Decision Making During Nuclear Power Plant Incidents – A New Approach to the Evaluation of Precursor Events

Smith C.L., Idaho National Laboratory, USA

And

Borgonovo E., Bocconi University, Italy

ABSTRACT

Renewed interest in precursor analysis has shown that the evaluation of near misses is an interdisciplinary effort, fundamental within the life of an organization for reducing operational risks and enabling accident prevention. The practice of precursor analysis has been a part of nuclear power plant regulation in the US for over twenty-five years. During this time, the models utilized in the analysis have evolved from simple risk equations to quite complex probabilistic risk assessments. But, one item that has remained constant over this time is that the focus of the analysis has been on modeling the scenario using the risk model (regardless of the model sophistication) and then utilizing the results of the model to determine the severity of the precursor incident. We believe that evaluating precursors in this fashion could be a shortcoming since decision making during the incident is not formally investigated. Consequently, we present the idea for an evaluation procedure that enables one to integrate current practice with the evaluation of decisions made during the precursor event. The methodology borrows from technologies both in the risk analysis and the decision analysis realms. We demonstrate this new methodology via an evaluation of a US precursor incident. Specifically, the course of the incident is represented by the integration of a probabilistic risk assessment model (i.e., the risk analysis tool) with an influence diagram and the corresponding decision tree (i.e., the decision analysis tools). The results and insights from the application of this new methodology are discussed.

1 INTRODUCTION

Precursor events can be defined as "*conditions, events and sequences that precede and lead up to accidents* [Phimister et al. (2004)]." In the recent past, the scientific community has shown renewed interest in precursor analysis, as testified by the seven-month 2003 project of the US National Academy of Engineering aimed at unifying the "*complex issue of accident precursor analysis* [Phimister et al. (2004)]." The issue was tackled from different perspectives coming to the decisive conclusion that precursor analysis is a multidisciplinary effort [Phimister et al. (2004)]. Patè-Cornell (2004) presents a probabilistic approach to utilize precursor analysis to create "*signals that action has to be taken … to reduce the risks of failure as much as possible within resource constraints.*" Carroll (2004) demonstrates the importance of knowledge management within organizations, so that precursors can be effectively addressed as "*signals of possible problems*" and "*opportunities to enact and*

improve organizational practices." Phimister et al. (2004) not only observe the interdisciplinary nature of precursor analysis, but also the fact that this practice is diffused across different industries[1].

In the nuclear industry, the US Nuclear Regulatory Commission (NRC) (please find a list of acronyms in Table 1) started the Accident Precursor Sequence Program in 1979 [Sattison (2004)]. Over a thousand licensee event reports are submitted to the Nuclear Power Plant (NPP) regulator, the NRC, each year. Contained within these reports are events ranging from inconsequential notices of minor plant deviations to quite serious depictions of incidents that came somewhat close to potentially impacting adequate cooling of the reactor core [so-called *precursor event* as defined in NRC (2001)]. Fortunately, the serious events are a small fraction of the total number of events [Sattison (2004)]. Further, the number of these events has been decreasing in the US over the last decade of operation, but these events still number in the range of 20 (or less) each year. Each year the "most risk significant" events are tabulated and ranked according to the conditional core damage probability (CCDP) in the NRC publication NUREG/CR-4674 (Table 2.) CCDP [Smith (1998)] is the risk metric utilized by the NRC to determine the seriousness of a precursor event. It is defined as the probability of core damage given the plant configuration observed during the initiating event situation or during the unplanned equipment outage [Smith (1998)].[2] The calculation of the numerical CCDP value is based on the probabilistic risk assessment (PRA) model and carefully considers the impact to the base-case model of aspects such as operator actions/recoveries, adjustments to dependent events like common-cause failure probabilities, and plant-centered initiating events.

If one dissects the precursor events that have occurred over the last 20 years, two items are revealed that seem common amongst them: (1) robust, redundant system construction, and (2) decision making by trained

---

[1]Sattison (2004) discusses the accident sequence precursor program of the US Nuclear Regulatory Commission. Precursor analyses in aviation can be found in Connel (2004) and Hart (2004). Tamuz (2004) compares precursor analysis methods in aviation, nuclear industry and healthcare. The importance of accident prevention in the chemical industry is underlined in the work of Kleindorfer et al. (2003).

[2]Key to public protection in the nuclear industry is to prevent release of radioactive material outside the power plant. The reactor core area contains the radioactive materials. Hence, damage to the core, besides impairing electricity generation, can potentially lead to emission of radioactive material to the public. Since the reactor core is also the part of the reactor where energy is produced, keeping its temperature low by providing cooling is essential to the safety of the power plant, as we shall see shortly in the discussion of the precursor event.

professionals. During an incident, in fact, events occur that change the configuration of the plant and response may be needed to bring the plant to a safe situation. In a real situation, based on diagnosis, the on-site decision maker locates people and resources to pursue what is perceived to be the best strategy. She/He is constantly receiving information and reassessing the strategy. Thus, as the works of Jae and Apostolakis (1992), Jae et al. (1993), Svenson (1998), and Smith et al (1999) illustrate, accident management can be viewed as a sequential decision problem under uncertainty.

This work proposes a methodology to allow the evaluation of the decision making aspects of a precursor event. In this respect, it adds to current precursor practice the analysis of decision making aspects which complement the probabilistic, organizational and corporate culture aspects of precursor analysis summarized in Patè-Cornell (2004), Carroll (2004) and Phimister et al. (2004). Furthermore, the methodology provides a structured approach in addressing and formulating questions on random events and accident management strategies triggered/requested by the precursor.

Central to the approach is the representation of the precursor event in the form of a decision analysis model. Decision analysis problems can be represented in the form of decision trees (DT) [Raiffa (1968), Clemen (1997), Pratt, Raiffa and Schlaifer (1995)], influence diagrams (ID) [Schachter (1986), Schachter (1988)], valuation networks [Shenoy (1992)], and sequential decision diagrams [Covaliu et al. (1995)][3]. Bielza and Shenoy (1999) offer a detailed comparison of ID's, DT's, valuation networks and sequential decision diagrams. The conclusion of the work is that none of the above representations is definitely superior to another [Bielza and Shenoy (1999)]. We make use of ID's and the corresponding DT's. However, what is uniquely described in our methodology is the utilization of insights and information derived from application of the PRA methodology to the sequence of events involved in the precursor, whereby we focus on decisions rather than the traditional approach taken in precursor analysis of looking at failure events.

---

[3] To the present list, one can add the representation of decision analysis problems in the form of Bayesian Networks [see Papazoglou (1999) and Neil et al. (2005).]

We discuss in detail the steps of the methodology, with special reference to how to let information contained in the PRA feed into the ID or DT. We show that this process: *i)* enables the analyst to determine equipment involved in the sequence, which, in its turn, *ii)* leads to identify accident management strategies, and *iii)* allows to estimate the corresponding random event probabilities. We show that a novel feature in the retrospective use of PRA is played by the discretization of the PRA event sequence, with the recalculation of the corresponding configurations. This feature, together with the decomposition of the decision analysis problem in its main elements[4], allows us to reveal what information on these items is contained in the PRA model and can be automatically inserted into the decision analysis model. We then show that the natural conclusion of the proposed approach is the evaluation of the decisions taken during the precursor incident. By appropriately defining the utility function [Kreps (1988), Keeney (1980)], an analyst can establish whether the course of action during the accident coincides with the course of action that a decision maker sharing the same utility function of the regulator or the industry would have undertaken.

The remainder of the paper is organized as follows. In Section 2, the methodology is presented. Section 3 demonstrates the methodology through application to the precursor event at the Davis-Besse Nuclear Power Station (loss of main feedwater) of 1985. Section 4 provides conclusions.

2 THE METHODOLOGY

In this Section, we discuss the methodology proposed in this work for revealing and evaluating the decision making aspects of precursor events. During the course of a precursor event, or, more generally, during an incident, plant operators face a sequential decision problem under uncertainty [see, for example, the work of Jae et al. (1993)][5]. They are faced with an initiating event that may require diagnosis and action in order to contrast

[4] In Clemen (1997), decision analysis elements are defined as alternatives, random events, consequences, objectives and attributes of the decision maker.

[5] It is worth to point out the difference of the problem tackled through the present approach and the problem dealt with in Jae and Apostolakis (1992) or Jae et al. (1993). In Jae and Apostolakis (1992), influence diagrams are utilized to establish the best course of action given a potential future accident situation. Thus, the best strategies are identified based on a model that describes what can happen in a future accident. In the present work, the accident has happened, but one has the problem of determining whether the adopted course of action has indeed been the optimal one. We also wish to point out

the progression of the incident and not to let the sequence reach the worst consequence (core damage, for example, in the nuclear industry).

