USING FAULT TREES TO DETERMINE THE ROOT CAUSE OF ROTATING EQUIPMENT FAILURES

by

Robert X. Perez

Senior Reliability Engineer

Citgo Petroleum Corporation

Corpus Christi, Texas

Robert X. Perez is a Senior Reliability Engineer for the Citgo Corpus Christi Refinery. He has previously written and has been a coauthor on several papers in the field of machinery vibration. His primary duties include troubleshooting rotating equipment problems, leading root-cause failure analysis teams, and serving as the plant consultant in the areas of vibration analysis and rotordynamics. He was instrumental in the implementation of a computer based vibration monitoring program and on stream piping inspection program for his refinery, and was the first in his plant to promote the use of Weilbull Analysis techniques to analyze mechanical failure data.

Mr. Perez is a registered Professional Engineer in the State of Texas and a member of ASME and the Vibration Institute. He received his B.S.M.E. degree from Texas A&M University, and a M.S.M.E. from the University of Texas.

ABSTRACT

The great value of using multidisciplinary task groups to conduct root cause failure analyses (RCFA) on pump and rotating equipment failures is discussed. The RCFA method offers its users a structured means of achieving continuous plant reliability improvements by targeting mechanical and organizational deficiencies in a process facility. One tool the author has found to be vital in the determination of the root cause (or causes) of rotating equipment failures is the fault tree method. This method provides a simple, graphical means of assessing the evidence collected by the RCFA team and elucidating the most probable failure scenario(s). Included are several real examples of fault trees from the petrochemical industry, involving pumps and other rotating equipment outages.

INTRODUCTION

It is not uncommon to see process facilities caught in the vicious cycle of failure, repair, blame, failure, repair, blame,...etc. Without the proper resources and commitment by management, this cycle will perpetuate itself, creating a divisive atmosphere among plant departments, and robbing an organization of profit. One means of breaking this counterproductive and costly cycle is by establishing a concerted plantwide reliability effort. One of the most powerful tools a reliability program can use is the root cause failure analysis (RCFA) team. If organized with multidisciplinary members and empowered by management, these teams can transform a maintenance organization into a more efficient and proactive entity.

The RCFA method goes beyond simply analyzing component failures; it attempts to ferret out the root failures and all significant contributing organizational factors. One powerful tool frequently used to determine the root cause of rotating equipment failures is the fault tree method. This method allows the analysis team to depict the system involved in terms of logical "and" and "or" gates. Once the fault tree is constructed, it can be analyzed and pruned by the investigation team. After all the unsubstantiated potential scenarios are crossed out on the fault tree, the root, or root causes, will come to light.

Trevo Kletz, in "Learning Accidents in Industry," said

> "..root cause investigation is like peeling an onion. The outer layers deal with technical causes, while the inner layers are concerned with weaknesses in the management system..I am not suggesting that technical causes are less important. But putting technical causes right will prevent only the LAST event from happening again; attending to the underlying causes may prevent MANY SIMILAR INCIDENCES."

WHAT IS AN RCFA AND WHY BOTHER WITH THEM?

In the study of major failures, it's typically seen that significant undesired events are the result of a series of events, similar to the chain reaction of dominos that are lined up one behind the other. They are in a metastable state until one domino is tipped over. The entire chain of dominos will fall in succession, unless the chain of events is broken. Studying chain of events, or probable scenarios is at the heart of RCFAs.

Consider this example: During the repair of a large reciprocating compressor, the maintenance supervisor discovers a damaged compressor rod requiring replacement. So, he decides to have a rod made in a local shop. Without consulting the original equipment manufacturer (OEM), the machine shop decides to fabricate the rod with cut threads. The OEM's experience with this compressor has led him to convert all compressor rods for compressors of this frame size to rolled threads. As a result of the improper fabrication, the rod fails due to fatigue in the thread area and causes extensive secondary damage inside the compressor. The repair, estimated to cost well over $100,000, is expected to take more than three weeks to complete.

If you study this example, you can discern the following events leading to the costly failure:

- The warehouse did not stock spares for this rod because it was a new compressor installation.
- The maintenance supervisor decides to have a rod fabricated without drawings.
- Neither the user nor the local shop investigated the thread requirements.
- Because the compressor was not equipped with vibration shutdowns, it ran for a significant amount of time before it was shut down.

There were several chances to break the chain of events leading to the catastrophic compressor failure. If the project engineer had ordered spare parts through the OEM, this failure probably would have been avoided. If either the maintenance supervisor or the

local machine shop had talked to the OEM, or studied the failed rod, they would have been aware of the importance of rolled threads. Lastly, if a vibration shutdown had been in place, the compressor would have shutdown after only minimal damage. Using the domino analogy to analyze the failure (Figure 1), we see there were six major events leading to the secondary compressor damage. These events were:

- No procedure in place to order spare parts for newly purchased equipment (latent root).
- The improper installation of the packing leads to rod scoring.
- Because a spare rod is not available and plant management wants the compressor back in operation as soon as possible, it was decided to have a replacement rod fabricated at a local machine shop.
- No one checks with the OEM about rod thread specifications (physical root).
- The rod fails after two days of operation.
- The broken rod causes extensive damage to the cylinder, packing box, distance piece, and cross-head.

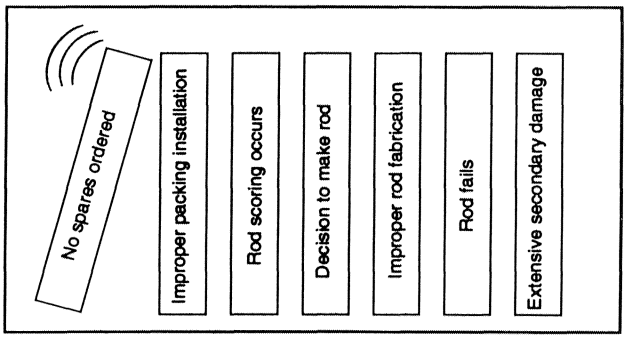

Figure 1. Events Leading to Compressor Failure.

