

Risk assessment and management are critical for maintaining product safety. Learn about some of the most popular methods that help you quantify risk for an organized and efficient approach to risk management.

Reliability Methodologies for Quantifying Risk

Risk is analyzed through categorizing the relationship between the probability of an event occurring and the resulting severity of the effects of that event, should it occur. Though there are several methods used by engineers to categorize risk, they all attempt to model the relationship between occurrence and severity through the use of levels.

On the most basic level of analysis, there is a simple dichotomy in regard to risk. This dichotomy is generally not between “risk” and “no risk,” as a basic assumption is that nearly all events contain some element of risk. Instead, the dichotomy is between “risky” and “not risky.” Standing on a chair is risky, while sitting on a chair is not risky. As events become more complex, the notion of risk becomes more complicated. Take, for example, a six-foot stepladder. Standing on the bottom step of the stepladder would be considered not risky. Standing on the very top of the stepladder is extremely risky. But what about standing on the middle step of the stepladder? Is this risky or not risky? It’s clear that risk increases as you climb higher on the ladder. At some point you enter an area of medium risk, where you begin to consider the effect of falling from a ladder at that particular height. At a higher step on the ladder you cross an acceptable level of risk, usually indicated by warning labels on the steps of the ladder, and enter the realm of high or severe risk. The notion of risk is no longer a simple dichotomy, and a prioritization of risk based on levels is necessary.

Risk quantification tools are used to define level of risk, with some events falling in a critical or high level, and other events falling in a very low or acceptable level. The events in between can then be categorized in a number of different ways. In some cases, simple three-step levels are used: high, medium, and low, and these may even be associated with a color-coded scheme such as red, yellow, and green. The United States Homeland Security Advisory System uses a combination of five colors (red, orange, yellow, blue, green), five titles (severe, high, elevated, guarded, low), and five descriptors (severe risk, high risk, significant risk, general risk, and low risk).



Source: DHS.gov

Some risk categorizations may be six levels: Frequent, Probable, Occasional, Remote, Improbable, Extremely Remote. There are also ten risk level breakdowns, associated simply by number: 10 through 1. The choice of risk categorization is up to you. The main objective is to select a prioritization scheme and then identify the levels of risk which fall above and below the acceptable level.

But how are risks assigned to these levels in the first place? How do you know if an identified risk is probable or not? This is where the need for quantification of risk comes into play. By being able to systematically quantify identified risks, you can focus on the most critical risk elements and be confident that your system is as safe and reliable as you want it to be.

Engineers have a toolbox of analysis techniques designed to quantify risk. By understanding these tools and their approach to risk assessment, you can choose the tool that best fits your requirements. Risk assessment tools include:

- Failure Mode and Effects Analysis (FMEA)
- Failure Mode, Effects and Criticality Analysis (FMECA)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Human Factors Risk Analysis (HFRA)

Quantifying Risk with FMEAs

A Failure Mode and Effects Analysis (FMEA) takes a bottom-up approach to system analysis. Your first step in a FMEA is to break down a system or process into discrete elements. This breakdown can be at any level you deem acceptable – it could be as detailed as evaluating each and every component in a large system, or simply identifying a number of high level tasks in a process. Regardless of the level of detail, once the breakdown is complete the next step is for you to determine the ways in which each element could potentially fail, and then to explore the possible resulting effects of those failures. The risk level of each of the identified effects must then be assessed. Depending upon the resulting risk level, the corresponding failure mode must be evaluated to determine if the failure mode is to be eliminated/mitigated, or if it is acceptable as is. The action you take is then based on this risk analysis.

In FMEAs, there are several mechanisms to choose from to quantify risk. These include Risk Priority Numbers (RPN), Mode Criticality, Criticality Rank, and Risk Level. The method you choose to employ depends on the data you are working with and how you have configured your FMEA worksheets.

