c) a burn-in test;

d) a dedicated control set as part of the control plan; and

e) assignment of safety-related special characteristics.

9.4.1.3 This requirement applies to ASIL C and D of the safety goal. A hardware part residual fault, with a diagnostic coverage (with respect to residual faults) lower than 90 %, shall only be considered acceptable if an argument for its sufficiently low probability of occurrence is provided by one of the following options:

a) dedicated measures are taken (NOTE 2 in 9.4.1.2 lists examples of dedicated measures), or

b) for a safety goal ASIL D, the following criteria are satisfied:

- a conservative data source is used;
- only a small portion of the failure rate (e.g. one particular failure mode) can violate the safety goal; and
- the resulting residual fault failure rate is smaller than one-tenth of the value corresponding to failure rate class 1 (according to 9.4.3.3);

c) for a safety goal ASIL C, the following criteria are satisfied:

- a conservative data source is used;
- only a small portion of the failure rate (e.g. one particular failure mode) can violate the safety goal; and
- the resulting residual fault failure rate is smaller than one-tenth of the value corresponding to failure rate class 2 (according to 9.4.3.3).

NOTE 1 Regarding this requirement, a microcontroller, an ASIC, or similar SoC can be treated as hardware parts.

NOTE 2 The proportion of safe faults of the hardware part can be considered when determining the coverage of the safety mechanisms. In this case the calculation of the coverage is done analogously to the calculation of the single-point fault metric, but at the hardware part level instead of at the item level.

9.4.1.4 This requirement applies to ASIL (B), C, and D of the safety goal. The failure rates for hardware parts used in the analyses shall be estimated in accordance with 8.4.3.

9.4.2 Evaluation of Probabilistic Metric for random Hardware Failures (PMHF)

9.4.2.1 This requirement applies to ASIL (B), C, and D of the safety goal. Quantitative target values of requirements 9.4.2.2 or 9.4.2.3 shall be expressed in terms of average probability per hour over the operational lifetime of the item.

NOTE 1 Failure rate and average probability of failure per hour over the operational lifetime of the item are different values even if they share the same unit.

NOTE 2 Operational lifetime only includes the operating hours.

9.4.2.2 This requirement applies to ASIL (B), C, and D of the safety goal. Quantitative target values for the maximum probability of the violation of each safety goal at item level due to random hardware failures as required in ISO 26262-4:2018, 6.4.5, shall be defined using one of the sources a), b), or c) of reference target values, as outlined below:

a) derived from Table 6,

b) derived from field data from a similar well-trusted design, or

© ISO 2018 – All rights reserved

c) derived from quantitative analysis techniques applied to a similar well-trusted design using failure rates in accordance with 8.4.3.

NOTE 1 These quantitative target values derived from sources a), b), or c) do not have an absolute significance but are useful for comparing a new design with existing ones. They are intended to make available design guidance as described in 9.1 and to make available evidence that the design complies with the safety goals.

NOTE 2 Two similar designs have similar functionalities and similar safety goals with the same assigned ASIL.

NOTE 3 Table 6 is typically chosen when no other source is available to determine the random hardware failure target value.

NOTE 4 The values in Table 6 are intended for items composed of a single system (e.g. Engine Management System, Electronic Stability Control System, Electric Power Assisted Steering System, Airbag Restraint System).

NOTE 5 The target values given in Table 6 are consistent with the use of handbook data, which are recognised as being conservative. If the evaluation of safety goal violations due to random hardware failures is done based on statistical data (e.g. from the field), the target values given in Table 6 can be adapted to avoid an artificial simplification in achieving the target values.

Table 6 — Possible source for the derivation of the random hardware failure target values

ASIL	Random hardware failure target values
D	$<10^{-8}$ h^{-1}
C	$<10^{-7}$ h^{-1}
B	$<10^{-7}$ h^{-1}
NOTE The quantitative target values described in this table can be tailored as specified in 4.2 to fit specific uses of the item (e.g. if the item is able to violate the safety goal for durations longer than the typical use of a passenger car).	

9.4.2.3 This requirement applies to ASIL (B), C, and D of the safety goal. When an item consists of several systems, the derived target value of requirement 9.4.2.2 may be directly allocated to each system composing the item. This can be applied, as long as each of these systems has the potential to violate the same safety goal and the corresponding item target value is not increased by more than one order of magnitude.

NOTE 1 The possibility described in requirement 9.4.2.3 can, for example, be used for legacy systems, that are involved in a new higher level functionality (e.g. new ADAS using Engine Management System, Electronic Stability Control System, Electric Power Assisted Steering System or Airbag Restraint System), and that had achieved the same safety goal in previous developments.

EXAMPLE If an ASIL D safety goal is allocated to an item comprised of several systems (up to ten), each of which has the potential to violate that safety goal, the target value of 10^{-8}/h can be allocated to each system.

NOTE 2 An example of a PMHF budget assignment, for an item consisting of two systems, is given in Annex G.

9.4.2.4 This requirement applies to ASIL (B), C, and D of the safety goal. A quantitative analysis of the hardware architecture with respect to the single-point, residual, and multiple-point faults shall provide evidence that target values of requirements 9.4.2.2 or 9.4.2.3 have been achieved. This quantitative analysis shall consider:

a) the architecture of the item;

b) the estimated failure rate for the failure modes of each hardware part that would cause a single-point fault or a residual fault;

c) the estimated failure rate for the failure modes of each hardware part that would cause a multiple-point fault;

d) the diagnostic coverage of safety-related hardware elements by safety mechanisms; and

e) the exposure duration in the case of multiple-point faults.

© ISO 2018 – All rights reserved