Before illustrating our methodology, we recall Clemen (1997)'s decision making process steps, as a benchmark against which distinctive features of our approach can be better illustrated. Step 1, "Identify the Problem," consists of the determination and the analysis of the problem. Step 2, "Identify objectives and alternatives," aims at the determination of the alternatives associated with the decisions to be taken in the problem, and of the decision maker values and objectives. Step 3 consists of the creation of the model, and in the assessment of probabilities and utilities. Step 4, "Choose the best alternative" consists in the evaluation of the alternatives. Step 5, "Sensitivity Analysis," foresees performing sensitivity analysis to establish whether further analysis is needed or if the decision maker feels confident enough to go to the best alternative implementation. The process is thought of as iterative in nature.

The first distinctive feature of our precursor decision analysis appears at this point. The decision analysis steps as per Clemen (1997), point towards a decision which is made now, but whose consequences fall in the future. In the present methodology, the analyst is reconstructing ex-post the decision making problems encountered during a precursor event. The scope of a decision analysis model in an ex-post reconstruction is to find the strategy that solves the decision making problem for the ex-post decision maker, i.e., to find what actions during the course of the accident sequence maximize the expected utility of the ex-post decision maker. One therefore answers the question of how the ex-post decision maker would have acted if She/He were faced by the same decision problem as the true actors. For instance, if the utility function represents the values and objectives of a regulator or an industry body, the analysis of the precursor event helps in establishing whether the decisions that were taken at the plant adhere to those that the regulator or the industry body would have taken. Since the method explicitly calls out the decision analysis aspects, it offers a structured way of revealing discrepancies between the on-site and ex-post decision makers' choices. One can assess whether eventual deviations were

---

that in creating a prospective model, one has to hypothesize events. In a retrospective model, one knows the events that have happened. Thus, model uncertainty is lower in the second case.

dictated by different views on the event probabilities, by partial information on the flow of events or by different utility functions. This last point could signal a disagreement between the on-site and ex-post decision maker attributes and objectives.

In order to derive such insights, we break down the approach in the following seven steps (Figure 1).

STEP 1: PRECURSOR EVENT ANALYSIS

This first step consists of gathering information on the incident evolution, the mitigating strategies adopted by the on-site decision maker, and of identifying the equipment and random events involved in the sequence. Such information is derived from relevant documentation (internal reports, industry reports, interviews) concerning the incident. The present step is the equivalent of the "Problem Identification" step of Clemen (1997). The difference between the two steps lies in the fact that, in a prospective decision analysis [Clemen (1997)], an analyst is gathering information to assess what events might be involved in the decision problem after the decision has been taken. In an ex-post analysis, one is reconstructing events that actually happened and what strategies have been selected against them.

STEP 2: PRA ANALYSIS

This step consists of following the accident sequence through the PRA model. Since the PRA model is a detailed study of the technical safety of a plant, it provides quantitative information on events and probabilities at each step in the accident sequence. We would like to point out that the utilization of the PRA model in connection with the decision analysis model requires some technical refinement of standard CCDP calculation procedures. The novelty is represented by the analysis of the plant configurations that are registered during the incident, each of which is resolved by a corresponding PRA model evaluation. We call this process "discretization," and note that it is similar to what is currently implemented on risk monitors at NPP's. However, our discretization takes place as a function of each modeled decision and the potential events that transpire from that point in time.

We illustrate this step as composed of four sub-steps.

- STEP 2.A: DISCRETIZATION AND IDENTIFICATION OF PLANT CONFIGURATIONS

The first step of the PRA analysis is to decompose the sequence of events into blocks of times where the plant was in a particular *configuration*. Thus, we are discretizing the plant state into time bins, where like time bins are grouped together into a single bin. This step is similar to that used by "risk monitors" in use at some NPPs.

- STEP 2.B: CONFIGURATION MAPPINGS

After the discretization and identification of each plant state over time, each state must be evaluated using the PRA model. To perform this step, the plant state during a particular configuration must be "mapped" into the PRA model. This mapping process requires the identification of specific basic events in the PRA that are impacted in any way by the component degradations or initiating events that occur at the start of the configuration. During this step, modeling of failures for the relevant phases in the incident is important to the CCDP calculation. Sometimes, failure of equipment not already modeled in the PRA model is encountered. Ultimately, these types of issues were resolved by either modifying the nominal PRA model (including the failure in the applicable fault tree) or utilizing "surrogate" components where necessary. The notion of surrogate components represents those physical parts of the plant's hardware that are not modeled directly in the PRA but such that, when failed, their impact on CCDP may be represented by using an associated component that is modeled in the PRA.

- STEP 2.C: CCDP CALCULATION FOR EACH CONFIGURATION

For each configuration, the PRA model is resolved by regenerating the overall core damage minimal cut sets using the new basic event data. One can introduce the analysis in a PRA dedicated software [see for instance SAPHIRE (Russell et al. (1999)].

As the incident progresses through time, the resulting values of the risk metrics vary through time. This implies that the same decisions taken at different points in time over the course of an incident are associated with a different level of risk (and, correspondingly, of risk perception). It is then possible to understand points in the incident that coincide with large *increases* in the risk metrics and to establish whether actions were taken at these points to counterbalance the increase in risk.

- STEP 2.D: ADDITIONAL INSIGHTS

The use of the PRA model provides analysts with the following additional insights. The first one concerns the identification of accident management strategies. PRA information can be extrapolated from the model and provided to analysts to identify the available possible mitigating strategies. For example, identification of the event tree sequences that *do not* lead to the accident can help with determining how best to get onto one of these sequences, thus identifying a set of potential mitigating strategies. Such strategies then would form the set of decisions to be evaluated through the decision analysis part of the approach.

Finally, we would like to remark that one can obtain information about what systems and components are most important to the prevention of the accident. One can elicit this information in a variety of ways from the PRA model. One can look at the dominating cut sets, or could focus on the importance measures such as Fussell-Vesely, or Risk Achievement Worth or the Differential Importance Measure [Borgonovo and Apostolakis (2001)].

STEP 3: IDENTIFICATION OF ACCIDENT MANAGEMENT STRATEGIES

This step is devoted to identifying the decisions made during the precursor, the alternatives available to the on-site decision maker at each decision point, and the corresponding trade-offs. In so doing, one benefits from the result of the precursor event analysis (Step 1) and of the PRA analysis (Step 2), as follows.

- STEP 3A: IDENTIFICATION OF THE STRATEGIES ADOPTED DURING THE INCIDENT

From the examination of the incident (Step 1), one can reconstruct the mitigating strategies that have been adopted during the precursor. In particular, one can identify the points in the event at which a strategy was selected and a certain course of action started. Not only, but analyzing analyzing the evolution of the event also allows to of what alternative were available to the on-site decision makers and to study of the trade-offs connected with the available strategies.

- STEP 3B: IDENTIFICATION OF ALTERNATIVE MITIGATING STRATEGIES THROUGH THE PRA MODEL

Since the basis of the PRA is an accurate technical description of the plant, the PRA analysis can be implemented so as to understand what equipment/system structure and components must intervene in order to

end the incident progression. Information of Step 2 can be viewed also from the prospective that discretization is equivalent to following the evolution of the precursor through the PRA model. It is possible then to highlight how the plant (and operators at the plant) *effectively* proceeds from left to right across the relevant ET (Figure 2), and therefore identify the equipment involved in the sequence and understand what alternative strategies were available to the on-site decision makers. The results of this analysis overlap and integrate the results of Step 1 conducted on the basis of the available documentation.

Once the available alternatives have been identified, the next task is then to understand whether the actions chosen by the on-site decision maker maximize the same objectives as the ex-post decision maker's ones. To do so, one needs to explicitly evaluate such decisions. As this is not possible via the PRA model, one needs to build a dedicated decision analysis model. This is accomplished in the next step.

STEP 4: IMPLEMENTATION OF THE DECISION ANALYSIS MODEL

As discussed in Section 2, to evaluate the decisions taken during a precursor event, one needs to create a decision analysis model. Core of the method is the building of the ID representing the sequential decisions and the random events involved in the incident. ID's are oriented graphs composed by nodes and arcs [Bielza and Shenoy (1999)]. The main advantage of ID's is their ability in synthesizing all the aspects of a decision analysis problem[6]. In the creation of the model, it useful to regard IDs as composed of three levels as defined in Jae et al (1992) or Bielza and Shenoy (1999). The first level is named graphical. At this level, an ID is regarded as a "*directed acyclic graph* [Bielza and Shenoy (1999)]" composed of arcs and nodes. Nodes can be of three types: chance nodes, decision nodes and value nodes [Schachter (1986)]. Arcs can have a different meaning. Arcs into utility and chance nodes refer to probabilistic dependence, arcs into decision nodes portrait the state of information. Once all the events and decisions involved in the model and their dependencies have been displayed, the structure of the conditional distribution of the node is assigned and constitutes the functional level. The assignment of values to the conditional probabilities and utilities takes place at the numerical level.

[6]In this respect, see the use of ID's in Cox et al. (2003) to represents the complex relationships at the basis of a generic methodology for representing beliefs about chemical hazards.

