ornl

OAK RIDGE NATIONAL LABORATORY

LOCKHEED MARTIN

ORNL/TM-13745

Reliability Review of the Remote Tool Delivery System Locomotor

J. B. Chesser

MANAGED AND OPERATED BY
LOCKHEED MARTIN ENERGY RESEARCH CORPORATION
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

ORNL-27 (3-96)

ORNL/TM-13745

RELIABILITY REVIEW OF THE REMOTE TOOL DELIVERY SYSTEM LOCOMOTOR

J. B. Chesser
Robotics and Process Systems Division
Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, Tennessee 37831-6304
Telephone: (423) 574-6327
Facsimile: (423) 574-5479

Date Published: April 1999

Prepared by the
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831
managed by
LOCKHEED MARTIN ENERGY RESEARCH CORP.
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-96OR22464

CONTENTS

PAGE

ABSTRACT

The locomotor being built by RedZone Robotics is designed to serve as a remote tool delivery (RTD) system for waste retrieval, tank cleaning, viewing, and inspection inside the high-level waste tanks 8D-1 and 8D-2 at West Valley Nuclear Services (WVNS). The RTD system is to be deployed through a tank riser. The locomotor portion of the RTD system is designed to be inserted into the tank and is to be capable of moving around the tank by supporting itself and moving on the tank internal structural columns. The locomotor will serve as a mounting platform for a dexterous manipulator arm. The complete RTD system consists of the locomotor, dexterous manipulator arm, cameras, lights, cables, hoses, cable/hose management system, power supply, and operator control station.

A failure mode and effects analysis (FMEA) and a fault tree analysis (FTA) of the locomotor were performed. The purpose of the analyses was to determine single-mode failures on the in-tank equipment (locomotor) that could cause damage to the tank or cause the equipment to be unretrievable. The FMEA approach includes each individual piece of equipment to determine its failure cause, failure mode, and failure effect. The FMEA results in a table of data. The FTA is a top-down approach, starting with the undesirable final events (tank damage or unretrievable locomotor in this analysis). The FTA results in graphical trees that show the sequence of failures leading to an undesirable event.

The value of these analyses was the determination of means of improving system reliability. Key means of improving system reliability are skilled assembly personnel to ensure proper assembly of the electrical and hydraulic connectors, cleaning and flushing the hydraulic system, routine hydraulic fluid testing, implementing proper procedures for bolted joint assembly, and thorough predeployment testing. The items to be observed in predeployment testing include all hydraulic components for leaks, electrical connectors for continuity, flexible hoses and cabling for crushing or pinching in mechanical components, sensors for correct signal polarity, the rotary unions for leaks or cross-talk between the various hydraulic passages, solenoid coils for excessive temperature, and the kevlar strength member for proper load bearing termination, and valves in enclosed compartments for overheating.

The lack of redundancy in the locomotor became apparent in the locomotor FTA. Several paths to the undesirable final events (tank damage or unretrievable locomotor) require only a single failure. This implies that to have high system reliability, individual components must have a high reliability. There is limited redundancy to compensate for failed components in general. Some components, such as the servo-valves have no redundancy. Note that the lack of redundancy is not accidental but a deliberate design choice on the part of RedZone. Additional redundancy presents additional failure paths. RedZone chose not to have filtration or redundant valving in the locomotor because that could potentially reduce reliability as a result of the higher component count.

If a servo-valve fails, its associated joint fails. This is particularly critical for the grippers. A failure of the gripper lock valving can leave the locomotor permanently stuck in place. There is no provision for an alternate means of releasing the locomotor grippers. Because of the method used to lock the gripper cylinders the only method for removing the locomotor is to remotely cut the cylinder barrel releasing the gripper.

RedZone has asserted that in the event of a valve failure on the positioning joints, the rotary actuators, gripper orientation, or vertical translation, a crude form of redundancy is available by utilizing the remaining functional joints. For example, there are three rotary actuators; if one of the rotary actuator fails, the remaining two can still be used to position the locomotor within the tank in a retrievable position. Compensation for failed positioning joints should be demonstrated in cold testing before relying on that technique.

Finally, a review of operations with hydraulic manipulators at Oak Ridge National Laboratory (ORNL) was performed. This was done to gain insight from actual operational experience with hydraulically actuated manipulators and mobile systems.

The only failure mechanism identified in reviewing operations of ORNL manipulators that had not been identified in the FMEA and FTA of the locomotor is vibration. The camera lightbulbs on the Houdini remotely operated vehicle (ROV) failed due to vibration, vibrating out of their sockets. Houdini is a tracked vehicle developed by RedZone, consequently significant vibration results from the contact and slippage of the tracks with the ground during operation. Vibration should not be a problem on the locomotor because of its method for locomotion; there is no slippage or intermittent contact. This will be confirmed in cold testing.

Hydraulic leaks were a significant problem on the Houdini. Part of this problem can be attributable to the vibration inherent in a vehicle. The solution finally used on Houdini, applying thread-locking compound to the hydraulic connectors, however, can be applied to the locomotor to prevent hydraulic leaks. Significantly, a major source of damage to the Houdini occurred during insertion and extraction through the tank riser. Insertion and retraction operations of the locomotor have not been examined because those procedures have not been developed. It is, however, expected that the locomotor will only be inserted and retracted a few times per tank (two or three times).

Experience with the modified light duty utility arm (MLDUA) showed the importance of regular hydraulic fluid testing. An increase of fluid particulates was detected and corrective action taken before any damage resulted.

Initial shakedown testing revealed problems on both the Houdini and the ORNL developed next generation munition handler (NGMH). The locomotor analyses pointed to initial testing as being significant for preventing failure.

Some remaining issues have not been thoroughly covered in the analyses in this report. Damage to the manipulator or tank occurring during insertion and extraction has not been considered. Certain out-of-tank failures could affect the locomotor. Some combinations of failures could result in the locomotor striking the tank. Evaluating the severity of a tank strike is outside the scope of this report, which is to determine only if damage is possible.

1. INTRODUCTION

The locomotor being built by RedZone Robotics is designed to serve as a remote tool delivery (RTD) system for waste retrieval, tank cleaning, viewing, and inspection inside the high-level waste tanks 8D-1 and 8D-2 at West Valley. The RTD system is to be deployed through a tank riser. The locomotor portion of the RTD system is designed to be inserted into the tank and be capable of moving around the tank by supporting itself and moving on the tank internal structural columns. The locomotor will serve as a mounting platform for a dexterous manipulator arm. The complete RTD system comprises the locomotor, dexterous manipulator arm, cameras, lights, cables, hoses, cable/hose management system, power supply, and operator control station.

This report describes a reliability review of the locomotor portion of the system. The purpose of the review is to determine single-mode failures on the in-tank equipment (locomotor) that could cause damage to the tank or cause the equipment to be unretrievable. A failure mode and effects analysis (FMEA) and a fault tree analysis (FTA) were performed to that end. The FMEA approach includes each individual piece of equipment to determine its failure cause, failure mode, and failure effect. The FMEA result is a table of data. The FTA is a top-down approach starting with the undesirable final events (tank damage or unretrievable locomotor in this analysis) and then determining the root events of the undesirable final events. The FTA result is a series of graphical tree structures with the base of each tree being a single final undesirable event and the branches being the events leading up to the final event. The goals of these analyses were to identify the locomotor failure and to identify actions to mitigate or prevent failures. The primary event of concern in performing the analysis was tank damage; of secondary importance was unretrievability of the locomotor. The analysis considered only the in-tank part of the RTD, the locomotor.

Section 2 of the report briefly describes the locomotor systems. Section 3 of the report describes in depth the FMEA and FTA methodology. Section 4 is a summary of the FMEA and FTA results. Section 5 is a brief discussion of hydraulic manipulator operational experience at Oak Ridge National Laboratory (ORNL) and how this experience applies to the locomotor. Section 6 is conclusions and discussion of steps to be taken to improve reliability, measures that were not taken to improve reliability, and unresolved issues. In the appendix are the FMEA tables, root causes developed from the FTA, the FTA, West Valley's "*Summary Design Criteria*," and RedZone's "*Locomotor Description Document.*"

The purpose of this reliability review is to ascertain soundness of the design of the locomotor, minimizing the possibility of tank damage and maximizing the probability of successful retrieval of the locomotor. Note that there are limitations to this review. Because of the lack of statistical data, survival times of components or failure probabilities are not known. Even with such statistical data the prediction of when a specific component may fail cannot be made. This review is to provide a qualitative assessment of the locomotor design and highlight weaknesses or limitations in the design.

2. LOCOMOTOR SYSTEM DESCRIPTION

The locomotor is briefly described in this section. The description given here is cursory because a more complete description is available in Appendix D in RedZone's "*Locomotor Description Document.*" The RTD locomotor is a three-joint planar work platform that operates attached to a deployment mast or the tank pipe columns. The major locomotor components are grippers, links, rotary joints, vertical translator, hydraulic system, dexterous manipulator, and video system. Schematics of the hydraulic system and the wiring harness are on the following pages.

1. Gripper mechanism: The gripper secures the locomotor to the deployment mast or to the internal tank columns when the locomotor steps off the deployment mast.

2. Link: A link connects two of the locomotor joint rotary actuators on the RTD locomotor. The link provides an attachment point for the tether, a structural connection between the rotary actuators, and a distribution path for wiring and hydraulics.

3. Rotary joint: Three rotary joints are used in the locomotor. Each rotary joint is a modular assembly containing a rotary vane actuator, bearings, and a resolver for position sensing.

4. Vertical translator: The vertical translation mechanism enables changing the height of the locomotor in the tank. It provides ± 6 inches of vertical travel. An LVDT provides operator feedback on the mechanism position.

5. Hydraulic system: The locomotor hydraulic system, in conjunction with the control electronics, provides the motion of the locomotor joints.

6. Dexterous manipulator: A dexterous manipulator is mounted on the locomotor link to perform work in the tank. The manipulator is a Schilling Titan T3.

7. Video system: Five black and white camera and light assemblies are used on the locomotor. Two cameras are mounted on each gripper, and one on the manipulator.

3. ANALYSIS METHODOLOGY

The purpose of the reliability analysis is to determine single mode failures on the in-tank equipment (locomotor) that could cause damage to the tank or cause the equipment to be unretrievable. An FMEA and a FTA were performed. The FMEA approach includes each individual piece of equipment to determine its failure cause, failure mode, and failure effect. The result of the FMEA is a table of data. The FTA is a top-down approach starting with the undesirable final events (tank damage or unretrievable locomotor in this analysis) and then determining the root events of the undesirable final events. The result of the FTA is a series of graphical tree structures with the base of each tree being a single final undesirable event and the branches being the events leading up to the final event. The goals of these analyses were to identify the locomotor failures and to identify actions to mitigate or prevent failures. The two events of concern in performing the analysis were tank damage and unretrievability of the locomotor. The analysis considered only the in-tank part of the RTD system, the locomotor.

3.1 FAILURE MODES AND EFFECTS ANALYSIS

The FMEA is an inductive analysis method (i.e., generates general conclusions from individual instances) utilized to systematically study the causes and effects likely to affect the components of a system. FMEA is a "bottom-up" analysis that begins at the lowest level of detail, and components and works upward to system-level faults, assessing the cause and effect of each failure mode of each component of a system. The FMEA produces a detailed description of how failures of individual components influence system behavior. The results obtained from this analysis method are qualitative in nature. As a minimum, the output from the analysis is a table listing individual components, the failure causes, failure modes, and the consequences of the individual failure modes. The FMEA included input and review by RedZone Robotics and West Valley Nuclear Services. The procedure for performing an FMEA is outlined below.

1. Each component in your system is identified. Overlooking a component or one of its failure modes in a critical safety area may render the entire exercise useless, so it is necessary to be systematic and thorough.
2. The functions that each part of the system performs are identified.
3. List separately the failure modes for each of the functions identified in the second step. A failure mode is best described as a simple two-word statement of how the function may fail to be performed. Failure modes are described by stating what the product "does" or "does not do" when it fails.
4. Identify the possible cause of the failure mode. The causes can be internal (e.g., mechanical defect) or external (e.g., failure of power supply) to the component.
5. Describe the effects that each failure mode of that component would have. The effects should be described in enough detail so that the severity of the effects can be judged.

There are many variations of the form utilized for FMEA analysis. The particular form used for the locomotor analysis included the following seven columns:

- Item: any level of hardware assembly (i.e., part, subsystem, and system). Some components, such as hydraulic hoses or the electrical cabling, were treated in aggregate at a system level. *Only in-tank items were considered in the FMEA.*
- Function: the purpose performed by an item.
- Failure cause: potential internal and external causes that could prevent the item from performing its intended function.
- Failure mode: how the item has failed (e.g., failed open or failed close).
- Consequence: the result of the failure.
- Prevention/detection/mitigation: steps that can be taken to prevent, detect, or reduce the severity of a failure. Prevention and mitigation steps are action items to be taken by RedZone in design or assembly, and operational procedures are to be implemented by West Valley Nuclear Services.
- Comments: clarification, explanation, or documentation of information in the other columns.

The FMEA is simply a formalized, systematic practice of common engineering sense. It categorizes and documents the considerations every good engineer always considers:

- What happens if this breaks?
- How can it break?
- What can I do to prevent it from breaking?
- What risk is involved?
- How shall I defend my design in light of established practices and the state of the art?

3.2 FAULT TREE ANALYSIS

FTA is a deductive system analysis because it constitutes reasoning from the general to the specific. The system is postulated to fail in a certain way, and branches of more basic faults contributing to the undesired event are developed systematically. In summary, inductive methods are used to determine what system states are possible, and deductive methods are used to determine how a system state can occur, where the system states of interest are usually failed states. Deductive reasoning is used to identify the primary or top event or events to be evaluated as well as the contributory events that could cause the *top event*. For safety analyses, top events usually have significant undesirable consequences. An undesired state of a system is specified as the top event, and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur.

A fault tree is a graphical logic diagram that shows the cause and effect relationship between contributory factors and the top event of interest. A set of event symbols is used to depict the cause-effect relationships. Causative events are referred to as input events and are located before a logic gate. The resulting event is referred to as the output event and is located after the logic gate. This cause and effect relationship is carried from the top event down to the level of component failures or external events. The top event, which serves as the starting point for the whole analysis, corresponds to an unwanted result such as a deterioration of the performance characteristics of the system or a change in function causing a hazard to the environment. Each different top event requires its own specific tree. A FTA that does not consider the right top events is useless.

FTA was initially developed to determine quantitative probabilities of top events, but it is also useful for qualitative analyses because of the systematic way that the various contributing factors are presented. A qualitative analysis is always necessary to structure a fault tree before a qualitative analysis can be performed. The efforts to determine, assign, and calculate probabilities are not always warranted. Because of the lack of statistical data for the locomotor components, only a qualitative analysis was performed. The goal of the qualitative analysis was to uncover all the root causes (contributory events) of the top events under consideration.

Selection of the top event or events is the first step in the construction of a fault tree. For the analysis of the locomotor *only two top events were considered: an event potentially causing tank damage, and the locomotor being unretrievable.* The qualifier *potentially* is used because the severity of event required to damage or breach a tank was not quantified for the purposes of this study. The contributory events that could cause the top event are then drawn after the top event as branches. They are separated from the top event by logic gates. Contributory events are then subjected in turn to the same process as the top event. The bottom level of each completed branch, a primary event, is a component failure, an error or other initiating event. Although only the in-tank portion of the RTD—the locomotor—was under review, some out-of-tank primary events (root causes) were identified. These events were not analyzed further for their contributory events (root causes).

The symbols used in fault trees can be grouped in the categories below. A graphical key to the symbols used in the locomotor analysis is shown in Figure 1.

3.2.1. Primary Event Symbols

Primary events are events that have not been developed further. Probabilities of primary events must be provided if the fault tree is to be used to compute the probability of the top event. There are four types of primary events:

- The Basic Event: The circle describes a basic initiating event. No further development is required. The appropriate limit of resolution has been reached.
- The Undeveloped Event: The diamond describes a specific fault event that is not developed further either because the event is inconsequential or because relevant information regarding the event is not available.
- The Conditioning Event: The ellipse is used to record any conditions or restrictions that apply to a logic gate. It is used primarily with the INHIBIT and PRIORITY AND gates.
- The External Event: The house symbol is used to signify an external event that is normally expected to occur and thus is not of itself a fault.

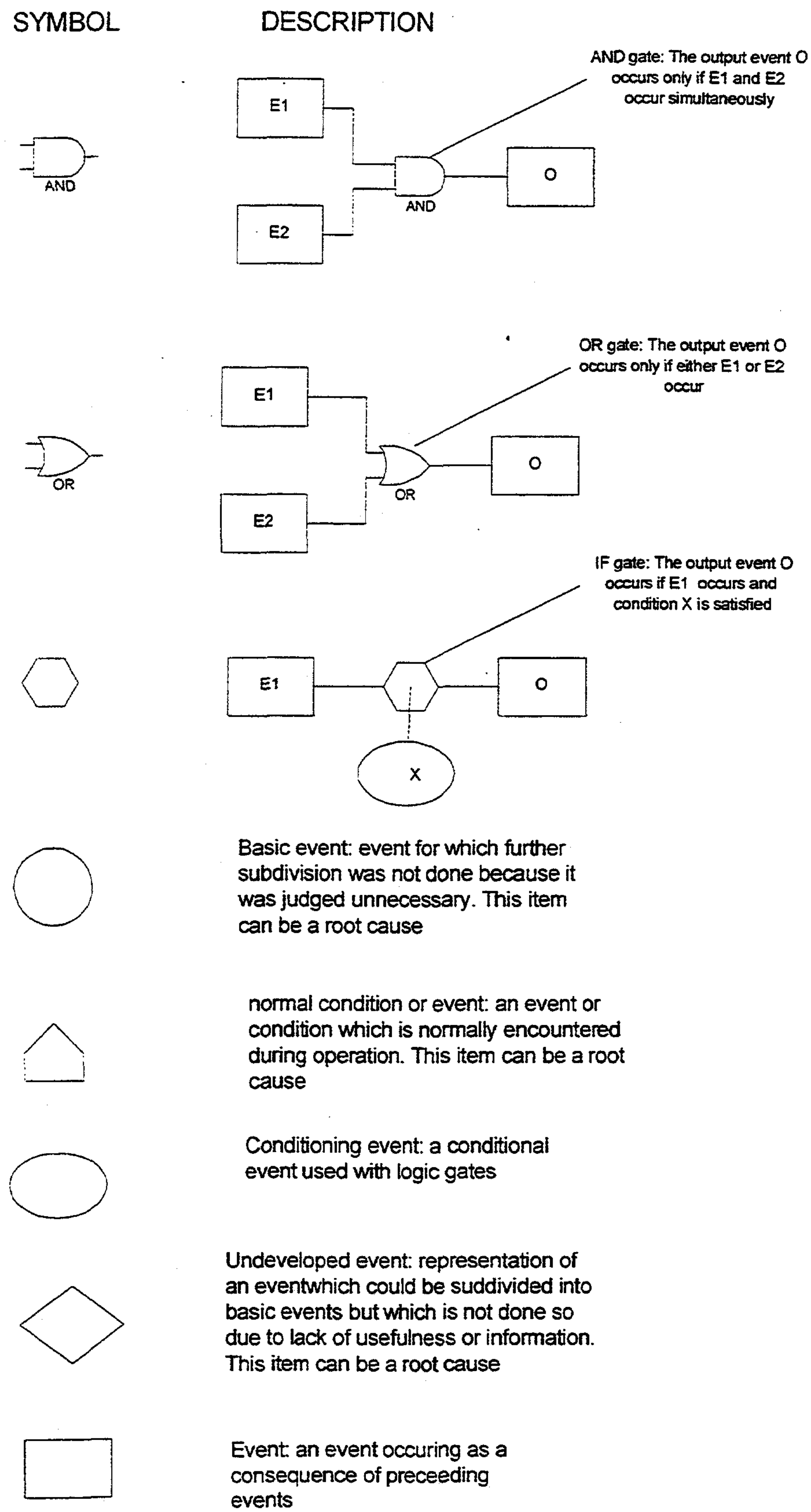


Fig. 1. Fault tree analysis symbols.

3.2.2 Intermediate Event Symbol

An intermediate event is a fault event occurring because of one or more antecedents' causes acting through logic gates. All intermediate events are symbolized by a rectangle.

3.2.3 Gate Symbols

There are two basic types of fault tree gates: the OR gate and the AND gate. Other gates are special cases of these two basic types.

- The OR Gate: The OR gate is symbolized by a shield with a curved base; it is used to show that the output event occurs only if one or more of the input events occur. Any number of input events may lead into an OR gate.
- The AND Gate: The AND Gate is symbolized by a shield with a flat base; it is used to show that the output fault occurs only if all the input faults occur. Any number of input events may lead into an AND gate.
- The INHIBIT Gate: The INHIBIT gate, represented by a hexagon, is a special case of the AND gate. The output is caused by a single input, but some qualifying condition must be satisfied before the input can produce the output. This qualifying condition is a conditional input, which is identified within an ellipse connected to the INHIBIT gate. The output condition occurs only if the input occurs under the condition specified by conditional input.

The two gates below are described for completeness but were not utilized in the locomotor analysis:

- The EXCLUSIVE-OR Gate: The EXCLUSIVE-OR gate, represented in one of the two ways indicated above, is a special case of the OR gate in which the output event occurs only if exactly one of the input events occurs. The quantitative difference between the inclusive and exclusive OR gates is generally insignificant, so the distinction is not usually needed.
- The PRIORITY-AND Gate: The PRIORITY-AND gate is a special case of the AND gate in which the output event occurs only if all input events occur in a specified ordered sequence.

Once a complete fault tree is constructed, it should indicate all the factors, events and interrelationships leading to the top event. The fault tree can be used either quantitatively or qualitatively to indicate where corrective actions could be taken. Quantitatively, the fault tree can be broken down into cut sets to determine the probability of the top event occurring. A cut set is the minimum sequence leading to the top event. Boolean logic and algebra are used to calculate this probability. The probabilities of each cut set sequence must be known to determine the probability of the top event. Quantitative fault trees to determine probabilities of occurrence of top events are generally costly. Statistical data may not be available for all significant events. Most of the benefits of fault trees derive from qualitative analysis. They can be used to ensure that single-point failures are not possible for critical systems and can provide an indication of the relative safety of a product or system.

Qualitatively, each bottom event can be evaluated in turn to determine where corrective measures could be taken. Checking the number of AND gates present in the fault tree can provide a quick evaluation of relative reliability. The AND gates are indicative of the need for all input conditions to be present to cause the output condition. The probability of the output condition is the product of the probabilities of the input condition. Conversely, the presence of many OR gates may be indicative of a relatively unsafe design because only one input condition is needed to cause the output condition. The probability of the output condition is the sum of the probabilities of the input conditions for an OR gate.

4. ANALYSIS SUMMARY

The full analysis results, the FMEA table is in Appendix A and the fault trees are in Appendix B. Some key results from the analyses are summarized here: predominant failure causes and key actions to be taken to prevent failure.

4.1 FMEA SUMMARY

The FMEA format utilized for the locomotor analysis included the following columns:

- Item: any level of hardware assembly (i.e., part, subsystem, system). Some components, such as hydraulic hoses or the electrical cabling were treated in aggregate at a system level. *Only in-tank items were considered in the FMEA.*
- Function: the purpose performed by an item.
- Failure cause: potential internal and external causes that could prevent the item from performing its intended function.
- Failure mode: how the item has failed (for example: failed open or failed close).
- Consequence: the result of the failure.
- Prevention/detection/mitigation: steps that can be taken to prevent, detect, or reduce the severity of a failure. Prevention and mitigation steps are action items to be taken by RedZone in design or assembly, and operational procedures are to be implemented by WVNS.
- Comments: clarification, explanation, or documentation of information in the other columns.

The two primary failure causes are improper assembly of electrical and hydraulic connectors and debris/dirt in hydraulic fluid. These two failure causes are common to a significant number of components. Some assumptions made in the FMEA must be noted. Radiation was discounted as a significant failure cause because of the use of radiation-resistant materials. The assumption of negligible radiation-induced failures may be negated if the in-tank life of the locomotor is extended past the design dose of 10 Mrad. The design dose rate was established by WVNS. Refer to "Summary Design Criteria Document for RTD System" in the Appendices. The FMEA did not look at the effect of failures of out-of-tank components on the locomotor (the in-tank portion of the system). Finally, defective design was largely ignored as failure cause. Poor design could cause any of the components to fail. Examples of defective design include undersized structural members for the loads encountered or improper tolerance.

The primary means of improving system reliability, as determined in the FMEA study, are skilled assembly personnel to ensure proper assembly of the electrical and hydraulic connectors, cleaning and flushing the hydraulic system, routine hydraulic fluid testing, proper procedure for bolted joint assembly, and thorough predeployment testing. The items to be observed in predeployment testing include: all hydraulic components for leaks, electrical connectors and the wiring harness for continuity, flexible hoses and cabling for crushing or pinching in mechanical components, sensors for correct signal polarity, the rotary unions for leaks or cross-talk between the various hydraulic passages, solenoid coils for excessive temperature, and the kevlar strength member for proper load bearing termination.

4.2 FAULT TREE SUMMARY

The fault tree was generated for qualitative analysis. No attempt was made to determine quantitative failure probabilities. Selection of the top event or events is the first step in the construction of a fault tree. For the analysis of the locomotor only two top events were considered: an event potentially causing tank damage and the locomotor being unretrievable. The qualifier *potentially* is used because the severity of event required to damage or breach a tank was not quantified for the purposes of this study. The contributory events that could cause the top event are then drawn after the top event as branches. Because this was a qualitative analysis some liberty was taken in the definition of the primary events.

The strict definition of an event is an occurrence that causes a change in the system state. An example of an event, taken from the locomotor analysis, is valve spool sticking. This event changes the state of a valve from operative to inoperative. The definition of event was expanded for the FTA performed on the locomotor. Failure mechanisms were included in the fault tree. A failure mechanism is the process involved in the cause of the failure. An example of a failure mechanism, taken from the locomotor analysis, is fatigue. The reason for expanding the fault trees to include mechanisms was to allow identification of the root causes that could lead to locomotor failure.

A summary of primary events, including failure mechanisms, is given in Table 1. Along with the primary events, preventive measures to be taken are listed. The preventive measures were taken from the FMEA table. These measures are action items to be taken by RedZone in design or assembly and operational procedures to be implemented by West Valley Nuclear Services. A few of the primary events are related to failures of items outside the hot area and were not addressed in either the FMEA or FTA and have no preventive measures listed.

One noticeable feature of the fault trees is a lack of redundancy. Most of the branches coming out of the top events have only OR gates. Very few branches have AND gates. This implies that to have high system reliability, individual components must have a high reliability. There is only very limited redundancy to compensate for failed components in general.

