(Goldman and Slattery, 1964, p. 27). Routine maintenance is a basic strategy that accompanies operation. It keeps at least the easily serviceable parts of machinery and structures in good repair and maintains a clean and healthy operating environment. All moving parts are kept well greased and free of condensation, dust, and rust. Routine maintenance is performed without interrupting the operation of the system. From a probabilistic point of view, routine maintenance is a *hazard control* activity. It has the potential to discover minor irregularities and incipient flaws that, overlooked or unattended, might develop into major failure. For example, an oil or cooling water pump failure can lead to turbine or generator bearing failure that takes the production unit off-line, thus causing thousands or millions of dollars in damage and repair cost. Although there is nothing obviously probabilistic about it, routine maintenance plays a significant role in the generally probabilistic system operation environment by its contribution to *reliability* and *longevity* of systems and equipment.

Corrective maintenance is performed in response to failure. This type of maintenance may be justified when damage associated with failure is minor or if no serious consequences are associated with failure. The damage is corrected after it occurs without a possibly unjustified interference with the running system.

Preventive maintenance is performed in anticipation of failure or after deterioration of equipment has been detected. Preventive maintenance may be mandatory when system failure is associated with serious consequences for the continued operation of the system or because of serious or unacceptable consequences for the public, public and private property, and the environment. Thus, both corrective maintenance and preventive maintenance are legitimate approaches under proper circumstances. The criteria for selecting one or the other are essentially the costs and consequences of failure.

The most desirable approach is *maintenance on demand*. Suppose a system's normal performance signature is known and continuously monitored. If departures beyond a normal band of deviations occur, alarms are triggered that alert operators of the need for inspection or immediate maintenance action. But also this kind of maintenance has probabilistic aspects as it raises the problem of false or failed alarms, which may trigger premature maintenance or miss the opportunity for preventive maintenance. No type of maintenance can eliminate all probability of failure because of the probabilistic character of systems. Other maintenance-related activities include rehabilitation, replacement, retirement, and removal. Although these aspects will not be specifically discussed, they all include engineering work with probabilistic aspects that is addressed here under *maintenance*.

5.2 Maintenance Management

A probabilistic approach to maintenance considers the system to be maintained as an assembly of components that exhibit random behavior with respect

to being operational or not. In developing a maintenance approach to such a system, the following steps need to be considered (LaPay, 1992):

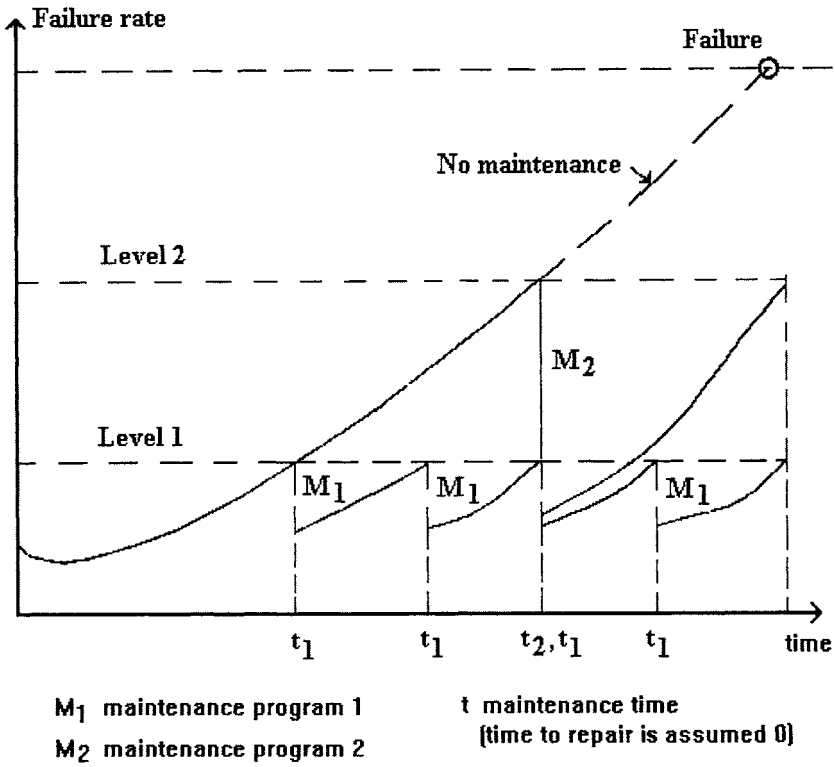

Figure 5-1: Maintenance applied periodically brings the failure rate down to or below an acceptable level. The indices identify two maintenance programs that differ by the time maintenance is applied and by the failure rate incurred (after LaPay, 1990).

