NOTE 3 An example of calculation of "single-point fault metric" is given in Annex E.

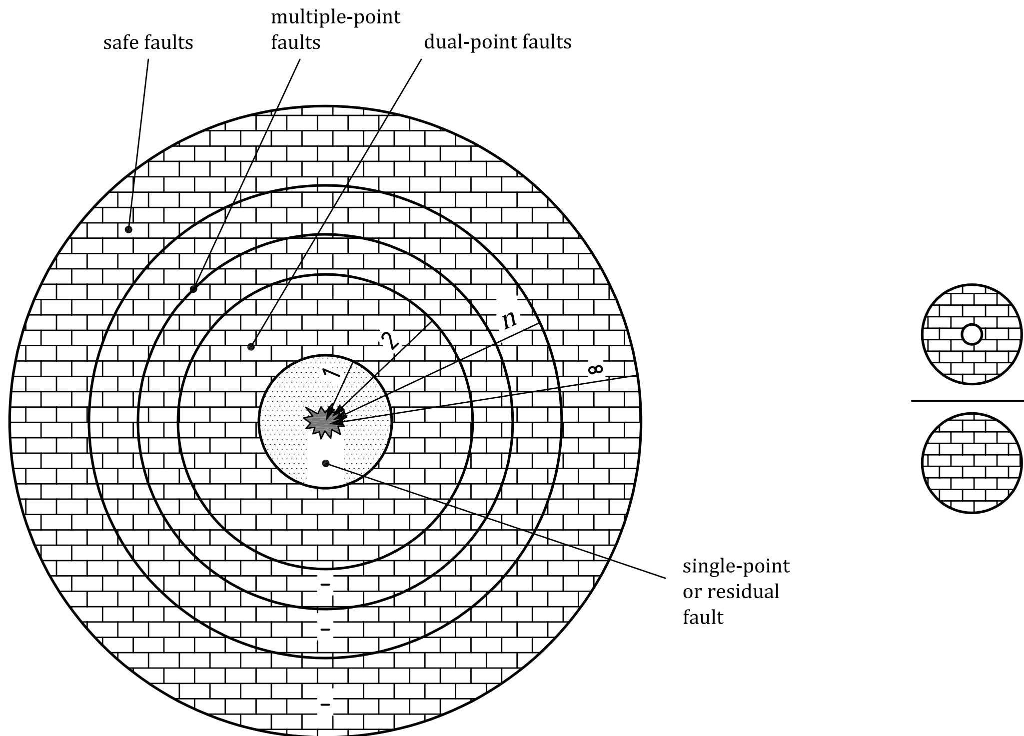

Figure C.2 — Graphical representation of the single-point fault metric

C.3 Latent-fault metric

C.3.1 This metric reflects the robustness of the item to latent faults either by coverage of faults in safety mechanisms or by the driver recognizing that the fault exists before the violation of the safety goal, or by design (primarily safe faults). A high latent-fault metric implies that the proportion of latent faults in the hardware is low.

C.3.2 This requirement applies to ASIL (B), (C), and D of the safety goal. The calculation in Equation (C.8) shall be used to determine the latent-fault metric:

$$1-\frac{\sum_{\mathrm{SR,HW}}\left(\lambda_{\mathrm{MPF,L}}\right)}{\sum_{\mathrm{SR,HW}}\left(\lambda-\lambda_{\mathrm{SPF}}-\lambda_{\mathrm{RF}}\right)}=\frac{\sum_{\mathrm{SR,HW}}\left(\lambda_{\mathrm{MPF,DP}}+\lambda_{\mathrm{S}}\right)}{\sum_{\mathrm{SR,HW}}\left(\lambda-\lambda_{\mathrm{SPF}}-\lambda_{\mathrm{RF}}\right)} \tag{C.8}$$

where $\sum_{\mathrm{SR,HW}} \lambda_x$ is the sum of λ_x of the safety-related hardware elements of the item to be considered for the metrics.

NOTE 1 Only the safety-related hardware elements of the item are considered for this metric.

EXAMPLE Hardware elements where all the faults are safe or multiple-point faults of order n, with n > 2, could be omitted from the calculations unless shown to be relevant in the technical safety concept.

