Design for Reliability

Course No: B02-005
Credit: 2 PDH

Daniel T. Daley, P.E. Emeritus

Continuing Education and Development, Inc.

P: (877) 322-5800
info@cedengineering.ca

DESIGN FOR RELIABILITY

By

Daniel T. Daley

Introduction

Design for Reliability (DFR) is the process conducted during the design of an asset that is intended to ensure that the asset is able to perform to a required level of reliability. The reason there is a separate and distinct focus on DFR is that historically most design processes have tended to ignore the specific activities during asset design that would ensure reliability performance at any specific level. Instead, the reliability of the asset turned out to be the performance level provided by:

- The reliability that naturally accompanied design required for structural integrity
- The reliability that was the result of standard or historic practices for specific companies (like using redundant components in highly stressed applications or using specific components or equipment with which there had been good experience.)

While those practices have gradually led to increasingly good reliability performance, the improvement is neither managed nor the result of a scientific approach.

The demand for specific performance levels and the desire to do so in an effective and optimized manner has resulted in the growing movement toward increasing application of DFR and its spread to industries where it had not been applied in the past.

Historic design practices have tended to focus on two elements:

- Functionality
- Robustness or Structural Integrity

While the focus on those characteristics tends to produce some basic level of reliability, they are increasingly less effective as the level of sophistication increases. Said another way, the pyramids are still there but few examples of car models more than ten years old tend to survive.

In developing the design for the devices with low long term survival rates (like car models that are absent within several years after the end of the model run), the following characteristics have typically been missed during the design process:

- The failure rate of key components has been ignored.
- The usable life for key components has been ignored.

- The cost of maintenance needed to maintain the inherent reliability was never considered.
- The availability was never considered in the design.
- The maintainability was never considered.
- Key Failure Modes for key components were never addressed.
- Key Failure Mechanisms known to be present in the working environment of the asset were never considered in the design.
- The design was never properly verified through pre-release testing.

As a way to avoid the missteps described above, the process of DFR was developed. Using DFR, the designer and builder can ensure that the product will provide a long reliable life. For customers who understand that reliability, availability and maintainability of their assets are critical to their business success, DFR is a tool they can demand suppliers employ to ensure their needs are met.

Several of the key elements of DFR are the following:

