

[Click here to return to Session Directory](#)



**DYNAMIC POSITIONING CONFERENCE**

**October 12-13, 1999**

**RELIABILITY SESSION**

---

**DP System Reliability –  
Quantitative vs. Qualitative Analysis**

**Marc D. Quilici**  
***EQE International***

---

## Overview

As shipboard systems become more complex and interrelated it is important to examine the methods used to assess the reliability of these systems. Traditionally, qualitative methods such as Failure Modes and Effects Analyses (FMEAs) have been used to identify any single failures that have the potential to prevent the system from accomplishing its intended purpose (i.e., station-keeping). Although rigorous application of the FMEA methodology will identify any single failures, as systems become more complex, the burden on the analyst to consider system interdependencies has risen significantly. This paper provides a brief overview of the FMEA methodology and a quantitative approach, which utilizes fault tree modeling of the system to determine the reliability and to aid in identifying any weak links in the system design. For the purpose of this paper, system refers to the entire set of equipment and operator actions necessary to provide the desired function. This includes the main hardware as well as portions of support systems (e.g., power, air, HVAC) whose operation or non-operation can affect the ability to provide the desired function. The advantages and disadvantages that apply to each of these methods are discussed along with examples of the application of the fault tree methodology to several deepwater drillship areas, and other types of systems in other industries. A summary of conclusions is provided in the last section.

## Failure Modes and Effect Analysis Methodology – Overview

Failure Modes and Effects Analysis (FMEA) has been used extensively over the years to ensure that one of the largest impediments to reliability of equipment and systems, the single point failure, is identified. Once the single point failures are identified, the single point failures are either designed out of the system or care is taken to ensure the associated critical component is of the highest achievable reliability. The process of developing the FMEA is a methodical examination of each component and the impacts to the overall system operational goal resulting from a failure of the component. In some cases, the effects may be fairly obvious, i.e., failure of a valve to open on demand results in loss of critical flow in a section of piping. The resultant effects of other failures, particularly in control systems or in support systems may be more difficult to categorize as to their effect on the overall operation. [Figure 1](#) shows an example FMEA worksheet used to document the analysis.

Depending upon the desired uses of an FMEA, different categories/criteria can be applied during the evaluation to allow the results to be ranked in order of importance. Two typical criteria which are used and their definitions include :

**Failure Frequency** - A relative assessment of the failure frequency associated with the failure mode based on historical data where available. Typically ranges are assigned as follows:

- Frequent - Frequency  $> 10^{-1}$
- Probable -  $10^{-1} > \text{Frequency} > 10^{-2}$
- Occasional -  $10^{-2} > \text{Frequency} > 10^{-3}$
- Remote -  $10^{-3} > \text{Frequency} > 10^{-6}$
- Improbable - Frequency  $< 10^{-6}$

**Class** - The assessed criticality of the failure. The criticality categories assigned and their associated definitions are:

- **Class I** - Safe, negligible impact to safety, no effect on the system. This class is assigned to those failures that fail only a portion of the redundancy necessary to perform a function and are easily diagnosed.
- **Class II** - Marginal, failure will degrade system to some extent but will not cause major system damage or injury to personnel. This class is assigned to those failures that: 1) fail one redundancy which is capable of performing the critical safety functions and are easily diagnosed to determine the failure or 2) fail only a portion of the redundancy necessary to perform a function but are not easily diagnosed.
- **Class III** - Critical, failure will degrade system's performance and/or cause personnel injury. If immediate action not taken, serious injuries or deaths may occur and/or loss of the system. This is assigned for those features which fail the capability to perform the critical safety functions from one redundancy and some diagnosis and interpretation is required to identify the failure.
- **Class IV** - Catastrophic, failure will produce severe system and/or multiple deaths or injuries. This is assigned for those failures which directly lead to full loss of one of the critical safety functions

In general, the consequences of failures determined to be class IV, are generally considered unacceptable in a final design, due to the severity of the consequences.