NOTE 2 Figure C.3 gives a graphical representation of the latent-fault metric.

NOTE 3 An example of calculation of "latent-fault metric" is given in Annex E.

This is a preview. Click here to purchase the full publication.
– All rights reserved

NOTE 4 For latent fault metrics of items implementing fault tolerance in order to address safety relevant availability requirements, it can be important to identify the multiple-point faults with a higher order than two. This can be applicable to latent faults of a redundant system, if the intention is to operate on the redundant system for significant amount of time after the primary system fails.

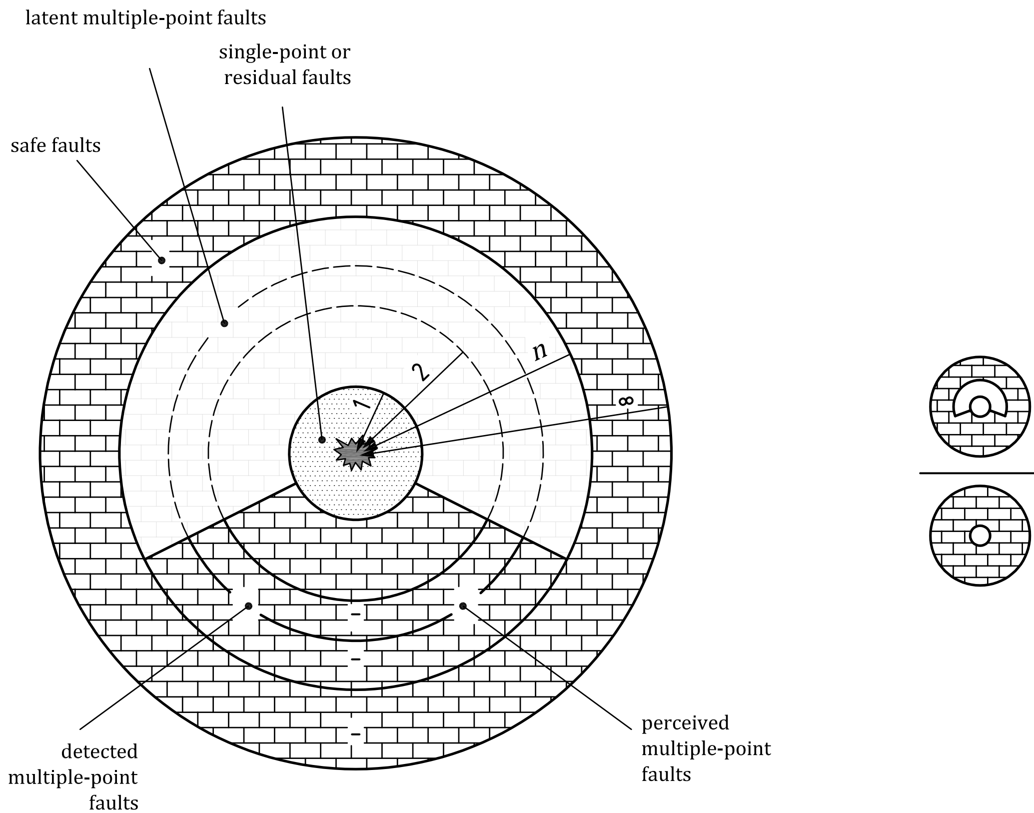

Figure C.3 — Graphical representation of the latent-fault metric

© ISO 2018 – All rig
This is a preview. Click here to purchase the full publication.

Annex D
(informative)

Evaluation of the diagnostic coverage

D.1 General

This annex is intended to be used as:

a) an evaluation of the diagnostic coverage to produce a rationale for:

— the compliance with the single-point fault and latent-fault metrics defined in Clause 8;

— the compliance with the evaluation of the safety goal violations due to random hardware failures as defined in Clause 9;

b) a guideline in order to choose appropriate safety mechanisms to be implemented in the E/E architecture to detect failures of elements.

