

---

## A New Method to Consider Human Actions in the Framework of a Dynamic PSA

*Martina Kloos, Jörg Peschke*

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS)

---

**Abstract:** The variety of accident sequences to be considered in the framework of a PSA derives from mutual dependencies between the physical process, the behaviour of the technical system, human actions and stochastic influences along the time axis. Because the conventional PSA approach is not able to adequately account for these interactions, so-called probabilistic dynamics methods have been developed. They generally achieve a more realistic modelling of accident scenarios and a more realistic safety assessment. At GRS, the method MCDET - a combination of Monte Carlo Simulation and the Discrete Dynamic Event Tree method - was developed. The implementation of MCDET was supplemented by a so called Crew-Module which allows - together with a deterministic dynamics code - to simulate human actions as a dynamic process evolving over time in interaction with the system and process dynamics. The Crew-Module accounts for communications between crew members and for performance shaping factors like stress, knowledge or ergonomics. This paper presents the Crew-Module and gives an overview of the results which may be obtained from its combination with MCDET and a deterministic dynamics code. The emergency operating procedure 'Secondary Side Bleed and Feed' in a German PWR is selected as an illustrative application.

### 1 INTRODUCTION

Over the past decades, the event tree analysis combined with fault tree analyses and with a few simulations performed by an appropriate deterministic dynamics code (like RELAP, ATHLET, MELCOR, or ASTEC) has gained widespread acceptance for analyzing the consequences of accident scenarios in a nuclear power plant. But experiences have shown, that the conventional PSA approach is not able to adequately handle the complex dynamics of accident scenarios while simultaneously accounting for stochastic influences. This is mainly due to the fact, that the analyses of human actions, of the behaviour of the technical system and of the physical process are decoupled from each other. I.e. the conventional PSA does not operate in the actual time/state space of the overall system of man, machine and physical process. Therefore, simplifications and compromises have to be made.

For instance, actual timing and process conditions are not part of the event tree model. They are available for only a few selected sequences judged to be representative for the spectrum of accident sequences. Thus, event tree analyses in a Level 1 PSA which are mainly concerned with the failure behaviour of safety and emergency system functions generally account only for the availability/unavailability of system functions at set points. No consideration is given, for instance, to situations where system functions which were successfully started fail to operate with the required capacity or fail to operate within the required mission time. Also human actions as part of the safety and emergency functions are usually considered just by two alternatives at set points, namely the successful execution and the omission of actions. Actual dependencies between the actions and the ongoing

system and process dynamics cannot be handled. Therefore, situations where the crew has to respond to changing process conditions (for instance, if successfully started safety systems fail to operate) and the process immediately reacts to corresponding interventions, remain unconsidered. The only information on the process dynamics which is taken into account is the time window available for a required action sequence. This time window is derived from one or two simulations of process situations (judged to be representative) and used to quantify the corresponding human error probability for different situations. Here the question arises, whether this approach is able to provide a realistic (or even conservative) safety assessment at the end.

In cases where timing and process conditions are judged to be relevant for the event tree model - for instance, in a Level 2 PSA where phenomena (like steam explosion or H<sub>2</sub> combustion) which do not permit a mechanistic modelling have to be handled - they are considered only in a rather coarse discretization (e.g. "early", "late" for the timing, "top", "bottom" for the location, or "small", "medium", "large" for magnitudes). This involves the risk, that accident sequences resulting from details in timing and process conditions remain unknown, but also that sequences with rather unlikely combinations of process conditions are taken into account.

Relevant accident sequences may also remain undetected, because the expert prescribes the order of events which would actually derive from the interaction between the dynamics of the overall system and the stochastics. That means, only accident sequences which follow the given order of events are taken into account. Therefore, it is arguable, whether the corresponding safety (risk) assessment can adequately account for the spectrum of event sequences that may actually evolve.

To overcome the deficiencies of the conventional PSA and to achieve a more realistic analysis of complex dynamic systems, probabilistic dynamics methods have been developed in recent years (*/1/, /2/*). At GRS, the method MCDET (Monte Carlo Dynamic Event Tree) was developed. It is a combination of Monte Carlo Simulation und the Discrete Dynamic Event Tree method (*/3/, /4/*). MCDET was implemented as a stochastics module which can operate in tandem with any deterministic dynamics code. The tandem is capable of handling the interaction over time between the stochastics as specified by the user and the dynamics as modelled by a deterministic dynamics code.

Because the combination of the module MCDET and a deterministic dynamics code is not able to account for human actions in sufficient detail, a so called Crew-Module was developed (*/5/*). The Crew-Module allows to simulate human actions as a dynamic process which evolves over time while interacting with the stochastics as modelled in MCDET and the system and process dynamics as modelled in the deterministic dynamics code. It accounts for communications between crew members as well as for so-called performance shaping factors like stress, knowledge or ergonomics which may affect human actions. Up to now, the Crew-Module has been restricted to errors of omission. In principal, the module would also allow the consideration of errors of commission, provided the experts are able to make assessments in this direction. The Crew-Module does not account for the mental process and the cognitive behaviour of the operators, as it was attempted, for instance, in */6/*.

The objective of this paper is to describe the Crew-Module and to give an overview of the results which may be obtained from its combination with MCDET and a deterministic dynamics code. Before this is done, an overview of the method MCDET is given in section 2. Section 3 presents the principles of human actions as modelled by the Crew-Module and explains, how the Crew-Module works in combination with MCDET and a dynamics code. Section 4 gives an illustrative application. Subject of the application is the emergency operating procedure 'Secondary Side Bleed and Feed' in a German PWR. Conclusions can be found in section 5.

## 2 THE PROBABILISTIC DYNAMICS METHOD MCDET

MCDET is a combination of Monte Carlo (MC) simulation and the Discrete Dynamic Event Tree (DDET) method.

MC simulation is the most straightforward numerical procedure for probabilistic dynamics analyses. It generates a random sample of event sequences according to the probabilistic information provided for stochastic events. Especially for a highly redundant system (characterized by safety functions with low failure rates), the computational effort of the MC analysis may be immense. In order to be able to adequately consider rare events (e.g. failures of safety functions with a low failure rate), a sufficiently large sample of sequences must be provided. Furthermore, the generation of each sequence requires a complete dynamics calculation starting from the initiating event and ending in one of the final states including damage states, states of no damage and controlled operation as well as the specified end of observation time.

