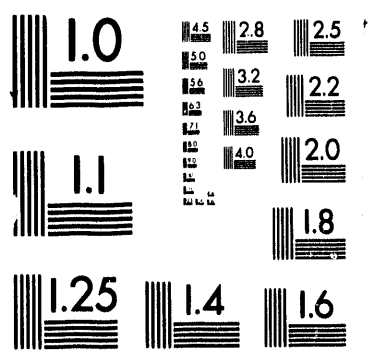
1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1
8.0
9.0

1 of 1

Conf-940312--9

LA-UR-93- 3424
N-6-93-R144

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

TITLE: **HANFORD HIGH LEVEL WASTE (HLW) TANK MIXER PUMP SAFE OPERATING ENVELOPE RELIABILITY ASSESSMENT**

AUTHOR(S): Stewart R. Fischer
James Clark



SUBMITTED TO: PSAM-II Conference
March 20–24, 1994
San Diego, CA



Los Alamos National Laboratory
Los Alamos, New Mexico 87545

# HANFORD HIGH LEVEL WASTE (HLW) TANK MIXER PUMP SAFE OPERATING ENVELOPE RELIABILITY ASSESSMENT

**Stewart R. Fischer**

**Probabilistic Safety Assessment Section**
**Engineering and Safety Analysis Group**
**Nuclear Technology and Engineering Division**
**Los Alamos National Laboratory**
**Los Alamos, New Mexico 87545**

**James Clark**

**Science & Engineering Associates**
**6100 Uptown Blvd., N.E.**
**Suite 700**
**Albuquerque, New Mexico 87110**

## INTRODUCTION

The US Department of Energy and its contractor, Westinghouse Corp., are responsible for the management and safe storage of waste accumulated from processing defense-reactor irradiated fuels for plutonium recovery at the Hanford Site. These wastes, which consist of liquids and precipitated solids, are stored in underground storage tanks pending final disposition.

Currently, 23 waste tanks have been placed on a safety watch list because of their potential for generating, storing, and periodically releasing various quantities of hydrogen and other gases. Tank 101-SY in the Hanford SY Tank Farm has been found to release hydrogen concentrations greater than the lower flammable limit (LFL) during periodic gas release events. In the unlikely event that an ignition source is present during a hydrogen release, a hydrogen burn could occur with a potential to release nuclear waste materials. To mitigate the periodic gas releases occurring from Tank 101-SY, a large mixer pump currently is being installed in the tank to promote a sustained release of hydrogen gas to the tank dome space.

An extensive safety analysis (SA) effort was undertaken and documented to ensure the safe operation of the mixer pump after it is installed in Tank 101-SY.[1] The SA identified a need for detailed operating, alarm, and abort limits to ensure that analyzed safety limits were not exceeded during pump operations. To further ensure that pump operations were being carried out safely, the Los Alamos National Laboratory Engineering and Safety Analysis Group Probabilistic Safety Assessment Section has reviewed the mixer pump initial, or Phase A operations, to determine the conditional probability of exceeding a prescribed set of safe operating envelope (SOE) boundaries. These boundaries were defined to be the operating, alarm, and abort parameters as monitored by mixer pump and other in-tank and ex-tank instrumentation and as specified by Chap. 6 of the mixer pump SA, operating procedures, and preprogrammed abort and alarm limits for pump operation.

The SA assessment was intended to identify any credible single or multiple failures that would result in an unacceptably high probability of exceeding instrument-monitored operating limits. This review only analyzed the conditional probabilities of failure to remain within the SOE per pump operation as defined by instrumentation alarm and abort limits during the short-duration Phase A pump operations. No consideration was given to the likelihood of individual initiators nor to coupling them to the conditional failures required to lead to conditions outside the SOE boundaries. Similarly, we did not consider the consequences of possible failures in this assessment.

## METHODOLOGY

A fault-tree approach was used to assess the potential failure for key control parameters that were implemented procedurally or controlled with the computer-based Data Acquisition and Control System (DACS). The assessment considered potential failures in both manual and automatic abort functions, as well as human errors and hardware failures during startup (i.e., preexisting conditions) and operating phases. Numerous assumptions were made in developing the fault trees; a primary one was that the reliability assessment represented a "snapshot" in time (with respect to procedure development) and is only applicable to Phase A testing. Fault-tree quantification was based on generic hardware failure data and on THERP[2] human reliability techniques.