After examining the vestiges of the failure, the rotating equipment (RE) engineer would discover a fatigue failure in the threaded portion of the rod. From this, he would conclude an improper thread design led to a stress riser and a shortened fatigue life. After talking to the OEM, he writes a report recommending that all compressor rods in the plant have rolled threads.

This recommendation will surely reduce rod failures; but the investigation did not uncover the latent root of failure. The stress riser, due to the improper thread design, is called the "physical root," because it did initiate the physical events leading to the secondary damage. However, there were significant events preceding the physical root that are of interest. If the RE engineer had had the time and resources, he would have discovered that the absence of a procedure requiring new equipment to be purchased with adequate spares directly initiated the sequence of events. This basic event is called the "latent root."

By requiring spare parts be purchased from the OEM for all new equipment, the latent root is eliminated, not only for this scenario but, potentially, for many other similar events. This example demonstrates the importance of ferreting out the "latent root" of rotating equipment failures. Stopping at the "physical root," deprives the organization of a valuable opportunity for improvement.

So, an RCFA is a detailed analysis of a complex, multievent failure, such as the example above, in which the sequence of events is hoped to be found, along with the initiating event. The initiating event is called the root cause, and factors that contributed to the severity of the failure or perpetuated the events leading to the failure are called contributing events.

The goal of the RCFA team or engineer is to uncover the latent root(s) of the failure and not to pin the blame on individuals involved in the sequence of events leading to the failure. If supported by management, implementation of the investigation team's recommendations can lead to lasting and widespread improvements in the organization.

WHEN IS AN RCFA JUSTIFIED?

A risk map can be used to explain the cost of failures (Figure 2). The cost of an individual event is on the abscissa, and on the ordinate, the annual frequency of the event. Rare events, also called sporadic events, such as the failure of a high speed compressor rotor, may occur only once every hundred years, while a more common failure, such as a mechanical seal failure, may occur several times a year. If, for example, the compressor rotor failure cost the plant $2,000,000 and was believed to have a frequency of 1/20 yr, it would be shown by point #1 on the risk map. This would represent an economic risk to the plant of $2,000,000 × 1/20 yr = $100,000/yr. If a pump seal, which costs $5,000 per event, had a frequency of 20/yr, it would be shown by point #2 on the risk map. This would represent an economic risk to the plant of $5,000 × 20/yr = $100,000/yr. Even though the seal failures are relatively inexpensive, the high frequency of occurrence exposes the plant to the same economic risk represented by a compressor rotor in the above example.

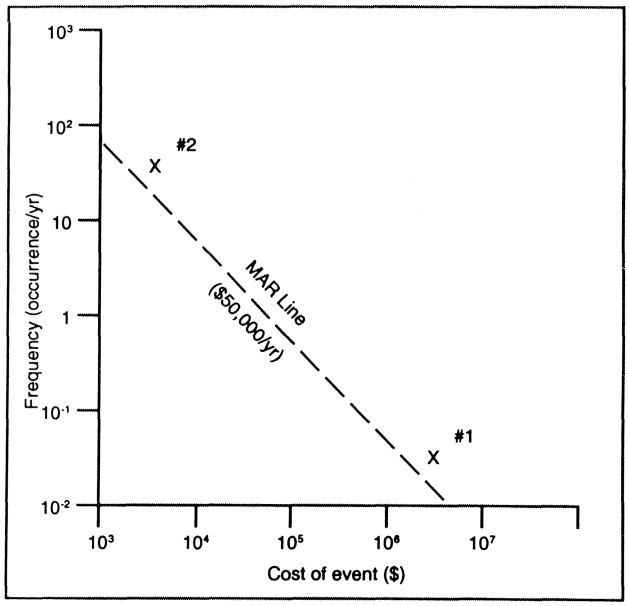

Figure 2. Example of Risk Map.

Plant management has to determine the maximum acceptable economic risk level for plant equipment. This maximum acceptable risk (MAR) can be shown as a line on the risk map (Figure 2). If repetitive events fall above the MAR line, an RCFA should be initiated.

Another means of determining when an RCFA should be conducted is by adopting a set of criteria for determining when an event is significant. The author's organization has decided to conduct an RCFA whenever:

- an employee or contractor is injured due to equipment failure.
- an equipment failure causes a fire or major release of product.
- an equipment failure leads to a greater than 24 hour unit outage.

- an equipment failure leads to a costly repair. (In the author's facility a major failure is one that cost over $100,000).
- "near misses," which are sequence-of-events that stop one step short of becoming major catastrophic events, are also investigated.

Established criteria, such as those above, and the risk map method, should both be used to determine when RCFAs are required.

WHY USE AN INTERDISCIPLINARY TASK GROUP?

The rotating equipment (RE) engineers are typically given ample resources to correct problems with mechanical roots, such as misalignment and imbalance problems; however, they are rarely afforded the time or resources to solve elusive mechanical problems with root causes that are nonmechanical in nature. Example of nonmechanical roots would be:

- upstream corrosion causing mechanical seal failures.
- poor piping design leading to flow instabilities in the pump suction and shaft fatigue failures.
- off-design performance due to improper flow control causing severe internal recirculation.
- thrust failures due to cavitation caused by erratic tower operations.

If the RE engineer is unsuccessful in identifying and correcting recurring nonmechanical root causes, he will be spurred to attack the mechanical causes of failure and strive to make components more forgiving. Examples of this are:

- Upgrading shaft metallurgy or design to improve fatigue life.
- Selecting a seal design that is capable of handling particulates.
- Improving the erosion resistance of the pump case to extend the life of a pump experiencing severe internal recirculation due to off-design operation.
- Upgrading the rating of a thrust bearing experiencing premature failures due to cavitation.

These types of equipment improvements do not correct the underlying cause of failure and may not preclude the occurrence of a repetitive failure mode.

By assigning an interdisciplinary investigation team consisting of mechanical, process, purchasing, safety, and operations personnel, to investigate elusive and costly failures, an organization can dramatically improve its chances of uncovering a latent root cause of failure, and factors contributing to the failure. Collectively, the RCFA group will take ownership of the investigation and provide the resources needed to secure evidence in the form of physical evidence, interviews, and tests required to arrive at believable and tenable conclusions.

