UCRL- 92057
PREPRINT

Reliability Study on the Lawrence Livermore National Laboratory Water-Supply System

H. K. Hasegawa
H. E. Lambert

This paper was prepared for submittal to
1st International Symposium on Fire Safety Science
Gaithersburg, MD - October 9-11, 1985

June 13, 1985

Lawrence
Livermore
National
Laboratory

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint is made available with the understanding that it will not be cited or reproduced without the permission of the author.

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

Reliability Study on the Lawrence Livermore National Laboratory Water-Supply System*

Harry K. Hasegawa and Howard E. Lambert**
Hazards Control Department, Lawrence Livermore National Laboratory
P. O. Box 5505 (L-442), Livermore, California 94550

ABSTRACT

We conducted a reliability analysis of the Mocho water-supply system for the Lawrence Livermore National Laboratory (LLNL) to determine if an adequate supply of water would be available in the event of a major fire. We used the digraph fault-tree approach for logic model generation. The initiating-enabling event interval reliability approach was used for a probabilistic evaluation of the Mocho system fault tree. In the event of a major fire, the Mocho system demand unavailability was calculated to be 3.6×10^{-4}. We identified 16 single-component failures that would cause failure of the control loop which monitors storage-tank level. These failures would go undetected by monitoring personnel at LLNL. Our recommended changes would provide a redundant measurement of the tank level, resulting in a decrease of the predicted system unavailability by about a factor of 50.

INTRODUCTION

The Fire Science Group at Lawrence Livermore National Laboratory (LLNL) conducted extensive fault-tree analyses of both dry-pipe and wet-pipe sprinkler systems.[1] The fault trees for these sprinkler systems contained one common basic event: No matter how reliable sprinkler systems and fire fighters are, a fire cannot be extinguished without an adequate water supply. To complete the fault-tree analysis, we conducted a reliability study of the Mocho water supply system, LLNL's primary water supply. The Mocho water supply system contained many control loops that maintained the water level in the system storage tanks and also alerted LLNL personnel in the event of low water level in the tanks.

The digraph fault-tree methodology used in this study is particularly useful for fault analysis of control systems.[2] We constructed a fault tree with the Top Event of "Insufficient Supply of Water in Storage Tanks and No Detection of Same in Bldg. 511." The initiating-enabling event interval reliability approach is used to perform a probabilistic evaluation of the fault tree and to compute various systems reliability characteristics, such as the unavailability of water in the event of a major fire.[3]

MOCHO WATER SUPPLY AND LLNL MONITORING SYSTEM

The main source of water to LLNL is the Hetch Hetchy Aqueduct, located 800 ft below ground at the Mocho pumping station, 8 mi south of LLNL. The water is first pumped

*This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract No. W-7405-ENG-48.

** Independent consultant, Oakland, California to the surface and into two standpipes. These standpipes have a capacity of 20,996 gallons each. The water flows by gravity from the standpipes to three main storage tanks located 1/2 mi south of LLNL on the hill above Sandia National Laboratories. The three storage tanks have a total capacity of 1,238,800 gallons and provide the head pressure necessary to supply LLNL. The tanks and standpipes are all at atmospheric pressure. The Central Control Room for the system is located on-site in Bldg. 511.

As an alternate or standby water supply, LLNL has water available from the Zone 7 water district. This water supply is used only during times when Hetch Hetchy water is unavailable due to tunnel maintenance, pump failure at the Mocho Pumping Station, or line failure between the Mocho standpipes and the storage tanks. The Zone 7 water supply must be activated manually on site.

Figure 1 is a simplified schematic of the LLNL water-control system. The system consists basically of two feedback subsystems: (1) the water-level control for the Mocho standpipes, and (2) the water-level control for the storage tanks. Any two of the three pumps at the Mocho pumping station control the water level in the standpipes. Water level in the storage tanks is controlled by opening a valve that causes the Mocho standpipes to drain; gravity feeds water as needed to LLNL from the storage tanks. Alarms, status indicators, and control signals are transmitted via frequency division multiplexed frequency-shift tone equipment. Selector switches, relays, water-level meters, and pilot lights display the data being transmitted and received on a control console in Bldg. 511. Manual commands from the control console can open or close valves at the water-storage tanks, and also start and stop pumps at the Mocho pumping station. The water level in the standpipes and storage tanks is continuously monitored in Bldg. 511. Any abnormal condition, such as a high or low water level in the storage tanks or in the standpipes, or any pump failure, initiates an audible and visible alarm at the control console.

