NOTICE

CERTAIN DATA CONTAINED IN THIS DOCUMENT MAY BE DIFFICULT TO READ IN MICROFICHE PRODUCTS.

EGG-M--90142

DE91 001821

APPLICATION OF PROBABILISTIC RISK ASSESSMENT TECHNIQUES DURING DESIGN PHASE FOR DRY STORAGE CASKS[a]

B. P. HALLBERT, D. G. SATTERWHITE, AND B. M. MEALE
Idaho National Engineering Laboratory, EG&G Idaho, Inc., P.O. Box 1625, Idaho Falls, ID 83415

ABSTRACT

Canisters containing Three Mile Island (TMI) spent fuel and debris are being stored in a storage pool at the Idaho National Engineering Laboratory (INEL). In order to store these canisters in dry storage casks, a system is being designed to remove entrained water from the canisters. The conceptual design for this drying process was evaluated in respect to the occurrence of a nuclear criticality. The system design was evaluated to address the mechanical failure of the components. Also, human interfaces with the equipment were assessed. The integration of these two facets resulted in a model that was quantified to calculate the occurrence frequency of a nuclear criticality. Changes to design, administrative guidelines, and procedures were recommended so that an acceptable level of risk based on nuclear criticality occurrence frequency could be achieved.

INTRODUCTION

After the Three Mile Island (TMI) accident, the Idaho National Engineering Laboratory (INEL) was contracted to store TMI spent fuel and debris collected during clean-up activities. The TMI debris was packaged in specially-designed canisters containing various neutron absorbing materials. The maximum activity loading for a canister is approximately 45,000 Ci, producing a maximum radiation field of approximately 1,500 R/hr at 1 cm. Regardless of moderator material, individual canisters are considered criticality safe under worst-case credible conditions due to their internal structure.

The TMI canisters, filled at TMI, were loaded in a special shipping cask that holds seven canisters and peridocially shipped by rail to the INEL. They were remotely removed from the shipping cask in the Test Area North (TAN) Hot Shop and placed in specially-designed storage modules in the TAN Storage Pool. The modules are a six-pack design, fabricated of stainless steel. Each of the six compartments are surrounded by removable strips of polyethylene, each of which is externally clad with Boraflex poison. The poison prevents criticality in the event of a pool-draining accident.

Development of dry casks for long-term storage of TMI spent fuel and debris was recently initiated. From a cost benefit perspective, the conceptual design [1] for the long-term storage casks needed to evaluate safety implications of storing TMI canisters without installing neutron poison spacers between them. Nuclear physics calculations indicate that, without the spacers, a criticality concern exists if more than one canister containing significant amounts of entrained water is placed in a storage cask. Therefore, it is essential to design a reliable drying process.

---

a. Work supported by the U.S. Department of Energy under DOE Contract No. DE-AC07-76ID01570.

DISCLAIMER

The canisters will be purged of water, using pressurized nitrogen while they are still in the TAN Storage Pool. However, the chance that unacceptable amounts of water will remain in them is not completely precluded. The process must ensure that canisters are "dry" before they are placed in the cask. This paper presents the methodology and results of an analysis that combined human reliability analysis (HRA) and probabilistic risk assessment (PRA) techniques to evaluate the design and make recommendations that would ensure an acceptably low probability of criticality frequency during operation.[a] This information was used to assist in the finalization of the design criteria and formulation of administrative procedures and controls for the drying process. This information was used to assist in the finalization of the design criteria and formulation of administrative procedures and controls for the drying process.

ANALYSIS AND APPROACH

When the risk analysis was initiated, the drying process was still in the conceptual design stage and hardware configurations had not been established. Likewise, procedures and administrative controls had not been formulated. Thus, the objectives of the analysis were to (a) determine an acceptable goal for the potential criticality occurrence frequency associated with the operation of placing TMI canisters into dry storage; (b) identify hardware failures and human actions that could result in an unacceptable level of risk based on potential criticality frequency; and (c) determine hardware and procedural requirements that would ensure safe operations.

Drying Process Description

The first step of the analysis was to review and evaluate the proposed drying system. The drying process required that the canisters be moved from the TAN Storage Pool and placed into a drying system. A simplified drawing of the system is shown in Figure 1. To dry the TMI canisters, nitrogen gas will be circulated through the canisters. The nitrogen enters at 16 to 18 psia and 250 to 270°F. The exiting nitrogen will be a nitrogen/water vapor mixture at 5 to 7 psia and variable temperatures. A liquid ring pump increases the pressure to about 20 psia. A condenser lowers the temperature of the process flow to 80°F. Upon entering a low pressure nitrogen tank, the bulk water will be separated from the nitrogen gas stream. Hygrometers are used to determine when the canisters' contents are "dry." When the hygrometers indicate that the exiting air has a dew point of 80°F or less, shutdown procedures are initiated.

