Reliability and Maintainability for Fire Protection Systems

HOWARD D. BOYD
Fire Protection, USA

CHARLES A. LOCURTO
Safety, R & M, and Quality Engineering, USA

ABSTRACT

Reliability and Maintainability (R&M) issues are discussed which pertain to Fire Protection (FP) systems. Although R&M technology has been developed primarily for military and electronic systems, the philosophies and methodologies are applicable to the field of Fire Protection. To illustrate this, the reliability of a representative system for a high rise building is analyzed. Chance of failure and MTBF (Mean Time Between Failure) indices are calculated for a sub-set of equipment which delivers electrical power to a pump automatically. The system power depends upon redundant Diesel Generators (DG's) which back-up the electric Utility Line. Actual failure data is derived for each equipment. The results raise concern over the appreciable chance of failure of such systems. The case where only one back-up DG is used (typically) represents a condition which is worse. Several Maintainability concepts are presented. These include specification design requirements, fault detection, isolation, built-in test, automatic test equipment, and schemes utilizing Computer Management Systems for periodic exercise and monitoring of FP equipment. Overviews of several adaptable contemporary R&M programs are provided. These include the treatment of purely mechanical equipment. The authors highly recommend incorporation of modern R&M technology into the Science of Fire Safety. This should reduce the present lag in R&M applications for FP systems.

INTRODUCTION

There is a significant lag in the application of R&M technology to the field of Fire Protection compared to fields such as military weapon systems. The original impetus for development of R&M programs was spurred by Congress in the 1940's to improve the faltering availability of American weapon systems during, and after World War II. R&M programs developed in the last 40 years deal primarily with military systems and their associated electrical and electronic equipment. However, the philosophies and methodologies developed in these programs have been applied to sundry other fields of endeavor. Amongst these, to name but a few, are the nuclear power industry, commercial aircraft, automobiles, and household equipment. We take the view, as others have done, that these R&M methodologies are also applicable to FP systems. There is a paucity of data on FP peculiar hardware compared to highly developed failure rate data and specifications for electronic components. Nevertheless, in our judgment there is sufficient data and information to support the full application of modern R&M methodologies to the field of FP and its associated systems.

To illustrate this, we have chosen to discuss R&M issues which pertain to the FP system of a high rise building. It is beyond the scope of this paper to present a full discussion of the many R&M methods and procedures which can apply. There is not sufficient room allocated here to analyze an existing high rise building. However, our main purpose is to discuss enough R&M issues to enhance the use of this technology in FP systems. Accordingly we have limited the scope of this paper to a discussion of some of the cogent R&M issues. For ease of presentation we have employed a simplified FP system which is representative and which does not necessarily include all the equipment hardware found in a specific, existing high rise building.

The discussion is divided into three parts. First the Reliability issues are presented; second the Maintainability issues, and the third part presents an overview of R&M program elements which can be adapted to FP systems.

RELIABILITY

Figure 1 relates to a representative or notional FP system for a high rise building. It includes some of the more important equipment existing in real cases. The basic features include a single electric water pump backed up by redundant Diesel Generators, an automatic controller with manual override, transfer switching, redundant standpipes, and other features typically found in a simple system.
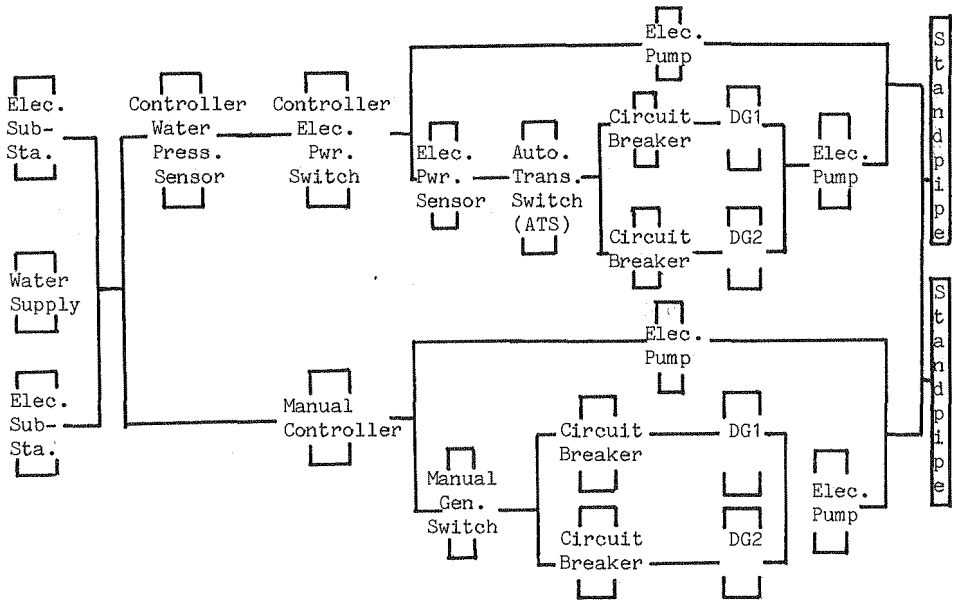