OTHER BENEFITS OF RCFA

The salient value of RCFAs have been discussed; but we also wish to mention their hidden value. The author has found the use of inter-disciplinary teams, and the widespread use of RCFA methods has had a profound and beneficial effect on their organization. These being:

- improved communication between departments.
- more trust between departments.
- improved understanding of how departments really work.
- improved understanding of procedures.
- reduction in the fear of making mistakes.

HOW TO CONDUCT A ROOT CAUSE FAILURE ANALYSIS.

It is the author's opinion, that to successfully initiate, complete, and implement the resulting recommendations of an RCFA investigation, the investigation team must have the support of management. Without the organization's commitment of resources to the goal of long term improvement, RCFA investigations will follow the route of undisciplined investigations, and will lack the support of all personnel that is required to make meaningful changes in the way we do our work.

To conduct an RCFA investigation, the author follows the six basic steps below:

- Organize an investigative team.
- Schedule meetings and assign tasks.
- Cull information/develop a fault tree.
- Advise management of initial findings.
- Issue a report and conduct a review meeting.
- Assign responsibility and track the completion of report recommendations.

Organize an Investigative Team

In the author's company, an RCFA is initiated by the Area Operations Manager where the unit outage or major equipment failure occurred by issuing a memo requesting an indepth analysis. The concept of an interdisciplinary team is utilized, selecting personnel from the following departments to participate:

- Operations(hourly and/or salaried)
- Maintenance(hourly and/or salaried)
- Process Engineering
- Maintenance Engineering
- Project Engineering
- Reliability Engineering

A reliability engineer is normally assigned the task of team leader. It is the responsibility of the team leader to schedule meetings, assign tasks, conduct meetings, draft reports, and assign responsibility for recommendations.

In the author's experience, the optimum investigative team size is five to seven. Groups smaller than four to five tend to lack the necessary blend of knowledge. In groups larger than seven, it is difficult to maintain the groups' focus and schedule meetings.

Schedule Meetings and Assign Tasks

Once an investigative team has been formed, the first task of the team leader is to contact team members and schedule an initial meeting as soon as possible. The scheduling of the initial meeting is crucial to the success of the investigation. Details of the failure, physical evidence, and process control system data can be lost or irretrievable within 72 hours.

During the first meeting, a description of the failure is presented to inform all personnel. With the experience of having conducted several investigations, the author has developed a standard RCFA procedures check list (Table 1), which describes,in abridged form, how to organize an investigative team, capture and preserve data, data analysis methods, and steps for closure of the investigation. During the initial meeting, responsibilities are assigned to team members for the following:

- Interview operating personnel.
- Collect samples for analysis.

- Obtain data from the process control system.
- Obtain copies of P&IDs, specification sheets etc..

Allow sufficient time for team members to accomplish their tasks and schedule the next meeting accordingly.

Table 1. Root Cause Failure Investigation Procedures.

Oraganize A Review Team
-utilize interdisciplinary skills concept
-select unbiased personnel
-utilize all levels of employees
-assign individual's responsibilities in the review process
-update management on a regular basis
-maintain the group's focus on the root cause
Preserve The Data (People, Position, Parts, Paper Data)
-interview and write down the names of the people present
-obtain a copy of the alarm summary
-obtain a printout of process data with the fastest sampling rate available
-mark position/photograph and collect any broken parts or samples for analysis
-photograph the area
-if applicable, pull strip chart recorder paper
-obtain copies of the work permits and the work orders
-list any non-routine events that occurred in the previous 48 hours
-utilize the data freezer form [3]
-operator to sketch a schematic and a short statement of what occurred
Analyze Data
-continue to gather information
-utilize the fault tree approach
-confirm or cull facts with the use of statistics
-formulate hypotheses and substantiate on the basis of proven facts
Conclude The Investigation
-issue the report
-conduct a review meeting
-assign responsibility for each recommendation
-track the results
-conduct follow up meetings

Cull Information and Develop a Fault Tree

During the succeeding meetings, the objective of the team is to review all the information. Inevitably, during the investigation, personal opinions are formed as to the cause of the failure. On occasion, these assumptions can disrupt the focus of the team.

This is where the value of fault tree analysis is appreciated. Construction of a fault tree will aid in focusing the group's attention on the facts relevant to the failure, culling unnecessary data, and eliminating personal assumptions as to the cause of the failure. In addition, fault tree models will assist the investigative team in conducting the investigation past the point of human intervention, so that flaws in procedures and management systems can be identified. Fault tree models will also provide the investigative team with a logical graphical representation of the system failure sequence, supporting their conclusions and recommendations.

Advise Management of Initial Findings

Some proponents of RCFA investigations stress that the team should work independently of any outside influence, and that findings should be kept confidential until the final report is issued. The author has found that it is preferable to advise management frequently as to the progress of the investigation. Open feedback on the progress of the investigation maintains management's support. Open feedback with plant personnel will educate employees as to the value of RCFA investigations and help eliminate the fear that this tool will be utilized for discipline. Removal of fear will increase the interest in participation in RCFA investigations by other employees.

Issue a Report and Conduct a Review Meeting

Once the team is satisfied that the latent roots or causes of the failure have been addressed and adequately supported by the use of fault tree analysis it is the responsibility of the team leader to draft a report.

Depending on the severity of the failure, a review meeting may be desirable. The review will serve several purposes:

- Present the team findings to management.
- Present the team's recommendations.
- Provide an opportunity to answer questions.

Assign Responsibility and Track Recommendations:

Once the recommendations have been accepted by management and prioritized, the responsible team member should provide the necessary support/documentation to assure that tasks are completed by maintenance, project engineering, or operations.

The authors' experience has proven that, without assignment of responsibility for the completion of recommendations, reports are issued and recommendations are agreed upon, but little meaningful progress is accomplished.