## Quantitative Reliability Assessment Methodology – Overview

Quantitative Reliability Assessment (QRA) has been applied to a wide variety of systems in a wide range of industries. One of the most adaptable QRA methods is the use of fault tree analysis to model the operation of equipment. The methodology was developed for the aerospace industry and has been applied to numerous other industries. The fault tree methodology focuses on the relationships between components and the logic of the fault trees is used to identify the overall impact to the ability of the system to perform its safety or operational function. For each safety function, the immediate causes of failure of the function are identified, sometimes in very broad terms. These causes are broken down further into the basic failures or human errors which may result in the failure of the function. The fault tree methodology is a very structured, methodical process which, by the nature of the method, assists the analyst in ensuring that each potential failure of the system is represented. [Figure 2](#) provides an example of the various symbols found in a graphical representation of a fault tree. The following describes each of the symbols found in [Figure 2](#). An example of a section of the tree proceeding from the general to specific is shown in [Figure 3](#).

The fault tree model is developed from logic gates, which are graphic representations of Boolean AND and OR operators, and basic events which are analogous to individual failures. The logic gates are used to define the relationships between the components and correctly identify and account for the system interdependencies. The graphical symbols seen in [Figure 2](#) are the symbols most often used in fault tree analysis. These symbols are: AND Gate, OR Gate, Transfer, and Basic Event. These symbols and their definitions are discussed below.

### **OR GATE**

(SEE SYMBOL LABELED OR-GATE)

A Boolean logic operator with one or more inputs which is true if any of the inputs to the gate are true. For example, in [figure 2](#), if any of the basic events, BASIC-EVENT-2, BASIC-EVENT-3, or BASIC-EVENT-4 which are input to the OR gate occur, the OR gate is considered to occur.

### **AND GATE**

(SEE SYMBOL LABELED AND-GATE)

A Boolean logic operator with one or more inputs which is true if all the inputs to the gate are true. For example, in [figure 2](#), if the basic event (labeled BASIC-EVENT-1) and the OR gate occur, the AND gate is considered to occur.

### **TRANSFER**

(BOX WITH A TRIANGLE BELOW - SEE SYMBOL LABELED TRANSFER)

Convenience for the analyst which denotes that this event is described in more detail in another place within the model (e.g., another page).

### **BASIC EVENT**

(BOX WITH A CIRCLE BELOW - SEE SYMBOLS LABELED BASIC-EVENT-X)

This symbol represents a basic component failure, human error, or maintenance unavailability. These events are representative of the lowest level of resolution in the model. Each basic event has an associated probability of failure associated with it if quantitative results are desired.

The fault tree modeling process starts with the big picture and then deductively decomposes the system down into individual faults. The development of the fault tree model begins by identifying the undesired condition to be examined, commonly referred to as the top event. This event may be defined as broadly or as narrowly as desired but this event definition sets the bounds of the analysis so care must be taken. This event is usually defined as failure to achieve a desired goal for example, "Failure to hold station". Once the top event is defined, the analyst performs a systematic review of each small piece of the system to determine how that event can happen, either in terms of basic events (e.g., Failure of the a thruster) or in terms of other broader events (e.g., Failure of electric power to the thruster). These broadly defined events are usually represented by AND or OR logic gates which are then examined in the same manner as the top event. The modeling process continues until all of the broad events are defined in terms of basic events and the associated logic gates. Dependencies on common support systems or equipment are identified in the logic during the model development. The fault tree logic model is then evaluated via a boolean reduction computer algorithm to determine the possible combinations of basic events that will result in occurrence of the top event. These possible combinations are referred to as cutsets. The cutsets may be qualitative in nature if no failure data is applied or quantitative if failure data is applied depending upon the desired goal of the analysis.

## **FMEA Benefits and Limitations**

As noted previously, FMEAs have been performed for a number of years and are readily recognizable and are generally an accepted means of demonstrating attention to reliability. If the analysts performing the FMEA are consistent in the handling of system interfaces and adhere completely to the established methods of examining the reliance of the main system on support systems, the methodology is completely

capable of identifying any single point failures that may exist in the system. The analysis is traceable in that every component included in the system has a worksheet filled out so the omission of any component can be identified by a straight comparison with the equipment list. Another benefit of the FMEA process is that it is basically a forms-based analysis and no special evaluation software is required. FMEAs may be maintained in a database, however, it is not required and any commercially available database software may handle the simple requirements for sorting and cataloguing. The FMEA process is a relatively straightforward analysis technique which can be performed by analysts who are familiar with the system requirements and operation.

The fact that the FMEA primarily represents a documentation trail that is used to assess the acceptability of the system design is one of the limitations of FMEAs. The static nature of an FMEA does not lend itself to an easy straightforward examination of modifications to a design. While examination of some modifications, such as an increase in the number of thrusters may be readily performed for the main equipment, dependencies which arise are not so easily incorporated and evaluated and oftentimes require a reexamination of a significant portion of the analysis.

