Reliability Analysis for Power to Fire Pump Using Fault Tree and RBD

Michael Anthony, PE
University of Michigan
(maanthon@umich.edu)

Robert Arno ITT Exelis
Information Systems
(Robert.Arno@itt.com)

Neal Dowling
MTechnology
(dowling@mtechnology.net)

Robert Schuerger PE
HP Critical Facility Services
(bschuerger@hp.com)

Abstract:
One of the most common questions in the early stages of designing a new facility is whether the normal utility supply to a fire pump is reliable enough to "tap ahead of the main" or whether the fire pump supply is so unreliable that it must have an emergency power source; typically an on-site generator. Apart from the obligation to meet life safety objectives, it is not uncommon that capital on the order of $100,000 to $ 1 million is at stake for a fire pump backup source. Until now, that decision has only been answered with intuition-- using a combination of utility outage history and anecdotes about what has worked before. There are processes for making the decision about whether a facility needs a second source of power using quantitative analysis. Fault Tree Analysis (FTA) and Reliability Block Diagram (RBD) are two quantitative methods used in reliability engineering for assessing risk. This paper will use a simple one line for the power to a fire pump to show how each of these techniques can be used to calculate the reliability of electric power to a fire pump. The paper will also discuss the strengths and weakness of the two methods. The hope is that these methods will begin tracking in the NFPA documents that deal with fire pump power sources and can be used as another tool to inform design engineers and authorities having jurisdiction about public safety and property protection. These methods will enlighten decisions about the relative cost of risk control with quantitative information about the incremental cost of additional 9's of operational availability.

.

Index Terms: *reliability, availability, failure rate, mean time between failure, mean time to repair, Fault Tree Analysis, Reliability Block Diagram, public safety, fire pump, emergency power*

I. INTRODUCTION

Risk assessment is an important issue in many areas of our lives, from the safety and well being of our families all the way to global concerns for the environment. Specific tools have been developed in the field of Reliability Engineering to help quantify various types of risks. Two of these tools are Fault Tree Analysis (FTA) and Reliability Block Diagram (RBD). Since mitigating the risk of causing a fire was one of the most driving concerns in the development of industrial and commercial power systems, it seems fitting to show how far we have come, that now a major concern has become not having power to fight the fire. So power to the fire pump has been selected as the risk to assess in this paper because the requirements for fire pump power supply originate in Articles 695 and 700 of the National Electrical Code and Chapter 9 of NFPA 20 (Standard for the Installation of Stationary Pumps for Fire Protection) but only contain the following qualitative statement:

"9.3.2 Other Sources. Except for an arrangement described in 9.3.3, at least one alternate source of power shall be provided where the normal source is not reliable." (NFPA 20-2010)*

In many cases, local building codes require that an on-site generator be installed for all high-rise buildings. In other cases, however, owners of non-high-rise buildings are effectively forced into installing a fire pump -- and the sprinkler system that depends upon it -- because of limited municipal fire protection services or because their insurance rates depend upon that fire pump providing water to the sprinkler system for life safety and/or property loss protection.

II. RELIABILITY TERMINOLOGY AND METRICS:

Much of the terminology of Reliability Engineering is common English words or terms borrowed from Statistics. It would probably be more correct to say that Reliability Engineering depends upon the subject of Statistics, since statistics and probability are used extensively for quantification of what is being analyzed. There are a group of important metrics or parameters for quantitative assessment that will first be defined to ensure the reader has complete understanding of how the terminology is being used in this paper.

Availability (A): Availability is the long-term average fraction of time that a repairable component or system is in service and satisfactorily performing its intended function. For example, if the electricity is off for one hour in a year, but the rest of the year the electricity is on, the availability of electrical power for that year is 8759 hours divided by 8760 hours, which is 0.999886.

$$Availability(A) = \frac{(time\ operating)}{(time\ operating + down\ time)}$$

An availability of 0.99999 means that the system has an average down time of 5.3 minutes (or 315 seconds) per year. It makes no difference in the availability calculation if there

978-1-4673-0651-5/12/$31.00 © 2012 IEEE

was one 5.3 minute outage, or 315 one-second outages. It could also be one outage of 1.77 hours in 20 years. In all three cases, the availability is 0.99999.