We now explore how the three levels (graphical, functional and numerical) are "filled in" in the case of a precursor analysis. As we are to show, this happens through of integration of the results of Steps 1, 2 and 3.

At the graphical level, one completes the elements of the model, namely:

- *Decision Node(s):* decision nodes represent the choice of a mitigating strategy or a course of action made during the precursor. The number of decision nodes and what alternatives/mitigating strategies they include is a result of Steps 1, 2 and 3.
- *Chance Nodes:* in the model, chance nodes represent the random events involved in the incident. Chance nodes are determined by Steps 1 and 2. However, it is useful to distinguish two groups of chance nodes. The first group entails chance nodes directly included in the PRA. Typically, these nodes represent random events related to equipment or operator actions that must perform during the event in order for a mitigating strategy to work. PRA analysis (Step 2) is then used to specify outcomes of nodes involving systems structures and components (Table 3). In addition, one can extract information on the consequences (core damage/Large Early Release) connected to a selected strategy (Table 3). The second group entails events that happened during the precursor but are not included in the PRA model. To this group belong events involving those equipment that, as Cheok *et al* (1998) point out, "*do not necessarily appear in the final quantified model, either because they have been screened initially, assumed inherently reliable or have been truncated in the solution of the model*."
- *Value node*: The last node (named value node) contains the decision maker utility for each consequence and is the terminal node of the model.

After the implementation of the graphical level of the ID, the functional and numerical level determination, i.e., the specification of the chance node outcomes and the corresponding probability assignment can be completed. For nodes with a correspondent in the PRA, the distributions are directly assessed by the PRA analysis. Equipment failure probabilities are results of the PRA calculation, as well as the probability of core damage, which is namely the CCDP. For nodes out of the PRA scope, probabilities can be derived from other sources. For instance, for random events associated with operator performance, the corresponding probabilities are

computed through an associated model (e.g., SPAR-H [Gertman et al. (2005)], NRC (1998), and Pyy's human decision method [Pyy (2000)]).

At the numerical level, the determination of the decision maker utility for consequences deserves a further digression. As mentioned, by ex-post decision maker we mean the person/institution that is analyzing and evaluating the decision making aspects of the precursor event. For example, the ex-post decision maker can be a regulatory body, the plant owner or an industry body. As discussed in the introduction of this section, the objectives of the decision maker, namely Her/His values, determine the attributes in the utility function. Such utility is, in the most general setting, a non-linear multi-attribute utility function, reflecting the decision tradeoffs (for instance, economic damage and protection of public safety). We refer to Keeney (1980) for the theoretical analysis of the problem of defining a multi-attribute utility function for a regulatory body. An industry decision maker would create a utility function reflecting Her/His values and objectives. In general, a multi-attribute utility function needs to be specified. We refer to Keeney and Raiffa (1993) for the theory of multi-attribute utility functions (see also Kreps (1988) for a review of Utility Theory).

STEP 5: EVALUATION OF THE ALTERNATIVES AND BEST STRATEGY DETERMINATION

Once all probabilities and utilities have been inserted in the model, the next step is the evaluation of the alternatives and the identification of the preferred strategy. Algorithms for the solution of influence diagrams are proposed in Schachter (1986). In our approach, the ID is next implemented on a decision support software and the corresponding DT is obtained and evaluated. DT's are the representation of a decision analysis problem that reveals the entire combination of outcomes and alternatives. Their main advantage is the simplicity of solution, while the principal limitation is connected to their size: it grows exponentially with the number of nodes. Clemen (1997) describes the roll-back technique for the solution of decision trees [see also Raiffa (1968)]. We note these procedures are implemented on standard decision analysis software that can be used in conjunction with the PRA one [see references TreeagePro and Winston (1998)].

STEP 6: SENSITIVITY ANALYSIS

Paralleling the steps in Clemen (1997), we include a step in the methodology for sensitivity analysis. Besides the general motivation that "*any effective decision analysis must include a thorough sensitivity analysis* … [Ringuest (1997),]"[7] there is a compelling reason to perform sensitivity analysis in evaluating the decision making aspects of precursor events. After obtaining the best strategy, the analyst ought to further explore the model, in order to derive insights on the stability of such a strategy with respect to "*imprecision* [Ringuest (1997)]" or uncertainty in the input parameters (sometimes this is called epistemic uncertainty or parameter uncertainty). As discussed in Ringuest (1997) "*a decision is considered insensitive if the probabilities … required for any other alternative to become preferred are not close to the original probabilities.*" Suppose that the analyst finds out that the optimal incident management strategy She/He derives from the decision analysis model is relevantly different from the one adopted by the actors. In such a case, it is important to corroborate the result and understand whether a small deviation of the inputs from their base case value is enough to cause the optimal policy to change.

As Ringuest (1997) discusses, a first way to obtain this type of information is to apply the so-called break-even analysis (the reader is referred to Frey and Patil (2002) and Patil and Frey (2004) for a thorough presentation of break even analysis). This type of sensitivity is usually available in standard decision analysis software.

A second way to inspect the stability of a strategy is to make use of the so-called strategy selection frequency diagram. At the basis of the diagram is a Monte Carlo input propagation. The preferred strategy corresponding to each input generation is registered. With a strategy-selection frequency diagram, an analyst gains information on how many times a strategy is selected over the possible combinations of the decision analysis model input values. Thus, if a strategy is always selected, one can consider the strategy stable in the sense of Ringuest (1997). We further refer to [Ringuest (1997)] for a review of more sophisticated sensitivity analysis methods

[7]About the relevance of sensitivity analysis in model creation and corroboration, we refer to Frey (2002), Frey and Patil (2002), Saltelli (2002), and Saltelli *et al.* (2000).

that address the problem of stability in decision making models to the choice of probability estimates and utility functions for single and multi-attribute problems.

STEP 7: INSIGHTS DERIVATION

The last step of the method is to derive/summarize the results of Steps 1-6 to provide insights on: i) what to focus in order to understand the motivation behind the on-site decision maker actions; and ii) what questions to ask in order to reconstruct what happened during the incident. In fact, one can lean on the structure of the methodology to show which element of the decision making process (alternatives, random events, probabilities, objectives) is the source of an eventual discrepancy.

- *Strategies*: one can formulate questions to the actors so as to understand whether all the accident management strategies revealed by the ex-post analysis were indeed envisioned by the on site decision makers. In that case, one can refer to the discrepancy as strategy overlooking.
- *Random Events*: the integration of the decision analysis and the PRA serves to make systematic the discussion of the random events involved in the incident. In the case that some of the random events have not been taken into consideration, we talk about event overlooking.
- *Probabilities*: The formulation of questions on the subjective view of random event probabilities perceived by the operators during the incident explains discrepancies in the actions taken, if disagreements between the ex-post decision makers' and the on-site decision makers' view of such probabilities emerge. In such a case, one can talk of subjective probability disagreement.
- *Objectives*: one can formulate questions so as to envision what were the objectives of the on-site decision makers when choosing one of the available mitigating strategies. Discrepancies with the ex-post decision maker's values and objectives can be the explanation to the choice of different courses of action during the precursor.

We wish to mention that the above list does not claim to be exhaustive, but has the purpose of exemplifying how the formal decision analysis process can help in the investigation of what happened during the precursor and in the explanation of the on-site decision maker actions and choices.

3 IMPLEMENTATION OF THE METHODOLOGY TO THE ANALYSIS OF THE PRECURSOR EVENT AT THE DAVIS-BESSE POWER STATION (1985)

To demonstrate the methodology, we use an actual precursor. The precursor event is the loss of main feedwater at the Davis-Besse station [NRC (1985)]. In studying the precursor, we follow the steps introduced in Section 2 (Figure 1).

STEP 1: PRECURSOR EVENT ANALYSIS RESULTS

The sequence of events involved in the incident is presented in Table 4. At 1:35 in the morning, while the plant was at 90% of full power, the first of two steam-driven main feedwater (MFW) pumps experienced an over-speed event, causing the pump to stop. Shortly after (approximately 1/2 min), the main steam isolation valves (MSIV) closed, which affected the other pump, MFW-2. At this same time, the plant scrammed. Over the course of the next 4-1/2 min, MFW-2 coasted down, providing the sole source of feedwater flow to the steam generators. With the main feedwater tapering off, it would have only been a matter of minutes before the auxiliary feedwater (AFW) system would have actuated automatically based upon a signal from the plant safety control system. At about 6 minutes after the loss of the first main feedwater pump, MFW-1, the secondary-side reactor operator (RO2) received permission from the person in charge of the control room, the shift supervisor (SRO1), to actuate AFW before the safety control system performed the actuation. This step was requested on the part of RO2 in order to preserve water inventory in the steam generators. Unfortunately, after going to the control panel (in the control room) to actuate the system, the operator incorrectly *isolated* the AFW system. At this point (6 minutes into the scenario), the plant had lost all feedwater to both steam generators.

