4. SIL VERIFICATION METHODOLOGY

ACNCOA001767 Digitally signed by ACNCOA001767 Date: 2020.02.06 11:01:46 +01'00'

4.1 Overview

The required risk reduction is determined during SIL Classification, representing the reliability specification on the SIF in order to achieve acceptable level of risk. The IEC61508 and IEC61511 standards provide procedures and requirements to achieve those risk reductions. Those requirements include Average Probability of Failure on Demand (PFDavg) or Probability of Failure per Hour (PFH) calculation, and redundancies demonstration, in the form of Hardware Fault Tolerance (HFT) assessment.

Both requirements must be complied with to achieve the SIL target, otherwise, appropriate modifications should be made. The following section provides a detailed explanation of both requirements.

4.2 Average Probability of Failure on Demand (PFDavg)

As specified in IEC61508 for SIL Classification process, a risk reduction target in the form of Average Probability of Failure on Demand (PFDavg) is determined during SIL Classification. In order to comply with the standard, the interlock (Safety Instrumented System or 'SIS') must be more reliable than the required PFDavg (or RRF, which is the mathematical reciprocal of PFDavg). PFDavg represents the probability that the interlock/SIS will fail to function when required. Probability of failure for each component level (i.e. sensor level, logic solver level and final control element level) are calculated individually and summed for the interlock to obtain Total PFDavg.
Table 1 shows the required Total PFDavg for each interlock/SIS with respect to SIL ranking.
It can be seen that the PFDavg requirements correspond to a maximum acceptable number of failures for a certain number of demands for each SIL. For example, a 10^{-1} PFDavg for SIL1 corresponds to less or equal to 1 failure every 10 demands, and 10^{-2} PFDavg for SIL2 corresponds to less or equal to 1 failure every 100 demands.

Table 1: Required PFDavg for SIL Rankings

Safety Integrity Level (SIL)	Target PFDavg	Risk Reduction Factor (RRF)
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤100
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤1000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to ≤10000
4	$\geq 10^{-5}$ to $<10^{-4}$	>10000 to ≤100000

For demand mode IPFs the achieved PFD = PFD(SE) + PFD(LS) + PFD(FE) shall be lower than 70 % of the higher PFD limit required for the SIL of the IPF . If this is not the case, test intervals, architecture or function components shall be changed so that the PFD is sufficiently reduced.

4.3 Hardware Fault Tolerance (HFT)

For Architecture Constraint assessment, this SIL Verification Study will use dangerous fault tolerance as depicted in chapter 6.2 table 4 of DEP 32.80.10.10 2014. However as per master tags in

4. SIL VERIFICATION METHODOLOGY

ACNCOA001767 Digitally signed by ACNCOA001767 Date: 2020.02.06 11:01:46 +01'00'

4.1 Overview

The required risk reduction is determined during SIL Classification, representing the reliability specification on the SIF in order to achieve acceptable level of risk. The IEC61508 and IEC61511 standards provide procedures and requirements to achieve those risk reductions. Those requirements include Average Probability of Failure on Demand (PFDavg) or Probability of Failure per Hour (PFH) calculation, and redundancies demonstration, in the form of Hardware Fault Tolerance (HFT) assessment.

Both requirements must be complied with to achieve the SIL target, otherwise, appropriate modifications should be made. The following section provides a detailed explanation of both requirements.

4.2 Average Probability of Failure on Demand (PFDavg)

As specified in IEC61508 for SIL Classification process, a risk reduction target in the form of Average Probability of Failure on Demand (PFDavg) is determined during SIL Classification. In order to comply with the standard, the interlock (Safety Instrumented System or 'SIS') must be more reliable than the required PFDavg (or RRF, which is the mathematical reciprocal of PFDavg). PFDavg represents the probability that the interlock/SIS will fail to function when required. Probability of failure for each component level (i.e. sensor level, logic solver level and final control element level) are calculated individually and summed for the interlock to obtain Total PFDavg.
Table 1 shows the required Total PFDavg for each interlock/SIS with respect to SIL ranking.
It can be seen that the PFDavg requirements correspond to a maximum acceptable number of failures for a certain number of demands for each SIL. For example, a 10^{-1} PFDavg for SIL1 corresponds to less or equal to 1 failure every 10 demands, and 10^{-2} PFDavg for SIL2 corresponds to less or equal to 1 failure every 100 demands.

Table 1: Required PFDavg for SIL Rankings

Safety Integrity Level (SIL)	Target PFDavg	Risk Reduction Factor (RRF)
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤100
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤1000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to ≤10000
4	$\geq 10^{-5}$ to $<10^{-4}$	>10000 to ≤100000

For demand mode IPFs the achieved PFD = PFD(SE) + PFD(LS) + PFD(FE) shall be lower than 70 % of the higher PFD limit required for the SIL of the IPF . If this is not the case, test intervals, architecture or function components shall be changed so that the PFD is sufficiently reduced.

4.3 Hardware Fault Tolerance (HFT)

For Architecture Constraint assessment, this SIL Verification Study will use dangerous fault tolerance as depicted in chapter 6.2 table 4 of DEP 32.80.10.10 2014. However as per master tags in