There are two common measures of availability, *inherent availability* and *operational availability*. The difference between the two is based on what is included as "down time" or "repair time." For inherent availability, only the time it takes to fix the equipment is included. Inherent availability assumes that the technician is immediately available to work on the equipment the moment it fails, and that he has all the parts, etc., necessary to complete the repair.

For operational availability, all the delays for scheduling, travel time, parts, etc. are included. If it takes 24 hours to fly a part in to repair the equipment, that adds to the "repair time."

Inherent availability and operational availability show different aspects of the system being analyzed. Operational availability would be the "real world": how the system really operates. There are usually delays between the time a piece of equipment fails and when the repair begins. Spare parts inventories are also very significant and directly impact operational availability. Therefore, when determining spare parts inventories, on-site personnel and their level of training, etc., operational availability is a useful tool.

Inherent availability is a more useful tool in analyzing the system design. Since there are wide variations in the maintenance practices from facility to facility, operational availability could vary significantly between two facilities with identical infrastructures. Eliminating all of the logistics involved with getting the parts and trained individuals to the piece of equipment, and counting only the actual repair time provides a more accurate evaluation of the infrastructure design. It shows the availability that is "inherent" to the design, if the spare parts inventory and repair are perfect.

In this paper all of the values and discussion concerning availability will be for inherent availability. It should also be noted that only the electrical power for the fire pump/controller is being discussed in this paper. The motor for the pump has been included in the analysis. But the analysis does not address whether the pump has water, or any of the mechanical issues involved with the fire pump providing water to fight a fire. Also, while many fire pump/controller systems can be built with an integral transfer switch, this analysis covers the more common situation in which the transfer switch is remotely mounted.

The *failure rate* (λ) is defined as the rate that a failure per unit time occurs in the interval, given that no failure has occurred prior to the beginning of the interval.

Mean time between failures (MTBF), as its name implies is the mean (average) time the equipment performed its intended function between failures.

For the case of a constant failure rate:

$$MTBF = 1/\lambda$$

Electrical equipment, along with many other types of equipment, has a relatively constant failure rate over much of its useful life. A common assumption for many types of reliability analysis is that all the equipment in the system to be analyzed falls within this statistical distribution where the failures are random and the failure rate is constant. All of the calculations shown below assume a constant failure rate for the equipment.

Mean time to repair (MTTR) is the average time it takes to repair the failure and get the equipment back into service.

Inherent Availability is mathematically defined as the mean time between failures divided by the mean time between failures plus the mean time to repair:

$$A = MTBF/(MTBF + MTTR)$$

Reliability (R) is the probability that a product or service will operate properly for a specified period of time under design operating conditions without failure. Reliability is time dependent. The longer the time, the lower the reliability, regardless of what the system design is. The better the system design, the higher the probability of successful operation *for a longer period of time*.

For a constant failure rate λ, reliability as a function of time R(t) is:

$$R(t) = e^{-\lambda t}$$

To summarize what as been provided above, there are five important metrics used to define the "reliability" of a system; *MTBF, MTTR, availability, reliability and time.* It has also been shown how these five factors are interrelated. What is not as obvious is that "availability" is relatively *time independent*, since it is the combination of two terms that are themselves averages over long periods of time (mean time between failure and mean time to repair). Reliability, as shown in the equation above, is very "time dependent."

Reliability is the "probability of success" for a given period of time. Reliability is a metric directly related to how often (or how fast) the system fails. As shown in Table 1, the system that failed once in a year for 5.3 minutes would have a much better reliability than the system that failed 315 times for one second, but no where near as good as the system that failed once in 20 years for 1.77 hours, even though all have the same availability.

Availability	Number outages per year	Failure rate - failure/hour	MTBF (hours)	MTBF (years)	Reliability (1 year)
0.99999	315	3.60E-02	27.81	0.0032	0%
0.99999	1	1.14E-04	8,760	1.0	36.78%
0.99999	0.05	5.71E-06	175,200	20	95.12%

Table 1: MTBF of outages examples

The reliability has dropped to 36.8% when the MTBF of the system is reached (see MTBF of 1 year). Therefore, the system that fails 315 times a year has a reliability of 36.8% a little over a day after you start it, while the system that fails

978-1-4673-0651-5/12/$31.00 © 2012 IEEE

one time takes a year to reach this same level of reliability. The last one takes 20 years for the reliability to drop to 36.8%!