Although the FMEA methodology is capable of identifying any single point failures within the system, the increased complexity of the systems including control functions and feedback mechanisms has greatly increased the burden on the FMEA analyst to consider many more potential effects which may result from any one failure. While it is not impossible to trace all the dependencies accurately, the potential for oversight is significantly increased by the complexity of the equipment and interactions.

The FMEA methodology does not provide a means to easily assess the potential for multiple failures which may be more likely than single failures in a mature field-proven design. Also, such observed failure mechanisms as common cause failures are not usually examined during the course of an FMEA.

In general, the FMEA is often viewed as a paper study that must be performed to satisfy a requirement to obtain Class on a vessel and cannot readily be used as a tool for operational guidance following a non-critical component failure. Unfortunately, a large majority of the valuable information assembled and evaluated to perform the FMEA is not readily accessible for other uses.

As in any type of analysis, the quality and applicability of the FMEA is dictated by the analyst's understanding of the system design and operation and the appropriate level and scope of the FMEA.

### **QRA Benefits and Limitations**

The QRA methodology itself assists the analyst to identify and evaluate the systems and all the system interdependencies in a logical fashion. The fault tree structure "keeps track" of the dependencies such that the impacts of single or multiple failures are properly cascaded through the modeled systems. Fault tree modeling allows the analyst to examine one small piece of the system at a time and not try and keep the entire system picture in mind. Oftentimes when an analyst must keep the entire system in mind, subtle interactions which significantly affect system reliability may be overlooked in favor of the 'big picture'. Identification of all single failure points within the system boundaries (including any modeled support systems) is a subset of the results obtained in a quantitative assessment. In fact, quantitative

analyses have identified single failures that were not identified in an FMEA conducted for the same system. These single failures resulted from complex support system interdependencies that are difficult to track in the FMEA style analysis.

In addition to identifying the single point failures, QRA provides information about multiple failures and their likelihood of occurrence, a numeric ranking of the system components in terms of their importance to system reliability, and a tool to allow the application of cost-benefit evaluations of design features/modifications. Changes to system designs/operational philosophies can be readily evaluated in terms of reliability using the existing quantitative model. An assessment of the actual reliability of the system following a failure or maintenance outage of a piece of equipment can be made relatively simply using the existing model. Such an evaluation can be used to assure that an equipment outage does not severely impact the system reliability or if it does, to minimize the time spent in that configuration.

As with any analysis methodology, QRA has its own set of drawbacks/limitations. The analysts performing the evaluation must be familiar with the system requirements and operation as well as experienced in fault tree modeling techniques. Also, due to the complexity of the model and the vast number of failure combinations which may lead to system failure, sophisticated computer analysis tools must be used. This has become significantly less important with the incredible power available in today's personal computers. In the past, large mainframe computers were required to solve the models at significant monetary and time expense, however today's codes solve the models for all practical purposes instantaneously at essentially no cost.

Another issue which has generally been raised as to the validity of a QRA is the issue of failure data which is used to quantify the fault tree model. Failure data is sometimes sparse and has great uncertainty bounds associated with it. Reasonable care needs to be taken in the application of any failure data and an evaluation of data applicability is important. However, the most important use of failure data should not be considered to be the generation of one number which represents overall system reliability. Rather the relative contributions of different single failures or multiple failure combinations should be considered to be the most important result of the analysis. Regardless of the failure data applied to quantify the model, all of the generated failure combinations represent valid ways for the system to fail if the model is correct. The quantitative ranking of these combinations, while sometime yielding surprises, needs to pass a sanity check by people familiar with system operation. Due to the uncertainty associated with the failure data, failure combinations within an order of magnitude in likelihood can be treated as having a similar likelihood of occurrence. Combinations which vary by more than an order of magnitude are expected to be of lower importance to system reliability and should accordingly be afforded less attention when considering design improvements or operational restrictions.

Similar to the FMEA, the quality and applicability of the fault tree analysis is dictated by the analyst's understanding of the system design and operation and the appropriate level and scope of the QRA.

