Useful Lifetime of a Machinery Safety Control System

Introduction

When a safety function is selected as the risk reduction for a hazard, a safety control system (SCS) is engineered and implemented to perform that function. There are two machinery application standards which engineers can utilized to design their safety control system. There is IEC 62061:2005 which is used to determine the Safety Integrity Level (SIL) for electrical, electronic and programable electronic systems. And there is ISO 13849-1 which is used to determine the Performance Level (PL) of non-complex parts of the control system such as, electrical, pneumatic, hydraulic or safety rated devices.

Both IEC 62061 and ISO 13849-1 base their hardware integrity requirements on a statistical analysis of component failure. The reliability formulas used for this analysis require an assumption of time for when the complete system or parts of the system will be replaced. This article will explain these aspects of time related to component reliability and why the components that make up a safety control system must be replaced or refurbished after the components reach their published useful life, typically 20 years.

Random Failure Rate

The hardware integrity aspect of a SIL or PL is the determination of the random hardware failure rate of the safety components in the control system. This failure rate is called the probability of dangerous failure per hour (PFHD). Statistically, this is a question of "when, not if" there will be a random hardware failure in a population of safety system components.

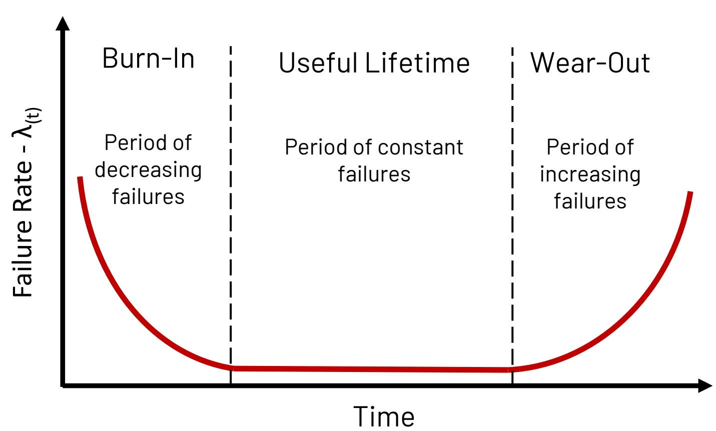
The analysis of safety component failure and the calculation of PFH originated in IEC 61508 which is the general functional safety standard for the certification of electronic devices such as safety PLC. The PFH calculations and other requirements of IEC 61508 are complex and impractical for a designer to apply to machinery control system design. As a result, both IEC 62061 and ISO 13849-1 were developed as a simplified approach for machinery safety applications.

Component Reliability

Since awareness of component failure is the basis of the PFHD calculations, a discussion of component reliability is warranted.

A good illustration of the life of a safety component can be seen in the reliability bathtub curve. When a safety component is put into service, it can have a high but exponentially decreasing failure rate which is called burn-in. Towards the end of its service, there is the point in time when a safety component will have an exponentially increasing failure rate which is called wear-out.

Reliability Bathtub Curve



The useful lifetime is when burn-in failures have been corrected and wear-out failures have not yet begun. Most important, during this time the failure rate remains relatively constant.

The reliability calculation methods in IEC 62061 and ISO 13849-1 are based upon this assumption of a constant failure rate. Therefore, for the PFHD calculations to remain valid, a safety component must only be applied within its useful lifetime. The following excerpt from IEC 61508-2 reinforces this concept by stating that unless useful lifetime of an electronic safety component is considered, any PFHD calculations are **meaningless**.

> "Although **a constant failure rate** is assumed by most probabilistic estimation methods this only **applies provided that the useful lifetime of elements is not exceeded. Beyond their useful lifetime** (i.e. as the probability of failure significantly increases with time) **the results of most probabilistic calculation methods are therefore meaningless. Thus any probabilistic estimation should include a specification of the elements' useful lifetimes.**" (IEC 61508-2:2010, Clause 7.4.9.5; Note 3)

Terms Used in the Standards

The primary reason that time and component reliability has confused designers is because ISO13849-1 and IEC62061 cover a broad range of technologies and use different terms to describe the aspects of time in the PL and SIL calculations.