The DDET approach organizes the computation of event sequences according to the tree structure known from the event tree analysis. All branches at a branch point (i.e. all alternative system and process conditions at a point in time) - also those of low probability - are tracked. Repeated calculations of dynamic situations shared by different sequences are avoided.

On the one side, DDET methods can adequately handle events associated by a time and a system state each of which may be either deterministic or random and discrete. Deterministic times and system states are taken into account as modelled by the applied deterministic dynamics code. Events which may occur randomly at a discrete point in time (e.g. failure at the 1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup>, etc. demand of a valve), or which are characterized by a random and discrete system state (e.g. availability/unavailability of safety functions) are handled according to the event tree structure.

On the other side, DDET methods lack a satisfactory treatment of events characterized by a time and/or system state which are random and continuous. These are, for instance, events where the failure of operating components may occur at any time within the required mission time, or events where operating components fail to function with the required capacity. In order to account for these events, DDET methods perform a discretization in time and/or state and consider all combinations of the discrete alternatives. To avoid a combinatorial explosion of the number of sequences, for instance, for scenarios characterized by a large number of safety functions with a relatively high failure rate, they are forced to apply a coarse discretization which consequently provides a less accurate PSA result. The accuracy of a result derived from a more or less detailed time discretization is hard to quantify.

The combination of MC simulation and the DDET approach as realized in MCDET is capable of accounting for any deterministic or stochastic event. Events associated with a time and a system state each of which may be either deterministic or random and discrete are generally treated by the DDET approach. MC simulation is used to handle events for which the timing and/or system state are random and continuous. MC simulation may also be applied for events with discrete alternatives in the timing and/or the system state, if the alternatives can adequately be represented in the MC sample.

MCDET provides a random sample of  $n$  DDETs. Each DDET is constructed on condition of a set of values randomly selected for the variables handled by MC simulation (MC variables). Instead of all combinations of discrete alternatives resulting from an underlying discretization, MCDET considers (only)  $n$  sets of values for the MC variables, no matter, for instance, how many system and safety functions with a high failure rate have to be taken into account.

The combination of MCDET with a deterministic dynamics code calculates, for each sequence of a DDET, the time histories of the process quantities and their likelihood. For each DDET, probability distributions are available for the process quantities and the corresponding system states (along the time axis). These distributions are conditional on the initiating event and on the values obtained from MC simulation. PSA statements are, finally, derived from the mean probability distributions over all DDETs. Each mean distribution provides an approximate summary of the stochastic variability of the quantities considered within a DDET. The mean distribution is provided together with a confidence interval which gives an indication of the possible error with which the mean probability derived from the sample may estimate the true probability. That means, MCDET allows the application of principles from statistics to estimate PSA quantities and to determine the accuracy of these estimates. In applications with computationally intensive models, a probabilistic "cut off" criterion can be introduced to keep the computational effort practicable. It has the effect, that all sequences with a conditional probability less than a user specified threshold value are ignored.

MCDET is implemented as a so-called stochastics module, i.e. as a library of routines which handle the stochastics in interaction with the dynamics. The routines are available to a scheduler program organizing the computation. The scheduler may use the routines in combination with an appropriate deterministic dynamics code simulating the system and process dynamics and with the Crew-Module which accounts for human actions.

### 3 THE CREW-MODULE

The main object of the Crew-Module is to simulate human actions as a dynamic process evolving over time in parallel to and in interaction with the behaviour of the technical system and the physical process.

#### 3.1 Principles of the model of human actions

A crew may consist of three or more individuals communicating with each other. Each crew member is responsible for a special task. There may be tasks which can be executed in parallel, and other tasks which can only be started, if some conditions (e.g. system and process conditions prescribed in the emergency procedure, or the confirmation from an operator of a successful task execution) are fulfilled. Information on the process and system state is given by the respective control room equipment like, for instance, indicators or alarms. It is read by the responsible operator and communicated to other crew members (supervisor, supervisor assistant).

On the one side, human actions may change the system state and affect the physical process. On the other side, the reaction of the process as indicated by the corresponding equipment in the control room affects the actions of the crew. Other factors which may influence human actions are so-called performance shaping factors like stress, knowledge or ergonomics and the communication between crew members. For instance, the information from an operator, that he is not able to correctly finish his task, may increase the stress level of the supervisor, and this may increase the likelihood to omit necessary actions (e.g. instructions) or to commit incorrect actions.

The Crew-Module is composed of a collection of scripts and routines. The scripts include the information necessary to describe the process of human actions, and the routines read and run the respective information. Three different scripts are defined, the 'BasicActions' script,

the 'ActionLists' script, and the 'AlarmIndicators' script. The structure of each script follows a special form.

The 'BasicActions' script comprises all basic actions relevant for the human actions to be modelled. Basic action means a simple action like, for instance, pushing a knob, shifting a switch, reading an instruction, simple communication (e.g. instruction of the supervisor to perform a special task), going to another place etc. Attached to each basic action are attributes which give information, for instance, on the operator performing the action, the operator or system component which is affected by the action, and on the time needed to execute the action. Probability distributions for random execution times must be specified within the stochastics module MCDET. For actions, for which human errors must be taken into account, the corresponding human error probability must also be specified within MCDET. For probability estimation, the ASEP (Accident Sequences Evaluation Program) or THERP (Technique for Human Error Rate Prediction) method may be used, for instance.

The 'ActionLists' script includes alternative sequences of basic actions. The action sequence to be realized may depend on the current state of the overall system (of man, machine and physical process) and, moreover, on its history. Therefore, each action sequence is associated with a corresponding initiation condition. All alarms and indicators which are relevant for the human actions to be modelled are defined in the script 'AlarmIndicator'. Attached to them are system and process conditions for their activation.

The main tasks of the Crew-Module routines are i) to read the information on alarms, basic actions and action sequences given in the corresponding scripts, ii) to check for conditions in the system and process state (including the relevant control room equipment) and in the crew performance, and iii) to run action sequences for which the conditions are fulfilled.