Because of the nature of the fault-tree analysis used in this assessment, a strong dependence on the operating procedures was inherent. This dependence also meant that subtle changes in procedures may render the fault-tree analysis incorrect or inadequate; thus, for the purpose of this analysis, four procedural documents were used.[3–6] These procedures had been approved by the Westinghouse Hanford Company (WHC) Test Review Group (TRG) and were the most recent procedures available at the time of this analysis. In these procedures, there are automatic pump aborts with manual abort backup, manually directed pump aborts with and without automatic alarm indications, and requirements to prohibit pump operation based on preexisting conditions and instrumentation readings. The SOE fault tree was structured around these considerations. Where system details were uncertain, we attempted to apply conservative assumptions and to document such modeling.

Operator training sessions, in which the DACS was used as a training simulator with a variable-speed drive and a motor simulator were observed to help quantify human error probabilities. These observations also identified several significant areas where human actions could defeat the instrumentation and abort protective logic established in the SA easily. These items, which resulted from the flexibility of the DACS system, included capabilities to easily disable aborts and to place instrumentation into a "manual," or instrumentation signal bypass, mode. Additionally, our understanding of the DACS/operator control process was enhanced through numerous detailed conversations with test engineers, DACS engineers and technicians, and safety analysts.

The scope of this reliability analysis included a review of both the DACS design as well as the interface between DACS and the test engineers or operators. The DACS system interfaces with all in-tank, ex-tank, and pump instrumentation and provides data monitoring, recording, and control of pump operation. This effort focused on the alarm and abort parameter monitoring and operational controls that ensure that the SOE is not exceeded.

## RESULTS

The overall results of the fault-tree analysis indicated that the conditional (i.e., assuming all initiating events are equally likely with a probability of a specific initiating event being 1.0) probability of operating outside the SOE is dominated by human error. Implementation of extensive operational/safety controls defined by Chap. 6 of the SA have resulted in detailed procedural requirements. These procedural efforts have helped to reduce the potential for human/operator error significantly. However, the Phase A test procedure,[3] coupled with the highly versatile and flexible DACS system, still provides numerous opportunities for inadvertent human error. Despite numerous single failures, the number of actual hardware failures that could conditionally result in the SOE being exceeded is relatively small.

## Selected Qualitative Insights

Because of the iterative nature of this reliability assessment (which started before the development of the test procedure), numerous insights and recommendations evolved that resulted in design and administrative changes. Some of our qualitative insights include the following.

1. A preliminary failure mode analysis of the DACS/operator system and control hardware [the variable speed drive (VSD) and instrumentation] was performed with respect to control of pump speed and test duration. In addition, a high-level fault tree of the DACS hardware control functions was coupled with operator actions to provide qualitative insight to mixer pump control. This review indicated a possible single failure of the VSD speed-sensing circuit that could result in pump overspeed. A single speed sensor was used to provide speed indication for monitoring and control purposes on DACS; it also was used by the VSD to control pump speed. To remedy this situation, a backup-motor frequency readout was installed in the DACS trailer, and it will be used to provide independent monitoring of pump speed.

2. The assessment identified possible communication delays associated with the DACS computer that could result in timing delays (up to 10 s or more) associated with pump shutdown actions. To remedy this problem, the final system design controls pump operation timing and provides alarms and abort signals from the programmable logic control (PLC) units, which have adequate frequency response.

3. The assessment suggested that possible single failures of the DACS timer circuit could result in extended pump run times unless backup timing is provided. To remedy this situation, an operator will monitor DACS control of the pump via independent readouts of time (stopwatch) and pump speed. The operator is required by the Phase A test procedure to abort the test if either of these parameters exceeds established limits.

4. The assessment indicated the need to establish a "Minimum Instrument List" to ensure that primary and backup instrumentation for maximum waste level, rate of level rise [i.e., radar gauge/Food Instrument Corporation (FIC) gauge], waste density [i.e., redundant Velocity Density Thermocouple Trees (VDTT) strings], etc. are fully operational during testing.

5. The preliminary assessment indicated a need to ensure that administrative controls for setting the maximum speed, the alarm/abort limits, and all operating limits are implemented. Acceptance test procedures have been implemented to provide assurance that instrumentation is functioning and that alarms and abort limits are set properly.

Numerous other insights identified specific problems for which corrective actions in the form of hardware, software, or administrative changes were taken.