Components, such as the servo-valves have no redundancy. It should be pointed out that the lack of redundancy is not accidental but a deliberate design choice on the part of RedZone. Additional redundancy presents additional failure paths. RedZone chose not to have filtration or redundant valving in the locomotor because that could potentially reduce reliability as a result of the higher component count. A comparison of the design approach chosen by RedZone to other approaches, which include redundant components, was not performed.

If a servo-valve fails, its associated joint fails. This is particularly critical for the grippers. A failure of a gripper lock control valve can leave the locomotor permanently stuck in place. There is no provision for an alternate means of releasing the locomotor grippers. RedZone has been requested to provide a plan on how to release the locomotor grippers remotely in the event of a gripper failure.

RedZone has asserted that in the event of a valve failure on the positioning joints, the rotary actuators, gripper orientation, or vertical translation, a crude form of redundancy is available by utilizing the remaining functional joints. This redundancy was not accounted for in the FTA. For example, there are three rotary actuators, should one of the rotary actuators fail the remaining two can still be used to position the locomotor within the tank to position it in a retrievable position. Compensation for failed positioning joints should be demonstrated in cold testing before relying on that technique.

RedZone has added a redundant signal path for energizing all the limp valves simultaneously. This redundant signal path has not been included in the FTA. It is not indicated for the following reasons: it does significantly affect the recommendations of the study and failure to energize the limp valve solenoids does not contribute to either of the top events under consideration.

A failure cause was discovered in the FTA that had not been uncovered in the FMEA. In identifying all the failure causes of the hydraulic valves in the fault trees, overheating of the hydraulic valves due to a potential lack of cooling was discovered. The valve coils are rated for temperatures over 240°F. Maintenance of temperature within valve coil rating can be determined during predeployment testing.

Table 1: Primary failure events developed from the FTA and preventative steps.

Primary events developed from fault tree analysis	Prevention
excessive coil current to hydraulic valves	not addressed in this analysis: this failure located outside the hot area
radiation degradation of organic materials: seals, insulators	seals and insulators are radiation resistant
hydraulic fluid incompatible with elastomers	elastomers selected to be compatible with hydraulic fluids
particulate contamination of hydraulic components	filtration in the HPU
grit on exposed hydraulic actuator rods	wiper seals
water contamination of hydraulic fluid	desiccant breather to prevent air moisture being drawn into fluid, high pressure hydraulic line next to water rinse line in rotary unions to prevent water leakage into hydraulic fluid, regular testing of hydraulic fluid to detect water contamination
exposure of hydraulic fluid to humidity in air	desiccant breather to prevent air moisture being drawn into fluid
excessive hydraulic fluid temperature	hydraulic fluid cooling
initial particulate contamination of hydraulic fluid	filtering hydraulic fluid during fluid transfer to HPU
hydraulic filter initially dirty	unlikely event; its risk can be minimized by periodic fluid testing
cabling pinched in moving components	predeployment testing
cable flexing	predeployment testing
cyclic mechanical loading of electrical connectors (dependent on joint, wire to connector, quality)	predeployment testing
poor environmental sealing of electrical connectors	hydraulic fluid is not conductive, all electrical connectors are inside sealed cavities inside the arm
high temperature exposure of electrical connectors	the only heat source is the hydraulic fluid, the hydraulic fluid is cooled
hydraulic pressure pulses	the arm has low kinetic energy and low flow rates preventing large pulses when valves are suddenly closed
hydraulic hose pinched between mechanical members	predeployment testing
improper hydraulic connector assembly	skill of the craft during assembly, predeployment testing
washdown/decontamination fluids incompatible with elastomers	elastomers selected to be compatible with fluids
damage of seals during assembly	skill of the craft during assembly, predeployment testing
failure of servo-valve driver electronics	not addressed in this analysis: this failure located outside the hot area. Potential for tank damage, however, is limited by the low velocity (low kinetic energy) of the system
failure of resolver driver electronics	not addressed in this analysis: this failure located outside the hot area. Potential for tank damage, however, is limited by the low velocity (low kinetic energy) of the system
compromised gasket or boot	Skill of craft during assembly, predeployment testing

Table 1 (Cont.'): Primary failure events developed from the FTA and preventative steps.

Primary events developed from fault tree analysis	Prevention
joint error checking software	not addressed in this analysis: this failure located outside the hot area. Potential for tank damage, however, is limited by the low velocity (low kinetic energy) of the system
gripper interlock relay failure	this failure located outside the hot area, however, RedZone has designed the relay system to require multiple failures
operator inadvertently releasing both grips	this event while a root cause must occur in conjunction with another event in order to cause a failure
a single grip insecurely placed on a pipe	this event while a root cause must occur in conjunction with another event in order to cause a failure
tether failure resulting in loss of electrical signal or hydraulic power	tether is equipped with a kevlar strength member to provide a load path, wiring in the tether is spiraled to minimize wiring stresses, aside from bending loads the hoses are not loaded
inadvertent activation of take-up spool stressing kevlar strength member	administrative control at WVDP to not permit retraction of tether unless decon spray is operating (keylock control), hardware failures that could lead to this failure were not analyzed
uncontrolled swing of locomotor during insertion	insertion plan not yet developed, further analysis not possible at this time
manipulator drops load	load carrying capacity of manipulator procedurally limited, limiting risk to tank
manipulator falls off locomotor	possibility of manipulator falling off is addressed by steps to prevent bolt failure
uncontrolled move of manipulator	not addressed in this analysis: this failure is outside the scope of this study which was limited to the locomotor
fatigue failure	the system has a low cycle life (<20,000 cycles)
structural component corrosion	components are plated and painted to minimize corrosion
structural component weld failure	the only structural welds are on the gripper cylinder barrels, the welds are plated to minimize corrosion
bolt failure	bolts are assembled with lockwashers, torqued to specification, and loctited, there will be QA steps in place to ensure proper assembly and documentation of assembly
locomotor positioned near tank wall	This event while a root cause must occur in conjunction with another event in order to cause a failure. The locomotor operates at low velocities and hence has low kinetic energy to be absorbed in the event of a tank strike
structural overload	locomotor was designed with a factor of safety, the locomotor operates in a controlled environment minimizing the possibility of a structural overload
excessive temperature in solenoid coil environment (explanation: some of the solenoid coils are in enclosed cavities and subject to poor cooling)	Predeployment testing, coils are rated to an excess of 230 °F
Solenoid valve fuse fails to blow	Fuse failing to blow is judged to be unlikely. Fuse failure to blow has to occur with an overcurrent condition to damage valve

5. HYDRAULIC MANIPULATOR OPERATIONAL EXPERIENCE AT OAK RIDGE NATIONAL LABORATORY

Operational experience of three hydraulic manipulators at ORNL is briefly summarized to provide insight into potential problems. The operational histories have been edited and summarized to highlight issues that are of concern to the locomotor. These summaries are not comprehensive of all the failures that occurred to the manipulators.

The three manipulators are the modified light duty utility arm (MLDUA), the Houdini remotely operated vehicle, and the next generation munition handler (NGMH). The MLDUA is a multi degree-of-freedom long-reach hydraulic arm utilized for waste cleanup operations at the Oak Ridge gunite tanks. The MLDUA was designed by SPAR aerospace. The Houdini is a tethered, hydraulically powered, track-driven vehicle. It is a remotely operated vehicle (ROV) and features a folding chassis to allow it to be introduced through tank penetrations. Houdini carries a bulldozer blade and a Schilling manipulator for performing work. RedZone designed the Houdini vehicle. The NGMH is an arm and vehicle combination designed for loading munitions onto aircraft. The NGMH was designed by ORNL. Both the MLDUA and the Houdini were designed for remote handling and have seen operational use. The NGMH was designed as a proof-of-concept demonstration for improving hands-on operations.

5.1 MLDUA OPERATION SUMMARY

As of November 1998, the MLDUA has logged 2860 hours in a waste tank. The accumulated surface dose to the MLDUA is 6750 rads. To date the only problems with the in-tank portion of the MLDUA, the arm itself, were a short in the wrist roll motor resulting in intermittent function of the wrist roll joint and small hydraulic leaks. The exact location of the short is unknown. The major joints of the MLDUA are hydraulic. The wrist roll, however, is electrical. The loss of reliability of the wrist has not impeded operations.

The hydraulic fluid of the MLDUA is regularly tested. There was a point during operations when the fluid particulate count spiked sharply for unknown reasons. The fluid filters and other filters were changed. The particulate count returned to its normal range and operations resumed.

5.2 HOUDINI OPERATION SUMMARY

The Houdini ROV has been used extensively for sampling, sluicing, and plowing. The maintenance required to the Houdini during the W-3 and W-4 tank cleanup campaigns is summarized.

During initial testing there were problems with loose connector pins on the tether end of the camera connector. The pins had not been crimped or soldered by the manufacturer. This problem was discovered during cold testing.

The most prevalent problem has been leaking or damaged hydraulic connectors and hoses and damaged electrical cables and connectors. The connectors and hoses have been damaged or loosened when the vehicle is folded for retraction or deployment. Vehicle-mounted and wrist-mounted cameras were damaged during insertion and retraction. In addition, the wrist camera powers and signal cable was cut during a retraction. A request was made to RedZone to route the wrist camera cable inside the Schilling Titan III manipulator for the next generation Houdini system. Because much of the damage to the vehicle occurred during retraction and deployment, a concerted effort was made to reduce the frequency of those operations.

During operations in tank W-3 hydraulic leaks were a significant problem. A full shift rarely went by without a hydraulic leak. Toward the end of operations in tank W-3 the Houdini was retrieved, and a series of repairs was performed. All the hydraulic lines were inspected, and all the connectors were tightened. The wrist camera lightbulbs had vibrated loose and were reinstalled. New azimuth limits were set for the onboard Schilling manipulator to keep it from putting stress on the hydraulic lines. Finally, all hoses were wire-tied to keep them from interfering with the vehicle frame opening and closing. Applying thread locking compound appears to have stopped the hydraulic leaks or reduced them to an acceptable level because there is only one mention of leaks in the tank W-4 performance assessment.

Two incidents in Houdini operations stand out. On October 17, 1997, in tank W-3 the shoulder bolt that secured the frame-folding cylinder fell out. The operator was able to fold the vehicle using the track drives. There was no indication that the bolt or threads had been damaged. The millwrights had been requested to use thread-locking compound on all bolts and to tighten them during maintenance activities. There was no documentation that this particular bolt had been tightened. Procedures were changed to include sign-offs.

On December 9, 1997, on initial deployment into tank W-4 it became apparent that the left track was not operating properly. The track did not operate at full speed and would periodically stall. The problem was traced to a broken wire in a servo-valve connector. The connector had failed. The connector on the servo-valve was not the original military style circular connector but a plastic Molex connector. The connector style had been changed because of the limited space in the vehicle body.

5.3 NGMH OPERATION SUMMARY

The NGMH was designed solely as a technology demonstrator. It was designed to demonstrate improved ammunition loading. It is a large hydraulic arm capable of handling payloads of up to 2500 lb. The arm was initially mounted on a floor stand and powered by a remote hydraulic power unit (HPU). After initial testing, the arm was mated to a vehicle and powered by the vehicle hydraulic system. The total operating life of the system is currently less than 500 hours.

During initial testing, after 40 hours of operation, debris left in the HPU reservoir, presumably by the HPU vendor, were ingested by the pump. The pump was destroyed, and the downstream filter cartridge ruptured. The filter cartridge was ruptured despite its 3000 psi rupture rating.

Shortly after this incident, O-rings in sandwich valves were ingested by the servo-valves, requiring overhaul of the servo valves. This failure was traced to improperly sized O-rings.

The vehicle uses hydraulic motors for its propulsion. The front wheel-pods can be extended to widen the wheelbase for stability. During maintenance it was discovered that the hoses to the front wheel-pods were getting snagged during retraction and extension of the wheel-pods. The outer rubber sheathing had been ripped off the hoses, exposing the inner wire braid.

5.4 IMPLICATIONS OF ORNL OPERATIONAL HISTORY TO THE LOCOMOTOR

The only failure mode identified in reviewing operations of Oak Ridge manipulators that had not been identified in the locomotor analyses is the vibration failure of the camera lightbulbs on the Houdini vehicle. The Houdini was a tracked vehicle, resulting in significant vibration from the contact and slippage of the tracks with the ground during operation. Vibration should not be a problem on the locomotor because of its method for locomotion; there is no slippage or intermittent contact. This should be confirmed in cold testing.

Initial testing revealed problems on both the Houdini ROV and NGMH. Initial testing is a recurring item in the locomotor analyses for preventing failure. Hydraulic leaks were a significant problem on the Houdini ROV. Part of this problem can be attributed to the vibration inherent in a vehicle. Applying thread-locking compound to the hydraulic connectors solved the problem on the Houdini. This technique can also be applied to the locomotor to prevent hydraulic leaks. Significantly, a major source of damage to the Houdini occurred during insertion and extraction through the tank riser. Insertion and retraction operations of the locomotor have not been examined because those procedures have yet to be developed. It is expected that the locomotor will only be inserted and retracted two or three times per tank. Careful planning and testing will help mitigate problems associated with the insertion and retraction operations.

The importance of regular hydraulic fluid testing is shown in the MLDUA experience. An increase of fluid particulate was detected, and corrective action was taken before any damage could result. It is recommended that WVNS initiate a regular fluid-monitoring program.

6. SUMMARY OF RESULTS

This section gives a summary of the review of the reliability of the locomotor portion of the Remote Tool Deployment System. In this review some important assumptions were made. These assumptions will be restated. First, the FMEA considered only the in-tank components of the locomotor. Failures of out-of-tank components that could cause failures to propagate to in-tank components were not included. Second, the FTA considered only two events: tank damage and the locomotor being unretrievable.

In this summary the findings based upon the analysis of RedZone's locomotor are discussed. Also discussed are findings based on a review operational experience at ORNL, which are applicable to the locomotor. The value of these analyses and review was the determination of means of improving system reliability.

Key means of improving system reliability are: skilled assembly personnel to ensure proper assembly of the electrical and hydraulic connectors, cleaning and flushing the hydraulic system, routine hydraulic fluid testing, proper procedure for bolted joint assembly, and thorough predeployment testing. The items to be observed in predeployment testing include:

- check all hydraulic components for leaks,
- check electrical connectors and wiring harness for continuity,
- examine flexible hoses and cabling for crushing or pinching in mechanical components,
- verify correct sensor signal polarity,
- test the rotary unions for leaks or cross-talk between the various hydraulic passages,
- check solenoid coils for excessive temperature,
- examine the kevlar strength member for proper load bearing termination.

Maintaining hydraulic fluid cleanliness is critical to the reliability of the locomotor. The servo-valves have no redundancy. Should they fail the locomotor could be unretrievable. Regular fluid testing was determined by the FMEA to be important to maintain system reliability. The importance of regular hydraulic fluid testing was shown from the MLDUA experience at ORNL. An increase of fluid particulate was detected and corrective action taken before any damage could result.

One noticeable observation from the FTA is a lack of redundancy in the locomotor. Most of the branches coming out of the top events have only OR gates. Very few branches have AND gates. This implies that to have high system reliability, individual components will have to have a high reliability. There is only very limited redundancy to compensate for failed components in general. Some components, such as the servo-valves have no redundancy. This lack of redundancy means that care will have to be taken in the assembly of the nonredundant components and appropriate preventive care must be taken. The most critical nonredundant components are the electrical connectors and the servo-valves.

In the case of the servo-valves, there is no redundancy. If a servo-valve fails its associated joint fails. This is particularly critical for the grippers. A failure of the gripper valving can leave the locomotor permanently stuck in place. There is no provision for an alternate means of releasing the locomotor grippers.

RedZone has asserted that in the event of a valve failure on the positioning joints, the rotary actuators, gripper orientation, and vertical translation, a crude form of redundancy is available. This redundancy, which was not accounted for in the FTA, is briefly outlined.

For example, only two out of three rotary actuators have to be operational to position the locomotor in the tank. There, however, are constraints. The locomotor must have failed so that it can be extended far enough to reach the next pipe. With one rotary actuator failed, the locomotor cannot reach a pipe from alternate orientations; therefore, there must not be any obstructions in the direction the locomotor can reach. Failure of the gripper tilt or rotate on one side can be compensated for by utilizing the opposite tilt and rotate to position the gripper with the failed tilt and rotate. The ability to compensate in this manner depends on the orientation of gripper with the failed tilt or rotate. These procedures for compensating for failed joints will have to be tested and demonstrated during cold testing of the locomotor before reliance can be placed in them.

One of the undesired events examined in the FTA is the locomotor striking the tank. This could occur, for example, by an uncontrolled move of the locomotor. The uncontrolled move could occur due to a servo valve failure. If the locomotor is positioned near the tank wall when an uncontrolled move occurs it could strike the tank wall. The locomotor operates at low velocities and therefore has low kinetic energy to be dissipated by the wall. Actuator velocity is a variable that can be adjusted by the user. There is an assumption that the tank wall is capable of dissipating even low kinetic energies. The amount of kinetic energy that the tank wall can safely dissipate in the event of a manipulator strike is outside the scope of this study. The amount of energy the tank wall can absorb is crucial to determining if a tank strike would breach the tank.

A review of operations with hydraulic manipulators at ORNL was performed. This was to gain insight into possible operational and design problems applicable to the locomotor.

The only failure mode identified in reviewing operations of Oak Ridge manipulators that had not been identified in the FMEA and FTA of the locomotor is vibration. The camera lightbulbs on the Houdini vehicle failed by vibrating out of their sockets. Houdini is a tracked vehicle, resulting in significant vibration from the contact and slippage of the tracks with the ground during operation. Vibration should not be a problem on the locomotor because of its method for locomotion; there is no slippage or intermittent contact. This will be confirmed in cold testing.

Initial shakedown testing revealed problems on both the RedZone developed Houdini and the ORNL developed NGMH. Initial testing is essential for identifying problems and taking corrective action to prevent failure. Operational experience showed that hydraulic leaks were a significant problem on the Houdini. Part of this problem can be attributed to the vibration resulting from operating the vehicle. Applying thread-locking compound to the hydraulic connectors solved the problem on the Houdini. This technique can also be applied to the locomotor to prevent hydraulic leaks.

Significantly, a major source of damage to the Houdini occurred during insertion and extraction through the tank riser. Insertion and retraction operations of the locomotor have not been examined because those procedures have yet to be developed. It is expected that the locomotor will only be inserted and retracted two or three times per tank. The relative infrequency of the insertion and retraction operation is no guarantee of lack of damage. Serious damage to the locomotor is possible with only a single insertion. Careful planning and testing can mitigate problems associated with this operation.

There are some remaining issues that have not been thoroughly covered in the analyses in this report. Damage to the manipulator or tank during insertion and extraction has not been considered. Certain out-of-tank failures could affect the locomotor. Some combinations of failures could result in the locomotor striking the tank. Evaluating the severity of a tank strike is outside the scope of this report

ORNL operational experience and the FTA (see item "uncontrolled swing of locomotor during insertion" in the table) point out potential hazards during insertion and extraction of the locomotor. Further analysis of insertion/extraction was not possible because those details are not yet available. Cold testing of insertion/extraction should reveal many of those potential problems. Particular attention should be paid to the survivability of any external hoses or cabling.

There are some out-of-tank failures that could have effects on in-tank components. These include failures of the following items: resolver electronics, servo-valve driver electronics, solenoid valve driver electronics, and tether take-up spool mechanism. These were identified by the FTA as potential failure causes but were not further investigated.

ACKNOWLEDGEMENT

The author would like to acknowledge the technical input of the following individuals: Peter Francino, RedZone Robotics, Inc.; Bruce Thompson, RedZone Robotics, Inc.; George Bernatz, West Valley Nuclear Services; Louis Huber, West Valley Nuclear Services; Pat Berton, West Valley Nuclear Services.

REFERENCES

1. E. E. Lewis, *Introduction to Reliability Engineer*ing, John Wiley & Sons, New York, 1987.

2. Society of Automotive Engineers, Aerospace Recommended Practice ARP-926, "Fault/Failure Analysis Procedure," 1997.

3. A. Villemeur, *Reliability, Availability, Maintainability and Safety Assessment: Methods and Techniques*, John Wiley & Sons, New York, 1992.

4. MLDUA operating log summary provided by R. L. Glassell.

5. MLDUA operations personal communication from R. L. Glassell to J.B. Chesser, ORNL.

6. B. L. Burks and D. D. Falter, *Houdini Remotely Operated Vehicle System Performance Assessment for Tank W-3 Waste Removal Operations*, ORNL/M-6535.

7. B. L. Burks and D. D. Falter, *Houdini Remotely Operated Vehicle System Performance Assessment for Tank W-4 Waste Removal Operations.*

8. J. B. Chesser, NGMH operations, personal recollection.

APPENDIX A

FMEA Table

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
hydraulic fluid	transmit power to actuators	moisture in fluid, air entrainment	degredation of fluid properties	reduced dynamic performance(reduced bulk modulus), reduced fluid lubricity, corrosion of other components	filtration, dessicant breather on reservoir, periodic hydraulic fluid testing, scheduled filter and breather element replacement	>10^7 rad resistant fluid. Fluid is Shell Tellus 32 as specified by West Valley
linear hydraulic actuators	actuate joints	grit on exposed rods, radiation embrittlement of seals, excessive fluid temperature, fluid incompatible with seals	seal breakdown	debris in hydraulic fluid (potential failure cause for other components), reduced dynamic performance due to seal leakage	wiper seals on exposed rods, seals are radiation and fluid compatible, fluid filtration	seals are Buna N
		hydraulic continuity failure (connector, hose failure)	inability to move cylinder,	DOF locked	predeployment testing and inspection	
		hydraulic continuity failure (connector, hose failure)	actuator limp	DOF limp	predeployment testing and inspection	
		mechanical overload	cylinder seal failure, rod buckling, burst cylinder	degraded dynamic performance, failure of DOF	factor of safety applied in design, Tarzan operates in controlled environment limiting potential for overload	not having reliefs to prevent overloads due to system dynamics is justified because of the low system kinetic energy

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
rotary hydraulic actuators	actuate joints	radiation embrittlement of seals, excessive fluid temperature, fluid incompatible with seals	seal breakdown	debris in hydraulic fluid (potential failure cause for other components), reduced dynamic performance due to seal leakage	wiper seals on exposed rods, check radiation compatibility of seals, fluid filtration	
		hydraulic continuity failure (connector, hose failure)	inability to move actuator	DOF locked	predeployment testing and inspection	
		hydraulic continuity failure (connector, hose failure)	actuator limp	DOF limp	predeployment testing and inspection	
		mechanical overload	actuator seal failure, burst actuator	degraded dynamic performance, failure of DOF, leaks	factor of safety applied in design, Tarzan operates in controlled environment limiting potential for overload	not having reliefs to prevent overloads due to system dynamics is justified because of the low system kinetic energy
gripper viewing cameras	provides viewing but not confirmation of grip	electrical continuity failure, radiation, impact washdown fluid leakage through seals	failure to provide useable television image	inability to see to perform a task	there are other television cameras providing alternate views, predeployment testing of seals, changeout cameras as necessary when arm is retrieved as allowed by ALARA concerns	camera hardened to 10^8 rad
manipulator viewing camera	provide viewing of the manipulator	electrical continuity failure, radiation, impact washdown fluid leakage through seals	failure to provide useable television image	inability to see to perform a task	there are other television cameras providing alternate views, predeployment testing of seals, changeout cameras as necessary when arm is retrieved as allowed by ALARA concerns	camera hardened to 10^8 rad

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
viewing lights	provide illumination for viewing	electrical continuity failure, impact, washdown fluid leakage through seals, aging	failure to provide illumination for useable television image	inability to see to perform a task	there are multiple lights providing redundancy, scheduled replacement, predeployment testing of seals, lights are operated at reduced voltage to extend life, lights are change as necessary as allowed by ALARA limits	
hydraulic manifolds	distribute hydraulic fluid to various valves	undertighten connectors, overtighten connectors, overpressure, design/manufacturing tolerance errors (ill fitting plugs, valves, connectors)	leaks	loss of hydraulic fluid, loss of control of Tarzan if leak is significant	skill of the craft by assembly personnel, predeployment inspection, overpressure testing,predeployment testing	
		corrosion (external cause water in hydraulic fluid)	debris in hydraulic fluid	failure cause for other components	filtration, dessicant breather on reservoir, periodic hydraulic fluid testing, scheduled filter and breather element replacement	
		hydraulic continuity failure (connector, hose failure)	inability to move actuators	Tarzan immobile	predeployment testing	

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
structural components, load bearing elements(pins, welds, etc...)	support Tarzan weight	manufacturing defects, corrosion, fatigue,overload	cracking, structural failure	Tarzan immobile, components fall off	proper choice of materials, structural welds have been eliminated with the exception of the linear actuator barrels, low number of lifetime cycles (<20,000 cycles), predeployment testing, plating and painting for corrosion resistance	
bolts, retaining rings, fasteners	attach/mount components	improper assembly, corrosion	fastener loosens	component falls off	predeployment testing, proper choice of materials, all bolts assembled with loctite and lockwashers and torqued to recommended values, signoff sheet for final assembly confirming torquing, loctiting, lockwasher presence	
hydraulic hoses	distribute hydraulic fluid	high temperature, radiation embrittlement, fluid incompatibility	hose embrittlement	debris in hydraulic fluid (potential failure cause for other components)	maintaining fluid temperature, radiation compatible hose, hose compatible with selected hydraulic fluid	tether hose is kevlar/PVC, hoses on locomotor are Parker nitrile hoses
		high temperature, radiation embrittlement, hydraulic fluid incompatibility, hose pinched between mechanical components, chemical incompatibility of hose with external environment	hose break	loss of hydraulic fluid, loss of control of Tarzan if leak is significant	maintaining fluid temperature, radiation compatible hose, hose compatible with selected hydraulic fluid, predeployment testing (examining for pinch points)	

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
hydraulic connector (connectors for both hydraulic fluid and water)	join hydraulic components together	high temperature, radiation embrittlement, fluid incompatibility, improper assembly procedure, overpressure	hose seperates from connector	loss of hydraulic fluid, loss of control of Tarzan if leak is significant	skill of the craft by assembly personnel, maintaining fluid temperature, compatible hose, hose compatible with selected hydraulic fluid, predeployment testing	
		overtighten connectors, undertighten connector, overpressure	leaks	loss of hydraulic fluid, flooding of link potentially causing electrical short, loss of control of Tarzan if leak is significant	skill of the craft by assembly personnel, predeployment testing	
wiring harness	distribute electrical signals and power	insulation failure(external causes: manufacturing, radiation, high temp, pinching, repeated flexing, chemical incompatibility with hydraulic fluid or external environment)	electrical short	loss of feedback signals, inability to control Tarzan, damage to electrical components	radiation and hydraulic fluid compatible insulation,test for proper continuity during manufacture, predeployment testing (examining for pinch points), electrical connections assembled per manufacturer recommendations using skill of the craft	wiring insulation is ETFE (>10^7 rad resistance), tether wires spiralled to reduce tether wire stress

