USE OF MASTER LOGIC DIAGRAMS AS A HAZARDS ASSESSMENT TOOL FOR NONREACTOR FACILITIES

G. A. Coles
Westinghouse Hanford Company
P.O. Box 1970
Richland, Washington 99352

ABSTRACT

The Hanford Site is under the jurisdiction of the U.S. Department of Energy. Its original mission of production of special nuclear materials has changed to nuclear waste management and environmental cleanup. Significant emphasis is being focused on waste management systems. Failure of these systems can result in threats to health, safety, and the environment. Westinghouse Hanford Company (WHC) is applying techniques borrowed from reactor safety analysis experience in safety analysis of these systems.

I. INTRODUCTION

The WHC is developing new uses for reactor risk assessment techniques in safety assessments of nonreactor nuclear facilities and operations. For example, master logic diagrams (MLD) are being used as tools to identify hazards for safety analysis. This approach augments, and has some advantages over, form-driven hazard assessment techniques used in the past. This paper describes use of the MLD as a hazard identification tool and describes a successful application of this approach.

II. METHOD

This section discusses hazards, hazards assessment, and how an MLD can be used in the identification of hazards in a facility safety analysis.

The following definition of hazard is used:

> "Hazard - A characteristic of a system/plant/process that represents a potential for an accident. The combination of a hazardous material and an operating environment such that certain unplanned events could result in an accident."[1]

Accordingly, hazards lead to accidents as a result of unplanned events. Hazards are not accident sequences. An accident sequence is the result of an initiator (unplanned event) propagating an unsafe condition (hazard) into an accident. However, some safety analysis documentation considers initiators to be hazards. The MLD does a good job of identifying both the initiators (unplanned events) and hazards (the unsafe conditions). The ultimate concern in a safety study is accidents, so both initiators and unsafe conditions (hazards) need to be addressed.

A facility hazards assessment is an investigation into potential harm represented by that facility. An MLD can organize, document, and display that process.

The MLD technique is borrowed from the reactor probabilistic risk assessment (PRA) method described in NUREG/CR-2300, "A PRA Procedures Guide."[2] In a reactor PRA, it is used as one the ways to identify initiating events. Reference 1 states that a summary fault tree or MLD can be constructed to guide the selection and grouping of accident-initiating events and to ensure completeness. This systemic technique adds rigor to the investigative process.

Hazard assessment procedures used in the past at WHC have typically been form driven. Most safety analysis reports done at the Hanford Site include a preliminary hazards assessment. Investigation is done by comparing plant or system characteristics to a generic list of potentially hazardous conditions. For each hazard identified, the cause, the effect, and any corrective or preventive measures are listed on a form.

The MLD method, like fault tree analysis, is a deductive technique that focuses on one particular undesired event (such as radioactive release) and provides a system for determining the cause of that event. The model consists of events connected by gates.

The gates define the interrelationship between events below that gate, such as "and" or "or" logic.

The MLD itself is a graphical model and is constructed in strictly defined levels with the undesired event being the top event or level 1. The use of levels is an ordering technique with a strategy of obtaining completeness at each level. With each succeeding level, the combination of events that can lead to the top event gain greater and greater specificity. Each level is complete in itself, but may be too general or too specific to be of value.

A limit of resolution consistent with the scope of the study is chosen. Modeling from the top event down, using more and more levels, greatly increases the size and complexity of the diagram and conveys more information. However, modeling in too much detail may not be beneficial to identifying general hazards and unplanned events.

One advantage of a completed MLD is that it identifies both the conditions (hazards) and the unplanned events that cause the hazards to become accidents. This benefits further safety analysis, because it not only identifies events and conditions but also describes the relationships between them that can lead to accidents.

III. SAFETY STUDY

Use of the MLD technique played a key role in a recent safety study. The purpose of this safety study was to support a decision on whether to continue a particular activity involving pumping hazardous liquid waste. Use of the MLD helped identify important accident scenarios that had been overlooked in previous safety analysis. This section describes the background leading up to this study, the study itself, the MLD constructed, and how an MLD benefitted the study.

A. Safety study background

This section describes the background and sequence of events leading up to a safety study that employed the use of an MLD. This study was conducted by WHC in the first half of 1992.

High-level radioactive liquid waste, a byproduct of the plutonium separation processes at the Hanford Site, is stored in large underground waste storage tanks. The first generation of tanks, built between 1943 and the mid-1960's, was single-shell carbon steel tanks encased in concrete. Of the 149 single-shell tanks (SST) constructed, the oldest have been in use for nearly 50 years. All of the SSTs have exceeded their design life.