Mission Time

The term Mission Time is defined in ISO 13849-1 as the period of time covering the intended use of the Safety Control System (ISO 13849-1:2015, 3.1.28). Mission time is about undetected random failures and is a chosen design parameter in the PFHD calculation. The simplified reliability formulas used in ISO 13849-1 are based upon an assumed mission time of 20 years.

Operation Time ($T10_D$)

The term Operation Time ($T10_D$) as used in the context of ISO 13849-1, Annex C is about component wear out. $T10_D$ is a physical property of a safety component which is dependent on how often the component is cycled. Requiring preventative replacement of a safety component with a $T10_D$ less than 20 years is permissible. If scheduled replacement is not practical, then ISO 13849-1 limits the performance level calculation validity to the lowest value of mission time or operational time ($T10_D$).

Proof Test Interval

IEC 62061 references the proof test interval (T_1) as a variable of time in the PFH_D calculations. The complexity of the PFH_D calculations vary based upon the subsystem design. One way that IEC 62061 has simplified these equations is by stating that (T_1) should be equal to the proof test Interval or useful lifetime of the component. In the Foreword of IEC 62061, the proof test interval is used synonymously with the ISO 13849-1 mission time. Therefore, the 20-year mission time is the recommended assumption in IEC 62061.

Terminology Relationship

The following relationships between the terms: useful lifetime, operation time, mission time and proof test interval can be used to simplify this topic.

- ***Mission Time ≤ Proof Test Interval:*** *If the mission time of a safety component is less than or equal to the proof test interval, then there is no need to proof test any safety component before replacing it.*
- ***Useful Lifetime ≥ Mission Time:*** *If the useful lifetime of a safety component is greater than or equal to the mission time, then the assumption of a constant failure rate for the SIL/PL calculation is valid.*
- ***Operation Time ($T10_D$) = Useful Lifetime:*** *These two terms are derived from different standards and apply to different technologies. But both terms relate to the concept of operating the safety component within its useful lifetime of the reliability curve.*

Conclusion

IEC 62061 and ISO 13849-1 use different terms for the aspect of time in their safety reliability calculation. However, to remain aligned, 20-years is the default assumption for useful lifetime. Safety system designers and users must be aware of this 20-year timeframe to proactively maintain the original safety system design reliability. The goal is to manage the replacement of the safety components, rather than running to the point of wear-out when the probability of dangerous failure is statistically greatest.