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
Wiring harness (continued)		insulation failure(external causes: manufacturing, radiation, high temp, pinching, repeated flexing, chemical incompatibility with external environment)	loss of electrical continuity	loss of feedback signals, inability to control Tarzan, damage to electrical components	using radiation compatible insulation, test for proper continuity during manufacture, predeployment testing (examining for pinch points), electrical connections assembled per connector manufacturer recommendations using skill of the craft	
rotary actuator rolling element bearings	minimize joint friction	mechanical overload	spalling, race denting	high friction, reduced dynamic performance, ultimately bearings seize locking the joint	factor of safety applied in design, Tarzan operates in controlled environment limiting potential for overload, mechanical testing to verify actuator design, low duty cycle and loads	hydraulic leakage provides bearing lubrication
		seal failure (external cause: high radiation, high temperature)	corrosion	high friction, reduced dynamic performance, ultimately bearings seize locking the joint	Proper selection of bearing material and lubrication	
		loss of lubrication	corrosion, spalling, wear	high friction, reduced dynamic performance, ultimately bearings seize locking the joint	bearing material selection prevent corrosion, low duty cycle and loads prevents wear	

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
sleeve bearings	minimize joint friction in the vertical translator	radiation, heat, grit	cracking	high friction, reduced dynamic performance, joint misalignment	predeployment testing, material selection	sleeve bearing material is PEEK
hydraulic fluid seals	prevent fluid leakage	high temperature, radiation embrittlement, fluid incompatibility	permanent compression set	debris in hydraulic fluid (potential failure cause for other components)	maintaining fluid temperature, radiation compatible seal, seal compatible with selected hydraulic fluid	these seals are buna N
		high temperature, radiation embrittlement, fluid incompatibility	seal leakage	loss of hydraulic fluid, loss of control of Tarzan if leak is significant	maintaining fluid temperature, radiation compatible seal, seal compatible with selected hydraulic fluid	
rotary joint resolvers	provide position feedback	high temperature, radiation, loss of electrical continuity	loss of position feedback	loss of servo loops	revert to controlling joints entirely manually, on-off switch controls	the possibility of a joint sensor failure causing an uncontrolled move of the joint when a joint is active is minimized by software checking of the joint error signal
		improper wiring	polarity reversal	unstable servo loop	predeployment testing	
vertical translation LVDT	provide position feedback	high temperature, radiation, loss of electrical continuity	loss of position feedback	loss of feedback to operator causing difficulty in returning to home position for recovery		LVDT signal not used in servo loops,
		improper wiring	polarity reversal		predeployment test	

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
gripper contact switches	verify gripper seating on valve	electrical continuity failure, contact corrosion (external cause: seal failure allowing corrosive vapors into switch)	fail off	interlock switches do not allow release of gripper	fail off can be over-ridden by "hot-wiring" around the failure	
		electrical continuity failure, seal failure allowing in-leakage of fluids	fail on	interlock switches allow release of both grippers	it is possible to detect fail on of the contact switches by in-service testing: open and close gripper to cycle switches and monitor switch signal	
lens cleaning valve	clean camera lens	loss of electrical continuity, solenoid failure	fail closed	inability to clean lens	there are other television cameras available	
		stuck spool, broken spring	fail open	continuous stream of water on lens hindering viewing	there are other television cameras available, water flow can be stopped at the water supply	
gripper control isolation valve	isolate gripper actuator from servo valve	loss of electrical continuity, solenoid failure	fail closed	inability to move gripper from position at time of failure	fuse on signal line reduces likelihood of excessive current damaging solenoid	fail closed is more likely than fail open
		stuck spool (external cause: debris in fluid, corrosion due to water in fluid), broken spring	fail open	inability to isolate gripper from erroneous servo valve operation	redundancy is provided by the gripper lock valve, fluid filtration and monitoring	25 um nominal filtration required

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
gripper lock control valve	lock gripper in closed position	loss of electrical continuity, solenoid failure	fail open (spool is positioned to connect bear lock line to tank)	inability to open gripper	fuse on signal line reduces likelihood of excessive current damaging solenoid	cylinder cannot be driven to override the bearlock. This failure requires other equipment to recovery from, recovery requires cutting the cylinder.
		stuck spool (external cause: debris in fluid, corrosion due to water in fluid), broken spring	fail closed	inability to lock gripper	redundancy is provided by the gripper control isolation valve, fluid filtration and monitoring	fail open is more likely than fail closed, 10 um nominal filtration required
gripper pressure reducer	reduce hydrualic pressure to gripper actuator to reduce gripper loads	stuck spool (external cause: debris in fluid, corrosion due to water in fluid), broken spring	spool stuck in closed position	inadequate flow to gripper, inability to operate gripper	in-service testing: determine cycle time to operate gripper and monitor for deviations	
			spool stuck in open position	excessive loading on gripper and pipe	in-service testing: determine cycle time to operate gripper and monitor for deviations, there is a safety factor applied to allowable pipe loadings	

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
gripper servo valve	control gripper position open or closed	loss of electrical continuity, solenoid failure	fail spool centered, slight spool bias possible	gripper position free floating	gripper control isolation valve can isolate servo valve failure	gripper control isolation valve needs to be interlocked with contact switches in order assure timely failure recovery
		flapper jet orifice clogs (external cause: dirty fluid, corrosion)	servo spool drives to extreme position	gripper drives full open of full closed	gripper control isolation valve can isolate servo valve failure, proper fluid conditioning, predeployment flushing, in-service fluid monitoring	gripper control isolation valve needs to be interlocked with contact switches in order assure timely failure recovery
fluid conductors to gripper	supply fluid to actuator	hose or hydraulic connector failure, see also hydraulic hoses and connector section	leaks	gripper not lockable	skill of craft by assembly personnel, predeployment testing	
gripper tilt isolation valve	isolate gripper tilt actuator from servo valve	loss of electrical continuity, solenoid failure	fail closed	inability to move gripper tilt from position at time of failure	fuse on signal line reduces likelihood of excessive current damaging solenoid	fail closed is more likely than fail open
		stuck spool (external cause: debris in fluid, corrosion due to water in fluid), broken spring	fail open	inability to isolate gripper tilt from erroneous servo valve operation	fluid filtration and monitoring	25 um nominal filtration required

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
gripper tilt servo valve	control gripper orientation	loss of electrical continuity, solenoid failure	fail spool centered, slight spool bias possible	gripper tilt position free floating	gripper tilt isolation valve can isolate servo valve failure	
		flapper jet orifice clogs (external cause: dirty fluid, corrosion)	servo spool drives to extreme position	gripper tilt drives full open or full closed	gripper tilt isolation valve can isolate servo valve failure, proper fluid conditioning - filtration can prevent, predeployment flushing	10 um nominal or better filtration required
fluid conductors to gripper tilt actuator	supply fluid to actuator	hose or hydraulic connector failure, see hose or connector section, mechanical overload to gripper tilt actuator	leaks	gripper tilt orientation not lockable by using isolation valves	skill of craft by assembly personnel, predeployment testing	there are no reliefs to prevent overloads due to system dynamics
gripper rotate isolation valve	isolate gripper tilt actuator from servo valve	loss of electrical continuity, solenoid failure	fail closed	inability to move gripper from position at time of failure	fuse on signal line reduces likelihood of excessive current damaging solenoid	
		stuck spool (external cause: debris in fluid, corrosion due to water in fluid), broken spring	fail open	inability to isolate gripper from erroneous servo valve operation	fluid filtration and monitoring	

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
gripper rotate servo valve	control gripper orientation	loss of electrical continuity, solenoid failure	fail spool centered, slight spool bias possible	gripper rotate position free floating	gripper rotate isolation valve can isolate servo valve failure	
		flapper jet orifice clogs (external cause: dirty fluid, corrosion)	servo spool drives to extreme position	gripper rotate drives full up or down	gripper rotate isolation valve can isolate servo valve failure, proper fluid conditioning - filtration can prevent, predeployment flushing	10 um nominal or better filtration required
fluid conductors to gripper rotate actuator	supply fluid to actuator	hose or hydraulic connector failure, see hose or connector section, mechanical overload to gripper rotate actuator	leaks	gripper rotate orientation not lockable by using isolation valves	skill of craft by assembly personnel, predeployment testing	there are no reliefs to prevent overloads due to system dynamics
vertical translation isolation valve	isolate vertical translation actuator from servo valve	loss of electrical continuity, solenoid failure	fail closed	inability to move vertical translation from position at time of failure	fuse on signal line reduces likelihood of excessive current damaging solenoid	fail closed is more likely than fail open
		stuck spool (external cause: debris in fluid, corrosion due to water in fluid), broken spring	fail open	inability to isolate vertical translation from erroneous servo valve operation	fluid filtration and monitoring	25 um nominal filtration required

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
vertical translation servo valve	control vertical translation position	loss of electrical continuity, solenoid failure	fail spool centered, slight spool bias possible	vertical position free floating	vertical translation isolation valve can isolate servo valve failure	
		flapper jet orifice clogs (external cause: dirty fluid, corrosion)	servo spool drives to extreme position	vertical translator drives full up or full down	vertical translation isolation valve can isolate servo valve failure, proper fluid conditioning - filtration can prevent, predeployment flushing	10 um nominal or better filtration required
fluid conductors to vertical translation actuator	supply fluid to actuator	hose or hydraulic connector failure, see hose or connector section, mechanical overload to vertical translation actuator	leaks	vertical translation position not lockable by using isolation valves	skill of craft by assembly personnel, predeployment testing	there are no reliefs to prevent overloads due to system dynamics. The inherent assumption is that low system kinetic energy does not require reliefs
rotary joint servo	control rotary joint position	loss of electrical continuity, solenoid failure	fail spool centered, slight spool bias possible	joint orientation fixed, slight velocity bias possible		there are three rotary joints, limited positioning capability remains with two rotary joints operational
		flapper jet orifice clogs (external cause: dirty fluid, corrosion)	servo spool drives to extreme position	rotary joint drives to either extreme travel limit	proper fluid conditioning - filtration can prevent, predeployment flushing	10 um nominal or better filtration required

Item	Function	Failure Cause	Failure Mode	Consequence	Prevention/Detection/Mitigation	Comment
rotary joint limp valve	enable joint position to be free floating	loss of electrical continuity, solenoid failure	fail closed	inability to limp joint	fuse on signal line reduces likelihood of excessive current damaging solenoid, there is an alternate signal path to energize the valve	fail closed is more likely than fail open
		stuck spool (external cause: debris in fluid, corrosion due to water in fluid), broken spring	fail open	inability to control joint with servo valve	fluid filtration and monitoring	25 um nominal filtration required
hydraulic rotary union	transfer hydraulic fluid through joints	seal failure (external cause: high radiation, high temperature, excessive manufacturing tolerances, overpressure)	leaks	reduced dynamic performance, external leakage, crosstalk between hydraulic lines routed through rotary union	maintaining fluid temperature, radiation compatible seal, seal compatible with selected hydraulic fluid, predeployment testing	there are no reliefs to prevent overloads on the vertical translation actuator due to system dynamics (lines to the vertical translation actuator are routed through one rotary union) this is justified due to the low system kinetic energy possible
		water in rotary joint	corrosion	corrosion particles and water in hydraulic fluid	place water line by high pressure hydraulic line so that seal failure results in hydraulic fluid leaking into the wash water, keeping the hydraulic fluid clean	
tether strength member	support Tarzan weight during insertion and retrieval	improper assembly, radiation, overload, exposure to incompatible chemicals	break in load path	inability to retrieve Tarzan	predeployment testing, verification of radiation tolerance of strength member	

APPENDIX B

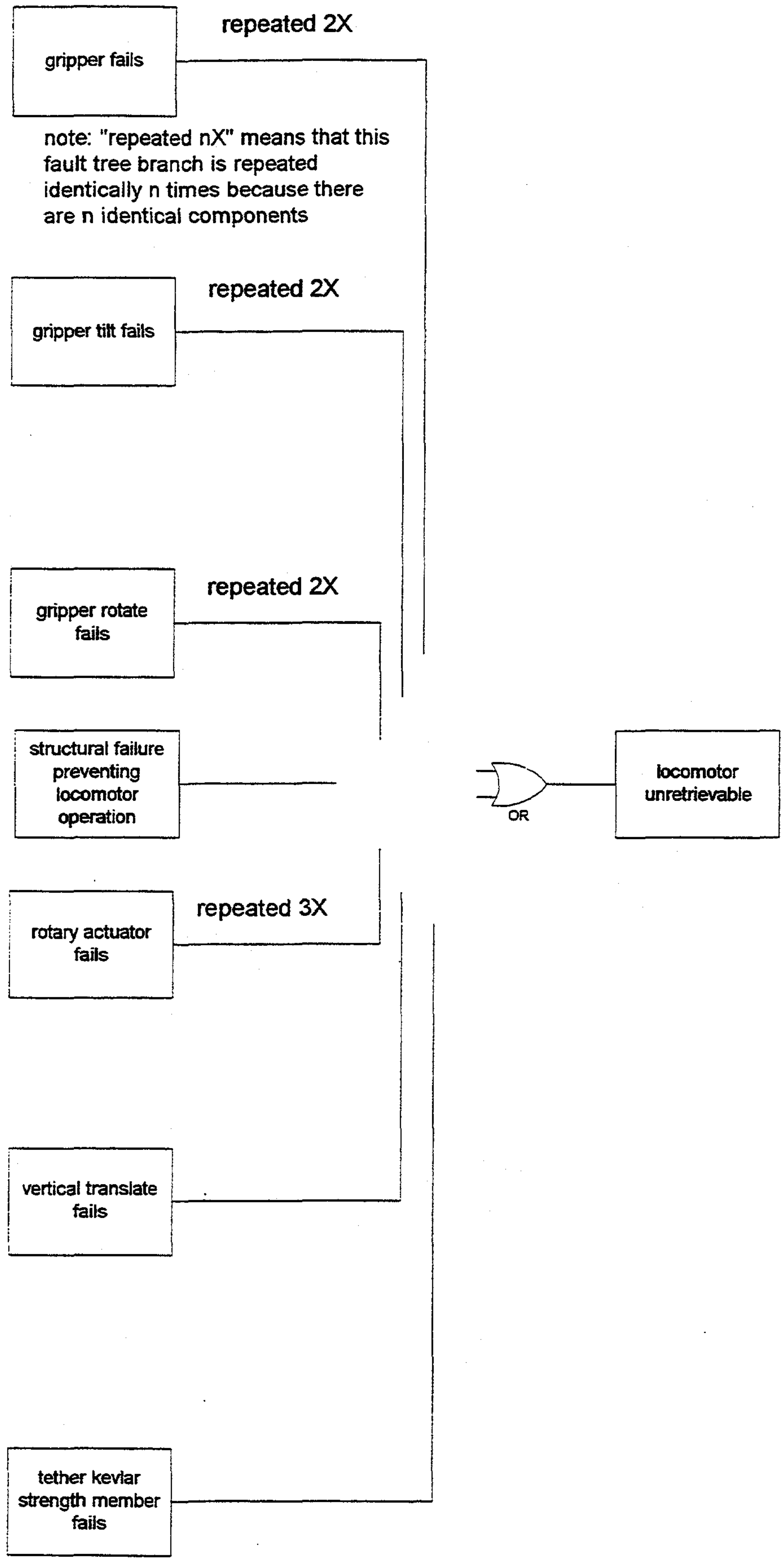
Fault Tree Analysis

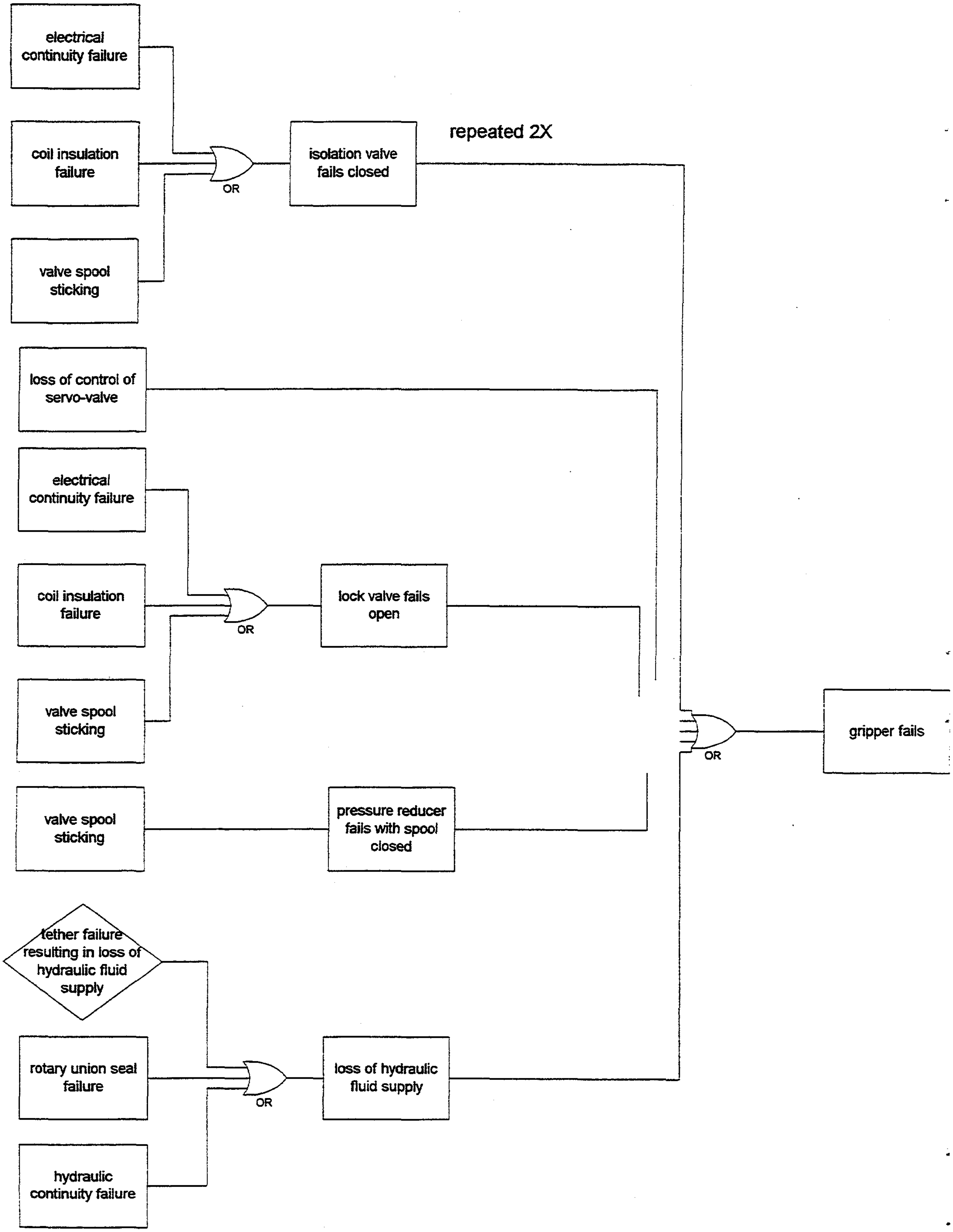
This appendix is divided into three sections. The first section is the fault tree for the top event "locomotor unretrievable," the second tier events preceding locomotor unretrievable, and the third tier events in the fault tree "locomotor unretrievable."

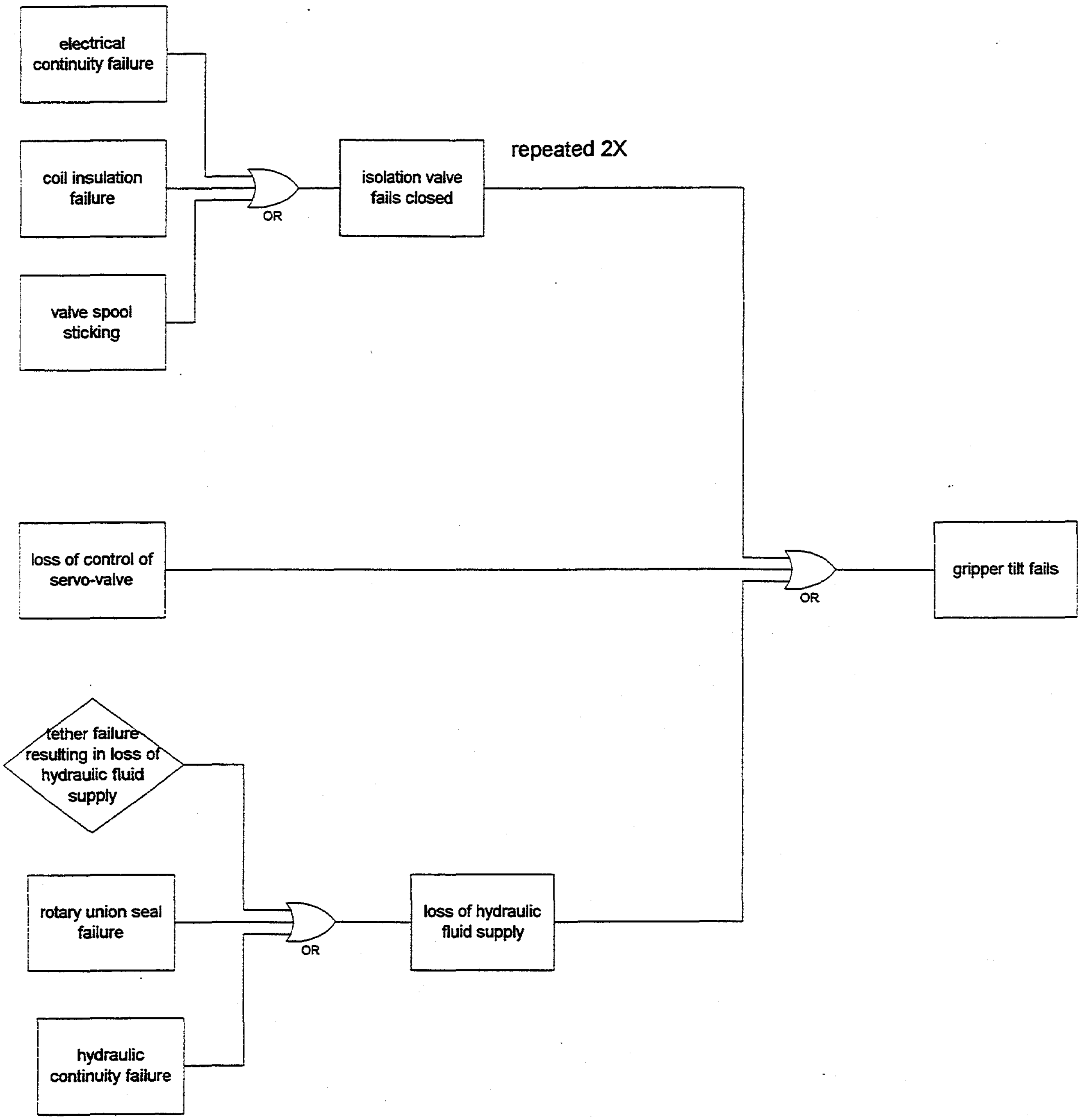
The second section is the fault tree for the top event "event potentially causing damage to tank," the second tier events preceding potential tank damage, and the third tier events in the fault tree event "event potentially causing damage to tank."

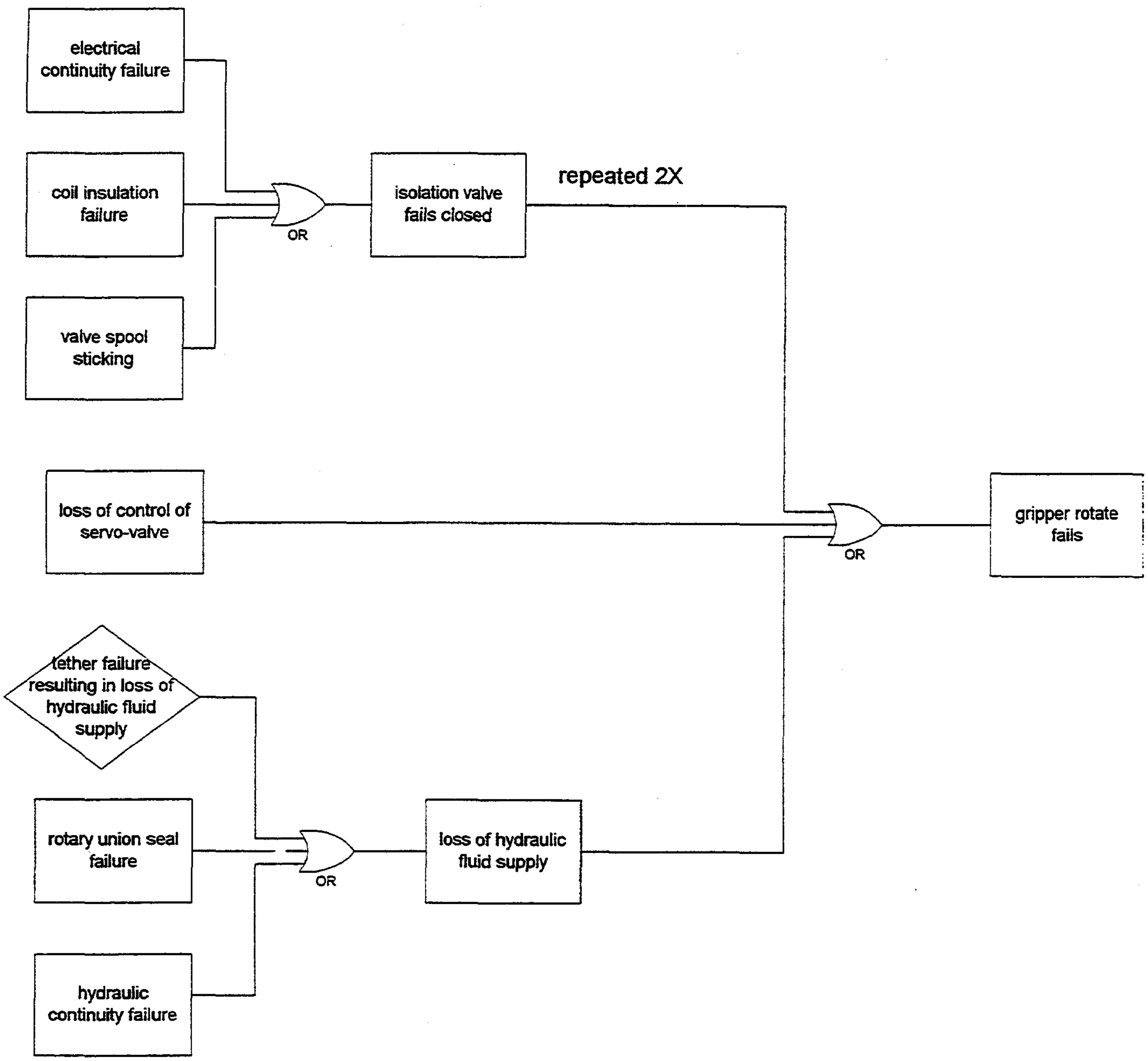
The third section is for events and causes below the level of events in the first two sections.

