MODULAR RELIABILITY MODELING OF THE TJNAF PERSONNEL SAFETY SYSTEM

J. Cinnamon, K. Mahoney, Thomas Jefferson National Accelerator Facility, 12000 Jefferson Avenue, Newport News, VA, 23606

Abstract

A reliability model for the Thomas Jefferson National Accelerator Facility (formerly CEBAF) personnel safety system has been developed. The model, which was implemented using an Excel spreadsheet, allows simulation of all or parts of the system. Modularity of the model's implementation allows rapid "what if" case studies to simulate change in safety system parameters such as redundancy, diversity, and failure rates. Particular emphasis is given to the prediction of failure modes which would result in the failure of both of the redundant safety interlock systems. In addition to the calculation of the predicted reliability of the safety system, the model also calculates availability of the same system. Such calculations allow the user to make tradeoff studies between reliability and availability, and to target resources to improving those parts of the system which would most benefit from redesign or upgrade. The model includes calculated, manufacturer's data, and Jefferson Lab field data. This paper describes the model, methods used, and comparison of calculated to actual data for the Jefferson Lab personnel safety system. Examples are given to illustrate the model's utility and ease of use.

1 BACKGROUND

1.1 Need for Safety Analysis

The Jefferson Lab PSS is responsible for preventing several types of danger to personnel. This system must detect unsafe conditions during the lifetime of the accelerator. An analysis of an accelerator safety system is a necessary requirement in determining if the system meets the original design specifications. If a safety system exceeds the failure rate of its design, changes can be made to improve physical implementation. A reliability study not only allows a system engineer to determine the system's current reliability, but also to identify the "weak links". The expense of unnecessary improvements can also be avoided by having realistic "before and after" data about the effects of any changes.

1.2 Scope of Study

The reliability model of the TJNAF Personnel Safety System (PSS) was developed to predict the safe and unsafe failure rates (λ_s & λ_u), availability, and actual TJNAF in-field failure information for PSS systems. The model uses the industry accepted reliability modeling techniques of the military standard MIL-STD-756B. This information is used to determine the true safety the PSS system.

2 METHOD

The TJNAF PSS system was modeled using Microsoft Excel™ as a platform to calculate reliability. The actual implementation of the study was done using a common-sense approach. Instead of the usual formula-focused method, the PSS was studied using a more graphical approach. The entire PSS system was drawn in block diagram form. Each major block was reduced into its constituents, and the resulting blocks were further reduced to the individual component level.

At this point, a special spreadsheet was built to contain the calculated reliability values for all PSS components. This master sheet was used as a reference source for information on each PSS part. Having a single source of reliability data greatly simplifies the process of developing the study. These values were then referenced whenever needed via pointers to the cell in the master database.

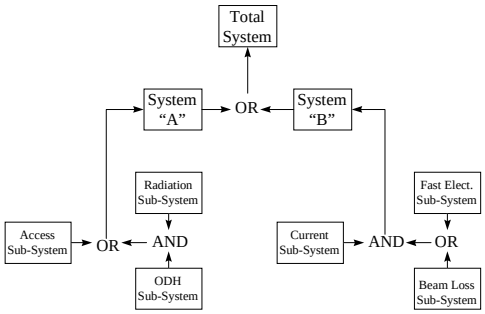
3 DEVELOPMENT

3.1 Preparation

The first step in beginning a reliability analysis is to develop a drawing of the system you wish to model. This drawing should be a schematic showing each major part of the system in block diagram form. The major sections of the system should show any interconnections between sub-systems to provide any information about interdependence. The each block of the system diagram should be separate and discreet from other blocks.

The level of detail at this point is very low. All that is needed is an understanding of what is to be under focus in the reliability study. Often, there are areas of an accelerator safety system which cannot or need not be included in the analysis.

0-7803-4376-X/98/$10.00 © 1998 IEEE



The purpose of the system picture is to logically group components of the system into blocks. These major blocks are used to determine the final system reliability. Each of the major sub-systems under investigation is further broken down into its sub-systems and components.

3.2 Identifying all components of the study

After the sub-system drawings are completed, a list of each unique component should be made. This is a time consuming process, but a necessary one. A single database should be constructed in a spreadsheet program capable of calculating complex formulas. The TJNAF PSS used Microsoft EXCEL™ because of the high availability of the program and ease in use of formulas.

3.3 Gathering information about components

The method for determining the individual component reliability begins by researching the component for information on proven reliability. This is information which the manufacturer has obtained after thorough research and experience. The values are usually dependent on the frequency of use and operating environment. It should be noted that the manufacturer's reliability quotes are often much better than the component's actual field reliability, so field data is also used.