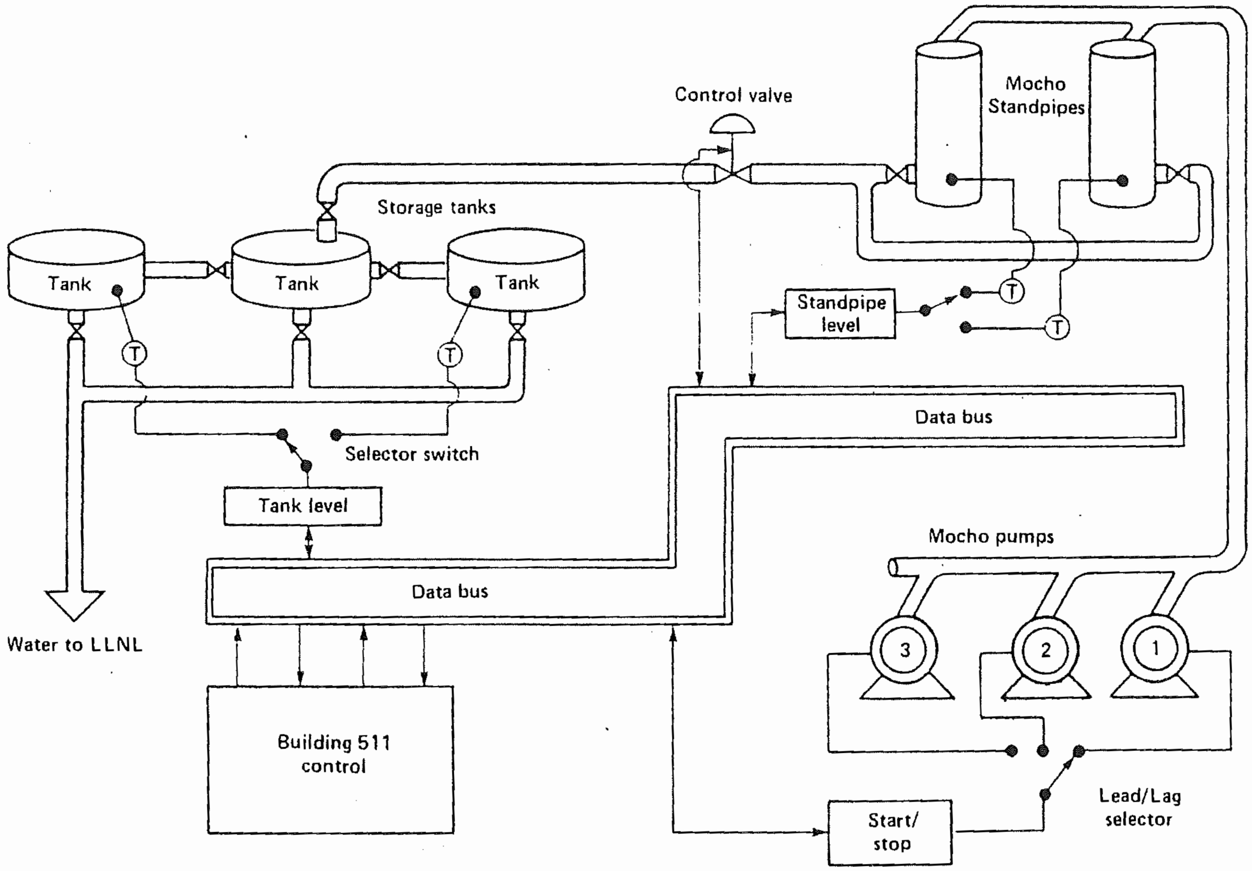


Figure 1. Simplified diagram of the Mocho water-supply system.

ANALYSIS OF THE MOCHO SYSTEM

We first had to understand and model the components of the water-supply control system. Digraph fault-tree analysis uses steps common to traditional fault-tree analysis. In assessing the adequacy of the Mocho water-supply system in the event of a major fire, we found 16 single events that would cause failure of the control loop which monitors storage-tank level. These failures would go undetected in Bldg. 511 because the feedback loop performs both control and detection functions.

We will briefly describe the digraph fault-tree methodology used to arrive at our recommendations.

Water Required to Fight a Major Fire

Based on firefighting experience in the chemical industry, LLNL's Fire Safety Division defined the amount of water necessary to extinguish a major fire on site: a continuous flow-rate of 3500 gallons per minute (gpm) for 4 hours, for a total of 840,000 gallons. In addition to the 1,283,800-gallon capacity of the three storage tanks, standpipes A and B contain 41,992 total gallons, and 180,180 gallons also sit in the line leading from the standpipes. We must also include the make-up capacity of the two Mocho pumps (1 lead and 1 lag) during this 4-hour period. The lead pump, No. 3, has a capacity of 1100 gpm; each of the lag pumps, No. 1 or 2, has a 500-gpm capacity (but only one pump can operate at a time). In 4 hours, the pumps have a total capacity of 1600 gpm, or 384,000 gallons. Therefore, the total capacity of the entire system plus make-up is 1,889,972 gallons. During 1981, the maximum daily water consumption was 950,000 gallons. Subtracting this amount from the Mocho system capacity leaves 939,972 gallons to fight a major fire, which exceeds the recommended 840,000 gallons. If the system is working, an adequate supply of water will be available for the postulated fire.

In the 15 years the Mocho system has been operating, however, the storage tanks have drained dry twice due to human error. Such errors can lead to an inadequate supply of water in the storage tanks, which no one in Bldg. 511 will detect. Since the total of the pump make-up plus the standpipes and the line leading from the standpipes is only 606,000 gallons, at least an additional 234,000 gallons must be in the storage tanks to meet the 840,000-gallon requirement. Therefore, if the level in the storage tanks drops below 234,000 gallons, there may not be enough water to extinguish the fire.

A normal low level in the tanks will generate an alarm in Bldg. 511, and accordingly LLNL personnel will take the appropriate measures, such as activating Zone 7 supplies.

Understanding the Water-Supply System

By touring the entire water-supply system and interviewing LLNL personnel familiar with it, we identified the following information germane to the digraph fault-tree analysis.

To eliminate redundancy, the independent measurement of water level in the storage tanks was removed, leaving only one sensor for three tanks. Pump No. 3, an 1100-gpm pump, is the lead; a 500-gpm pump is the lag. In a No. 3 failure, either No. 1 or No. 2 becomes the lead pump. With No. 3 out of service, the water makeup to the standpipes takes longer but the system can be successfully operated in this mode. The main water valve will not open if either the standpipe is in a low-water-alarm condition or if the water tanks are in a high-water-alarm condition. A spurious signal for condition will cause the main water valve to close, and this results in the storage tanks standing at low level. In the event of a complete failure of the Mocho system, it takes approximately 15 min to cut in the Zone 7 water supply. The existing controls for the Mocho system include over 100 mechanical relays for logic and timing. Understanding the operational sequence of the control system was important to a detailed analysis of its reliability.

