



Improved Modeling of Mechanical Failures Through Adoption of Use Factors

Chris O'Brien
Exida Consulting
Sellersville, PA 18960, USA
cobrien@exida.com

Keywords: safety instrumented system, mechanical component failure metrics, random failures, systematic failures, cyclical life testing, FMEDA, low demand applications, stress multipliers, use factors

Abstract

As industry adoption of the IEC 61508 [1] and IEC 61511 [2] functional safety standards spreads the need for accurate reliability data for equipment used in Safety Instrumented Systems (SIS) increases. Reliability data is needed for both electronic and mechanical devices. The methodology for determining failure rates for electronic equipment is fairly well accepted and applied the same can not be said for mechanical equipment. The methods utilized to generate failure rates for mechanical components vary dramatically in approach and outcome. These different methods can lead to significant differences when calculating the reliability of a safety instrumented function (SIF).

Methods utilized to determine mechanical reliability for components utilized in safety systems are reviewed and recommendations for the most appropriate methodology are given.

Introduction

Currently there are at least three diverse methods in use to calculate the failure metrics for mechanical components that are used as part of a SIS. These methods are;

1. analysis of field return data,
2. cyclical life testing (fatigue analysis) and
3. Failure Modes Effects and Diagnostic Analysis (FMEDA).

The shortcomings of utilizing field return data to calculate failure rates are well documented and will not be addressed in detail [3]. We will review the methodology of cyclical life testing and examine why applying this technique for SIS will almost always lead to optimistic reliability calculations. We will then introduce concepts that will improve the accuracy of FMEDA's when they are utilized for mechanical components.

To begin it is useful to review the failure types as defined by IEC 61508. IEC 61508-4 provides the definition for both random hardware failures and systematic failures. In the standard we find:

Random Hardware Failure

Failure occurring at a random time which results from one or more of the possible degradation mechanisms in the hardware.

Note 1 - There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising of many components occur at predictable rates but unpredictable (i.e. random) times.

Systematic Failures

Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factor.



In addition to these failure rates, the definition of Wear Out and Useful Life is important and will play an important role in our review of methods to determine mechanical failure rates.

Wear Out

The point at which a component or piece of equipment has been subjected to enough stress cycles that it is weakened to the point where its failure rate increases significantly.

Note - Since essentially all safety systems reliability calculations assume a constant failure rate, safety instrumented systems must be replaced before they reach this point.

Useful Life

The operational time interval between infant mortality failures and wear out failures on the bathtub curve where the failure rate of a device is relatively constant.

Mechanical Failure Modes

There are many factors that contribute to and determine the failure rate for a mechanical component. These factors include material selection, surface finish, corrosion, temperature, temperature cycling, vibration and loading. Some companies and certification agencies have maintained that random failures for a mechanical component do not exist. That in fact all failures of mechanical components are either systematic failures or are the result of fatigue. This statement may be theoretically true in an idealistic world but it is incorrect when applied to reliability calculations for functional safety and can be **dangerously misleading** to functional safety professionals who are not intimately familiar with mechanical failure modes.

The origins of fatigue analysis

Fatigue analysis in mechanical engineering has been studied for over 150 years. The topic first gained prominence in the 1800's due to the sudden failure of railroad car axles. The axles were made of ductile steel, but failed in a manner that was more typical of brittle materials. Upon investigation it was learned that the rotation of the axle resulted in the material being subjected to alternating tensile and compressive loads. These cyclic loads resulted in the propagation of cracks that acted to reduce the effective area of the axel cross section until the point where it could no longer support the load. At this time the axle would fail in a sudden and catastrophic manner, similar to a brittle material failure. We can call this type of loading macro loading, which represents the primary load(s) that the component is designed to transfer.

Mechanical components can also fail when micro loadings result in the weakening of the part to the point of failure. Examples of micro loading include temperature cycling, corrosion and vibration. Some will claim that these are examples of systematic failures and that a properly engineered and applied part will not be susceptible to these micro loads. It is important to note that these failure modes are identical to those that cause random failures in electronic components and are the "many degradation mechanisms" referred to in the definition of random hardware failure. The origin of these failures is a random flaw in the component that results in a point of stress concentration. When micro loads are applied to a component over an extended period of time, some portion of the population will fail. As such these random flaws lead to random failures.

Dangers of Using Cyclical Life Test Data to Calculate Failure Rates

Fatigue is only one of many failure modes and is most appropriately associated with the end of useful life, not as a measure of failure rates to be utilized in determining the reliability of safety instrumented systems. The importance of wear out depends on whether you are in a low demand or continuous demand application. In a continuous demand application such as machine safety there can be instances where the fatigue limit of the component is reached, however in low demand applications it should be nearly impossible to reach the wear out point of the component as the number of cycles over the mission time of the safety instrumented function should be an



extremely small number. Therefore cyclical testing results have little relationship to random failures in a low demand application.