The drying system can accommodate four canisters simultaneously. Once the canisters are verified dry, they are removed from the dryer and placed in a long-term storage cask. The cask holds seven canisters; therefore, two drying cycles are necessary for loading one storage cask.

The cask-drying mission was defined functionally by using a goal tree approach. The goal tree is illustrated in Figure 2. Since the desired change in the design was to store fuel canisters without the costly neutron absorbing materials, it was necessary to identify operational methods whereby a combination of equipment and/or operator failures would not result in two or more canisters being placed in storage without being completely dried. Safe operation requires that all canisters be thoroughly dried and that no canisters bypass the drying process.

---

a. The work documented in this paper was performed for the TMI Dry Cask Development Project at the Idaho National Engineering Laboratory.

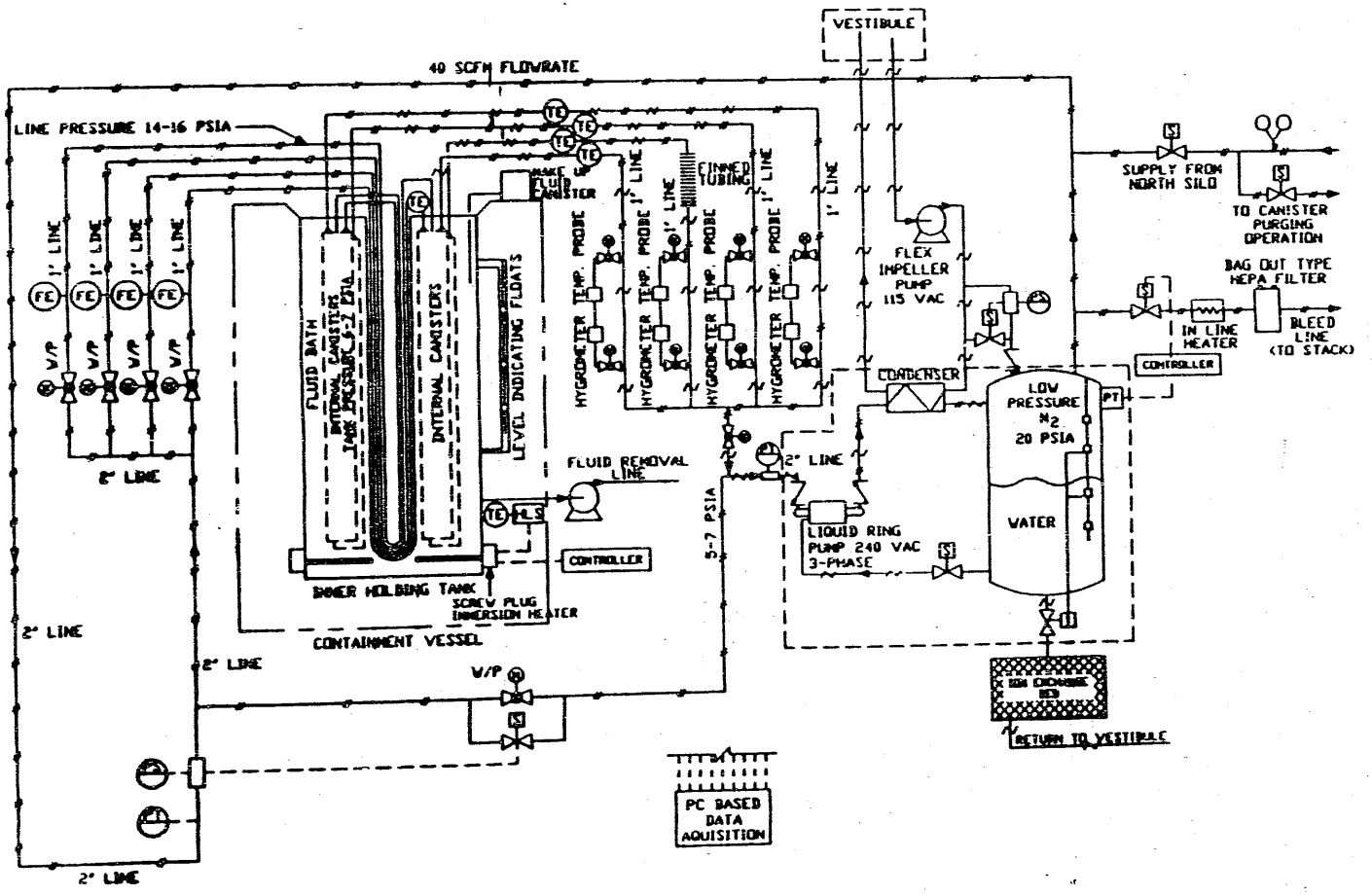

FIG. 1. Simplified schematic for drying system.