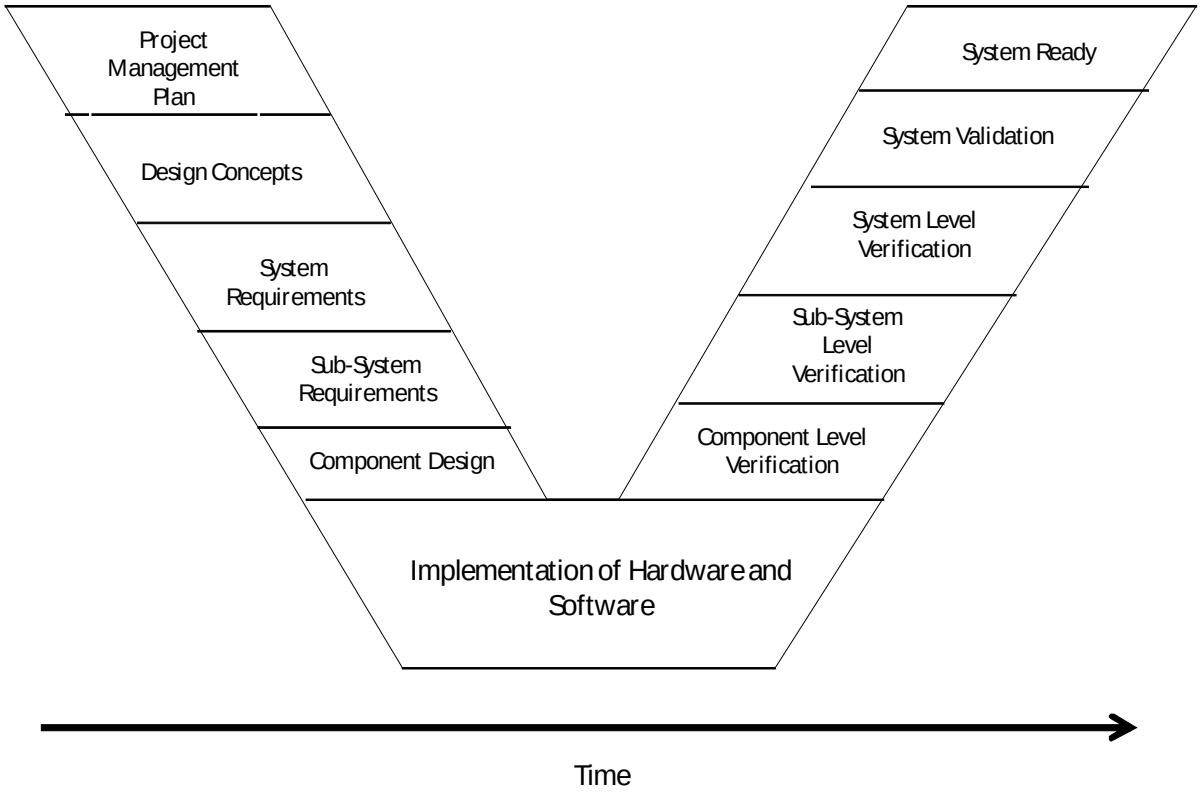
1. Concurrent Engineering – Concurrent engineering is the characteristic of properly applied DFR that ensures the conventional design is not completed before reliability requirements are identified and addressed.
2. Configuration Design – The physical configuration is first of several characteristics that decide the reliability of an asset. Depending on the severity of a specific service and the maximum economic reliability of available components, it may be necessary to build redundancy into some locations.
3. Component Selection – The second characteristic that determines reliability is the choice of components. Clearly, there are always choices to make concerning the components that make up an asset. Choosing components that are capable of the expected loading, designed to survive the severity of service and have been adequately tested to determine failure rate and usable life, will help ensure the desired reliability.
4. Design and Build – It is possible to create a solid configuration and select robust components and still produce an asset that is unreliable. There are design and assembly practices like use of protective grommets at points of wear, use of strain relief at bends, or changes in direction that ensure the configuration and components deliver the expected performance.
5. Verification and Performance Testing – Systems and complete assemblies do not always perform as expected. Interactions between dynamic components can produce unexpected effects. As a result, it is necessary to verify that the asset functions as expected. It is also necessary to simulate the wear and tear that represents an entire life using accelerated testing.

6. Customer Needs - Another important element of DFR is acknowledging the fact that the customer's needs are frequently much different than the seller's needs. For the asset to meet the customer's needs, the asset must be designed with the customer's needs in mind.