PERFORMING A FAULT TREE ANALYSIS

Fault Tree Definitions

A fault tree is a graphical representation of the top event, known as final events, and all possible events believed to have caused the top event. The fault tree should include all machine failures as well as human faults that may have led to the top event. By using logical gates, such as "and" and "or" gates, the RCFA team can pictorially depict all possible scenarios on one schematic. This greatly simplifies the analysis and review processes. Typical symbols used in fault trees are listed in Table 2.

The fault events and basic events in the fault tree can be divided into failures and faults. A component failure is a malfunction that requires the component to be repaired or replaced before it can successfully function again. As in the compressor example above, where the compressor rod broke and required replacement. A fault is a malfunction that is reversible. For example, if an operator allows a tower level to drop too low, it can cause a pump to cavitate severely. But this situation is reversible; if the tower level returns to the correct level, the pump will stop cavitating. This situation did not require any parts replacement to return the system to normal operation.

Constructing a Fault Tree

As previously discussed, fault trees are reliability and safety engineering tools that assist in focusing the teams' efforts, ferreting out the root or latent causes of failures, and eliminating false assumptions. Fault trees can be utilized as explanatory or exploratory tools. Explanatory fault trees serve as a visual explanation of the obvious, and the not so obvious, possibilities that were investigated. Exploratory fault trees help the investigative team discover any possibilities that they may have overlooked. As a exploratory/explanatory tool, fault trees map the investigative course the team has chosen to research.

Table 2. Logic and Event Symbols Used in Fault Trees.

OR Gate	OR Gate	The output event occurs if any of the input events occur
AND Gate	AND Gate	The output event occurs only when all the input events exist simultaneously
INHIBIT Gate / Condition	INHIBIT Gate	The output event occurs when the input event occurs and the inhibit condition is satisfied
Output Event / Delay Time / Input Event	DELAY Gate	The output event occurs when the input event has occurred and the specified delay time has expired
Intermediate Event	INTERMEDIATE Event	A fault event that results from the interactions of other fault events that are developed through logic gates such as those defined above
Basic Event	BASIC Event	A component failure that requires no further development. A basic event is the lowest level of resolution in a fault tree

Construction of a fault tree is quite simple. In a team meeting, on a chalk board or presentation note pad, the group must first define the top event, which is the failure of interest. After definition of the top event, the next step is to develop all sequences of events capable of leading to the system failure or top event. This step requires evaluating all possible combinations of events or single events in series or parallel configurations capable of causing the top event (Ask why or how this could happen?). To develop a complete fault tree, the team must:

- Start with the top event and ask: What events (intermediate or basic events) could have caused the top event to occur? If, for example (Figure 3) either one of two events named, I and II, needed to occur, an "OR" is used above the two events I and II. If both were required to occur, an "AND" is used.

- Then, the team must analyze each upstream event related to events I and II. The team must ask: What events (intermediate or basic events) could have caused the downstream events I and II to occur. If either one of two events were required for event I to occur, an "OR" gate is used above the upstream events III and IV, and if both events were required to occur, an "AND" gate is used.

- This procedure is followed until all upstream events are basic events or faults and the team is satisfied it has captured all potential scenarios related to the top event.

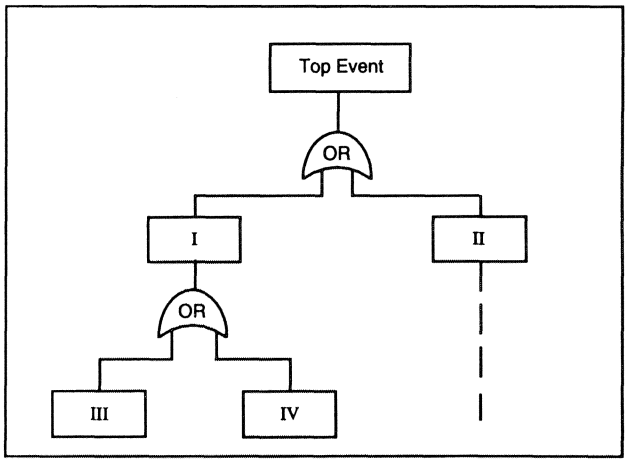

Figure 3. Constructing a Fault Tree.

Pruning the Fault Tree

Once completed, pruning of the fault tree is started. The author's method of pruning the fault tree is to list all the possible methods of verifying the root cause or initiating event. Data supporting an initial event can be visual inspection, testing of systems, component analysis, process data, or theoretical verification. Any initial event on the fault tree must be verifiable by the aforementioned methods. Any initial event that cannot be substantiated by this method is removed (i.e., pruned) from consideration as a root cause of the top event.

Once pruning of the fault tree is complete, the investigative team can review the remaining root or roots and compare these with their initial assumptions. Recommendations can be compared to the fault tree to determine if the true roots of the failure are being addressed.

SAMPLE FAULT TREE

As an example, lets develop a fault tree for the following electrical circuit (Figure 4). The top event of interest will be MOTOR FAILS TO START (Figure 5). Asking why the motor fails to start in our example yields two independent possibilities: motor failure or no power to motor. Being independent, their failure modes indicate that these two events are connected to the top event through an OR gate.

Reviewing the schematic indicates four independent possibilities for lack of power to the motor: switch open, fuse failure, wire failure, or power supply failure. Each of these failure modes is

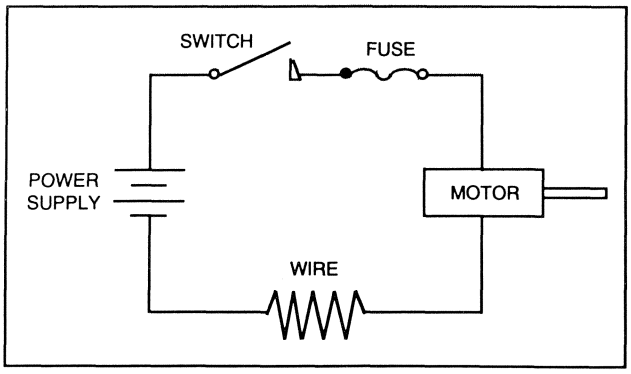

Figure 4. Fault Tree Example.