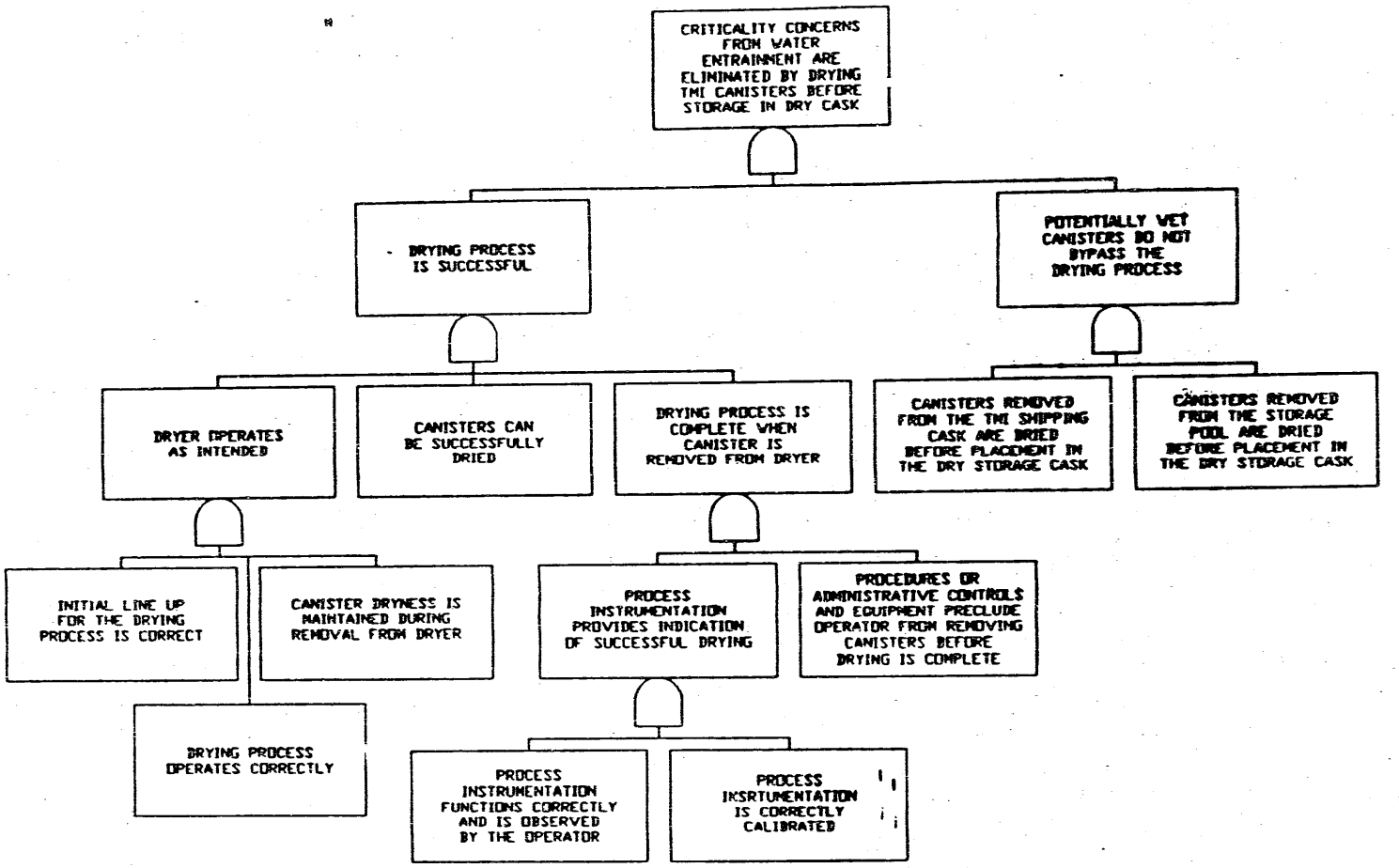

FIG. 2. Goal tree developed for TMI Dry Storage Cask Risk Assessment.

Integrated Risk Assessment Approach

Because the drying process was still in the conceptual design stage, the methodology used for this analysis had to be flexible to accommodate future changes in design requirements. The systems analysis was conducted to determine the hardware and instrumentation required to achieve the proposed mission. For every element on the goal tree, the systems analyst postulated failure modes for the equipment, instrumentation, and support systems. Although a satisfactory definition of equipment failures was developed, it became apparent that many of the failure modes could also be achieved by operator error. For example, a control instrument could fail in such a mode that an operator would (incorrectly) assume that the drying process was complete and that the canister's contents were dry. On the other hand, the control instrument could perform its function correctly, but an operator error (misreading an instrument or reading the wrong instrument) could result in the same failure of placing a canister with entrained water in storage. Therefore, operator error was incorporated into the model.

