

Safety Integrity Level

Useful lifetime of SIL-capable instruments



Useful lifetime

To ensure that a safety instrumented system (SIS) can perform its safety function with the required reliability the useful lifetime of the constituent parts must be taken into account. For each element there will usually be a useful lifetime given in the manufacturer's functional safety manual. In other cases the functional safety manual may just point to the guidance found in IEC 61508-2 and this should be used to define a useful lifetime of equipment.

According to section 7.4.9.5 of IEC 61508-2:2010 a useful lifetime, based on experience should be assumed.

More practical guidance is given in the accompanying notes:

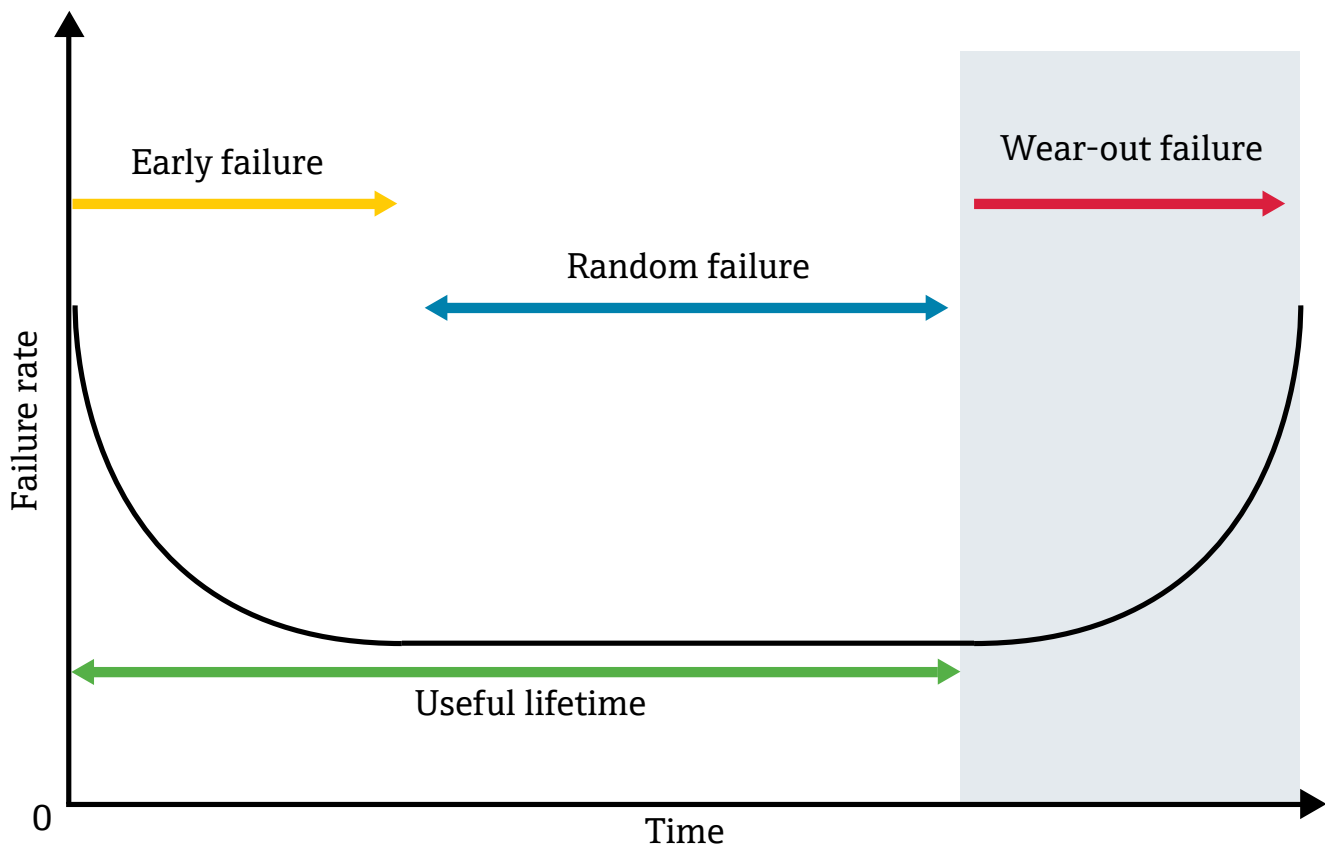
According to section 7.4.9.5 note 3 of IEC 61508-2 experience has shown that the useful lifetime often lies within a range of 8 to 12 years.

Care should be taken where a manufacturer promotes extended lifetimes as these will often need to be reduced depending on the environmental conditions to which the equipment is subjected.

The probability of failure on demand (PFD) of a constituent part of a SIL-rated SIS uses the failure rate data for individual electronic components as part of the calculation. The familiar 'bath tub' curve applies here where for the major parts of their useful life components have a known failure rate. After a certain time the failure rate will increase due to aging of components.

A.11.5.2.1 of IEC61511-2:2016 - The useful lifetime is the period of time, in which the failure rate of a device is extensively constant. The probabilistic calculation of the overall PFDavg of the SIS (which should satisfy the SIL requirement for each SIF implemented by the SIS) is based on these failure rates. After the end of the useful lifetime the failure rates can rise gradually, e.g. by aging.