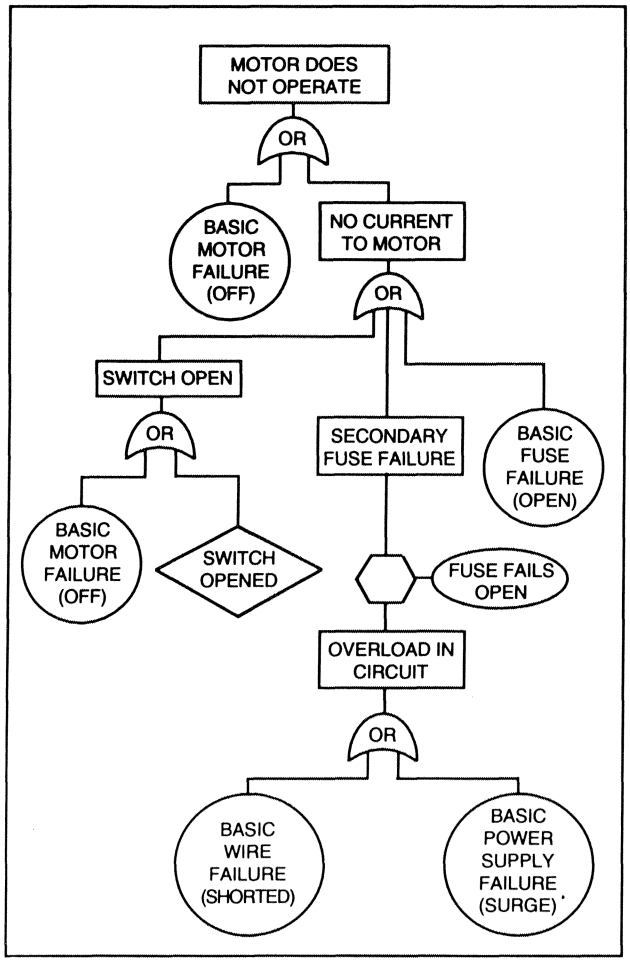

Figure 5. Fault Tree for Motor Failure.

independent of the other and therefore would be connected to the intermediate event of (no power to motor) via an OR gate.

Pursuing the switch open intermediate event yields two potential root causes: Switch failure and switch in the open position. Continuing on the fuse failure intermediate event leads to two other potential causes: Basic fuse failure or overload in the circuit. Having developed the fault tree to the level of root causes, methods of verification can now be developed, i.e.:

- Motor Failure - test motor on an independent circuit.
- Switch Open - visual inspection and test switch.
- Wire Failure - perform continuity checks.
- Fuse Failure - visual inspection or continuity check.
- Power Supply Failure - test power supply.
- Overload in Circuit - test for shorted wire.

Having developed the fault tree and determined the cause for the motor not starting, the investigative team can decide how far to extend the fault tree into potential latent roots.

In this example, through physical verification fuse failure, power supply failure and wire failure were pruned from the fault tree as potential basic events. The switch failure was determined to be the cause of the motor not starting.

Having pruned the fault tree of basic events through the use of verification, the investigative team can decide how far to extend the fault tree into potential latent roots. Potential latent roots of the switch failure could be:

- Poor switch quality.
- Low switch rating.
- Improper installation (procedures).
- Poor specifications (wrong switch selected).

EXAMPLE 1: SLURRY PUMP FIRE

Top Event: A 300 hp, turbine-driven, hot oil pump experienced a seal failure that led to a significant release of 700+°F oil. The subsequent fire, which engulfed the pump and associated piping, caused no injuries and was quickly extinguished. Because the event met the refinery's definition for a significant event, a multidisciplinary task group, composed of an operations engineer, reliability engineer, operations manager, area operations supervisor, and the safety manager was assigned to investigate it.

After gathering data associated with the event, a fault tree was constructed (Figure 6). Initially, some members of the team believed the pump failure was the result of a poor pump design. However, pruning the fault tree led the team to the conclusion that the product release was a consequence of a thrust bearing failure, caused by the following:

- historical flow-related vibration problems and
- a plugged suction strainer, caused by coke formation in the tower bottoms. Note: The excessive coke formation was found to be the result of an improper tower operating procedure. (This was the latent root cause of the top event.)

As a result of the teams findings, the process unit changed their tower operating procedure. Since that time, there has not been a single thrust bearing failure. (It is interesting to note operations personnel on the team were convinced the latent root of the failure was the improper operating procedure for the tower, even though they originally believed the cause of the failure was the pump design.)

The RCFA team's recommendations also urged the area reliability engineer to work on ways to improve pump hydraulics and suction strainer performance so that bearing life could be extended.

EXAMPLE 2: FLUIDIC CATALYST CRACKING UNIT (FCCU) STEAM TURBINE FAILURE:

Now, look at an example where a fault tree analysis was used on an actual unscheduled unit outage. In an FCC unit, the catalyst regeneration air blower is driven by a motor and a hot flue gas

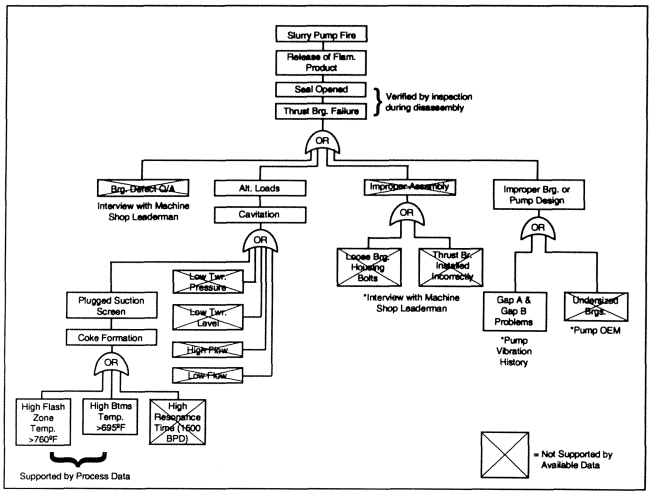

Figure 6. Fault Tree for Slurry Pump Fire Investigation.

expander. At the end of the power recovery train is a steam turbine, used for startup purposes only.