Concurrent Engineering

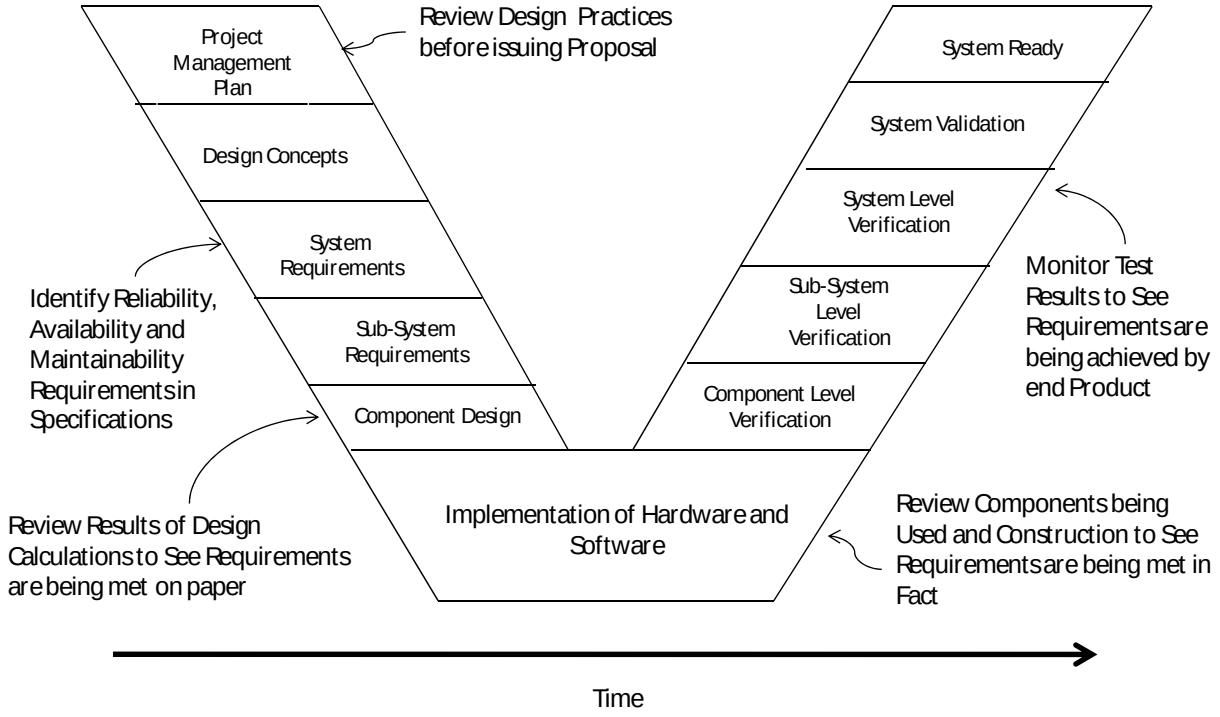
While it might sound trite, for Concurrent Engineering to be successful, it must happen at the same time as the corresponding step of the conventional design process. Most designers have an established design process they use and the process will proceed on a given schedule independent if the concurrent DFR process keeps up or not. The challenge for those responsible for DFR is to determine how to effectively integrate the steps required for DFR into the conventional design process and to see that the DFR keeps up with other design activities.

A useful tool in identifying key tie points between the conventional design process and DFR is the Systems Engineering V-model. This model portrays the steps typically needed to ensure the design of an asset, which must function as a completely integrated system, is capable of doing so. An example of this model is as follows:



While this model may not precisely match the design process for any single designer, it does represent the generic steps that should be followed when dealing with the design of an integrated system. The advantage of understanding the design process in a generic manner is that key milestone dates can be identified. Once the key milestone dates are determined, it is then possible to identify the timing of Concurrent Engineering activities to ensure reliability requirements are being addressed.

The following version of the Systems Engineering V-model has been modified to highlight key points in the generic process when an owner might wish to interface with the design and development process to see that his or her needs are being met. This model does not describe the timing of DFR steps but by reviewing the results, it provides a mechanism to see they are being accomplished in a timely manner.



Obviously, steps like defining Reliability, Availability and Maintainability requirements are activities that the owner should do before contacting the designer. Those performance characteristics are standards that are based solely on the owners business model and business needs. The owner should decide his needs before allowing himself or herself to be influenced by the designer or seller. If the owner is asking for unrealistic performance, that fact will be made apparent in competitive bids.

Defining Your Requirements

For purposes of this brief course, let's focus on three characteristics:

- Reliability
- Availability
- Maintainability

Reliability is the ability of an asset to survive a specific period of time without failure. There are a variety of ways to view the ability to survive and the period of time. Each is dependent on the specific business needs of the asset.

If you are in the airline business, the primary period of interest is each individual mission and secondary is longer term performance. In this case, once a plane takes off, it is absolutely critical that it completes the mission without a failure. If the plane passes pre-mission checks, it must be capable of completing the mission. It is better to fail the pre-mission checks than pass with marginal likelihood of mission success.