Some of the reasons that cyclical life testing cannot determine random failure rates include:

- Some cyclic testing is not done until failure [4]. Those results are particularly inconclusive.
- Failure rates based on cyclic tests done until failure represent only those failures that are a result of the macro stresses that a component is subjected to and exclude failures that result from the culmination of micro stresses that are experienced by the component.
- Random hardware failure rates based on fatigue limits tend to result in extremely optimistic results for low demand applications. Since components used in a low demand application will see only a fraction of the cycles that a component would experience before it reaches end of life, the impact of failure rates based on cycles often is insignificant and can lead the designer to ignore true random failure modes.
- Low cycle failure modes are excluded. When a device is used in a low cycle mode, it may only be moved once a month or even once per decade. Applications such as this have additional challenges and failure modes. One such mode is cold welding of an elastomer to a metal component which can happen when the materials are left in contact for prolonged periods of time and not moved. Another failure mode excluded is bonding of components due to corrosion.
- Fatigue analysis can lead to poor decisions in material selection for components used in SIS. An example of this would be the selection of a carbon steel spring over a stainless steel spring. While a carbon steel spring will generally survive more cycles than a similar stainless steel spring, it is more susceptible to corrosion from water which typically will result in it having a shorter useful life and a higher random failure rate in a safety application.

FMEDA Methodology

If we had a complete understanding of all flaws that existed in each unique component and could predict with certainty the macro and micro stresses that the component would be subjected to, we could create the perfect model. This model would need to be adjusted for each component in each installation and we would expect it to yield application and environment specific results. However this approach is not possible and not practical. What we do have are analysis techniques that can be borrowed from electronics reliability engineering such as FMEDA [5, 6].

There are several sources for failure rates for mechanical components. This data can be utilized to create an FMEDA for a device that will be part of a SIF [7]. This initial FMEDA can be thought of as the baseline analysis, one that represents a failure rate that would be expected when the device is subjected to normal occurring or average micro stressors. It has been observed that there can be deviations from the predicted failure rates and that these deviations can be correlated with increased failure rates for specific components due to one or more micro stressors. This increased stress level can be modeled as stress multipliers and applied to the components within the device that are susceptible to those stressors. Stress multipliers that are frequently encountered include:

- Corrosion
- Elevated Temperature
- Cycling Temperature
- Low Frequency Vibration
- High Frequency Vibration



It is convenient to think of these stress multipliers as Use Factors and to apply them to mechanical component applications where they can reasonably be expected to occur. The derived failure rate for a component would be modeled as:

$$\lambda_{\text{derived}} = \lambda_{\text{base}} + (F_c * \lambda_{\text{base}}) + (F_{te} * \lambda_{\text{base}}) + (F_{tc} * \lambda_{\text{base}}) + (F_{vif} * \lambda_{\text{base}}) + (F_{vhf} + \lambda_{\text{base}})$$

In addition to the Use Factors, care must be taken to identify any additional failure modes that may be present in a device that will be static for an extended period of time. As discussed, one such mode is cold welding of two dissimilar materials. This failure mode could reasonably be foreseen in a solenoid valve that was energized and never cycled during its mission time. A preferred method to increasing the failure rate for the device is to move the valve periodically so that this cold welding does not occur. In addition to preventing this failure mode, the periodic cycling of the valve can provide additional diagnostic coverage and improve the reliability of the SIF. This requirement, if needed to achieve safety, should be clearly documented in the safety manual of the product.

Connecting Theory with Operations

Actual data from multiple plants show that the failure rates of pressure relief valves of similar design vary widely. Some but not all of this variation can be accounted for in the difference in operational and maintenance procedures. Upon examination of the failure data it was discovered that the variation in failure rates correlated with the location of pressure relief valves manufactured with carbon steel springs. It was found that the higher failure rates occurred when the pressure relief valves with carbon steel springs were located outdoors with no protection from rain.

The increase in failure rates was the result of corrosion of the spring washers to the valve stems. Some might argue that this is a systematic failure, but this objection doesn't hold up for three reasons. Firstly, it is impractical to say that no devices with carbon steel springs can be used outdoors. Secondly although the failure rates were meaningfully higher for pressure relief valves with carbon steel springs, they were not elevated to the point where you would disallow the use of these valves in outdoor applications. Thirdly the pressure relief valves functioned properly, i.e. within specification, up to the point that the (random) failure occurred, unlike a systematic failure which would basically prevent the relief valves from ever functioning properly. As a result, a Use Factor for corrosion is the most appropriate way to model the presence of stresses introduced by corrosion that are above what were captured in the baseline FMEDA.

Conclusion

The field of reliability engineering as applied to safety instrumented systems continues to mature. As more focus is placed on mechanical components and devices the techniques to model and analyze them improve. While life testing is an important activity in the design of reliable products it has several significant shortcomings when it is used to model devices used in low demand safety applications. It is recommended that the FMEDA technique be used and that additional consideration be given to identifying low cycle failure modes and to the appropriate application of Use Factors.

REFERENCES

1. IEC 61508, Functional Safety of electrical / electronic / programmable electronic safety-related systems, 2000.
2. ANSI/ISA SP84.00.01 – 2004 (IEC 61511 Mod.), Application of Safety Instrumented Systems for the Process Industries, Raleigh, NC, ISA, 2004.
3. Goble, W. M. and Siebert, J., "Field Failure Data – the Good, the Bad and the Ugly," exida, Sellersville, PA, USA June 2007.



4. "TUV Certificate," Report No. S 194/02, 18.02.2003, Unternehmensgruppe TUV Rheinland/Berlin-Brandenburg, 2003
5. W. M. Goble and A. C. Brombacher, "Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems," Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999.
6. Goble, W. M., "Accurate Failure Metrics for Mechanical Instruments," Proceedings of the IEC61508 Conference, Germany: Augsburg, RWTUV, January 29-30, 2003
7. J. V. Bukowski, W. M. Goble, "Development of a Mechanical Component Failure Database," Proceedings 2007 Annual Reliability and Maintainability Symposium, Orlando, FL, January 2007