(a) Identify systems, structures, and components: There should be a clear understanding of the scope of equipment and structures to be addressed by the maintenance program. Areas of commonality should be identified so that the scope and cost of the program can be minimized.

(b) Understand system operational characteristics: It is important to understand the total system operational behavior and the interrelationships between

components; identify redundant paths that allow shutdown of equipment without loss of service.

(c) Identify failure mode characteristics: Failure modes typical to the system must be identified. Examples are seepage and erosion in embankment dams; overtopping of embankments; sliding of embankments, foundation seepage and pressurization of rock foundations; deformation of concrete dams by concrete swelling or foundation movements; tunnel, pipeline, and penstock leakage; valley slope creep and slides; settling of embankment dams and associated rupturing of the core; jamming of gates by concrete swelling, failure of gate operation device; failure of emergency gates; structural failure of gates; penstock corrosion; trashrack collapse; turbine runner failure, generator insulation and bearing failure; operation errors, external events, and so on.

(d) Understand aging and deterioration behavior: Generic and project specific data should be obtained.

(e) Understand basis of design : Strength inherent in the design should be identified and quantified.

(f) Understand environment and loadings of system and components: Data on the environment and loading conditions to which the equipment and structure are subjected should be collected. Historic records should be consulted and the exceedance probability for critical natural events (high winds, floods, snow, ice, earthquakes) should be prepared.

(g) Understand existing maintenance procedures: The current maintenance process should be reviewed and existing maintenance procedures should be incorporated into the evaluation process. The need for new procedures or the modification of existing procedures can then be identified.

The evaluation of these steps forms the basis for the selection of a maintenance program. The maintenance budget can be estimated and the extent and frequency of the most effective maintenance activities can be determined. An indicator of the need for maintenance is the increase of failure rates or other symptoms beyond an acceptable level. Figure 5-1 illustrates the increase of failure rate with time. If failure rates are not known or failures are acceptable, other measurable indicators must be defined and monitored instead. Such an indicator is the stress state in a component. When a safe level of stress is exceeded, maintenance, repair, or rehabilitation are explored as possible methods to correct the problem. Figure 5-1 also illustrates the use of two maintenance programs, one program with short maintenance intervals and another with longer intervals. The level of reduced stress state achieved by the two programs is not necessarily the same. A criterion for judging the two programs could be the expected remaining life of the component that results from the two maintenance programs.

5.3 Reliability-Centered Maintenance (RCM)

Reliability ranks high among maintenance objectives. This was brought out in the responses to survey questions (Section 1.6.2, Question 8). Other objectives are ensuring the safety of process operations, minimizing cost, completing the work on time, and meeting external requirements. Different emphasis on these objectives could lead to various "centered" maintenance approaches, such as *safety-centered maintenance*, *economy-centered maintenance*, or *reliability-centered* maintenance (RCM). Reliability-centered maintenance gives the highest priority to service reliability, which implicitly requires reliability of all contributing system components (e.g., structures and equipment), competent management, and expertise of O&R personnel. Prioritizing reliability could also mean compromising safety by skipping a preventive shutdown to avoid service disruption; or it could mean *overmaintaining*, thereby causing a higher than necessary cost as a consequence of unnecessary shutdowns, and premature replacement of operable components. It could also mean rushing repairs to minimize downtime at the expense of repair quality. If one objective is given the highest priority in a maintenance program, others must still be included as secondary objectives or constraints that put limits on trade-offs in favor of the *central* objective. Economy-centered maintenance could mean maintenance at minimum cost, or minimizing the cost of overall O&M. Also, safeguards would be required to prevent such an approach from becoming overly *centered* on economy, for example, by taking risks in stretching maintenance intervals, and by taking shortcuts on safety and reliability measures, to minimize maintenance cost and loss of service costs accruing from a shut down production process. *Safety-centered maintenance* could mean sacrificing service reliability and economy by frequent and extended downtime to avoid unexpected breakdown. For industries in which safety is of overriding concern, such as the nuclear industry, a safety focus should be mandatory. In the hydro industry, mandatory provisions require meeting minimum maintenance requirements that address the various objectives mentioned here. Such mandatory requirements are usually imposed on the industry as the consequence of damages and losses caused by the neglect of safety objectives or constraints in favor of other objectives (see Section 1.5.1).