Event sequence for storage-level control Water use by LLNL or neighboring Sandia National Laboratories will cause the level in the storage tanks to drop. When the level in the storage tanks drops to approximately 12 ft-6 in., a water-pressure transducer will cause the automatic water valve to open, and water begins to flow from the Mocho standpipes. This water flows into the top of the No. 2 storage tank that is connected to No. 1 and No. 3 through service valves located at the bottom of the tanks. The automatic valve remains open until a water level of about 14 feet is reached in the storage tanks.

Event sequence for standpipe-level control As the automatic valve at the storage tanks open and water begins to flow, the level in the standpipes drops. When the level drops to 12 ft-6 in., the No. 3 pump starts pumping into the top of the No. 1 standpipe, connected by bottom piping to the No. 2 standpipe, from which water flows to the storage tanks. However, water flows through the automatic valve faster than No. 3 can pump, so the water level continues to drop. When the standpipe level reaches 8 ft-8 in., the lag pump automatically starts pumping. The combined output of both lead and lag pump is greater than the amount of water flow through the automatic valve, so the level will now rise again in the standpipe. When the level rises to 12 ft-10 in., the lag pump switches back off. When the automatic water valve at the storage tanks closes, the level in the standpipe rises until it reaches 13 ft-5 in., at which point the lead pump cuts off and everything comes to rest.

Failure Modes and Effects Analysis

With input from LLNL personnel, we performed a detailed Failure Modes and Effects Analysis, FMEA, on the Mocho system. The results from this study provided much of the information to construct the digraph and the fault tree, and the probabilistic evaluation of the fault tree.

SYSTEM DIGRAPH

A digraph is a multivalued logic model useful in constructing fault trees of control systems. The digraph consists of both nodes and edges (or arrows) connecting the nodes. A node represents a process variable and an edge represents the gain or the relationship between the nodes. A Top Event is defined as a deviation or disturbance and is the starting variable in the digraph. In this case, the Top Event is "Insufficient Supply of Water in Storage Tanks and No Detection of Same in Bldg. 511." The digraph is then constructed deductively, similar to constructing a fault tree. The limit of resolution in the digraph is equipment failure, human error, or environmental conditions.

The next step is to find the control loops in the digraph. A synthesis algorithm is devised to construct the fault tree from the digraph. Basically, the algorithm delineates how a control loop can cause or pass a disturbance, resulting in an occurrence of the Top Event.

The advantages of constructing a digraph are that the topology of the system variables is displayed and that the digraph resembles the system schematic; in addition, the digraph can consider multivalued logic and timing. By contrast, a fault tree bears no relationship to the schematic, and cannot effectively consider multivalued logic and timing.

The Preliminary System Digraph

The preliminary system digraph (Fig. 2) shows the structure of the detailed digraph.

The Top Event variable is "Flow rate to LLNL." The cycles in the digraph show the two basic feedback loops: (1) the storage-tank-level-control feedback loop, and (2) the standpipe-level-control feedback loop.

The detected variable in both cases is static pressure and the manipulated variable is flow-rate through the main control valve (for the storage tanks) or through the Mocho pumps (for the standpipes). An arrow from one variable (the independent variable) to the other variable (the dependent variable) indicates that a change in the independent variable causes a change in the dependent variable.