Figure D.1 shows the generic hardware of an embedded system. Typical failure modes of the hardware elements of this system are shown in Table D.1. Each element listed in the leftmost column is associated with one or more failure modes which are captured in the column to the right of the element. The listing does not claim exhaustiveness and can be adjusted based on additional known failure modes or depending on the application.

Additional detail on the safety mechanisms associated with these element faults are referenced in each row (Tables D.2 to D.10). The effectiveness of these typical safety mechanisms for the given elements is categorized according to their ability to cover the listed failure modes to achieve low, medium or high diagnostic coverage of the element. These low, medium and high diagnostic coverage rankings correspond to typical coverage levels at 60 %, 90 % or 99 %, respectively.

The assignment of the failure modes and their corresponding safety mechanisms can vary from that listed in Table D.1 depending on:

a) variations in the source of the failure mode detected by the diagnostic;

b) the effectiveness of the safety mechanism;

c) the specific implementation of the safety mechanism;

d) the execution timing of the safety mechanism (periodicity);

e) the hardware technologies implemented in the system;

f) the probability of the failure modes, based on hardware in the system; and

g) a more detailed analysis of the failure modes and their classification into several sub-classes with different failure mode coverage levels.

In summary, Table D.1 provides guidelines which are adapted based on analysis of the system elements.

These guidelines do not address specific constraints that can be specified in the safety concepts in order to avoid the violation of the safety goals. These constraints, such as timing aspects (periodicity of diagnostic) for example, are not considered when evaluating the generic typical diagnostic coverage by

This is a preview. Click here to purchase the full publication.

– All rights reserved

the safety mechanism. They will be considered when evaluating the specific diagnostic coverage by a safety mechanism used in the item to avoid the violation of the safety goals.

EXAMPLE A safety mechanism can have a high generic typical diagnostic coverage in this annex but if the diagnostic test interval used is longer than the diagnostic test interval needed to comply with the relevant fault tolerant time interval, the specific diagnostic coverage with respect to the avoidance of violation of the safety goal, will be much lower.

Therefore Tables D.2 to D.10 can be used as a starting point to evaluate the diagnostic coverage of these safety mechanisms and the claimed diagnostic coverage is supported by a proper rationale (e.g. using fault injection methods or analytical arguments). In addition, the given information is intended to help define the failure modes of the element; however, the relevant failure modes are ultimately dependent on the application in which the elements are used.

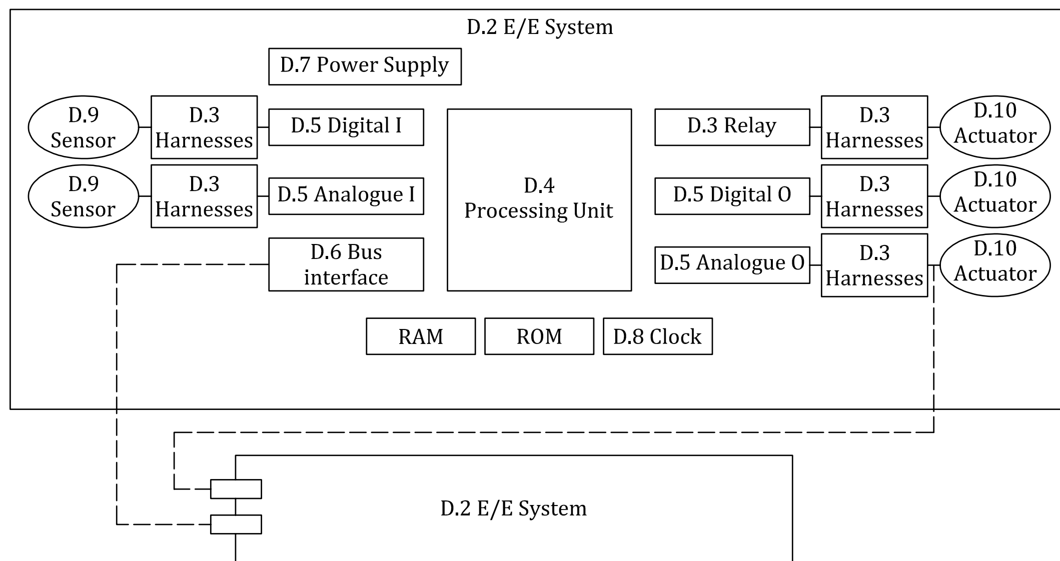

Figure D.1 — Generic hardware of a system

Tables D.2 to D.10 support the information of Table D.1 by giving guidelines on techniques for diagnostic tests. Tables D.1 to D.10 are not exhaustive and other techniques can be used, provided evidence is available to support the claimed diagnostic coverage. If justified, higher diagnostic coverage can be estimated, up to 100 % for simple or complex elements.