LaPay (1992) states that "reliability-centered maintenance philosophy requires that resources be concentrated on those components which are critical to plant operation and safety. The prioritization process is based upon the impact of the equipment on plant availability, plant safety, economic, and other plant specific factors." It is a basic premise of multiobjective optimization that compromises among objectives are necessary in order to arrive at a feasible solution. This kind of optimality that restricts the optimum seeking procedure by side objectives and constraints of an administrative, political, environmental or other nature in favor of tradeoffs among objectives is known as *Pareto optimality*. To make a difference with

respect to *general* maintenance, RCM must maximize reliability, while serving all other objectives at or within agreed upon limits.

A plant maintenance program under the RCM label must address the following aspects (LaPay, 1992):

(a) Critical component identification: A prioritized list of critical components and documentation of these components is prepared that must be included in the program. Critical components are those that must function for the process to function.

(b) Requirements, definitions, and documentation for each critical component For each identified component, the following information items are prepared and made part of a readily accessible database:

- related industry codes and standards
- regulatory requirements
- technical specifications
- vendor documentation
- vendor recommendations for inspection and maintenance
- vendor warranty (life expectancy)

(c) Component performance definition: The component's function, possible failure modes, root causes (trigger events), and impacts of subcomponent failure are documented. This information is used to identify key equipment problems to be addressed by maintenance.

(d) Maintenance activity selection: Equipment requirements and performance needs, including historical performance are evaluated. Any new techniques, such as diagnostic and monitoring techniques, that support more effective performance should be evaluated.

(e) Activity breakdown into tasks: Every activity is broken down into tasks, and tasks are broken down into steps. Related procedures may emerge.

(f) Detailed task definition: The major steps of each maintenance task must be described with detailed step-by-step instructions, including lists of spare parts, tools, and other necessary resources. These task descriptions form the basis for the plant maintenance procedures and training programs.

(g) Procedure development: The task descriptions are incorporated into preventive maintenance procedures, but are also applicable to corrective maintenance. Also, the human factor is addressed, which provides maintenance personnel with documentation for their activities by on-site (by desktop and notebook) computer displays.

The functional performance designed into equipment must be understood and combined with all external requirements imposed on the equipment to provide an effective and justifiable maintenance program.

5.4 Maintenance Times

5.4.1 Corrective Maintenance Time

Corrective maintenance, also called *breakdown maintenance*, is initiated by a breakdown event. The elapsed time from breakdown to when maintenance ends is a probabilistic quantity, because many events surrounding the maintenance activity contribute to the length of the outage. All maintenance policy can do is to reduce the uncertainty inherent in maintenance work without being able to completely eliminate uncertainty in all aspects. Hence, maintenance time is a stochastic variable and the occurrence of maintenance time over a period of time, such as the life of the component, has the characteristics of a stochastic process. A process that alternates between operation and shutdown periods is also called a *renewal process* or a *birth–death process*, with the startup of the operation being construed a birth or renewal, and the shutdown being a failure or death. The literature on such processes provides examples of the analytical treatment of such processes with applications to maintenance (Parzen, 1965; Ross, 1992).

The life span of a system or a component consists of periods during which it is operating and periods when it is shut down. The time from the start-up of an operation to a shutdown or unexpected breakdown, and on to a new start-up, is the *cycle time*. The cycle time consists of two periods, operation time and downtime. *Operation time* begins with start-up and terminates with failure. It is also called *time to failure TTF*. *Downtime* is the time the system or equipment is down for repair. It is also called *time to repair TTR*. Downtime begins with failure and ends with completed repair. Cycle time is also called *time between failures TBF*:

$$TBF = TTF + TTR \tag{5.4-1}$$

where *TTF* and *TTR* are observed random realizations. The operation cycle is illustrated in Figure 5-2. Each cycle marks a period of random length, *TBF*, that is the sum of two random variables.

