PREHEP: Human Error Probability Based Process Unit Selection

Martin Visser and Peter A. Wieringa, *Member, IEEE*

***Abstract*—This paper describes a methodology to use human error probabilities (HEPs) as a basis for selecting functional process units in the design phase. The method helps to understand the influence of human error (HE) on functional robustness of the units in earlier design phases, e.g., at the functional analysis level. This methodology can be used to detect the need for human operator support.**

The method consists of several steps. First alternative configurations of functional process units 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 is used to simulate the fault diagnosis process and to identify the initiating failures. The probability of a top event due to human error can then be found, by using existing HEP-data and by normalizing the failure probabilities of the equipment. The methodology is demonstrated for two examples of functional process units each with two levels of complexity.

***Index Terms*—Alarm management, engineering design process, fault tree, human reliability, operator support.**

I. Introduction

A. Introduction

HUMAN error (HE) is extremely commonplace, with almost everyone committing at least some errors every day [1], [2]. Most errors are recoverable having no 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]. In addition, little is known about the details of the system during the first phases of the design process; e.g., the human–machine interface (HUMIF) [5]–[8] will not be known in this phase and little information will be available about the human operational actions, e.g., reading of data and execution of the procedures. Guidelines to design procedures with the human execution error in mind have been generated [9]. Nevertheless, a human reliability study [2] can only be performed at the detailed design phase and not at the global design phase. We will present a method to predict human error probabilities (HEPs) (PREHEP) in earlier design phases based on assumptions about the actions during alarm handling of process units.

Manuscript received June 25, 1999; revised November 7, 2000. This work was supported by Everest, a subsidiary of the Dutch company, Pink Roccade nv. This paper was recommended by Associate Editor R. Rada.

The authors are with the Man-Machine Systems, Faculty of Design, Engineering, and Production, Delft University of Technology, Delft, 2628 CD, The Netherlands (e-mail: p.a.wieringa@wbmt.tudelft.nl).

Publisher Item Identifier S 1094-6977(01)03526-X.

B. Methodology

Elementary modules, further called functional process units (FPUs), with their HEP will be identified. An FPU covers a part of the process and performs one of many functions, which are necessary to accomplish the overall goal of the system. Some examples of the FPUs are fluid storage unit, steam supply unit, heat supply unit, cooling unit, and pressure unit.

In this paper, only mechanical failures MFs of components in an FPU are considered. We assume that the error probabilities of the human actions may be obtained using the technique for human error rate prediction (THERP)-handbook of Swain and Guttmann [10]. Although some of the values are derived for nuclear systems and not for the process industry. the following steps of the methodology have been defined (Fig. 1):

1) functional process unit analysis;
2) generate alternative configurations;
3) perform human reliability assessment, i.e., determine
   a) tasks;
   b) top event(s);
   c) initiating events;
   d) operator-action event tree;
   e) human operator diagnosis diagram.
4) HEP for an FPU.

C. Closer Look at PREHEP

The steps of the methodology are briefly described in the following paragraphs.

1) Functional Process Unit Analysis: In this step, FPUs will be identified. These units perform a lower level function such as controlling the temperature. Definition of the physical boundary of a FPU is an important issue here and includes the definition of input, output signals, and disturbances.

2) Generate Alternative Configurations: For each FPU, different configurations with increasing complexity will be generated. Environmental, safety, and reliability demands affect the choice for specific components. The complexity of the FPUs 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. We assumed that for all configurations a minimal number of alarms points, controls, and indicators (HUMIF) will be designed.

The definition of complexity for the configurations is important. A good definition of system complexity doesn't really exist

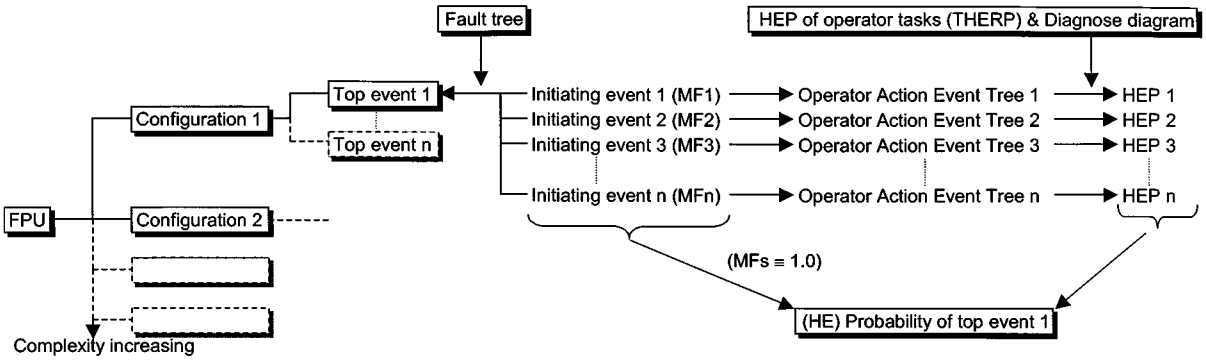

Fig. 1. PREHEP: approach to determine the human error probabilities (HEPs) for a functional process unit (FPU).

[4]. Since we are concentrating on the control room operator actions, it is better to focus on the task complexity which is associated with the task demand load (TDL) [11]–[13]. The TDL is inherent to the task associated with the procedure and is independent on the human performance. The HUMIF has a strong influence on the TDL [13] and is part of the operator's internal representation [14].

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 that may be triggered after an initiating event occurs. Consider the case of two pumps where one pump is enough to fulfill the goal. When a pump stops, another pump may take over, causing maybe only one alarm. In case, only one pump is designed, more alarms due to the absence of a flow may be generated, e.g., a high alarm on a level indicator before the pump. Thus, the TDL is higher and the system is more complex according to our definition.The more consecutive alarm points, the more complex a system will be.

3) Human Reliability Assessment [2]: In summary, the following has to be determined.

a) *Tasks*: The definition of the operator tasks for each configuration will be identified.
b) *Top event(s)*: The determination of the most important top events for the FPUs. These are the events with a high impact on safety or production.
c) *Initiating events*: The identification of initiating events. Each FPU 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 an FPU or outside a unit. The latter category can be considered as disturbances.
d) *Operator-action event tree (OAET)* [2]: Derivation of operator action event trees for the initiating events caused by a mechanical failure (MF) of one of the components of a FPU. System dynamics determine the time between each alarm and thus the possibility of the operator to react to one or more alarms at the time. The system dynamics are not known in the design phase and are not taken into account. In addition, the event dynamics itself are not known, e.g., a defected 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 of their dynamics. The OAETs will be derived only with the information available for a FPU, because the contents of the process before or after a FPU are not known.
e) *Human operator diagnosis diagram*: Development of diagnosis diagrams to describe the fault diagnosis. The diagnosis diagrams are used to find the initiating event that caused the event.

4) HEP for a Top Event of a Configuration: Calculation of the HEP for a top event by inserting the HEPs (obtained with THERP) into the event and fault trees. A mechanical failure probability of one is assumed for all the initiating mechanical failures in this step.

II. Functional Process Units

A. Step 1: Functional Unit Analysis

In this step, two FPUs (a fluid storage unit and a heat exchange unit) will be identified. The selected fluid storage unit consists of a tank, a pump, and a control valve after the tank. This FPU is further referred to as a fluid storage unit (FSU). The process before the FSU determines the inflow, which can be considered as a disturbance. The heat exchange unit uses a steam heat exchanger to warm up the process fluid (PF). The steam flow is controllable. This FPU is further referred to as HEU: heat exchange unit. The flow rate and temperature of the PF act as a disturbance.

B. Step 2: Generate Alternative Configurations

For two different task complexity levels, distinct configurations will be determined. The difference in complexity of the fluid storage unit is caused by the selection of alternative parts due to the volume and the more hazardous liquid that has to be pumped in case the more complex configuration is considered. The difference between the configurations for the heat exchange unit is smaller. There are only two different solutions for almost the same number of components.

The following notation (ISO 3511 [15]) in the piping and instrumentation (P&I) diagrams is used for a measured property. F: flow; L: level; P: pressure; S: speed; T: temperature; G: position. For an instrument function the following notation is used. I: indicating; C: controlling; A: alarming.

1) FSU: The P&I diagrams are presented for two different task complexity levels of the FSU.