## Quantitative Insights—Individual Control Parameters

Numerous single hardware failures for individual sensor circuits were identified; however, their failure probabilities are in general less than $10^{-4}$. In addition, operator errors are associated with each individual circuit or prestart calculation that could lead to failure of a given sensor circuit or failure to secure startup of the mixer pump without proper verification of prestart conditions. Both the preexisting failure of each instrumentation circuit and the failure of the operator to correctly verify prestart conditions before mixer pump operation dominate the individual sensor circuit or calculation failures. In addition, human errors associated with programming and set point entry errors contribute significantly to individual circuit failure. Table 1 shows the conditional failure probability for each individual test control parameter (i.e., each control parameter is considered separately). Each control parameter probability is the sum of the individual fault-tree cut sets for each parameter modeled. The manual abort item in Table 1 includes preexisting and operational

Table 1. Conditional failure probability of individual Phase A SOE test parameters

| Parameter | Conditional Total Failure Probability |
|---|---|
| **Automatic Aborts** | |
| 2/3 Vent Flow Split (SY-102, 103) | 1.0e-02 |
| Tank Level High | 5.4e-04 |
| Motor Amps | 5.1e-04 |
| Pump Speed | 4.8e-04 |
| High/Low 101-SY Vent Flow | 3.0e-04 |
| Column Pressure | 2.3e-04 |
| VDTT Strain | 1.6e-04 |
| Discharge Pressure | 7.5e-05 |
| MIT Strain | 6.4e-05 |
| Oil Moisture | 6.2e-05 |
| Column Strain | 5.8e-05 |
| Hydrogen Concentration High | 5.6e-05 |
| Pump Vibration | 5.4e-05 |
| Oil Temperature | 5.3e-05 |
| Dome Pressure | 3.6e-05 |
| Waste Temperature | 2.7e-05 |
| Pump Flow | 1.7e-05 |
| Test Time | 6.3e-06 |
| **Manual Aborts** | |
| Foaming | 1.0e-02 |
| Hydrogen Concentration Low | 3.0e-03 |
| Dome-to-Ambient $\Delta T$ | 1.0e-03 |
| Level Rise Rate | 1.0e-03 |
| Operator Fail to Abort on Alarm | 7.0e-04 |
| Operator Fails to Verify No Adverse Weather | 1.0e-04 |

failure probabilities for the following items: the dome-to-ambient-temperature difference; the low initial hydrogen concentration; the level rise rate; the waste density; the weather conditions; and foaming. The single largest contributor to the manual abort failure probability is failure of the operator to monitor the camera during the short Phase A tests. Also, no significant cut sets appear for waste density because of extensive redundancy of this parameter.

As summarized in Table 1, conditional sensor/circuit failures range from 1.0E-2 to 6.3E-6, depending on the individual parameter. For some sensor/circuit failures, recovery by the operator may be possible before the SOE is exceeded. This is particularly true if the evolving condition is slow in its rate of progression toward exceeding the SOE condition. An example would be waste tank temperature, where because of the total mass of waste, temperature rise rates generally would be expected to be slow. This could be contrasted with the mixer pump speed circuit, which could see a rapid rate of rise in speed, and thus, the operator would have very little time to react to an evolving situation. However, no credit has been given to the relative factors. It is interesting to note that those circuits where failure probabilities are less than 1.0E-4 generally are dominated by a single failure or a few operator errors, whereas those where failures are greater than 1.0e-04 are dominated by operator errors. Finally, as was previously mentioned, giving no credit for redundancy in similar types of conditions monitored (i.e., speed, pump flow, pump current, etc.) introduces additional conservatisms into this analysis. No attempt has been made to correlate sensors to fundamental parameters monitored.

The conditional failure probability of individual sensors and associated circuits is dominated by operator errors such as misreading instruments or miscalculations during the 2/3 vent flow calculation, the level-rise calculation, or the dome-to-ambient-temperature-difference calculation. In addition, dominant contributors include failure of the operator to monitor and discover foaming, failure of the operator to verify that weather conditions are adequate before pump operation (the product of two operator errors), failure of the operator to shut the system down upon reaching an abort limit, preexisting loss of control power to mixer pump interrupt circuit breakers, and miscalibration of sensors and associated circuits. Preexisting hardware failures of individual sensors, I/Os, I/O power supplies, alarm and abort circuits, and the video camera are significant contributors to conditional failures.

Finally, some common-cause failures contribute slightly to circuit failures. These consist primarily of common-cause miscalibration of sensors/circuits, a common-cause DACS programming error; a preexisting common-cause failure of both PLCs; and, a preexisting common-cause failure of some sensors as is, low, or intermittent.

