SIL-Degradation for Existing (Legacy) Safety Systems: 4 factors that affect SIL Performance

PipeSystemConsult GmbH Blog 4 - May 2018

For existing (legacy) safety systems approaching the 10-year age mark, there are four significant issues that Operators should be aware of, in order to avoid SIL-Degradation of their safety instrumented systems (SIS).

1. Mission-Time

The Mission Time (MT) is the time interval for which a SIS should operate without requiring major refurbishment or complete replacement. In VDI/VDE 2180-3, ‚Mission-Time' (T2) is defined more specifically as the interval after which all elements have to be tested with complete proof test coverage (CPT=100%); in practice this likely means complete refurbishment or replacement. MT could be chosen based on the useful life of the main devices, such as safety logic solver (‚ESD system'). A typical value of MT is 15 – 20 years.

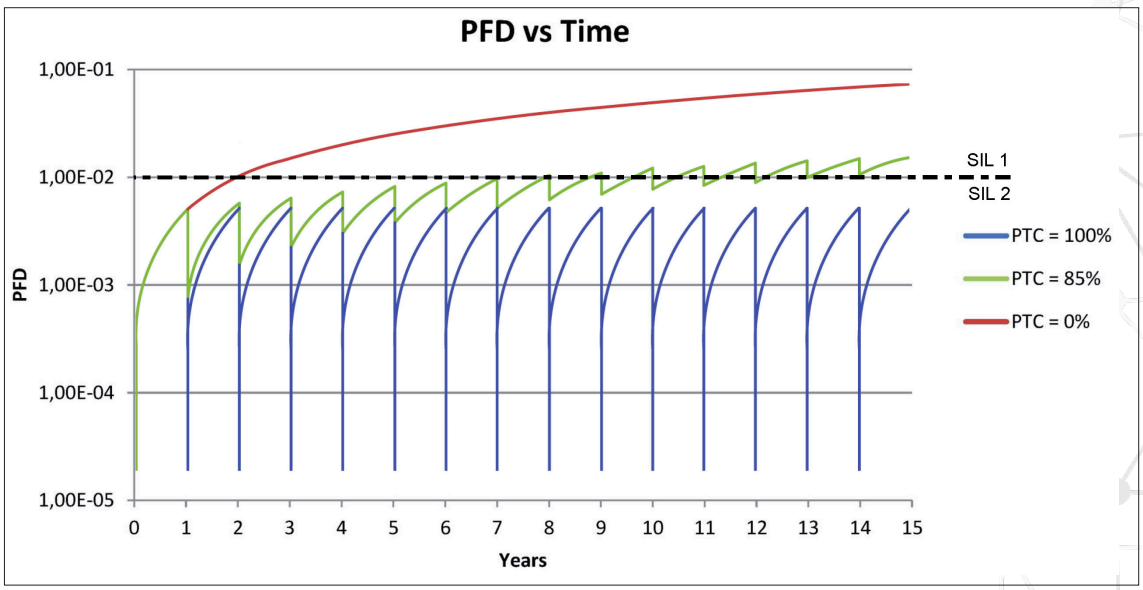
The MT should be defined in the Safety Requirements Specification (SRS) in accordance with IEC 61511, §10 (VDI/VDE 2180-2, §6). For legacy systems, this value might not be clear and it may be tempting for Operators to push this value out in order to delay OPEX. However, even for plant that has not reached the MT limit, the effect on SIL-rating when combined with incomplete proof-test coverage can be significant, as shown below.

2. Proof Test Coverage (C_{PT})

Proof test coverage (C_{PT}) (deutsch: Prüftiefe) is the fraction of dangerous undetected failures that can be revealed by regular testing. When considering achieved SIL ratings, C_{PT} has an effect on PFDavg over the Mission Time as per the simplified formula shown below:

$$PFD_{AVG} = C_{PT}\ 1_D\ TI/2 + (1\text{-}C_{PT})\ 1_D\ MT/2$$

This can be demonstrated graphically on this chart.



SIL-Degradation (PFD vs Time)

PipeSystemConsult GmbH
Adelheidstrasse 12
80798 Munich, Germany

Telefon: +49 (0)89 326 021 36
Fax: +49 (0)89 374 135 23
Email: info@pipesyscon.com

PipeSystem Consult GmbH

The blue line shows how PFD is ‚reset' after the regular proof test, e.g., every 12 months, assuming a theoretical coverage of 100%, i.e., all potential failures detected. At the other extreme, the red line shows how PFD increases logarithmically if no proof testing is carried out at all. The green line shows a realistic C_{PT} of 85%; even in this case, the PFD increases over time, such that by the end of Mission Time (in this case 15 years), the PFDavg for the hypothetical SIS shown may have crossed the threshold between SIL-2 and SIL-1 (SIL-Degradation). Therefore, as mentioned above, the MT and C_{PT} in combination can have a significant effect on achieved SIL-rating over plant lifetime.