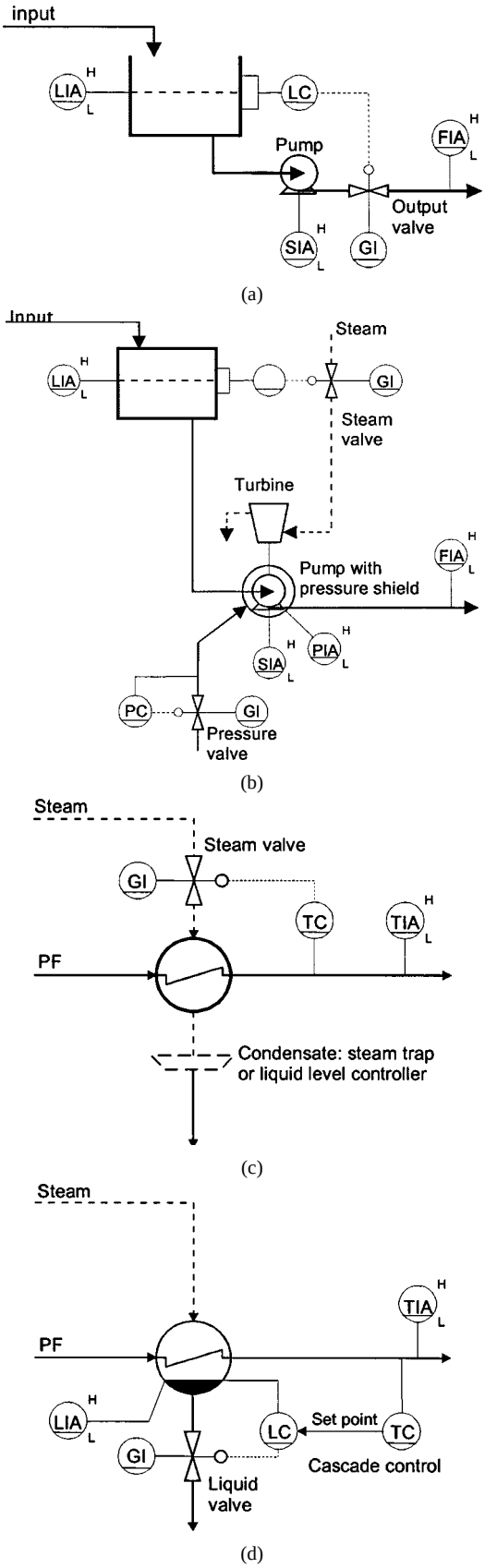

Fig. 2. Fluid storage units (FSUs) and heat exchange units (HEUs) in a low and high complexity configuration.

a) Task complexity low: The P&I diagram [Fig. 2(a)] presents the FSU for the low task complexity. 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).

b) Task complexity high: Here again the level control consists of a tank and a pump [Fig. 2(b)]. In this case, we assume that the system is filled with a hazardous liquid. In addition, we assume a larger flow. This requires a variable speed driven pump instead of a discharge throttling of the pump [16]. Generally, a pump with a steam turbine will be used. The control valve in this case is used to control the steam flow to the turbine. Furthermore, a pressure-shield around the pump has been added to prevent the escape of the process fluid. Because of the possibility of more consecutive alarms, the task complexity is slightly higher.

2) HEU: The P&I diagrams are presented for two different task complexity levels of the HEU.

a) Task complexity low: The P&I diagram for the HEU with low task complexity is depicted in Fig. 2(c). The rise in temperature of the process fluid is accomplished with a steam heat exchanger. The temperature is feedback controlled using the steam valve in the steam supply. After the heat exchanger, a steam trap to condense the steam (this could also be a liquid level controller) can be added into the design.

b) Task complexity high: This configuration differs slightly from the low complexity HEU [Fig. 2(d)]. The condensation will be done in the heat exchanger. The temperature control is done by cascade control where the temperature control affects the (water) level controller. A fluid valve is used in the outflow of the exchanger to control the level in the heat exchanger. Because of the possibility of more consecutive alarms, the complexity is slightly higher than the previous example.

III. Step 3: Perform Human Reliability Assessment

A. Step 3i: Task Analysis

The hierarchical task analysis (HTA) [2] for an FPU consists of 1) start up (bring plant to operational state), 2) maintain normal operation, and 3) shut down (bring plant to nonoperational state). The task "*maintain normal operation*" implicates the maintaining of the level of the tank for the FSU and maintaining the temperature for the HEU. Due to the limited nature of this paper, only the task "*maintain normal operation*" will be considered. This task is split into two subtasks: "*monitor system*" and "*fault detection and diagnosis*." We assume that the operator executes these tasks by following procedures. Hence, the task performance is rule-based instead of knowledge-based [17].

1) Monitoring Tasks: The monitoring tasks for the low and high complexity configurations are summarized in Table I.

The HEU has a common task for both configurations [Fig. 2(c) and (d)]: "*detection of a reduced capacity of the heat exchanger*." This will be done by "*monitoring the position of the valve*," because the position of the valve gives the human operator, indirectly, information about the state of the heat exchanger. If the capacity of the heat exchanger is reduced, the position of the valve is controlled toward its maximum. This holds for the low as well the high complexity configuration. In

TABLE I
MONITORING TASKS FOR FSU AND HEA

FSU	HEU
Low task complexity Figure 2A	*Low task complexity Figure 2A*
• Level in tank (LI). • Flow out (FI). • Position of output valve (GI). • Speed of pump (SI).	• Temperature (TI). • Position of steam valve (GI).
High task complexity Figure 2B	*High task complexity Figure 2B*
• Level in tank (LI). • Flow out (FI). • Position of steam valve (GI). • Speed of pump (SI). • Position of pressure valve (GI). • Pressure shield (PI).	• Temperature (TI). • Position of liquid valve (GI). • Level in heat exchanger (LI).

TABLE II
FAULT DETECTING TASKS FOR FSU AND HEA

FSU	HEU
Low task complexity Figure 2A	*Low task complexity Figure 2C*
• Alarm level in tank (LA). • Alarm speed pump (SA). • Alarm flow out (FA).	• Alarm temperature (TA).
High task complexity Figure 2B	*High task complexity Figure 2D*
• Alarm level in tank (LA). • Alarm speed pump (SA). • Alarm flow out (FA). • Pressure shield (PA).	• Alarm temperature (TA). • Alarm level in heat exchanger (LA).

addition, for the high task complexity configuration, the task "*monitor the level in the heat exchanger*" in the heat exchanger gives an extra indirect indication about the capacity of the exchanger. Thus, the task "*detecting a reduced capacity*" may be easier for that configuration.

2) Fault Detection and Fault Diagnosis Tasks: The fault (alarm) detecting tasks for the low and high complexity configurations are summarized in Table II. The fault diagnosis tasks will be treated in Sections III-D and III-E.

B. Step 3ii: Identification of Top Event(s)

Identification of top events can be done using several criteria with respect to safety, quality, or reliability. For the FSU several top events can be identified, such as

1) an overflow of the tank;
2) pump dry;
3) empty tank (resulting in pump dry);
4) no outflow.

Note that if the level in the tank is not normal, all these four top events may occur. In this paper, only the top event of an "*overflow of the tank*" will be considered.

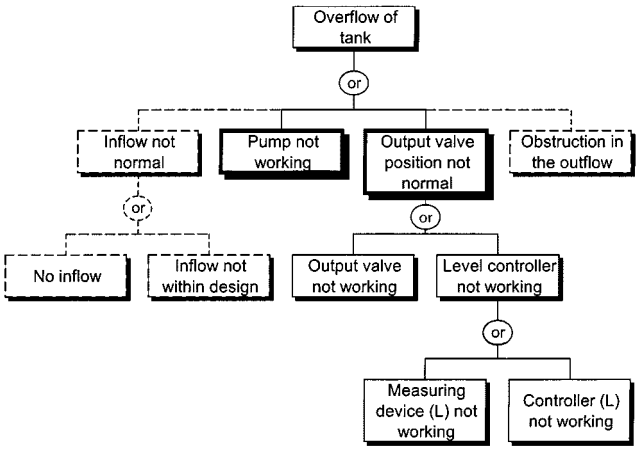

Fig. 3. System fault tree for low complexity FSU.

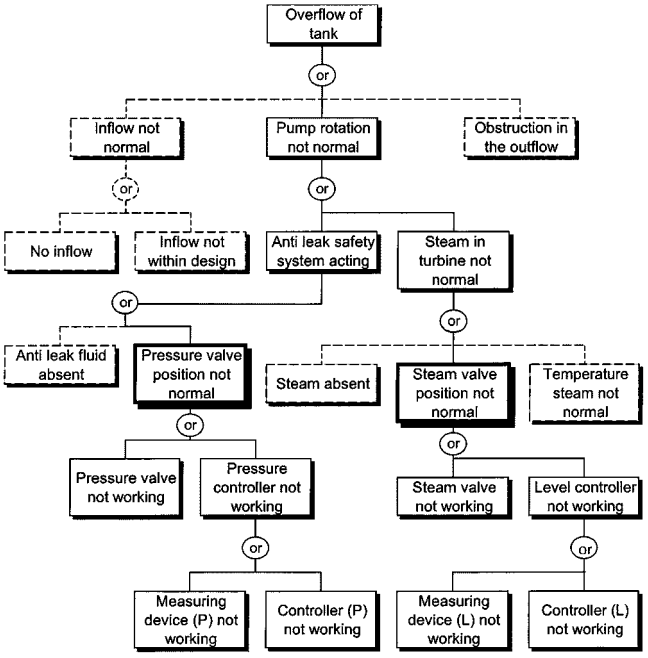

Fig. 4. System fault tree for high complexity FSU.