Sixty-six of the SSTs (approximately 44%) are either suspected or known to have leaked liquid radioactive waste to the ground, and the remaining tanks can be expected to start leaking at any time in the future. Therefore, in the past, the practice has been to reduce the volume of liquid in the underground tanks. Part of this liquid waste reduction policy is to pump as much drainable liquid waste as possible from the SSTs. This minimizes the volume of liquid available to leak into the ground. This process is know as interim stabilization.

Interim stabilization is accomplished by salt well pumping via jet pumps. A salt well is the casing that extends down into the waste from the pump (see left-hand diagram in Figure 1). With the jet pumps, the supernatant floating on top of the waste and the interstitial liquid from within the solid wastes are drawn out. The intakes for these pumps are located in a salt well that includes screens that are imbedded in the stored waste. The resultant liquid waste is transferred to a double-containment receiver tank (DCRT) and accumulated for a period of time (see right-hand diagram in Figure 1). From these tanks the waste is transferred to storage or into the waste concentration system for volume reduction.

After about 105 of 149 tanks had been interim stabilized, this activity was deferred from 1985 to 1989 due to lack of double-shell tank space. Studies indicated that this decision posed no undue risk. Interim stabilization activities were suspended again on August 29, 1991, due to concerns related to Public Law 101-510, Section 3137.[3] This law prohibits accidental (or otherwise) addition of radioactive waste to certain tanks, referred to as the watchlist tanks. Interim stabilization activities will continue after applicable safety studies are performed. This safety study was a part of that effort.

B. Safety study scope

The safety of interim stabilization activities for remaining nonwatchlist tanks was evaluated.[4] Preliminary analysis indicated that the existing safety analysis report, written in 1981 for this activity, may not identify all plausible hazards for current operations. For example, much of the salt well piping, which is

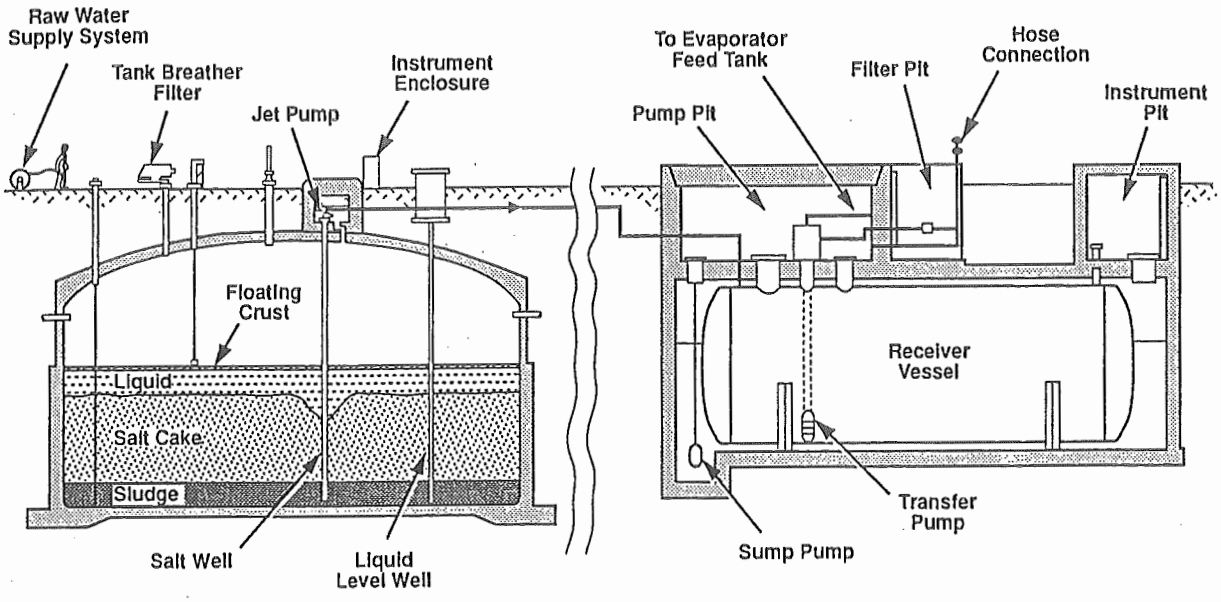

FIGURE 1 TYPICAL SALT WELL-DCRT SYSTEM

direct-buried carbon steel lines, is now past its design life, giving it a high failure frequency. It is possible that a line could leak and waste could pool at the ground surface while the Radiation Monitor System is failed. Accordingly, one of the early steps in this safety study was a hazards assessment. The MLD approach was chosen.

Facility familiarization found that the interim stabilization activity involves a number of different waste tanks and supporting systems. Some tanks and systems are supported by different engineering and maintenance groups. Major components include the SSTs, jet pumps; transfer lines; valve and diversion stations; and the DCRT and associated ventilation, instrumentation, power, and radiation monitoring systems. The investigation included examining facility descriptions, previous safety analyses, and drawings, and having discussions with the cognizant engineers.