5.4.2 Preventive Maintenance Time

Preventive maintenance interferes with the occurrence of random failures by replacing the random variable *time to failure* by a scheduled *time to maintenance*, *TTM*, which is followed by the *preventive maintenance time*, *PMT*, the scheduled

downtime. Thus, the duration of the preventive maintenance cycle, the *time between maintenance*, *TBM*, is

$$TBM = TTM + PMT. \tag{5.4-2}$$

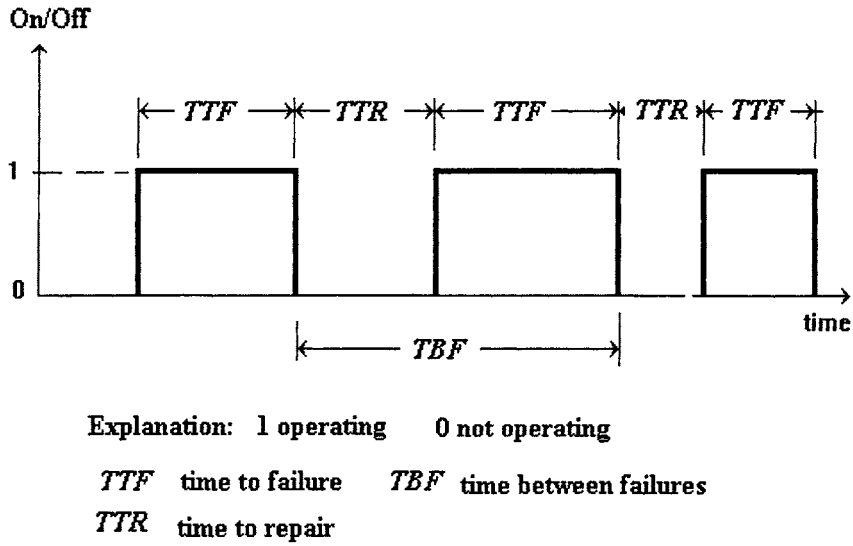

Figure 5-2: Corrective maintenance is initiated by a random failure. The ensuing time to repair *TTR* is composed of many time contributions by work that is performed under uncertainty, which makes *TTR* a random variable. With the process start-up at the end of the repair period begins the next time to failure, *TTF*, that again ends with a random failure. The time between failures, or cycle time, *TBF*, is the sum of two random variables and therefore also a random variable.

Since failures cannot be eliminated completely, a series of scheduled maintenance cycles may be disrupted by an unexpected shutdown, a random failure, followed by a random *TTR*, as illustrated in Figure 5-3. A perfectly successful preventive maintenance program would eliminate all random *TBF*'s and replace them by an uninterrupted series of *TBM*'s. However, even if the safety issue is central,

achieving a reduction of the probability of failure to zero may be prohibitively expensive or technically simply impossible. Some components of hydrosystems, such as large dams, qualify for safety-centered maintenance, and special maintenance approaches have been instituted for them (Section 1.3.4). The primary goal in these cases must be to minimize the probability of unexpected failure, subject to few, if any, secondary objectives and constraints.

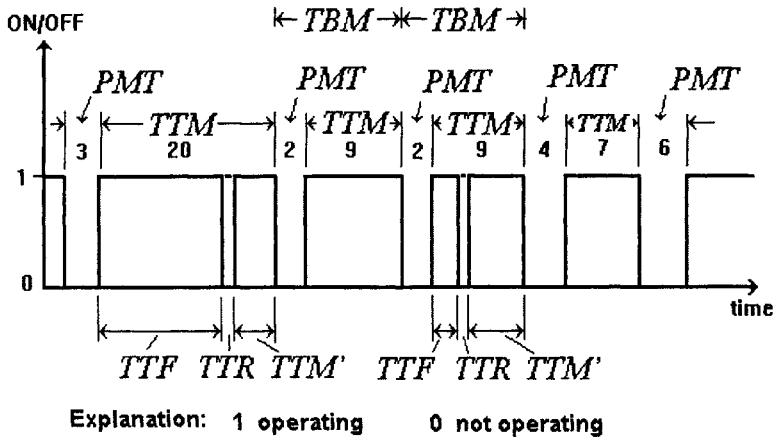

Figure 5-3 : For preventive maintenance, the time between two successive maintenance periods is the time between maintenance, *TBM*, or cycle time. It is the sum of the time to maintenance,*TTM*, and preventive maintenance time, *PMT*. Unexpected breakdowns during *TTM* are possible, but their duration should be short and their probability should be small.