The selected top event for the HEU is "*a nonnormal output temperature*."

C. Step 3iii: Identification of Initiating Events

Initiating events caused by mechanical failure of the components are derived for each top event using a fault tree. Initiating events due to so-called latent HEs, e.g., maintenance errors, are not considered. Other component failures, such as "*fluid pipe rupture*," will not be considered in this paper. Such initiating events can be added when necessary.

Fig. 3 displays the fault tree for the low complexity FSU and Fig. 4 for the high complexity FSU. We assume that for the high complexity FSU the pump will be stopped automatically (by the anti leak safety system) if the pressure in the shield around the pump becomes too high or too low. Fig. 5 displays the fault tree for the HEU for both low and high complexity.

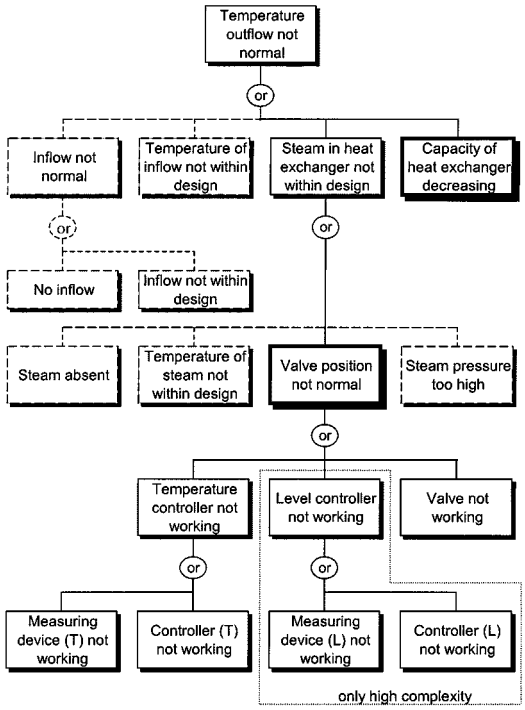

Fig. 5. System fault tree for low and high complexity of the HEU.

TABLE III
INITIATING EVENTS AND ASSOCIATED MECHANICAL FAILURES

Initiating Event	Mechanical Failure	Fault Tree	OAET
Pump not working *Low complexity FSU*	• Pump defect	Fig. 3	Fig. 6
Output valve position not normal *Low complexity FSU*	• Output valve defect. • Level controller defect. • Level measuring device defect.	Fig. 3	Fig. 7
Steam valve position not normal *High complexity FSU*	• Steam valve defect. • Level controller defect. • Level measuring device defect.	Fig. 4	Fig. 8
Pressure valve position not normal *High complexity FSU*	• Pressure valve defect. • Pressure controller defect. • Pressure measuring device defect.	Fig. 4	Fig. 9
Valve position not normal *Low complexity HEU*	• Steam valve defect. • Temperature controller defect. • Temperature measuring device defect.	Fig. 5	Fig. 10
Capacity of heat exchanger decreasing *Low and High complexity HEU*	• Corrosion, Sedimentation	Fig. 5	Fig. 11 Fig. 13
Valve position not normal *High complexity HEU*	• Liquid valve defect. • Temperature controller defect. • Level controller defect. • Temperature measuring device defect. • Level measuring device defect.	Fig. 5	Fig. 12

In Figs. 3–5, the initiating events caused by components outside a FPU are displayed with dashed lines. They will not be treated further here.

The term device "X" "*not working*" in the figures refers to a mechanical failure (device "X" "*defect*") or to a human operator error. Table III shows the initiating events and the associated mechanical failures.

The event trees are the same for an initiating event "*valve position not normal*" but the fault diagnosis will be different for each of the defect components initiating an event tree. This is treated in the next step of the methodology.

D. Step 3iv: Operator-Action Event Trees

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.

We assume that the operator performs the actions mentioned in the OAET alone without support system and that there are no false alarms, i.e., an alarm always implies a failure of a component. We assume that a component fails in the worst possible manner. Furthermore, only the initiating events caused by a failure of the components of a FPU are used to derive an OAET. The initiating events that will be used are shown in Table III (solid lines in Figs. 3–5). The detection error probabilities, DEP1 to DEP6 in the event trees, are treated in Section III-D.3. The fault diagnosis error probabilities (FDEPs) are treated in Section III-E.

1) Event Trees for the FSU:

a) Task complexity low: The event trees for the low complexity FSU are depicted in Figs. 6 and 7. The event trees are initiated by two different initiating events: "*pump defect*" and "*output valve position not normal*."

The OAET of the initiating event "*pump defect*" has three phases (Fig. 7). 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, then a recovery path in phase C exists. This pattern of phases is applied in all the event trees.

b) Task complexity high: The event trees for the high complexity FSU are depicted in Figs. 8 and 9. The event trees are initiated by two different initiating events: "*steam valve position not normal*" and "*pressure valve position not normal*." We assume that the pump will be stopped by the "*anti-leak safety system*" if the pressure in the shield around the pump becomes too low or too high. The human operator can detect this only by an alarm indicating a low rotation of the pump.

2) Event Trees for the HEU: The first phase in the event trees for the initiating event "*heat exchanger capacity decreasing*" is different. The detection part of this phase consists now of a monitoring task instead of an alarm detection task. Note that if in the position of the valve drifts to its maximum a decrease of capacity is implicitly indicated.

a) Task complexity low: The event trees for the low complexity HEU are depicted in Figs. 10 and 11. The initiating events are "*steam valve position not normal*" and "*heat exchanger capacity decreasing*."

b) Task complexity high: Figs. 12 and 13 present the event trees for the initiating events "*liquid valve position not normal*" and "*heat exchanger capacity decreasing*" of the high complexity HEU.

The OAETs show that for some initiating events (mostly in the high complexity configuration) the possibility exists to avert its effect on the FPUs performance. This indicates some degree

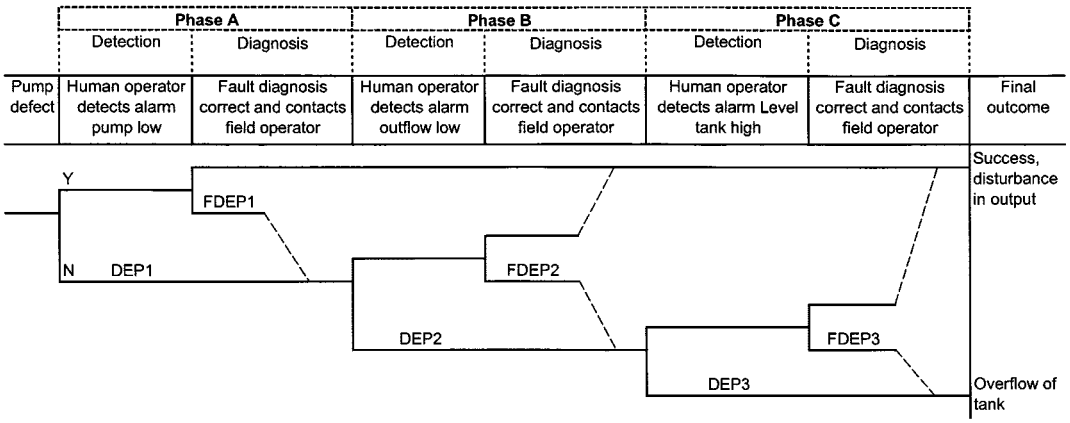

Fig. 6. Event tree for low complexity FSU starting with initiating event "pump defect."

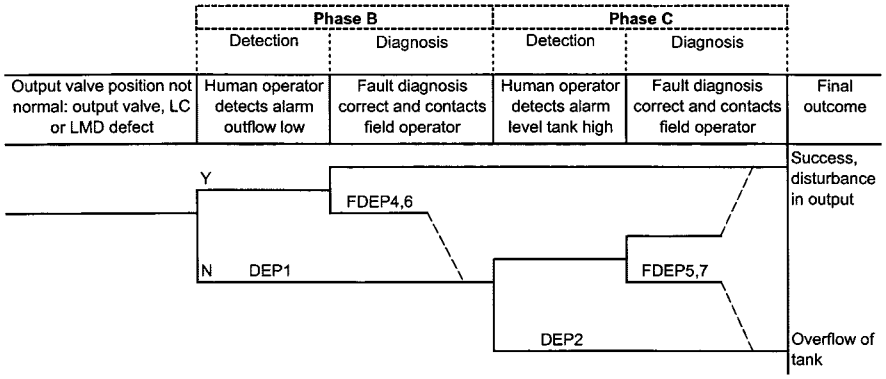

Fig. 7. Event tree for low complexity FSU starting with initiating event "output valve position not normal" due to a defect output valve, level controller (LC), or level measuring device (LMD).