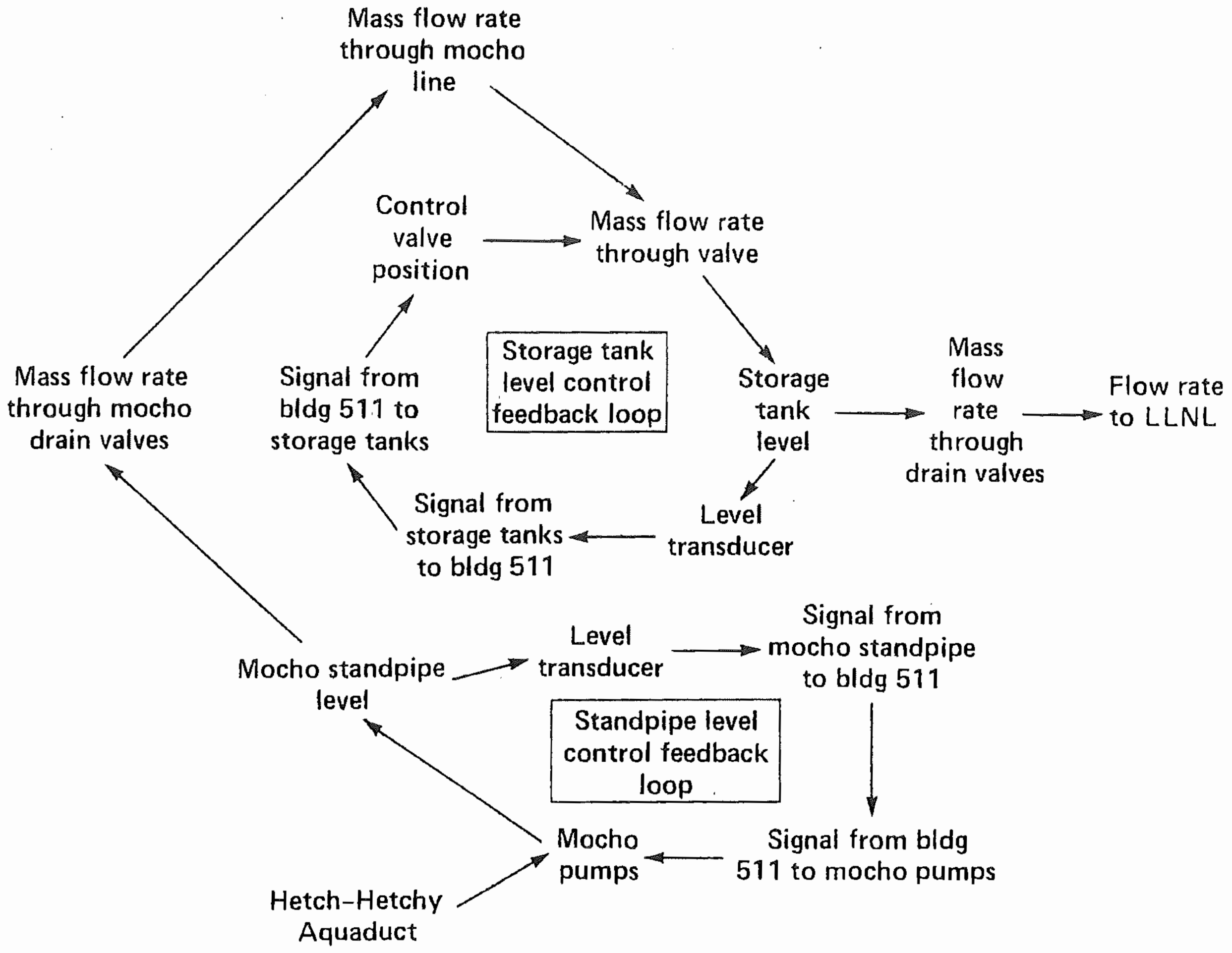

Mass flow rate through mocho line
Control valve position
Mass flow rate through valve
Storage tank level control feedback loop
Mass flow rate through mocho drain valves
Signal from bldg 511 to storage tanks
Storage tank level
Mass flow rate through drain valves
Flow rate to LLNL
Signal from storage tanks to bldg 511
Level transducer
Level transducer
Signal from mocho standpipe to bldg 511
Mocho standpipe level
Standpipe level control feedback loop
Mocho pumps
Signal from bldg 511 to mocho pumps
Hetch-Hetchy Aquaduct

Figure 2. Preliminary system digraph.

The Detailed Digraph

The detailed system digraph is segmented according to sites: the Mocho pumps, the Mocho standpipes, the storage tanks, and Bldg. 511. Each digraph was made using the control system schematic. Because of the magnitude of the detailed system digraphs, only the digraph of the Mocho standpipes is included as an example in Fig. 3.

Events which inactivate control loops as well as the information flow appear with the symbol "0:". In addition, system variables which deviate from their normal values appear in dashed circles. Inactivation events and system disturbances appear as basic events in the fault tree, which is discussed below.