An essential feature of the Crew-Module is its flexibility. Any attribute can be defined for basic actions and any quantity of the overall system can be selected to specify a condition of the 'ActionLists' and 'AlarmIndicator' scripts. The Crew-Module may account for errors of omission as well as for errors of commission (so far an assessment is possible) and for the change and influence of performance shaping factors. The mental process and the cognitive behaviour are not modelled.

### **3.2 The Crew-Module in combination with MCDET and a dynamics code**

The combination of the Crew-Module with a deterministic dynamics code is capable of handling the interaction within the overall system of crew performance, system behaviour and physical process at each point in time. Coupling the stochastics module MCDET to this combination provides a simulation tool which can account for stochastic influences on the dynamics of the overall system, and vice versa, for the influence of this dynamics on the stochastics (e.g. on the order of stochastic events, on the magnitude of failure rates and probabilities, etc.).

The Crew-Module routines are available to a scheduler which organizes the alternate calculations of the Crew-Module, the deterministic dynamics code and the stochastics module MCDET. The scheduler starts the probabilistic dynamics calculations by transferring all user provided information on human actions (as given in the BasicActions' and ActionLists script), on the system and process dynamics (as modelled in the deterministic dynamics code) as well as on the stochastics (as specified in MCDET) to corresponding program and storage items. These items are permanently updated during the calculations.

For the construction of a DDET, the scheduler, first, calls the relevant MCDET routine to set the initial and boundary conditions. Depending on the conditions, either the deterministic

dynamics code or the appropriate Crew-Module routine is activated to start the calculation of the first DDET sequence. As long as the system and process dynamics is calculated and human actions have not been initiated, a Crew-Module routine checks whether a condition (specified in the 'AlarmIndicators' script) is fulfilled to start human actions.

Suppose a condition to start human actions is fulfilled, then the scheduler interrupts the calculation of the deterministic dynamics code and activates the Crew-Module routine which derives the time-dependent information on the sequence of (basic) human actions to be executed. The sequence reflects the process of human actions where tasks may be executed one after the other or in parallel. When the action sequence is finished or reaches a basic action which needs information from the physical process, the calculation of the Crew-Module routine terminates. In this case, the scheduler activates the deterministic dynamics code to calculate the system and process dynamics according to the information (for instance, on the system state change performed at time  $t$ ) provided by the Crew-Module. During the calculation, the relevant Crew-Module routine checks, whether the system and process state in combination with the state of human actions may produce a new sequence of human actions. If so, the calculation of the deterministic dynamics code is interrupted and control is given to the Crew-Module which selects a new time-dependent sequence of actions. If at the end of the calculation of the dynamics code performed according to the information of the Crew-Module, a condition is realized to continue the calculation of human actions, the relevant Crew-Module routine is activated. If not, the calculation of the system and process dynamics is continued either until a condition for human actions is fulfilled or until an absorbing state (e.g. a state of controlled operation or the user specified end of execution time) is reached.

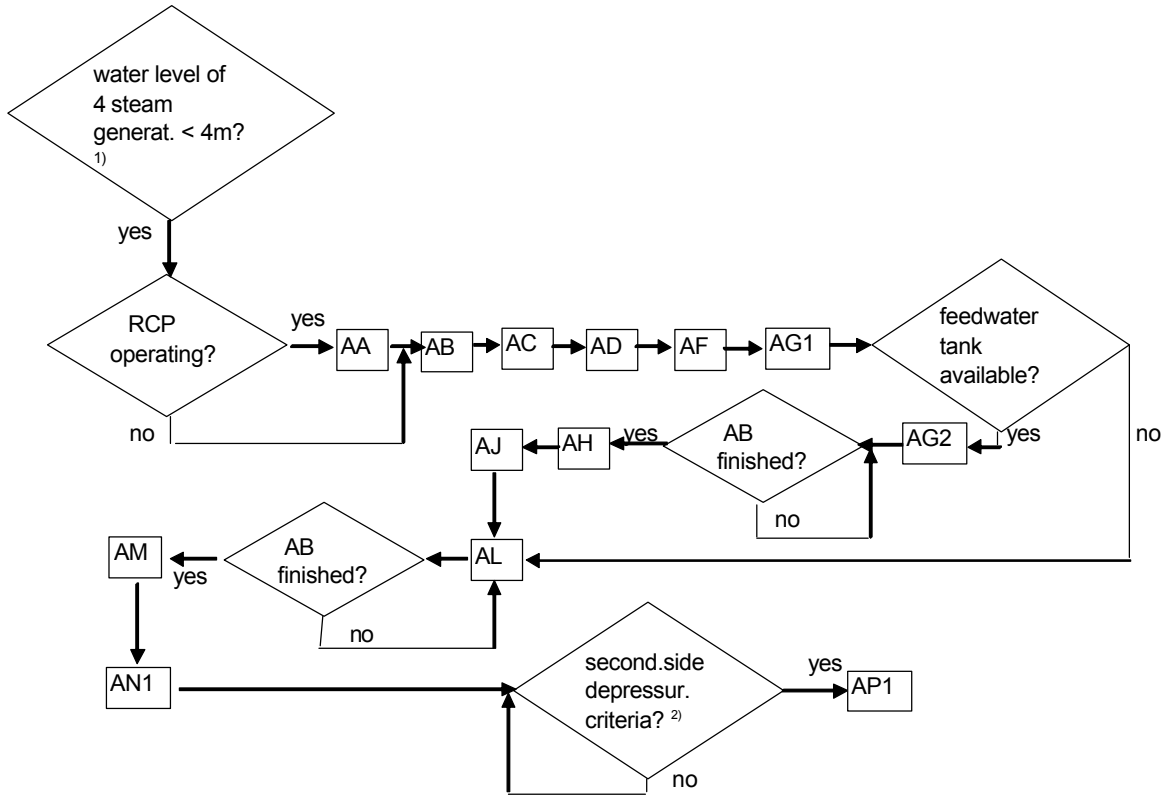
As soon as the state of the overall system of human actions, technical system and physical process is available for a point in time, the relevant routine of the MCDET module checks for conditions of stochastic events. If a stochastic event has to be handled by MC simulation, for instance, in case of a random execution time for a basic action, MCDET randomly selects a value from the corresponding probability distribution which is then taken into account for the ongoing calculation. If a branching has to be realized, because, for instance, a human action may be omitted or not, MCDET selects the branch to be calculated next (e.g. the branch where the action is executed), while the information of all other branches, which still have to be calculated (e.g. the branch where the action is omitted), is kept in memory according to a first-in-last-out structure. If the MCDET routine detects an absorbing state or calculates a sequence probability which falls below a user defined threshold, the calculation of the current sequence is terminated. In this case, the scheduler calls the MCDET routine which selects the next branch to be calculated. This is the branch which was stored last. The scheduler actuates the dynamics calculation with the initial conditions memorized on this branch. If there is not any branch left to be calculated, the construction of a DDET is completed. The construction of a new DDET starts with the activation of the MCDET routine which provides the initial and boundary conditions.