## Examples of QRA Applications

QRA has been applied in a variety of industries to assess the reliability of systems and to serve as a design and operational tool to maintain reliability at as high a level as possible. It is a mature analysis tool which is readily adaptable to evaluate any type of system, be it mechanical, electrical, instrumentation/control. Specific examples of the use of fault trees models to examine reliability for deepwater drill ship systems are discussed below, including the information gained and the impact the analysis had on the design/operational process.

**Drawworks Control System:** A fault tree analysis was performed to evaluate the reliability of the system during normal operation. The model included the control system hardware and software as well as portions of the supporting systems necessary for drawworks control system operation. Two types of scenarios were evaluated, failures which resulted in downtime and those that had the potential for equipment damage or serious injuries to personnel. Overall the system was found to be well designed for reliability however, several design issues were identified which were not consistent with good reliability design practices. The system was found to have a lack of full redundancy in the remote rack PLCs, and potential for downtime if either power source failed.

**Blowout Preventer (BOP) MUX Control System:** During familiarization of the analyst with the specific system being analyzed, a system design/documentation error was identified before the system was built. Although system testing would have found the error prior to actual operation, a significant cost in rework, retest, and late delivery was avoided.

**Blowout Preventer (BOP) MUX Control System:** A fault tree analysis of the MUX control system was performed to evaluate the ability of the system to properly control disconnect and well control operations. The model included the control system hardware as well as portions of the supporting systems necessary for BOP MUX control system operation of critical stack functions. The analysis identified several single spurious failures which would effectively disable both of the redundant hydraulic supplies to the redundant control pods, thereby preventing the control system from providing the designed safety functions.

**Blowout Preventer (BOP) MUX Control System:** A fault tree analysis of the MUX control system was performed to evaluate the ability of the system to properly control disconnect and well control operations. The model included the control system hardware as well as portions of the supporting systems necessary for BOP MUX control system operation of critical stack functions. Evaluation of the fault tree model identified a lack of true redundancy in the hydraulic supply to the primary and secondary disconnect functions. An inexpensive modification was proposed and implemented in the hydraulic system which significantly increased the overall system reliability and redundancy

**Blowout Preventer (BOP) MUX Control System:** A fault tree analysis of the MUX control system was performed to evaluate the ability of the system to properly control disconnect and well control operations. The model included the control system hardware as well as portions of the supporting systems necessary for BOP MUX control system operation of critical stack functions. The analysis process identified that little attention had been paid to critical signals which were located on single circuit cards. The solenoid

fire card circuits could be easily switched to redundant cards for improved safety function operability and reliability.

**Riser Handling System:** A fault tree analysis of the riser handling system was performed to examine the reliability of the riser handling system and its potential for downtime which would directly disable the ability to run riser prior to drilling. The model included the entire riser handling system as well as portions of the supporting systems necessary for riser handling system .

**Chemical Process Plant Operations:** A fault tree analysis was performed to evaluate the process control system at two chemical process plants. The fault tree assessments demonstrated OSHA requirements could be met by identifying software checks and interlocks (minimal cost) and inexpensive instrumentation additions. The \$60,000 studies identified ways to reduce risk by factors of 80 and 65 below initial new designs. It also demonstrated two expensive features proposed to reduce risk were not nearly as effective as an alternative solution, potentially saving \$250,000 per plant (52 plants), or reducing risk by another factor of seven.

**Power Plant Safety Assessments:** Numerous risk assessments have been conducted on power plant and have recently been used to perform cost-benefit analysis and to justify less costly modifications on the basis of increased reliability/safety associated with the lower cost modification. These analyses have consisted of using fault tree techniques to evaluate safety modifications suggested by plant vendor. In one plant, of the approximately \$50,000,000 safety modifications suggested by the vendor, only 1/10 had significant safety benefit. Over \$20,000,000 were not implemented, and others were revised to increase their benefit to safety. The total cost reduction was 40%, with an increased safety of 33% based on a study which cost \$200,000. For another plant, \$30,000,000 safety modifications were suggested by the vendor to improve safety. The analysis was used to show that alternate modifications would increase safety about the same, but cost less than \$5,000,000 based on the study which cost \$400,000.

## Conclusions

While QRA has not been previously used to evaluate the reliability of DP systems or to obtain classification for a DP vessel, the potential exists to utilize this tool. The benefits derived from the use of QRA are significant. The QRA, while identifying the same single point failures as an FMEA, also yields additional valuable information which can be used to maintain a highly reliable system. The model is a dynamic tool which can be used to easily evaluate the reliability impacts of system modifications or of equipment failures.

