Driving Decision Points Employing Failure Mode and Effects Analysis

Tech Brief 151101 FE

Integrated Systems Research, Inc.

November, 2015

steve.carmichael@isrtechnical.com

Abstract:

The primary value of a Failure Mode and Effect Analysis (FMEA) is being able to identify the key decision points which drive the success of a design. The FMEA, by defining the negative space, focuses the creativity and analytical effort where it is most needed. This tech brief addresses the inherent weakness of the multiplicative approach in determining the Risk Priority Number (RPN) in a FMEA and the potential pitfalls to consider when mitigating risk through redundancy.

RPN – Multiplicative Approach

In a Failure Mode and Effect Analysis (FMEA), the typical method for determining the Risk Priority Number (RPN) for each failure mode is by multiplying the values assigned to the severity, frequency of occurrence, and detectability of the failure. The standard procedure is to assign a value from 1 to 10 for each of these three categories. The highest RPN that can be generated with this approach is 1000 (i.e., 10 x 10 x 10). The lowest possible RPN value is 1. No category is ever assigned the value of zero.

A fundamental fallacy with the multiplicative approach is that a potentially catastrophic failure mode can easily be masked with a nuisance. For example, a potential failure mode that will compromise the mission of a system or result in significant harm will have a severity of 10. If the frequency of this failure mode, however, is very low and the ability to detect it prior to service is high the RPN number for this potentially catastrophic failure mode is 10 (i.e., 10 x 1 x 1).

On the other hand, a potential failure mode could be virtually imperceptible to the customer and therefore have a value of 1.0 assigned to its severity but have a higher RPN than a potential catastrophic failure. If a nuisance occurs frequently and is difficult to detect prior to being placed in service then its RPN is 100 (1 x 10 x 10). This nuisance has a higher RPN value than a potential catastrophic failure. Aliasing, catastrophic failures with nuisances, makes it difficult for an engineer to identify where the creative and analytical resources should be focused for a successful design.

Another potential problem with the multiplicative approach is the tendency to concentrate on risk management rather than looking for better design alternatives. In a broad stroke, risk is consequence per unit time. Risk, however, as a technical concept, requires an actual statistical warrant, an understanding of causality, relational independence, and consequence propagation in order for it to be defined and used in a meaningful way.

In a FMEA the criticality of a failure mode is the product of the severity and frequency of occurrence. In a strict sense, however, this criticality is not a measure of risk. In reality, the FMEA is a means of prioritizing potential failures. Attempting to assign actual risk, in a technical sense, using a FMEA can defeat its real objective. Even when a potential failure mode has an extreme severity, if the frequency of occurrence is low it is possible for a nuisance to have the same level of criticality. The problem is that the multiplicative RPN approach makes the FMEA appear to be more than a prioritizing methodology.

Since the RPN value is the product of both the criticality and detectability, there tends to be a concentration on detectability to lower the RPN value. Increasing detectability is desirable, but robust designs tend to have low criticality and are also insensitive to input variation. Concentrating only on detectability can actually result in less robust designs which require a relatively high amount of preventative maintenance and surveillance for successful operation.

RPN – Place Holder Approach

An alternative to the multiplicative approach, in determining the RPN value, is the place holder method. Using this method each component of the RPN is given a place holder. Severity is assigned the hundreds, frequency of occurrence is assigned the tens, and detectability is assigned the ones.

The criteria ranking is consolidated from 10 to 5 categories. Table 1 illustrates this consolidation for the severity ranking. Similar consolidation occurs for frequency of occurrence and detectability.

Table 1 – Severity Ranking

Severity Evaluation Criteria			
Effect	**Mission and Personnel Effect**	**Rank**	**Alt Rank**
Minor	The customer(s) of the process will not notice the effect of the failure. No impact on supplier's or customer's process	1	100
Very low	Nature of failure only causes slight delay or minor rework. Slight customer annoyance	2	
Low	Failure causes minor problems which take a small amount of time to overcome. Some customer dissatisfaction and/or impact on their process	3	200
Moderate	Failure causes problems which have a noticeable impact on business performance metrics. Medium customer dissatisfaction, e.g. extra effort or rework needed	4	
Significant	Failure causes customer dissatisfaction, e.g. disrupts customer's operations or add cost	5	300
Very significant	Failure causes significant customer dissatisfaction, e.g. disruption or cost	6	
High	High degree of customer dissatisfaction due to failure such as system shutdown that has a medium impact on the customer's operations	7	400
Very high	Major degree of customer dissatisfaction due to impact of failure on their process - delay or extra cost incurred. Significant impact on business metrics	8	
Critical with warning	Failure causes own or customer's process to stop completely with some warning	9	500
Critical with no warning	Failure causes own or customer's process to stop completely without warning	10	

