TECHNICAL REPORT

ISO/TR 9839

First edition
2023-08

Road vehicles — Application of predictive maintenance to hardware with ISO 26262-5

Véhicules routiers — Application de la maintenance prédictive au matériel à l'aide de l'ISO 26262-5

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

Reference number
ISO/TR 9839:2023(E)

© ISO 2023

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

COPYRIGHT PROTECTED DOCUMENT

© ISO 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO 2023 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **2**
5 Literature survey of degrading faults ... **4**
5.1 General ... 4
5.2 Degrading faults in industry standards ... 4
5.2.1 JEDEC JEP122H[4] ... 4
5.3 Degrading faults in technical publications ... 5
5.3.1 Advanced CMOS Reliability Update: Sub 20 nm FinFET Assessment[5] ... 5
5.3.2 Circuit-Based Reliability Consideration in FinFET Technology[6] ... 6
5.3.3 Intermittent Faults and Effects on Reliability of Integrated Circuits[7] ... 6
6 Literature survey on predictive maintenance ... **6**
6.1 General ... 6
6.2 Predictive maintenance in industry standards ... 6
6.2.1 IEC 61508[9] ... 6
6.2.2 IEEE Std 1856[3] ... 6
6.3 Predictive maintenance in technical publications ... 7
6.3.1 A Survey of Online Failure Prediction Methods[10] ... 7
6.3.2 An Odometer for CPUs[11] ... 7
6.3.3 Circuit Failure Prediction for Robust System Design in Scaled CMOS [12] ... 8
6.3.4 A Circuit Failure Prediction Mechanism (DART) for High Field Reliability [13] ... 8
6.3.5 Predicting Remediations for Hardware Failures in Large-Scale Datacenters[14] ... 8
6.3.6 Improving Analog Functional Safety Using Data-Driven Anomaly Detection [15] ... 8
7 Degrading faults and the ISO 26262 series ... **8**
7.1 Understanding the lifecycle of degrading faults ... 8
7.2 Classification of degrading faults ... 12
7.3 Quantifying degrading fault base failure rate ... 12
7.3.1 Industry standards and models ... 12
7.3.2 Field data ... 13
7.3.3 Expert judgement ... 13
8 Applying predictive maintenance ... **13**
8.1 Diagnostic coverage (DC) evaluation for predictive mechanisms ... 13
8.2 Considering random hardware metrics ... 13
8.2.1 Impacting the SPFM and LFM ... 13
8.2.2 Application as a dedicated measure ... 14
8.3 Considering RUL prediction ... 14
Annex A (informative) **An approach to handling degrading faults** ... **16**
Bibliography ... **18**

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects.*

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

Introduction

Hardware elements wear out or degrade with time and usage. The presence of certain faults can cause the rate of degradation to increase. If the rate of degradation exceeds critical thresholds, then a hardware element can fail during its normal expected lifespan. Addressing fault behaviours which change over time is difficult. Functional safety standards such as the ISO 26262 series have traditionally addressed degrading faults with avoidance measures and simplified assumptions of static behaviours.

Understanding of degrading faults is improving over time. Many industries are taking proactive steps to control degrading faults using predictive maintenance. Predictive maintenance can detect degrading faults and predict remaining useful life. Safety mechanisms based on predictive maintenance are not explicitly discussed in the ISO 26262 series.

This document provides a survey of current state of the art for degrading faults and predictive maintenance techniques. Approaches are presented to consider degrading faults and predictive maintenance techniques in an ISO 26262 safety argument. Much of the content is focused on semiconductors, but the concepts can be applied to other hardware elements.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

Road vehicles — Application of predictive maintenance to hardware with ISO 26262-5

1 Scope

This document is intended to be applied to the usage of predictive maintenance methods for the detection of degrading faults in safety related E/E hardware elements. It applies to hardware elements developed for compliance with the ISO 26262[1] series in which degrading faults are shown to be relevant due to, for instance, the technology used.

Specific technical implementations of predictive maintenance solutions are not in scope of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 26262-1, *Road vehicles — Functional safety — Part 1: Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 26262-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
degrading fault
fault whose characteristics are not constant and degrade over time, that can result in an error or failure when stimulated after degradation exceeds a critical threshold

Note 1 to entry: Permanent and intermittent faults can first manifest as degrading faults. Transient faults do not manifest as degrading faults.