After 1/2 min, the AFW pumps tripped due to the system isolation. The operators were now aware that a very serious situation existed. Two-and-a-half minutes later, the steam generators boiled (essentially) dry. A total time of only 9 minutes had elapsed from the loss of one MFW pump to boiling both steam generators dry.

At the time 9 minutes, SRO1 sent two groups of two equipment operators into the plant to restore the AFW system. They had to perform two actions: (1) restore the AFW isolation valves, which were locked valves in

locked rooms three levels below the control room; and (2) restart the AFW pumps, via restoring tripped throttle valves to their original position.

After a total of 16 minutes from the start of the scenario, and after the steam generators had been "dry" for five minutes, both SRO2 and RO2 suggested to SRO1 that feed-and-bleed (F&B) cooling had to be initiated. The plant technical specification called for F&B cooling to be started at this point. The SRO1 decided to continue attempts to restore AFW even though he understood that if he waited too long, even F&B cooling would not be able to adequately cool the primary system resulting in a possible core fuel melt. But, after additional three minutes, the AFW pumps were realigned and successfully started, thereby injecting cooling water into the steam generators. The AFW system continued to operate, thereby ending the scenario.

STEP 2: PRA ANALYSIS RESULTS

We now illustrate the results of the PRA analysis of the precursor example[8], with reference to Steps 2.A, 2.B and 2.C.

We start showing that, utilizing the corresponding ET of the PRA model, it is possible to follow the accident sequence highlighting how the plant (and operators at the plant) *effectively* proceeds from left to right across the loss of MFW ET (Figure 2) – Step 2.A –. This illustration is shown in Figure 2 with the closure of the MSIVs. At that point, the plant is (and effectively was) experiencing a loss of MFW initiating event and is at the starting node of the ET shown in Figure 2. As the incident continues, the secondary-side reactor operator attempted to start the AFW system (at time 6 min), but in fact isolated the AFW. Consequently, at a time of 6 minutes, in Figure 2, one follows the down branch under the AFW ET top event (node "L") representing failure of the AFW. Recall that down branches in an ET represent failure of the system at that node. Continuing on in the precursor event sequence, at a time of 9 minutes, one reaches the point where the senior reactor operator had to make the decision of whether to proceed to feed-and-bleed cooling or continue trying to restore the inoperable

[8]For the purpose of illustrating the methodology the model that was used was the publicly available Surry NUREG-1150 model developed for the US Nuclear Regulatory Commission as part of the NPP Severe Accident Risk program [Bertucio et al (1990)]. This model was implemented in the SAPHIRE software [Russell et al. (1999)].

AFW pumps. At this node on the ET, we do not proceed since feed-and-bleed cooling had not been called for in the Davis-Besse-85 precursor (indeed, it did not either fail or succeed). Read through the PRA model, the decision to restore AFW signals that the senior reactor operator effectively attempted to interrupt the present sequence and to end up on a different sequence not resulting in core damage. As a result of the analysis, eight relevant configurations are identified. These configurations are summarized in Table 5.

After the discretization and identification of each plant state over time, each state must be evaluated using the PRA model (Step 2.B.) To perform this step, the plant state during a particular configuration must be "mapped" into the PRA model. This mapping process requires the identification of specific basic events in the PRA that are impacted in any way by the component degradations or initiating events that occur at the start of the configuration. The relevant basic events for each of the configurations for the Davis-Besse-85 precursor have been identified and adjusted appropriately for each configuration. During this step, the need to reproduce real events that happened during the sequence has required additional modeling efforts and the use of surrogate components.[9] For each configuration (Step 2.C), we have utilized SAPHIRE to resolve the PRA by regenerating the overall core damage minimal cut sets using the new basic event data. A summary result of the PRA CCDP calculation is shown in Figure 3. Let us analyze in greater detail results for the next three configurations (2, 3, and 4, respectively). Figure 3 shows that the risk (as measured by the CCDP) is increasing as the event evolves. This increasing risk is due to the fact that, as the accident progresses, additional component failures or other complications are resulting in changes to the plant state.

- **STEP 3: AVAILABLE MITIGATING STRATEGIES IDENTIFICATION**

Steps 1 and 2 provide us with all the elements to come to the identification of alternatives. We have seen that the first course of action has been selected at a time of around 6 minutes in the precursor event sequence. The PRA

[9]For example, the modeling of the single-train failure of the MFW system for the first one-half minute of the incident is important to the CCDP calculation in this time period. Adjustments to the PRA model have been necessary to account for the fact that, initially, MFW pump 1 was failed while pump 2 continued to operate.

analysis has lead to the determination that the alternatives faced by the operating crew at t=6 min were either to wait for the AFW automatic actuation or to manually actuate AFW via an instrument panel in the control room (Table 6). The tradeoffs of this decision are as follows. Manual actuation of AFW, if successful, would gain a few minutes of extra time compared with waiting for automatic actuation. However, an error in actuation of AFW may cause the plant to proceed one step further in the accident sequence (Figure 2). From the event description, it emerges that one element taken into consideration by the operators was certainly the time to core damage.

A second decision problem was faced by the operators later during the precursor, at t=9 min, when the plant entered Configuration 6, after AFW isolation. If we return to the PRA model conditional upon this configuration, we can determine the alternatives available to the operating crew. The alternatives are (and were) either to wait for restoration of the AFW system or to initiate F&B cooling. The tradeoffs of this decision are (and were) as follows. Hesitation in going to F&B could turn the incident into an accident (with its economic and safety losses). On the other hand, if the AFW turns out to be available, the operators would be able to bring the plant to a safe shutdown without further economic losses. In that case, going to F&B cooling would unnecessarily expose the plant to an economic loss and cause an extended plant shutdown.

STEP 4: THE DECISION ANALYSIS MODEL

From the analysis of the precursor event (Step 1), the corresponding PRA analysis (Step 2) and the alternatives identification (Step 3) we have all the elements to build the graphical level of the decision analysis model.

The resulting ID is displayed in Figure 4. Figure 4 shows the connections between the two time periods leading to the representation of a sequential decision making problem that is typical of event incidents. We note that the discretization reproduces the configuration study performed in the PRA analyses (Step 2). Table 6 offers a summary of the nodes of the Davis-Besse-85 precursor ID of Figure 4.

Let us now describe the graphical level of the ID in detail.

Decision Nodes: As per the results of Step 3, two decision nodes are needed (Figure 4, Table 6). In fact, the decision making problem can be formulated in terms of a first decision to be taken at around t=6 min from the

beginning of the precursor and a second decision at t=9 min. The informational arc between the two nodes symbolizes the fact that the second decision is made with the decision maker aware of the results of the first decision.

Chance Nodes: let us start with nodes OA6 and OA9. Each of the alternatives at t=6 or 9 min involves an operator action. We denote these operator actions through the "OA6" and "OA9" nodes in Figure 4. As an example, node OA6 represents the event "The operators will perform correctly the required actions given the strategy chosen at t=6 min." If the strategy is to manually actuate AFW, then the success or failure of the operators to perform their tasks influences the status of the AFW. In the actual precursor, isolation of AFW resulted. The AFW6 chance node represents the event "The AFW system functions." We note that the AFW6 outcomes are related on the one hand to the specific incident situation (the operators indeed disabled it) and the stochastic behavior of the system components (e.g., turbine-driven pump failure to start). These elements have to be considered in the calculation of the AFW6 non-actuation conditional probabilities.

Continuing in the ID of Figure 4, the next chance node refers to the level of water in the secondary coolant system. In fact, the coolant inventory (represented by node "SecInv6") affects the potential for core damage. We note that incorrect diagnosis or monitoring of this level may affect decisions later in the scenario. This possibility is represented by the "DiagLev6" chance node. The informational arc connecting node "DiagLev6" to the decision node "Wait or F&B" represents the fact that the next decision depends on the decision maker information on the coolant inventory level. This decision is to be taken in the case the AFW is not working. We note that waiting for restoration of AFW may jeopardize the chance of successful F&B. Nodes CD6 and CD9 represent the events "core damage between 6 and 9 min" and "core damage after 9 min" respectively.

In terms of events contained in the PRA model, nodes AWF6, AFW9, CD6, and CD9 in the ID come directly from the PRA (Figure 4.) Nodes OA6, OA9, DiagLev6, represent random events associated with human actions.

Value Node: For our trial study, we consider safety maximization as the Decision maker objective. We utilize then a single attribute function [U(c)] defined as:

$$U(c) = \begin{cases} -1 & \text{if core damage is reached} \\ 1 & \text{otherwise} \end{cases} \quad (1)$$

U(c) assigns minimum utility to any strategy leading to core damage, as the end nodes of the DT are binary, with one branch corresponding to core damage and another corresponding to no core damage.

Figure 4 displays the graphical level of the ID. At the functional level decision alternatives and chance event node outcomes and the corresponding conditional distribution assignments are stated. To represent all of the potential resulting sequences it is possible[10] to obtain a DT which reveals the functional level of the ID[11].