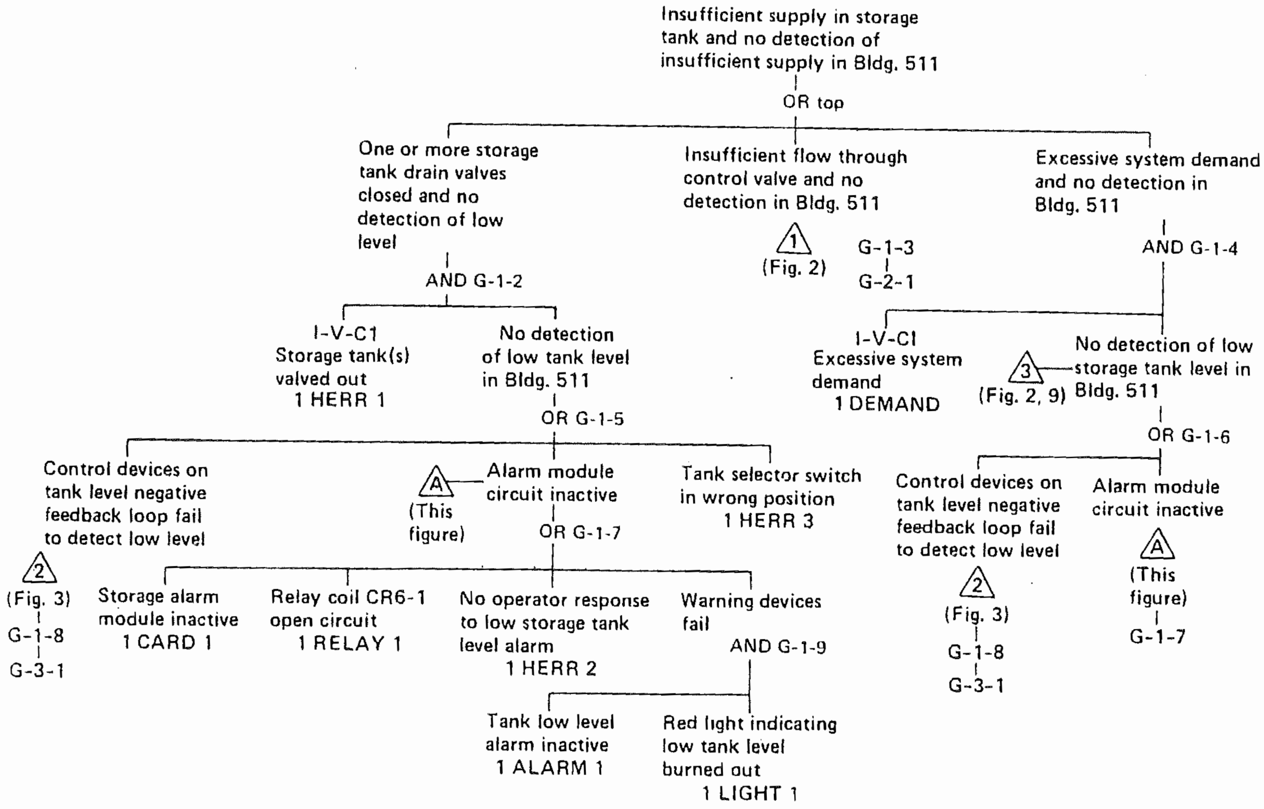

Insufficient supply in storage tank and no detection of insufficient supply in Bldg. 511
OR top
One or more storage tank drain valves closed and no detection of low level
AND G-1-2
Insufficient flow through control valve and no detection in Bldg. 511
1
(Fig. 2)
G-1-3
G-2-1
Excessive system demand and no detection in Bldg. 511
AND G-1-4
I-V-C1
Storage tank(s) valved out
1 HERR 1
No detection of low tank level in Bldg. 511
OR G-1-5
I-V-CI
Excessive system demand
1 DEMAND
3
(Fig. 2, 9)
No detection of low storage tank level in Bldg. 511
OR G-1-6
Control devices on tank level negative feedback loop fail to detect low level
2
(Fig. 3)
G-1-8
G-3-1
A
(This figure)
Alarm module circuit inactive
OR G-1-7
Tank selector switch in wrong position
1 HERR 3
Control devices on tank level negative feedback loop fail to detect low level
2
(Fig. 3)
G-1-8
G-3-1
Alarm module circuit inactive
A
(This figure)
G-1-7
Storage alarm module inactive
1 CARD 1
Relay coil CR6-1 open circuit
1 RELAY 1
No operator response to low storage tank level alarm
1 HERR 2
Warning devices fail
AND G-1-9
Tank low level alarm inactive
1 ALARM 1
Red light indicating low tank level burned out
1 LIGHT 1

Figure 3. Detailed digraph of Mocho standpipes.

Fault-Tree Construction

Since the whole fault tree is 10 pages long, only the first page is displayed in Fig. 4. The causes are displayed for the Top Event:

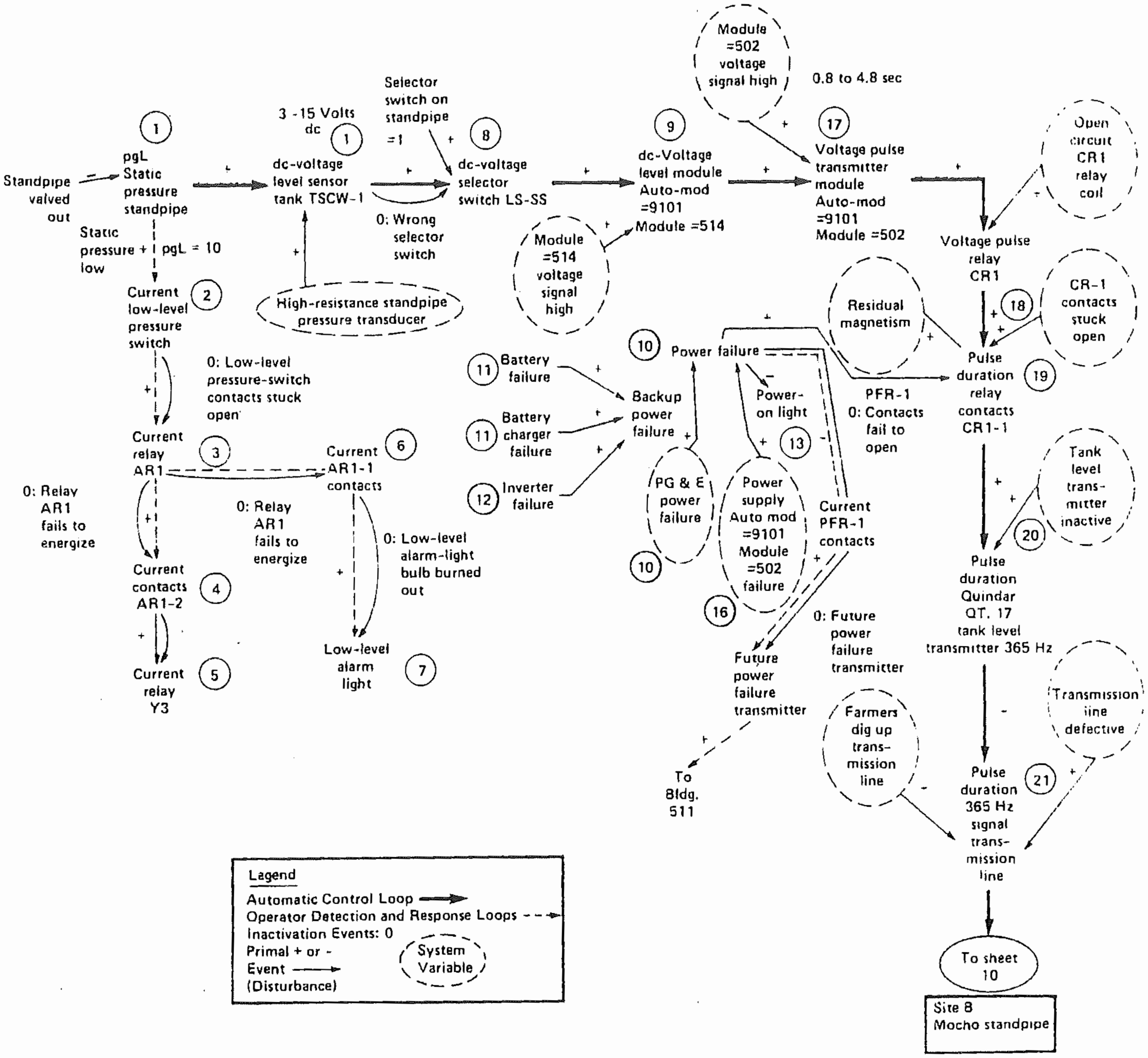
- o one or more storage-tank drain valves closed and no detection of low tank level;
- o insufficient flow through control valve and no detection in Bldg 511.