To reduce the computational effort, the scheduler organizes the dynamics calculations in a way which avoids repeated calculations of the same dynamic situation.

#### **4 ILLUSTRATIVE APPLICATION OF THE CREW MODULE IN COMBINATION WITH MCDET AND A DETERMINISTIC DYNAMICS CODE**

For illustration purposes, the emergency operating procedure (EOP) 'Secondary Side Bleed and Feed' is selected. This EOP is employed in German Pressurized Water Reactors (PWR) to achieve the protection goal of steam generator injection after the loss of feedwater supply. The work flow diagram in Fig. 1 shows the sequence of general tasks as they are given in

the written EOP description. For this application, the EOP is modelled up to the time, when the steam generators are depressurized (i.e. task AP1 of the diagram in Fig. 1).



The rectangles represent the EOP tasks:

- AA: Switch off of the reactor coolant pumps (RCP).
- AB: Simulation of the reactor protection system (takes place in the emergency feedwater building outside the control room).
- AC: Installation of the mobile pump (in the emergency feedwater building).
- AD: Inspection of the availability of the feedwater tank (in the engine house).
- AF: Permanent monitoring of the system and process state.
- AG1: Closing of the warm-up valves of the feedwater pumps to keep pressure in the feedwater pipe.
- AG2: Isolation of the feedwater tank.
- AH: Pressurization of the feedwater tank.
- AJ: Locking of the auxiliary steam stop valves to keep pressure in the feedwater tank.
- AL: Opening of valves to make available water content of the feedwater pipe after secondary side depressurization.
- AM: Placing the emergency feedwater lines into operation.
- AN1: Start of the mobile pump.
- AP1: Opening of the main steam relief control valves.

<sup>1)</sup> Process criterion for EOP initiation

<sup>2)</sup> Condition for the secondary side depressurization is fulfilled, if one of the following criterias occurs:

- pressurizer relief valve opens several times, or
- pressurizer water level > 9.5 m, or
- coolant temperatur in the primary system > 310°C.

**Fig. 1:** Work flow diagram of the EOP 'Secondary Side Bleed and Feed' as considered in the illustrative application.

The illustrative application is restricted to the stochastics in the actions of the crew, i.e. stochastic influences on the behaviour of the technical system or on the physical process are not considered. Human error probabilities are derived from the ASEP-method (Accident Sequence Evaluation Program, /7/). The probability distributions for the random times needed to execute actions (like reading a display, pushing a knob, giving an instruction etc.) are obtained by expert judgment. The type of all these distributions is specified as uniform. The knowledge uncertainties identified are represented by the mean values of the corresponding subjective probability distributions. The deterministic dynamics code MELCOR was used to simulate the system and process dynamics after the loss of feedwater supply.

Because of the great extent of the procedure, only some aspects can be presented in this paper. The detailed exemplary description in section 4.1 intends to show, what kind of information is necessary to model human actions and what kind of different interactions can take place even for a rather small part of the procedure. Section 4.2 presents some results and a discussion of the analysis.

#### 4.1 Exemplary description of the complexity of the model of human actions

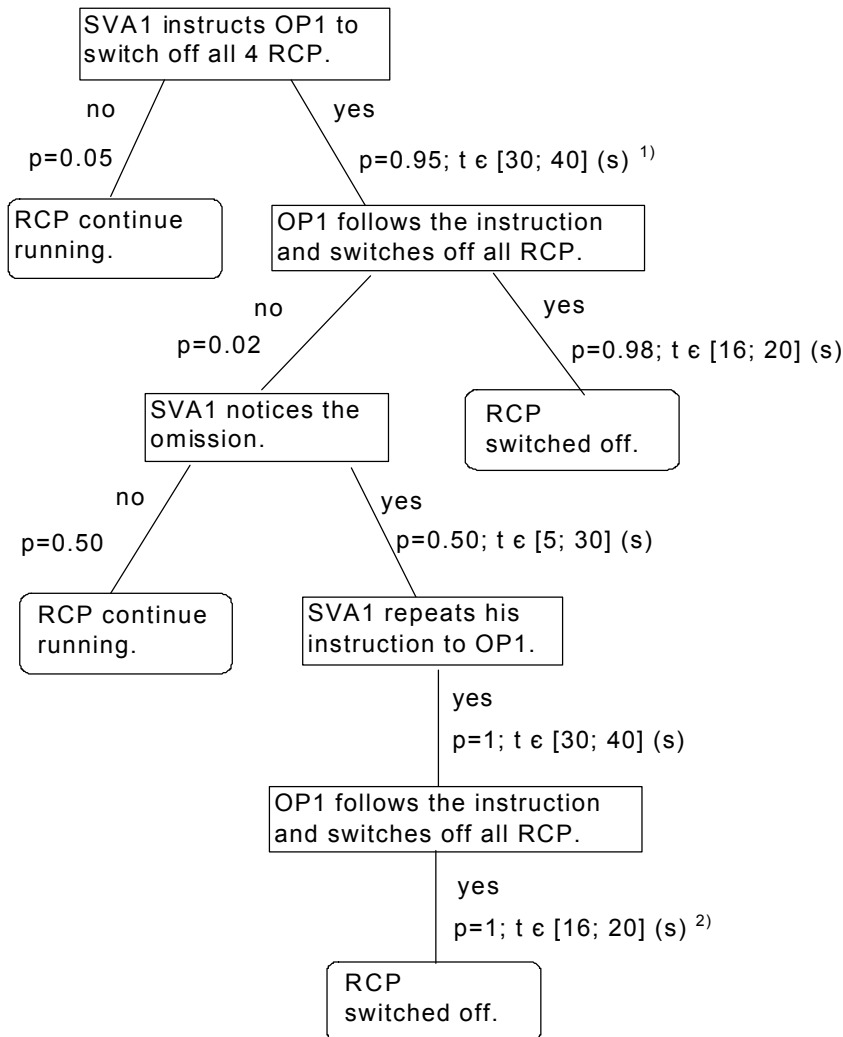
The EOP 'Secondary Side Bleed and Feed' is a rather extensive procedure. Therefore, a detailed exemplary description of the corresponding model of human actions is given only up to task AA of the diagram in Fig. 1 (Switch off of the reactor coolant pumps). A more extensive description can be found in /5/.