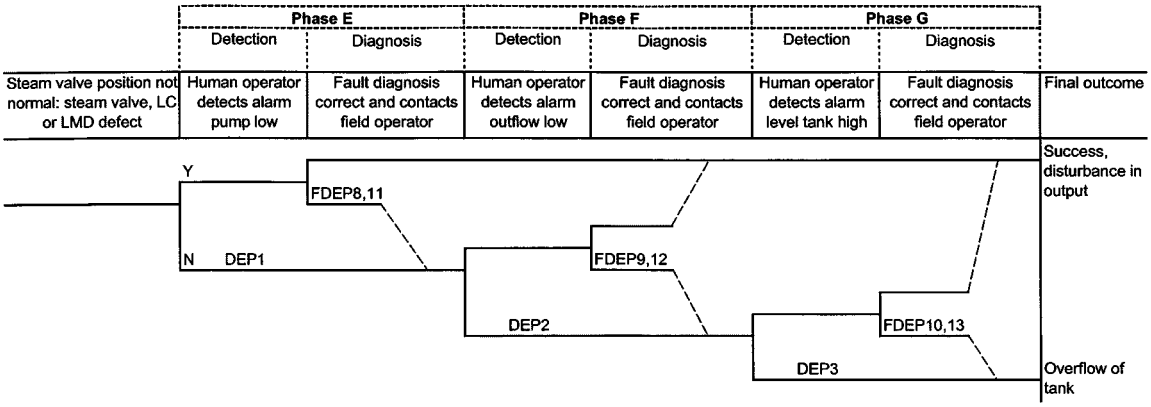

Fig. 8. Event tree for high complexity FSU starting with initiating event "steam valve position not normal" due to a defect steam valve, level controller (LC), or level measuring device (LMD).

of robustness. Smaller and simpler FPUs will not exibit such robustness such as, the low complexity FSU. Causal relations between events may improve the robustness of the FPU.

3) HEs for the Nodal Points: The operator can make several time independent errors while performing the task "*human operator detects an alarm low (or high)*" (indicated by the detection error probability DEP1 to DEP4 in all the event trees in Figs. 6–13).

1) Missing an alarm due to inattention or the assumption of a false alarm.
2) Selecting the wrong mimic on the HUMIF.
3) Detecting wrong alarm high (or low) instead of low (or high).

The HEU has a common task: detection of a decrease in capacity of the heat exchanger. This task is done in the low complexity configuration by performing the task "*monitor the valve position*." The human errors associated with the task "*human operator detects valve position to maximum*" (Fig. 11: detection error probability DEP5) are as follows.

1) Monitoring of the position of the valve not performed.
2) Selecting wrong mimic and thus thinking it is of different equipment.

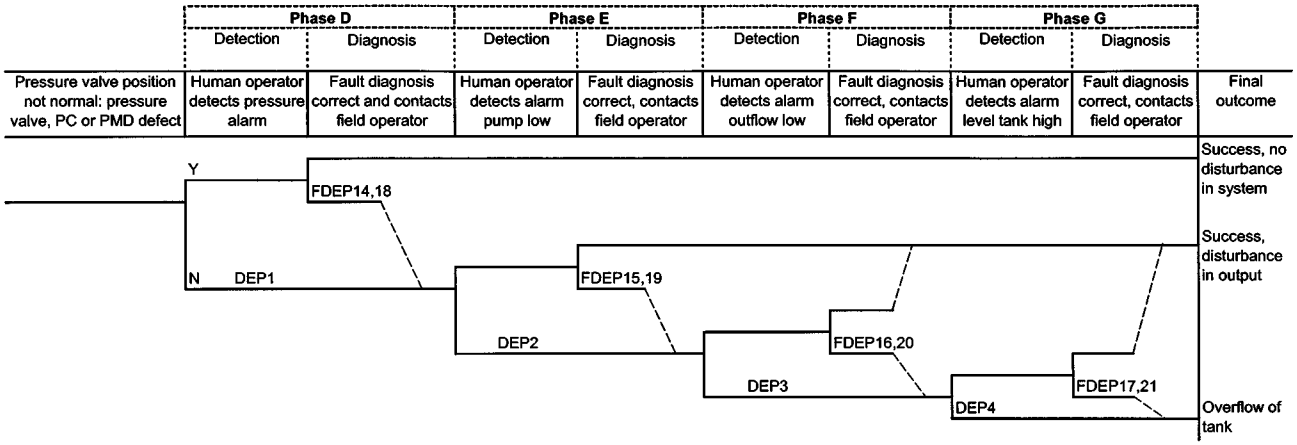

Fig. 9. Event tree for high complexity FSU starting with initiating event "pressure valve position not normal" due to a defect pressure valve, pressure controller (PC), or pressure measuring device (PMD).

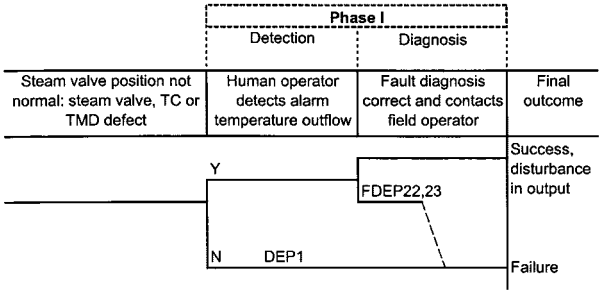

Fig. 10. Event tree for low complexity HEU starting with initiating event "steam valve position not normal" due to a defect steam valve, temperature controller (TC), or temperature measuring device (TMD).

3) Dynamic check reading error, human operator does not detect a trend in the value.

The decrease in capacity of the heat exchanger is in the high complexity configuration also detected by performing the task "*monitor the valve position*." In this configuration, there is an additional task "*monitor the level in the heat exchanger*" to detect the decrease in capacity. The errors for the task "*human operator detects valve position at maximum and level at minimum*" (Fig. 13: detection error probability DEP6) consist of the same list as above, and consist of the additional errors for the task "*human operator detects level in heat exchanger at minimum*."

1) Monitoring of the level in the heat exchanger not performed.
2) Selecting wrong mimic and thus thinking it is of different equipment.
3) Dynamic check reading error, human operator does not detect a trend in the value.

E. Step 3v: Human Operator Diagnosis Diagrams

After the human operator detects an alarm, several steps will be followed to diagnose the event. These steps are part of an (assumed) procedure and are described in the diagnosis diagrams. The diagnosis diagrams for the low and high complexity configurations of the FSU are displayed in Figs. 14 and 15. The diagnosis diagrams for the low and high configurations of the HEU are displayed in Figs. 16 and 17. The triangular tags labeled "A" in the diagnosis diagrams refer to Fig. 18.

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 basic human error probabilities (BHEPs) may be too big because of the summing up of the probabilities due to the "OR" functions in the diagnosis diagrams.

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 FSU (Fig. 6) using Table IV. Table IV displays the decision points of Fig. 14, with the text for the success paths, i.e., a correct fault diagnosis.

Phase A: The human operator detects the alarm "*pump low*" and starts the fault diagnosis (Fig. 14 at the top). The success path through the diagnosis diagram to detect that the pump is defective (Table IV).

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 (Fig. 14 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) as shown in Table IV.

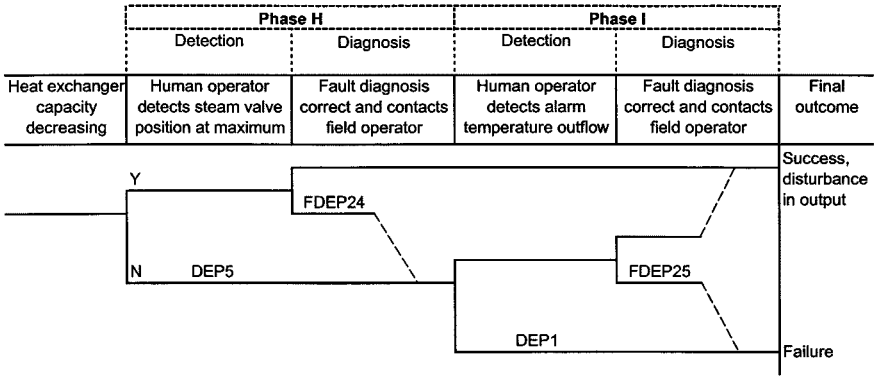

Fig. 11. Event tree for low complexity HEU starting with initiating event "capacity of heat exchanger decreasing."