FIGURE 1. National Fire Protection System for a High Rise Building.

It should be noted that Figure 1 is a reliability block diagram. Accordingly, it shows which equipment must operate (i.e., in series), and those equipments which may work as either one or the other, to perform the required function (i.e., in parallel). This approach helps to visualize the concepts of single failure points, and the idea of redundancy. A single failure point exists in any mode of operation wherein a failure of a specific unit of hardware

will completely fail the total protection system. The following summaries present several reliability issues pertaining to the system represented in Figure 1.

● In the fully automatic mode of operation, before there is time for the arrival of the Fire Department with auxiliary water (pumped in through siamese or "Y" connections) there are four single failure points. One is the water supply, and others are the controller water pressure sensor, the controller electrical power switch and the electric pump. These must operate for the system to be successful.

● There are three single failure points in the manual override mode of operation. These are the water supply, the manual controller switch and the pump.

● It is obvious that single failure points are the weak links. One has to assess the risk of allowing them to dominate the reliability of the system. The recommended practice is to design them out of the system by using redundant, or stand-by techniques.

● This system includes a redundant standpipe architecture. It is desirable because if one fails the other may work. However, reliance on redundancy must always be wary of equipment susceptability to failure modes whose physics of failure are such that the redundancy does not really exist. In other words, both units may fail because of equal susceptability to aging, cracks (particularly in cast iron), freeze-ups and rust. Experience tells us, for example, that one of the overall weakest reliability characteristics of the system in Figure 1 could be the pipe water distribution system, in spite of redundancy.

● One of the difficulties associated with analyses of Fire Protection Systems is the lack of historical failure data on hardware equipments which comprise the system. However, some progress can be achieved. To illustrate this, let us consider a limited portion of the hardware elements in Figure 1. We limit our investigation to a portion which supplies electric power to the pump automatically. Also to make it easier we will modify the system arrangement and use an elementary fault tree type of illustration of the logic involved. Accordingly this subsystem fails to supply electrical power, as shown in Figure 2.

● The sources of the failure data for each equipment in Figure 2 are as follows:

DIESEL GENERATOR: Fails while running. The failure rate, $\lambda = 6 \times 10^{-4}$/HR. (Reference 1, P. 1211). The λ is for emergency standby DG's. This data was gathered by IEEE team visits to nine operating nuclear power plants. The failure rate data are also substantiated by the report Diesel Generator Reliability at Nuclear Power Plants, Data and Preliminary Analysis. Electrical Power Research Institute, EPRI NP-2433, Interim Report, June 1982.

CIRCUIT BREAKER: Fails open. $\lambda = 0.14 \times 10^{-6}$/HR. (MTBF = 815 years) (Reference 2). The failure data is obtained from the MIL handbook equipment failure summaries for typical electrical circuit breakers.

AUTOMATIC TRANSFER SWITCH (ATS): Fails to transfer to Utility line. $\lambda = 0.14 \times 10^{-6}$/HR. (Reference 1, p. 120). The data are for indoor ac circuit breakers for all modes of failure. This is a conservative estimate for ATS switch failure (the data is not readily available).

```
                    ┌─────────────┐
                    │   Lack of   │
                    │ Electrical  │
                    │    Power    │
                    │   to Pump   │
                    └─────────────┘
```

