosis).

Table 2 : BHEP of diagnosis of a single event.

Available time for diagnosis of single event	BHEP obtained with	
	THERP table 20-1	Diagnose diagram
5 minutes	0.75	0.08 to 0.26
30 minutes	0.01	0.015 to 0.06

The BHEP obtained from THERP should be corrected for low task complexity systems by applying a PSF. Thus, the diagnose diagrams are a good approach to determine the BHEP of fault diagnosis.It is impossible to assess the effect of all the PSFs due to the absence of knowledge about the MMI, situation and human factors. However, if this method is applied during design of a chemical process some of the PSFs can be determined:

(1) The factor "training" (The Internal PSF's) is omitted, because we assume that the operator is skilled and well trained.

(2) The influence of the factor "stress" (The Stressor PSF's) on the control room operator is taken into account by assuming a higher stress level for the condition that there are only 5 minutes available to perform a fault diagnosis.

(3) The influence of "task load" (The Stressor PSF's) is already taken into account in this methodology by using the diagnose diagrams.

Table 1 depicts the various levels undertaken during design of a system. However, on which level can the derived methodology be implemented? On the function level, the implementation is expected to be possible by creating standardised FCGs. These FCGs can be implemented into computer design programmes as modules. The designer can than select equipment with the desired mechanical failure (MF) rate based on the BHEP associated with that equipment as initiating event.

A question arises if the implementation of this methodology is possible on the goal level. The goals can be too global. For a large plant such as a nuclear power plant this will be the case for all the goal levels, top goal, goal and sub-goal level.[14] Decomposition into sub-goals reveals the critical functions. For instance, a sub-goal like: "control level under various normal conditions" consists of many critical functions, like control nuclear power, neutron flux distribution, turbine generator system, etc. Such critical function groups are essentially the same as the FCGs addressed in this paper. Thus, the implementing of this methodology is only possible on the level of functions.

The only remaining problem on the functional level is the unknown mechanical failure rate of the equipment that determines the probability of a top event. If the equipment is selected, than the associated mechanical failure rates are known. Before this step, it is only possible to work with estimated or average mechanical failure rates.

VERIFICATION

It was found that the BHEP decreases with increasing task complexity. This result is shown in table 3 where the BHEPs of the top events are depicted against the maximum number of consecutive alarm points in a configuration. The table depicts the normal condition (second column: 30 minutes to perform fault diagnosis) and the condition under stress (first column: 5 minutes to perform fault diagnosis).

Table 3: The BHEP for the top events

FCG	5 minutes	30 minutes
Low Complexity HTC (one alarm point)	0.3779	0.0889
High Complexity HTC (two alarm points)	0.1630	0.0081
Low Complexity LLC (three alarm points)	0.1124	0.0055
High Complexity LLC (four alarm points)	0.0440	0.0004

As previous stated we assume the maximum number of consecutive alarm points as a measure for the task complexity. Thus, the BHEP decreases with an increasing task complexity. In the higher complexity FCGs, the operator has more recovery opportunities due to more available information.

Table 3 shows that the BHEPs of a top event for the condition under stress (5 minutes) decreases from a very high (unacceptable) BHEP to a more acceptable one. The BHEP of the normal situation (30 minutes) decreases from an acceptable BHEP to a very small BHEP. This can be explained as follows: The configurations with few alarms provide too little information for the operator in case of the condition under stress. Therefore, the operator has not much possibility to recover from an incorrect fault diagnosis.

This conclusion and table 3 do not imply that the more alarm points the lower the BHEP. The HEP for missing consecutive alarms above 10 are not available. It is plausible that an adverse effect of the number of alarms on the BHEP can be seen for large alarm sequences. This suggests that there exist a minimum BHEP for a certain number of alarm points.

Table 4. The pros and cons of the presented method.

Pro	Con
▪ Information about HE available in an early design stage.	▪ Based upon ideal situation with ideal Man-Machine interaction design.
▪ The designer can balance the choice of a configuration of a FCG with the desired HEP for a top event.	▪ Implementing Basic HEP into event trees, because the influence of the PSF's is unknown. Therefore, the overall HEP of a top event of a FCG is also normative.
▪ The possibility of inserting the FCGs into computer designing programmes for chemical processes. The selection of the BHEP can be done than maybe based on the system dynamics. Slow dynamics: normal condition and fast dynamics: situation under stress.	▪ The method disregards the effects of the events outside the FCG that follow on an initiating event in a FCG. The contents of the process before or after a FCG are not known.
▪ No invention of the wheel again. All the known information about a FCG can be implemented in a standardised FCG and is thus available for any designer.	▪ All the possible functional control groups and their different complex configurations have to be identified.
▪ Simple method based upon the information available for a functional system. The method can be applied to any part of a process by using a modular set-up.	▪ Dependencies between human action are not considered in this survey. This is more interesting in case of more operators.
▪ The BHEP of fault diagnosis is determined with a more realistic approach. THERP applies the same BHEP for fault diagnosis in all situations, which is only dependent on the time between the events. In the approach presented here the BHEP are dependent on the time between events and on the type of system by applying diagnose diagrams.	▪ Special situations are not considered. For example during start-up, there may occur many false alarms; thus, the probability of missing a real alarm increases. ▪ The effect of the size of a plant is not taken into account.