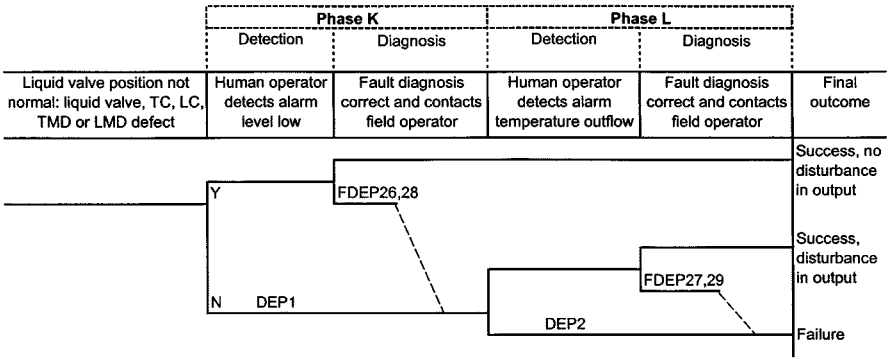

Fig. 12. Event tree for high complexity HEU starting with initiating event "liquid valve position not normal" due to a defect liquid valve, temperature or level controller (TC or LC), temperature or level measuring device (TMD or LMD).

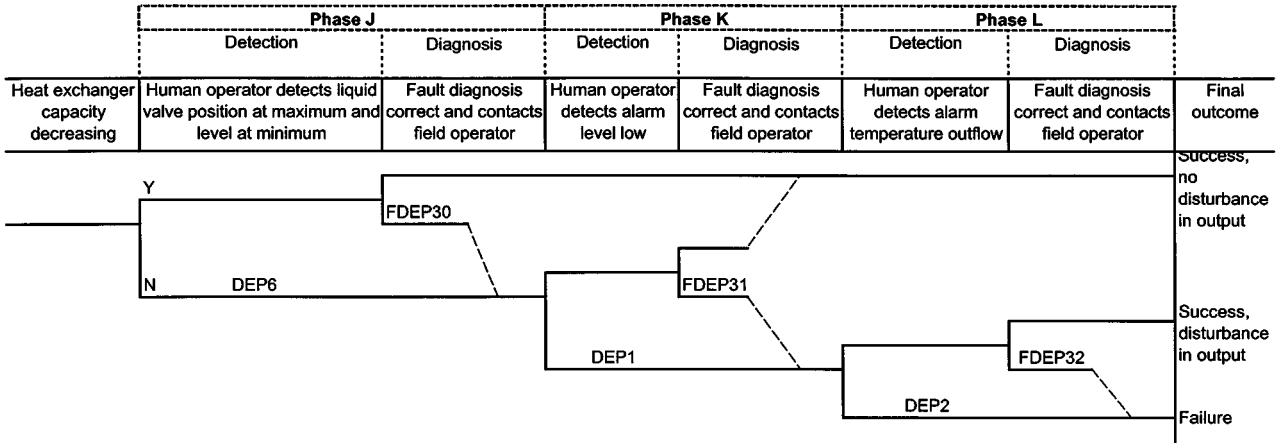

Fig. 13. Event tree for high complexity HEU starting with initiating event "capacity of heat exchanger decreasing."

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 HE. The HEs for an operator performing the task "*check the status of an indicator*" (CE1) are 1) selecting wrong mimic and 2) check reading error.

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

1) first indicator: selecting wrong mimic;
2) first indicator: check reading error;
3) second indicator: selecting wrong mimic;
4) second indicator: check reading error.

The human errors for an operator performing the task "*check the history status of an indicator*" (CE3) are 1) selecting (history) wrong mimic and 2) dynamic check reading error, human operator does not detect a trend in the value. At decision points in the diagnosis diagrams, the operator may select the wrong branch. The associated error probabilities are not depicted in the diagnosis diagrams.

IV. Step 4: BHEP for a FPU

The BHEPs for the event and diagnosis diagrams will be determined. We assume that the required time for the operators

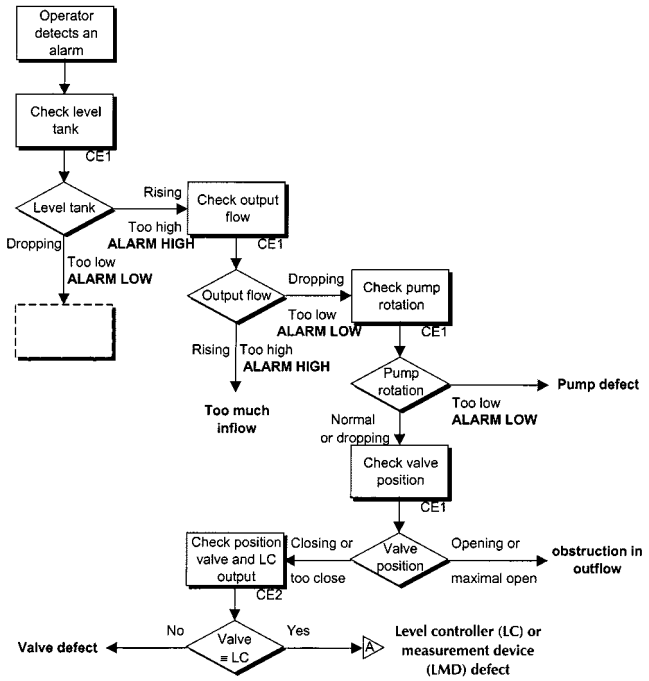

Fig. 14. Diagnosis diagram for the low complexity FSU.

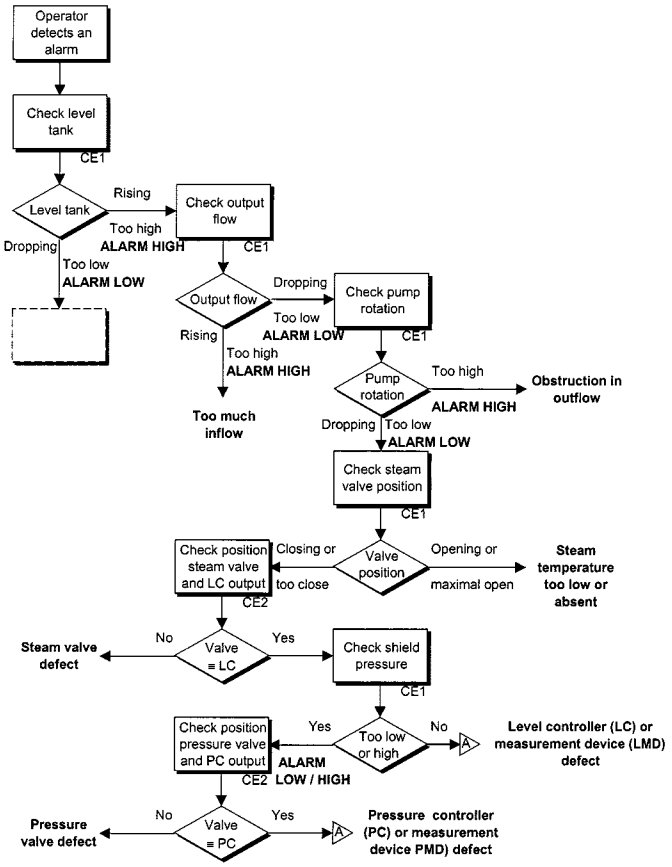

Fig. 15. Diagnosis diagram for high complexity FSU.

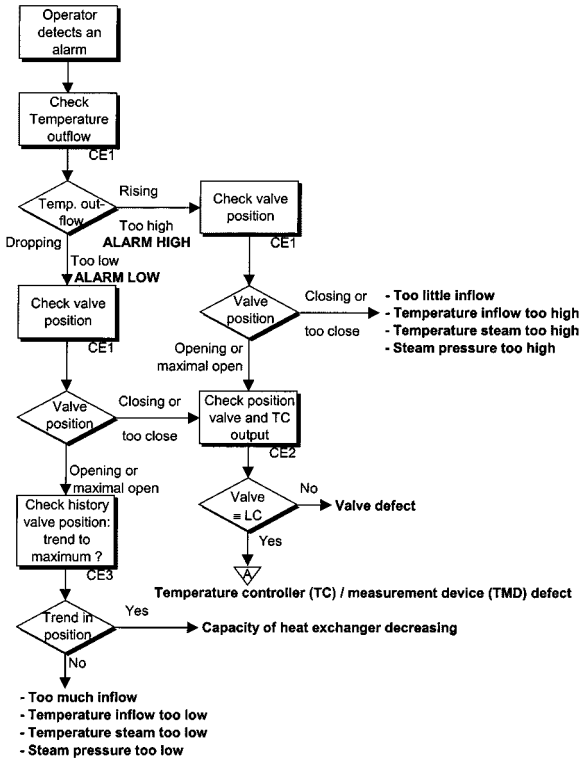

Fig. 16. Diagnosis diagram for low complexity HEU.