The discussion above demonstrates the importance of using both reliability and availability as metrics to determine how dependable the component or system is.

"Unreliability" or "Probability of failure" and "unavailability" can also be used in place of reliability and availability.

Unreliability = Probability of failure = 1 – Reliability
Unavailability = 1 - Availability

III. FAULT TREE ANALYSIS:

Fault Tree Analysis (FTA) is a top-down approach where an undesirable event is identified as the "top event" in the "tree" and the potential causes that could lead to the undesirable event are identified as "branches" below. Fault Tree Analysis uses Boolean Algebra (AND gates, OR gates, etc.) in a graphical representation to show the logical interrelationships between the initiating "basic events," such as component failures, etc. in the branches to other branches and the top event. The "OR" gate has an output if any of the inputs are true. The "AND" gate has an output if all of the inputs are true.

If the failure rate and repair data is available for all of the initiating "basic events" in the Fault Tree, quantitative results (unreliability and unavailability) can be calculated for the "top event" and each of the branches.

FTA is an excellent tool to analyze specific failures that have critical importance. By working backwards from the failure to be prevented down to all of the items that could cause this particular failure, interfaces between equipment and systems can be brought to light that may be overlooked with other types of analysis.

IV. RELIABILITY ANALYSIS

The Gold Book, IEEE Standard 493-2007, Recommended Practice for Design of Reliable Industrial and Commercial Power Systems [1] provides the methodology, along with failure and repair data required to perform reliability analysis on the electrical and mechanical systems.

Table 2 lists the failure and repair data used in the analysis of power to the fire pump.

The first task required to perform reliability analysis is to define "failure" for the system. For this example, "failure" is loss of power to the fire pump. Please note: There is no attempt to determine whether the fire pump is needed when the power fails. The probability of "no power to the fire pump" AND "fire" at the same time is much more extensive analysis.

Part Description	MTBF (Hours)	MTTR (Hours)
Utility power - single	4,478.5	1.32
Utility power - two independent sources	28,077	0.52
Transformer	2,642,019	37.23
Fused Disconnect	3,829,588	3.95
Generator	545.1	4.10
Circuit Breaker	2,644,087	1.52
ATS	101,642	5.73
Motor and Starter	348,699	7.96

Table 2: Failure and repair data used for the fire pump

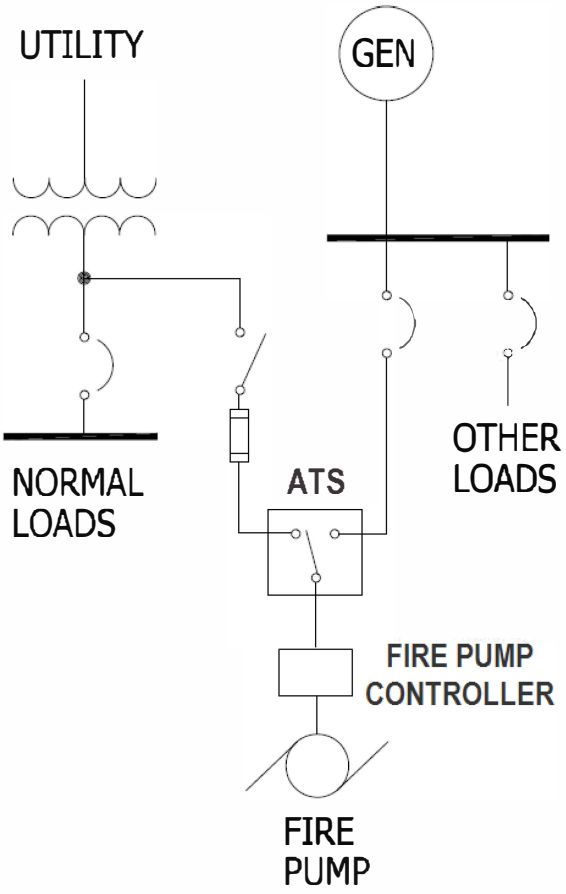

Figure 1: One-line diagram for power to fire pump

The one-line diagram for the fire pump is shown in Figure 1. The normal source of power consists of utility power to a transformer, with the fused disconnect connected on the line side of the main circuit breaker. The alternate source is a standby generator supplying power thru a circuit breaker to an Automatic Transfer Switch (ATS) that is de-coupled from the fire-pump/controller system.

