

Reliability Modeling Analysis

A system's overall reliability can be determined by the development of reliability models. The complexity of these reliability models are dependent upon various factors such as mission profiles, function criticality, and redundancy characteristics. The general approach is to capture the modeling effort with the use of Reliability Block Diagrams. The image to the right (click image) illustrates how a more complex system's configuration maybe represented by a Reliability Block Diagram.

For each system the mission profile or usage profile varies. For example a combat aircraft's mission profile may be expressed in a maximum mission duration of six hours, with a required probability of mission success (reliability) of 98%. Whereas, a financial institution data processing system must provide a continuous operation, twenty four hours a day, every day of the year, and it may be expressed in achieving a target operational availability.

The model could be concerned with just showing the critical functions and the associated failures modes, as derived in the FMECA. This information may further be used in the FTA of the safety engineering.

Redundancy or back-up mechanisms will enhance the reliability of a system, but augment the Life Cycle Support (LCC). Questions that would need to be considered, is whether the system should employ "active redundancy or standby redundancy ".

The actual decision for the system redundancy could also be dictated by other engineering constraints, for example the safety requirements might mandate a 2 out of 3 voting redundancy

Active Redundancy

The approach here would have redundant elements that would support a fault tolerant architecture. In this case, the active redundancy, all of the redundant elements are utilised by the system, e.g. they are powered up. However, in the event that one (or more) element fails, the system is capable of performing its required function and operation. The redundant elements incorporated into a design could be a simple affair or consist of very complex elements. With a more complex configuration the architecture could consist of a combination of elements having no redundancy, a couple of elements having dual redundant, to several elements in parallel etc.

The final system configuration would be influenced by the actual required reliability and availability requirements, which takes into consideration whether the system is repairable or non-repairable. For example a system is required to operate for a given operating time period, and maintenance is not possible. Such as a commercial airliner making a transatlantic crossings, its redundant architecture would have taken into consideration the fact that a repair could not be implemented for the several hour flight duration,. In the case of a satellite or space probe, it is required to operate for several years and during this time no maintenance would be feasible.

Another example might be a data processing system which is required to have a high operational availability and must provide a continuous service of 24 hours a day, seven days a week, 365 days a year. This type of system could be an air traffic control system to a financial banking system. To support the operational availability requirement, a maintenance philosophy may be developed, that would ensure that all repair actions (corrective maintenance tasks) are completed with one or two hours of a failure.

In the following given example is a simple Dual Redundant Configuration. The system's reliability can be calculated as given. This calculation assumes that the systems are identical, other words each having the same failure rate and that the failures follow an exponential distribution pattern.

<p>System Reliability: $R_{sys} = 1 - Q_{sys}$</p> <p>Where:</p> <p>$Q_{sys} = Q1 \times Q2$</p> <p>$Q1 = Q2$</p> <p>$Q1 = \text{Component Unreliability} = 1 - R_{equip}$</p> <p>Equipment Reliability: $R_{equip} = e^{-\lambda t}$</p>	<p>System</p>
---	----------------------

Standby Redundancy

There might be instances where a system must achieve an operational availability and itself cannot afford an extend downtime. With repair actions of a failed unit being possible, but the implementation of an active redundant configuration not considered feasible, due to economic or operational reasons. It may be more appropriate to utilize a standby redundant configuration. An example of this could be a field power generation plant. The power

distribution configuration would consist of two 800 KVA diesel generators. One would be online (running) continuously and the other would be in a standby state (not running). In the event that the operational generator experiences a failure (or where the need to perform preventative maintenance exists), the standby generator would be brought on-line. This would then permit a repair action to be implemented on the failed generator set.