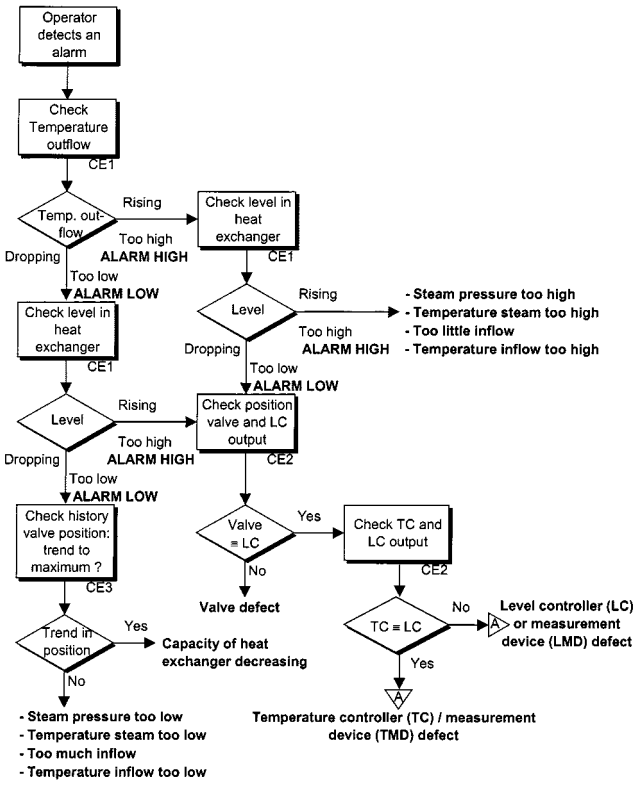

Fig. 17. Diagnosis diagram for high complexity HEU.

to perform fault diagnosis is 30 min. 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 min 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 min and represents a situation under stress. The BHEP will be determined for both conditions.

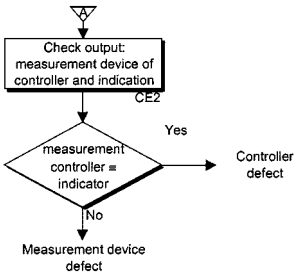

Fig. 18. Diagnosis diagram to decide between a defect controller or measurement device; low task complexity HEU has one alarm point; high task complexity HEU has two alarm points; low task complexity FSU has three alarm points; and high task complexity FSU has four alarm points.

TABLE IV
EXAMPLE OF A CORRECT FAULT DIAGNOSIS PATH IN DIAGNOSE DIAGRAM FOR INITIATING EVENT "PUMP DEFECT" (FSU, FIG. 14)

Fig. 14 / Fig. 6	Level tank	Output flow	Pump rotation
Phase A	Rising	Dropping	Too low Alarm low
Phase B	Rising	Too low Alarm low	Too low Alarm low
Phase C	Too high Alarm high	Too low Alarm low	Too low Alarm low

The handbook by Swain and Guttmann [10] is used to obtain the BHEPs. Table VIII summarizes the BHEPs and the error factors (EFs). The BHEPs will be explained here using references to the technique for human error rate prediction (THERP) [10] tables and items within brackets ( ).

a) The probability of the HE "*missing an alarm*" with sound is, according to the handbook, almost negligible [THERP Table 20–23 item (4)]. This value takes into account the perception, acknowledge of the alarm, decision as to what action is appropriate, and initiation of that action. The error of an operator assuming the alarm is a false alarm is included in these values.

It is more likely that a busy operator does not detect a consecutive alarm after detecting the first one. The BHEPs are different for the detection of consecutive alarms. The probabilities of THERP Table 20–23 are for alarms "closely in time," meaning within seconds or within a time period such that the operator perceives them as a group. This is not always the case in the event trees considered here. If the time between alarms is large, they may be considered individually, thus resulting in a lower BHEP.

b) The HE "*selecting wrong mimic*" is obtained from THERP Table 20–9. Item one, selecting wrong display when it is dissimilar to adjacent displays, is not used here, because it is assumed that the FPUs will be used more than once in the HUMIF. Thus, the selected items are selecting wrong display from similar-appearing displays with clearly drawn mimic lines [item (2)] and 2) selecting wrong display from well-delineated function groups on the MMI [item (3)].

c) The HE "*detecting a wrong alarm: low (high) instead of high (low)*" is not described in the handbook. Instead, the error of commission "*wrong letters recorded*" of THERP Table 20–10 item (9) will be used, because the text in the alarm list is L or H.

d) The HE of not "*monitoring the position of a valve*" or not "*monitoring the level in the heat exchanger*" is very small, because the decrease in capacity of a heat exchanger is very slow. THERP uses 0.0001 for a very small HEP.

e) The BHEP of check reading a display can be found in THERP Table 20–11. Each of the items (1)–(6) of THERP Table 20–11 is used, because these items can all be found in the process industry.

f) The BHEP of "*dynamic check reading*" is obtained from two THERP Tables, 20–11 and 20–16. Check reading is again obtained from THERP Table 20–11. The BHEP of dynamic check reading is obtained by multiplying the BHEP of check reading with a modifying factor of 1.0, assuming a skilled person with optimum task load (THERP Table 20–16 item 3).

g) The HE "*selecting a wrong branch at a decision point of a diagnosis diagram*" is not described in the handbook. It is likely that the probability of selecting a wrong branch is less with the aid of an alarm. To obtain the BHEP, dynamic reading of the low or high (L or H) alarm will be used (THERP Table 20–10 item 9) assuming a skilled operator (THERP Table 20–16 item 3). For the wrong selection of a branch without alarm, the value of THERP Table 20–10 (9) is multiplied with a factor 2.0 [THERP Table 20–16 (4)] assuming a skilled operator with more stress, because of the more difficult decision.

For the normal condition where the operator has 30 min to perform a fault diagnosis the BHEPs in Table V will be applied. In the case of stress (5 min to perform a fault diagnosis), the BHEPs will be modified by a factor five (THERP Table 20–16 items 5 and 6). This modification is not done for the HEs associated with the task "*detection of a decrease in capacity of the heat exchanger*," because the decrease in capacity is very slow. Thus, the BHEPs of these errors are taken the same (the BHEPs of Table VI) for both conditions (5 and 30 min).

Table VI shows the BHEP of the initiating events and the BHEP of the top events of the FSU and HEU assuming a mechanical failure probability equal to 1. This makes a comparison possible between the BHEP of the top events. Note that the BHEPs are calculated by using the median of the HEPs for all the steps.

V. DISCUSSION

A. General Discussion of the Methodology

The configurations of the FPUs that were taken as examples are realistic and are obtained from our industrial partners. We focussed on two different levels of complexity for a FPU. 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 FPU and the criteria with respect to safety, reliability, and product quality determine the choice of the top event. For instance, the FSU in our example performs a

TABLE V
BHEP FOR HUMAN OPERATOR (HO) ERRORS USING THE THERP HANDBOOK [10]

Human Error (HE)		HEP		THERP[9] table and items
		BHEP	EF	
a)	Human operator (HO) missing first alarm	0.0001	10	20-23 (4)
	HO missing second alarm	0.001	10	20-23 (4)
	HO missing third alarm	0.002	10	20-23 (4)
	HO missing fourth alarm	0.004	10	20-23 (4)
b)	HO selects wrong mimic	0.0005 – 0.001	10 - 3	20-9 (2)-(3)
c)	HO detects wrong alarm high (or low) instead of low (or high)	0.001	3	20-10 (9)
d)	HO does not monitor position of valve or level in tank	0.0001	3	
e)	HO check reading error	0.001 – 0.006	3	20-11 (1)–(6)
f)	HO dynamic check reading error	0.001 – 0.006	3	20-11 (1)–(6), 20-16 (3)
g)	Selecting wrong branch in decision point (with alarm)	0.001	3	20-10 (9)
	Selecting wrong branch in decision point (without alarm)	0.002	3	20-10 (9), 20-16 (4)

TABLE VI
BHEP FOR THE INITIATING EVENTS AND TOP EVENTS

Low complexity FSU	BHEP	
Initiating event	5 minutes	30 minutes
Pump	0,0008	7,26E-06
Valve	0,0279	0,0013
LC	0,0440	0,0021
MDL	0,0440	0,0021
Top event		
Overflow tank	**0,1124**	**0,0055**

