Table 36 *(continued)*

Part/subpart	Short description	Failure modes
Phase locked loop (PLL)	Hardware part/subpart controlling an oscillator in order to generate a square wave signal that maintains a constant phase angle (i.e. lock) on the frequency of an input, or reference signal. It can be used as clock in a digital circuit.	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect frequency of the output signal (i.e. outside the expected range, including harmonics when applicable, e.g. EMC emissions) Incorrect duty cycle of the output signal (i.e. outside the expected range) Drift[c] of the output frequency Jitter too high in the output signal Loss of lock condition (i.e. phase error, output clock not in sync with input clock not leading to incorrect frequency and incorrect duty cycle) Missing pulse in the output signal Extra pulse in the output signal
Generic		
Operational amplifier and buffer	Hardware part/subpart integrating a DC-coupled high-gain voltage amplifier with a differential input and, usually, a single-ended output.	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect gain on the output voltage (i.e. outside the expected range) Incorrect offset on the output voltage (i.e. outside the expected range) Incorrect output dynamic range (i.e. outside the expected range) Incorrect input dynamic range (i.e. outside the expected range) Output voltage accuracy too low, including drift[c] Output voltage affected by spikes[b] Output voltage oscillation[a] Settling time of the output voltage too low

[a] An oscillation is an instability of the part/subpart caused by internal failure, e.g. regulation loop failures, lower or negative hysteresis for a comparator, etc.. Oscillation includes any repetitive voltage and current variation (i.e. periodic pulse).

[b] A spike is a non-repetitive variation on the output voltage or current, i.e. pulse due to load jumps, etc.

[c] Drift is a slow and continuous variation of a parameter (i.e. current, voltage, threshold, etc.) outside the expected range reported into the circuit specification. Slow variation means slower than maximum fault handling time interval. For example drift covers floating or stuck at open failure modes.

[d] Several of the failure modes reported for the ADC or DAC can be grouped into two main sets: static error and absolute accuracy (total) error. Static errors are errors that affect the accuracy of a converter when it is converting static (DC) signals and can be completely described by four terms: offset error, gain error, integral nonlinearity, and differential nonlinearity.

NOTE 1 Each term can be expressed in LSB units or sometimes as a percentage of the full scale range (FSR). For example, an error of ½ LSB for an 8-bit converter corresponds to 0,2 % FSR.

NOTE 2 The absolute accuracy (total) error is the maximum value of the difference between an analogue value and the ideal mid-step value. It includes offset, gain, and integral linearity errors, and also the quantization error in the case of an ADC.

Table 36 *(continued)*

Part/subpart	Short description	Failure modes
Analogue switch	Hardware part/subpart capable of switching or routing analogue signals based on the level of a digital control signal. Commonly implemented using a "transmission gate".	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit or tri-stated) Offset too high affecting the output signal Resistive or capacitive coupling between control signal and output signal including crosstalk Attenuation of the output signal Drift[c] affecting the output signal Spikes[b] affecting the output signal , e.g. during switching
Voltage/Current comparator	Hardware part/subpart comparing an input analogue signal with a predefined threshold (i.e. voltage or current constant value) and producing a binary signal at the output; the output depends on which is higher between the input signal and the threshold and it remains constant as the difference has the same polarity.	Voltage/Current comparator not triggering when expected Voltage/Current comparator falsely triggering Output is stuck (i.e. high or low) Output is floating (i.e. open) Oscillation[a] of the output

[a] An oscillation is an instability of the part/subpart caused by internal failure, e.g. regulation loop failures, lower or negative hysteresis for a comparator, etc.. Oscillation includes any repetitive voltage and current variation (i.e. periodic pulse).

[b] A spike is a non-repetitive variation on the output voltage or current, i.e. pulse due to load jumps, etc.

[c] Drift is a slow and continuous variation of a parameter (i.e. current, voltage, threshold, etc.) outside the expected range reported into the circuit specification. Slow variation means slower than maximum fault handling time interval. For example drift covers floating or stuck at open failure modes.