The failure and repair data given for each of the items listed under "Part Description" includes all of parts that make up the assembly. For example, the "fused disconnect" assembly consists of the failure and repair data for a fuse, low voltage disconnect switch, low voltage cable and a cable termination.

978-1-4673-0651-5/12/$31.00 © 2012 IEEE

Cut #	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
1	67	8.30E-02	ATS	ATS1: ATS	8.30E-02
2	30	3.70E-02	GENERATOR-FTR	GEN3: GENERATOR	4.30E-02
			UTILITY-FAILS	UTL: UTILITY SINGLE CIRCUIT	8.60E-01
3	4.2	5.20E-03	GENERATOR-FTS	GENERATOR FAILS TO START	6.10E-03
			UTILITY-FAILS	UTL: UTILITY SINGLE CIRCUIT	8.60E-01
4	1.5	1.80E-03	STARTER	MAGNETIC MOTOR STARTER FAILS	1.80E-03
5	0.4	4.30E-04	ATS-FTS	ATS FAILS TO SWITCH	5.00E-04
			UTILITY-FAILS	UTL: UTILITY SINGLE CIRCUIT	8.60E-01
6	0.1	1.40E-04	GENERATOR-FTR	GEN3: GENERATOR	4.30E-02
			TRANSFORMER	XFMR1: TRANSFORMER < 600 V (FMEA)	3.30E-03
7	0.1	9.80E-05	FUSED-DSW	FUSED DISCONNECT SWITCH	2.30E-03
			GENERATOR-FTR	GEN3: GENERATOR	4.30E-02

Table 4: Cut set report for fault tree of Figure 2

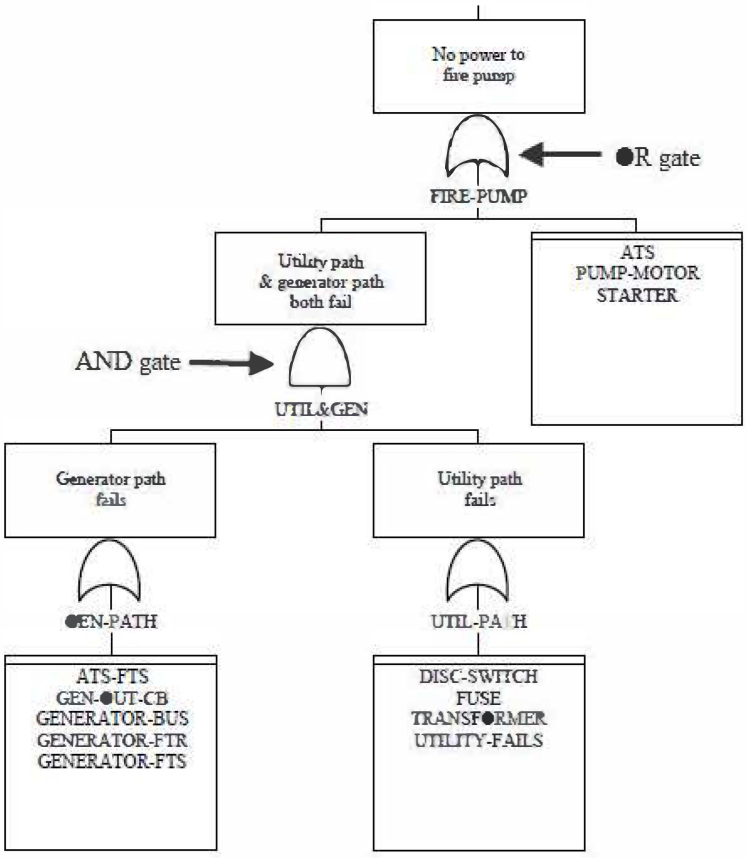

Figure 2: Fault Tree for power to the fire pump.