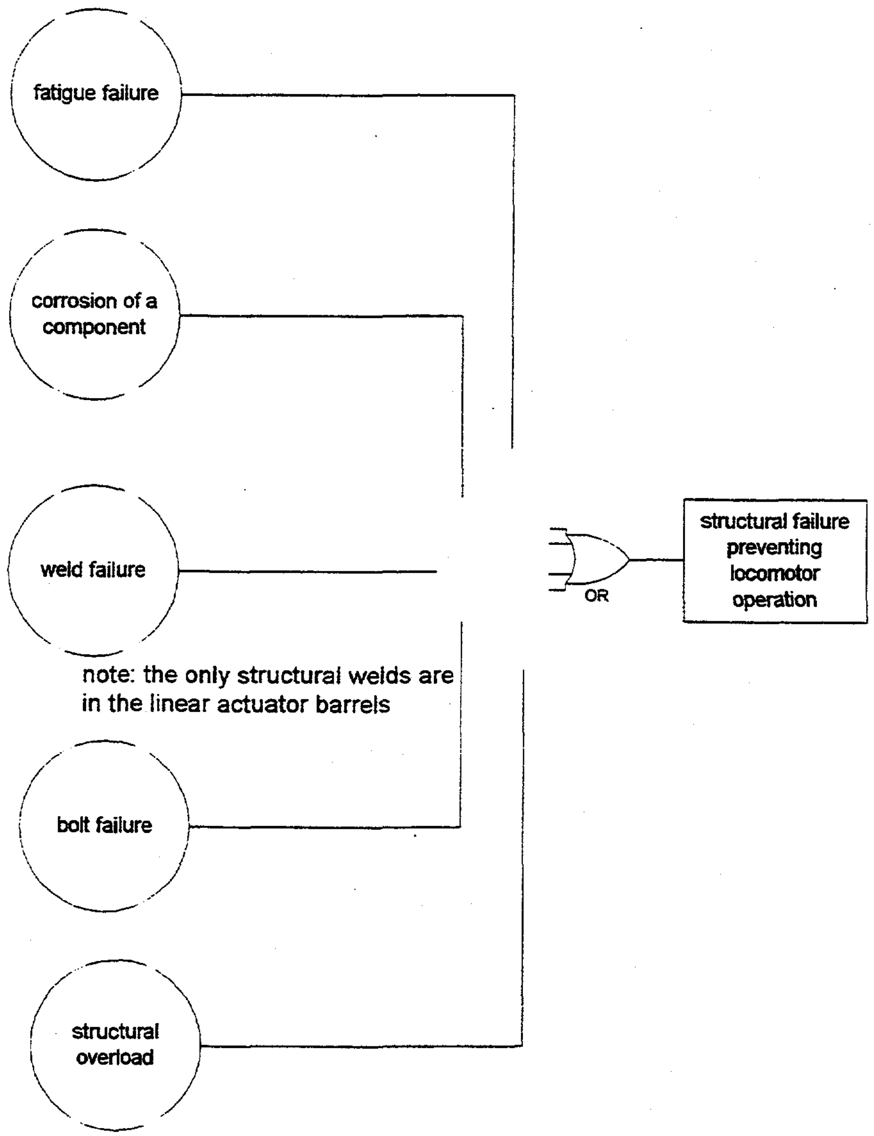
The first section begins on the next page.

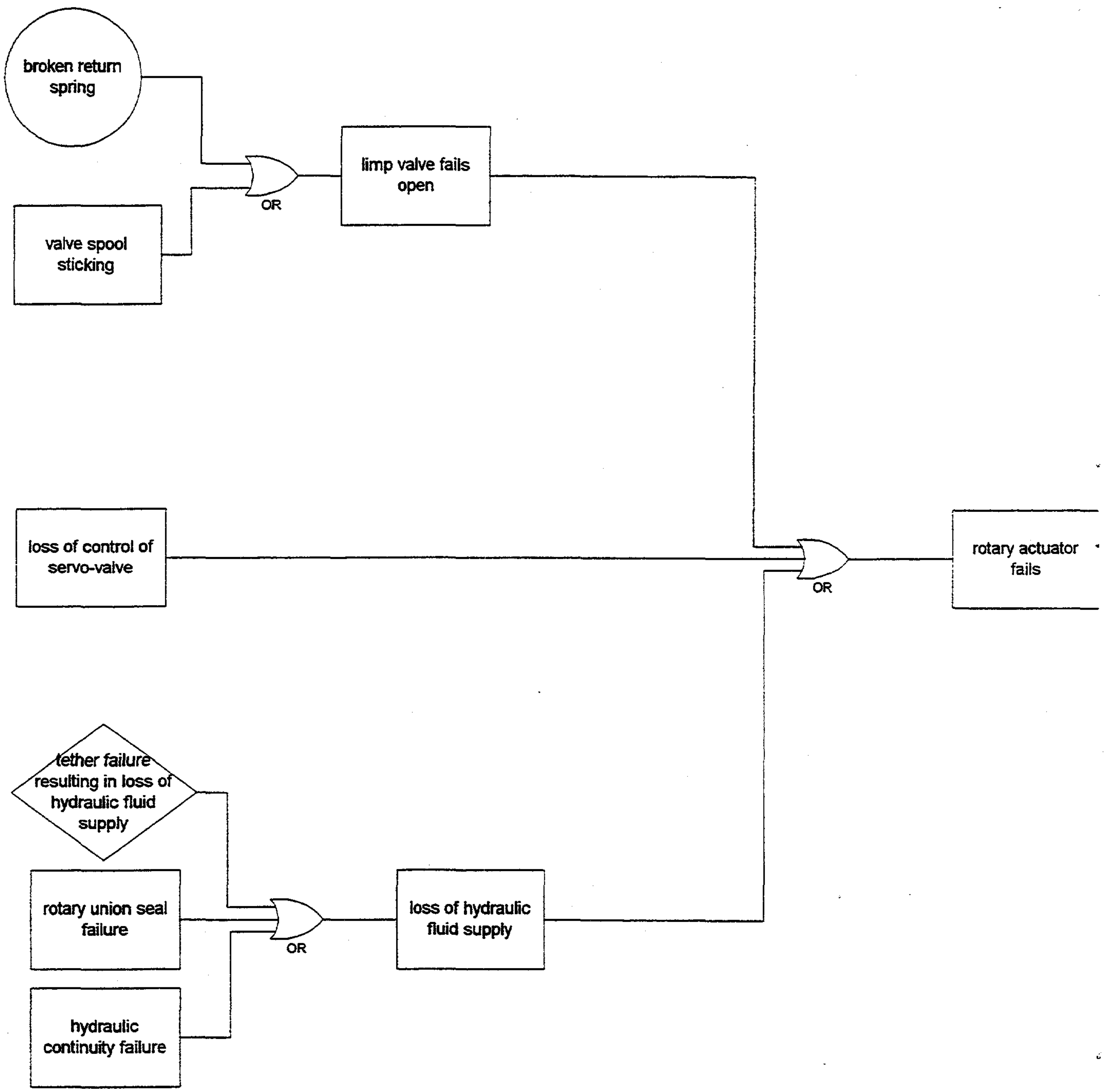

gripper fails
repeated 2X
note: "repeated nX" means that this fault tree branch is repeated identically n times because there are n identical components
gripper tilt fails
repeated 2X
gripper rotate fails
repeated 2X
structural failure preventing locomotor operation
OR
locomotor unretrievable
rotary actuator fails
repeated 3X
vertical translate fails
tether kevlar strength member fails

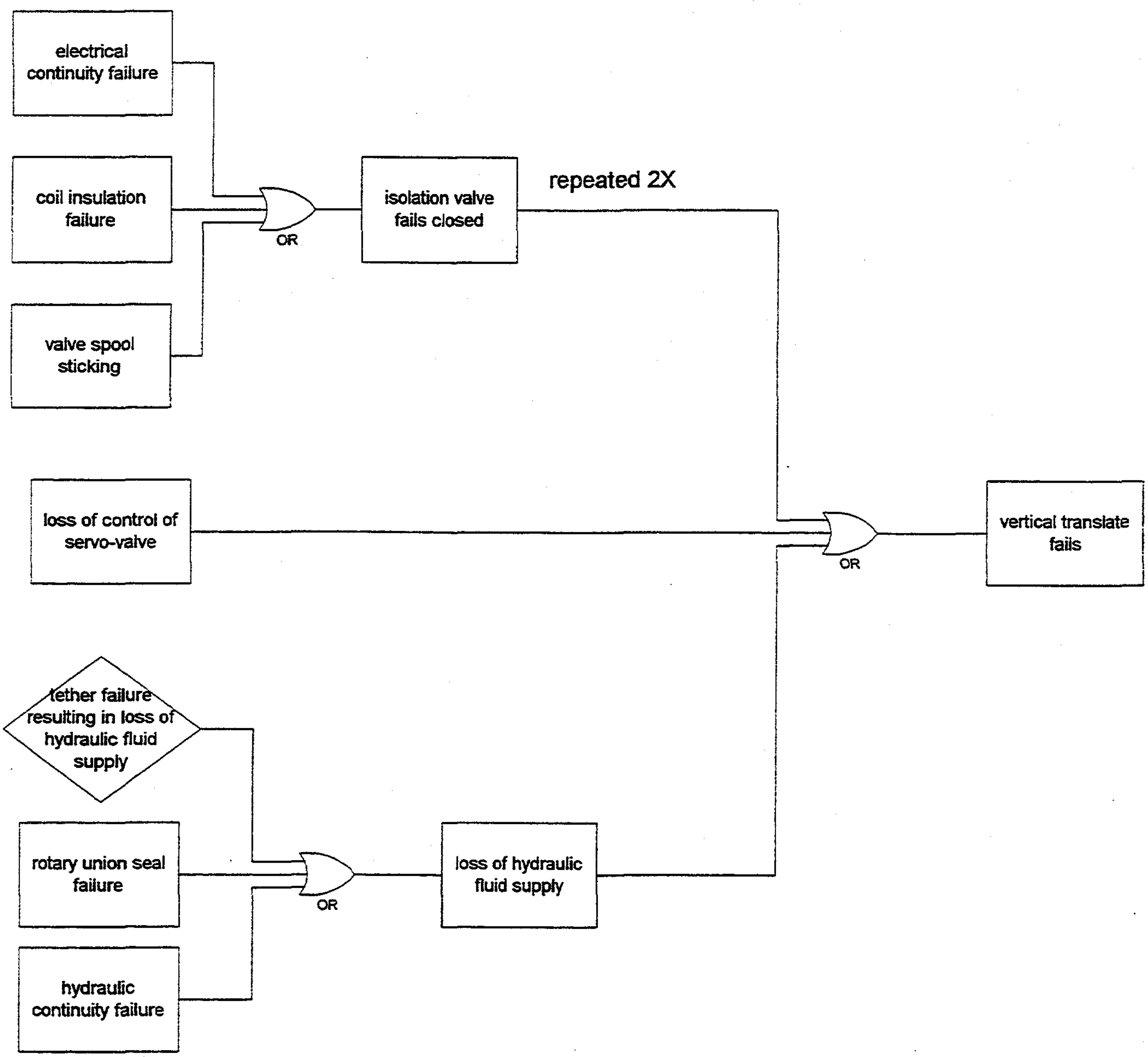

electrical continuity failure
coil insulation failure
valve spool sticking
OR
isolation valve fails closed
repeated 2X
loss of control of servo-valve
electrical continuity failure
coil insulation failure
valve spool sticking
OR
lock valve fails open
valve spool sticking
pressure reducer fails with spool closed
tether failure resulting in loss of hydraulic fluid supply
rotary union seal failure
hydraulic continuity failure
OR
loss of hydraulic fluid supply
OR
gripper fails


electrical continuity failure
coil insulation failure
valve spool sticking
OR
isolation valve fails closed
repeated 2X
loss of control of servo-valve
OR
gripper tilt fails
tether failure resulting in loss of hydraulic fluid supply
rotary union seal failure
hydraulic continuity failure
OR
loss of hydraulic fluid supply

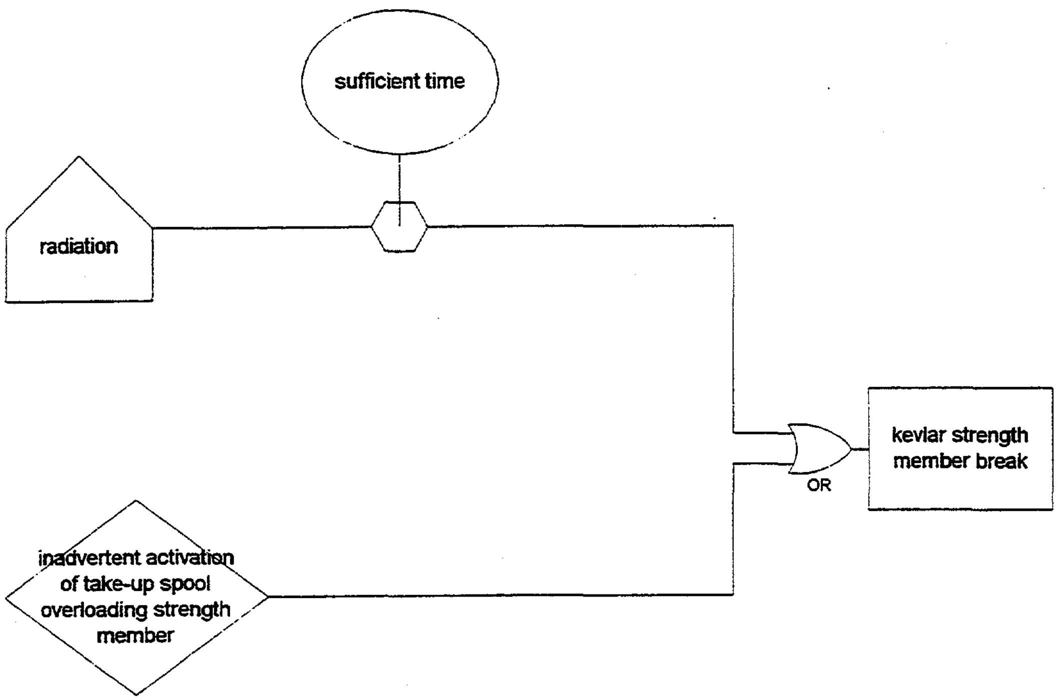

electrical continuity failure
coil insulation failure
valve spool sticking
OR
isolation valve fails closed
repeated 2X
loss of control of servo-valve
OR
gripper rotate fails
tether failure resulting in loss of hydraulic fluid supply
rotary union seal failure
hydraulic continuity failure
OR
loss of hydraulic fluid supply


fatigue failure
corrosion of a component
weld failure
note: the only structural welds are in the linear actuator barrels
bolt failure
structural overload
OR
structural failure preventing locomotor operation

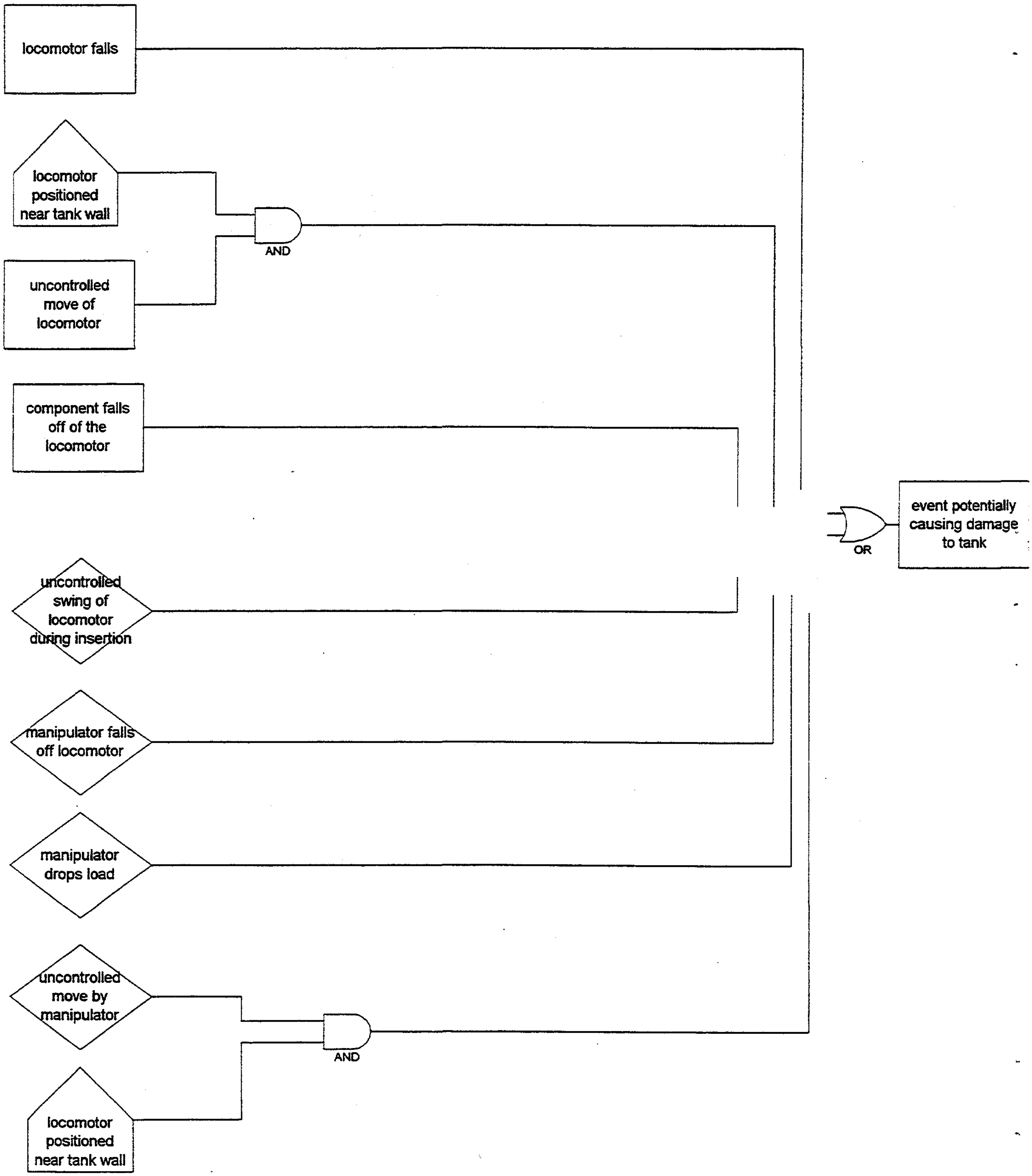

broken return spring
valve spool sticking
OR
limp valve fails open
loss of control of servo-valve
OR
rotary actuator fails
tether failure resulting in loss of hydraulic fluid supply
rotary union seal failure
hydraulic continuity failure
OR
loss of hydraulic fluid supply

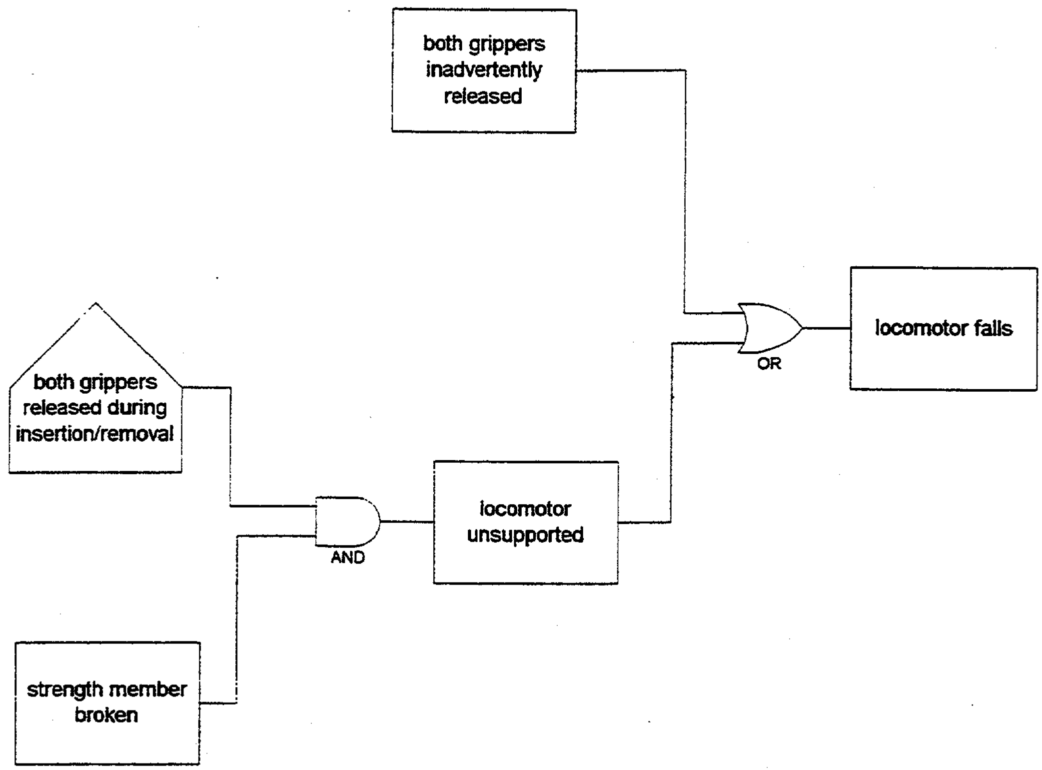


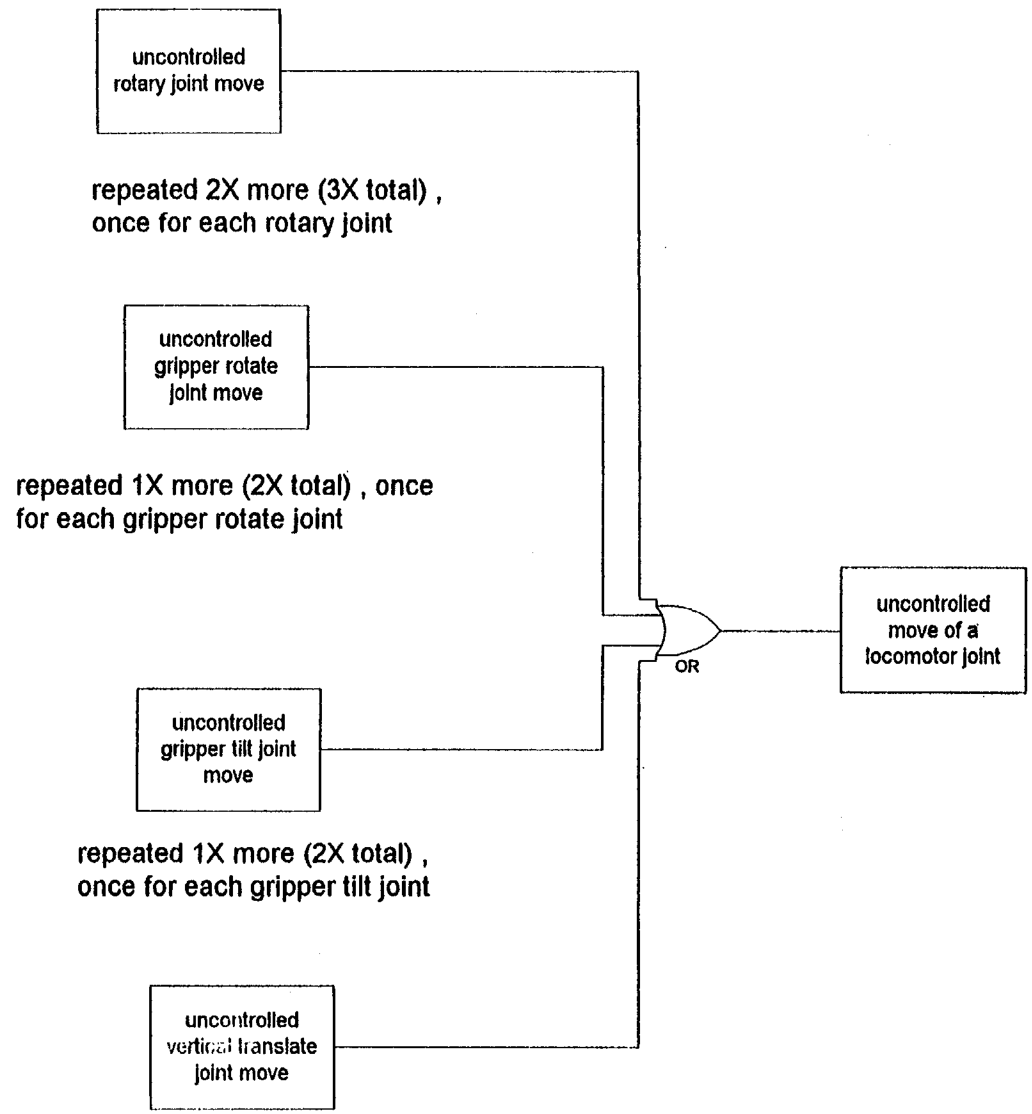
electrical continuity failure
coil insulation failure
valve spool sticking
OR
isolation valve fails closed
repeated 2X
loss of control of servo-valve
OR
vertical translate fails
tether failure resulting in loss of hydraulic fluid supply
rotary union seal failure
hydraulic continuity failure
OR
loss of hydraulic fluid supply

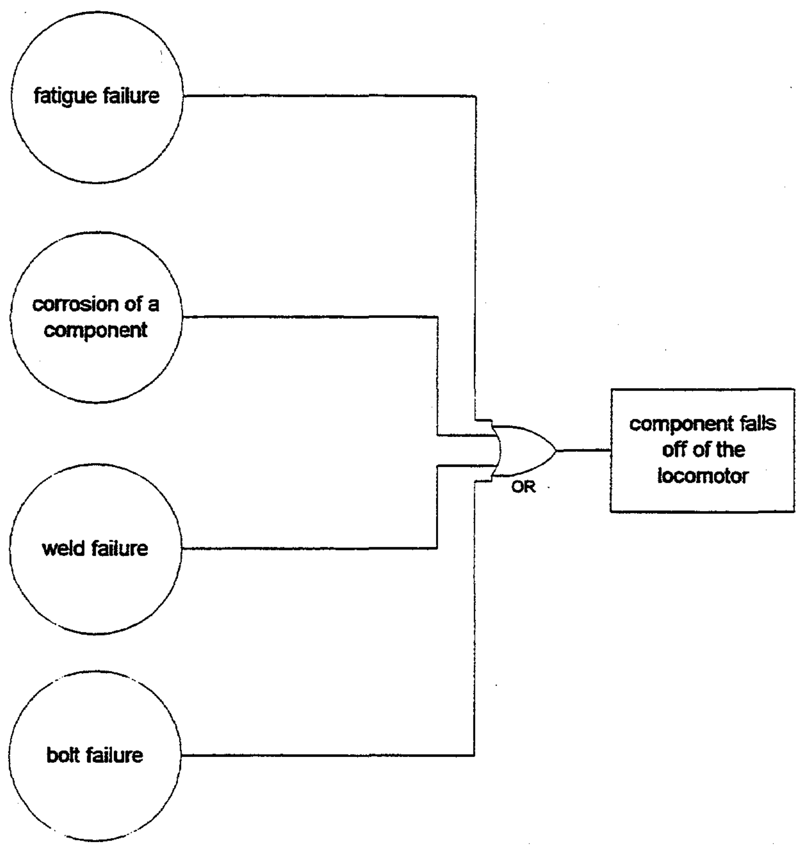

sufficient time
radiation
kevlar strength member break
OR
inadvertent activation of take-up spool overloading strength member