The execution of the EOP requires a crew of operators which have to execute different tasks within and outside the control room. The crew considered in this application consists of 8 members: a supervisor (SV) , 2 supervisor assistants (SVA1, SVA2) and 5 other operators (OP1,...,OP5). OP1 is concerned with the monitoring of the primary side, OP2 with the monitoring of the secondary side, while OP3, OP4 and OP5 are mostly outside the control room for inspection purposes.

The initiating event is the loss of steam generator water injection ( $t_0 = 0$ ), while power supply is available. The EOP actions are initiated, as soon as the corresponding displays in the control room indicate, that the water level of all 4 steam generators passes below 4 m. It is assumed that the displays operate correctly, and that they immediately indicate the process condition. Diagnosis and decision problems are not assumed, because the signals and criteria to start the EOP are clear. After the process condition for the EOP was indicated - this happens at  $t = 1709$  s according to the calculations of the deterministic dynamics code -, OP2 has to perform the first actions.

Actions associated with a time specification in the description below are considered as basic actions. OP2 arrives at the displays indicating the steam generator level after some delay time (1-20 s). He checks the display information (2-4 s for each of the 8 displays) and informs SV about the current situation (4-8 s). For controlling purposes, SV goes to the displays (1-5 s), reads them (16-32 s for 8 displays), and selects the written instructions to find out what to do (30-45 s). He instructs SVA2 to call back OP3, OP4 and OP5 into the control room (4-8 s), goes to the side desk (1-5 s) to check the 16 displays which indicate the availability of power supply (2-4 s for each display) and instructs SVA1 to undertake the operation control of the procedure (10-20 s) as long as he is concerned with the organization of the emergency task force (240-360 s). SVA2 who was instructed to call back OP3, OP4 and OP5, goes to the loud-speaker installation (1-5 s) and gives the respective instructions (20-30s). The times the operators need to return to the control room are 240-300 s for OP3 and OP4 and 480-600 s for OP5.

After SVA1 got the instruction to undertake the command, the next task to be executed would be task AA of the work flow diagram in Fig. 1. Task AA requires switching off the reactor coolant pumps (RCP). The stochastics in the actions of task AA is shown in Fig. 2. In a similar way, the stochastics with respect to other tasks of the procedure is handled. A complete description can be found in /5/.



<sup>1)</sup> SVA1 instructs OP1 to switch off all RCP with the probability  $p=0.95$ . SVA1 needs a time  $t$  of 30-40 s for the instruction.

<sup>2)</sup> It is assumed that repeated instructions are correctly executed.

**Fig. 2:** Stochastics in the human actions of task AA of the EOP ‘Secondary Side Bleed and Feed’

Due to human errors, different sequences of human actions may evolve. They differ in the time, when tasks are performed and in system states depending on whether a task is correctly accomplished or not. Fig. 2 shows two sequences with the 4 RCP switched off. The time, when the pumps are switched off, varies due to random times of preceding actions, errors of omission and delay times of recovery actions. Fig. 2 also shows two sequences

where human failure avoids a successful execution of task AA with the consequence that the pumps continue running.

At the end of task AA, i.e. at one of the final states of task AA (each achieved at different times), SVA1 waits for OP3, OP4 and OP5 to return to the control room. Depending on the time the operators need to come back and on the time SV needs for his organization task, different situations may happen. For example, if SV finished his work before one of the operators arrives at the control room, he informs SVA1 that he is ready to take back the command, and SVA1 gives SV a brief report about the current state of the procedure (60-90 s). In case, SVA1 has forgotten to instruct OP1 to shut off the RCP, SV notices this omission with a probability of 0.5, and recovery of the omission takes place, i.e. SV himself instructs OP1 to switch off all pumps (30-40 s). With a probability of 0.5, SV does not realize the omission, and the pumps continue running. Depending on the arrival time of OP3, OP4 and OP5, SV may first instruct OP3 to connect the mobile pump (120-150 s), then OP4 to perform the simulation of the reactor protection system, and finally OP5 to check the integrity of the feedwater storage tank (60-90 s). Evidently, the time when an operator is instructed, affects the time when the task for which he is responsible, is finished. Again, this affects the times when activities of other tasks can be started.

If the operators arrive at the control room, before SV is in command, SVA1 gives the corresponding instructions. If SV finished his organization task in the meantime and is ready to take back the command, he has to wait until SVA1 finishes his instructions to the operators. Of course, the time delay until SV takes back the command, affects the starting time of the recovery action in case task AA has been omitted, and this time affects the time, when the RCP are switched off.

Depending on whether the RCP are switched off and, if so, when they are switched off, the system and process criteria to depressurize the steam generators are reached earlier or later. It is assumed that the corresponding displays and alarms in the control room operate correctly and indicate the process situation immediately. Suppose the process criteria are indicated, then the depressurization of the steam generators can be initiated not before some preliminary actions (for instance, the simulation of the reactor protection system) have been executed. That means, the further sequence of human actions after the occurrence of the process criteria depends on the actions which have been performed so far. Of course, all actions may also be affected by performance shaping factors. For instance, the critical process situation in combination with the action sequence performed so far may raise up the stress level of the operators, and a higher stress level may increase the error probability.

As can be seen from the description above, even a small part of the EOP outlined in Fig. 1 leads to a variety of sequences. These sequences derive from the mutual dependencies along the time axis between human actions, the technical system, the physical process and the stochastics in human actions. Therefore, a valid assessment of human reliability has to account not only for human errors and the corresponding probabilities, but also for these interactions along the time axis.