[d] Several of the failure modes reported for the ADC or DAC can be grouped into two main sets: static error and absolute accuracy (total) error. Static errors are errors that affect the accuracy of a converter when it is converting static (DC) signals and can be completely described by four terms: offset error, gain error, integral nonlinearity, and differential nonlinearity.

NOTE 1 Each term can be expressed in LSB units or sometimes as a percentage of the full scale range (FSR). For example, an error of ½ LSB for an 8-bit converter corresponds to 0,2 % FSR.

NOTE 2 The absolute accuracy (total) error is the maximum value of the difference between an analogue value and the ideal mid-step value. It includes offset, gain, and integral linearity errors, and also the quantization error in the case of an ADC.

Table 36 *(continued)*

Part/subpart	Short description	Failure modes
Sample & hold	Hardware part/subpart sampling the voltage of a continuously varying analogue input signal and holding its value at a constant level for a specified minimum period of time.	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect sampling leading to gain/offset error on output voltage dependent on input signal Incorrect gain on the output voltage (i.e. outside the expected range) Incorrect offset on the output voltage (i.e. outside the expected range) Incorrect output dynamic range (i.e. outside the expected range) Incorrect input dynamic range (i.e. outside the expected range) Output voltage accuracy too low during hold phase, including drift[c] Output voltage during hold phase affected by spikes[b] Output voltage oscillation[a] during hold phase Output does not settle sufficiently accurate during hold time
Analogue multiplexer	Hardware part/subpart consisting of multiple analogue input signals, multiple control inputs and one output signal.	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect channel selection Offset affecting the output signal too high Resistive or capacitive coupling among input channels and output signal including crosstalk Resistive or capacitive coupling among selectors and output signal including crosstalk Incorrect output dynamic range (i.e. outside the expected range) Attenuation of the output signal Drift[c] affecting the output signal Spikes[b] affecting the output signal (i.e. during switching)

[a] An oscillation is an instability of the part/subpart caused by internal failure, e.g. regulation loop failures, lower or negative hysteresis for a comparator, etc.. Oscillation includes any repetitive voltage and current variation (i.e. periodic pulse).

[b] A spike is a non-repetitive variation on the output voltage or current, i.e. pulse due to load jumps, etc.

[c] Drift is a slow and continuous variation of a parameter (i.e. current, voltage, threshold, etc.) outside the expected range reported into the circuit specification. Slow variation means slower than maximum fault handling time interval. For example drift covers floating or stuck at open failure modes.

[d] Several of the failure modes reported for the ADC or DAC can be grouped into two main sets: static error and absolute accuracy (total) error. Static errors are errors that affect the accuracy of a converter when it is converting static (DC) signals and can be completely described by four terms: offset error, gain error, integral nonlinearity, and differential nonlinearity.

NOTE 1 Each term can be expressed in LSB units or sometimes as a percentage of the full scale range (FSR). For example, an error of ½ LSB for an 8-bit converter corresponds to 0,2 % FSR.

NOTE 2 The absolute accuracy (total) error is the maximum value of the difference between an analogue value and the ideal mid-step value. It includes offset, gain, and integral linearity errors, and also the quantization error in the case of an ADC.

Table 36 *(continued)*

Part/subpart	Short description	Failure modes
Voltage references	Hardware part/subpart producing a constant DC (direct-current) output voltage regardless of variations in external conditions such as temperature, barometric pressure, humidity, current demand, or the passage of time.	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect output voltage value (i.e. outside the expected range) Output voltage accuracy too low, including drift c Output voltage affected by spikes[b] Output voltage oscillation[a] within the expected range Incorrect start-up time (i.e. outside the expected range)
Passive network	Hardware part/subpart consisting of a network of passive devices (resistor and capacitor) providing a specific low pass transfer function	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect output dynamic range (i.e. outside the expected range) Incorrect attenuation of the output signal (i.e. outside the expected range) Incorrect settling time (i.e. outside the expected range) Drift[c] affecting the output signal Oscillation[a] affecting the output signal (i.e. due to crosstalk, coupling or parasitic effects) Spikes[b] affecting the output (i.e. due to crosstalk, coupling or parasitic effects)

[a] An oscillation is an instability of the part/subpart caused by internal failure, e.g. regulation loop failures, lower or negative hysteresis for a comparator, etc.. Oscillation includes any repetitive voltage and current variation (i.e. periodic pulse).