Only once during the history of the system has a drain valve to a storage tank been closed and the selector switch not been changed to measure the water level in tank No. 1. This event caused the system to drain and, since a full tank was being monitored, simultaneously inactivated the control loop that operates the valve. Consequently, the remaining two tanks drained with no detection in Bldg. 511. The event — excessive system demand — has been included in the fault tree for completeness; however, as described earlier, this event is no longer a possibility and so will be excluded from further consideration.

It is important to note that if the storage-tank-level feedback loop is inactive or out of tolerance, then a Top Event will occur. The feedback loop is used simultaneously to control level in the storage tanks, and also to send a signal to Bldg. 511 in the event of a low level. If the control valve is open, and the loop fails out of tolerance, then the control loop will command the valve to close for a longer period of time than desired, resulting in a low level in the storage tank. If the loop is inactive, the control valve will fail to open when it should, again resulting in a low level in the storage tanks.

A "close all valves" signal can result in the valve being closed for too long. Two things can cause this: a spurious high storage-tank-level signal, or a low standpipe-level signal (which can be a spurious signal, or due to the feedback loop being inactive or out of tolerance, or due to failures that can cause an actual low standpipe level).

Another cause of a low tank level is an insufficient supply from the Mocho pumps.



Standpipe valved out
1
pgL Static pressure standpipe
Static pressure + I pgL = 10 low
Current low-level pressure switch
2
0: Low-level pressure-switch contacts stuck open
Current relay AR1
3
0: Relay AR1 fails to energize
Current contacts AR1-2
4
Current relay Y3
5
3 -15 Volts dc
1
dc-voltage level sensor tank TSCW-1
High-resistance standpipe pressure transducer
Selector switch on standpipe =1
8
dc-voltage selector switch LS-SS
0: Wrong selector switch
Current AR1-1 contacts
6
0: Relay AR1 fails to energize
0: Low-level alarm-light bulb burned out
Low-level alarm light
7
Module =514 voltage signal high
9
dc-Voltage level module Auto-mod =9101 Module =514
Module =502 voltage signal high
0.8 to 4.8 sec
17
Voltage pulse transmitter module Auto-mod =9101 Module =502
Open circuit CR1 relay coil
Voltage pulse relay CR1
CR-1 contacts stuck open
18
Residual magnetism
Pulse duration relay contacts CR1-1
19
PFR-1 0: Contacts fail to open
10
Power failure
Power-on light
13
11
Battery failure
11
Battery charger failure
12
Inverter failure
Backup power failure
PG & E power failure
10
Power supply Auto mod =9101 Module =502 failure
16
Current PFR-1 contacts
0: Future power failure transmitter
Future power failure transmitter
To Bldg. 511
Tank level transmitter inactive
20
Pulse duration Quindar QT. 17 tank level transmitter 365 Hz
Transmission line defective
Farmers dig up transmission line
Pulse duration 365 Hz signal transmission line
21
To sheet 10
Site 8 Mocho standpipe
Legend
Automatic Control Loop
Operator Detection and Response Loops
Inactivation Events: 0
Primal + or - Event (Disturbance)
System Variable

Figure 4. Fault tree of Mocho standpipes.

Note that we do not consider the case of drained Mocho standpipes. This is because a low standpipe level will cause the control valve to close, resulting in a low level in the storage tanks (which means that the fault-tree logic for draining the standpipes will generate non-minimal cut sets, since additional failures must occur to drain the standpipes). However, we do consider draining the pipe leading away from the standpipes, which can occur simply by closing the drain valve in standpipe No. 2. Since the standpipe level is constant in this case, the valve will continue to remain open until the pipe is drained. Note that throughout the fault tree, when a detection loop fails, an AND gate is generated. This is the result of the feed-forward operator described in Lapp and Powers.[2,3]

QUALITATIVE FAULT-TREE EVALUATION

The fault tree contained 98 basic events, and an additional 640 minimal (min-cut) sets. Min-cut sets, also known as the system failure modes, are combinations of basic events which cause the Top Event to occur. The number of min-cut sets according to order is given below (order rèfers to the number of basic events in a min-cut set):

ORDER	1	2	3	4	5	6	7
MIN-CUT SETS	16	19	134	244	163	56	8

The 16 single-event min-cut sets are single failures of control devices on the storage-tank-level feedback loop as described earlier. Of the 98 total basic events, 72 basic events are initiating events, and 26 are enabling events. As described in Dunglinson et al., enabling events inactivate the system's mitigative or protective features but do not cause the Top Event to occur.[4] For example, an inactive alarm or burned-out light does not cause a low level but does fail the operator in the event of an alarm condition. For initiating events, we must compute the frequency of occurrence; for enabling events, we compute the demand unavailability when the initiating event occurs. Reliability data for the 98 basic events were obtained from actual system experience during the last 15 years.