High complexity FSU	BHEP	
Initiating event	5 minutes	30 minutes
Steam valve	0,0046	4,54E-05
LC	0,0129	0,0001
MDL	0,0129	0,0001
Pressure valve	0,0031	7,28E-06
PC	0,0057	1,46E-05
MDP	0,0057	1,46E-05
Top event		
Overflow tank	**0,0440**	**0,00036**

Low complexity HEU	BHEP	
Initiating event	5 minutes	30 minutes
Valve	0,1131	0,0236
TC	0,1588	0,0338
MDT	0,1588	0,0338
Capacity exch. decreasing	0,0088	0,0004
Top event		
Temp. not good	**0,3779**	**0,0889**

High complexity HEU	BHEP	
Initiating event	5 minutes	30 minutes
Valve	0,0108	0,0005
TC	0,0408	0,0019
MDT	0,0408	0,0019
LC	0,0408	0,0019
MDL	0,0408	0,0019
Capacity exch. decreasing	0,0006	5,05E-06
Top event		
Temp. not good	**0,1630**	**0,0081**

buffering function. Thus, the top event is "*overflow of tank*" (safety and reliability criteria). The top event would be different for a FSU that provides cooling water: "*no outflow*" (safety and reliability criteria). The top event of the HEU is a "*nonnormal temperature of the output*" (safety and quality criteria). In case the unit is used for direct heating, the top event would be "*absence of fluid*" (reliability and quality criteria), which can result in damage to the heat exchanger (safety criteria).

The initiating events can be due to human or system failure. The human related initiating events, e.g., an error of commission, require a detailed knowledge of the whole process and the working conditions, which are not known at the early design phases. In this survey only mechanical failures are considered. In addition, the initiating events that are due to damage of the components, like a ruptured pipe or a defect nonreturn valve, are not treated in this paper but can be added to the fault trees.

The event trees that we developed are more comprehensive than normal in a HRA, because for every alarm that the operator does not detect, a possible recovery path exists. Such recovery paths are realistic for operators in control rooms. For instance, it is possible that an operator conceives, due to a second alarm, that the first fault diagnosis was incorrect. This is only realistic for a small number of alarms as indicated in THERP Table 20–23 by the reduced probabilities for recovery after detecting a consecutive alarm.

Diagnosis diagrams represent the designed operating procedures and are used to determine the probability for not achieving the top goal in a FPU. The flow charts only include two options at each decision block. In reality, one may find more bifurcations. Furthermore, the procedures are symptom-based which enables the operator to act in a developing event according to the symptoms that are present [2].

Each phase in the OAET models the human operator functions: detection, check, and diagnose. The latter two are explicit in the diagnosis diagrams. It should be noted that the other cognitive functions [17] (planning, execution) are not included in our method. Hence, HEPs associated with execution errors are not considered.

We assumed that the operator always starts at the top of the diagnosis diagram after detecting an alarm. Another approach could be to start at the "*check box*" that belongs to 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) and 2) starting at the check box associated with the detected alarm for an alarm point on a "*component*" (direct alarm).

In reality, it is likely that an 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, for such cases, not realistic. For example, the pump in the low complexity FSU [Fig. 2(a)] 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 defective 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, Fig. 2(a)], 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 (diagnosis diagram) while performing a fault diagnosis. This is not

TABLE VII
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

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 (diagnosis diagram step). This is a very small error (BHEP $= 0.001$) according to THERP Table 20–7 item (1) and has not been taken into 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.* [18].

THERP suggests a much higher BHEP for a human operator performing fault diagnosis under stress (5 min) than was obtained using the diagnosis diagrams (Table VII). This can be explained as follows. First, the modifying factor of five, that we assumed to obtain a situation with stress, could be too small. Second, 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 min), 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 min). 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 min to perform a fault diagnosis).

The BHEP obtained from THERP should be corrected for low task complexity systems by applying a performance shaping factor (PSF). Thus, the diagnosis diagrams are a good approach to determine the BHEP of fault diagnosis.

It is impossible to assess the effect of all the PSFs at the early design phase considered in this paper because the HUMIF is not yet defined at that phase. However, some of the PSFs can be determined.

1) The factor "*training*" (internal PSFs) is omitted, because we assume that the operator is skilled and well trained.
2) The influence of the factor "*stress*" (stressor PSFs) on the control room operator is taken into account by assuming a higher stress level for the condition that there are only 5 min available to perform a fault diagnosis.
3) The influence of "*task load*" (stressor PSFs) is already taken into account in this methodology by using the diagnosis diagrams.

Various levels of detail can be identified during a design process. The methodology PREHEP can be implemented on the function level where standardized FPUs are used. The designer can than use the methodology to select equipment which accomplishes an acceptable probability for the top event. Alternatively, the designer can decide if human operator support systems are necessary.

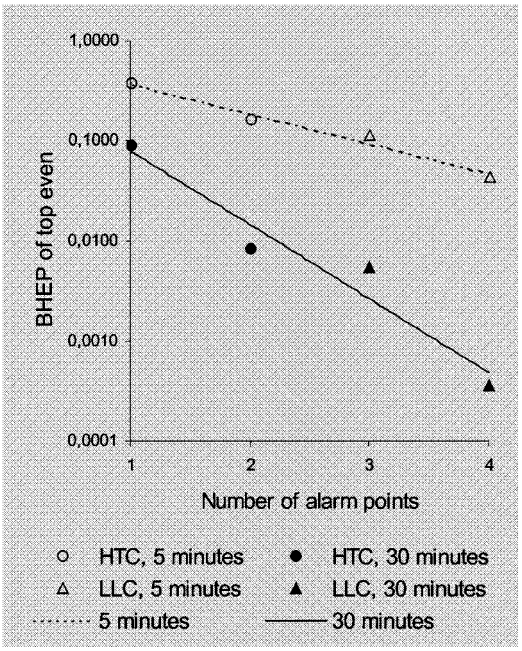

Fig. 19. BHEPs of the top events against the number of alarms in a configuration.

TABLE VIII
BHEP OUTPUT WITH OR WITHOUT DISTURBANCE

Available time for diagnosis of single event	BHEP low complexity FSU (Fig. 9)	
	No disturbance	Disturbance
5 minutes	0.7654	0.2315
30 minutes	0.9482	0.0518

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 subgoal level [19]. Decomposition into subgoals reveals the critical functions. For instance, a subgoal 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 FPUs addressed in this paper. Thus, the implementation of this methodology is only possible in the design phase where the functions are defined.

In order to perform a field system reliability study the only remaining problem on the functional level is the unknown mechanical failure probability of the equipment. If the equipment is selected, then the associated mechanical failure probabilities are known. Before this step, it is only possible to work with estimated mechanical failure probabilities.

B. Discussion of the Results

It was found (Table VI) that the BHEP decreases with increasing task complexity which is, for the examples we choose, proportional to the number of alarm points in a configuration (Fig. 19). Fig. 19 shows the normal condition (lower curve: 30 min to perform fault diagnosis) and the condition under stress (upper curve: 5 min to perform fault diagnosis).

TABLE IX
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 FPU 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 FPU is also normative.
▪ The possibility of inserting the FPUs into computer programmes for designing chemical processes. The selection of the BHEP may then be done 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 FPU that follow on an initiating event in a FPU. The contents of the process before or after a FPU are not known.
▪ No invention of the wheel again. All the known information about a FPU can be implemented in a standardised FPU 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 is dependent on the time between events and on the type of system by applying diagnosis 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.

As previously stated we assumed 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 FPUs, the operator has more recovery opportunities since more information is available, e.g., in the form of alarms. This is shown in Fig. 19, the BHEPs of a top event for the condition under stress (5 min) decreases from a very high (unacceptable) BHEP to a more acceptable one. The BHEP of the normal situation (30 min) decreases from an acceptable BHEP to a very small BHEP. This can be explained as follows.

A configuration with only one alarm point has a higher failure probability than a configuration with four alarm points. A decrease of the BHEP for a FPU with a high task complexity is the result of the following.

1) The number of initiating events for a top event increases with increasing system complexity. Since, an increase in system complexity is associated with an increase in task complexity.
2) The probability to miss an alarm decreases for consecutive alarms that are well separated in time due to THERP Table 20–23.
3) The probability of an unsuccessful or wrong fault diagnosis decreases for every phase of the event trees due to more extensive diagnosis (see diagnosis diagram in Fig. 17).