[b] A spike is a non-repetitive variation on the output voltage or current, i.e. pulse due to load jumps, etc.

[c] Drift is a slow and continuous variation of a parameter (i.e. current, voltage, threshold, etc.) outside the expected range reported into the circuit specification. Slow variation means slower than maximum fault handling time interval. For example drift covers floating or stuck at open failure modes.

[d] Several of the failure modes reported for the ADC or DAC can be grouped into two main sets: static error and absolute accuracy (total) error. Static errors are errors that affect the accuracy of a converter when it is converting static (DC) signals and can be completely described by four terms: offset error, gain error, integral nonlinearity, and differential nonlinearity.

NOTE 1 Each term can be expressed in LSB units or sometimes as a percentage of the full scale range (FSR). For example, an error of ½ LSB for an 8-bit converter corresponds to 0,2 % FSR.

NOTE 2 The absolute accuracy (total) error is the maximum value of the difference between an analogue value and the ideal mid-step value. It includes offset, gain, and integral linearity errors, and also the quantization error in the case of an ADC.

Table 36 *(continued)*

Part/subpart	Short description	Failure modes
Current source (including bias current generator)	Hardware part/subpart delivering or absorbing a current (i.e. reference current) which is independent of the voltage across it. It typically includes multiple branches which are routed to other circuits requiring a reference or bias current.	One or more outputs are stuck (i.e. high or low) One or more outputs are floating (i.e. open circuit) Incorrect reference current (i.e. outside the expected range) Reference current accuracy too low , including drift[c] Reference current affected by spikes[b] Reference current oscillation[a] within the expected range One or more branch currents outside the expected range while reference current is correct One or more branch currents accuracy too low , including drift[c] One or more branch currents affected by spikes[b] One or more branch currents oscillation[a] within the expected range

[a] An oscillation is an instability of the part/subpart caused by internal failure, e.g. regulation loop failures, lower or negative hysteresis for a comparator, etc.. Oscillation includes any repetitive voltage and current variation (i.e. periodic pulse).

[b] A spike is a non-repetitive variation on the output voltage or current, i.e. pulse due to load jumps, etc.

[c] Drift is a slow and continuous variation of a parameter (i.e. current, voltage, threshold, etc.) outside the expected range reported into the circuit specification. Slow variation means slower than maximum fault handling time interval. For example drift covers floating or stuck at open failure modes.

[d] Several of the failure modes reported for the ADC or DAC can be grouped into two main sets: static error and absolute accuracy (total) error. Static errors are errors that affect the accuracy of a converter when it is converting static (DC) signals and can be completely described by four terms: offset error, gain error, integral nonlinearity, and differential nonlinearity.

NOTE 1 Each term can be expressed in LSB units or sometimes as a percentage of the full scale range (FSR). For example, an error of ½ LSB for an 8-bit converter corresponds to 0,2 % FSR.

NOTE 2 The absolute accuracy (total) error is the maximum value of the difference between an analogue value and the ideal mid-step value. It includes offset, gain, and integral linearity errors, and also the quantization error in the case of an ADC.

5.2.2.2 About transient faults

As defined in ISO 26262-1:2018, 3.173, a transient fault is a fault that occurs once and subsequently disappears. Soft errors such as Single Event Upset (SEU) and Single Event Transient (SET), are defined as transient faults (see 5.1.2). ISO 26262-5:2018, 8.4.7 states that transient faults are considered when shown to be relevant due, for instance, to the technology used and can be addressed either by a quantitative approach, specifying and verifying a dedicated target “single-point fault metric” value to them or by a qualitative rationale based on the verification of the effectiveness of the internal safety mechanisms implemented to cover these transient faults.

In terrestrial analogue circuits, transient faults are caused by alpha-particle or neutron hits or by electromagnetic interference such as power transients and crosstalk. They can cause SEU or even SET also called Analogue Single Event Transients (ASETs), such as transient pulses in operational amplifiers, comparators or reference voltage circuits.