The section on the following pages is for top event "event potentially causing damage to tank."


locomotor falls
locomotor positioned near tank wall
AND
uncontrolled move of locomotor
component falls off of the locomotor
uncontrolled swing of locomotor during insertion
manipulator falls off locomotor
manipulator drops load
uncontrolled move by manipulator
AND
locomotor positioned near tank wall
OR
event potentially causing damage to tank

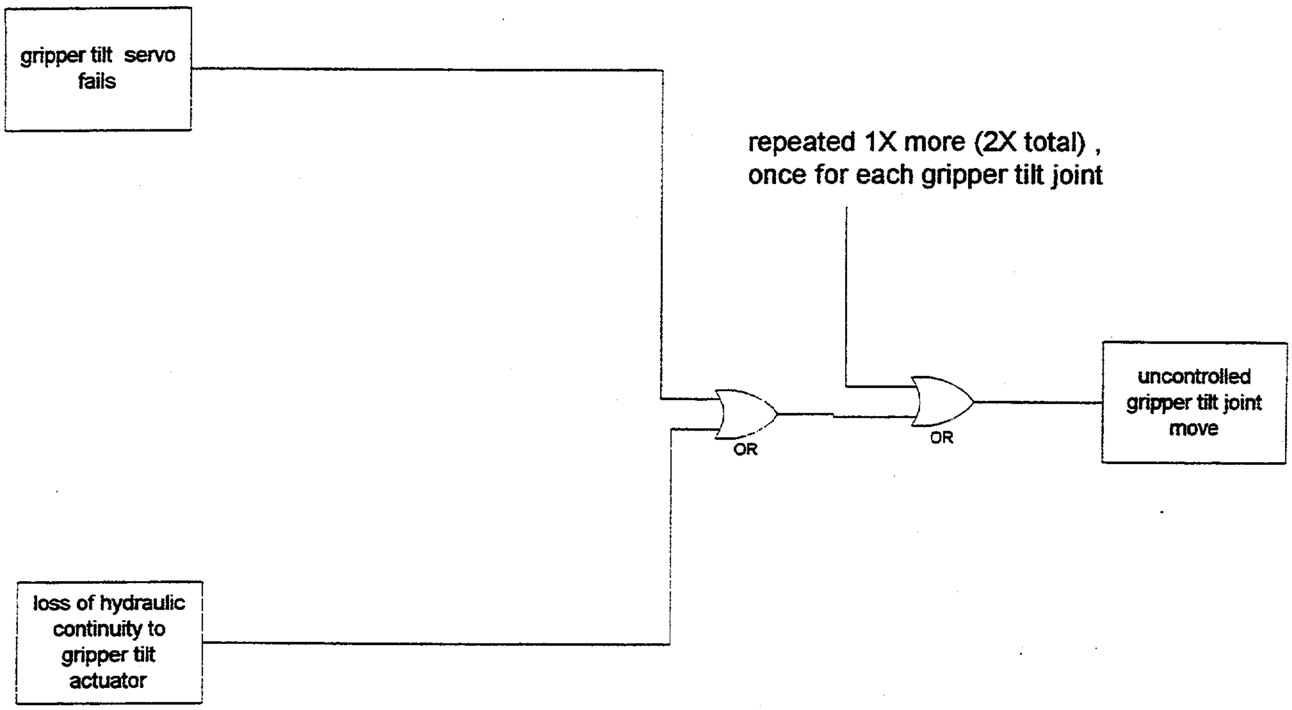

both grippers inadvertently released
locomotor falls
OR
both grippers released during insertion/removal
AND
locomotor unsupported
strength member broken

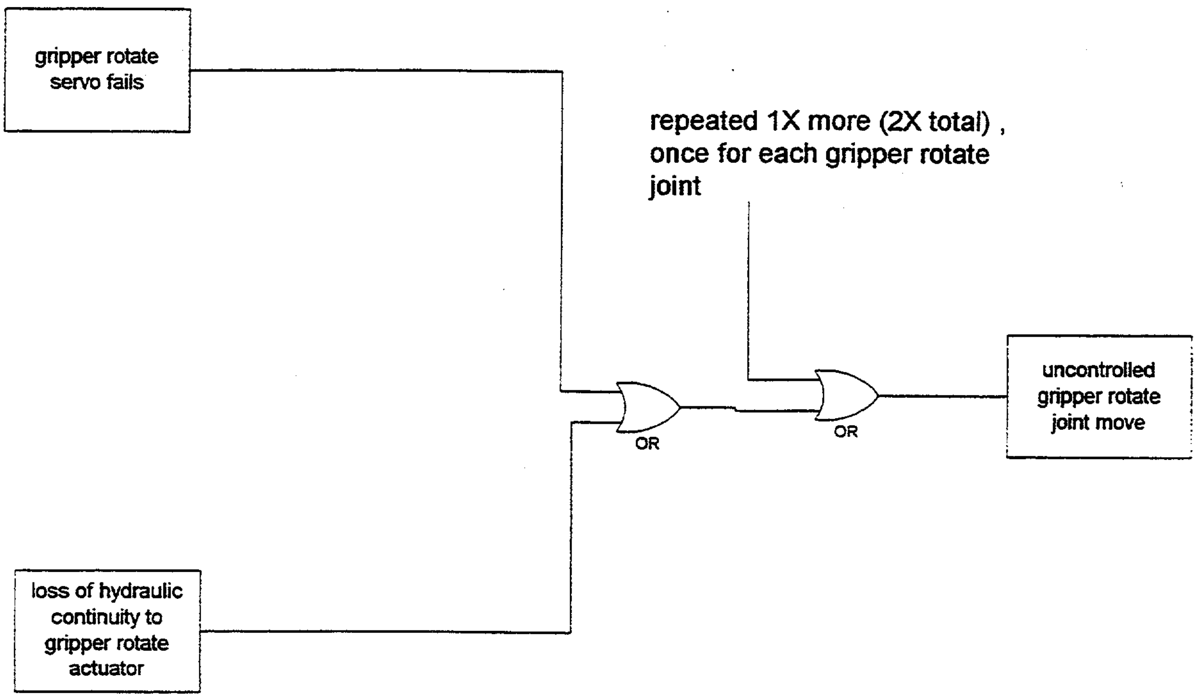

uncontrolled rotary joint move
repeated 2X more (3X total), once for each rotary joint
uncontrolled gripper rotate joint move
repeated 1X more (2X total), once for each gripper rotate joint
uncontrolled gripper tilt joint move
repeated 1X more (2X total), once for each gripper tilt joint
uncontrolled vertical translate joint move
OR
uncontrolled move of a locomotor joint

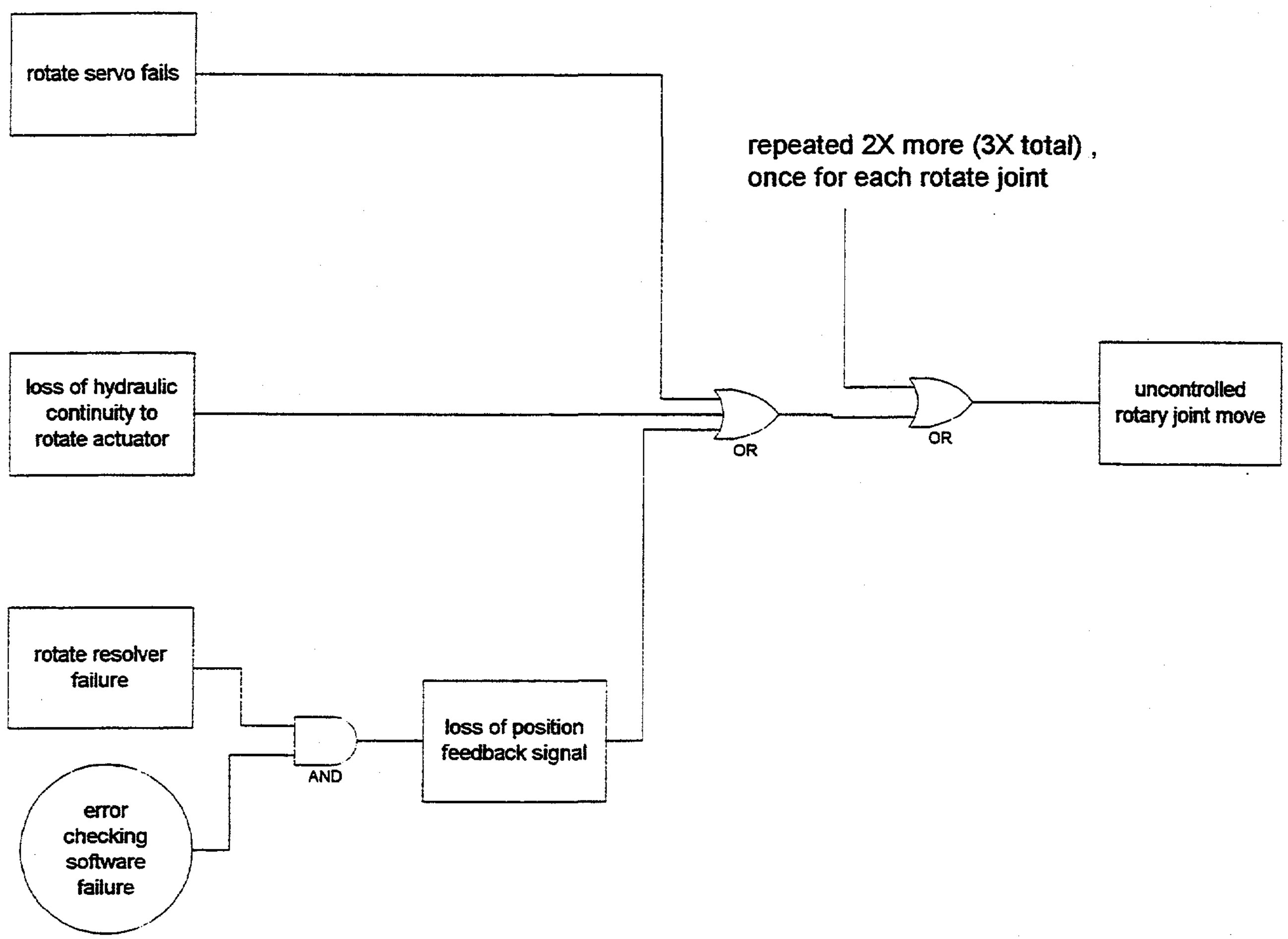


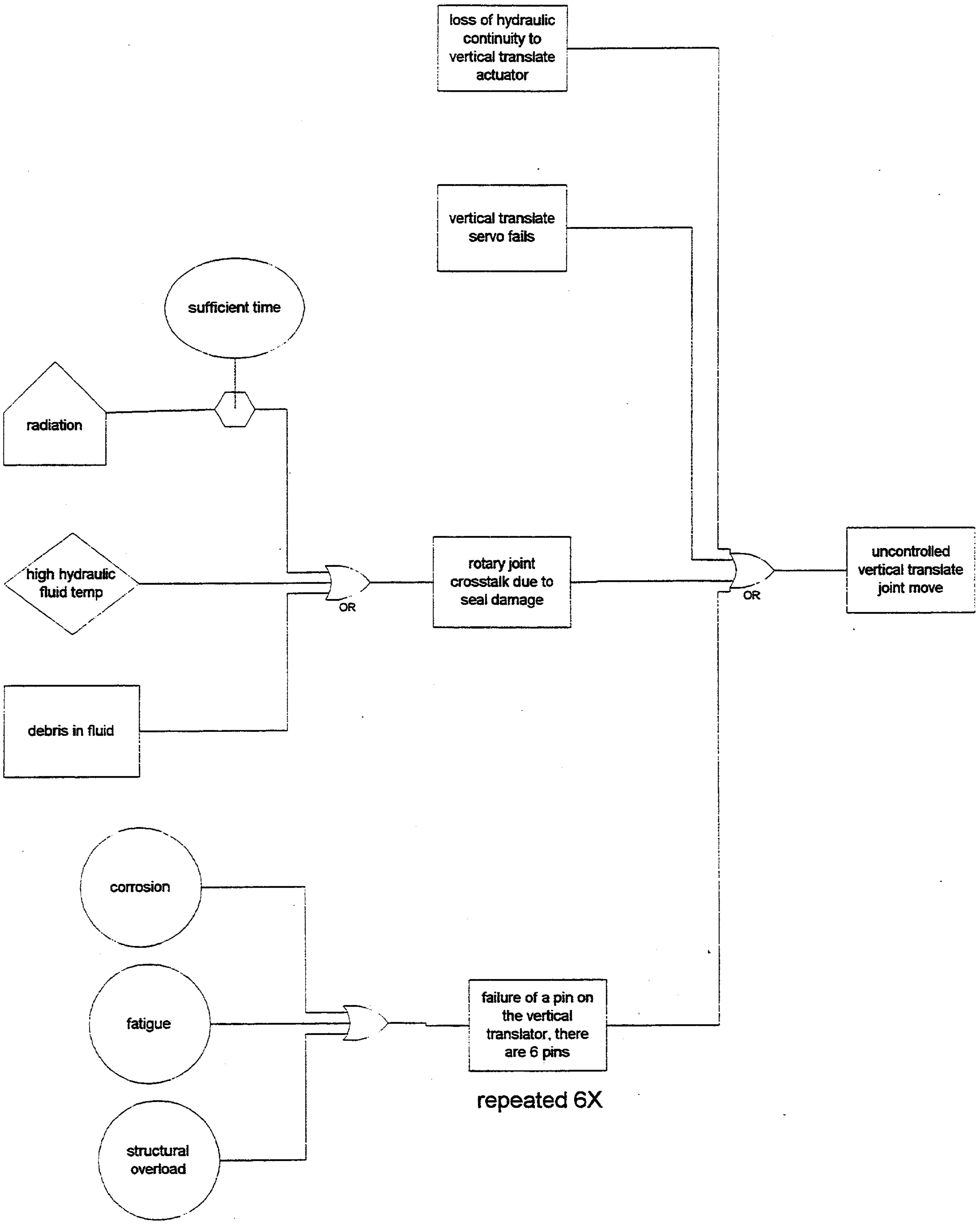
fatigue failure
corrosion of a component
weld failure
bolt failure
OR
component falls off of the locomotor

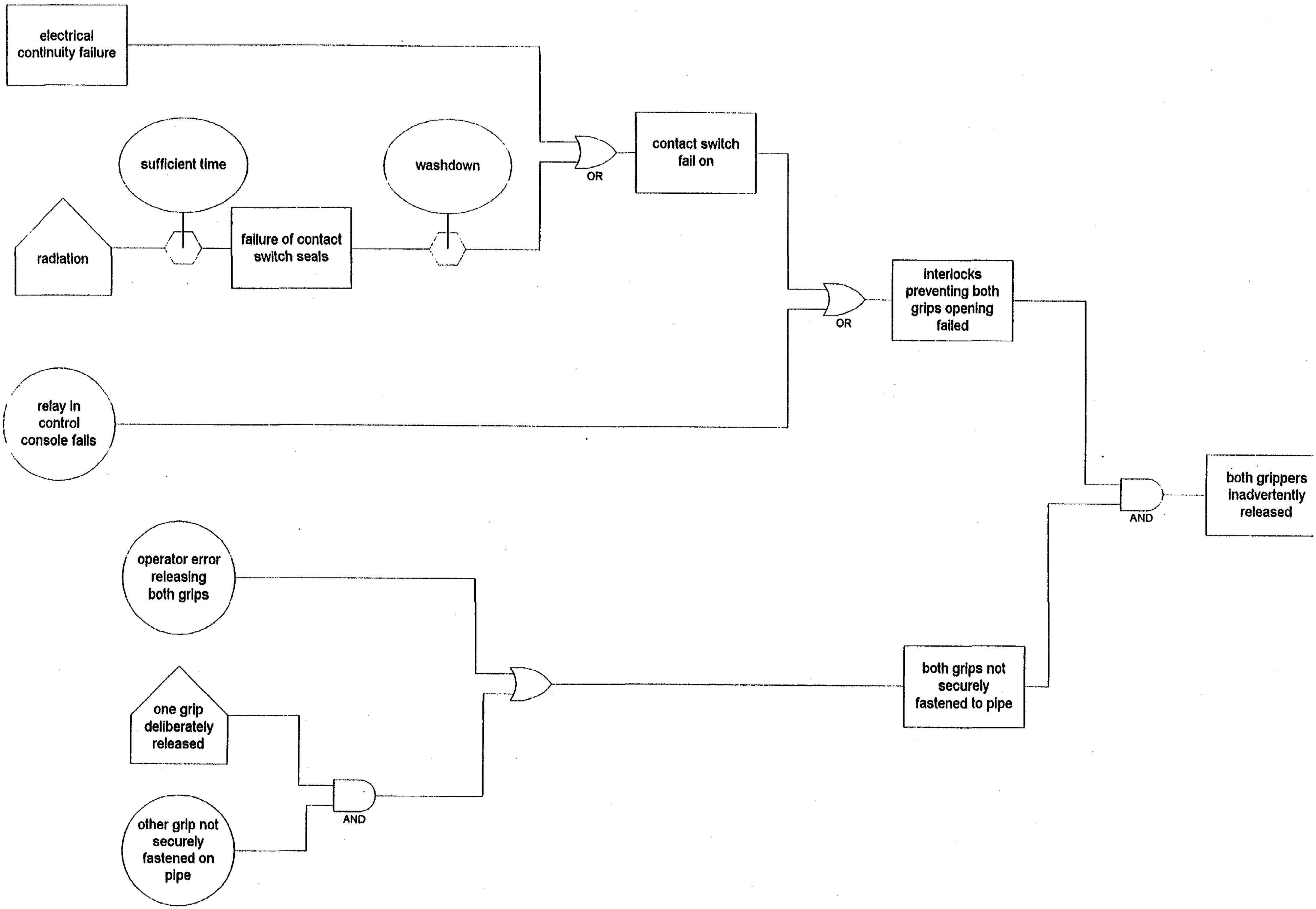
The following section is for all events below the tier of events covered in the sections “locomotor unretrievable” and “event potentially causing damage to tank.”

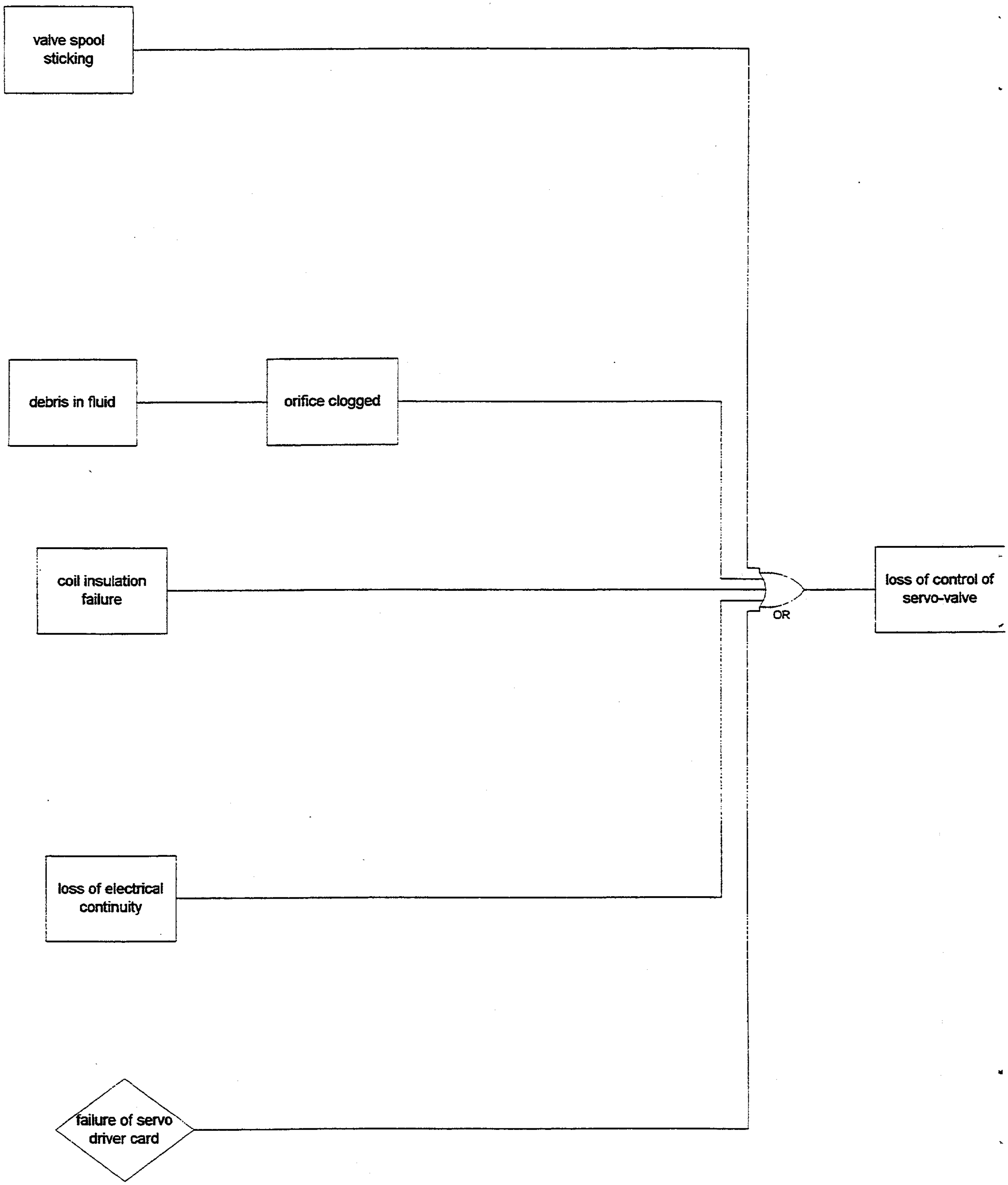

gripper tilt servo fails
repeated 1X more (2X total) , once for each gripper tilt joint
OR
OR
uncontrolled gripper tilt joint move
loss of hydraulic continuity to gripper tilt actuator

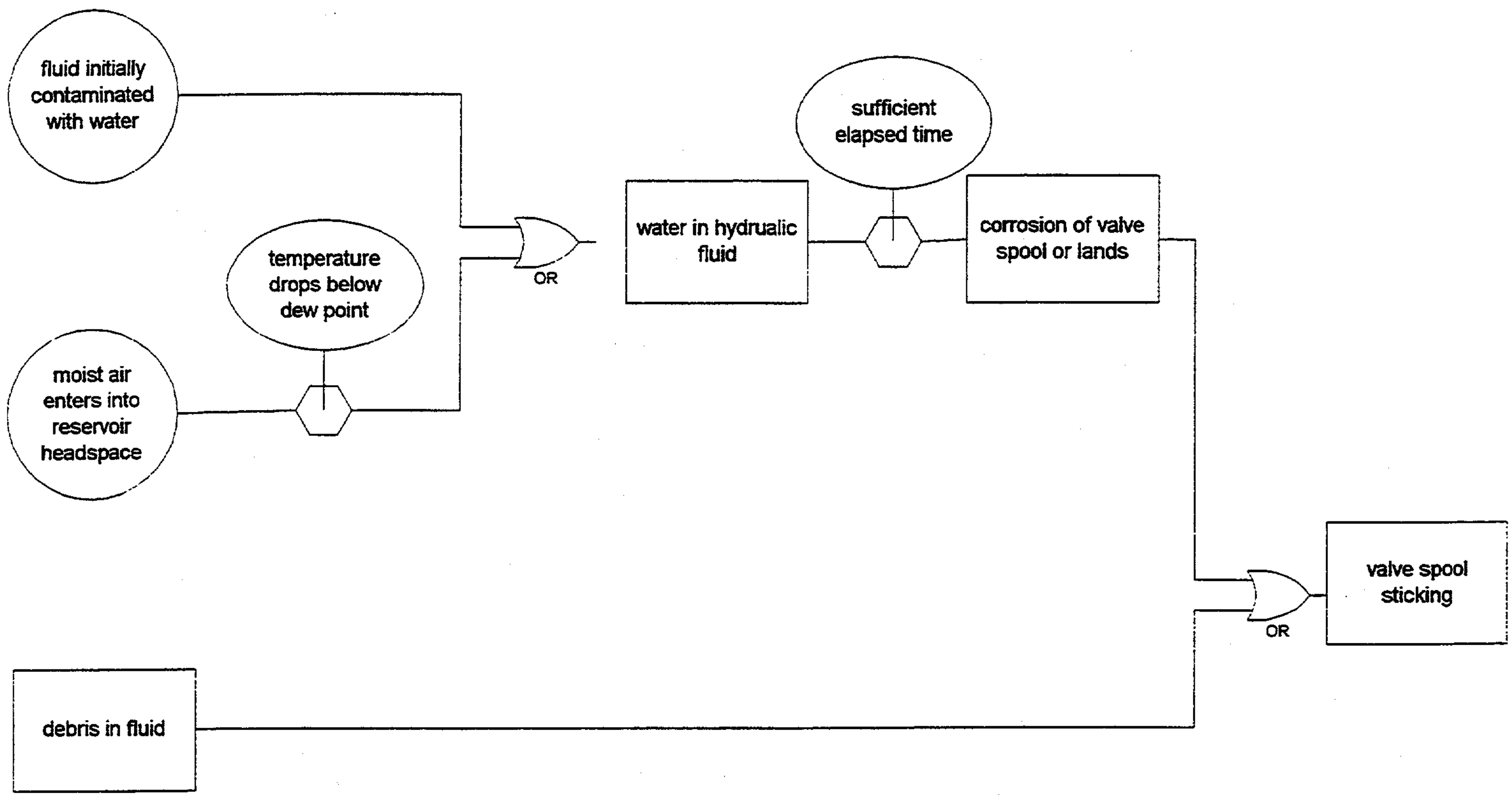

gripper rotate servo fails
repeated 1X more (2X total), once for each gripper rotate joint
uncontrolled gripper rotate joint move
OR
OR
loss of hydraulic continuity to gripper rotate actuator