In preventive maintenance, *TTM* is a scheduled time, whereas *PMT* is still subject to random fluctuations, as not all its time components can be accurately predicted. Generally, *PMT* is much smaller than *TTM* and the fluctuations of *PMT*

can be absorbed in *TTM*, so that *TBM* can be part of a fixed maintenance schedule. From time to time, the scheduled *TBM*'s are disrupted by an unexpected shutdown. Then the *TBM* cycle has to be reset in some suitable way. All a preventive maintenance policy can accomplish is to reduce the frequency and size of failures, in other words, it can lengthen *TTF*, and reduce the size and variability of *PMT*. Thus, the frequency and size of the disruptions of the production process are reduced.

Example: Suppose the preventive safety-centered maintenance schedule of a structure is scheduled on an annual basis beginning with *PMT* = 10 days followed by *TTM* = 172 days. This cycle is followed by a second *PMT* = 10 days and a *TTM* = 173 days. Then the annual cycle starts all over again. If *PMT* has a standard deviation of 0.5 days, and is normally distributed around a mean of 10 days, there is a probability of 95 % that *PMT* will not exceed 11days (see Section 2.6.3). This day in exceess of the scheduled *PMT* is absorbed by the *TTM* period and the maintenance schedule remains fixed.

5.4.3 Downtime

The time between shutdown and start-up is the *time to repair*, *TTR*. This time is not the same as *repair time*. The repair time is just one component of the time to repair. Therefore, the total time from shutdown to start-up is also called *downtime* to avoid confusion. The various downtime components are to some extent project-dependent. Their names differ from source to source. Listings from two sources are given in Table 5-1. The activities associated with the time components are similar for corrective and preventive downtimes, but their length and variability can be significantly different.

The Navord time set is used in the time plan of Figure 5-4. The layout of a repair time plan shows analogy to serial and parallel systems (Chapter 4), as well as networks. A network consists of nodes connected by branches. In activity planning, a node represents an event, and a branch represents an activity. Passage through the event-activity network can only be in the direction of time, from a completed activity marked by an event or node to a subsequent activity marked by a branch emanating from the preceding node. Networks that simulate activity schedules are directed networks with restrictions on movements from a completed event to the next event. There is a critical sequence of activities with each depending on completion of a preceding activity and a resulting critical time which indicates the minimum time the completion of all sequential activities requires. Usually there are also parallel activities that can be carried out simultaneously, but they must all be completed before the next activity based on their completion can begin. Waiting times may result in parallel branches of the network. For example, obtainment of spare parts

can begin as soon as the fault has been identified, but the spare parts must be available before replacement can begin, as illustrated in Figure 5-4. Since the minimum time excluding all waiting times is a stack of random variables representing the many individual activity times, it is likely to have a normal distribution (see Section 3.4.2).

Table 5-1: Terminology of Maintenance Time Components
(after Navord, p. 2.3, 1970; and Goldman and Slattery, p. 27, 1964)

Navord (1970)	Goldman and Slattery (1964, p. 27)
Fault identification time	Reaction time (delay time)
Team assembly time	Administrative time
Tool and equipment assembly time	Preparation time
Fault localization time	Fault location time
Gaining access time	Item procurement time
Spare part obtainment time	Supply time
Repair or replacement time	Fault correction time
Alignment and adjustment time	Adjustment and calibration time
Reassembling time	Final test time
Testing time	

The sum of fault location time and team assembly time is the *delay time*. In corrective maintenance, this time represents the *surprise effect* of the unexpected breakdown. In preventive maintenance, the delay time does not exist, because prior planning clears the way for an immediate start of the *active repair time*. This time consists of all time components that deal with repair in contrast to waiting for some activity to be completed. Preventive maintenance also may not require tool and equipment assembly time or spare part obtainment time after shutdown occurs. These activities can be completed in anticipation of the shutdown. Thus, preventive maintenance may shorten downtime considerably compared with corrective maintenance because of elimination of the surprise effect and by using preparatory parallel activities that would otherwise have to be serial activities commenced after shutdown. This means that time components may have smaller standard deviations