During normal operation, the power recovery train appeared to have been inadvertently shutdown by construction personnel installing new conduits in the local power recovery train logic panel. Operations attempted to restart the power recovery train with the startup steam turbine. During startup of the steam turbine, high thrust vibration was observed and seal oil in large quantities began leaking from the inboard bearing housing. The unit was shut down for repair of the steam turbine.

An RCFA was requested by the area operations manager. A team was formed and the initial meeting was held. In the initial meeting it was decided that two questions required further investigation:

- What caused the initial shutdown of the power recovery train?
- What was the cause of the start-up steam turbine failure?

Assumptions were quickly formed in the plant. These were:

- Train shutdown was caused by personnel working in the logic panel.
- Turbine failure was due to loss of lube oil and steam deposits

Assignments were made in the initial meeting and team members conducted interviews, captured process control data, collected turbine components for inspection, gathered equipment drawings and sent samples of deposits found in the steam turbine for analysis.

In the following meetings, the data was reviewed and two fault trees were constructed. The first fault tree (Figure 7) was used to determine the initial cause of the power recovery train shutdown. Armed with process control data, vibration data, and interviews with personnel in the area, the team concluded that the train shutdown was caused by construction personnel working in the logic panel, creating a short circuit which initiated a safety system shutdown.

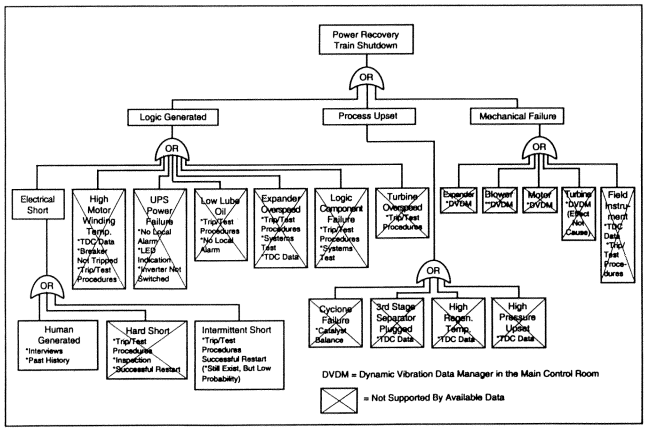

Figure 7. Fault Tree for Power Recovery Train Trip.

The investigative team did not stop at the point of human intervention and place blame. Further review indicated that it was common practice to perform as much capital project or preparatory work for a turnaround as possible before the unit was shutdown. The review team concluded that this was the latent root cause of the top event in the fault tree. A list was developed of critical equipment with safety shutdown systems and the recommendation was made to limit preturnaround work in these areas.

The second fault tree (Figure 8) was used to address the cause of the turbine thrust shoe failure. It was initially assumed loss of lube oil or steam deposits resulted in the bearing failure. However, after

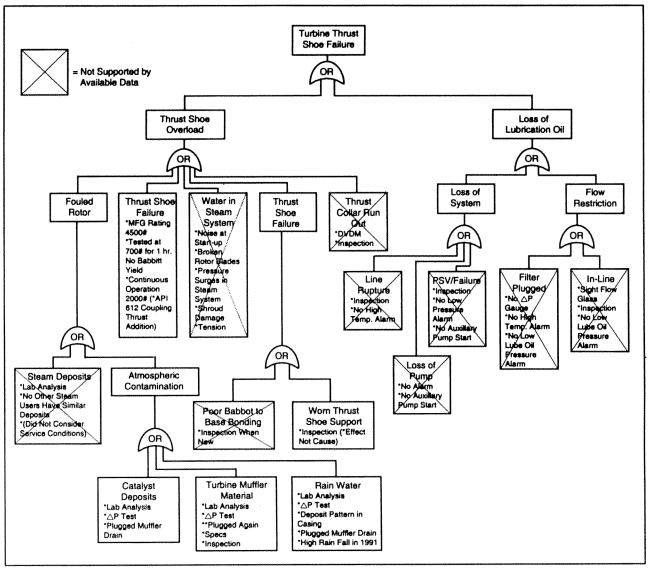

Figure 8. Fault Tree for Steam Turbine Thrust Bearing Failure.

reviewing the available process data, alarm histories, and the testing of instrumentation associated with the lube oil system, these assumptions were quickly eliminated.

Review of the composition analysis of the material deposited in the steam turbine did not match the composition of solids in the steam system. Furthermore, inspection of the equipment in the field yielded the following information:

- Instrumentation for windmilling steam was not in service.
- The low point drain in the turbine exhaust muffler was plugged
- Deposits, similar to those found in the steam turbine buckets, were also encountered in low points in the turbine exhaust.

After pruning of the fault tree, the conclusion of the team was that the origin of the deposits was atmospheric and catalyst dust. After the unit was repaired, inservice tests were performed to verify that without windmilling steam the steam turbine acts as a compressor and pulls in contaminants through the exhaust silencer. The recommendations of the review team were to recommission the windmilling steam system, add windmilling steam instrumentation testing to the standard maintenance practices for turnarounds, unplug the turbine exhaust silencer drains, and inspect the exhaust silencer during the next scheduled outage. The latent root cause in this situation was the lack of education. Training sessions were conducted with operations and instrumentation technicians to describe the windmilling steam system, its function, and the proper procedures for decommissioning control systems interconnected with interlocks and safety shutdown systems.

EXAMPLE 3: HEATER FAILURE DUE TO COKING

Here is an interesting RCFA which highlights the fact that, sometimes, incidences involving rotating equipment failures can actually be initiated by nonrotating equipment malfunctions. In this incident, an extended outage occurred in a process unit because of a "coked-up" heater pass. The fault tree analysis was vital in the identification of a pair of root causes that were both unrelated to the pumps involved in the incident.