In addition to the failure and repair data in Table 1, two direct probabilities are included in the analysis; the probability of the generator starting is 0.99394 and the probability of the ATS transferring is 0.99. For the fault tree, the all data are entered as probability of failing, so the two probabilities are entered as probability of the generator not starting of 0.00606 (GENERATOR-FTS) and the probability of the ATS not transferring of 0.01 (ATS-FTS).Figure 2 shows the Fault Tree used to analyze the power to the fire pump. Table 3 shows the reliability analysis for the Fault Tree in Figures 2 using reliability software to calculate the unreliability (probability of failure) and unavailability.

Description of Fault Tree	Probability of Failure (1 Year)	Unavailability	Availability
Power to Fire Pump - single utility & generator	12.33%	0.00010770	0.9998923

Table 3: Fault tree analysis results

One of the great benefits of fault tree analysis is that it identifies the minimal cut sets of basic events that lead to system failure. A minimal cut set is one where failure of every basic event in the cut set is necessary for system failure. A report is produced that lists the minimal cut sets in order from most likely to least likely. This can help in the assignment of scarce resources when trying to decrease the risk of system failure. A cut set report for the fire pump system appears in Table 4. This report identifies the ATS as a major contributor to system unreliability: two-thirds of system failures are due to this component. (As a one basic event minimal cut set, it is also shown to be a single point of failure.) The failure of the utility AND the failure of the generator to start or run is responsible for about one-third of system failures. The failures of other components are responsible for very little of the probability of system failure.

V. RELIABILITY BLOCK DIAGRAMS:

As stated in the introduction, the other common methodology to perform reliability calculations to be used for this paper is Reliability Block Diagram (RBD). RBD is a graphical representation of the components that make up the system, showing how they are connected. For electrical systems, the one-line diagram is used, and each major component, such as switchboard, generator, transformer, etc. is represented as a block on the diagram. The failure and repair rates for each component are entered in the block that represents it in the RBD. The blocks are connected in the same manner as the flow of electrical power, including parallel paths where they exist. Calculations are then performed to determine the reliability, availability and, mean time between failures (MTBF) for the system modeled in RBD.

For two blocks in series with failure rates of $\lambda 1$ and $\lambda 2$, (FR in blocks) the reliability as a function of time R(t) is:

$$R(t) = R(1) \text{ X } R(2) = e^{-(\lambda 1 + \lambda 2)t}$$

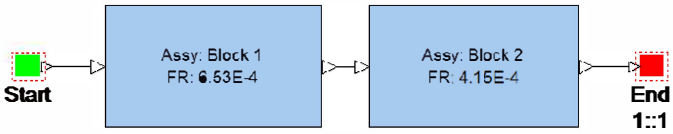

Figure 3: RBD with two blocks in series

For two blocks in parallel with redundancy, where 1 out of 2 is necessary for successful operation, the reliability as a function of time R(t) is:

$$R(t) = R(1) + R(2) - [R(1) \text{ X } R(2)] = e^{-\lambda 1 t} + e^{-\lambda 2 t} - [e^{-(\lambda 1 + \lambda 2)t}]$$

The junction in Figure 4 with 1::1 is the input; the junction with 1::2 is the output. The 1::2 in the output junction sets the redundancy for that junction to be 1 out of 2.

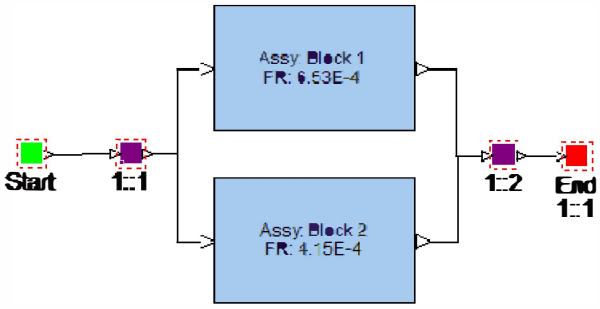

Figure 4: RBD with two blocks in parallel

RBDs for many systems have blocks combined in both series and parallel. If the components of the system are repairable, this further complicates the matter. For complex systems with multiple interconnections, where some of the components are neither in series nor in parallel but in a stand-by mode (such as a generator plant that is only active during a utility failure) direct analytical calculations are impractical. The reliability is calculated using a computer program that does random simulations, called a Monte Carlo simulation.