MTBF = 1.5 Months

```
        ┌─────────┐                          ┌─────┐    ┌──────┐
        │   DG    │                          │ ATS │    │ Line │
        │ System  │                          └─────┘    └──────┘
        │  Fails  │
        └─────────┘                        Fails to     Utility Line
                                           Transfer     not avail-
     MTBF = 1.2 months                     to Utility      able
                                              Line
   ┌────────┐        ┌────────┐         λ= 0.14 x     λ= 1.71 x
   │  DG1   │        │  DG2   │             10⁻⁶/R        10⁻³/HR
   │ Fails  │        │ Fails  │
   └────────┘        └────────┘              (C)           (D)
```

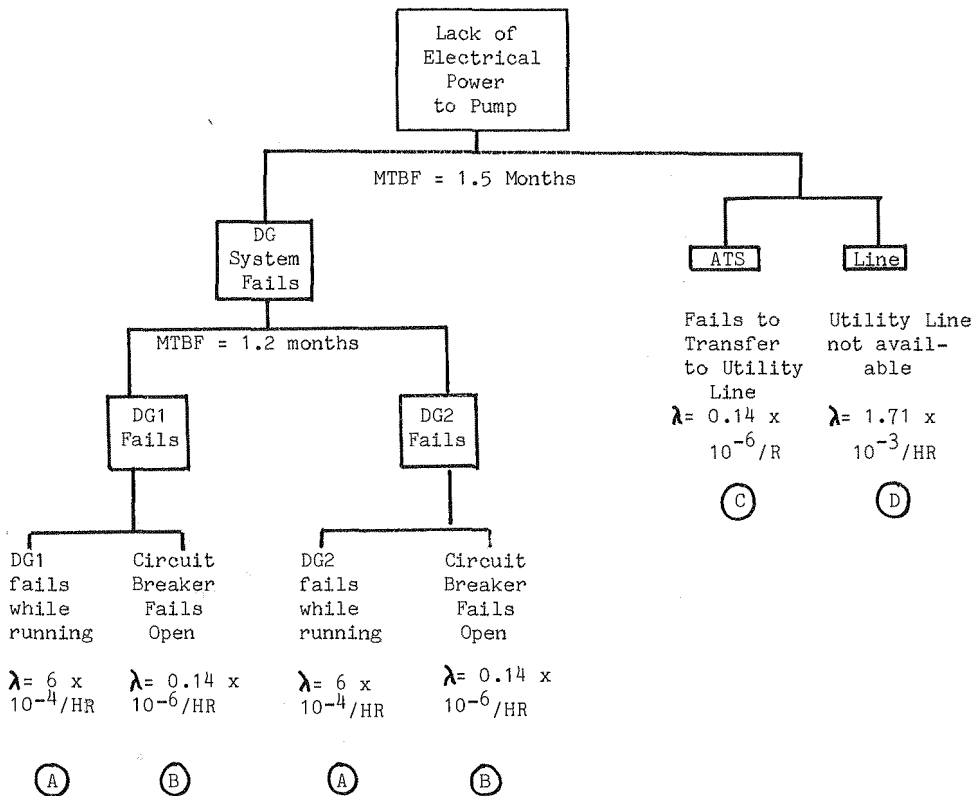| DG1 fails while running	Circuit Breaker Fails Open	DG2 fails while running	Circuit Breaker Fails Open
$\lambda = 6 \times 10^{-4}$/HR	$\lambda = 0.14 \times 10^{-6}$/HR	$\lambda = 6 \times 10^{-4}$/HR	$\lambda = 0.14 \times 10^{-6}$/HR
(A)	(B)	(A)	(B)

FIGURE 2. Elementary Fault Tree for Power Interruption to Pump.

UTILITY LINE NOT AVAILABLE: Failure is either unacceptable interruption
or lack of power when needed. (From reference 3 the MRBF = 200 HRS.
Utility interruption = 43.8/year. From reference 4 Utility power inter-
ruption = 0.6/month. MRBF = 1200 HRS. Utility interruption = 7.3/year.)
After reviewing these data with persons who have some experience with
power interruptions we settled on an estimate of 15 Utility interruptions
per year, or $\lambda = 1.71 \times 10^{-3}$/HR.

• From Probability Theory[1] the failure rate of the redundant generator sub-
  system is:

  $\lambda_{DG1} + \lambda_{DG2} = 2 (6 \times 10^{-4}) = 12 \times 10^{-4}$/HR. The MRBF = 1.2 months.