© ISO 2018 – All rig
This is a preview. Click here to purchase the full publication.

Table D.1 — Analysed failure modes

Element	See tables	Analysed failure modes
General elements		
E.E Systems	D.2 — E/E Systems	No generic failure modes available Detailed analysis necessary
Electrical elements		
Relays	D.3 — Electrical elements	Does not energize or de-energize Individual contacts welded
Harnesses including splice and connectors		Open circuit Contact resistance Short circuit to Ground (d.c. coupled) Short circuit to Vbat Short circuit between neighbouring pins Resistive drift between pins
Sensors including signal switches	D.9 — Sensors	Detailed analysis necessary Typical failure modes to be covered include: — Out-of-range — Offsets — Stuck in range — Oscillations See also ISO 26262-11:2018, 5.5 for integrated sensors and transducers.
Final elements (actuators, lamps, buzzers, screens...)	D.10 — Actuators	No generic failure modes available Detailed analysis necessary
General semiconductor elements		
Power supply	D.7 — Power supply	Drift and oscillation Under and over Voltage Power spikes See also ISO 26262-11:2018, 5.2

NOTE 1 The relevant failure modes and fault models are identified on a case by case basis and typically depend on the technology and the implementation used. See ISO 26262-11:2018, 4.3.1 for details on semiconductor fault models.

EXAMPLE If an element has the failure modes x, y, and z with a failure mode distribution of X, Y, Z then the effective diagnostic coverage is calculated as follows:

$$K_{DC} = X \times K_{FMC,x} + Y \times K_{FMC,y} + Z \times K_{FMC,z}$$

where

K_{DC} is the diagnostic coverage of the hardware element;

X is the failure mode distribution for failure mode x; $K_{FMC,x}$ is the failure mode coverage of failure mode x;

Y is the failure mode distribution of failure mode y; $K_{FMC,y}$ is the failure mode coverage of failure mode y;

Z is the failure mode distribution for failure mode z; $K_{FMC,z}$ is the failure mode coverage of failure mode z; and

$X + Y + Z = 100\ \%$

NOTE 2 For semiconductors, see ISO 26262-11:2018, 4.3 for details on the relationship between fault models, failure modes and related distribution.

This is a preview. Click here to purchase the full publication.

– All rights reserved

Table D.1 *(continued)*

Element	See tables	Analysed failure modes
Clock	D.8 — Programme sequence monitoring/Clock	Incorrect frequency Jitter See also ISO 26262-11:2018, 5.2
Non-volatile memory	ISO 26262-11:2018, Table 32	See ISO 26262-11:2018, 5.1, Table 29
Volatile memory	ISO 26262-11:2018, Table 33	See ISO 26262-11:2018, 5.1, Table 29
Digital I/O	D.5 — Analogue and digital I/O	Incorrect I/O See also ISO 26262-11:2018, 5.1, Table 30
Analogue I/O		Incorrect I/O See also ISO 26262-11:2018, 5.2, Table 36
Processing Unit	D.4 — Processing units / D.8 — Programme sequence monitoring/Clock	Incorrect output See also ISO 26262-11:2018, 5.1, Table 30

NOTE 1 The relevant failure modes and fault models are identified on a case by case basis and typically depend on the technology and the implementation used. See ISO 26262-11:2018, 4.3.1 for details on semiconductor fault models.