- *Risk Priority Numbers (RPN)*
RPNs are based on a FMEA approach adopted in FMEA methodologies such as those defined by SAE, AIAG, and Ford. To use RPNs, you evaluate the Severity, Occurrence, and Detection levels of each failure mode using a 1-10 scale. RPN is then calculated as:

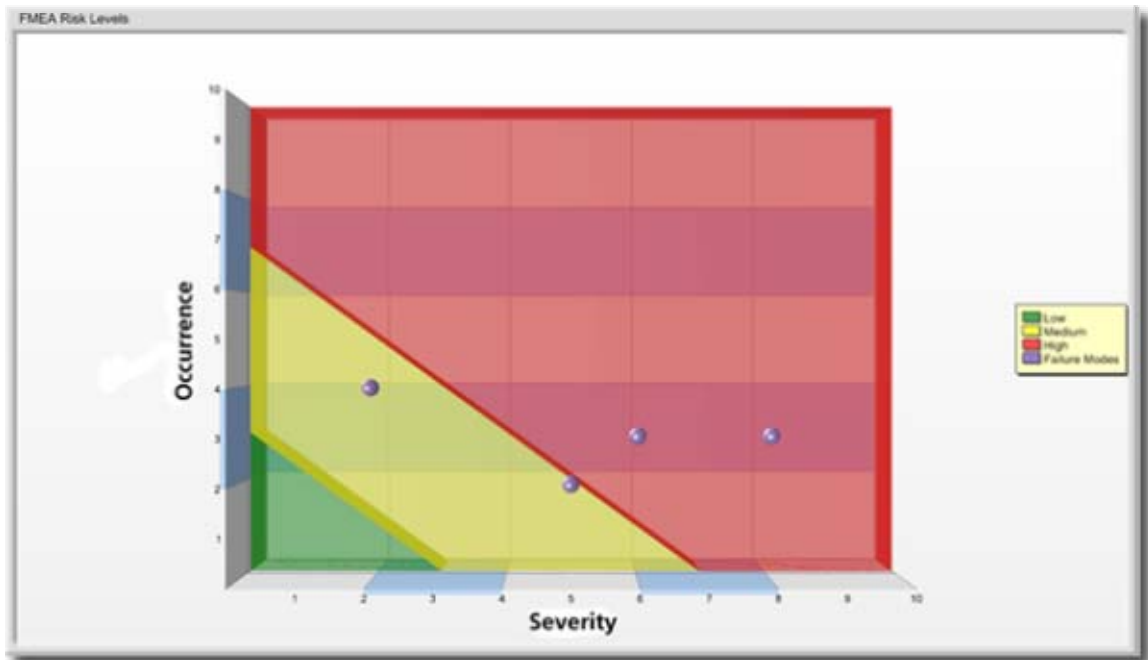
$$RPN = Severity * Occurrence * Detection$$

- *Mode Criticality*
Mode criticality is a numerical value that can be calculated and applied to each failure mode. Mode criticalities are based on a FMECA approach defined in MIL-STD-1629, a commonly used FMECA methodology. Mode Criticality is computed using the following equation:

$$Mode\ Criticality = Failure\ Effect\ Probability * Failure\ Mode\ Ratio * Failure\ Rate * Operating\ Time\ of\ the\ System$$

- *Risk Level*
Risk Level is a technique described in Paul Palady's book *FMEA – Failure Modes & Effects Analysis – Predicting & Preventing Problems Before They Occur*. The

risk level results in a graphical overview of failure modes based on a three-level assessment: high, medium, or low. The axis values on the graph are risk-based criteria such as Severity and Occurrence.



A Risk Level Graph charting the severity and occurrence of failure modes. The color coding system makes it easy to identify levels of risk.

- **Criticality Rank**
Criticality rank is an approach described in the SAE ARP5580 FMEA standard. Criticality ranking provides a systematic way to rank failure modes based on a multi-criterion Pareto system. Failure modes are assessed by the analyst in terms of severity and probability of occurrence. The weighting scale can be set by the user and may be based on industry accepted values.

For more details on each of these risk techniques, please read our previous *eFlash* article, [Learn Why FMEAs Are a Preferred Tool of Reliability Professionals](#).