Due to the intrinsic nature of analogue technology (in which transient or noise effects are considered by design), the susceptibility to transient faults is lower than in digital circuits by orders of magnitude. Therefore, the analysis of those effects can be limited in a first approximation to their digital part (e.g. the digital decimation filter of a sigma-delta ADC).

However in some cases, like in the early part of the conversion cycle of an ADC (see Reference [28]) or in a PLL (see Reference [20]) or differential switched-capacitor circuits (see Reference [10]), the vulnerability to soft error can be high. In those cases, more detailed analyses are done and appropriate countermeasures are identified (see Reference [1]).

For mixed signal components, the impact of soft errors in the digital part is considered as described in 5.1.7.2.

NOTE Soft Error Rate evaluation by irradiation tests in analogue circuits is not a simple task. In this case measurement is done mainly by more detailed analyses of the analogue part.

5.2.3 Notes about safety analysis

5.2.3.1 General

The examples and guidelines given in 5.1 can be valid for an analogue or mixed signal component. The following clauses describe some of the topics that can require additional clarification for an analogue or mixed signal component.

5.2.3.2 Level of granularity of analysis

One of the key aspects for the safety analysis of analogue elements is the proper identification of the granularity of the analysis. On one hand, a lower level of granularity is beneficial as it allows for a better understanding of the failure modes and failure mode distributions. On the other, a higher level of granularity allows for a clear allocation of safety mechanisms. Analogue elements are often used to interface with physical objects making it useful to also consider mechanical characteristics and differentiate the failure modes accordingly.

As seen in ISO 26262-9:2018, Clause 8, qualitative and quantitative safety analyses are performed at the appropriate level of abstraction during the concept and product development phases. The level of abstraction can be consequently adjusted depending on the target of the analysis. Qualitative analysis is more suited to identify failure modes while quantitative analysis quantifies their failure rates and distributions.

EXAMPLE A linear voltage regulator is monitored using a windowed voltage monitor. The voltage monitor is at the output of the regulator and is able to detect over-voltage conditions. If the output value moves outside of a defined tolerance it is to be considered faulty e.g. 1,2 V ± 0,12 V. If the analysis focuses on the output of the regulator it can be relatively easy to discriminate between types of failures (e.g. safe because it fails within the allowed range, safety related because of over or under voltage) and quantify the protection offered by the voltage monitor. However, it is difficult to quantify the likelihood of each type of failure as required for metric computation. If the analysis goes inside the regulator and focuses, for instance, on faults of the bandgap it is easier to analyse propagation and likelihood of each failure of the regulator but not simple to quantify the protection that the external voltage monitor offers on the bandgap itself.

For the safety analysis, the type of safety mechanisms can drive the selection of the level of granularity. If the safety mechanisms addressing analogue features are located at system or element level, descending in the component hierarchy can lead to an overly complex analysis. The quantification of the failure mode distribution can require an investigation of higher granularity. For instance, applying an equal distribution to the failure modes of the linear voltage regulator can give less accurate results than applying an equal distribution to the blocks composing the linear voltage regulator as, for instance, the bandgap, the buffer, the driver, etc. With respect to terminology, in line with the classification described in 4.2, the linear voltage regulator is to be considered a part and the bandgap, the buffer, the driver, etc. subparts.

5.2.3.3 Deriving failure mode distributions for analogue components

The failure distributions for analogue components are dependent on the circuit implementation and targeted process. Each supplier provides details on the failure mode distributions to be used in the analysis.

EXAMPLE 1 A uniform failure mode distribution can be used for the initial analysis, e.g. if five failure modes are defined, each failure mode is allocated 20 % distribution. The uniform failure mode distribution is considered in the example in 5.2.3.5.

EXAMPLE 2 A more detailed distribution for each failure mode can be considered based on area; if the area of the circuit or circuits identified as the root cause for the defined failure mode is 5 %, then the allocated failure mode distribution is 5 %.

Applicable failure modes and the level of detail of the failure mode distributions are justified according to the circuit implementation and its physical area and documented accordingly.

5.2.3.4 About safe faults

ISO 26262-10 [61] states that safe faults can be faults of one of two categories:

— all n point faults with n > 2, unless the safety concept shows them to be a relevant contributor to a safety requirement, or

— faults that will not contribute to the violation of a safety requirement.