Prior to the coking occurrence, one of the pumps which supplies the heater with charge was repaired and was prepared for service. Before the repaired pump was started, flow was lost to the heater,

even though the spare was still on line. The loss of process flow resulted in a heater shutdown and the addition of emergency steam into all the heater passes. Soon after reigniting the heater burners, with the emergency steam on, operations noticed that the #3 pass (Note: There are four heater passes in all) exhibited a loss of oil flow, prompting a unit shutdown.

A fault tree (Figure 9) was useful in determining the most likely causes of the unit outage. After pruning the fault tree, it was determined that two events had to have occurred to cause coking in pass #3. These were:

- loss of flow from the heater charge pumps.
- loss of emergency steam flow to one of the heater passes.

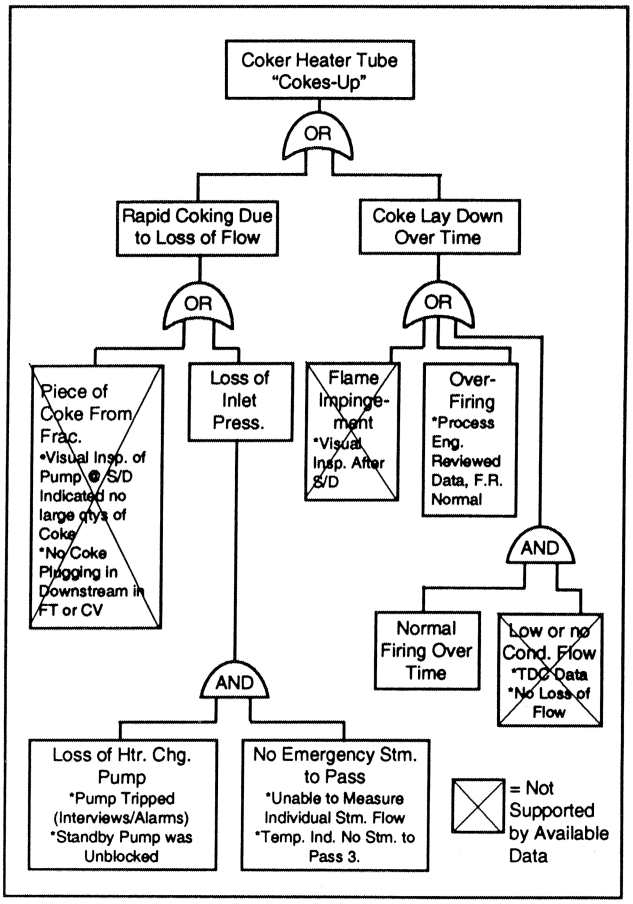

Figure 9. Fault Tree for Heater Failure.

Interviews confirmed that flow was lost when the spare heater charge pump was installed and its isolation valves were opened. Based on the fault tree analysis, the investigation team concluded the check valve on the spare pump was leaking, allowing unit charge to flow back through the spare pump's suction and back to the suction vessel. Once the spare pump was blocked in, the recirculation flow ceased and flow to the heater was re-established. (Note: The maintenance department discovered later that the check valve in the spare pump's discharge line was inoperative due to an eroded flapper stud bolt.)

However, the team was not able to confirm why the emergency steam, which was admitted to all four passes, did not prevent coking in the #3 pass. It was decided that the steam line to the #3 pass was probably partially plugged due to spalled coke that had previously accumulated in the process piping.

The team's findings spurred them to recommend the following in hopes of precluding the recurrence of a similar unit outage in the future:

- Flow transmitters be installed in each heater pass to allow operating personnel to monitor individual emergency stream flows.
- The current operating procedures be reviewed to determine if a longer delay is required before re-establishing oil or steam flow to the heater prior to reigniting the heater burners, after a heater trip.
- Alarm setpoints for heater inlet pressure, outlet temperature, and heater tube-skin thermocouples be established.

This case study illustrates a classic example of a failure due to a series of events. These were:

- Spare pump fails and requires repair.
- During reinstallation, the spare pump's suction and discharge valves are opened.
- Spare pump's discharge check valve leaks.
- Reverse flow through spare pump robs the heater of flow.
- Low heater flow causes heater shutdown.
- The heater burners were reignited.
- Emergency steam flow injected into heater passes to preclude coking.
- Inadequate steam to #3 pass leads to coking
- Operations failed to recognize indications that the #3 pass is "coking up"

While it is easy to see the pattern developing once the data is assimilated, during a crisis situation, waving "red flags" are not always seen by personnel on the scene. This is why it is imperative that the lessons learned by RCFA be used to place lasting safe-guards in place; so that regardless of who is present when these initial events occur again, the chain of events will be broken before a unit outage occurs.

EXAMPLE 4: CONTAMINATION OF THE PLANT AMINE SYSTEM

During the startup of a portion of our hydrotreating unit, the introduction of a gas stream laden with H2S gas resulted in the contamination of the plant liquid petroleum gas (LPG) system. Under suspicion initially, was a Lean DEA pump (P-1), which failed during the hydrotreater startup. This pump and its spare have had a history of pump shaft failures and, for this reason, were considered unreliable.

However, a fault tree analysis elucidated the fact that the Lean DEA pump (P-1) failure was not the initiating event leading to the contamination of the plant amine system. Two distinct means of contaminating the LPG system (Figure 10) were uncovered, both of which would have resulted in the loss of flow or turbulent two phase flow in the Lean DEA pump (P-1) and an eventual shaft failure due to fatigue. So, the team was able to demonstrate the P-1 shaft failure was secondary in nature, unrelated to the primary sequence of events leading to the contamination of the plant's LPG system.

The two LPG contamination scenarios derived from the team's fault tree were:

- A lack of water level in a recycle gas scrubber could have allowed gas to back into the rich DEA system. The path denoted by light shading in Figure 11 illustrates how contaminated gas could have flowed from the hydrotreater unit, through the P-1 pump, causing a two phase flow condition, and into the LPG system.