EXAMPLE If an element has the failure modes x, y, and z with a failure mode distribution of X, Y, Z then the effective diagnostic coverage is calculated as follows:

$K_{DC} = X \times K_{FMC,x} + Y \times K_{FMC,y} + Z \times K_{FMC,z}$

where

K_{DC} is the diagnostic coverage of the hardware element;

X is the failure mode distribution for failure mode x; $K_{FMC,x}$ is the failure mode coverage of failure mode x;

Y is the failure mode distribution of failure mode y; $K_{FMC,y}$ is the failure mode coverage of failure mode y;

Z is the failure mode distribution for failure mode z; $K_{FMC,z}$ is the failure mode coverage of failure mode z; and

$X + Y + Z = 100\ \%$

NOTE 2 For semiconductors, see ISO 26262-11:2018, 4.3 for details on the relationship between fault models, failure modes and related distribution.

© ISO 2018 – All rig
This is a preview. Click here to purchase the full publication.

Table D.1 *(continued)*

Element	See tables	Analysed failure modes
Communication		
Data transmission (to be analysed with ISO 26262-6:2018, D.2.4)	D.6 — Communication bus (serial, parallel)	Loss of communication peer Message corruption Message unacceptable delay Message loss Unintended message repetition Incorrect sequencing of messages Message insertion Message masquerading Message incorrect addressing

NOTE 1 The relevant failure modes and fault models are identified on a case by case basis and typically depend on the technology and the implementation used. See ISO 26262-11:2018, 4.3.1 for details on semiconductor fault models.

EXAMPLE If an element has the failure modes x, y, and z with a failure mode distribution of X, Y, Z then the effective diagnostic coverage is calculated as follows:

$K_{DC} = X \times K_{FMC,x} + Y \times K_{FMC,y} + Z \times K_{FMC,z}$

where

K_{DC} is the diagnostic coverage of the hardware element;

X is the failure mode distribution for failure mode x; $K_{FMC,x}$ is the failure mode coverage of failure mode x;

Y is the failure mode distribution of failure mode y; $K_{FMC,y}$ is the failure mode coverage of failure mode y;

Z is the failure mode distribution for failure mode z; $K_{FMC,z}$ is the failure mode coverage of failure mode z; and

$X + Y + Z = 100\ \%$

NOTE 2 For semiconductors, see ISO 26262-11:2018, 4.3 for details on the relationship between fault models, failure modes and related distribution.

Table D.2 — E/E Systems

Safety mechanism/ measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	D.2.1.1	Low	Depends on diagnostic coverage of failure detection
Comparator	D.2.1.2	High	Depends on the quality of the comparison
Majority voter	D.2.1.3	High	Depends on the quality of the voting
Dynamic principles	D.2.2.1	Medium	Depends on diagnostic coverage of failure detection
Analogue monitoring of digital signals	D.2.2.2	Low	—
Self-test by software cross exchange between two independent units	D.2.3.3	Medium	Depends on the quality of the self-test

This is a preview. Click here to purchase the full publication.
– All rights reserved

Table D.3 — Electrical elements

Safety mechanism/ measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	D.2.1.1	High	Depends on diagnostic coverage of failure detection
NOTE This table deals only with safety mechanisms dedicated to electrical elements. General techniques like a technique based on a data comparison (see D.2.1.2) are also able to detect failures of electrical elements but are not integrated in this table (already included in Table D.2 — E/E Systems).			

NOTE The following tables deal with safety mechanisms mainly applied to components at a system level. Additional details on safety mechanisms that could be integrated in the component are described in ISO 26262-11:2018:

— 5.1 for digital components;

— 5.2 for analogue and mixed signal components;

— 5.3 for programmable logic devices;

— 5.4 for multi-core components; and

— 5.5 for sensors & transducers.