The hazards represented by this activity include a wide range of phenomena that could lead to a release of hazardous material. Whereas reactor safety studies primarily focus on loss of core cooling as the dominant contributor to risk, the risk represented by the subject pumping activity was represented by a wider range of risk contributors.

C. Safety study MLD

As stated earlier, the MLD is a graphical model. A description of the model follows. A graphical representation of the entire model is not shown, because it is 1 page deep and 20 pages wide.

The model (or tree) is seven levels deep. More levels are possible, but the objective in this case is to understand, in general, the hazards and initiating events, not to represent in detail all variations of events leading to an accident.

The top event in the MLD (level A) for this assessment is "Uncontrolled Release of Hazardous Waste Caused by Interim Stabilization Activity." This describes the undesired event of concern for the subject activity. Accordingly, all hazards and initiating events identified by this model are related to uncontrolled release of hazardous waste.

The second level (level B) subdivides this release into two categories: (1) "Airborne Release of Stored Waste Caused by Interim Stabilization Activity" and (2) "Liquid Release of Stored Waste Caused by Stabilization Activity." Airborne releases include gases and aerosols. Liquid releases consist primarily of leaks to the ground. For this study, any release that consisted of both airborne material and liquid to the ground (such as in explosions) was considered under the "airborne release" branch. At this level, there is a total of two subdivisions (gates).

The third level (level C) subdivides both airborne and liquid releases still further into physical locations: (1) release from an SST or associated pump pit; (2) release from transfer piping or valve pits; (3) release from a DCRT; or (4) release from watchlist tanks caused by mistransfers. These represent the physical locations that the liquid waste could travel through during the pumping activity. This results in a total of eight gates.

The fourth level (level D) subdivides each branch into the source and nature of the release or the phenomenological form of the release. Any release that happens must be the result of some occurrence. There is a limited set of phenomena that can lead to an occurrence. To help identify possible phenomena, industry-wide hazard checklists were consulted.

Since the subdivisions below the fourth level vary with the physical location of the liquid waste, not all are listed. However, examples of these include (1) airborne release from excitation of waste material from SST dome or DCRT structure collapse; (2) airborne release from chemical explosions; (3) airborne release from liquid spray; (4) airborne release from an open ventilation path; (5) airborne release from fire; (6) airborne release from an underground leak that pools to the surface; (7) airborne release from liquid entrainment in ventilation flow; (8) breach of tank; (9) breach of piping; (10) overfilling of tank; and (11) misrouting and dissolving of a "healed" (dried) leak pathway. There are a total of 27 gates in level D.

The fifth, sixth, and seventh levels (levels E, F, and G) model combinations of conditions and unplanned events that lead to an uncontrolled release. Specifically, combinations of conditions and unplanned events lead to a release occurrence that

- Can be characterized by some phenomena
- Occurs at some physical location
- Is either an airborne or a liquid release
- Can be generally classified as an Uncontrolled Release of Hazardous Waste Caused by Interim Stabilization Activity.

Following is an example of how events at levels E, F, and G can contribute to an event in level D. One of the contributors to gate D3, "Airborne Release from SST or Pump Pit Caused by Spray," is gate E8, "Airborne Release Caused by Spray Leak in SST Pump Pit Piping." Gate E8 (shown on the top of Figure 2) is an and-gate; therefore, the following must exist for E8 to occur:

- F11, "Breach in Jet Pump Piping or Valve Bodies in Pump Pit Leads to Spray"
- F12, "Dispersion of Aerosols or Vapors Through Air Gap Around Pump Pit Cover"
- F13, "Failure of Jet Pump Low-Pressure Shutdown Interlock."

There are a number of contributors to gate F11 (a breach) including such conditions and events as freezing, random leaks in pipes or valve bodies, cranes falling onto the pump pit, and seismic events. These final contributors and many others are the output of this MLD modeling. They represent a set of conceived unplanned events (initiators) and unsafe conditions (hazards) for the safety study. Contributors could be subdivided further. For example, gate G6 could be subdivided into gasket failures, pipe breaks, etc. We chose, however, to do more detailed work during the accident sequence analysis phase of the study.

Although the portion of the MLD in Figure 2 looks like a common fault tree (the MLD is, in fact, called a summary fault tree in Reference 2), it can not be treated as one. Normally, fault trees are solved for cutsets. However, the MLD for cutsets was not solved, because the cutsets obtained from this modeling process can be misleading. For example, if failure of a particular valve leads to a moderate consequence and failure of that valve during a fire leads to a higher consequence, boolean solution will subsume the higher consequence scenario.