On the other hand, taking the long term view from a business perspective, it is also not acceptable that planes experience a high rate of failure during pre-mission checks or at any other time outside of the mission. Were that to happen, there would be a lot of unhappy customers and the overall asset availability would negatively impact profitability.

In this situation, the design requirements for reliability must identify failures during missions as absolutely unacceptable and non-mission failures as a negative profitability and cost impact. While choices involving the first requirement are independent of lifecycle cost, the choices involving the second can be determined by balancing initial costs with long term costs and profitability.

The above example is just one of an infinite number of possible ways that business needs can be used to determine reliability requirements. The pattern portrayed by the example above provides an approach that can be applied to many situations:

- Failures that can result in injury or environmental insult are independent of economic analysis. They should be absolutely prevented by the design and accompanying systems of controls (like pre-flight tests).
- Failures that only impact economic performance should be decided based on lifecycle cost analysis.

Availability is the second characteristic that should be defined by the owner. The profitability of an asset is based on three issues. The first is the value of the product produced by the asset when it is functioning. The second is the production rate of the asset or the amount of valuable product that is produced when the asset is operating.

The third is the portion of time the asset is capable of operating and producing the desired product. This third characteristic is another way of describing availability.

More specifically, availability is the portion of the total time than an asset is functioning and able to produce the desired product. Availability is affected by two forms of down time:

- Planned Downtime or the time the asset is not functioning as a result of the need to perform needed regeneration or renewal.
- Unplanned Downtime or the amount of time the asset is down as a result of unplanned failures. In turn, unplanned downtime is the product of the frequency of failures (or reliability) and the timeliness of the response to failures (or maintainability).

There are a variety of ways that availability can be addressed during the design process. Unplanned downtime can be improved by addressing reliability (as described in the prior section) and maintainability (as will be described in the next section).

Planned downtime can be addressed by identifying the specific elements causing each planned outage and designing them in a manner that minimizes the required planned downtime.

The number of incidents of planned downtime can be determined by identifying components called “Run-Limiters”. Run-Limiters are the components that determine the maximum run-length of an asset. When a Run-Limiter reaches the end of its useful life, the asset must be shutdown for renewal of that component. The amount of time the asset must remain down once shut down is determined by elements called “Duration-Setters”. The critical path duration of the steps of work needed to renew Duration-Setters determines the minimum down time.

By identifying the Run-Limiters and Duration-Setters and making them more robust or easier to renew, it is possible to increase the availability of an asset.

The third characteristic mentioned above is Maintainability. Maintainability is a measure of the ability to restore the Inherent Reliability of an asset in a ratable period of time. It is important to keep in mind that the objective of both planned and unplanned repairs are to restore the inherent reliability of the asset, Rather than just restoring the functionality of the asset and leaving the asset “good as old”, it is important to remove the defect and leave the asset “good as new”.

An anecdotal example is useful in explaining maintainability:

If you take your car to the corner mechanic for repair and he says, "'I'll be done in an hour, but I don't know how long it will last", it is not maintainable because he cannot assure the Inherent Reliability is restored.

On the other hand, if the mechanic says, "When I finish it will be as good as new, but I don't know how long it will take", it is also not maintainable because the period of repair is not ratable.

For the car to be maintainable, the mechanic must be able to say, "I will have it complete in two hours and it will be as good as new".

The elements of a repair process that would lead to questionable ability to restore Inherent Reliability are as follows:

- Tasks that the mechanic cannot see when doing
- Repairs than cannot be tested when complete
- Instances in which the Failure Mode of a component is not apparent and cannot be tested to confirm the presence of the defect
- Instances where working space or cleanliness requirements are so significant that makes it unlikely the repair will be completed without imbedding another defect in the system
- Instances where there are multiple simultaneous defects and fixing one does not fix the others

The elements of a repair process that would lead to questionable ratability of repair duration are as follows:

- Steps that must be completed with the mechanic "standing on his head"
- Steps that require "trial and error" methods
- Steps requiring unusual skill levels for mechanics
- Repairs that have not been completed in the past and built into an easily understood and repeatable processes

In order to conduct a maintainability analysis during the design process for an asset, it will be necessary to identify the Predictive, Preventive and Repair tasks that are expected over the life of the asset. Preparing a comprehensive list of those tasks will require that the owner perform a Reliability Centered Maintenance (RCM) analysis or some other form of Failure Modes and Effects analysis that identifies all the Failure Mechanisms present in the operating environment and all the Failure Modes that are expected with each component. The Predictive, Preventive or Repair tasks are the activities required over the life of an asset to avoid failure or to recover once a failure has occurred.

DFR for Sellers

In most cases where DFR is applied, it is applied with the seller's business model in mind. In this context, I am assuming that the seller is also the designer or has control of decisions made during the design process.

In some cases, the seller of a product may base his income stream solely on the initial sale of the product and have little liability or opportunity after the asset has been sold. Many plants fall into this category. Unless a catastrophic event occurs that can be shown to be the result of an engineering blunder and if the seller was found liable for the effects of failures, the seller receives final payment at the conclusion of the project. He walks away with no further liability for poor reliability or opportunity associated with the sales of replacement parts or service.

In other cases, the seller's business model is more like a marriage agreement. Initially the owner is tied to the seller by a warranty agreement. After the expiration of the warranty for the asset, the seller is tied to the seller through a long-term service agreement and an agreement to supply replacement parts. As a result, the seller's business model contains both near-term liability and long-term opportunity.

In the first case described above, the primary tie to the seller's business model is through the impact on the seller's reputation. In the second case, the seller's reputation is at stake as well as several different income streams.

In defining requirements for reliability, availability and maintainability of a product, the seller considers all of the following elements in one way or another:

- Marketable Product – Or the ability to produce a product that is attractive yet affordable.
- Reputation – Or the ability to be viewed by potential customers as an acceptable source.
- Income streams – Or a revenue producing connection with the seller's business model.
- Initial Profitability – Or the ability to push a product out the door that competes in the market place while providing an acceptable margin of profit to satisfy the stockholders.
- Short-Term Liability – Or few enough failures during the warranty period to avoid exceeding the amount allowed for in the selling price.
- Long-Term Liability – Or a balance of few enough failures over the long-term to avoid a negative impact on reputation while there is enough failures to support income streams associated with service and parts sales.

- Functional Design – Or the ability of products to provide increasingly sophisticated functionality while avoiding the reduction in reliability typically associated with unproven technology.
- Product Integrity – Or the general robustness of the product to avoid non-reliability related catastrophic failures.

Clearly all these issues impact the reliability related choices made by sellers. While many seller's might say, "We only wish we were good enough to create designs based on all those factors", it is useful to look at a few examples:

- How long does a "three-year" automobile battery typically last? Not much more than 3-years.
- For almost any appliance that comes with a warranty, how long after the end of the warranty does it begin to experience nuisance failures? Not long.

Clearly, for products sold in large numbers where the technology and forms of deterioration are well known, the sellers are much more able to match the end of life with the end of seller's liability. Rather than "designed obsolescence", this is better described as "you get what you pay for".

By understanding his business model and adapting the design to fulfill the needs of his own business model, the seller is making wise business decisions.

The seller can use the various steps of DFR to optimize the design and construction of his products around his own requirements.

The DFR process for the seller includes the following kinds of steps conducted in an integrated manner with the conventional design steps.

Steps of DFR for Sellers

- RBD – Reliability

  The Reliability Block Diagram method for analyzing the reliability of a design consists of creating a model of the system functionality in which a single block is used to represent each component that is likely to fail over the life of the asset. Once the model is complete, each block is loaded with values that represent the reliability performance of that block.