For initiating events, we will assume a fault-duration time of 1 h. This includes the amount of time required for Bldg. 511 personnel to detect and diagnose the cause of failure and to take action after a failure of the Mocho system has occurred. For the Top Event to occur, we will assume no detection in Bldg. 511, although low water pressure will be detected on site. The fault-duration time for enabling events, 0.13 years, corresponds to the average time a failure can exist with an inspection interval of 3 months.

Probabilistic Evaluation of the Fault Tree

We used the computer code IMPORTANCE to evaluate probabilistically the Mocho System fault tree.[5] The following probabilistic measures were computed:

- Frequency of occurrence of initiating events,
- Frequency of occurrence and mean occurrence time when insufficient supply of water exists in the system,
- Unavailability of the Mocho system when a major fire occurs, and
- Ranking of initiating events, enabling events, and min-cut sets according to their probabilistic importance.

Probabilistic importance assesses the quantitative contribution of enabling events, initiating events, and min-cut sets to the Top Event occurrence frequency. A probabilistic ranking according to importance is necessary because it is virtually impossible for an analyst to visually inspect all the min-cut sets and to assess the relative contribution of a component to system failure (<u>viz.</u> the 98 basic events and 640 min-cut sets in the Mocho system fault tree).

Initiating-Event Fault Tree

One fault tree was generated by simply taking the Boolean union of all initiating events. Since there were 72 initiating events, this fault tree generates 72 single-event min-cut sets. Table 1 displays the results of this fault tree. The Top-Event frequency — the number of challenges to the system — is 20.4 per year, which is consistent with historical data. Table 1 also lists the ranking of the initiating events through rank 9. We see that the following events are most important:

- Electric utility (PG&E) power failure.
- Oiler relay failure (to Mocho pumps).
- Noise on transmission line.

We assume that the dominant failure cause of the "close all valves" transmitter is noise on the transmission line.

Table 1 Results from the initiating-event fault tree. The mission time is 15 yrs.

Rank	Basic event description	Importance value	Failure rate per year	Mean fault duration (hr)
1	I-V-C1 PG&E power failure	0.232	5.00	1.00
2	I-P-A2 Oiler failure relay PCW #1	0.155	3.33	1.00
2	I-P-A1 Oiler failure PCW #3	0.155	3.33	1.00
3	I-V-D1 Close all valve transmitter failure on	0.464 E-01	1.00	1.00
3	I-V-D2 Noise on line to control valve transmitter	0.464 E-01	1.00	1.00
3	I-P-D1 Noise on line from standpipe to Bldg. 511	0.464 E-01	1.00	1.00
4	I-P-A2 Control power contacts R3-1 transfer open	0.218 E-01	0.47	1.00
4	I-P-A1 Control power contacts R9-1 transfer open	0.218 E-01	0.47	1.00
5	I-V-C1 High resistance WLT #1 transducer	0.186 E-01	0.40	1.00
5	I-P-B1 High resistance standpipe pressure transducer	0.186 E-01	0.40	1.00
6	I-P-B1 Farmers dig up transmission line	0.155 E-01	0.333	1.00
7	I-P-B1 Power supply Auto-Mod #9109 failure off	0.124 E-01	0.267	1.00
8	I-V-C1 Tank level module voltage high	0.617 E-02	0.133	1.00
8	I-V-D2 Valve module contacts open	0.617 E-02	0.133	1.00
8	I-P-D1 Pump switch module voltage high	0.617 E-02	0.133	1.00
8	I-P-B1 Module #514 voltage signal high	0.617 E-02	0.133	1.00
8	I-P-B1 Module #502 voltage signal high	0.617 E-02	0.133	1.00
8	I-P-A1 PCW #3 motor fails to function	0.617 E-02	0.133	1.00
8	I-V-D2 TCW S-tank level rec card voltage high	0.617 E-02	0.133	1.00
8	I-V-D1 Standpipe level module failure (on)	0.617 E-02	0.133	0.13 yr
8	I-V-D1 Tank level alarm module failure (on)	0.617 E-02	0.133	0.13 yr
9	I-P-A2 Pressure switch out of tolerance	0.311 E-02	0.670 E-01	0.13 yr
9	I-P-A1 Pressure switch out of tolerance	0.311 E-02	0.670 E-01	0.13 yr
9	I-V-C2 2400-Hz receiver fails low	0.311 E-02	0.670 E-01	1.00
9	I-V-C2 Valve stem failure	0.311 E-02	0.670 E-01	1.00
9	I-V-C1 Residual magnetism relay CR1	0.311 E-02	0.670 E-01	1.00
9	I-V-D2 Relay coil CR7 open circuit	0.311 E-02	0.670 E-01	1.00
9	I-V-C1 Open circuit relay CR1	0.311 E-02	0.670 E-01	1.00
9	I-V-D1 CR5-3 contacts close	0.311 E-02	0.670 E-01	1.00
9	I-P-D1 TSCW level receiver voltage high	0.311 E-02	0.670 E-01	1.00
9	I-P-A1 Lead pump receiver failure off	0.311 E-02	0.670 E-01	1.00
9	I-V-C1 Level transmitter fails low	0.311 E-02	0.670 E-01	1.00
9	I-P-D1 CR3-2 contacts transfer open	0.311 E-02	0.670 E-01	1.00
9	I-P-D1 CR1A-1 contacts transfer open	0.311 E-02	0.670 E-01	1.00
9	I-V-C2 Agastat TDR-4 contacts transfer open	0.311 E-02	0.670 E-01	1.00
9	I-V-D2 Flow valve selector switch opens	0.311 E-02	0.670 E-01	1.00
9	I-P-A1 PSR6 contacts transfer open	0,311 E-02	0.670 E-01	1.00
9	I-V-D1 CR2A-1 contacts close	0.311 E-02	0.670-01	1.00