Quantifying Risk with Fault Trees

A fault tree is an analytical methodology used to determine the probability of a single, top-level event. Fault tree tools use pictorial representations of a system and show how a sequence of events may lead towards the top-level event. Lower level events, referred to as basic events, represent hardware, software, or human failures for which the probability of failure is given based on historical and predicted data. As the basic events are linked in sequence via logic gates to the top-level event, probability and statistical calculations are used to provide the measurement of the risk of the specific event being analyzed. Typically, fault tree analysis is used to evaluate defined undesired or catastrophic events, so that your time and efforts are used most wisely, i.e., on the areas of greatest importance and consequence.

Fault tree analyses can be used for risk assessment in both a qualitative and quantitative manner. Using cut set analysis, fault trees can provide information on the paths of events that lead to the undesirable system event. For a thorough quantitative analysis, a fault tree analysis can be used to evaluate the probability of a detrimental event.

Qualitative Risk Assessment Using Cut Sets

Using this approach, a fault tree is analyzed by first determining what the minimal cut sets are. Cut sets are defined as a combination of events which cause the topmost event to occur. Using mathematical techniques and computing the probabilities of the individual cut sets of a system, the overall probability of the top-level event can be determined.

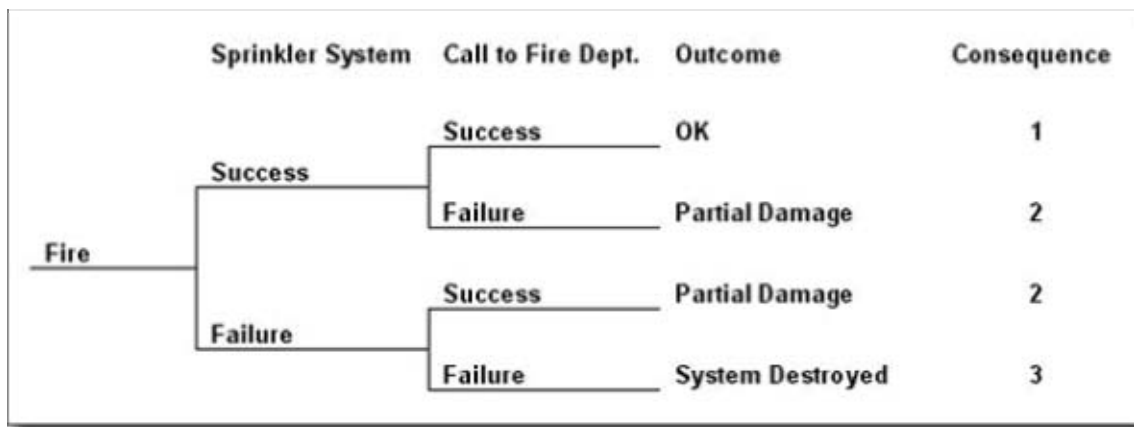
Quantitative Risk Assessment Using Probabilities

Quantitative analysis uses a variety of exact calculation methods to determine the likelihood of occurrence of the top-level event based on the failure or repair data entered for lowest-level events. Using various mathematical methods, the probability of the top level event can be computed based on the underlying probabilities of all the lower level events. Fault tree analysis tools automate this computation, which can be quite intensive depending on the scale of the fault tree.

Quantifying Risk with Event Trees

Event tree analysis is based on a binary tree diagram, with each set of branches indicating an event occurring or not occurring, or an item failing or not failing. Event trees are useful for assessing the consequences resulting from an undesired event, and have been used to assess the results of an accident or catastrophic event.

The following example of an event tree was constructed to analyze the possible outcomes of a system fire. The system has two components designed to handle this event: a sprinkler system and an automated call to the fire department. If the fire department is not notified, the fire will be mostly contained by the sprinkler system. If the sprinkler system fails as well, the system will be destroyed.



An Event Tree diagram used to analyze the outcomes of a system fire.

The event tree starts with the initiating event - an event which disrupts normal system operation. From the initiating event, the event tree displays the sequence of subsequent events which ultimately lead to overall system success or failure. The probabilities of the ending consequences can then be computed based on the probabilities of the events leading to up to it. Using this technique, you can employ risk reduction strategies for undesirable consequences which have the highest probabilities of occurring.