Once the useful lifetime is reached then the PFD values supplied by the manufacturer are no longer valid, as such no meaningful evaluation of the suitability of the equipment to perform its safety function can be made.



Functional safety management plan

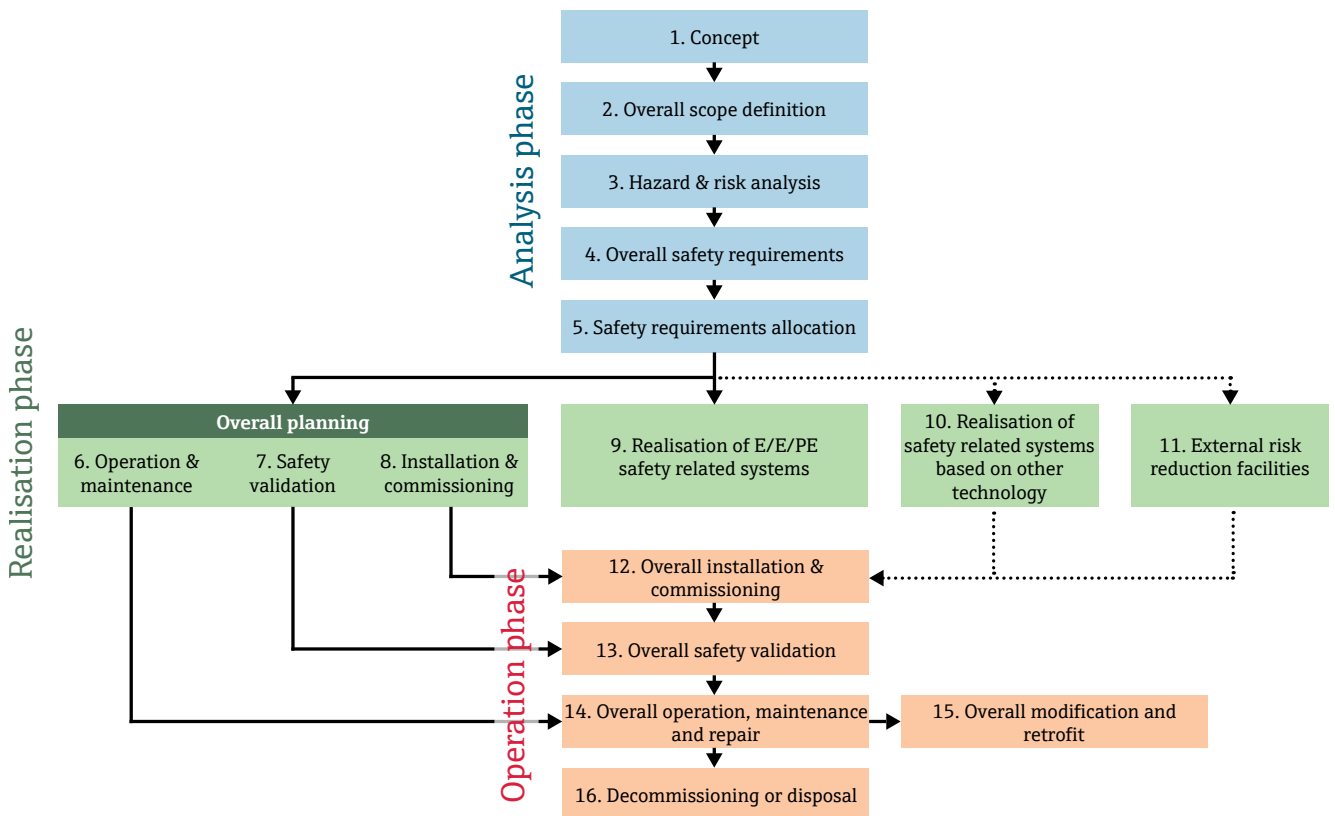
Within a functional safety management plan the need for replacement of equipment should be addressed and planned as part of the maintenance activities of the safety instrumented function (SIF).

A.5.2.5.1 The intent of 5.2.5.1 of IEC 61511-1:2016 is to ensure that effective management procedures are in place to:

- Ensure that all recommendations resulting from hazard analysis, risk assessment, other assessment and auditing activities, verification and validation activities are satisfactorily resolved.
- Determine that the SIS is performing in accordance with its safety requirements specification (SRS) throughout its operational lifetime.

IEC61508 gives guidance on lifecycle planning and the useful lifetime of equipment should be addressed as part of stage 6 'Overall operation and maintenance planning' within the realisation phase. Replacement of equipment would be covered by lifecycle stage 14 'Overall operation, maintenance and repair' in the operational phase.

Often the SIS can be maintained by replacement of equipment with identical items, but where this is not possible due to obsolescence it will be necessary to refer to the FSM lifecycle stage 15 'Overall modification and retrofit' and revisit the realisation section.



UK

Endress+Hauser Ltd
Floats Road
Manchester
M23 9NF

Tel: 0161 286 5000
Fax: 0161 998 1841
info@uk.endress.com
www.uk.endress.com