The numerical level of the ID consists in the assignment of probabilities and the numerical values of utilities. Values for the probabilities of nodes AWF6, AFW9, CD6, and CD9 are directly fed into the ID from the PRA model. In particular, the probabilities for nodes CD6 and CD9 are CCDP's, and are the result of a calculation performed through the PRA model. The probabilities of the remaining nodes have been assessed either by means of human reliability databases or programs (when available) or derived from expert opinion. A total of 20 probabilities are supplied as input to the model.

STEP 5: ALTERNATIVE EVALUATION RESULTS

To determine the preferred strategy, the influence diagram has been implemented in the software DataPro [see (TreeagePro)] and has been resolved through the corresponding DT. The numerical resolution of the DT leads to identify the following strategy that maximizes the decision maker utility: Wait for automatic actuation of AFW at t=6 minutes, and go directly to F&B at t=9 minutes.

STEP 6: SENSITIVITY ANALYSIS RESULTS

A thorough sensitivity analysis exercise has been applied to the decision model. Our purpose has been to evaluate the stability of the preferred alternative to uncertainty in the estimation of the probabilities.

---

[10]This operation is allowed by common commercial decision analysis software as DATAPRO (TreeagePro) and @Risk [(Winston (1998).]

[11]For the Davis-Besse-85 precursor the DT corresponding to the ID of Figure 4 contains 1024 branches and its printable size is 22 pages.

We have conducted two types of sensitivity analysis. A series of one-way break even analyses, with the probabilities varying in their assigned ranges. No strategy reversals were registered. To corroborate this finding, we have then obtained a strategy selection frequency diagram letting all probabilities vary between 0 and 1, i.e., we have inspected the whole input parameter space. The result is illustrated in Figure 5. Figure 5 shows that for all combinations of the probability values, the strategy that maximizes the expected utility at t=6 min is wait, followed at t=9 min by going to F&B, and we can conclude that the preferred strategy is stable in respect of imprecision/uncertainty in the estimation of the input probabilities.

STEP 7: INSIGHTS

We are now left with the comparison of the model results with the actual decisions/actions taken by the on-site decision makers during the incident. From Steps 5 and 6 of the analysis of our example, we have seen that the best course of action for a decision maker possessing the utility function of eq. (1) is to wait at t=6 min, followed by F&B at t=9 min. However, the on-site decision maker's selected strategy was indeed opposite to the estimated best one. Instead of waiting for automatic actuation at 6 minutes, the secondary operator attempted to initiate AFW. Later during the incident, the decision maker decided not to pursue F&B but to wait for restoration of AFW. These discrepancies raise the question as to what is the cause of the different choice. In Section 2, Step 7, we have proposed a list of items that can help drive the investigation.

- *Strategies*: as far as the available strategies are concerned, one can state that there was no strategy overlooking (see Section 2, Step 7.) This is a consequence of the fact that the strategies in this precursor are dictated mainly by technical constraints. Thus, the mitigating strategies envisioned ex-post and available on-site coincide. It is, however, evident from the incident descriptions, obtained by interviewing the operators at the plant at the time of the incident, that the decision to manually actuate AFW was taken in order to "buy time" with respect to coolant inventory [NRC (1985)].
- *Random Events and Probabilities*: Given the last statement of the above item, it is possible that the on-site decision maker did not consider the potential for human error while initiating AFW. Hence, a first source of discrepancy is event overlooking. To actually infer that the operators did not consider at all the possibility of

human error, one would need to interview the players formulating ad hoc questions. Alternatively, if the operators did account for this possibility, they may have trivialized the probability that the AFW system could in fact be isolated.

- *Objectives*: As far as the objectives are concerned, from the analysis of the actual facts and interviews taken at the time of the incident [NRC (1985),] it appears that the main objective of the decision makers was to enhance plant safety.

Unfortunately, since the event occurred over 20 years ago, it is impossible to interview the players of the incident. As mentioned, it is not the purpose of this method to make a judgment on whether the decisions taken were “good” or “bad”, but to provide insights regarding on what to focus to understand the motivation behind such decisions. The scope of the present analysis has been to illustrate the methodology. The results of the specific example may be of interest for the analysis of similar happenings, but they are not necessarily extendable. Current practices vary among industries and evolve with time. For example, the decision of manually actuate F&B in the nuclear realm could be seen as exceeding technical specifications. The nuclear industry has implemented very severe restrictions against such violations since the DB-1985 incident. What can be repeated is, of course, the analysis procedure. In particular, the above findings show that the utilization of decision analysis models together with PRA enables a methodological reconstruction of the decision analysis aspects of precursor events, which cannot be achieved solely by the risk analysis supporting the CCDP calculation. It is this feature, the examination of decisions, that marks this methodology’s addition to current applications of precursor analyses.

4 CONCLUSIONS

This work has proposed a methodology for the analysis of precursor events in consideration of both their risk analysis and decision making aspects. At the core of the methodology is the joint utilization of tools both in the PRA and the decision analysis realms, with the creation of an ID and/or the corresponding DT that synthesizes results of the PRA analysis and decision making aspects of the problem. PRA analysis feeds into the ID and DT at various levels by determining points in time and plant configurations at which choices among alternatives

(mitigating strategies) were made. The decision analysis model allows a rigorous inclusion and evaluation of plant states, system structures and components involved in the accident sequence, their configurations, and consequences of their eventual failure.

We have seen that to utilize the PRA model to evaluate precursors in decision-space requires several innovative elements with respect to the current practice. In particular, one must "follow" the accident sequence on the corresponding event tree, reevaluating the model in correspondence to the evolution of the accident, similarly to what is done in risk monitors at NPPs. A further advantage of the synthesis of the PRA information with the decision analysis model is the incorporation in the ID, and therefore in the analysis, of aspects not included in the PRA. On the other hand, the PRA model appears to be well suited for aiding in identifying and quantifying alternative mitigating strategies and for indicating when, in a sequence of unfavorable events, critical decisions are to be made.

The methodology offers the possibility of quantitatively evaluating the decision making process from different perspectives, by specifying an appropriate utility function containing attributes and objectives corresponding to the perspective of the ex-post decision maker.

We have presented the methodology as split into seven steps. We have illustrated their application through the analysis of a precursor event that happened at the Davis-Besse power plant in 1985. We have described the results of the event risk analysis, following the precursor via PRA model. From the PRA analysis and of the analysis of the precursor event, we have illustrated the implementation of the corresponding decision analysis model. We have illustrated the link between the PRA model to the ID. More technically, we have analyzed, for each level of the ID, what information flows from the PRA to the ID. After completing the three levels of the ID, we have evaluated the preferred mitigating strategies from the perspective of a decision maker characterized by a single attribute utility function over the event consequences. We have then illustrated the last step of the method. Namely, we have illustrated what relevant questions emerge from analysis of the precursor event in terms of: *i)* determination of the alternative mitigating strategies the on-site decision makers envisioned at the moment of the accident and whether or not different strategies were viable; *ii)* determination of whether the on-

site decision makers underwent an event overlooking – for the Davis-Besse-85 precursor, it appears as if the on-site decision makers overlooked the event of an operator error while actuating auxiliary feedwater; - *iii)* analysis of the risk view of the on-site decision makers in terms of perception of the event probabilities based on the available information during the accident; iv) comparison of the on-site decision makers objectives and ex-post decision maker's ones. These results closely follow the NRC staff's conclusions related to the event -- for example they noted the need to have short-term actions related to the "adequacy of emergency procedures, operator training and available plant monitoring systems for determining need to initiate feed-and-bleed cooling following loss of steam generator heat sink." [NRC, 2005]

The results of our analysis allow us to conclude that PRA coupled with IDs or DTs can be used successfully to model decisions, events, and dependencies during precursor incidents. In addition, use of formal decision-analysis tools leads to a systematic analysis approach that grants an improvement over an analysis that is based solely on physical aspects of the situation or on simple engineering judgment.

Acknowledgments. The authors wish to thank the anonymous referees for very insightful and careful comments that have greatly contributed to the realization of this manuscript.

5 REFERENCES

[Bertucio et al (1990)] Bertucio, R. C. and J. A. Julius, 1990: "Analysis of Core Damage Frequency: Surry, Unit 1 Internal Events," *NUREG/CR-4550*, SAND86-2084, Volume 3, Revision 1, Parts 1 and 2, April 1990.

[Bielza and Shenoy (1999)] Bielza C. and Shenoy P.P., 1999: "A Comparison of Graphical Techniques for Asymmetric Decision Problems," *Management Science*, 4511, pp. 1552-1569.

[Bieder et al. (1998)] Bieder, C., Le Bot, P., Desmares, E., Bonnet, J.-L., Cara, F., 1998: "MERMOS: EDF's New Advanced HRA Method," PSAM 4, New York, pp. 129–134, Springer-Verlag, London, 1998.