Analogue components are characterized by continuous signal regions and as such, tolerances are taken into consideration when used in systems. The tolerances on analogue functions as specified as part of the safety requirements allocated to that analogue component can be less constrained than the actual tolerance of the analogue component itself. For this reason, the fraction of the failure mode that leads to parametric failure or drift, but which remains within these tolerance ranges is safe. An analogue component has therefore an inherent capability to tolerate a fault. These faults are safe faults.

EXAMPLE 1 A resistor is used to limit the current flowing through a specific branch. A failure in the accuracy of the resistor increasing its value (e.g. of 50 %) but not preventing the current limiting function would be a safe fault.

A specific fault in an element can have a different classification depending on the specific safety requirement considered. For more details see ISO 26262-5.

Depending on the system configuration and the safety requirements some failure modes are not relevant, i.e. they cannot violate the requirements. In this case, these failure modes can be classified as safe: They contribute to the hardware safety metrics increasing the failure rate of safe faults.

EXAMPLE 2 An output driver can have an output slope control to limit the rise and fall times of the output value for EMI purposes. If the slew rate is irrelevant for the violation of the safety goal, failures in this slope control would be safe faults.

EXAMPLE 3 If a voltage regulator is used to supply digital circuits only, failure modes affecting the stability and the accuracy of the output voltage within the OV/UV thresholds can be classified as safe.

5.2.3.5 Example of quantitative analysis for an analogue component

A detailed example of quantitative analysis for analogue components is described in Annex D.

5.2.3.6 Dependent failures analysis

As noted in ISO 26262-9:2018, 7.4.2, NOTE, the analysis of dependent failures is performed on a qualitative basis because no general and sufficiently reliable method exists for quantifying such failures.

The steps reported in 4.7 are applicable also for analogue and mixed signal components. In the dependent failures analysis, there are aspects that can be clearly considered when addressing analogue components, parts or subparts.

Analogue circuits are by nature sensitive to noise and interference among different blocks or functions. For this reason, structures to guarantee sufficient independence by means of isolation and separation (e.g. by implementing barriers and/or guard-rings or placing circuits at certain distances or separating the power supply distribution and even the ground layer) are implemented for functional reasons. In fact, substrate, power supply and global signals like bias, clock or reset are often considered as a source of interference and special care is taken to reduce such effect. This good design practice, usually followed for functional reasons, provides benefits in terms of dependent failures avoidance.

Analogue circuits can be very sensitive to process variation resulting in mismatches in the device behaviour. To ensure the “same” transfer function of two blocks, as in the case of redundant parts, the symmetry of the design and physical layout is a key factor. In such cases, special attention is taken to ensure exactly the same layout of the two blocks including orientation, symmetrical placing, routing etc.; therefore diversity is not always a viable solution to improve the common cause failure avoidance for analogue circuits.

As a consequence of these aspects, the dependent failures initiators are often addressed by techniques ensuring isolation or separation instead of with techniques aiming to differentiate their effects.

In other cases, diversity can still be a valid technique to achieve the detection or avoidance of dependent failures. For instance, in a dual channel approach, using two diverse ADC architectures (e.g. successive approximation ADC and sigma delta ADC) can reduce significantly the probability of common cause failures.

5.2.3.7 Verification of the architectural metrics computation

This sub-clause is addressing a specific part of the safety analysis verification: the verification of the architectural hardware safety metrics and in particular the fraction of safe faults and the failure mode coverage.

Possible approaches include:

— expert judgment founded on an engineering approach given that any data, either qualitative or quantitative, is supported by rationale and relevant arguments, and is documented accordingly;

NOTE 1 In some cases, such arguments can be derived from the functional characterization of the hardware elements responsible for the claimed parameters. The aim of the functional characterization is the systematic failure avoidance and not the hardware random failure but, in some cases, it can be used as evidence to prove the level of coverage with respect to a specific failure mode: This is the case in which the aim of a safety mechanism is to detect 100 % of one of more failure modes and this capability is guaranteed by design.