## 4.2 Selected results

In section 4.1, the model of human actions is described in detail for only a small part of the EOP 'Secondary Side Bleed and Feed' outlined in Fig. 1. In a similar way, human actions regarding the other tasks of the EOP are modelled. Attached to each action modelled as a basic action (see section 3.1) is the information on i) the operator who performs the action, ii) the operators or system components which are affected by the action and iii) the time needed to execute the action. A total of about 150 basic actions are specified for the tasks of

the EOP. The information on the stochastics, i.e. on the probability distributions of the random execution times and on the human error probabilities, is specified in MCDET.

In this illustrative application, a sample of 500 discrete dynamic event trees (DDETs) was generated. All DDETs comprise a total of about 45000 different sequences. Probability distributions for process quantities, system states and human action characteristics (like, for instance, the execution times for tasks to be performed in the EOP) are available for each DDET. PSA statements are derived from the respective mean probability distribution over all DDETs. The mean distribution is given together with a confidence interval which indicates the possible error with which the mean probability derived from the sample may estimate the true probability. In the following, mean probability distributions are presented for a selection of time variables which are relevant for the EOP 'Secondary Side Bleed and Feed'.

The initiating event is the loss of steam generator feedwater injection, while power supply is available. The EOP is to be started, when the water level of all 4 steam generators passes below 4 m. In order to reduce the thermal energy contribution of the 4 RCP, the first task of the EOP is to switch off all RCP. The time, when all RCP are switched off, affects the critical time, when the steam generators can be depressurized. That means, if the RCP are switched off early, the critical time is delayed and the crew members have more time to accomplish their tasks. Similarly, the time when the process criteria for the depressurization of the primary side are fulfilled, is affected. This time is very critical for the current EOP, because the occurrence of the criteria for the primary side depressurization before the secondary side depressurization has been executed means the failure of the EOP.

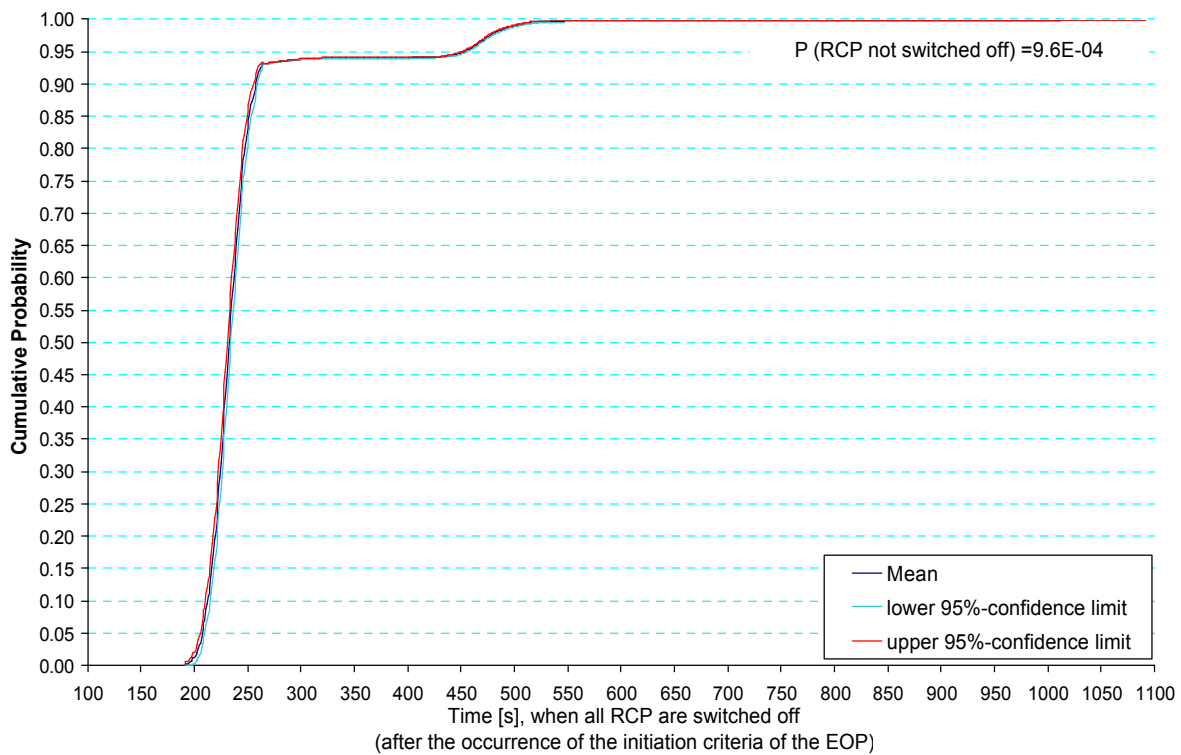
The many different sequences of the 500 DDETs show a rather large variation of the time, when the RCP are switched off. Fig. 3 presents the corresponding mean probability distribution. The indicated times relate to  $t=1709$  s – the time when the process condition for the initiation of the EOP is given. So, all RCP shut off at 400 s means, for instance, that the RCP are switched off 400 s after  $t=1709$  s. As can be seen in Fig. 3, there is a probability of about 0.94, that the RCP are switched off within  $t=300$  s. The probability to exceed  $t=450$  s is about 0.05, and the probability to exceed  $t=900$  s is about  $8.4E-4$ . With a probability of  $9.6E-4$ , the RCP are not switched off and continue producing thermal energy. In this case, the system and process criteria for steam generator depressurization are given at  $t=1736$  s. If the RCP are switched off after 900 s, there is a time profit of less than 240 s until the process criteria for the steam generator depressurization are fulfilled; the time profit is more than 420 s, if the RCP are switched off within  $t=300$  s. From the distribution given in Fig. 3, it can be concluded, that a time profit of more than 420 s can be achieved with a probability of 0.94.