### Quantitative Insights—Total System Reliability

Table 2 presents the dominant cut sets and the total conditional failure probability for these test control parameters to remain within the SOE given an initiating event. Table 2 includes common-mode failures such as power supply or PLC failure, which would disable groups of instruments.

The total conditional failure probability for Phase A tests to remain within the SOE was computed to be 0.027. Table 2 lists the dominant cut sets or failure modes, which contribute over 95% of the total conditional failure probability. Including calibration errors for 9 sensors contributes an additional 3.3% of the total conditional failure probability. As discussed before, operator errors associated with detecting out-of-range preexisting conditions during prestart checks dominate. Given equal probability of an initiating event, the failure to identify abnormal ventilation flow (i.e., the 2/3 flow split calculation) has the highest conditional probability for failure to remain within the SOE during the prestart phase. For the pump operational phase, the failure of the operator to monitor the video camera and abort on foaming dominates the probability of the SOE being exceeded. Similarly, during the pump operational phase, the dominant hardware failure is associated with failure of control power to the mixer pump circuit breakers.

When reviewing these results, one must keep in mind the very significant assumptions and/or conservatisms that have been used. Some of these are listed below.

1. All control parameters are assumed to be independent, and no recovery credit was given for sensors that may provide backup indication for the same operating parameter; i.e., motor amps or pump discharge pressure would provide an indication of pump speed.

2. All control parameters were assumed to be equally important. Equal treatment of all control parameters by the operator was assumed.

3. Only conditional probabilities were considered. In effect, all initiating events were assumed to be equally likely. Clearly, some events are more likely than others. To obtain accident probabilities, the study would have needed to include accident initiator frequencies, all mitigation paths, and operator actions and account for redundancy in function, for example, pump speed and flow.

4. No effort was made to distinguish between slow and rapid envelope excursions. For slow evolutions, operator recovery is more likely.

5. Generic hardware failure data were used throughout.

**Table 2.** Integrated Phase A test total conditional failure probability

| Dominant Cut Set | Probability | Importance (%) |
|---|---|---|
| Minimum 2/3 flow calculation | 0.01 | 36.4 |
| Video camera observation during testing | 0.01 | 36.4 |
| Preexisting failure of low $H_2$ sensor | 2.88e-03 | 10.5 |
| Dome-to-ambient-temperature-difference calculation | 1.0e-03 | 3.6 |
| Level rise calculation | 1.0e-03 | 3.6 |
| Operator fails to initiate manual abort | 7.0e-04 | 2.5 |
| Preexisting loss of control power to breaker | 3.36e-04 | 1.2 |
| Video camera fails | 2.28e-04 | 0.8 |
| Operator fails to check natural phenomena | 1.0e-04 | 0.3 |

## CONCLUSIONS

This reliability assessment has examined the operator and equipment capabilities required to maintain the operation of the mitigation test-by-pumping for Tank 101-SY within the specified SOE. The study looked at the conditional probability that the procedures and equipment would accomplish this. The qualitative insights into the DACS/Operator interface that were gained resulted in test procedure development, operator training, strict administrative controls, and design and operational improvements. The quantitative results from the study identified the dominant cut sets that, given the above assumptions, should potentially reflect the test parameters most likely to be exceeded during testing. Unfortunately, the key assumptions make useful interpretation of the quantitative results difficult at best. Additional qualitative arguments were made in an attempt to obtain meaningful results from the quantitative results.

## REFERENCES


1. Los Alamos National Laboratory Report LA-UR-92-3196, Revised, "A Safety Assessment for Proposed Pump Mixing Operations to Mitigate Episodic Gas Releases in Tank 241-SY-101: Hanford Site, Richland, Washington," L. H. Sullivan et al.

2. NUREG/CR-1278, SAND80-0200, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," A. D. Swain, H. E. Guttman, June 1983.

2. Westinghouse Hanford Company, "Test Procedure for Tank 101-SY Mitigation-by-Mixing Test Phase A," WHC-SD-WM-TPI-004, Rev. 0 (December 1992).

3. Westinghouse Hanford Company, "Tank 101-SY Mitigation-by-Mixing Test Alarm Response Procedure," WHC-SD-WM-PROC-004, Rev. 0.

4. Westinghouse Hanford Company, "Tank 101-SY Mitigation-by-Mixing Test Abnormal Operating Procedure," WHC-SD-WM-PROC-005, Rev 0.

5. Westinghouse Hanford Company, "101-SY Mitigation Testing Acceptance Test Procedure," WHC-SD-WM-ATP-046, Rev 0.

DATE
FILMED
2/8/94
END