Table D.4 — Processing units

Safety mechanism/ measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
Self-test by software: limited number of patterns (one channel)	D.2.3.1	Medium	Depends on the quality of the self-test
Self-test by software cross exchange between two independent units	D.2.3.3	Medium	Depends on the quality of the self-test
Self-test supported by hardware (one-channel)	D.2.3.2	Medium	Depends on the quality of the self-test
Software diversified redundancy (one hardware channel)	D.2.3.4	High	Depends on the quality of the diversification. Common mode failures can reduce diagnostic coverage
Reciprocal comparison by software	D.2.3.5	High	Depends on the quality of the comparison
HW redundancy (e.g. dual core lockstep, asymmetric redundancy, coded processing)	D.2.3.6	High	It depends on the quality of redundancy. Common mode failures can reduce diagnostic coverage
Configuration register test	D.2.3.7	High	Configuration registers only
Stack over/under flow Detection	D.2.3.8	Low	Stack boundary test only
Integrated hardware consistency monitoring	D.2.3.9	High	Coverage for illegal hardware exceptions only
NOTE This table deals only with safety mechanisms dedicated to processing units. General techniques like one based on data comparison (see D.2.1.2) are also able to detect failures of electrical elements but are not integrated in this table (already included in Table D.2 — E/E Systems).			

© ISO 2018 – All rig
This is a preview. Click here to purchase the full publication.

Table D.5 — Analogue and digital I/O

Safety mechanism/ measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring (Digital I/O)[a]	D.2.1.1	Low	Depends on diagnostic coverage of failure detection
Test pattern	D.2.4.1	High	Depends on type of pattern
Code protection for digital I/O	D.2.4.2	Medium	Depends on type of coding
Multi-channel parallel output	D.2.4.3	High	—
Monitored outputs	D.2.4.4	High	Only if dataflow changes within diagnostic test interval
Input comparison/ voting (1oo2, 2oo3 or better redundancy)	D.2.4.5	High	Only if dataflow changes within diagnostic test interval
[a] Digital I/O can be periodic.			

Table D.6 — Communication bus (serial, parallel)

Safety mechanism/ measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
One-bit hardware redundancy	D.2.5.1	Low	—
Multi-bit hardware redundancy	D.2.5.2	Medium	—
Read back of sent message	D.2.5.9	Medium	—
Complete hardware redundancy	D.2.5.3	High	Common mode failures can reduce diagnostic coverage
Inspection using test patterns	D.2.5.4	High	—
Transmission redundancy	D.2.5.5	Medium	Depends on type of redundancy. Effective only against transient faults
Information redundancy	D.2.5.6	Medium	Depends on type of redundancy
Frame counter	D.2.5.7	Medium	—
Timeout monitoring	D.2.5.8	Medium	—
Combination of information redundancy, frame counter and timeout monitoring	D.2.5.6, D.2.5.7 and D.2.5.8	High	For systems without hardware redundancy or test patterns, high coverage can be claimed for the combination of these safety mechanisms

Table D.7 — Power supply

Safety mechanism/ measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
Voltage or current control (input)	D.2.6.1	Low	—
Voltage or current control (output)	D.2.6.2	High	—

This is a preview. Click here to purchase the full publication.
– All rights reserved

Table D.8 — Programme sequence monitoring/Clock

Safety mechanism/ measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
Watchdog with separate time base without time-window	D.2.7.1	Low	—
Watchdog with separate time base and time-window	D.2.7.2	Medium	Depends on time restriction for the time-window
Logical monitoring of programme sequence	D.2.7.3	Medium	Only effective against clock failures if external temporal events influence the logical program flow. Provides coverage for internal hardware failures (such as interrupt frequency errors) that can cause the software to run out of sequence
Combination of temporal and logical monitoring of programme sequence	D.2.7.4	High	—
Combination of temporal and logical monitoring of programme sequences with time dependency	D.2.7.5	High	Provides coverage for internal hardware failures that can cause the software to run out of sequence. When implemented with asymmetrical designs, provides coverage regarding communication sequence between main and monitoring device NOTE Method to be designed to account for execution jitter from interrupts, CPU loading, etc.

Table D.9 — Sensors

Safety mechanism/ measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	D.2.1.1	Low	Depends on diagnostic coverage of failure detection
Test pattern	D.2.4.1	High	—
Input comparison/ voting (1oo2, 2oo3 or better redundancy)	D.2.4.5	High	Only if dataflow changes within diagnostic test interval
Sensor valid range	D.2.8.1	Low	Detects shorts to ground or power and some open circuits
Sensor correlation	D.2.8.2	High	Detects in range failures
Sensor rationality check	D.2.8.3	Medium	—

© ISO 2018 – All rig
This is a preview. Click here to purchase the full publication.