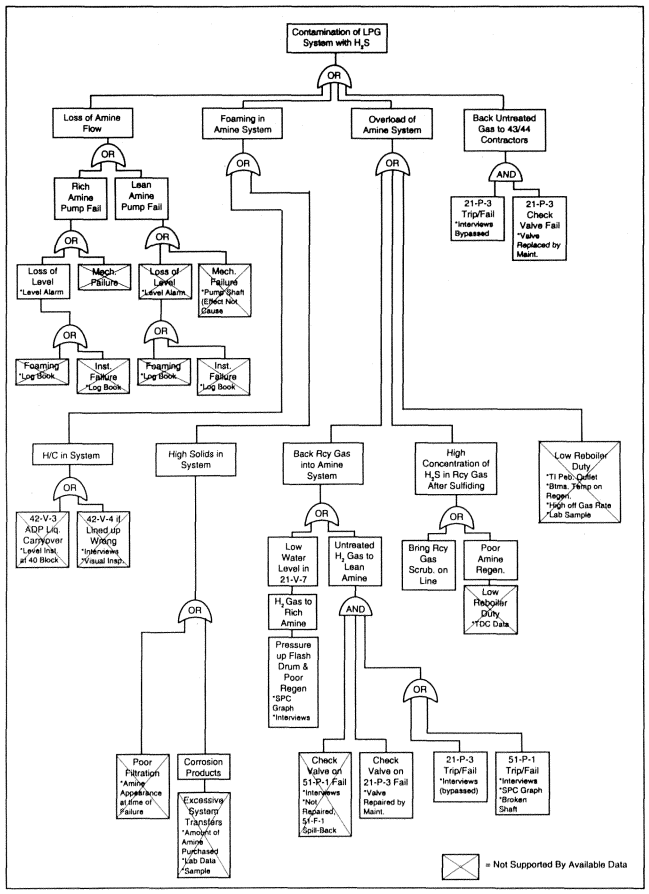

Figure 10. Fault Tree for Amine System Contamination Study.

• A discharge check valve failure, and a trip of the Lean DEA booster pump (P-3) could also have allowed gas back into the DEA system. (Note: These are different pumps than the ones mentioned above) This allowed H2S laden gas to back into the lean DEA system. The path denoted by dark shading in Figure 11 illustrates how contaminated gas could have flowed from the hydrotreater unit, causing a no flow condition, into the LPG. This action would have backed flow through the F-1 filter and back into the DEA system, causing a no flow condition at the P-1 pump.

As noted, both of these sequence of events could have resulted in the loss of flow or two phase flow in the P-1 pump. The resulting impeller excitation was believed to have contributed to the pump shaft failure observed following the LPG system contamination.

It is interesting to note that the investigation team was not able to determine which of these two scenarios actually occurred. They were able to narrow the choices down to only two likely scenarios. The reader may not initially see the value in the team's nondefinitive conclusions. But the reader should realize that what the investigation team did was uncover two highly likely scenarios capable of leading to the contamination of the LPG system. In other words, the investigation team conducted an abbreviated process hazards review of the lean and rich DEA systems and discovered these potential accidents waiting to happen. This illustrates another valuable secondary benefit of the RCFA method.

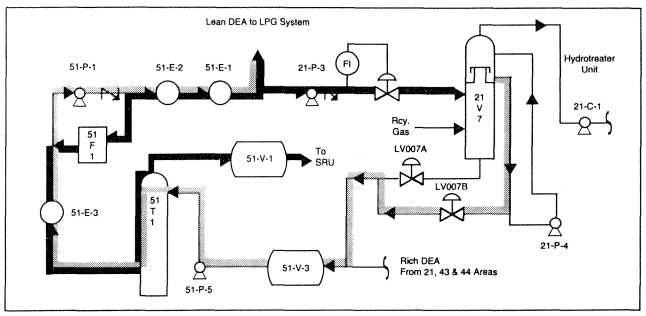

Figure 11. Rich/Lean DEA Flow Diagram.

As a result of the investigation, the team recommended:

• Modify the operating procedures to insure a water level is present in the recycle gas scrubber during the hydrotreater startup.

• Trip testing procedures verifying the proper operation of the reverse flow prevention instrumentation for the P-3 pumps be developed.

• The removal, inspection, and cleaning of the P-3 discharge check valve during all planned unit turnarounds.

Again, in this example the author shows an occasion where pumps were blamed for a major unwanted event and then exonerated. It is not uncommon to find in RCFAs that original assumptions are proven to be groundless. By maintaining its objectivity and attention to the facts, the team can be assured of success in culling assumptions and unsubstantiated scenarios from the definitive scenario(s) that can stand the test of scrutiny.

CONCLUSION

The author has shown in the examples contained in this tutorial the value of fault trees in determining the root cause of complex multievent failures, such as those typically occurring in rotating equipment. While the techniques presented here are powerful, the author believes they can only be successfully employed if the following prerequisites are present:

• The full support of management

• Qualified multidisciplinary team members

• Adequate resources in the form of time, consultants, if required, analysis equipment, etc.

• RCFA training

• Acceptance of these methods by all those in the organization

Initiating RCFA programs in plants is the first step in realizing the continuous organizational improvements obtained by RFCAs and fault trees.

REFERENCES

1. AIChE, Hazards Evaluation and Reliability Analysis of CPI Systems Course, Houston, Texas (March 1989).
2. AIChE, "Guidelines for Hazard Evaluation Procedures," Center for Chemical Process Safety (1992).
3. Reliability Center Inc. and Failsafe Network Inc., Failure Analysis Investigation Methods Course (February 1991).
4. Fussel, J.B., and Wagner, D.P., "Fault Tree Analysis as a Part of Mechanical System Design," AIChE, Hazards Evaluation and Reliability Analysis, Texas (March 1989).
5. Department of Labor, "29 CFR Part 1910 - Process Safety Management of Highly Hazardous Chemicals," Notice (February, 1992).
6. American Petroleum Institute, "Management of Process Hazards, API Recommended Practice 750, First Edition" (1990).

7. Arey, R.W., "Reliability Through Improved Failure Analysis—A Closer Look," National Petroleum Refiners Association Paper, Atlanta, Georgia (February, 1985).

8. Citgo Petroleum Corp., "Incident Investigation Manual" (October, 1991).