[Borgonovo and Apostolakis (2001)] Borgonovo E. and Apostolakis G.E., 2001: "A new importance measure for risk-informed decision making," *Reliability Engineering & System Safety*, 72 (2), pp. 193-212.

[Carroll (2004)] Carroll J.S., 2004: “Knowledge management in High-Hazard Industries,” in *Accident Precursor Analysis and Management*, Phimister J.R., Bier V.M. and Kunreuter H.C. (Eds.), The National Academic Press, Washington D.C., USA, ISBN 0-309-092167.

[Cheok et al (1998)] Cheok M.C., Parry G.W., and Sherry, R.R., 1998: "Use of Importance Measures in Risk-Informed Regulatory Applications," *Reliability Engineering and System Safety*, 60, pp. 213-226.

[Clemen (1997)] Clemen R.T., 1997: “Making Hard Decisions: An Introduction to decision analysis,” II Edition, *Duxbury Press*, Pacific Grove, Calif, USA; ISBN 0534260349.

[Connell (2004)] Connell L. J., 2004: “Cross-Industry Application of a Confidential Reporting Model,” in *Accident Precursor Analysis and Management*, Phimister J.R., Bier V.M. and Kunreuter H.C. (Eds.), The National Academic Press, Washington D.C., USA, ISBN 0-309-092167.

[Covaliu et al. (1995)] Covaliu Z. and Oliver R.M., 1995, “Representation and Solution of Decision Problems Using Sequential Decision Diagrams,” *Management Science*, 41 (12), pp. 1860-1881.

[Cox et al. (2003)] Cox P., Niewöhner J., Pidgeon N., Gerrard S., Fishoff B. and Riley D., 2003: “The use of Mental Models in Chemical Risk Protection: Developing a Generic Workplace Methodology,” *Risk Analysis*, 23 (2), pp. 311-324.

[Frey (2002] Frey C. H., 2002: "Introduction to Special Section on Sensitivity Analysis and Summary of NCSU/USDA Workshop on Sensitivity Analysis," Risk Analysis, 22 (3), pp. 539-545.

[Frey and Patil (2002)] Frey C. H. and Patil S.R., 2002: "Identification and Review of Sensitivity Analysis Methods," *Risk Analysis*, 22 (3), pp. 553-571.

[Gertman et al. (2005)] Gertman D., Blackman H., Marble J., Byers J., Haney L. and Smith C., 2005: “The SPAR-H Human Reliability Analysis Method,” *NUREG/CR-6883*, August 2005.

[Hart (2004)] Hart C.A., 2004: “Stock on a Plateau: A Common Problem,” in *Accident Precursor Analysis and Management*, Phimister J.R., Bier V.M. and Kunreuter H.C. (Eds.), The National Academic Press, Washington D.C., USA, ISBN 0-309-092167.

[Jae and Apostolakis (1992)] Jae M. and Apostolakis G.E., 1992: “The Use of Influence Diagrams for Evaluating Severe Accident Management Strategies,” *Nuclear Technology*, 99:142–157.

[Jae et al. (1993)] Jae M., Milici A. D., Kastenberg W. E. and Apostolakis G. E., 1993: “Sensitivity and Uncertainty Analysis of Accident Management Strategies Involving Multiple Decisions,” *Nuclear Technology*, 104, 13-35.

[Keeney (1980)] Keeney R.L., 1980: “Utility Functions for Equity and Public Risk,” *Management Science*, 26 (4), pp. 345-353.

[Keeney and Raiffa (1993)] Keeney R. and Raiffa H., 1993: "Decisions with Multiple Objectives" *Cambridge University Press*, Cambridge, U.K., ISBN 0-521-43883-7.

[Kleindorfer et al. (2003)] Kleindorfer P. R., Belke J. C., Elliott M. R., Lee K., Lowe R. A., Feldman H. I., 2003: "Accident Epidemiology and the US chemical industry: Accident History and Worst Case Data from RMP Info," *Risk Analysis*, 23 (5), pp. 865-881.

[Kreps (1988)] Kreps D.M., 1988: "Notes on the Theory of Choice," Underground Classics in Economics, *Westview Press Inc.*, Colorado, USA, ISBN 0-88133-7553-3.

[Neil et al (2005)] Neil M., Fenton N. and Tailor, M., 2005: "Using Bayesian networks to model expected and unexpected operational losses," *Risk Analysis*, 25 (4), pp. 963-972.

[NRC (1985)] "Loss of Main and Auxiliary Feedwater Event at the Davis-Besse Plant on June 9, 1985," *NUREG-1154*, US Nuclear Regulatory Commission, Washington, DC, July 1985.

[NRC (1998)] "Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)," *NUREG-1624*, US Nuclear Regulatory Commission, Washington, DC, 1998.

[NRC (2001)] "Status Report on Accident Sequence Precursor Program and Related Initiatives," *SECY-01-0034*, US Nuclear Regulatory Commission, Washington, DC, March 1, 2001.

[NRC (2005)] "A Prioritization of Generic Safety Issues – ISSUE 122: Davis-Besse Loss Of All Feedwater Event Of June 9, 1985 - Short-Term Actions (Rev. 4)," *NUREG-0933*, US Nuclear Regulatory Commission, Washington, DC, June 2005.

[Papazoglou (1999)] Papazoglou, I.A. 1999: "Bayesian decision analysis and reliability certification," *Reliability Engineering and System Safety*, 66 (2), pp. 177-198.

[Patè-Cornell (2004)] Patè-Cornell E., 2004: On signal, Response and Risk Mitigation: A probabilistic Approach to the Detection and Analysis of Precursors," in *Accident Precursor Analysis and Management*, Phimister J.R., Bier V.M. and Kunreuter H.C. (Eds.), The National Academic Press, Washington D.C., USA, ISBN 0-309-092167.

[Patil and Frey (2004)] Patil S.R. and Frey C.H., 2004: "Comparison of Sensitivity Analysis Methods Based on Application to a Food Safety Risk Assessment Model," *Risk Analysis*, 24 (3), pp. 573-585.

[Pratt, Raiffa and Schlaifer (1995)] Pratt J.W., Raiffa H. and Schlaifer R., 1995: "Introduction to Statistical Decision Theory," *The MIT Press*, 904 pages, ISBN 0262161443

[Phimister et al. (2004)] Phimister J.R., Bier V.M. and Kunreuter H.C. (Eds.): "Accident Precursor Analysis and Management," *The National Academic Press*, Washington D.C., USA, ISBN 0-309-092167.

[Pyy (2000)] Pyy, P., 2000: "An approach for assessing human decision reliability," *Reliability Engineering and System Safety*, 68:17–28, 2000.

[Raiffa (1968)] Raiffa H., 1968: "Decision Analysis: Introductory Lectures on Choices under Uncertainty," Random House, New York, NY, USA.

[Ringuest (1997)] Ringuest J.L., 1997: "L_p-metric Sensitivity Analysis for Single and Multi-Attribute Decision-Analysis," European Journal of Operational Research, 98, pp. 563-570.

[Russell et al. (1999)] K.D. Russell, et al., 1999: "Systems Analysis Programs for Hands-on Reliability Evaluations (SAPHIRE) Version 6.0 - System Overview Manual," *NUREG/CR-6532*, May 1999.

[Saltelli et al (2002)] Saltelli A., Tarantola S. and Campolongo F., 2000: "Sensitivity Analysis as an Ingredient of Modeling", *Statistical Science*, 19 (4), pp. 377-395.

[Saltelli (2002)] Saltelli A., 2002: "Sensitivity Analysis for Importance Assessment," *Risk Analysis*, 22 (3), p. 579-590.

[Sattison (2004)] Sattison M.B., 2004: "Nuclear Accident Precursor Assessment: The Accident Sequence Precursor Program," in *Accident Precursor Analysis and Management*, Phimister J.R., Bier V.M. and Kunreuter H.C. (Eds.), The National Academic Press, Washington D.C., USA, ISBN 0-309-092167.

[Schachter (1986)] Schachter R.D., 1986: "Evaluating Influence Diagrams," *Operations Research*, 34 (6), pp. 871-882.

[Schachter (1988)] Shachter R.D., 1988: "Probabilistic Inference and Influence Diagrams," *Operations Research*, 364, pp. 589-604.

[Smith (1998)] Smith, C. L. 1998, "Calculating Conditional Core Damage Probabilities for Nuclear Power Plant Operations," *Reliability Engineering and System Safety*, 59:299–307, 1998.

[Smith et al (1999)] Smith C., Borgonovo E. and Apostolakis G.E., 1999: "Review of International Activities in Accident Management and Decision Making in the Nuclear Industry," Technical Report, MIT-NED-EDF-1999-01, May 1999.

[Shenoy (1992)] Shenoy P.P., 1992: "Valuation-Based Systems for Bayesian decision analysis," *Operations Research*, 403 (May, 1992), pp. 463-484.