An essential task of the EOP 'Secondary Side Bleed and Feed' is to pressure up the feedwater storage tank in order to use its water inventory for steam generator injection. The successful execution would lead to a delay of the process conditions for primary side depressurization. The diagram in Fig. 1 shows that task AH (Pressurization of the feedwater storage tank) can be performed only, if task AB (Simulation of the Reactor Protection System) is accomplished and the feedwater storage tank is available. Because technical failures are not assumed in this application, the availability of the feedwater storage tank is given. Nevertheless, the time needed to control the storage tank is taken into account. Obviously, the written EOP instructions suppose task AH to be executed, if the criteria for steam generator depressurization are given. This situation would occur, if the criteria are fulfilled after task AB was accomplished. For that reason, the probability distributions for the time, when task AB is finished and for time, when the process criteria for the secondary side depressurization are given, are of particular interest. These distributions are given in Fig. 4 and Fig. 5.

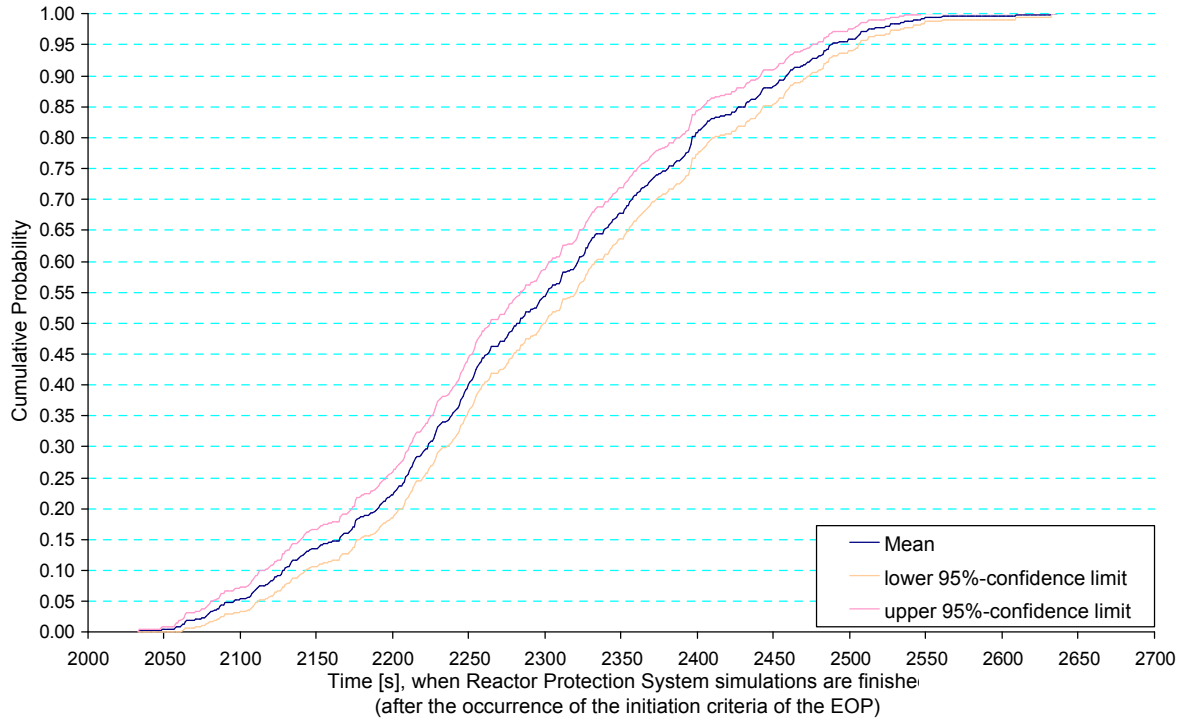
The distribution in Fig.4 shows, that the probability to accomplish task AB later than 2190 s (after  $t=1709$  s) is about 0.8. On the other side - as can be seen from Fig. 5 -, the process

criteria for the secondary side depressurization occur earlier than 2193 s with a probability of about 0.95. This would imply, that the actions of task AH are not performed with a high probability, because after accomplishing task AB, the crew is forced to start the depressurization of the steam generators. In fact, the results of the analysis show, that with a probability of about 0.82, the process criteria for steam generator depressurization already occur, while task AB is still performed. Therefore, the next tasks to be executed are tasks AM, AN1 and AP1 instead of task AH. The essential issue of the EOP to pressure up the feedwater storage tank is neglected with a very high probability. It is remarkable, that the reason for this are not the unavailability of the feedwater tank inventory or human errors which would lead to the omission of the tank pressurization, but the dependencies over time between human actions, the technical system and the physical process in consideration of random execution times.

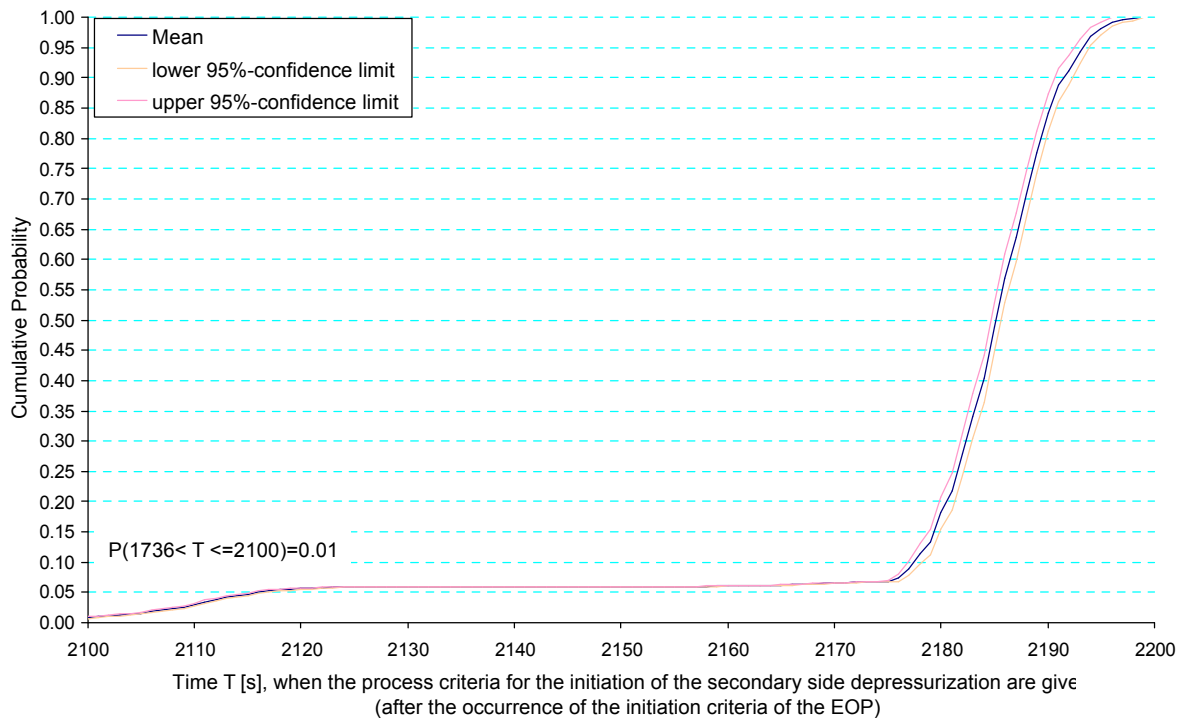
This illustrative application demonstrates an essential advantage of probabilistic dynamics methods in contrast to the conventional PSA approach. Probabilistic dynamics methods are capable of detecting situations which were not thought of before, but which may occur with a relatively high probability. Moreover, they provide much more insight into complex nonlinear systems than it is possible using the conventional PSA approach.