When performing a Monte Carlo simulation, multiple random series of simulations are performed on the RBD. These simulations are test runs through the system (from the start node through the end node) in order to determine if the system completes its task or fails. During each iteration or test, the software uses the properties of each block to decide whether that block is operating or not and therefore determines if the whole system is operating.

Shown in Figure 5 is the RBD for power to the fire pump. The junctions with 1::2 Sb are standby junctions.

978-1-4673-0651-5/12/$31.00 © 2012 IEEE

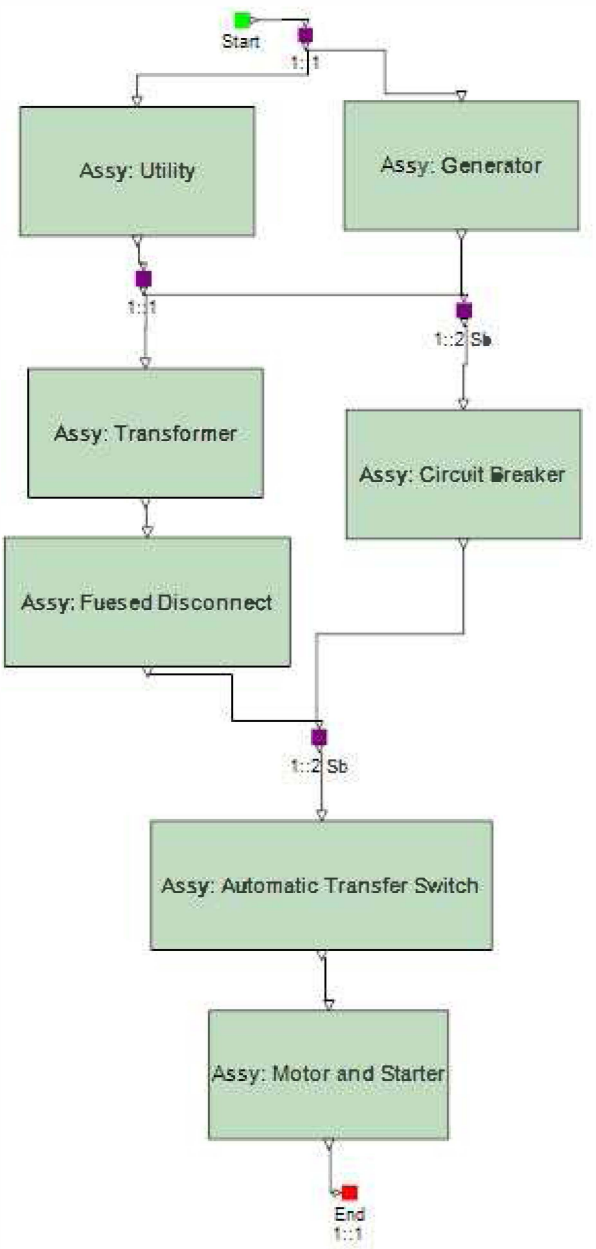

Figure 5: RBD for power to the fire pump

There are two special functions to a standby junction. First, in addition to setting the junction so 1 out of 2 is required for success, the priority of which is "normal" and which is "alternate" is also set. The second special function is the probability that the junction will transfer from "normal" to "alternate" can also be set. The probability of the generator starting of 0.99394 is in the standby junction below the generator and the probability of the ATS transferring is 0.99.

Three RBDs for power to the fire pump were calculated to show how RBD can be used for comparison of similar designs. The three RBDs consist of power to the fire pump from a single utility, power to the fire pump from two separate utilities, using an ATS and the RBD shown in Figure 5 of power to the fire pump from a single utility and a generator using an ATS. For all three, in addition to calculating the probability of failure for 1 year, the probability of failure for 5 years was also included. It is important to keep in mind that all of the reliability analysis in this paper is just for the reliability of power to the fire pump. There was no attempt made to determine if the fire pump was actually needed (because of a fire) at the same time power was not available. The probability of "no power to the fire pump" AND "fire" at the same time requires a much more extensive analysis.