  Determination of the system reliability can be done in two ways. Either set of mathematical relationships can be used to calculate the overall reliability of the complete system. A more accurate and flexible way the analysis can be completed is by using a computer program to simulate the

expected performance. In the computerized approach, the survival or each block is modeled using a Monte Carlo simulation. When the Monte Carlo simulation produces a failure in any block, the overall system responds as it would in the real life system. If the failed component is unspared and the component is critical to the functionality of the overall system, the system experiences a failure. If the failed component is spared with a redundant component, the system continues to operate, but without the luxury of redundancy for the failed component.

By setting the program to run for the entire required life span (say 30 years) and by running a hundred or more simulations, the program is able to provide a reasonable estimate of the system reliability over its entire life with a high degree of confidence.

- RBD – Availability

  Once the RBD analysis for reliability is complete, it is further possible to use the RBD software to calculate the expected availability for the system.

  This process begins with identifying all the periods of planned outage, the length of time the system will be down for each outage, and the condition of the system at the conclusion of each planned outage. For instance, if components that experience increased likelihood of failure as they age are renewed during the outage, the system may be viewed as “good as new”. If those components are not renewed, the system will be viewed as “good as old”.

  Once unavailability for planned outages is accounted for, it is necessary to account for unavailability for unplanned outages. The RBD analysis for reliability, described above, will identify all the assumed Failure Modes that will occur over the entire life of the asset. By analyzing those Failure Modes, it should be possible to determine how long it will take to respond and recover from each. The recovery time can be associated with each block in the RBD model and another series of one-hundred 30-year life spans can be simulated. This run will provide an accurate average availability for the system.

- Build as Designed

Performing the detailed reliability analysis during the design process provides the designer with insights concerning areas that will be highly sensitive to build issues. For instance, if a likely Failure Modes for a specific component is related to being overheated, the installation process can be designed to shield the device from unusual heating during installation.

Components with a high likelihood of infantile failure can be subjected to "burn-in" to eliminate those that would fail early. Components that come from questionable populations can all be tested prior to use. Where exotic materials are used, it is possible to provide "positive material identification" steps to ensure the right type and quality of material is being used. Where key conditions or functionality is obscured as the build process proceeds, it is possible to create interim inspection steps to ensure the last step has been completed correctly before proceeding.

Ultimately, the objective is to create a process for building the asset that results in a product as close to design as possible.

- Verification and Testing Tools

  Once the system is complete, several forms of testing are possible. If the finished product is the first of many, it is possible to expose the system to forms of testing that might lead to destructive results. If the product is one-of-a-kind, the typical testing is limited to functional testing and stress testing within allowable limits of the design. In either case, the objective will be to expose the asset to various forms of functional problems or stress that can occur over the life of the asset.

  Considering products for which a large number will ultimately be built, the following forms of testing are valuable:

  - HALT – Highly Accelerated Life Testing is examination accomplished during the manufacturing process. It exposes critical elements to normally high stress levels at increased frequency rates to simulate the wear an asset will experience over its entire life.
  - HASS – Highly Accelerated Stress Screen is a form of testing similar to HALT except it is applied at the end of the manufacturing process to completed assets and using stresses that may be at a destructive level for marginal components.

- HASA – Highly Accelerated Stress Audit is a process similar to HASS except it is done during the manufacturing run using randomly selected items to ensure the on-going manufacturing process is continuing to deliver the required quality.
- ESS – Environmental Stress Screen is similar to the testing described above but only focusing on extremes of temperature, humidity and other environmental factors.
- RDE – Robust Design Experiment is similar to the testing described above except it is intended to determine an assets ability to withstand misuse. In this case, the form of misuse might be a form of use that is beyond the intent of the design but not beyond the limits of possibility.

When considering one-of-a-kind products, the following tests are advisable:

- FMEA Mitigation – During Failure Modes and Effects analysis that are conducted as a part of DFR during the design of an asset, it is likely that various forms of mitigation will be identified. This mitigation will take the form of either physical changes to the design or administrative or procedural controls. The associated failures should be simulated during testing to see if mitigation is effective.
- Full Functionality Tests – The asset should be tested over its full range of operation and abnormal, yet possible, conditions.
- Hydrotesting and testing other components within design limits – All components designed with a specific level of robustness intended to safely survive unusual loading should be tested to the design limits.