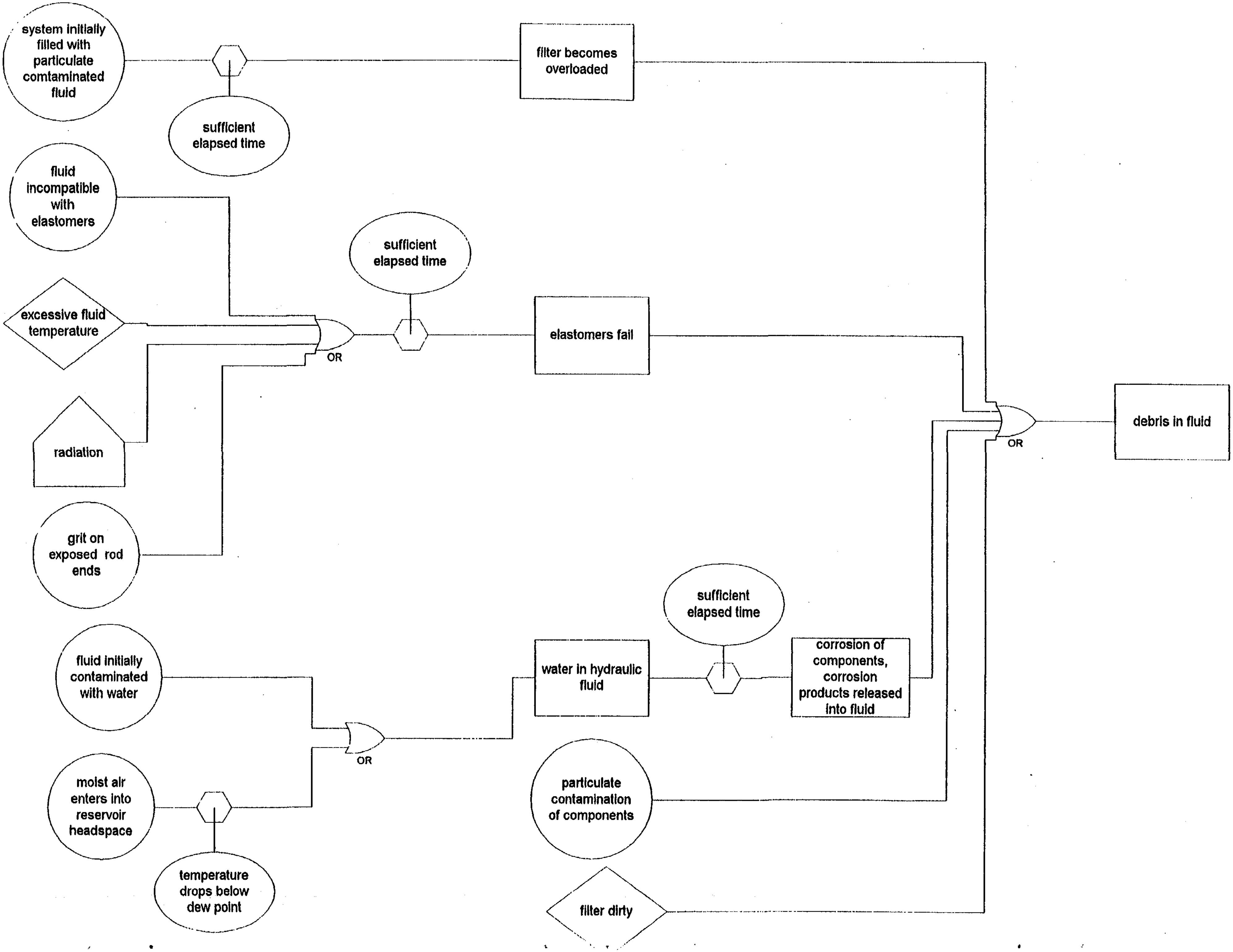

rotate servo fails
repeated 2X more (3X total) , once for each rotate joint
loss of hydraulic continuity to rotate actuator
OR
OR
uncontrolled rotary joint move
rotate resolver failure
AND
loss of position feedback signal
error checking software failure

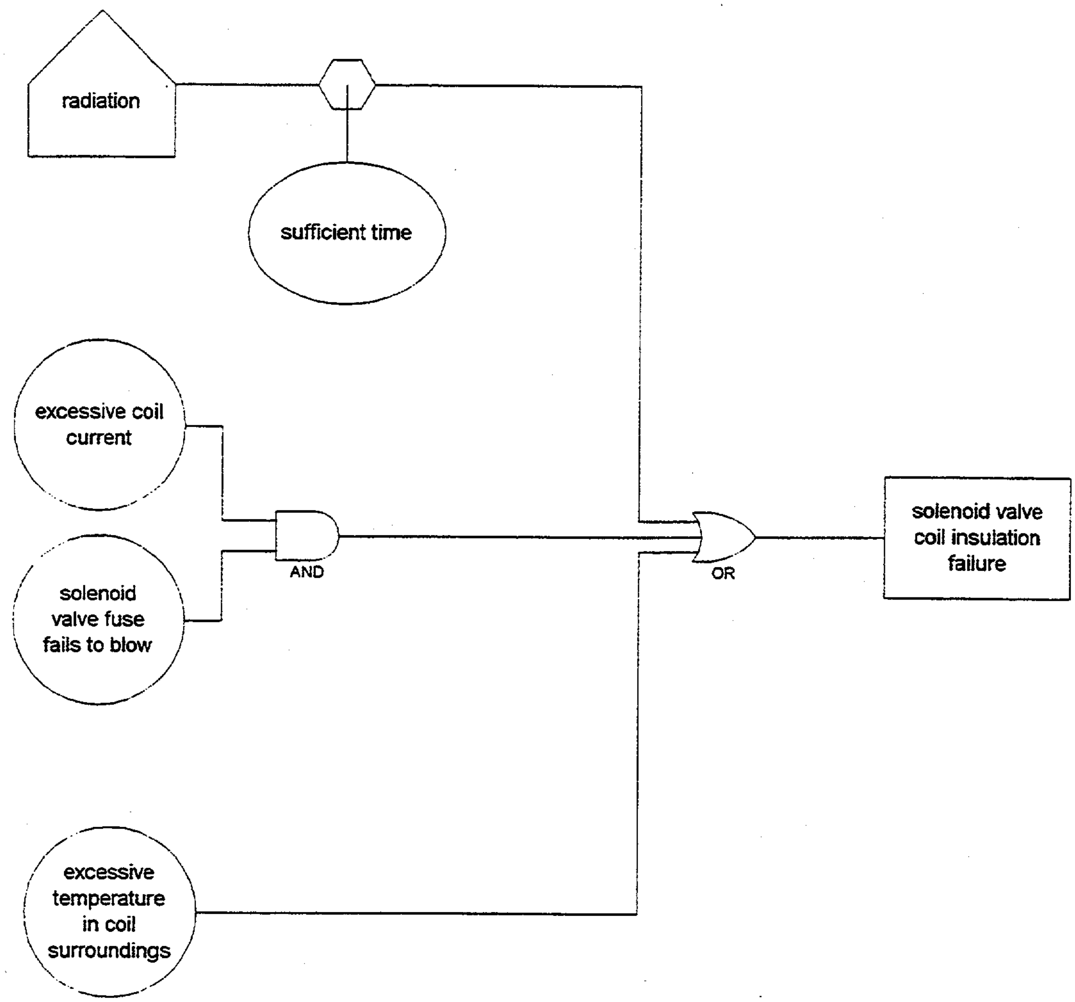

loss of hydraulic continuity to vertical translate actuator
vertical translate servo fails
sufficient time
radiation
high hydraulic fluid temp
debris in fluid
OR
rotary joint crosstalk due to seal damage
OR
uncontrolled vertical translate joint move
corrosion
fatigue
structural overload
failure of a pin on the vertical translator, there are 6 pins
repeated 6X

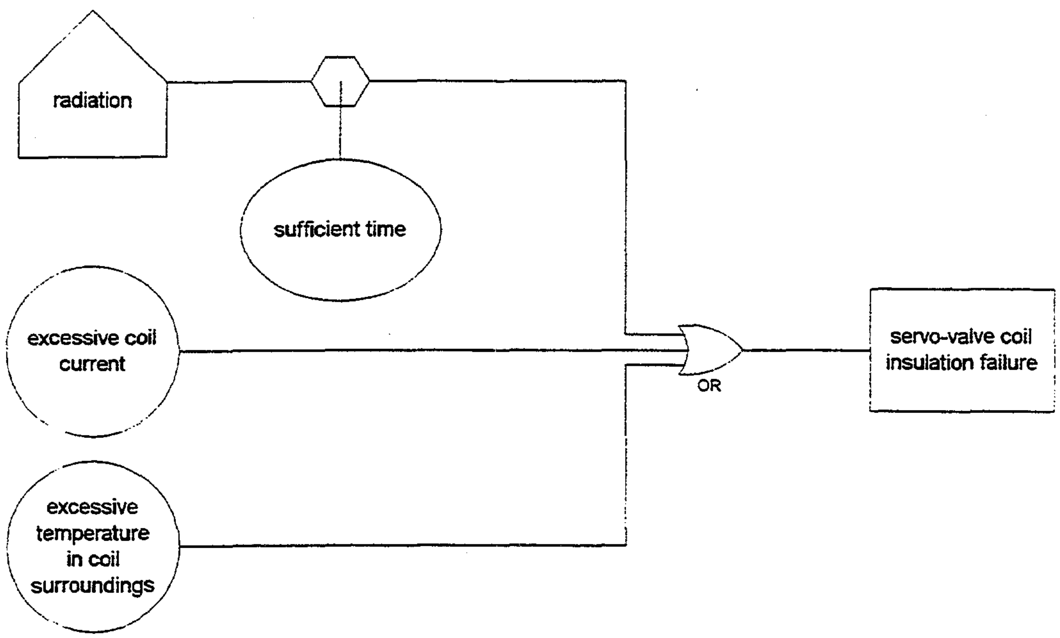

electrical continuity failure
sufficient time
washdown
radiation
failure of contact switch seals
contact switch fail on
OR
interlocks preventing both grips opening failed
OR
relay in control console fails
both grippers inadvertently released
AND
operator error releasing both grips
one grip deliberately released
other grip not securely fastened on pipe
AND
both grips not securely fastened to pipe

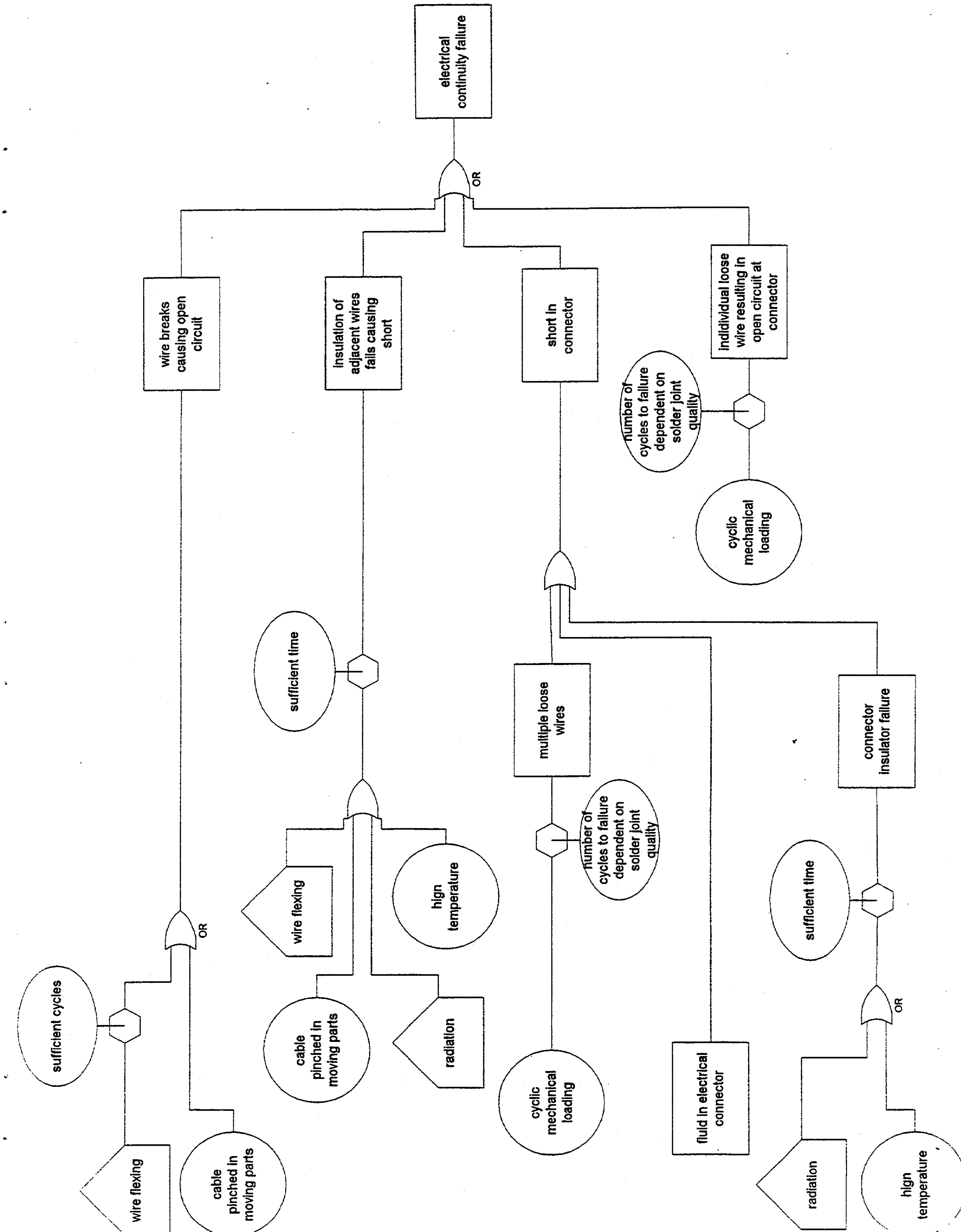

valve spool sticking
debris in fluid
orifice clogged
coil insulation failure
loss of electrical continuity
failure of servo driver card
OR
loss of control of servo-valve

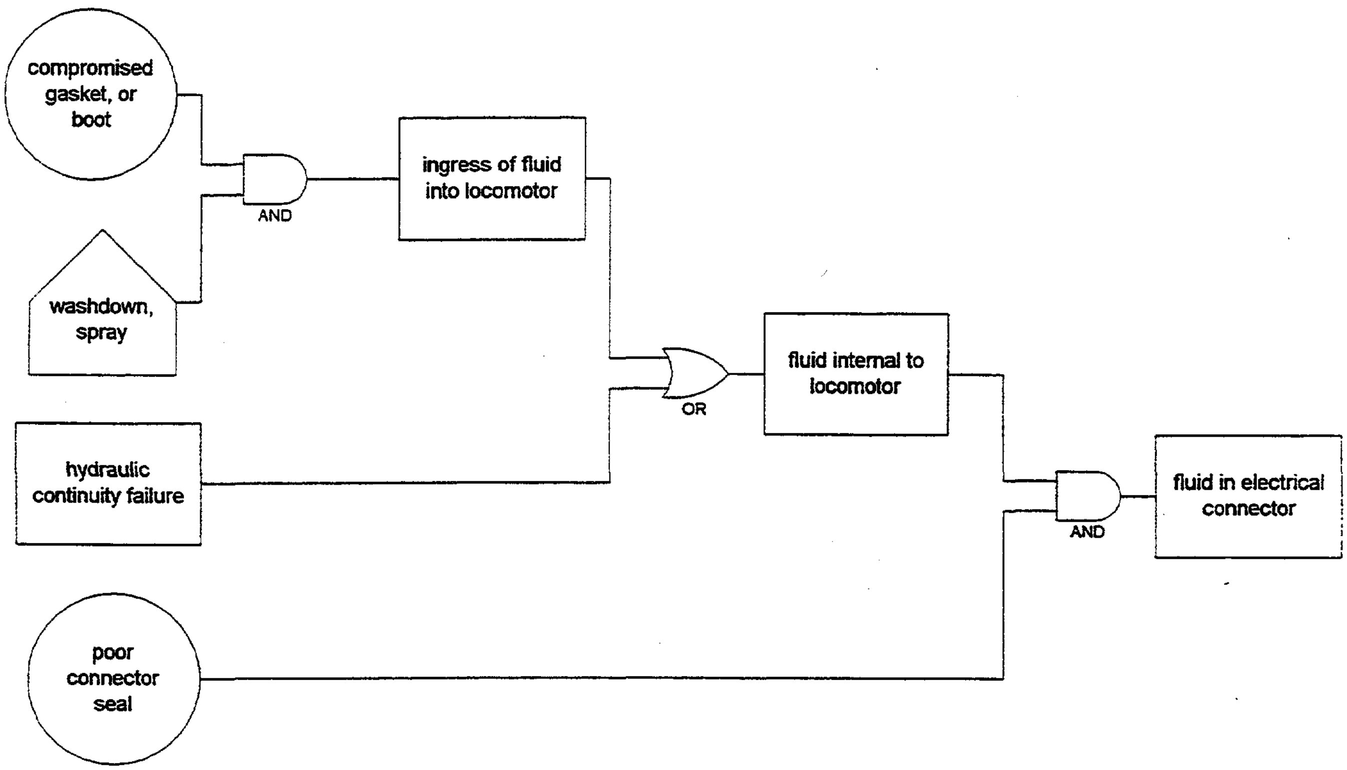

fluid initially contaminated with water
temperature drops below dew point
moist air enters into reservoir headspace
OR
water in hydrualic fluid
sufficient elapsed time
corrosion of valve spool or lands
OR
valve spool sticking
debris in fluid

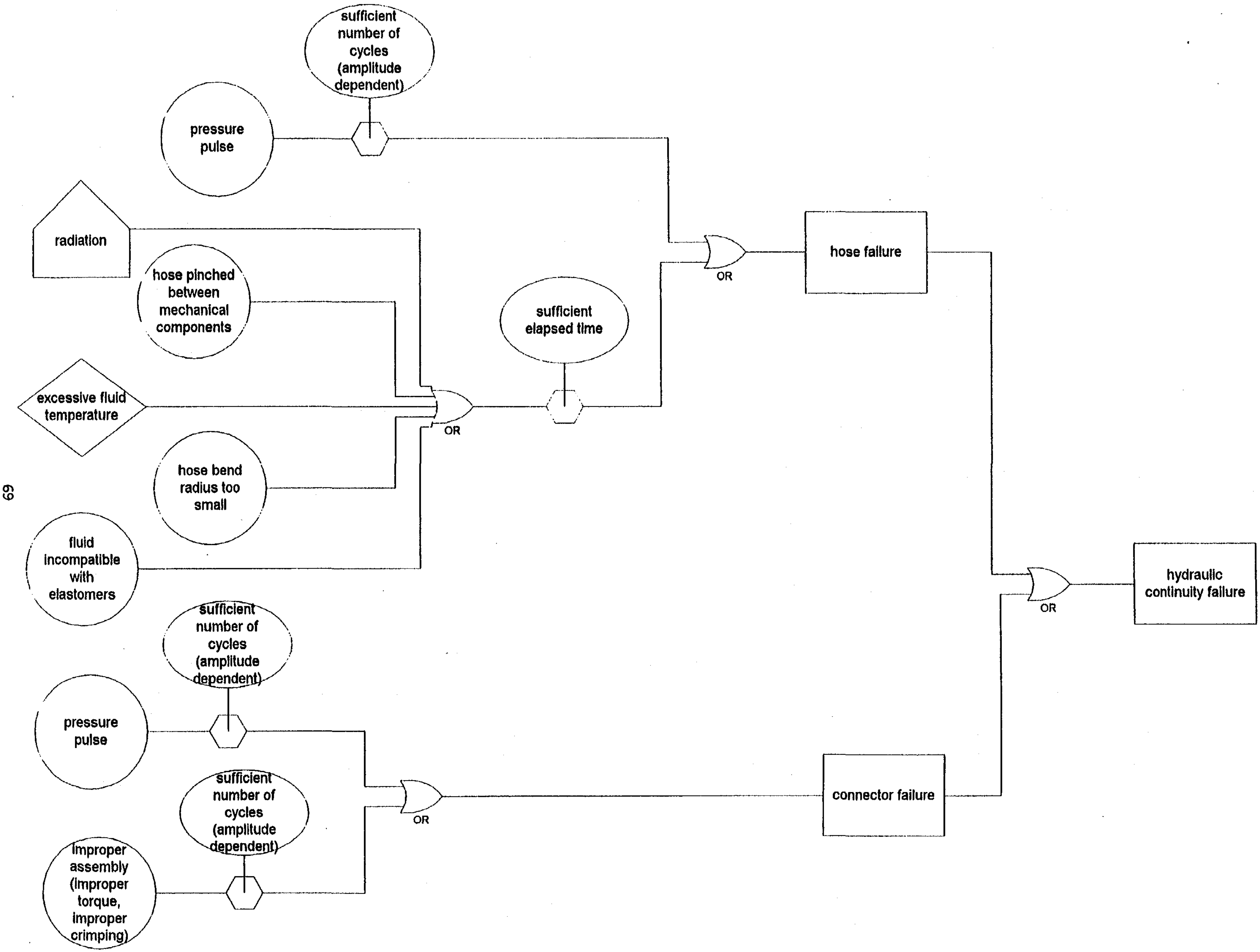

system initially filled with particulate comtaminated fluid
sufficient elapsed time
filter becomes overloaded
fluid incompatible with elastomers
excessive fluid temperature
radiation
grit on exposed rod ends
OR
sufficient elapsed time
elastomers fail
debris in fluid
OR
fluid initially contaminated with water
moist air enters into reservoir headspace
temperature drops below dew point
OR
water in hydraulic fluid
sufficient elapsed time
corrosion of components, corrosion products released into fluid
particulate contamination of components
filter dirty


radiation
sufficient time
excessive coil current
solenoid valve fuse fails to blow
AND
OR
solenoid valve coil insulation failure
excessive temperature in coil surroundings

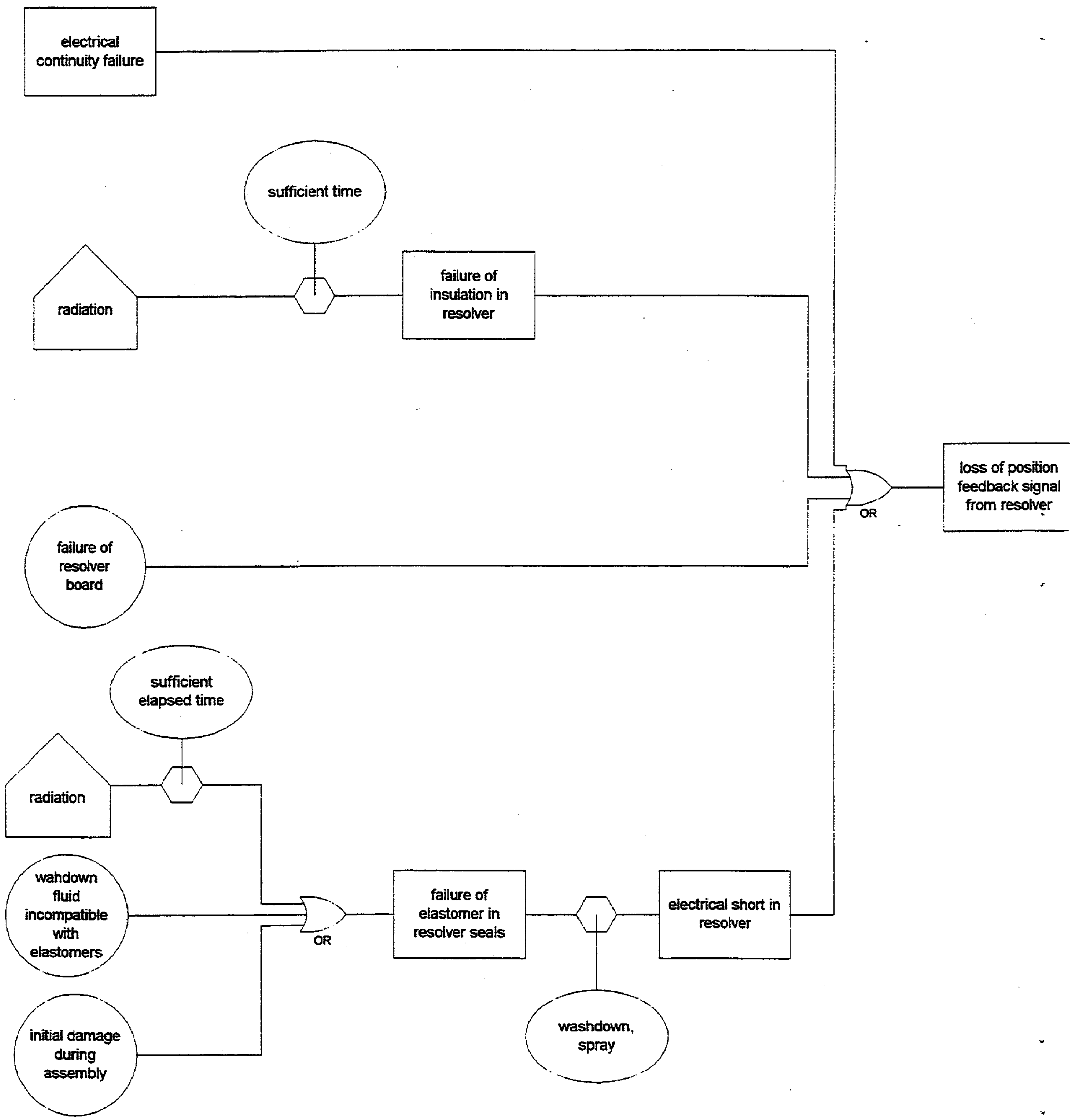

radiation
sufficient time
excessive coil current
excessive temperature in coil surroundings
OR
servo-valve coil insulation failure