The event trees are affected by the last two points as follows. The probability of detecting the first alarm does not change, but the probability of an unsuccessful fault diagnosis decreases. Thus, the BHEP of success in the first phase in the event tree of a high complex system decreases. The probability that the operator misses the second alarm during later phases increases when a high number of alarms occur closely in time (THERP Table 20–23). The THERP Table 20–23 provides a value of 0.25 for ten or more alarms closely in time and a factor 0.001 for alarms that occur isolated. It is well known that in today's control rooms much more than ten alarms are generated during abnormal situations. Thus, the value given by THERP may be too low for high numbers of alarms and the fact that such conditions occur under stress. The BHEP for fault diagnosis also increases at later phases of the event tree because of point 3) shown above. Thus, it is plausible that the BHEP associated with an initiating event will increase with the number of alarm points. Hence, the findings summarized in Fig. 19 and the above rationale suggests that there exist a minimum BHEP for a certain number of alarm points.

The outcome in some event trees consists of "*success, no disturbance in the output*" and "*success, disturbance in the output.*" For example, the high complexity FSU (Fig. 9). If the operator detects a not normal pressure in the shield around the pump in time, then a disturbance in the outflow can be prevented. It is striking that the BHEP of the outcome "*success, no disturbance in the output*" becomes smaller and the BHEP of the outcome "*success, disturbance in the output*" becomes larger in case of the condition under stress (Table VII). This can be explained using Fig. 9 for a condition under stress (5 min). In the first phase, the probability to detect a "*pressure alarm*" decreases and the probability to perform a "*correct fault diagnosis*" decreases. Thus, the outcome "*success, no disturbance*" decreases also and the outcome "*success, disturbance*" increases due to the very small increase of the BHEP of the failure "*overflow of tank.*" This effect is very realistic. For example: In case of a system with fast dynamics, more events will have taken place before the operator performs a correct fault diagnosis and ap-

propriate counter actions. In the meantime, the possibility of a disturbance in the systems output will increase.

The BHEP associated with a pump failure in the low task complexity FSU is very small (Table VI) because several recovery paths can be taken. The other OAET has fewer recovery paths. In addition, the initiating event "*pump defect*" is the only one with a direct alarm point indicating a failure. All the other failures have an indirect alarm point indicating a failure. Thus, a low BHEP is expected for a failure with a direct alarm point.

The BHEP associated with a decrease in capacity of the heat exchanger is also very small. This is in accordance with what can be expected; well-trained operators use the valve position as an indication for the state of the heat exchanger. The BHEP of the high task complexity configuration confirms the assumption that a decrease in functional capacity of the system is easier to detect compared to the low task complexity configuration. This is due to the additional task, which is to monitor the level in the heat exchanger.

The BHEP associated with a valve failure in all the FPUs are also smaller than the BHEP associated with a defect controller or a defect measuring device. Therefore, to ascertain low overall failure probabilities in these FPUs it is necessary to have a smaller mechanical failure probability for the controller and measuring device than for the rest of the components.

C. Pros and Cons of Method

There are several pros and cons of the methodology presented in this paper. The main ones are presented and discussed in Table VIII. Further work needs to be carried out to implement the method into the design process. This can be done by implementing the method first on the functional design level. Inserting the approach as modules into computer programs for designing processes is one possibility. The feasibility of implementing the method also on a higher level has to be examined.

VI. Conclusion

A methodology has been presented to incorporate operator error probabilities into functional analysis of elementary process subsystems. The approach consists of determining the initiating events for a top event of a functional unit using a fault tree and then deriving the OAET for these events. The fault diagnosis in the OAET is done with the aid of a diagnosis diagram. The initiating events of the fault tree are triggered by mechanical failures. With all the mechanical failure probabilities set 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 identifying the need for redundancy. The complete process is not taken into account, because the HUMIF and the dynamics of the process are not known in the preliminary design phases. The results of the example configurations indicate the following.

1) The BHEP of a top event decreases with increasing task complexity (measure for task complexity: actions taken by the operator to detect consecutive alarm points in a configuration). In a very simple system, too few recovery paths exist due to the limited number of alarm and measuring possibilities to perform detection and diagnosis.
2) Indirect indications for component failure reduce the BHEP at higher complexity configurations due to better detection performance.
3) The BHEP associated with an alarm point directly associated with component failure is improving diagnosis performance.

Conclusion 1) and Fig. 19 do not imply that the more alarm points the lower the BHEP. The HEP for missing consecutive alarms above ten are not available. It is plausible that an adverse effect of the number of alarms on the BHEP can be seen for large and fast alarm sequences. This suggests that there exist a minimum BHEP for a certain number of alarm points.

The pros and cons of the methodology are summarized in Table IX.

References

[1] B. Kirwan and L. K. Ainsworth, *Guide to Task Analysis*. New York: Taylor & Francis, 1992.

[2] B. Kirwan, *A Guide to Practical Human Reliability Assessment*. New York: Taylor & Francis, 1994.

[3] G. Johannsen, A. H. Levis, and H. G. Stassen, "Theoretical problems in man-machine systems and their experimental validation," *Automatica*, vol. 30, no. 2, pp. 217–231, 1994.

[4] H. G. Stassen, "Hoe complex is een industrieel proces voor een procesoperator," in *Inspelen op complexiteit, Alkemade M. J. A. Samson bedrijfsinformatie b.v., Alphen aan den Rijn/Zaventem*, 1992, pp. 184–195.

[5] J. P. Scanlon, *Guidelines for the Design of Man-Machine Interfaces: Level 0*. Div. Automatic Control, N-7043 Trondheim, Norway: Sintef, 1981.

[6] ——, *Guidelines for the Design of Man-Machine Interfaces: Level 1*. Div. Automatic Control, N-7043 Trondheim, Norway: Sintef, 1981.

[7] J. Wirstad, *Guidelines for the Design of Man-Machine Interfaces: Level 2*. Div. Automatic Control, N-7043 Trondheim, Norway: Sintef, 1982.

[8] E. van Ravenzwaaij, N. V. Kema (Arnhem, The Netherlands), and H. G. Stassen (Tech. Univ. Delft The Netherlands), *Guidelines for the Design of Man-Machine Interfaces: Level 3*. Div. Automatic Control, N-7043 Trondheim, Norway: Sintef, 1986.

[9] J. Sharit, "Applying human and system reliability analysis to the design and analysis of written procedures in high risk industries," *Hum. Factors Ergon. Manufact.*, vol. 8, no. 3, pp. 265–281, 1998.

[10] A. D. Swain and H. E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Applications*. Washington, DC: U.S. Nuclear Regulatory Comm., 1983.

[11] S. Bi and G. Salvendy, "Analytical modeling and experimental study of human workload in scheduling of advanced manufacturing systems," *Int. J. Hum. Factors Manufact.*, vol. 4, pp. 205–234, 1994.

[12] W. Z. Gang, A. P. Macwan, and P. A. Wieringa, "Quantitative degree of automation," *Man-Mach. Syst. Contr.*, p. 26, 1996.

[13] J. H. M. Andriessen and P. A. Wieringa, *Influencing Complexity Means Man-Machine Interface*. Tech. Univ. Delft, The Netherlands Fac. WbMt: Vakgroep M&R, 1995, p. 15.

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

[15] "ISO 3511-4:1987 EN Technical drawings—Symbols for instrumentation—Basic symbols for process computer, interface and shared display/control functions,".

[16] S. M. Walas, *Chemical Process Equipment*, H. Brenner, Ed. London, U.K.: Butterworth, 1988.

[17] J. Rasmussen, "Skills, rules and knowledge: Signals, signs and symbols; and other distsinctions in human performance models," *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-13, pp. 257–266, 1983.

[18] A. P. Macwan, P. A. Wieringa, and A. Mosleh, "Quantification of multiple error expressions in following emergency operating procedures in nuclear power plant control room," in *Preprints of the PSAM-II*, G. E. Apostolakis and J. S. Wu, Eds. San Diego, CA, 1994, vol. 2, pp. 066-15–066-20.

[19] Design for Control Rooms of Nuclear Power Plants , Nederlandse Elektrotechnisch Comité (NEC). Normcommissie NEC 45 “Kerntechnische instrumentatie." Dutch Inst. Normalization, Delft, The Netherlands, Nov. 1989.

Martin Visser received the M.Sc. degree from the Department of Man-Machine Systems, Faculty of Design and Engineering, Delft University of Technology (DUT), Delft, The Netherlands, in 1998, while working on PREHEP.

Peter A. Wieringa (M’90) received the M.Sc. and Ph.D. degrees from the Delft University of Technology (DUT), Delft, The Netherlands, in 1980 and 1985, respectively.

From 1988 to 1990, he was trained in microvascular research at the University of Virginia, Charlottesville. He continued this research at the DUT and the University of Amsterdam, Amsterdam, The Netherlands. In 1991, he became Associate Professor in man-machine systems and studies human supervisory behavior and reliability of complex systems at the DUT.

Dr. Wieringa was a Fellow of the Royal Dutch Academy of Sciences from 1987 to 1991 and received an International Fogarty Fellowship (NIH) in 1998.