Quantifying Risk with Human Factors Risk Analysis

Human Factors Risk Analysis is a specific type of Process FMEA (HF PFMEA), which is used to assess the risk of human error. Human error is a significant factor in the design and operation of systems, and has measurable monetary and safety consequences. An HF PFMEA acknowledges that not only will equipment and software fail, but also that humans will make mistakes, either accidentally or by deviating from accepted policies and practices. Clearly an important element of risk assessment, human factors risk analysis is a continually growing field of interest in overall risk reduction strategies.

There are six steps in performing a human factors risk analysis which display similarity to standard PFMEAs:

1. Break down the process into discrete tasks.
2. Identify the human errors that may lead to system failure for each task.
3. Determine the worst-case effect of each error on the system.
4. Identify factors that may influence the likelihood of the error occurring.
5. Define barriers and controls to either prevent the error from occurring or mitigate its effect.
6. Perform a risk assessment of errors and their effect to determine how the risks are to be addressed.

For the final step of the process, two methods can be used for quantifying risk: a Risk Assessment Code (RAC) and a Risk Matrix.

Risk Assessment Code (RAC)

The RAC value is determined based on two factors of the worst-case effect of an error: 1) its severity, also known as mishap/hazard severity, and 2) its likelihood of occurrence, sometimes referred to as mishap/hazard probability. The RAC value is a numeric value based on a scale that varies by application and practicality. Common RAC scales range between 1 = high/critical and 5 = minor/negligible. Other RAC ranges, such as the example in MIL-HDBK-882D, use a larger scale of 1 through 20 with groupings of values 1-5 = high, 6-9 = serious, etc.

Risk Matrix

A Risk Matrix is based on the same risk analysis concept as the RAC, but takes this analysis a step further by creating a two-dimensional array that visualizes the relationship between severity and occurrence. The number of rows and columns in a risk matrix varies, with a common matrix being five-by-five.

To build the risk matrix you rank the likelihood of an effect and the severity of an effect. For a five-by-five matrix, the likelihood could range from 1 = very unlikely to 5 = very likely, and the severity could range from 1 = very low severity to 5 = very high severity. To make evaluation of the matrix easier, a color-coded prioritization is often used, with colors mirroring those of a traffic light. High risk values which must be eliminated or mitigated appear in red. Medium risk values are highlighted with yellow, indicating that barriers and controls must be applied to reduce the risk of the effect. Low risk values are marked with green to indicate an acceptable level.

| | | | | | | |
|----------------------|---|--------------------|----|----|----|----|
| Likelihood of Effect | 5 | 5 | 10 | 15 | 20 | 25 |
| | 4 | 4 | 8 | 12 | 16 | 20 |
| | 3 | 3 | 6 | 9 | 12 | 15 |
| | 2 | 2 | 4 | 6 | 8 | 10 |
| | 1 | 1 | 2 | 3 | 4 | 5 |
| | | 1 | 2 | 3 | 4 | 5 |
| | | Severity of Effect | | | | |

A Risk Matrix using three-color coding.

For more details about Human Factors Risk Analysis, you can read our prior *eFlash* feature article [System Risk: The Human Factor](#).

Conclusion

At the core, risk assessment strategies must employ some method of quantifying risk in order to be effective. There are several reliability methodologies which you can use to help you in your own risk management goals. The choice depends on the amount of information you have about your system, as well as the level of detail required in order to achieve your safety objectives. Whether you select FMEA, fault tree analysis, event tree analysis, or human factors risk analysis, you will have an effective tool to help you achieve your goals.

Relex Software Corporation offers a suite of analysis tools to support all your risk assessment needs. [Relex FMEA](#) is a fully featured FMEA/FMECA tool which supports the common published FMEA standards and enables you to customize your FMEA based on your requirements. [Relex Fault Tree](#) is a complete fault tree analysis (FTA) tool with powerful diagramming features, a wide range of gates and events, and a sophisticated calculation engine. [Relex Event Tree](#) provides comprehensive event tree analysis (ETA) and is integrated with Relex Fault Tree for seamless analyses. [Relex Human Factors Risk Analysis](#) (HFRA) provides a systematic approach for the evaluation and mitigation of risk due to human error. For more information, please visit the Relex Web site at www.relex.com.