With the place holder method the three values are added together rather than multiplied. This ensures that the criticality is never aliased with controllability. The lowest RPN value that can be obtained with the place holder approach is 111. The highest value is 555.

In regards to using the analysis at a decision point, one may choose to use the value of the last two digits to determine whether or not to proceed with the design approach. If this approach is taken then controllability or risk management is the strategy that has been adopted. Regardless of the decision point criteria, however, using the place holder approach eliminates the possibility of the criticality of the failure mode being masked.

If addressing the criticality of the failure mode, however, is the chosen approach it forces the engineer to consider changing the design so as to either eliminate the failure mode or provide redundancy so that it does not compromise the mission of the system or function of the component. If redundancy is the chosen approach, careful consideration needs to be given to ensure that the added complexity created by the approach does not defeat the objective of reducing risk and increasing reliability.

Redundancy[1]

Redundancy in engineering has become a fundamental paradigm in the design of systems with high criticality. Employing this approach successfully requires careful consideration of independence and propagation. In order for redundancy to actually exist the parallel element(s) providing the same function are required to be independent. This is not necessarily as simple to evaluate as it might first seem. Secondly, the addition of the redundancy should not create the possibility of creating a greater risk than what already exists. The following examples illustrate these two concepts.

One example of a loss of system independency occurred in June of 1982. At 37,000 feet above the Indian Ocean a British Airways 747 lost power in all four engines. No one ever thought it possible that an aircraft with four engines could lose all its propulsion. The crew had never been trained to deal with the scenario. Fortunately, as the aircraft descended the engines came back to life. What happen was the aircraft had entered a cloud of volcanic ash and all of the engines became clogged. The engines had lost operational independence through a common link, the ash. As the aircraft descended out of the ash cloud the engines were able to restart.

[1] This section is highly indebted to John Downer, *When Failure is an Option: Redundancy, Reliability and Regulation in Complex Technical Systems*, LSE Discussion Paper No 53, May 2009

A common link can also be human elements creating a loss of independence. A multiple engine failure occurred on a Lockheed L-1011 when the same personnel servicing all three engines refitted the oil-lines without the O-rings to prevent in-flight leakage. It is now required that separate crews service two engine aircrafts. Identifying the potential loss of independency of redundant elements is essential to ensuring that the redundancy has actually reduced the criticality of a failure mode.

Lastly, it is possible that the addition of redundant elements in a system can detract from its reliability due to the element adding the possibility of additional failure modes. For example, an aircraft with four engines versus two engines has a lower chance of experiencing an all engine out failure, but the two engine aircraft has a lower probability of a single engine failure such as an explosion or containment failure. An explosion or containment failure can create a greater hazard than a single engine out. This is the argument that led Boeing to conclude a two engine 777 was a lower risk system than having four engines.

Although redundancy is a powerful concept in increasing the reliability of complex systems, care is required to ensure that the objective for employing the approach is actuality realized. It is possible for an attempt to create redundancy to be self-defeating.

Conclusions

The place holder method, for computing the RPN in a FMEA, provides the benefit of not aliasing potential catastrophic failure modes with nuisances. It keeps the focus on prioritizing potential failure modes rather than attempting to assign risk in a technical sense. This facilitates a more productive means of allocating creative and analytical resources in the design process.

Redundancy is a common and useful engineering paradigm to increase the reliability and address the criticality of a design function within a system. For the approach to be successful, however, the relational independence and failure propagation associated with the redundant elements have to be adequately addressed in the decision making process. Awareness of these requirements helps the engineer productively assess alternatives in the creative process of design.