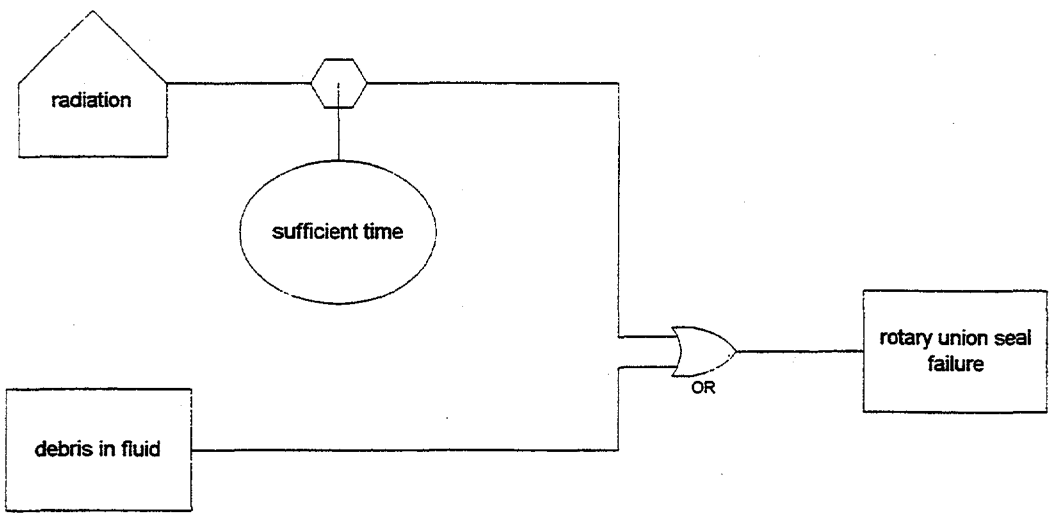

electrical continuity failure
OR
wire breaks causing open circuit
insulation of adjacent wires fails causing short
short in connector
individual loose wire resulting in open circuit at connector
number of cycles to failure dependent on solder joint quality
cyclic mechanical loading
sufficient time
multiple loose wires
connector insulator failure
number of cycles to failure dependent on solder joint quality
sufficient time
wire flexing
high temperature
OR
sufficient cycles
cable pinched in moving parts
radiation
cyclic mechanical loading
fluid in electrical connector
OR
wire flexing
cable pinched in moving parts
radiation
high temperature


compromised gasket, or boot
washdown, spray
AND
ingress of fluid into locomotor
hydraulic continuity failure
OR
fluid internal to locomotor
poor connector seal
AND
fluid in electrical connector



sufficient number of cycles (amplitude dependent)
pressure pulse
radiation
hose pinched between mechanical components
excessive fluid temperature
hose bend radius too small
fluid incompatible with elastomers
OR
sufficient elapsed time
OR
hose failure
sufficient number of cycles (amplitude dependent)
pressure pulse
sufficient number of cycles (amplitude dependent)
Improper assembly (improper torque, improper crimping)
OR
connector failure
OR
hydraulic continuity failure

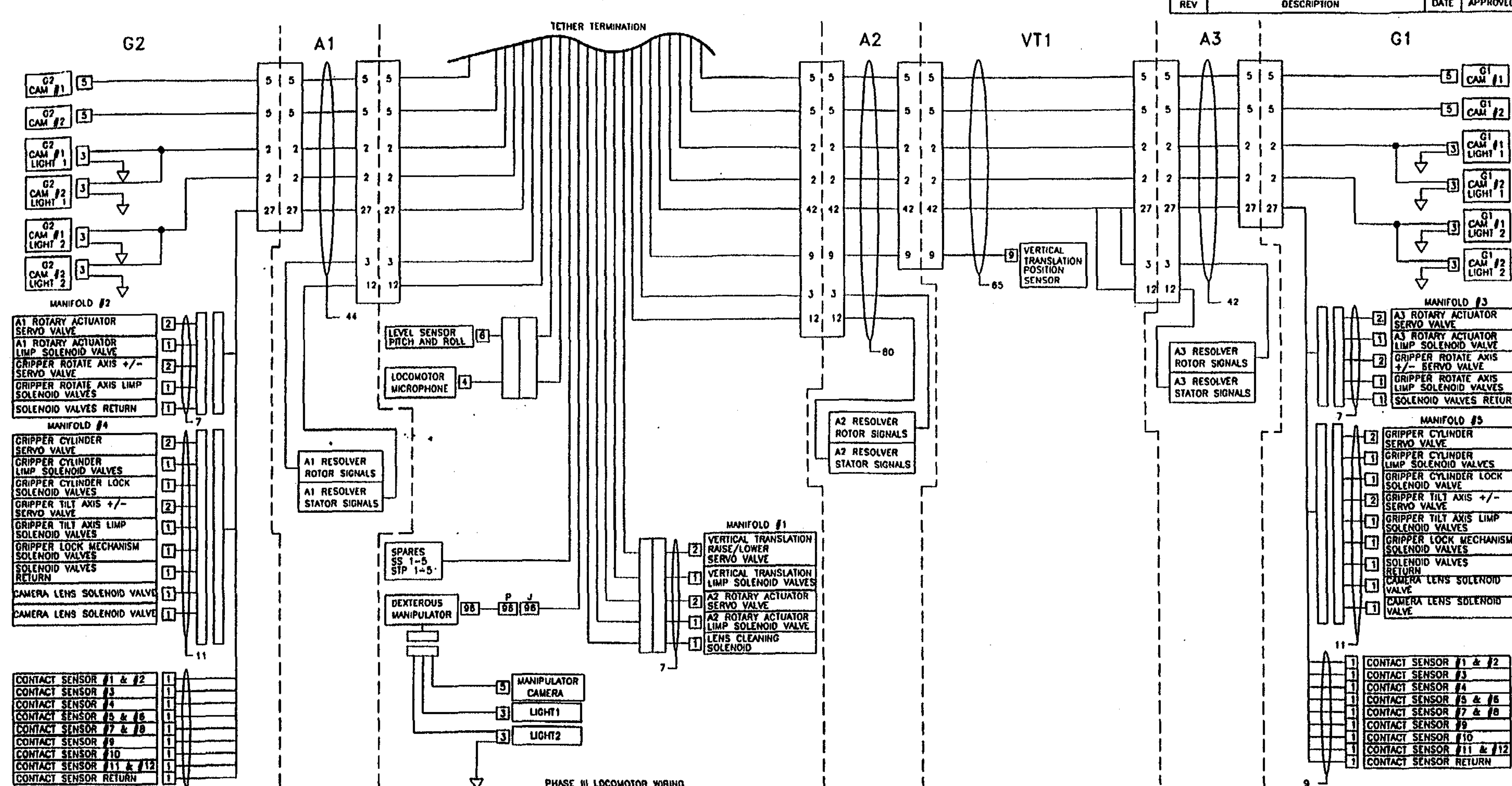

electrical continuity failure
sufficient time
radiation
failure of insulation in resolver
loss of position feedback signal from resolver
OR
failure of resolver board
sufficient elapsed time
radiation
wahdown fluid incompatible with elastomers
initial damage during assembly
OR
failure of elastomer in resolver seals
electrical short in resolver
washdown, spray


radiation
sufficient time
debris in fluid
OR
rotary union seal failure

APPENDIX C

RedZone Hydraulic and Wiring Schematic

REVISIONS			
REV	DESCRIPTION	DATE	APPROVED



INFORMATION ONLY

DASH NO	NEXT ASSY	QTY

UNLESS OTHERWISE SPECIFIED

REMOVE ALL BURRS AND BREAK ALL SHARP EDGES TO .015 MAX.
CHAMFER 1ST THREAD ON EXTERNAL THREADS 45°.
C'SK 1ST THREAD OF TAPPED HOLES 90° TO MAJOR DIA.
DIMENSIONING AND TOLERANCING IN ACCORDANCE WITH ASME Y14.5M-1994.

DO NOT SCALE DRAWING
ALL DIMENSIONS ARE IN INCHES
TOLERANCES: X.XX ±.020 X.XXX ±.005 ANGLES ±0°30'
SURFACE TEXTURE 125

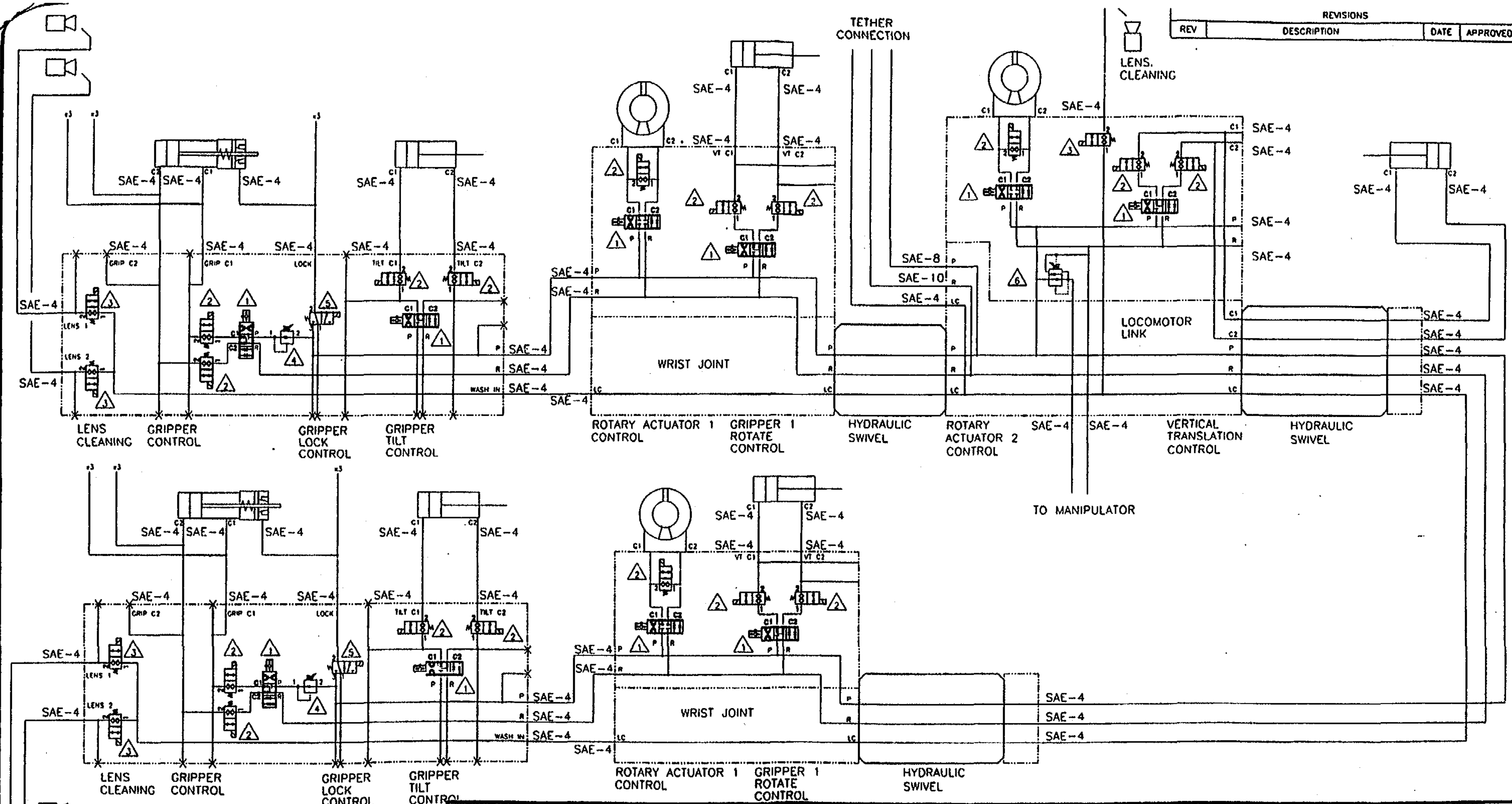
THIRD ANGLE PROJECTION | TREATMENT: | MATERIAL:

AUTHORIZATION		
DFTG:	MGD	3/11/98
DSGNR:		
CHKR:		
ENGR:		
APP:		
APP:		

REDZONE ROBOTICS, INC. 2425 LIBERTY AVENUE PITTSBURGH, PA 15222-4639 412-765-3064

LOCOMOTOR WIRING BLOCK DIAGRAM

CAGE CODE	SIZE		REV
0K896	B	98004006	5



1. MOOG, 30 SERIES, SERVO VALVE
2. HYDRAFORCE, SV08-26, SOL. VALVE, 2-WAY
3. SPARTAN SCIENTIFIC, 3800 SERIES, SOL. VALVE
4. SUN HYDRAULICS, PBDB-LAN, PRESSURE REDUCING VALVE
5. HYDRAFORCE, SV08-30, SOL VALVE, 3-WAY
6. SUN HYDRAULICS, PPDB-LAN, PRESSURE REDUCING/RELIEVING VALVE

DASH NO	NEXT ASSY	QTY
DRAWING REFERENCE		

UNLESS OTHERWISE SPECIFIED

REMOVE ALL BURRS AND BREAK ALL SHARP EDGES TO .015 MAX.
CHAMFER 1ST THREAD ON EXTERNAL THREADS 45°.
C'SK 1ST THREAD OF TAPPED HOLES 90° TO MAJOR DIA.
DIMENSIONING AND TOLERANCING IN ACCORDANCE WITH ASME Y14.5M-1994.

DO NOT SCALE DRAWING
ALL DIMENSIONS ARE IN INCHES
TOLERANCES: X.XX ±.020; X.XXX ±.005; ANGLES ±0.50°
SURFACE TEXTURE 125

THIRD ANGLE PROJECTION
TREATMENT:
MATERIAL:

AUTHORIZATION		
DFTG:	RJG	03/13/98
DSGNR:		
CHKR:	[signature]	6/19/98
ENGR:	[signature]	6/19/98
APP:		
APP:		

REDZONE ROBOTICS, INC.
2425 LIBERTY AVENUE
PITTSBURGH, PA 15222-4639
412-765-3064

LOCOMOTOR HYDRAULIC SCHEMATIC

CAGE CODE	SIZE		REV
0K896	B	98004017	–
SCALE: 1:8	WEIGHT:	SHEET 1 OF 1	

REVISIONS			
REV	DESCRIPTION	DATE	APPROVED

APPENDIX D

Locomotor Description Document

Locomotor Description Document

Document Number: 98004-REPT-004.1

Prepared for
West Valley Nuclear Services

Release Date: June 19, 1998

Prepared by
RedZone Robotics, Inc.
2425 Liberty Avenue
Pittsburgh, PA 15222-4639
412-765-3064

Thomas Miller
Project Manager

Frank Robb
Mechanical Engineer

Table of Contents

List of Figures

Section 1: Introduction

The Remote Tool Delivery (RTD) system overcomes many of the limitations of existing tank waste retrieval technologies. The RTD system converts the liability of extensive internal structures into an asset during tank waste retrieval. The tank internal structure is used as "scaffolding" to gain access to the tank interior, walls, ceiling, and floor. The RTD system is inserted into the tank by a Deployment Unit through a tank riser and rotated to its operating position. The RTD system can be operated from its deployment mast to perform tasks in the immediate area of the riser or, the RTD locomotor can "step off" the deployment mast and support itself on adjacent structures in the tank.

In such cases where greater mobility is needed, the RTD locomotor reaches out and secures itself to a nearby existing structural member inside the tank and then releases from the Deployment Unit mast. The RTD locomotor can then navigate around the tank by moving from structural member to structural member. The RTD locomotor can also translate vertically in the tank. The combined motion capabilities of The RTD locomotor allow it to reach all areas and elevations of a tank, provided sufficient structural members exist.

The RTD locomotor performs work by manipulating tools or equipment using a dexterous manipulator mounted on the locomotor. The RTD system can work alone or as a companion technology to a long-reach arm or floor-based system to perform waste retrieval.

The RTD system consists of four major components: an Operator Control Station, a Hydraulic Power Supply, a Deployment Unit, and the RTD locomotor. This document describes the RTD locomotor.

2.1 RTD Locomotor

The RTD locomotor is a three joint planar work platform that operates attached to a deployment mast or to the pipe columns in the tank (Figure 2-1). The locomotor is comprised of seven major components: grippers, link, joints, vertical translation mechanism, locomotor hydraulic system, dexterous manipulator and video system. The components of the RTD locomotor are described in the following sections.

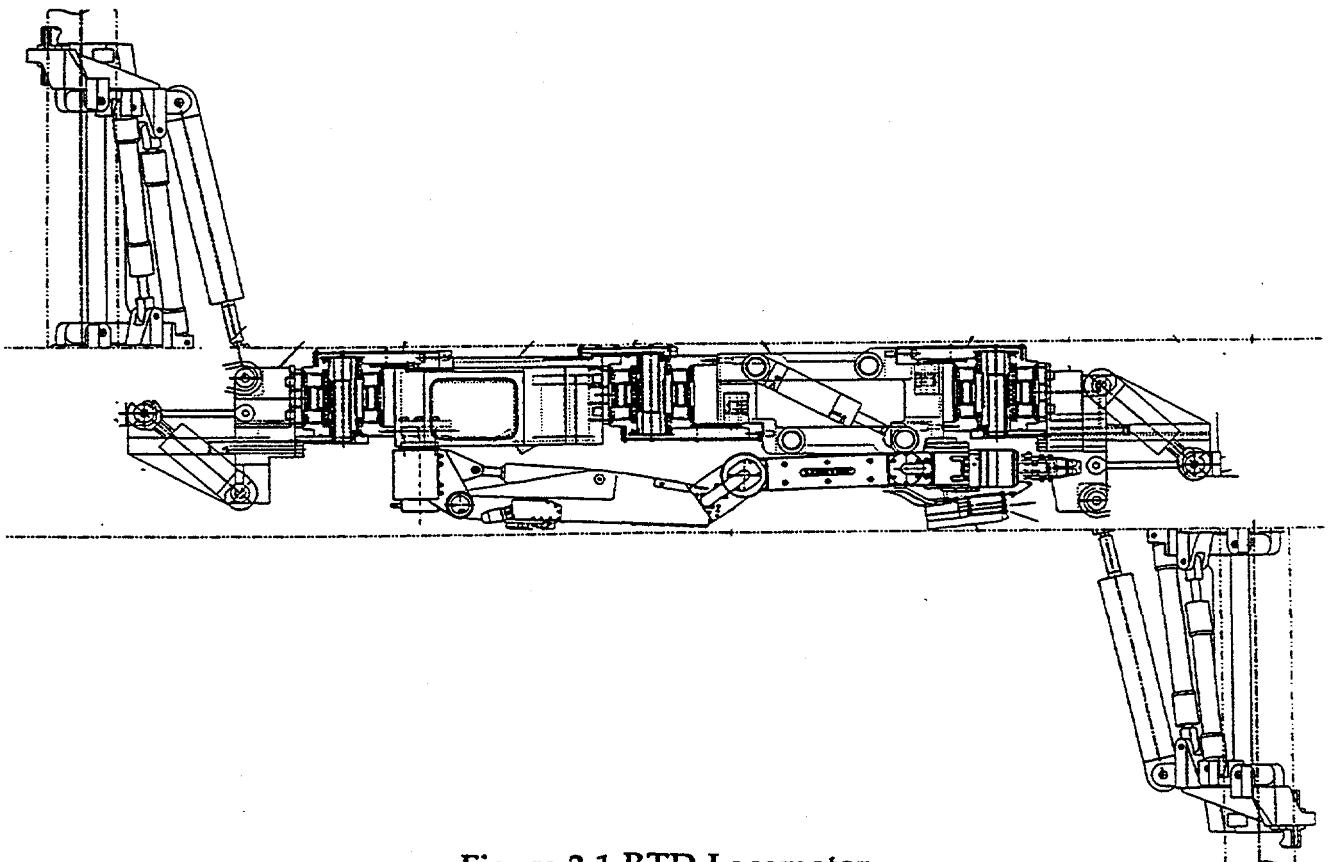


Figure 2-1 RTD Locomotor

2.2 Gripper Mechanism

The grippers on the RTD locomotor provide the following functions:

1. They secure the locomotor to the deployment mast during deployment and retrieval, or when the locomotor is used as a mast mounted manipulator to perform work tasks in the area of the deployment riser.

2. They secure the locomotor to the internal tank structure when the locomotor is used as a mobile platform for the dexterous manipulator.

A gripper mechanism is mounted to both ends of the RTD locomotor. Each gripper mechanism consists of a gripper base and a gripper frame assembly which supports the pipe column gripping components. The gripper frame assembly is connected to the gripper base with a two degree of freedom actuated linkage (See Figure 2-2). The gripper base connects to the locomotor joint.

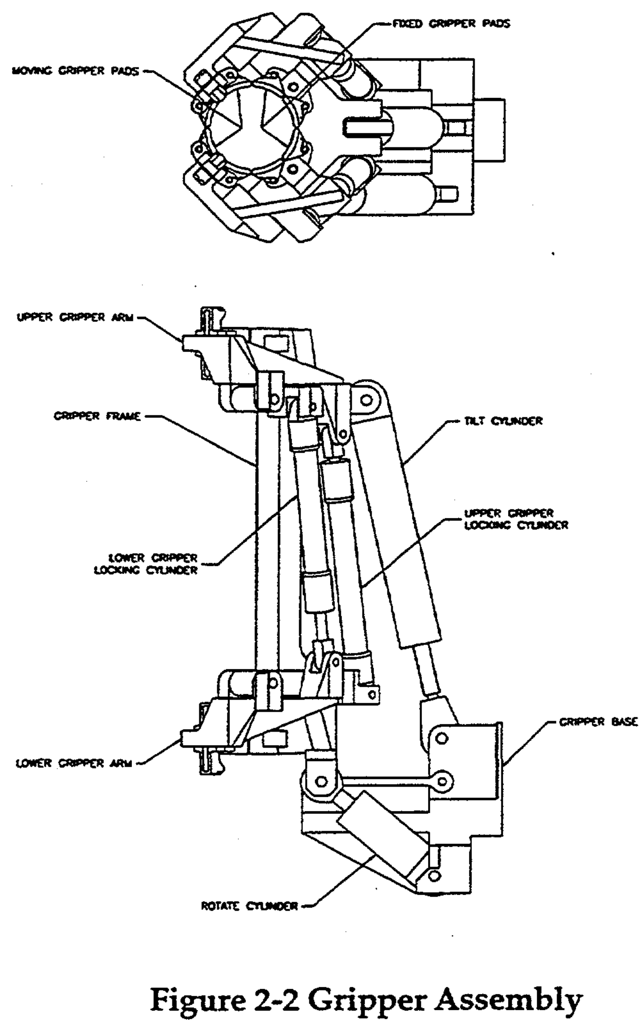


Figure 2-2 Gripper Assembly

Each gripper assembly has 16 gripper pads which make contact with the tank pipe column. The pads are mounted in pairs on pivoting links. The pads are free to pivot in the pivoting links. This double pivot allows best possible alignment of the gripper pads to the pipe column for load distribution. Four pairs of gripper pads are mounted to moving arms. The arms open to allow the gripper to be removed from a pipe column and provide adjustment to allow the gripper to close securely on different pipe diameters. Hydraulic cylinders are used to actuate the moving arms. Each moving arm has a hydraulic cylinder. The hydraulic cylinders for the moving arms contain an integral locking feature to secure the gripper to the pipe column in the event of a hydraulic system failure. A contact switch is located at each pair of gripper pads. The contact switches give a positive indication that the gripper is properly seated on the pipe column.

The gripper mechanism has three modes of operation: *open*, *close*, and *lock*.. The open mode (Figure 2-3) moves the gripper arms to release the gripper from a pipe column. The close mode (Figure 2-4) moves the gripper arms to secure the gripper to a pipe column. The lock mode holds the gripper arms in a fixed position to prevent the gripper from releasing from a pipe column. The gripper defaults to the lock mode of operation should a failure occur.

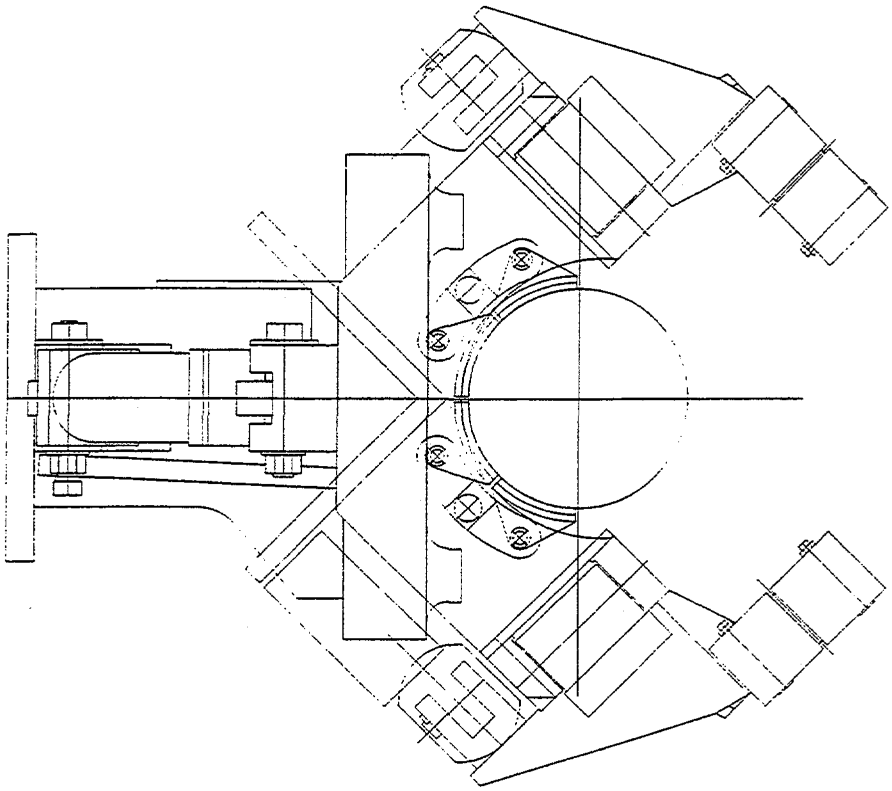


Figure 2-3 Gripper Assembly - Top View - Open

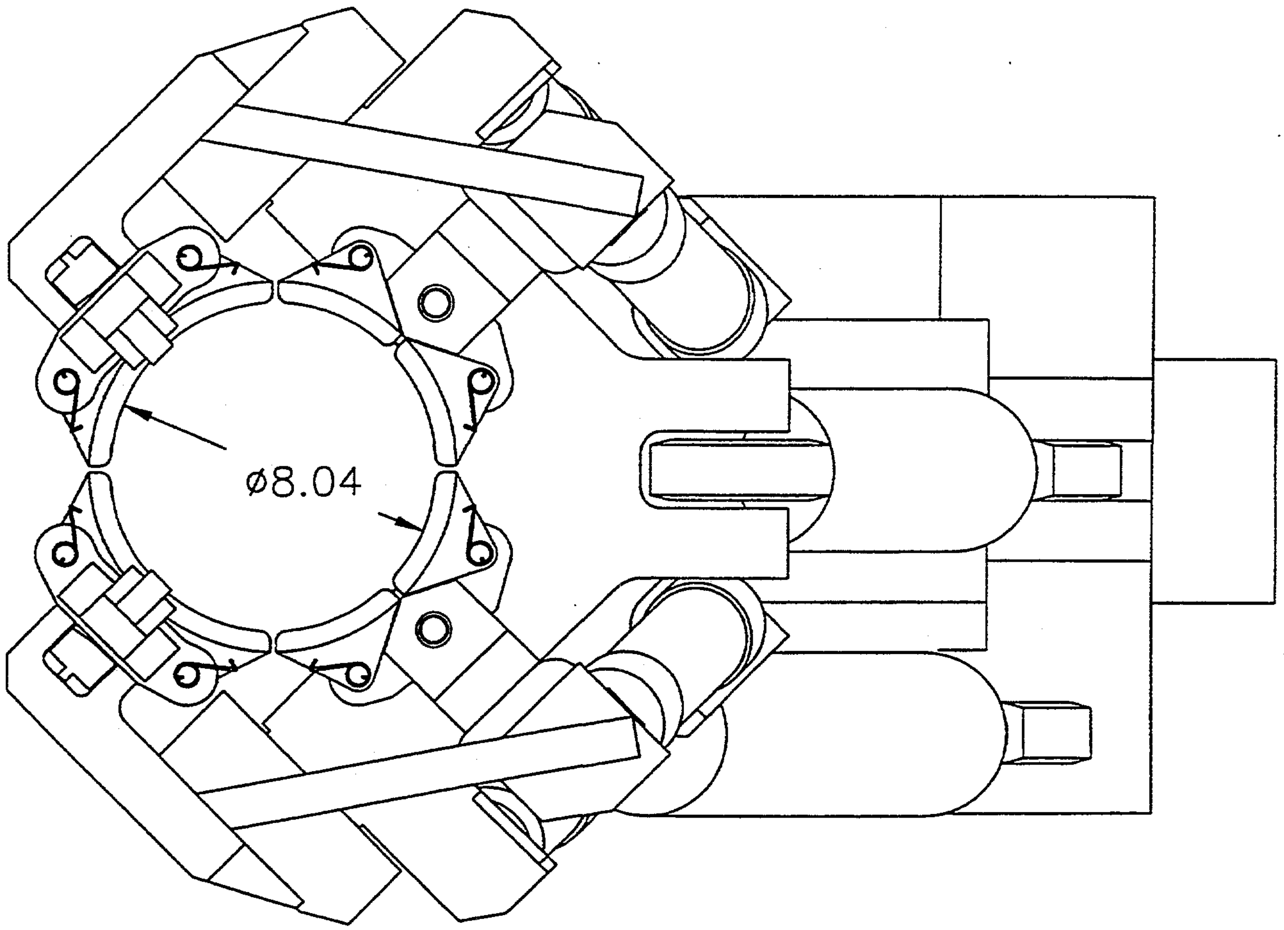


Figure 2-4 Gripper Assembly - Top View - Closed

The gripper mechanism is designed to minimize the contact stresses induced in the tank pipe columns while providing sufficient rigidity for locomotor and dexterous manipulator operations.