DFR for Owners

By comparison, the requirements set by the owner are quite different from those set by the seller. Typically the owner has a different product than the seller of an asset. The asset being purchased by the owner ultimately becomes part of the owner's capacity for producing his product.

While the seller's focus is on the elements of his business model, the owner's focus must be on the owner's business model. The elements of the owner's business model include the following:

- A 30-year life
- Production rate

- Production quality
- Efficiency and energy consumption
- Safety
- Environmental performance
- Operating costs
- Maintenance costs
- Outage requirements
- Renewal requirements and frequency
- Reliability
- Availability
- Maintainability
- Etc.

Each of those characteristics is an element that must be addressed in the design and provided in a consistent manner for the life of the asset. As a result, the features of the design that provide those characteristics must be analyzed to ensure reliability for the life of the asset. For instance, if specific characteristics or components are needed to ensure the asset is capable of the design production rate or efficiency, those characteristics or components must be shown to be reliable. It is not sufficient that the reliability analysis shows that an asset remains functional; the reliability analysis must show that the asset retains production capacity and efficiency.

The following describes DFR tools that can be used to ensure the owner's objectives are met:

DRF for Owners – Requirements

All too often owners believe that some generally accepted standard of performance rules the characteristics of the products they purchase. They believe that generally accepted standards will protect them and see their needs will be met.

It is unreasonable to expect that unstated characteristics that add to the initial cost of a product will be provided by the supplier unless they are clearly described in specifications. This is particularly true in competitive bidding situations. A supplier who provides features not clearly described in the specifications is unlikely to be the low bidder.

As a result, it is critical that owners determine all the characteristics that must be provided in their assets and clearly identify them in the specifications. The list of owner requirements shown above provides a useful starting point but is not exhaustive.

DRF for Owners – Reliability

The process of calculating the anticipated reliability of an asset using the RBD technique described above is an excellent tool for meeting the owner's needs. There are two steps that must be accomplished to complete this activity in a way that supports the owner's requirements:

1. The owner must confirm that the results of the RBD calculations do, in fact, meet his requirements for reliability and do so over the entire life of the asset.
2. The owner must obtain a copy of the RBD analysis along with the assumed performance for each and every component. This will enable the owner to compare component design expectations to actual performance.

DFR for Owners – Availability

The process of calculating the anticipated availability of an asset using the RBD technique described above is also an excellent tool for meeting the owner's needs. As with the case for reliability analysis, there are two additional steps needed to meet the owner's needs:

1. The owner must confirm that the RBD calculations do, in fact, meet his requirements for availability over the entire life of the asset.
2. The owner must obtain a final copy of the information used to describe component level performance in the RBD analysis. Again, if actual performance proves to be different than assumed, the owner will want to require that the OEM or sub-tier suppliers take corrective action.

DFR for Owners – Maintainability

Maintainability is one of the most difficult characteristics to evaluate. First, it is necessary to perform some form of Reliability Centered Maintenance (RCM) analysis during the design to identify all the proactive and reactive tasks that will be required over the life of the asset. Second, it will be necessary to perform a realistic "walk-thru" for each and every anticipated task to ensure that it both restores the Inherent Reliability of the asset and does so in a ratable, repeatable period of time.

If the supplier is not in the business of performing on-going maintenance, this activity may require the seller to hire additional resources (with maintenance backgrounds) to perform the analysis.

On the other hand, the owner should be in a position to assess the Maintainability analysis performed by the seller to determine if it is comprehensive and realistic.

Harvesting Long-Term Benefits

While it is likely there will be some near-term benefits associated with the application of DFR (owing to increased reliability during the early life of an asset), the greatest benefits that can be achieved by using DFR comes in the long-term. That benefit is the result of continuing to observe and maintain the information created as a part of the DFR for the entire life of the asset.