EXAMPLE 1 A voltage monitor as described in 5.2.4.2 is a typical safety mechanism used to detect overvoltage and under-voltage failure modes affecting the voltage regulator. If, during the hardware design verification, the functional characterization of the voltage monitor shows that:

— any event leading to a regulated voltage outside the expected range defined in the specification for enough time to make the supplied hardware circuit malfunction is detected by the voltage monitor; and

— any event leading to a variation of the regulated voltage inside the range defined in the specification for any time does not affect the correct behaviour of the hardware circuit supplied by the regulator;

then, such characterizations can be used as arguments to claim a detection equal to 100 % of the mentioned failure modes.

— as mentioned in 4.8, fault injection simulation during the development phase is a valid method to verify completeness and correctness of safety mechanism implementation with respect to hardware safety requirements. Fault injection using design models can be successfully used to assist the verification. This method can be applied to analogue and mixed signal components; and

NOTE 2 The fault injection campaign can be limited to a subset of faults or failures that are judged to be critical in a specific case. The most critical failure modes are identified after considering their distribution, their claimed amount of safe faults, their claimed level of detection and the safety mechanisms or safety requirements responsible for those levels.

— a combination of the above methods, i.e. fault injection which supports expert judgment by providing arguments and evidence for the cases judged more critical and /or addressable by fault injection method alone.

5.2.4 Examples of safety mechanisms

The following tables give a non-exhaustive list of examples of commonly used analogue safety mechanisms that complements the information contained in ISO 26262-5:2018, Annex D.

Some analogue safety mechanisms have a digital output signal which is used to control the reaction to a failure and bring the component to a safe state. In many cases, this information is stored so that it can be communicated through a digital interface. Other analogue safety mechanisms control or suppress a fault from resulting in the violation of a safety requirement and do not interface with the digital domain.

To comply with ISO 26262-5:2018, 8.4.8, the safety mechanisms described in the following tables can require additional measures to detect faults affecting them that, as dual-point faults, can lead to the violation of the safety goal.

The examples given in Table 37 to Table 40 are not exhaustive and other techniques can be used.

NOTE 1 It is not possible to give a general guidance on the DC because it strongly depends on the specific technology, type of circuit, use case etc.

NOTE 2 Evidence is provided to support the claimed diagnostic coverage.

Table 37 — Power supply

Safety mechanism/ measure	See overview of techniques	Notes
Over and under voltage monitoring	5.2.4.2	Typically an analogue circuit with an output latched in a digital core.
Voltage clamp (limiter)	5.2.4.3	Typically used to suppress voltage transients or spikes.
Over-current monitoring	5.2.4.4	Typically an analogue circuit with an output latched in digital core.
Current limiting	5.2.4.5	Typically an analogue circuit with feedback to an analogue control loop (e.g. to disable regulator main pass element).
Power on reset	5.2.4.6	Functional block which keeps the circuit in a known initialized state until power supply rails and/or the clock signal are stable.

Table 38 — Analogue I/O

Safety mechanism/ measure	See overview of techniques	Notes
Resistive pull up/down	5.2.4.1	Typically used on input signals to avoid floating conditions due to pin failure or external pin interconnect failure.
Filter	5.2.4.8	Analogue or digital circuit, typically used to suppress high frequency signal variation, like an output from analogue over & under voltage monitoring circuit.

Table 39 — Miscellaneous analogue components

Safety mechanism/ measure	See overview of techniques	Notes
Analogue watchdog	5.2.4.7	Typically a monostable circuit used to monitor proper operation of an oscillator.
Thermal monitor	5.2.4.9	Typically an analogue circuit with an output latched in digital core, or feedback to an analogue circuit control loop (e.g. to disable affected circuit).
ADC monitoring	5.2.4.11	An analogue circuit typically controlled and evaluated by a digital circuit.
Analogue BIST	5.2.4.10	Typically an analogue circuit controlled by a digital circuit that verifies correct functionality of analogue safety mechanisms like under/over voltage monitoring, current limit protection and thermal protection circuits.

Table 40 — Analogue to Digital converter

Safety mechanism/ measure	See overview of techniques	Notes
ADC attenuation detection	5.2.4.12	Typically an analogue circuit controlled by a digital circuit that validates the ADC conversion path by measuring a known and stable signal value.
Stuck on ADC channel detection	5.2.4.13	Typically an analogue circuit controlled by a digital circuit that validates the ADC conversion path by measuring a known and stable signal value.