The system and operational information required to perform either an FMEA or a QRA are virtually the same so no additional effort is required in that area. The major area of difference in the effort to perform an FMEA or a QRA is what is done with that information. The FMEA process involves evaluating the overall effects to the system of a failure in each component. The documentation of this effort is the major cost associated with an FMEA, whether it be paper based or contained in a database. The fault tree examines each part of the system, only considering the immediate impacts on the directly affected components. The analyst does not have to consider the overall effects but rather the component and

system interdependencies. The major cost associated with a QRA is the development of the fault tree model itself and assuring that it accurately reflects the operation of the system. Depending upon the level of data to be applied to either the FMEA or QRA model, the cost of data collection and analysis can be another significant cost. In general, data collection and analysis costs may be slightly higher for the QRA model. This is primarily due to the need to more accurately determine the component failure rates than the quantitative ranking shown earlier for the FMEA. The FMEA results consist of an identification of the single point failures. The QRA results rank each single and multiple failure combination in terms of likelihood, providing an assurance that the single faults identified are the most likely ways for the system to fail.

In a previous demonstration of the utility of using a QRA model, two single failures were identified which were missed in a standard FMEA. These single faults were failures in a support system, which due to dependencies and interactions within the system, resulted in the direct failure of both redundancies of the main system responsible for providing the safety function. The FMEA analysts themselves confirmed the correctness of the failures and commented that they 'could' have found them within the FMEA framework. While this is true, the complexity of the system provided a severe impediment to the FMEAs ability to identify these types of faults. The fault tree model, rather than impeding the identification of these items, actually helped to focus the analyst on the critical areas and dependencies which resulted in the single faults.

In addition to the identification of the most likely faults, the results of a quantified fault tree model provides calculated importance factors which can be used to identify the criticality of individual failures. These importance factors are a valuable aid to determining where, if any, changes to the system will be of the greatest benefit to increasing the overall reliability of the system. Such changes may be as simple as being more explicit in the operating procedures, increased inspection frequencies or testing, or may be more complex such as actual configuration changes to add additional redundancy or flexibility of operation. The key is, these tools can provide guidance as to the most cost-effective way to increase overall reliability.

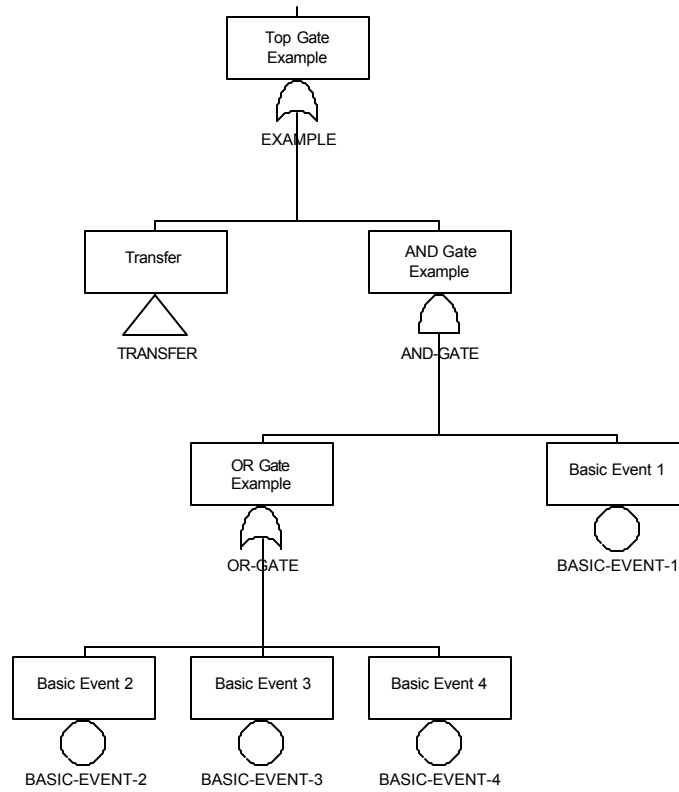
As noted above, the areas which are most costly in each type of analysis are different for each analysis type. A study of a Blowout Preventer (BOP) Multiplex (MUX) Control system was performed which included both an FMEA and a QRA model. The cost of performing each type of analysis was within five percent of each other with the fault tree analysis being slightly higher. There was not complete independence between the two analyses however. The cost savings on this project were derived by confirming the FMEA results for individual failures using the fault tree model. If the fault tree model were not available and additional means for confirming the correctness of the FMEA were used, there would have been virtually no cost difference between the analyses.