CONCLUSIONS

A methodology has been presented to incorporate BHEP associated with operator errors and functional analysis. The approach consists of determining the initiating events for a top event of a functional group using a fault tree and then deriving the Operator Action Event Tree (OAET) for these events. The fault diagnosis in the OAET is done with the aid of a diagnosis diagram. With all the mechanical failure rates equal to one, the overall BHEP for the top event can be derived (using the outcome of the event trees).

One has to bear in mind that the probabilities can be used only as an aid for choosing equipment layout and applying redundancy. The complete process is not taken into account, because the MMI and the dynamics of the process are not known in the preliminary design phases.

The results of the example configurations indicate that: The BHEP of a top event decreases with increasing task complexity (measure for task complexity: maximum number of consecutive alarm points in a configuration). In a very simple system, too few recovery paths exist.

The pros and cons of the methodology are depicted in table 4. Further work needs to be carried out to derive the best procedure of implementing the method into the design process.

REFERENCES

[1] B. Kirwan, L. K. Ainsworth, « Guide to task analysis », Taylor and Francis, London, ISBN 0-7484-0058-3, 1992.

[2] B. Kirwan, « A guide to practical human reliability assessment », Taylor and Francis, London, ISBN 0-7484-0052-4 (cloth), 0-7484-0052-3 (paper), 1994.

[3] G. Johannsen, A.H. Levis, H.G. Stassen, « Theoretical problems in man-machine systems and their experimental validation », *Automatica 30(2)*, pp 217 – 231, 1994.

[4] H.G. Stassen, « Hoe complex is een industrieel proces voor een procesoperator », Inspelen op complexiteit, Alkemade M.J.A. Samson bedrijfsinformatie b.v., Alphen aan den Rijn / Zaventem. ISBN 90-14-03883-6, pp 184-195, 1992.

[5] J.P. Scanlon, « Guidelines for the design of Man-Machine Interfaces: Level 0 », tc-6 (Man-machine communications) of EWICS, Sintef, division of automatic control, N-7043 Trondheim, NTH Norway, 1981.

[6] J.P. Scanlon, « Guidelines for the design of Man-Machine Interfaces: Level 1 », tc-6 (Man-machine communications) of EWICS, Sintef, division of automatic control, N-7043 Trondheim, NTH Norway, 1981.

[7] J. Wirstad, « Guidelines for the design of Man-Machine Interfaces: Level 2 », tc-6 (Man-machine communications) of EWICS, Sintef, division of automatic control, N-7043 Trondheim, NTH Norway, 1982.

[8] E. van Ravenzwaaij, H. G. Stassen, « Guidelines for the design of Man-Machine Interfaces: Level 3 », tc-6 (Man-machine communications) of EWICS, Sintef, division of automatic control, N-7043 Trondheim, NTH Norway, 1986.

[9] A.D. Swain, H.E. Guttmann, « Handbook of Human Reliability Analysis with emphasis on nuclear power applications », NUREG/CR-1278, 1983.

[10] H.G. Stassen, G. Johannsen, N. Moray, « Internal representation, internal model, human performance model and mental workload », Automatica *26*, pp 811 – 820, 1990.

[11] S. Bi, G. Salvendy, « Analytical modelling and experimental study of human workload in scheduling of advanced manufacturing systems », The international journal of human factors in manufacturing, vol. 4, pp. 205 – 234, 1994.

[12] Zhi Gang Wei, Anil P. Macwan, P.A. Wieringa, « Quantitative degree of automation », Man-Machine Systems and Control, Fac. WbMt, Tu Delft, p 26, 1996.

[13] J.H.M. Andriessen, P.A. Wieringa, « Influencing complexity by means of the man-machine interface », Fac. WbMt, Vakgroep M&R, TU Delft, p 15, 1995.

[14] « Design for control rooms of nuclear power plants », Nen 10964 1e druk, november 1989. Nederlandse Elektrotechnisch Comité (NEC), Normcommissie NEC 45 "Kerntechnische instrumentatie", Dutch institution of Normalisation, Kalfjeslaan 2, Postbox 5059, 2600 Delft.

[15] A.P. Macwan, P.A. Wieringa, A. Mosleh, « Quantification of multiple error expressions in following emergency operating procedures in nuclear power plant control room », Preprints of the PSAM-11, Apostoakis, G.E. and WU, J.S. San Diego: 2 (1) 066-15 066-20, 1994.