Especially important in the analysis of operator errors is the quality of the human-machine interface and the use of administrative controls. In this instance, "quality" refers to how well the equipment and procedures actually support the human in successfully completing the tasks. The operators' key interfaces with process control systems are through the equipment used to control the process and through the procedures they follow in conducting operations. A number of safety features (e.g., interlocks, annunciators) were proposed for the process. However, they will ultimately all be administratively controlled.

Thus, it was not sufficient to merely model a safety device as preventing unintentional early removal of a canister because it was possible for an operator, believing that the canister was dry, to merely deactivate the safety device. A careful consideration of the number and types of administrative controls, as well as requirements for the quality of the human-machine interface, had to be performed. This would ensure that no single failure or simple, common mode failure could inadvertently bypass the intended safety features of the drying system.

Fault tree analysis (FTA) was selected as an appropriate approach to provide quantitative assessments of significant failures. Fault tree models identify fault logic and basic (faulted) events that individually, or taken in combination, could lead to the occurrence of water being present in two of the seven canisters in a cask. It was assumed that entrained water in two canisters constituted a critical configuration. Therefore, the top event was defined as "water entrainment in two TMI canisters stored in the same cask."

Following construction of the fault tree, a functional analysis of the system was conducted to determine ways personnel actions could circumvent a successful drying process. Once these critical human actions were identified, fault sequences were formulated to disclose both the logical relationships between the tasks and the ways human errors could propagate through the fault tree to challenge higher level safety goals. HRA was performed to assign error rates to these identified activities.

The HRA was paired with the systems analysis fault trees to provide an integrated analysis of the sources of risk that could challenge the safety of the drying process. This step was necessary to ensure that all significant requirements identified by the goal tree were accounted for in the risk assessment and also to ensure that the human contribution to hardware failure or bypassing control systems were considered.

After quantifying the risk model, dominant sets of events were analyzed to determine any remedial actions or necessary redundancies that by including in the design or operational requirements would reduce the level of risk to an acceptable value. Independent verification by a second operator, procedures with check-offs and sign-offs, job performance aids for performing minor calculations, etc. were recommended as measures that could reduce the possibility of a single operator error leading to the removal of a potentially wet canister from the drying process. A redundant train of hygrometers, strategic placement of check valves, and highly reliable data buses for the automated control systems were also recommended to enhance the reliability of hardware in the drying system.

The analysis results indicated that, by implementing the operational and hardware improvements, the potential criticality frequency for a drying campaign was less than 4.0E-5 for a 60-cask storage campaign. This was judged to be acceptable; and design and implementation could proceed without undue risk.

BENEFITS AND INSIGHTS

Often risk analyses are conducted after a process and/or system has been designed and constructed. Therefore, recommendations resulting from the PRA analysis are very costly because once built, it is cost-prohibitive to upgrade sections of a system to achieve an acceptable level of risk that should have been defined at the outset of the project. The design philosophy of "make it so it can't happen" can be an expensive one. Defining an acceptable level of risk and designing a commensurate system or process achieves the maximum cost benefit.

This project illustrates that a large benefit can result by involving risk assessment analysts during the conceptual stages of design. The cost benefit realized from the performance of the analysis during the design phase was approximately $2 million because the analysis determined that an acceptably low level of risk could be achieved without installing neutron absorbing material in the storage casks.

Also, performing an integrated analysis involving both hardware and human reliability is very beneficial. Very few process control systems operate without the assistance of people who calibrate, maintain, start up, run, and shut down these very expensive systems. The occasional hardware failure is easy to understand and is expected. Human errors, on the other hand, happen in many different ways and for many different reasons. The integration of a human reliability and systems analysis was an essential element in providing an accurate and complete disclosure of system failures.

Results from the risk analysis identified the sources of failures and the mechanisms (or event sequences) that could challenge mission success. Based on the results, analysts were able to work with designers to provide operational safety requirements (OSRs) based upon an identified risk profile to ensure safe operation of the drying system. Developed in this way, the OSRs provide a basis for ensuring that fault sequences identified are addressed by administrative controls prior to operation of the facility.

REFERENCES

1. A. J. Palmer ltr to Distribution, Call for Conceptual Design Review, AJP-01-89, March 15, 1989.

END

DATE FILMED

11 / 29 / 90