RESULTS OF THE MOCHO SYSTEM FAULT-TREE ANALYSIS

Table 2 lists the system-reliability characteristics of the Mocho system fault tree. We predict that the Mocho system will have an inadequate supply of water to extinguish a major fire on the average of 3.1 times per year. It must be pointed out that this number corresponds only to a low level in the storage and not necessarily to a totally dry condition. Another measure of system adequacy is the demand unavailability of the system in the event of a major fire. The demand unavailability is calculated to be 3.6 x 10^{-4}. Comparing this number to historical data, we see that during the 15-year life of the system, it has been dry twice. If we assume that the system was unavailable for 4 hours each time, this results in a system unavailability of (8 hours x 1 year/8760 hours)(system lifetime/15 years) = 6.1 x 10^{-5} year.

Since this number does not include other times in which the storage tanks might have been low instead of dry, we see that the calculated unavailability, 3.6 x 10^{-4}, agrees reasonably well with the historical data, 6.1 x 10^{-5}. Table 2 also ranks the initiating events through rank 4, which includes the basic events that are single-event min-cut sets. The one exception is PG&E failure, which requires failure of the backup-power supply system as well. These single events are failure of control devices on the tank-level feedback loop, which would go undetected in Bldg. 511.

Table 2. Ranking of most important initiating events with the following conditions: insufficient level in storage tank and no detection; mean time to system failure = 2847.6 h (0.325 year); mean time to system repair = 1.0367 h (0.0432 day); mean fault duration = 1 h.

Rank	Basic Event Description		Importance Value	Failure Rate per Year
1	I-V-D2	Noise on line to control valve transmitter	0.325	1.00
2	I-V-C1	PG&E power failure	0.163	5.00
3	I-V-C1	High resistance to WLT #1 transducer	0.130	0.400
4	I-V-D2	Valve module contacts open	0.0432	0.133
4	I-V-C1	Tank-level module voltage high	0.0432	0.133
4	I-V-D2	TCW storage tank level rec card voltage high	0.0432	0.133

Table 3 ranks the enabling events. We see that failure of components in the backup power supply system (the inverter, battery, and battery charger) are dominant enabling events. The next most important enabling event is failure of the operator in Bldg. 511 to respond to a low-level tank alarm. We assign a probability of 0.01 for this event, which is consistent with data given by Swain and Guttman.[6] Table 3 also ranks the most important min-cut sets. These min-cut sets include the important initiating and enabling events described above.

Table 3. Ranking of most important enabling events, with insufficient level in storage tank and no detection. Ranking is for the enabler (sequential contributory) basic event importance (a measure of interval reliability).

Rank	Basic Event Description	Importance Value	Failure Rate per Year	Mean Fault Duration (h)
1	Inverter failure, storage tank	0.564 E-01	0.267	0.130
1	Battery failure at storage tank	0.564 E-01	0.267	0.130
1	Battery charger failure, storage tank	0.564 E-01	0.267	0.130
2	No operator response to low tank level	0.433 E-02	*0.100 E-01	--
3	Relay coil CR6-1 open circuit	0.377 E-02	0.670 E-01	0.130
3	Storage alarm module inactive	0.377 E-02	0.670 E-01	0.130
4	No operator response to low standpipe level	0.557 E-03	*0.100 E-01	--

*Represents a downward probability.

Based on our analysis, we recommend that each storage tank in the Mocho water-supply system has its own independent water-level sensor. If this is done, we estimate that the probability of system unavailability would decrease by a factor of 50. Restoring this independent measurement would result in no single-event minimal cut sets in which failures would go undetected.

In summary, we feel that the use of the digraph fault-tree methodology enabled us to perform a very detailed, complete, and accurate analysis of the water-supply system. The results seem reasonable because the failure-rate data was derived directly from the system's 15-year operating experience. This general methodology is ideal for the analysis of large and complex systems.

REFERENCES

1. H. K. Hasegawa, N. J. Alvares, A. E. Lipska, H. W. Ford, S. Priante, and D. G. Beason, "Fire Protection Research for Energy Technology Projects: FY 80 Year-End Report," Lawrence Livermore National Laboratory, Livermore, California, UCRL-53179 (1981).

2. S. A. Lapp and G. J. Powers, "Computer-Aided Synthesis of Fault-Trees," IEEE Trans. on Reliability, R-26 (April 1977, pp. 2-13.

3. S. A. Lapp and G. J. Powers, "The Synthesis of Fault Trees," in Nuclear Systems Reliability Engineering and Risk Assessment, J. B. Fussell and G. R. Burdick, eds., SIAM (1977).

4. C. Dunglinson and H. E. Lambert, "Interval Reliability for Initiating and Enabling Events," IEEE Transactions on Reliability, R-32, 2 (1983).

5. H. E. Lambert, "IMPORTANCE: The IMPORTANCE Computer Code," Lawrence Livermore National Laboratory, Livermore, California, UCRL-79529 (1977).

6. Swain and Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," Nuclear Regulatory Commission, Washington, D.C., NUREG-1278 (1983).

KJA

Technical Information Department · Lawrence Livermore National Laboratory
University of California · Livermore, California 94550