[Svenson (1998)] Svenson O., 1998: "A Decision Theoretic Approach to an Accident Sequence: When Feedwater and Auxiliary Feedwater Fail in a Nuclear Power Plant," *Reliability Engineering and System Safety*, 59:243–252, 1998.

[Tamuz (2004)] Tamiz M., 2004: "Understanding Accident Precursors," in *Accident Precursor Analysis and Management*, Phimister J.R., Bier V.M. and Kunreuter H.C. (Eds.), The National Academic Press, Washington D.C., USA, ISBN 0-309-092167

[TreeagePro] TreeAgePro, decision analysis Software by Treeage Software Inc., Williamstown, MA, USA.

[Winston (1998)] Winston W., 1998: "Financial Models Using Simulation and Optimization," *Palisade Editor*, Newfield, NY, USA. Software: @Risk (.palisade.com.)

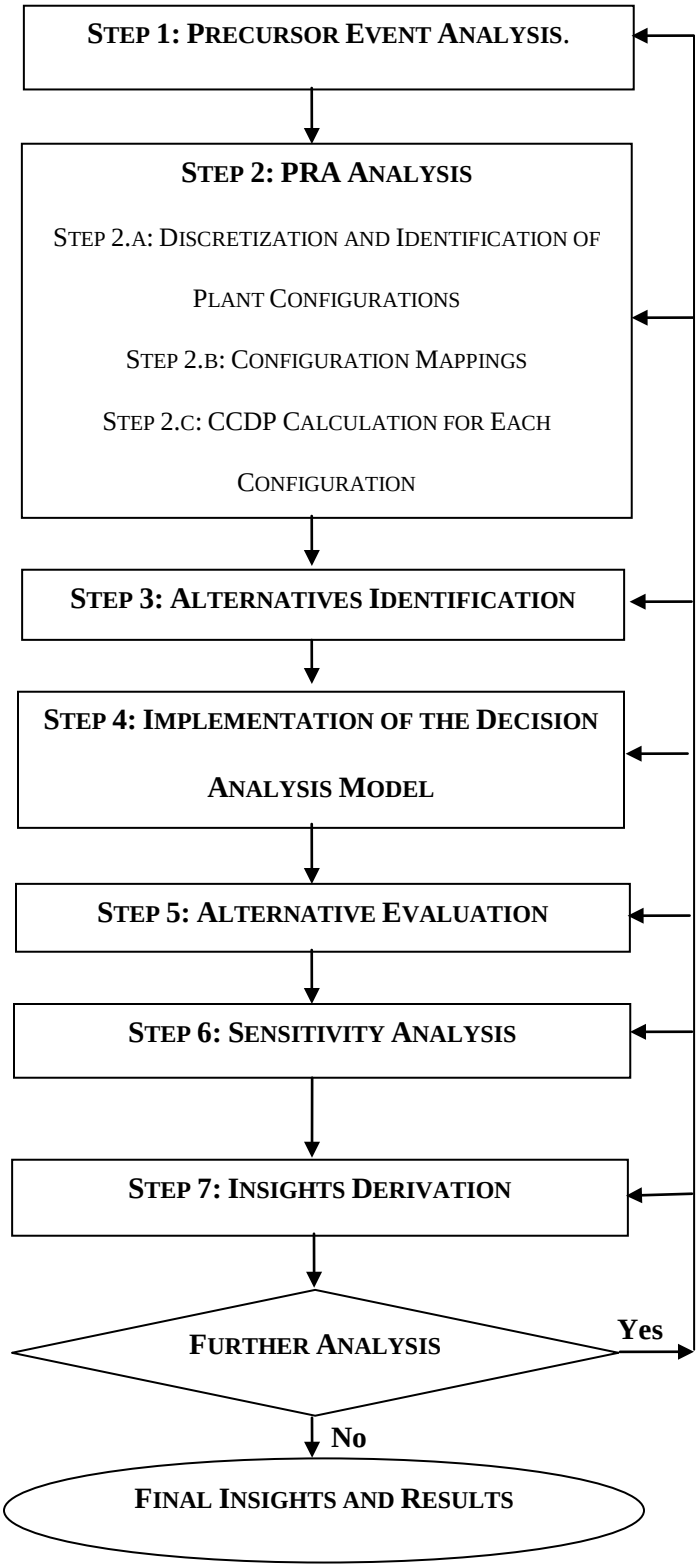

Figure 1: Methodology steps for inclusion of decision making aspects in precursor analysis.

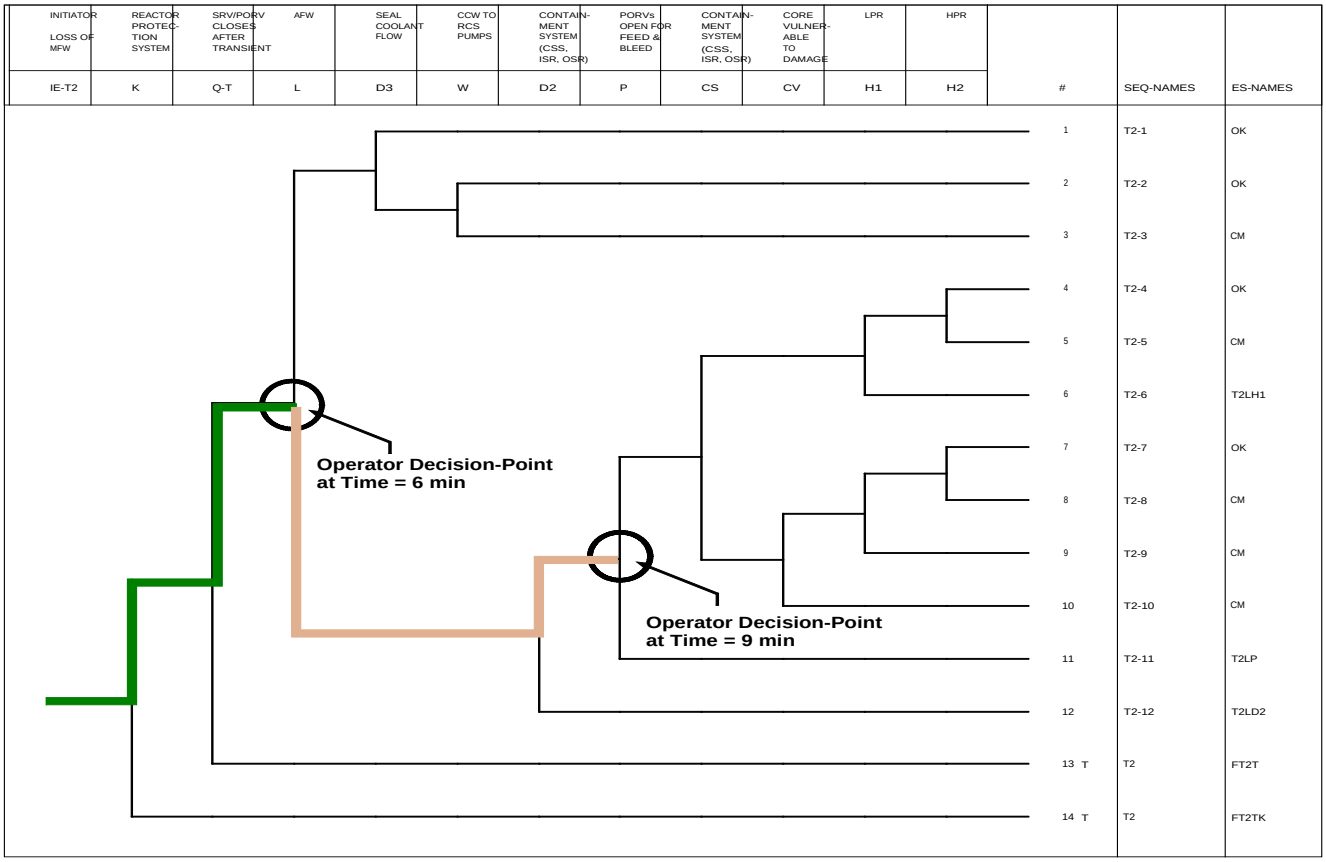

Figure 2: The path followed by the incident as represented in the corresponding sequence of the PRA model. The incident started out as a partial loss of MFW and then turned into a complete loss of MFW.

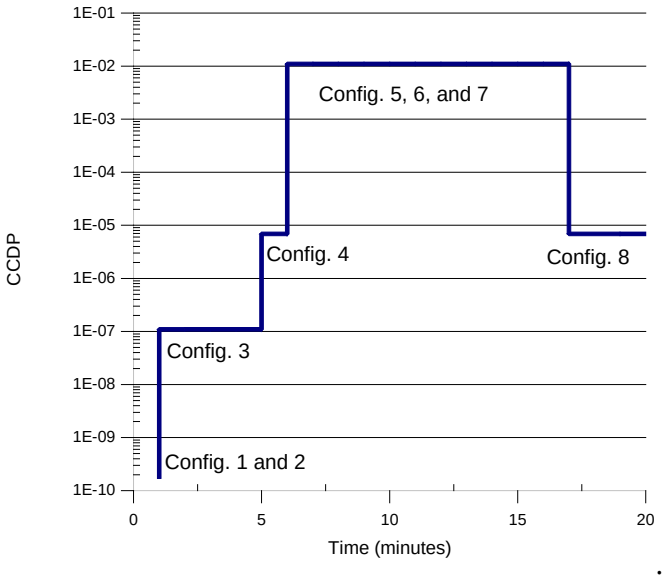

Figure 3: CCDP results for the configurations during the Davis-Besse incident.