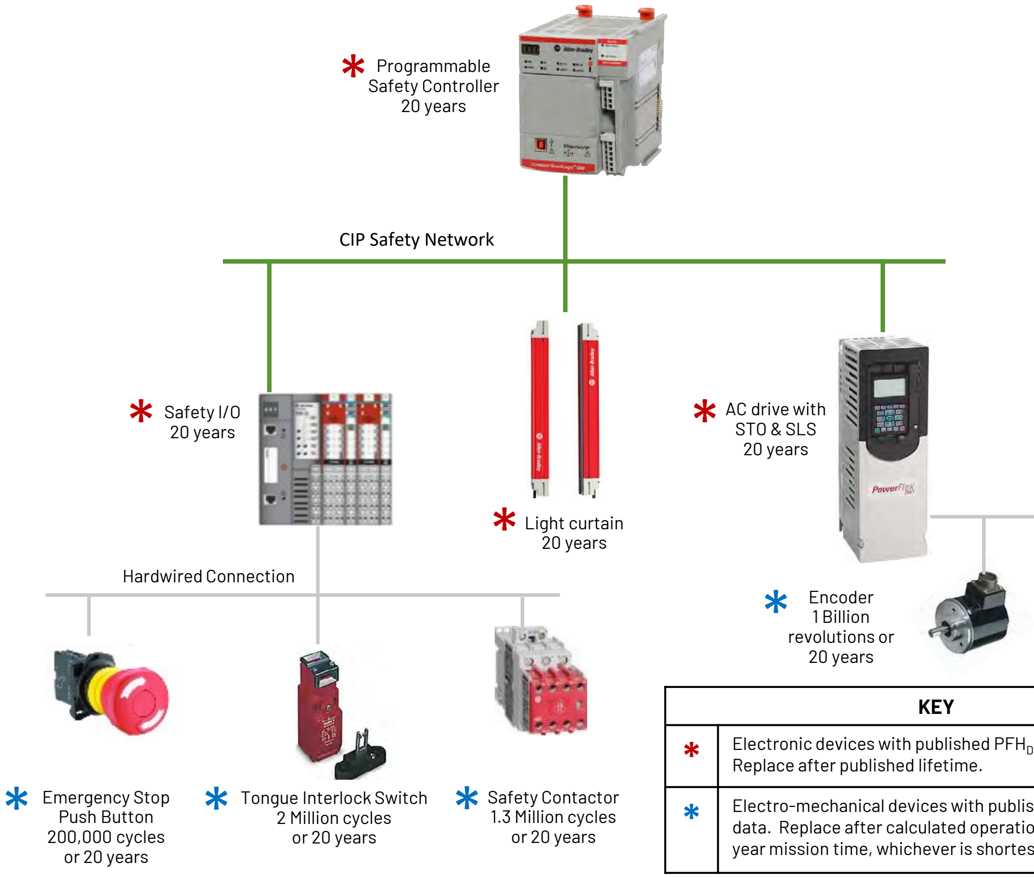
Frequently Asked Questions

Why should I care? I have seen industrial safety components last longer than 20 years and have not had a failure yet.

As the bathtub curve illustrates, it is just a matter of time. The longer a safety component has been in use, the failure rate is exponentially going up. While it is true that some safety components can last longer than 20 years, it is also true that they can fail before 20 years. Nobody can predict when a safety component will fail due to a random hardware failure. The reliability calculations in both IEC 62016 and ISO 13849-1 are based upon well-known concepts of component reliability and predictive modeling. This statistical analysis requires a default assumption of useful life. Once that timeframe is reached, the calculations are no longer valid.

Do I need to replace all safety control system components after 20 years?

Yes, the safety components must be replaced after 20 years for the safety performance calculations to remain valid. Certain high wear electromechanical components (i.e. contactors, valves, or switches) may need to be replaced before the 20-year timeframe. Below is a typical GuardLogix architecture illustration which shows what safety components may need to be replaced or refurbished.



KEY	
*	Electronic devices with published PFH_D reliability data. Replace after published lifetime.
*	Electro-mechanical devices with published $B10_D$ reliability data. Replace after calculated operation time ($T10_D$) or 20-year mission time, whichever is shortest.

Can I extend the life of my safety controller by doing my own Proof Test or FMEDA?

Proof testing and FMEDA are not tests that a safety control system engineer can design with 100% effectiveness. These analysis techniques are performed by the component designers during the development process of the safety controller. The goal of proof testing is to identify all dangerous undetectable failures. However, if the failures are undetectable, how does one test for them? Typically, these tests are run outside the typical diagnostic test and required deeper understating of potential failure modes. Similarly, a failure modes, effects, and diagnostic analysis (FMEDA) is a detailed systematic analysis technique of the hundreds of electronic components that make up the safety controller. These techniques are too complicated for a typical safety application engineer to perform which is why replacement after the published useful life or mission time is required.

What is the key take-away?

If you are using IEC 62061 or ISO 13849-1 to apply a SIL or PL to your safety control system, then be aware of the published mission time for each element/component which is typically 20 years. Proactively plan for the replacement of the safety control system components rather than running them to the point of failure. Include the component replacement requirements in the machinery documentation and provide instructions so the user can manage this phase of the machinery lifecycle appropriately.

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608, FAX: (65) 6510 6699
UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800, Fax: (44)(1908) 261-917

Publication SAFETY-WP040A-EN-P - June 2023