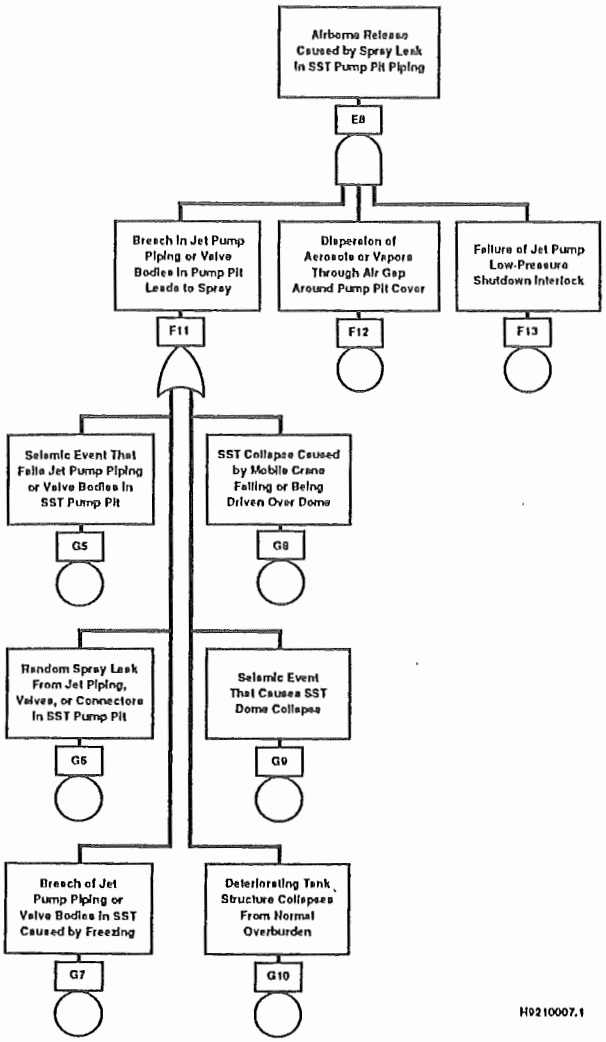

FIGURE 2 EXAMPLE SECTION OF MLD

To recapitulate, the following summarizes the MLD by level:

- Level A--Uncontrolled release (top event)
- Level B--Airborne or liquid release
- Level C--Physical location of release
- Level D--Source and nature of release
- Levels E, F, and G--Hazardous conditions and unplanned events that lead to release.

D. Study results

This subject study identified five hazard/accident categories requiring further evaluation. Accident sequence analysis, including the use of event trees and source term calculations, was performed on the five categories. The five categories were

- Breach of waste confinement piping or equipment in SST pump pits, DCRT pump pits, or valve pits that result in liquid spray
- Equipment fires in an SST or DCRT
- Hydrogen accumulation within the DCRTs
- Waste transfer line leaks/breaks
- Waste stability following mistransfers.

Accident analysis resulted in 130 accident sequences, several of which were shown to result in unacceptable risk if certain additional controls were not implemented.

In some cases, hazards/accidents identified by the MLD had been identified years earlier, but were discounted in the safety analysis report as not being significant at that time. Additionally, some hazards/accidents identified by the MLD had not been identified. In our opinion, the rigor and organization of the MLD were key to these results. For example, spray from small leaks in connectors in certain pump pits contributes significantly to inhalation doses of radioactive material. Addressing the phenomenological form of the release in level D aided in this discovery.

One of the great benefits of the MLD in the subject study was that it defined the interrelationship between the hazards and elements of an accident. It helped identify elements of accident sequences: initiating events, conditional events, and failure of mitigating systems. Accident sequences could be organized according to hazard/accident categories. Accordingly, it made the transition to accident sequence analysis easier.

V. CONCLUSIONS

Use of the MLD was successful in identifying hazards and unplanned events in a safety study we performed. We believe this process to be more deductive than form-driven hazard identification methods

previously used. We believe this method to be particularly useful on complex nonreactor nuclear facilities that may have a wide range (phenomenologically) of risk contributors. We believe this process is a good precursory analysis to follow-on accident sequence analysis. In general, it helped organize, document, and display the hazard and unplanned event investigation process.

REFERENCES

1. *Guidelines for Hazard Evaluation Procedures*, Prepared by the Battelle Columbus Division, Battelle Memorial Institute, for The Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York (1985).

2. W. HICKMAN et al., "A PRA Procedures Guide," *NUREG/CR-2300, Vol. 1*, U.S. Nuclear Regulatory Commission (1982).

3. "Safety Measures for Waste Tanks at Hanford Nuclear Reservation," Section 3137 of *National Defense Authorization Act for Fiscal Year 1991*, Public Law 101-510 (1990).

4. S. M. STAHL and G. A. COLES, "Safety Study of Interim Stabilization of Nonwatchlist Single-Shell Tanks," *WHC-SD-WM-RPT-048, Rev. 0*, Westinghouse Hanford Company (1992).