The grippers are fabricated from aluminum for weight reduction. Electroless nickel plating overcoated with epoxy paint is used for corrosion protection of the aluminum.

2.3 Vertical Translation Mechansim

A vertical translation mechanism is provided so that the height of the locomotor in the tank can be changed (See Figure 4-3). The vertical translation mechanism is as an actuated four bar linkage. The linkage is operated by a hydraulic cylinder placed on the diagonal of the linkage. The cylinder produces +/- 6 inches of vertical motion of the linkage. An LVDT provides mechanism position information to the operator. The position sensor is needed so that the locomotor can be aligned for deployment and retrievial.

The vertical translation mechanism has four modes of operation: *raise, lower, limp,* and *hold*. The raise and lower modes are used to move the mechanism in the vertical direction, and the hold mode is used to maintain a fixed position. The fail-safe state of the vertical translation mechanism is the limp mode.

The links and end connections for the vertical translation mechanism are made from titanium.

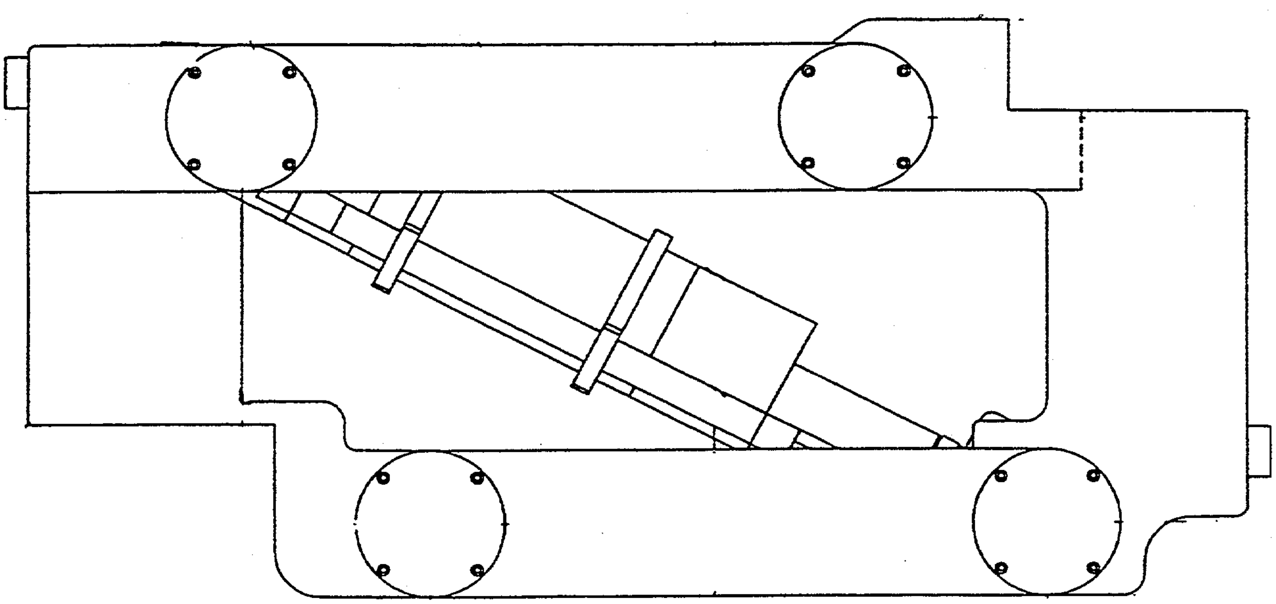


Figure 4-3 Vertical Translation Mechanism

2.4 Link

A link connects two of the locomotor joint rotary actuators on the RTD locomotor. The link provides a structural connection between the two actuators. It also provides an attachment point for the tether termination as well as distribution of hydraulic and electrical circuits. The dexterous manipulator is mounted on the link.

The interior of the link serves as an electrical cable and hydraulic hose passageway. All hoses and cables on the locomotor are internally routed where possible to prevent damage from contact with tank structure to improve system reliability.

The link is fabricated from aluminum for weight reduction. Electroless nickel plating overcoated with epoxy paint is used for corrosion protection of the aluminum.

The link is designed to minimize the decontamination time for the locomotor. The exterior surfaces of the link are smooth to prevent contamination buildup, and the internal chamber of the link is sealed to prevent internal contamination.

2.5 Joints

Three locomotor joint assemblies are used in the RTD locomotor. Each locomotor joint is a modular assembly containing a hydraulic rotary vane actuator with integral bearings, a hydraulic rotary union, and a position sensor. (See Figure 2-6) The joint has low friction to enable a limp fail-safe condition. The integral rotary union passes hydraulic fluid between locomotor links. A through-hole in the rotary union allows electrical cables to pass through the rotary joint. Each joint contains a resolver for position sensing. The resolver provides absolute position feedback. Resolvers are used for their resistance to interference and degradation by ionizing radiation. Actuator specifications are given in Table 2-1.

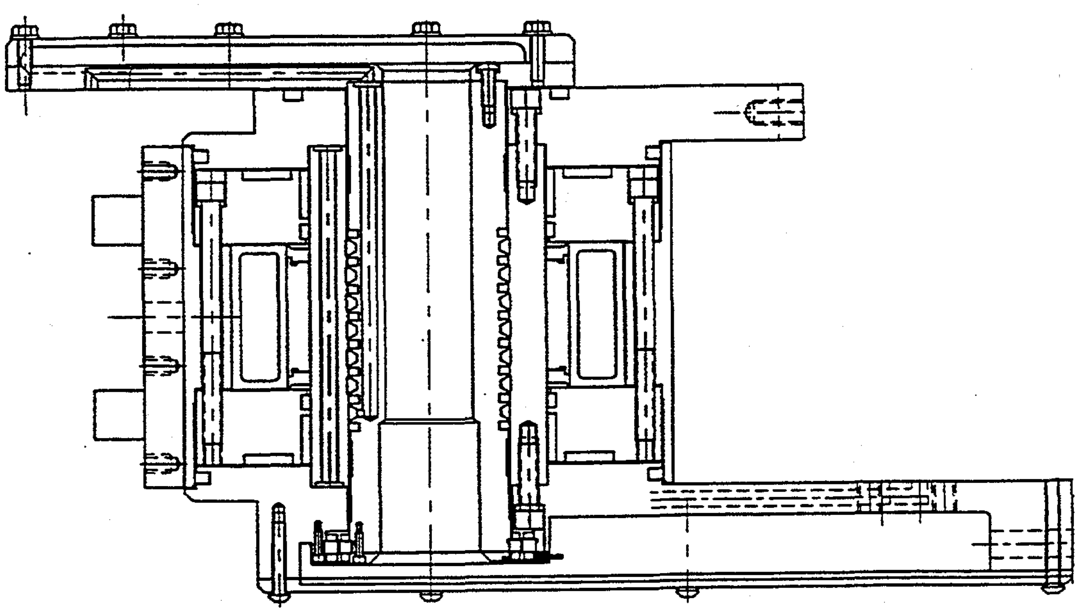


Figure 2-6 Locomotor Joint

Actuator Style	Single Vane Type, Double Shaft Configuration
Hydraulic Fluid	Shell Tellus 32 mineral oil
Ambient Temperature	0 °F to 100 °F
Environment	Caustic, pH 9 - 12, may be pH4-6 for short period
Actuator/Swivel Friction	250 ft-lbf maximum
Cross Vane Leakage	0.1 gpm maximum at suggested operating pressure
Swivel Leakage Rate	0.01 gpm to Tank line at 3000 psi No leakage between other passages or to external
Radiation	Peak Dose Rate of 500 rad/hr Total Cumulative Dose of 10^7 rad
Rotation Travel	270 deg
Rotational Speed	10 deg/sec maximum
Torque	31,000 in-lbf minimum
Operating Pressure	3,000 psi
Moment Load	150,000 in-lbf
Axial Load	1800 lbf

Table 2-1 Locomotor Joint Specifications

The locomotor joints are fabricated from 4130 steel with a corrosion protective finish.

2.6 Locomotor Hydraulic System

The locomotor hydraulic system, in conjunction with control electronics, provides controlled motion of the locomotor joints, grippers and vertical translation mechanism. Hydraulic fluid is supplied to the locomotor by pressure and return hoses in the tether. Hydraulic fluid is also supplied to the dexterous manipulator.

The locomotor hydraulic system uses radiation hardened servo valves and directional control valves to operate the hydraulic actuators. The servo valve electronics are located outside the tank environment to protect them from radiation exposure. Hydraulic manifolds in the locomotor provide hydraulic power distribution throughout the locomotor and mounting locations for the servo and directional control valves.

Additional valves are needed to meet fail-safe requirements, i.e., fail-safe limp of the locomotor joints and vertical translation mechanism. These valves are also incorporated in the manifolds.

A multi-passage hydraulic rotary joint is incorporated into the locomotor joint rotary actuator to pass fluids through the locomotor. This provides a more compact design and eliminates the use of hoses in this high flex area.

Stainless steel tubing and manifold passages are used where possible to minimize the use of flexible hoses to improve reliability. Figure 2-7 shows the hydraulic schematic of the locomotor.

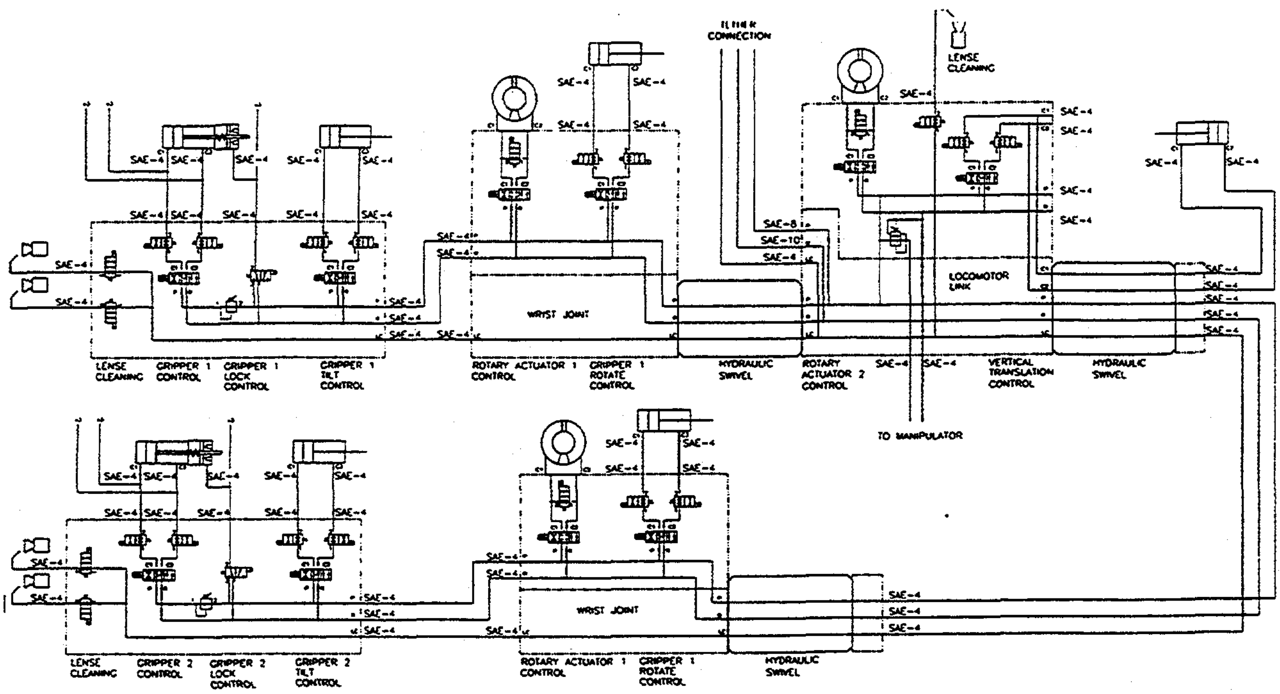


Figure 2-7 Locomotor Hydraulics Schematic

2.7 Video System

Five black and white camera and light assemblies are used on the locomotor. Two cameras are mounted on each gripper to assist the operator in positioning the gripper on the pipe column. One camera is mounted on the dexterous manipulator to provide a view of the manipulator work area. This camera can also be used to provide some overview capability.

All of the cameras are based on the Rees R980 camera with a Chalnicon image tube. This camera will operate at a dose rate of 10^5 rad/hr and survive a total dose of 10^8 rad. This comfortably exceeds the dose rate and total dose expected for the RTD system. Customized housings are used for all cameras. The cameras and lights are sealed for underwater use. Mounting of the lights is designed to minimize heat transfer to the cameras.

Lens cleaning is provided by a water/air spray nozzle at the camera. Lens cleaning is initiated from the Operator Control Station. A separate lens cleaning control is provided for each camera. A spray of water from the nozzle dislodge waste material from the camera lens. A subsequent air blast removes water droplets. This lens cleaning system has been demonstrated on the Houdini™ system at ORNL and is very effective.

2.8 Dexterous Manipulator

The locomotor is equipped with a dexterous manipulator to perform work in the tank. The dexterous manipulator is mounted to the locomotor link. The locomotor is used as a mobile base for the dexterous manipulator. The dexterous manipulator is controlled from the Operator Control Station.

A Schilling Titan T3 manipulator is used. Specifications for the Titan T3 manipulator are listed in Table 2-2. The payload capacity of the Titan T3 manipulator is limited to 100 lbf by a pressure regulating valve in the locomotor.

Payload	180 lbf at full reach at 3000 psi
Reach	75.4 inches
Wrist Torque	60 ft-lbf
Jaw Closure Force	1000 lbf
Weight	221 lbf
Operating Pressure	3000 psi maximum
Hydraulic Fluid	Shell Tellus 32 or equivalent

Table 2-2 Titan T3 Manipulator Specifications

2.9 Locomotor Control Strategy

Two locomotor control methods are provided for the operator to move the locomotor in the tank. The control method will be selected with a switch on the control console. The control methods are described below.

2.9.1 Joint Control

The simplest method for controlling the motion of the locomotor is independent control of each joint. A rocker switch is provided for each locomotor joint. Each joint is servo controlled and will follow the control input. Joint speed will be limited to prevent unwanted locomotor dynamics.

2.9.2 Coordinated Joint Motion

With this control method, the rotation of all three joints will be coordinated by the control system to achieve the operator specified movement of the free locomotor gripper. A three degree of freedom joystick will be used to control the position and orientation of the free gripper of the locomotor. The control system will determine the required motion of the actuators to achieve the desired gripper position and orientation. Joint speed will be limited to prevent unwanted locomotor dynamics.

Appendix 1: Revision History

98004-REPT-004.1 Initial Release

APPENDIX E

Summary Design Criteria Document for RTD System

WEST VALLEY NUCLEAR SERVICES CO., INC.
10282 ROCK SPRINGS ROAD
P.O. BOX 191
WEST VALLEY, NY 14171-0191

FAX MESSAGE

ATTENTION: Joel Chesser ORNL

TELEPHONE NO. (423)574-6327 **FAX NO.** (423) 576-2081

DATE: 9/25/98 **NO. OF PAGES** (including cover page): 8

SUBJECT: Summary Design Criteria Document for RTD System

Joel,

See attached WVNS-SDC-018, Rev 1, dated 2/11/98.

G. Bernatz

George F. Bernatz
Advanced Tank Farm Equipment
(716) 942-4310
FAX 942-2193

SUMMARY DESIGN CRITERIA

Remote Tool Delivery (RTD) System for Tanks 8D-1 and 8D-2
(Project Title)

WVNS-SDC-018

Revision Number 1

Revision Date 02/11/98

ER/ECN No. ER #3984
ECN #11262

NOTE: If the Summary Design Criteria is being developed for a component rather than a system or facility - follow questions in EP-3-002 Section 4.4 before proceeding. If HLW designation is "YES" this form cannot be used.

HLW: ______ N/A X NO ______

1.0 Programmatic Information

1.1 System number 55A

1.2 Need date for conceptual design 8/97

1.3 Total project budget (if available) $ Rough Estimate - $3.5M

1.4 Project Completion dates and milestones (if available) 3/99

2.0 Complete statement of the problem

2.1 Specific description of the need Provide a remotely operated tool delivery system for waste retrieval, tank cleaning, viewing and inspection within HLW tanks 8D-1 and 8D-2. The RTD system will deploy through a riser and provide the mechanical means for tank cleaning, viewing and inspection. The RTD system will provide a stable, yet moveable mounting platform inside the tank for a dexterous manipulator arm and visual inspection equipment and is capable of using a variety of tools such as spray wands, suction wands, and other end effectors in order to mechanically clean and then inspect the inside of the tank. The RTD system shall permit viewing greater than 99.9 percent of the tank floor, walls and internal structural members. Tank internal structural members make it very difficult to maneuver the RTD system within the tank. The RTD system includes a moveable mounting platform dexterous manipulator arm, camera/lights, attachment interface for a variety of end effectors, cable/hoses, cable/hose management system, deployment equipment, power supply unit and operator control station.

2.2 Radiological considerations Exposure to high radiation field (500 R/hr peak) of gamma radiation from predominately cesium 137 source within the HLW tanks. The in-tank equipment shall function during and after immersion in the waste liquids, and be able to be decontaminated without damage from sprayed pressurized water (10,000 psi maximum) that may contain decontamination chemicals such as detergents and nitric acid. The design shall minimize internal sharp corners, crevices, and internal and external pockets that may trap contamination.

2.3 Operational parameters Remotely operated; use of a mobile crane is prohibited for normal operation and service; incorporate provisions for fail-safe operation; remotely retrievable when operational and in the event of equipment failure; maximize the reliability of all components; be easily maintained; operator controls shall be user friendly.

2.4 Equipment interfaces 1) All risers in tank 8D-1 and 8D-2 with a nominal internal diameter of 25 inches at the tank top 2) Tank pump support truss structure 3) Rotek bearing assembly of mobilization pump 4) High-Level Liquid Waste Storage (WTF-System 8) 5) Sludge Mobilization and Transfer System (SMTS-system 55)

2.5 Functional requirements 1) The RTD system shall be able to move and position tools and equipment to provide complete wash down capability of the tank floor, walls and internal structural members (up to 12 feet off of the tank bottom for tank 8D-1 and up to 22 feet off of the tank bottom for tank 8D-2).

2) The RTD system shall be able to position visual inspection equipment (camera/lights) to view greater than 99.9 percent of the tank floor, walls, and internal structural members.

3) The RTD system shall include a dexterous manipulator arm and be able to move/handle a payload of 100 lbs. minimum at the end of the dexterous manipulator arm (A payload capacity of 200 lbs. Is desirable but not required).

4) The RTD system should use a Rees R93/04 camera (or approved equivalent) with zoom and air purge on the lens and provide remote pan/tilt movement of the camera/lights.

5) The RTD system shall be supported by the existing mobilization pump support structure (truss) and if possible, should utilize the existing mobilization pump's "Rotek" bearing assembly.

6) The RTD system shall be capable of being deployed into tank 8D-1 or 8D-2 using any riser with a nominal diameter of 25 inches at the tank top, decontaminated, removed and relocated to another riser. In addition, the RTD in-tank equipment shall fit within a 23 inch diameter envelope established by a decontamination spray ring located in the riser just above the opening into the tank. If the RTD system incorporates features for decontamination of the in-tank equipment and tether, thereby eliminating the need for the decontamination spray ring, the envelope size may be increased to 24.75 inch diameter.

7) Be retrievable by remote means when operational and in the event of equipment failure.

8) The RTD system and dexterous manipulator arm shall be capable of supporting the reactant forces of 100 lbs minimum caused from tool use (such as: spray wand and brush/scraper) through its full range of travel.

9) Minimize stresses applied to the tank and prevent damage to the tank structure during normal operation or in the event of equipment failure.

10) Operate within the tank environment as follows: Air at ambient temperature between 45 and 95 degrees Fahrenheit, Relative Humidity up to 100%, vapors from the tank waste may be caustic or acidic; tank waste liquids will primarily be at pH 9 to 12 but may range from pH 4 to 6 during the final stages of tank cleanup.

11) Maximize the RTD system's efficiency (tank area coverage) at each riser deployment and minimize the number of riser transfers.

12) The RTD system shall be designed to maximize reliability of all components, to remain operational for a minimum of 2 years without requiring routine maintenance when installed into the tank environment and remain operational after exposure to the radiation field to a minimum of 10,000,000 R total integrated dose. Simplicity of the design shall be paramount. The actual in-tank operating time for the equipment is 4500 hrs minimum (based on 6 hrs/day, 365 days/yr for 2 years).

13) The cables/hoses shall be designed with a management system to prevent entanglement, to permit cable/hose replacement, to permit cable/hose disconnection between radiologically hot and cold areas and to permit effective decontamination.

14) The RTD system may be electrically or hydraulically powered. If hydraulically powered, the hydraulic system shall use Shell Tellus 32 Petroleum based fluid.

15) The operator controls shall be user friendly and use standard replaceable components. The operator control station shall visually display in-tank operation of the end effectors.

16) The RTD system may be attached to a mast, or be a floor-based mobile unit, or be a mobile unit maneuvering above the floor using tank internal structural members or be some other approved system.

17) The RTD system shall support the removal of residual waste samples for analysis.

18) The RTD system shall be capable of deploying sensors (such as a gamma probe) for use in estimating the amount of waste remaining in the tank.

19) The preferred material for in-tank equipment are stainless steel and titanium. Carbon steel and aluminum materials with protective coatings to prevent corrosion and aid in decontamination may also be used.

20) All provisions for lifting shall be designed such that the combined shear stress or maximum tensile stress on any load bearing part shall **NOT** exceed 1/3 of the tensile yield strength of the material and also **NOT** exceed 1/5 of the ultimate tensile strength of the material.

21) For contamination control, the RTD system shall provide a containment system which seals to the WVNS containment building as required and be capable of withstanding negative pressure (vacuum) of 3 inches of water column.

3.0 **Requirements** **Rationale**

3.1 Hazard Classification or hazard category 2 (WV-365)

3.2 Reference: WVDP-227 Rev. 4, Table 1 WVDP Facility Identification and Classification Matrix.

3.3 Quality Level C (QM-2) "Q-List" WVDP-204, Rev. 4
HLW tank riser equipment (internal to tank)

3.4 Safety Class C (QM-3) "Q-List" WVDP-204, Rev. 4
HLW tank riser equipment (internal to tank)

3.5 Codes/Standards Control Systems-ISA Standards; Electrical-NEC; Structural Members-AISC Steel Manual (seismic qualification not required); Pump API-610 (or manufacturer's standard); Piping-ANSI B31.3
Reference - Table 3 of "Q-List" WVDP-204, Rev. 4

3.6 Fire Protection Design N/A (WVDP-177)

3.7 DOE Orders N/A

3.8 Reference or interface drawings 900D-557, 558, 1125, 1170, 1473, 1513, 1515, 6746, 7225; 904D-101, 108, 109, 110, 111, 116, 117, 118 & 119; Rotek bearing per Floway dwg D87-01080-1

3.9 Boundaries stated in applicable SARs, EAs or Permits: WVNS-SAR-002

4.0 Q-List (WVDP-204) reviewed and updated as necessary X Yes ____ No

Author [signature] Date 2/10/98

Cognizant System Design Manager [signature] Date 2/10/98

INTERNAL DISTRIBUTION

1-4. J. B. Chesser
5. D. C. Haley
6. R. L. Kress
7. S. L. Schrock
8-9 Laboratory Records
10. Laboratory Records – RC

EXTERNAL DISTRIBUTION

11. George F. Bernatz, West Valley Nuclear Services Co., Inc., Mail Stop 54B, P.O. Box 191, 10282 Rock Springs Road, West Valley, New York 14171-0191.
12. Pat A. Berton, West Valley Nuclear Services Co., Inc., Mail Stop 54B, P.O. Box 191, 10282 Rock Springs Road, West Valley, New York 14171-0191.
13. Barry L. Burks, The Providence Group, 11020 Solway School Road, Knoxville, Tennessee 37931.
14-24. Bill Hasselbacher
25. K. Louis Huber, West Valley Nuclear Services Co., Inc., P.O. Box 191, West Valley, New York 14171-0191.
26. Bruce Thompson, RedZone Robotics, Inc., 2425 Liberty Avenue, Pittsburgh, Pensylvania 15222-4639.