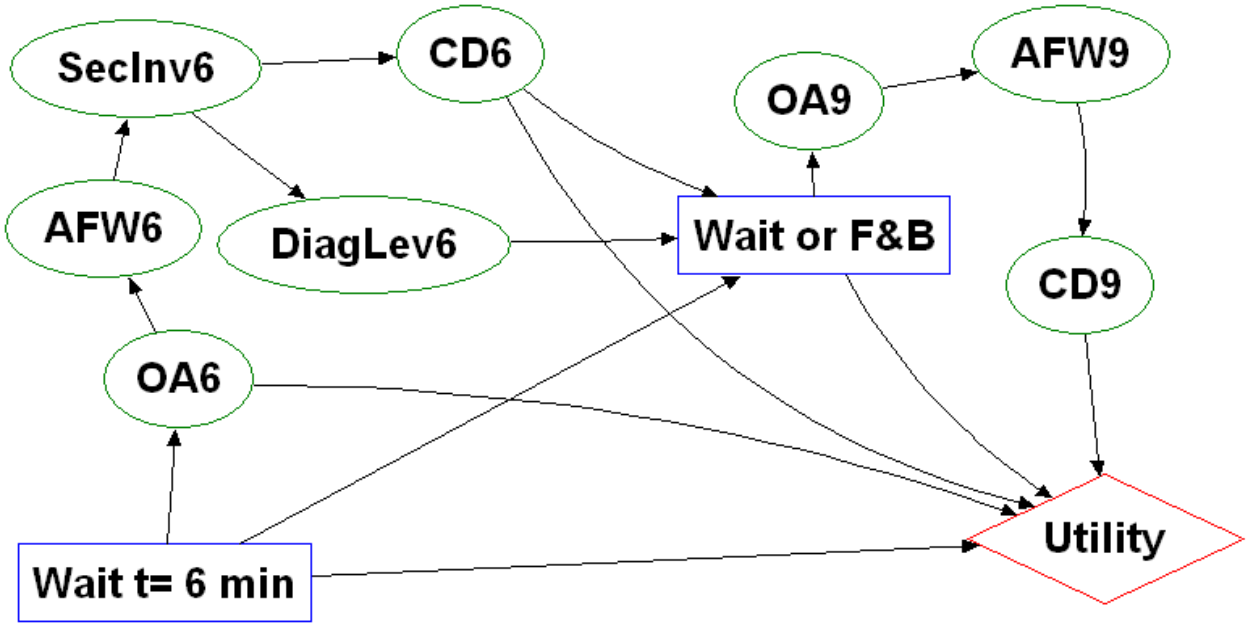

Figure 4: The ID representing the critical decision points in the Davis-Besse precursor incident; nodes AFW6, CD6, AFW9, and CD9 are direct input from the PRA.

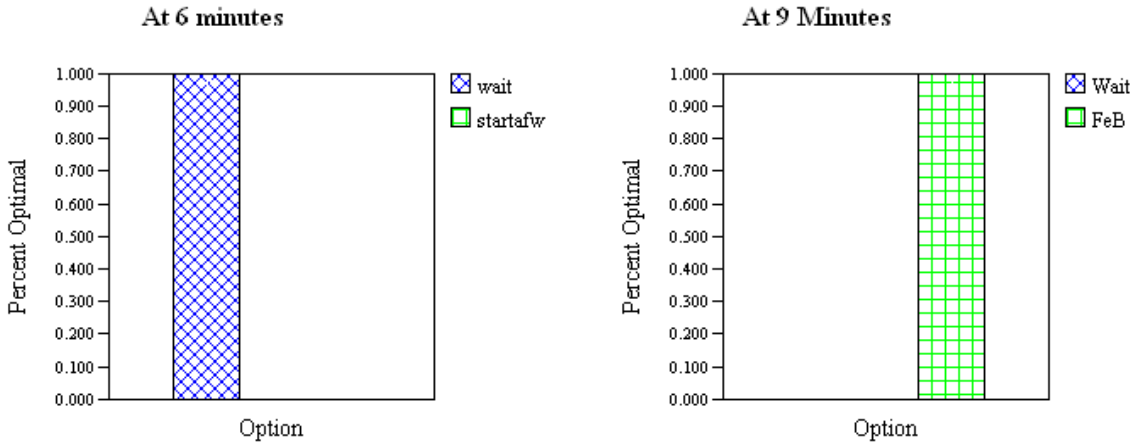

Figure 5: Strategy Selection for any combination of probability values at t=6 and t=9 minutes.

Table 1: List of Acronyms

Acronym	Full name
AWF	Auxiliary Feedwater
CCDP	Conditional Core Damage Probability
DT	Decision Tree
ET	Event Tree
F&B	Feed and Bleed
ID	Influence Diagram
MSIV	Main Steamwater Isolation Valve
NRC	Nuclear Regulatory Commission
NPP	Nuclear Power Plant
PRA	Probabilistic Risk Assessment
RO	Reactor Operator
SRO	Shift Supervisor

Table 2: Events resulting in a CCDP greater than 1E-4 between 1996 and 1997

Incident	Plant	Date	CCDP
Loss of off-site power with emergency diesel generator B unavailable	Catawba 2	2/6/1996	2E-3
Reactor trip with loss of emergency service water train A and turbine-driven auxiliary feedwater pump	Wolf Creek	1/30/1996	2E-4
Potential inadequacy of residual heat removal pump	Haddam Neck	8/1/1996	2E-4

Table 3: PRA elements translate in the Decision Analysis model at the graphical level

PRA	↔	DECISION ANALYSIS MODEL EQUIVALENT
Safety System Failure	↔	Random Event
Equipment Failure	↔	Random Event
Mitigating Strategies	↔	Decision Alternatives
core damage/Large Early Release	↔	Consequence

Table 4**:** Time of actions for the loss of MFW event at Davis-Besse.

Time	**Action**
0.0 min	MFW1 pump trip (the reactor and turbine trip at t = 30 sec)
0.5 min	MSIV closed (MFW2 pump coast down over 4.5 min.)
6.0 min	RO2 incorrectly trips SFRCS (which isolates AFW)
6.5 min	AFW pumps trip on overspeed
7.0 min	RO2 finds error of AFW isolation
7.0 min	RO1 resets SFRCS. Since AFW isolated, it does not reset
7.5 min	RO1 open press. spray, RCS press. Decreases
9.0 min	Both steam generators boil dry
9.0 min	RO1 and SRO1 send equipment operators to restore AFW
11.0 min	RO2 sent RO1 to reset startup feedwater pump, primary PORV opens
16.0 min	RO2 and SRO2 recommend feed-and-bleed be initiated
16.5 min	RO2 starts the startup feedwater pump into steam generator 1
18-20 min	AFW pumps align and begin to function

Table 5: Configurations for Davis-Besse during the loss of MFW precursor.

Configuration	**Time**	**Description**
1	0.0 min	The nominal plant state
2	0.0 min	Loss of MFW1 pump
3	0.5 min	Plant trip and MSIV closed
4	5.0 min	Complete loss of MFW system and plant in tripped state
5	6.0 min	Loss of MFW and isolation of AFW
6	9.0 min	Both steam generators boil dry, still no MFW or AFW
7	16.5 min	Startup feedwater pump injects into steam generator 1, still no MFW or AFW
8	19.0 min	AFW pumps align and begin to function

Table 6: List of nodes and explanation for the Davis-Besse-85 decision analysis model.

Node	Type	Alternatives/Outcomes/Values
Wait t=6 min	Decision	Wait AFW
		Start AFW manually
OA6	Chance Node	Operator error in AFW Actuation
		No operator error in AFW Actuation
AFW6	Chance Node	AFW actuates
		AFW does not start
SecInv6	Chance Node	Secondary level high
		Secondary level low
DiagLevel6	Chance Node	Correct Monitoring of Secondary Inventory level
		Incorrect Monitoring of Secondary Inventory level
CD6	Chance Node	core damage happens before 9 minutes
		No core damage before 9 minutes
Wait or F&B	Decision	Wait for restoration of AFW
		Go to Feed and Bleed (F&B)
OA9	Chance Node	No Operator Error
		Operator Error
AFW9	Chance Node	AFW available after t=9 min
		AFW not available after t=9 min
CD9	Chance Node	Core damage after t=9 min
		No Core Damage after t=9 min
Utility	Value Node	-1 if core damage happens
		1 if no core damage happens