5.2.4.1 Resistive pull up/down

Aim: To define a default voltage for a circuit node.

Description: A resistor is connected from a circuit node to either a supply voltage or ground to define a default voltage in the event that the driving signal becomes disconnected/high impedance. Commonly used on I/O pins.

EXAMPLE An un-driven or disconnected device/module input pin would be at an unknown voltage level. A pull-up resistor to the I/O supply voltage (or module supply voltage) or pull-down resistor to ground is used to keep the input at a known voltage level. The circuit itself could be a passive resistor or an active circuit like a current mirror.

5.2.4.2 Over & under voltage monitoring

Aim: To detect, as early as possible, when a regulated voltage is outside the specified range.

Description: The regulated voltage is compared via a differential input pair to a low and/or a high analogue reference voltage representing the limits of the specified operating range. The monitor output will change state when the regulated voltage is outside of the defined voltage window indicating a fault.

EXAMPLE A window comparator is used to monitor the output of a Low Drop Out (LDO) regulator with reference voltages set to the minimum and maximum specified voltage levels in regulation.

5.2.4.3 Voltage clamp (limiter)

Aim: To prevent the voltage of a circuit node from exceeding the maximum voltage that can be safely supported.

Description: A voltage clamp limits the positive and/or negative voltage of a circuit node to an acceptable level determined by system and/or device process capability. Voltage clamps can be biased or unbiased. Unbiased clamps typically use Zener diodes to define the reference voltage while biased

clamps use a voltage source in combination with specialized diodes (Zener, Schottky) to define the acceptable voltage level. Voltage clamps are typically used to protect against transient events.

EXAMPLE An ESD protection circuit is a specialized voltage clamp typically implemented on I/O pins. It is designed to shunt the energy of a high voltage electrostatic discharge on the I/O pins away from the internal circuitry to ensure that internal circuitry is not exposed to excessive voltage levels during the ESD event.

5.2.4.4 Over-current monitoring

Aim: To detect, as early as possible, when the output current exceeds a certain value.

Description: The implementation of over-current monitoring can vary. A typical approach for a voltage regulator circuit with an MOS output device is to add a sense FET in parallel with a regulator main FET. The sense FET current, which is proportional to the main FET current, flows across a sense resistor. The voltage drop across the sense resistor is amplified and monitored by a voltage monitor.

NOTE The output of an over-current monitor is a digital output which is subsequently used as feedback to an analogue circuit control loop, and/or latched in a digital core which interfaces to the control and/or status monitoring circuits.

5.2.4.5 Current limiter

Aim: To limit output current to a maximum level in order to maintain a safe operating area of the output device and prevent electrical overstress.

Description: A closed loop system using negative feedback from a current monitor to reduce the drive to the output device thereby limiting the output current.

5.2.4.6 Power on reset

Aim: To hold the outputs of a system in a known state (typically off) until internal nodes have stabilized upon power up or power reset conditions.

Description: Typically, a bandgap-derived voltage reference is compared to an attenuated supply voltage in order to detect the minimum specified supply voltage which will ensure correct operation. Hysteresis is typically required to prevent oscillation as the attenuated supply voltage exceeds the reference voltage.

EXAMPLE An under-voltage monitor is a mechanism used to detect and drive power-on reset.

5.2.4.7 Analogue watchdog

Aim: To monitor proper operation of an oscillator.

Description: Typically implemented with a monostable circuit (one shot) which is reset on each cycle of the oscillator. If an oscillator transition does not occur within a specified time period defined by the monostable circuit, a fault signal is produced.

5.2.4.8 Filter

Aim: To avoid transients potentially causing failures:

Description: A filter can be used in multiple ways as a safety mechanism.

EXAMPLE 1 A bypass capacitor can be used to suppress voltage transients. An RC time constant is used to evaluate whether the duration of a fault which has the potential to violate the safety goal is within the maximum fault handling time interval.

EXAMPLE 2 A digital de-glitch circuit can be used to filter level shifted analogue voltage comparator outputs.