• The reliability (R_s) and chance of failure of the system in Figure 2, in a
  one-month period, are determined as follows:
  From Probability Theory:

  $$R_s = R_A^2 R_B^2 + R_C R_D - R_A^2 R_B^2 R_C R_D \qquad (1)$$

_____
[1]See also MIL-STD-756B Reliability Modeling and Prediction.

by substitution:

$$R_S = (.64920)^2 (.99993)^2 + (.9993)(.29194) - (.42146)(.99979)^3 (.29194)$$

$$R_S = 0.59032 = 59\%$$

The chance of failure in one month = 41%

● The Mean Time Between Failure for the above is obtained by integration of the time (t) dependent equation 1, determined as follows:

$$MTBF = \int_0^\infty R_S(t)\, dt \tag{2}$$

By integration:

$$MTBF = \frac{1}{2\lambda_A + 2\lambda_B} + \frac{1}{\lambda_C + \lambda_D} - \frac{1}{2\lambda_A + 2\lambda_B + \lambda_C + \lambda_D} \tag{3}$$

By substitution:

$$MTBF = \frac{1}{.0012} + \frac{1}{.00171} + \frac{1}{.00291}$$

MTBF: 1074.5 HRS.

MTBF: 1074.5/720 = 1.5 months

● The analysis outlined above is not intended to be exhaustive. It is intended to illustrate the value of utilizing this type of methodology. Caution is advised when applying these limited results because a number of enhancing and detracting factors should also be considered. Some of these are as follows:

  - only random, independent failures are considered.
  - failure rates are assumed to be constant; i.e. no aging of equipment was considered.
  - uncertainty of derived failure rates exists.
  - major components have not been analyzed in detail.
  - probable faults in the electrical substations should also be considered.
  - Many Fire Codes in the United States require emergency power for Life Safety-related subsystems such as smoke control and sprinkler systems. Unfortunately in many existing buildings these systems are rife with single failure points resulting from using the same wiring throughout the system. The analysis should be extended to include Life Safety subsystems.

● The foregoing numerical results are not fully complete because of the assumptions and limitations outlined above. Nonetheless, the results of this simple analysis cannot be dismissed from the truth. Therefore, the managers of real fire protection systems which depend on electrical back-up generators, especially those cases which depend on a single back-up generator, would be well advised to review the reliability of their FP system. The chance of failure is appreciable, with a low MTBF.

● There are many other reliability analytical and management procedures which can and should be applied in a typical FP system for a high rise building. However, the foregoing may be enough to illustrate the plausibility of such

analyses, and the ability to develop rational issues in spite of the lack of sophisticated data.

MAINTAINABILITY

Maintainability plays an important role in the long term average failure rate of any real Fire Protection System. Experience has shown that with thorough viligance for maintenance, the long term reliability and the availability of the system is improved. The following presents issues which arise on this subject:

● It has been shown mathematically (reference 5), that the force of mortality (system failure characteristic) is diminished by the practice of ideal maintenance philosophies. This means that a FP system which is poorly maintained and exercised will have a higher long term average failure rate than has the same system when it is maintained with a dedicated program, and exercised periodically.

● Exercises such as those where the Fire Department comes to measure pump output pressure periodically are fundamental to good maintainability.

● Maintainability parameters can be used in design. The probability of detection of a failure, the probability of isolation (failures in one unit of a redundant system, for example, are difficult to isolate) and the probability of restoration (involves difficulty and time required to restore a downed system to full operational status) are each predictable, specifiable, and measurable hardware design parameters.

● Detections of failure are enhanced not only by periodic visual inspections, but also by the efficacy of built-in-test (BIT) and automatic test equipment (ATE). Important detection parameters to be monitored in high rise building applications are water column pressure, electrical power in, pump starting characteristics, and the maintenance of critical system water pressure. Some advanced cases exist which utilize computer systems with programs so arranged that they can automatically exercise every generator and also measure the protection system parameters. Automatic exercise periods are typically one-half hour each week. (Refer, for example, to the Honeywell Computer Management System, Delta Program 1000).

● As always, nature is a jealous mistress. The return on investment in sophisticated BIT and ATE schemes is limited by the effectiveness of the BIT equipment itself. The BIT equipment will require outstanding reliability characteristics which are at least an order of magnitude better than the FP system hardware which it monitors.