**Fig. 3:** Probability distribution of the time, when all RCP are switched off (after the occurrence of the initiation criteria of the EOP).



**Fig. 4:** Probability distribution of the time, when the simulations of the Reactor Protection System are finished (after the occurrence of the initiation criteria of the EOP).



**Fig. 5:** Probability distribution of the time, when the process criteria for the initiation of the steam generator depressurization are given (after the occurrence of the initiation criteria of the EOP).

## 5 CONCLUSIONS

Probabilistic dynamics methods have been developed, because the conventional PSA approach is not capable of adequately accounting for the complex dynamics of accident scenarios in interaction with stochastic influences. At GRS, the method MCDET - a combination of Monte Carlo Simulation and the Discrete Dynamic Event Tree method - was developed. MCDET is implemented as a so-called stochastics module, i.e. as a library of routines which handle the stochastics in interaction with the dynamics. The module MCDET operates in tandem with any deterministic dynamics code.

Because the combination of the module MCDET and the dynamics code is not able to consider human actions in sufficient detail, a so called Crew-Module was developed. The Crew-Module allows to simulate human actions as a dynamic process which evolves over time while interacting with the stochastics as modelled in MCDET and the system and process dynamics as modelled in the deterministic dynamics code. The combination of MCDET, the Crew-Module and the dynamics code allows an integral simulation of an overall system where human actions, the technical system, the physical process and stochastic influences are the main interacting parts in the course of time.

The Crew-Module is able to account for errors of omission as well as for errors of commission (so far an assessment is possible). Performance shaping factors like stress, knowledge, ergonomics, etc. which may affect human actions may also be considered. The Crew-Module does not intend to model the mental process and cognitive behaviour of the crew members. Nevertheless, the combination of the Crew-Module, the stochastics module MCDET, and an appropriate deterministic dynamics code provides a more realistic assessment of the consequences of accident scenarios than the conventional event tree method. More over, as is shown by the illustrative application, the combination is able to give an assessment of the efficiency of emergency operating procedures and allows a comparison of the efficiency of different measures of human actions.

Subject of the illustrative application is the emergency operating procedure 'Secondary Side Bleed and Feed' in a German PWR. The process dynamics was simulated for the scenario 'Loss of steam generator water injection, while power supply is available'. The effects of the interaction between the stochastics, human actions and the system and process dynamics are represented by a sample of 500 discrete dynamic event trees (DDETs). Each DDET provides probability distributions for process quantities, system states and human action characteristics (like, for instance, the execution times for EOP tasks). PSA statements are derived from the mean probability distributions over all DDETs. Each mean distribution is given together with a confidence interval which indicates the possible error with which the mean probability derived from the sample may estimate the true probability.

The illustrative application demonstrates an essential advantage of probabilistic dynamics methods in contrast to the conventional PSA approach. Probabilistic dynamics methods provide a more realistic modelling and, therefore, a more realistic safety assessment of accident scenarios. They are capable of detecting situations which were not thought of before, but which may occur with a relatively high probability. Moreover, they provide much more insight into complex nonlinear systems than it is possible using the conventional PSA approach.

## ACKNOWLEDGEMENTS

The developments of MCDET and the Crew-Module were sponsored by the German Federal Ministry of Economics and Technology within the framework of the projects RS 1111 and RS

1148. The authors wish to thank W. Fassmann and M. Sonnenkalb for their important contributions to the projects.

## REFERENCES

1. N. Siu, Risk assessment for dynamic systems: An overview, *Reliability Engineering and System Safety* 43 43-73 (1994).
2. P.E. Labeau, C. Smidts, S. Swaminathan, Dynamic reliability: towards an integrated platform for probabilistic risk assessment, *Reliability Engineering and System Safety* 68 219-254 (2000).
3. E. Hofer, M. Kloos, B. Krzykacz-Hausmann, J. Peschke, M. Sonnenkalb, Methodenentwicklung zur simulativen Behandlung der Stochastik in probabilistischen Sicherheitsanalysen der Stufe 2, Abschlussbericht, GRS-A-2997, Gesellschaft für Anlagen- und Reaktorsicherheit, Germany (2001).
4. M. Kloos, J. Peschke, MCDET - A Probabilistic Dynamics Method Combining Monte Carlo Simulation with the Discrete Dynamic Event Tree Approach, *Nuclear Science and Engineering* 153, 137-156 (2006).
5. J. Peschke, W. Fassmann, M. Kloos, M. Sonnenkalb, Methodenentwicklung für die Berücksichtigung menschlicher Eingriffe im Rahmen einer dynamischen PSA der Stufen 1 und 2, Abschlussbericht, GRS-A-3340, Gesellschaft für Anlagen- und Reaktorsicherheit, Germany (2006).
6. T. Shukri, A. Mosleh, S.H. Shen, Implementation of a Cognitive Human Reliability Model in Dynamic Probabilistic Risk Assessment of a Nuclear Power Plant (ADS-IDA), UMNE-97, Center for Technology Risk Studies, University of Maryland, College Park (1997).
7. A.D. Swain, Accident Sequences Evaluation Program Human Reliability Analysis Procedure, Washington (DC): US NRC, 1987