Description of RBD	Availability	Probability of Failure (1 Year)	Probability of Failure (5 years)
Power to Fire Pump - single utility source	0.9996663	86.38%	99.99%
Power to Fire Pump - two utility sources	0.9999025	34.58%	87.92%
Power to Fire Pump - single utility & generator	0.9999169	12.47%	48.99%

Table 5: Reliability analysis using RBD for power to fire pump

We observe an improvement in reliability (1 – Probability of Failure) from 13.62% with utility-only as power source to 87.53% with the addition of an alternate power source. When capital decisions are being made about life, property and process protection, the availability improvement from only 0.9996663 to 0.9999169 should be taken into consideration with respect to other risk mitigation alternatives.

VI SUMMARY

After reading this paper and following through with the analysis, questions should arise as when, why and which of these analysis techniques to use. The answer is highly dependent on what the analysis is intended to evaluate.

The answer to the questions of when and why to perform the analysis is largely driven by the level of reliability needed for the installation and the economics of the situation. The greater the need for reliability the more likely the analysis will be of benefit. It can also be very cost effective to

978-1-4673-0651-5/12/$31.00 © 2012 IEEE

perform the analysis when comparing multiple options to determine the point of diminishing returns for the design.

The answer to which of the two techniques to use depends upon what is being evaluated by the analysis and what type of results are needed from the analysis. As shown by this example, for many types of evaluations either one is acceptable and the choice is driven more by what is available and the comfort level of the person doing the evaluation. For other types of analysis, there can be specific advantages to one over the other.

The most fundamental difference between FTA and RBD is that FTA focuses on failure and RBD focuses on success.. FTA concentrates on a particular failure characteristic and how it could propagate through the system. It looks for combinations of failures that could cause the top failure of the fault tree. This makes it ideal for focusing on a specific issue or area of a large system. The FTA may appear difficult to use, especially if you have a large complex system with many component interactions. However, developing the overall fault tree produces a rank-ordered set of "failure causes" that can help prioritize the use of scarce resources.

The RBD looks at combinations for success within the system being analyzed. Typically, it follows the one-line diagram, making it easy to understand by engineers with minimal experience with Reliability Engineering. This makes RBD an easy tool to use for determining the reliability of specific designs and for comparing multiple design variations to determine the point of diminishing returns.

There are also basic differences between these two analyses in how the calculations are performed. FTA is a static analysis over a fixed mission time. FTA analysis is performed using Boolean Algebra. Simple RBDs can be calculated with series and parallel combinations of the blocks, which is similar to using Boolean Algebra as FTA does. More advanced RBDs may include time varying solutions which utilize different probability density functions for repair or replacement. For the more complex RBDs, such as those with standby components and repairable parts, the software performs Monte Carlo Simulations. Monte Carlo Simulations are many iterations of random failures in which for each one the software determines if the system is operational (or failed), how long it ran before it failed (if it did) and how long it would take to fix what failed. Then it totals all of the simulations and provides the overall results for the whole RBD.

VII. CONCLUSION

This paper has shown how the tools of Fault Tree Analysis and Reliability Block Diagram can be used to provide quantitative analysis for the power to the fire pump. In the 2011 revision of the National Electrical Code a significant reference to ANSI/IEEE 493-2007, *Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems* was added to Informational Note 2: of Section 700.12 - Emergency Systems. This method is an extension of that revision by providing a specific example to inform design engineers, the Fire Marshall and the Authority Having Jurisdiction (AHJ) that there are specific tools available to provide quantitative results for risk assessments. It is hoped that these methods will become more widely applied and will result in effective capital deployment for building premises life safety and property protection as well as become more widely used in guiding public power security decisions for the so-called "last-mile" of power distribution.

REFERENCES

1. IEEE Standard 493 – 2007, *Recommended Practice for Design of Reliable Industrial and Commercial Power Systems.*
2. "What Five 9's Really Mean and Managing Expectations," by Robert Arno, Peter Gross, PE and Robert Schuerger, PE, IEEE Industry Applications Society Conference 2008
3. Fault Tree Handbook (NUREG-0492), US Nuclear Regulatory Commission, Washington, DC, 1981
4. National Electrical Code (NFPA 70-2011) , National Fire Protection Association, Quincy, MA
5. Standard for the Installation of Stationary Pumps for Fire Protection (NFPA 20-2010) National Fire Protection Association, Quincy, MA

978-1-4673-0651-5/12/$31.00 © 2012 IEEE