● Again, much progress has been made in maintainability design for military weapon system development. This technology can be directly tailored for use in FP fault detection and isolation design. We have covered only a smattering of the available concepts here.

R & M PROGRAM ELEMENTS

The following presents an overview of several R&M programs and practices which exist in other fields, and which should be adapted to FP systems.

968

- The program elements included in such highly developed procedures as <u>Reliability Program for Systems and Equipment Development and Production</u> MIL-STD-785B, and <u>Maintainability Program Requirements</u> MIL-STD-470 are directly applicable.

- A military publication called: <u>Application of Reliability-Centered Maintenance to Naval Aircraft, Weapon Systems and Support Equipment</u> MIL-HDBK-266 (AS) deals with an advanced concept in maintenance. Its detailed procedures assist in determination of the significant items to be maintained, the method of partitioning the system to a workable level, the method for evaluation of failure consequences and methods for how to schedule maintenance tasks. Although this is slanted towards Naval equipment the genre of hardware is much the same as it is for commercial Fire Safety systems.

- Typical R&M program plans include techniques which would be useful in research, development, and test and evaluation phases of FP system design. Two special techniques will be mentioned here:

    One is a <u>Reliability Allocation, Analysis and Assessment (RAAA)</u> study. This consists of an initial and periodic analytical assessment which compares reliability estimates with measurement of critical components as part of the technical evaluation phase of a given program. Included are numerical apportionment of requirements in hardware procurement specifications, assessment of designs by stress analysis, and measurement of the impact of systematic improvements of failure and suspected failure mechanisms through specific corrective actions. A proposed military standard entitled <u>Procedures for Performing a Reliability Stress Analysis of Mechanical Equipment</u> is close to publication. Preliminary copies are available.

    Another analytical technique is known as a <u>Maintainability Allocation, Analysis and Assessment (MAAA)</u> study. This consists of an initial and periodic assessment which compares maintainability estimates with measurement and achievement, as a part of the program technical evaluation of progress. Included are numerical apportionments of maintainability requirements, such as allowable detection and isolation characteristics, assessment of built-in-test effectiveness by progressive measurements, optimization of inspection periods, evaluation of ease of maintenance, and progressive analysis of design parameters.

- Some additional techniques which are available as part of a well-determined R&M Program are listed, briefly, below. The scope of this paper does not allow a discussion of each at this time:

    - Failure Modes and Effects Criticality Analysis
    - Electrical and Mechanical Reliability Stress Analysis
    - Quality Assurance (much work is being done on assurance of quality and reliability. The technical literature is available). This should be particularly important for inclusion in specifications and contract requirements for the acquisition and procurement of critical FP hardware.

- <u>Design Guidelines for Prevention and Control of Avionic Corrosion</u> NAVMAT P 4855-2, June 1983. Department of the Navy. Although this guide addresses the general subject of avionic equipment, it also presents many highly developed concepts which are directly applicable to mechanical as well as electrical equipment. This guide is intended to direct the designer's attention to the use of techniques and methods which will eliminate, prevent and reduce corrosion. It is not the last work on corrosion prevention, but

rather a document which can direct the attention of a FP system designer to a complex problem.

● There are many other valuable R&M program elements and military standards and handbooks, which could be adapted to the design and evaluation of FP systems. We could only touch upon a few at this time.

CONCLUSION

The discussion presented in this paper is intended to engender interest in the efficacy of applying existing R&M technology to the design and evaluation of Fire Protection systems. Initial development of military R&M methodologies has become the cornerstone for design of tailored R&M programs for many commercial and military scientific applications. Accordingly, we highly recommend the foregoing concepts, and others available in the R&M technical literature, for full incorporation into the Science of Fire Safety. This will help to reduce the lag in application of this technology to the design and development of Fire Protection systems such as those for high rise buildings.

REFERENCES

1. IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Stations. IEEE Std. 500-1984.

2. Reliability Prediction of Electronic Equipment, MIL-HDBK-271D, 15 January 1982, Rome Air Development Center, Griffiss Air Force Base, New York.

3. Locurto, C. A. and several application engineers (represents an extreme case opinion of Utility Line failure rate). Unpublished paper.

4. Kesterson, A. and Maker, P. Computer Power-Problems and Solutions. EC&M, December 1982, p. 67.

5. Pieruschka, E. Principles of Reliability. Prentice-Hall, Inc., 1963.