3.4 Calculating Component Reliability Values

If the reliability value for a given component is already known, the numbers can be directly entered into the Master database. If this is not the case, the values must be determined using what information is available.

If the *Failure rate* is available,
Failure Rate (λ) = 1/MTBF in Failures per Hour
Single-Component Reliability = Exp(-λ * time interval)

If the *MTBF* is given,
MTBF = Mean Time Between Failure (in Hours)
Failure Rate (λ) = 1/MTBF in Failures per Hour
Single-Component Reliability = Exp(-λ * time interval)

If the *Minimum Operations* information is given,
Minumum Operations Lifetime = # of ops.
MTBF = (in Hours)
Failure Rate (λ) = 1/MTBF in Failures per Hour
Single-Component Reliability = Exp(-λ * time interval)

3.5 Inclusion of Values in Database

Once the individual component reliability is determined, the value is entered into the Master database. The MTBF values may be calculated and entered for use in *Availability* determination. A column containing the actual in-field MTBF values for a component is kept for reference. A value for the Mean Time to Repair is entered into the MTTR column. This represents the time needed to replace or repair the component in the field. The time interval of the study is also an important factor in determining reliability. This value should be the time between system re-certifications, usually 6 months or 1 year.

4 ARRANGING COMPONENTS TO SIMULATE SYSTEM

The components are arranged in a spreadsheet model according to their pattern of usage in the actual system. This technique for reliability modeling allows the system under study to be easily examined for current reliability, and later dynamically improved as new components are put into service. In addition, the use of component "pointers" instead of numbers in the sub-system modeling make updates easier.

4.1 Previous Methods of Analysis

The more common approach to modeling an area is to write out a formula such as the one below. This shows the reliability as equal to the product of the reliability values of each of its constituents.

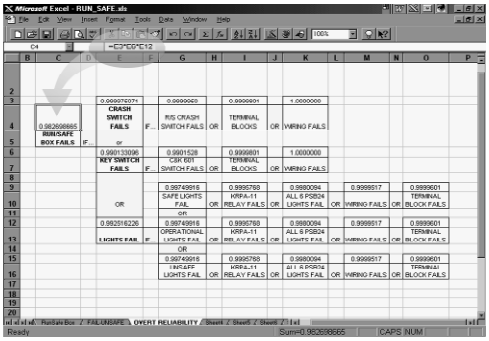
$$R_{system}=((R_{unit\ 1}) \text{ OR } (R_{unit\ 2}) \text{ AND} \ldots (R_{unit\ n}))$$

4.2 TJNAF Method

The method used in the TJNAF reliability analysis involved the use of spreadsheet blocks to produce a more visual and easily modified picture of a system. The formulas are the same, but in a more graphical arrangement. This use of spreadsheet cells provides unique advantages when calculating large systems.

When information about a part is entered into the master database, often only certain information is needed to calculate reliability. The rest of the information may clutter the view of the important material. Pointers were used to reference the master database reliability values wthout displaying every piece of information about the part.

Spreadsheets of several systems can be opened together and interlinked using "drag and drop" pointers. These pointers consist only of the cell location of the information needed.



4.3 Linking sub-systems

When the reliability of a single component or individual system is determined, the process of interconnecting with other systems begins. The larger system groups are formed by linking the reliability values from individual system sheets to a single sheet. The values are arranged as they exist in-field and a single value for the larger system is produced. As more and more systems are unified, the reliability of the complete system is approached.

The key benefit of using a modular model in a spreadsheet is having the ability to quickly change things. As the size of a study expands, the need for an easier and less time consuming approach expands exponentially.

SUMMARY

The methods used be the TJNAF Safety System Personnel involved in the study have proved to be valuable and worth mention to other accelerator safety groups. The modularity affords a great deal of flexibility in generating scenarios of system revision and investment. This study has allowed our engineers to determine the cost-to-improvement ratio for upgrades on the TJNAF system. This has provided the Safety group with the data needed to save countless dollars on unnecesary “improvements”, and permitted the components truly needing attention to be seen.

FUTURE

Sometime in the future, the analysis of the study will be expanded to include a Markov Analysis. This will be instrumental in providing more realistic information about safety and availability issues.

REFERENCES

[1] MIL-217F Standards Document

[2] MIL-756B Standards Document

[3] U.K. Department of Health and Social Serices. Functional safety of programmable electronic system: generic aspects. London: DHSS; 1987.

[4] Petschenik, N.H. Practical priorities in system testing. IEEE Software 2(5):18-23; 1985.

[5] Simmons, J.M. Safety shutdown systems. *Advances in Instrum.* 42(1): 115-122; 1987