By way of example, consider an anti-friction (ball) bearing. This kind of device has a readily available B-10 life that describes the point in time that 10% of the bearings population will have failed. This life is based on loading and severity of service. Assume that a designer must select an anti-friction bearing for a specific application. Obviously, he picks one that has the proper dimensions and speed. Beyond that he picks one that will sustain the maximum loading. He will also pick one that is intended for the severity of the conditions expected. If the designer recommends Preventive Maintenance, he would likely recommend replacement at the B-10 point in its life.

Once in service, it is likely that conditions will be different than those assumed during the design. It is likely that actual loading will be less than the maximum for most of the operating time. The severity may be either greater or less than assumed. While the assumed Failure Mode is based on the allowable number of fatigue cycles, the actual failure mode may be the result of dust and grit intrusion. The only way to understand how real-life differs from DFR assumptions is to closely monitor the results of the real-life experience and to alter assumed characteristics and recalculate new expectations.

At any rate, the usable life assumed during the design of the asset and the required program of Predictive and Preventive Maintenance may be far different in real-life than that assumed during the design. Over the life of the asset, the owner certainly wants to prevent failures (by replacing wearing components prior to failure). He also wants to minimize maintenance costs (by harvesting all the usable life from components).

The following describes some of the benefits that will result from continuing to use and update the DFR information, including the RBD analysis, over the entire life of the asset.

- Knowing what to expect concerning overall asset reliability – This provides the owner with the ability to demand corrective action be taken by the supplier when actual performance is less than what's promised.

- Knowing what to expect concerning the reliability of individual components – This provides the owner with the ability to identify the exact cause when system failure does not meet expectations. It also provides a basis for owners to demand corrective action from sub-tier suppliers when the principal OEM is unable to show that components are not performing as promised.
- Knowing what to expect concerning the usable life of individual components – This provides the owner with the ability to create programs of Predictive and Preventive Maintenance that are effective while not overly conservative.
- Knowing the Predictive Maintenance and Preventive Maintenance needed to maintain the Inherent Reliability of an asset – This provides the owner with the ability to understand the reliability and availability that can be expected over the entire life of the asset and how much it will cost to secure that performance.
- Knowing the proper way to repair an asset in a way that will restore the Inherent Reliability – This provides an owner with an assurance that he knows how to maintain an asset and that the maintenance procedures both restore Inherent Reliability and can be done in a ratable, repeatable amount of time.
- Maintaining an on-going relationship with suppliers of the overall asset and the individual components – This provides the owner with the ability to put his suppliers on notice that by agreeing to supply an asset, they are accepting some degree of accountability for that asset over the entire asset life.
- By maintaining a copy of the RBD model and updating component factors with accurate information as actual component data is generated, knowing what the actual system reliability and availability will be – This provides the owner with realistic expectations for assets. If a number of components perform at a level far less than expected, the owner should expect poor performance from the overall asset. As a result, the owner will know which components must be upgraded to more robust versions to achieve the required reliability and availability.

Conclusion

When reliability, availability or maintainability is an important characteristic of an asset, there is only one way to ensure the required characteristics are delivered. That is through the application of DFR. If DFR is not used, the level of reliability performance delivered by any asset will be determined by design processes that are not specifically intended to determine that form of performance.

Said another way, it would be like assuming a car will be rugged because it is designed to be fast. Focusing your design attention on one characteristic does not ensure another.

To deliver reliability, you must focus on reliability. To deliver availability, you must focus on availability. To deliver maintainability, you must focus on maintainability.

To deliver reliability for the entire life of an asset, you must focus on reliability for the entire life of the asset. To deliver availability for the entire life of an asset, you must focus on availability for the entire life of the asset. To deliver maintainability for the entire life of an asset, you must focus on maintainability for the entire life of the asset.