[Return to text](#)

FMEA Worksheet		Component ID:		Component Description:							
Component	Failure Mode	Effects On		Class				Failure Frequency	Detection Method	Compensating provisions and remarks	
		Other Components	Whole System	I	II	III	IV				

**Figure 1: Example FMEA Worksheet**

[Return to text](#)



**Figure 2: Fault Tree Symbols**

[Return to text](#)

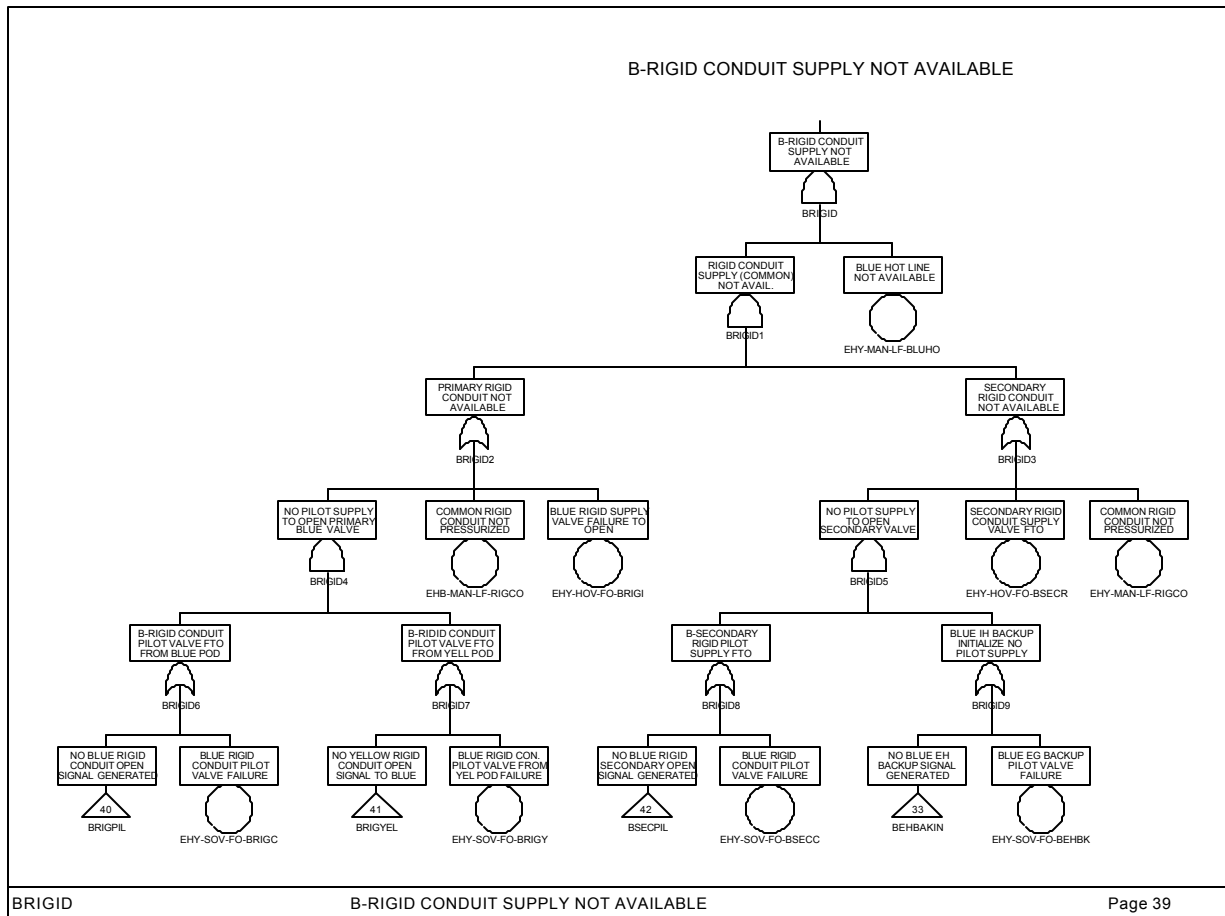


Figure 3: Fault Tree Development Example