So what are the actual achievable C_{PT}'s in practice? Exida, for instance, has published data which shows that the C_{PT} for an actuator/valve assembly can vary from 57-99%, depending on whether a partial or full stroke test is performed, in best case combined with monitoring of seat leakage under operating conditions. In order to make a realistic estimate of actual C_{PT}, Operators should compare their documented proof-test procedures with Manufacturer's published data (as per Safety Manual) and / or industry sources such as Exida's SERH database. The next release of NAMUR NE 106 (planned for 2018) will provide C_{PT} bands for generic proof test activities, so this should give additional guidance.

3. Useful Life

The calculation of PFD is based on the assumption of constant failure rate during the so-called ‚useful life' of a component. The useful life is derived from the 'bath-tub' model and considers that wear-out conditions eventually lead to increasing and unpredictable failures. Manufacturers define the useful life based on statistical analysis of field-installed devices, or alternatively this may be calculated by theoretical methods such as FMEDA.

Useful life may be surprisingly short. For instance, one Manufacturer defines the useful life of a solenoid valve as between 3 - 10 years, depending on power consumption and fail-safe configuration (e.g. de-energise to trip). Useful life can be further reduced by harsh operating environment or process conditions.

The main reason to be aware of useful life, is that once this is exceeded for a single component of a safety loop, then the entire basis for SIL-calculation is no longer valid, since the assumption of constant failure rate no longer holds. Plant maintenance programs should maintain a record of useful life of safety-critical components, such that these can be replaced or refurbished in time to avoid SIL-Degradation.

PipeSystemConsult GmbH
Adelheidstrasse 12
80798 Munich, Germany

Telefon: +49 (0)89 326 021 36
Fax: +49 (0)89 374 135 23
Email: info@pipesyscon.com

PSC | PipeSystem Consult GmbH

4. Actual demand/failure rate

Finally, the HAZOP / SIL / LOPA analysis carried out at the start of a Project will have made certain assumptions for demand and failure rate. These are often based on Operator experience of similar plant or industry standard values. IEC 61511-1 §16.2 requires Operators to collect actual operating data to ensure that original risk analysis assumptions are still valid (see also VDE/VDI 2180-1 and Namur NE 93 / 130).

For a Plant that has been in operation for 10 years, there should be sufficient operating data available in order to confirm or update HAZOP / LOPA assumptions. Such data can also support 'Proven-In-Use' evaluations, where manufacturer certification is missing or outdated. In many cases, evaluation of such data can work in Operator's favour, since demonstration of lower demand rate and/or better than assumed equipment failure rates may allow reduction of SIL-requirements. On the other hand, an increased frequency of trips or dangerous events may require installation of additional protections or improvement in the integrity level of existing SIFs.

Here are the questions that Operators of existing plant should ask:

-What is my Mission Time?

-What is the actual proof test coverage of my regular safety loop testing?

-Have any of the components in my SIL-Loops exceeded their useful life?

-Do I have operating data to back up the assumptions of demand and failure rate?

PSC provides audit and assessment services according to IEC 61511 to identify gaps in FSM documentation and operating practice that might lead to SIL-degradation for legacy plant.

PipeSystemConsult GmbH
Adelheidstrasse 12
80798 Munich, Germany

Telefon: +49 (0)89 326 021 36
Fax: +49 (0)89 374 135 23
Email: info@pipesyscon.com

PSC | PipeSystem Consult GmbH

Hier sind nun die Fragen, die Betreiber von bestehenden Anlagen sich stellen sollten:

-Wie hoch ist meine Einsatzzeit?

-Was ist die eigentliche Prüftiefe meiner Wiederholungsprüfung?

-Haben die Komponenten in meinen Sicherheitsschleifen ihre Nutzungsdauer überschritten?

-Verfüge ich über Betriebsdaten, um die Annahmen der Anforderungs- und Ausfallrate zu stützen?

PSC bietet Audit- und Bewertungsdienstleistungen gemäß DIN EN 61511, um Lücken in der FSM-Dokumentation und Betriebspraktiken zu identifizieren, die zu einer „SIL-Degradation" führen können.

PipeSystemConsult GmbH
Adelheidstrasse 12
80798 Munich, Germany

Telefon: +49 (0)89 326 021 36
Fax: +49 (0)89 374 135 23
Email: info@pipesyscon.com

PSC | PipeSystem Consult GmbH