Note 2 to entry: Degrading faults do not create errors or failures until degradation exceeds critical thresholds. The capability to generate an error or failure is related to the current state of degradation.

Note 3 to entry: Degrading faults exhibit abnormal conditions which can cause an error or failure over time. Normal degradation does not exhibit abnormal conditions which are necessary to be classified as a fault. Normal degradation can result in a loss of functionality after expected lifespan has elapsed but cannot be considered a fault as it is not abnormal.

3.2
degrading fault detection time interval
DFDTI
timespan from the occurrence of a *degrading fault* (3.1) to its detection

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

3.3
degrading fault handling time interval
DFHTI
sum of the *degrading fault detection time interval* (3.2) and the *degrading fault reaction time interval* (3.4).

Note 1 to entry: The degrading fault handling time interval is a property of a *predictive maintenance* (3.5) related safety mechanism.

Note 2 to entry: The degrading fault handling time interval is considered in addition to the fault handling time interval. See Figure 4.

Note 3 to entry: The timespan from occurrence of a *degrading fault* (3.1) until it has the capability to generate an error or failure is the maximum degrading fault handling time interval that can be specified for a predictive maintenance related safety mechanism to support the functional safety concept.

Note 4 to entry: A *degrading fault* (3.1) is covered in a timely manner by the corresponding safety mechanism if there is detection and reaction within the degrading fault handling time interval.

3.4
degrading fault reaction time interval
DFRTI
timespan from the detection of a *degrading fault* (3.1) to reaching a safe state or reaching emergency operation

3.5
predictive maintenance
techniques that are used to detect *degrading faults* (3.1), predict *remaining useful life* (3.6), and react appropriately

Note 1 to entry: Approaches include the use of data driven methods such as machine learning applied locally or on a remote system. Guidance for developing safety related ML systems can be found in ISO/IEC TR 5469[2].

Note 2 to entry: Prediction of *remaining useful life* (3.6) can be used to replace a faulty element before it can cause an error or failure.

3.6
remaining useful life
RUL
length of time from the present time to the estimated time that the item or element is expected to no longer perform its intended function within desired specifications

Note 1 to entry: RUL can be estimated using *predictive maintenance* (3.5) or with other approaches.

Note 2 to entry: RUL can be estimated for expected degradation or degradation in the presence of a fault.

[SOURCE: IEEE Std 1856-2017[3], modified — The phrase "system (or product)" was replaced with "item or element".]

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

4 Abbreviated terms

ADAS	Advanced Driver Assistance System
ADS	Automated Driving System
AI	Artificial Intelligence
BEoL	Back End of Line (sometimes BEOL)
BFR	Base Failure Rate

© ISO 2023 – All rights reserved

BLM	Barrier Layer Material
CHC	Channel Hot Carrier
COTS	Commercial Off The Shelf
DC	Diagnostic Coverage
DFDTI	Degrading Fault Detection Time Interval
DFHTI	Degrading Fault Handling Time Interval
DFRTI	Degrading Fault Reaction Time Interval
DRAM	Dynamic Random Access Memory
EM	Electromigration
ESD	Electrostatic Discharge
FEoL	Front End of Line (sometimes FEOL)
FET	Field Effect Transistor
FDTI	Fault Detection Time Interval
FHTI	Fault Handling Time Interval
FTTI	Fault Tolerant Time Interval
HCI	Hot Carrier Injection
ILD	Inter-Layer Dielectric
LFM	Latent Fault Metric
ML	Machine Learning
MoL	Middle of Line (sometimes MOL)
MEoL	Middle End of Line (sometimes MEOL)
MPFDTI	Multiple Point Fault Detection Time Interval
NBTI	Negative Bias Temperature Instability
NVM	Non-Volatile Memory
PCM	Phase Change Memory
PHM	Prognostics and Health Management
RUL	Remaining Useful Life
SBD	Soft Breakdown
SHE	Self-Heating Effect
SILC	Stress-Induced Leakage Current
SM	Stress Migration

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

SoC	System on Chip
SPFM	Single Point Fault Metric
TDDB	Time Dependent Dielectric Breakdown
TDJD	Time Dependent Junction Degradation
TID	Total Ionizing Dose

5 Literature survey of degrading faults

5.1 General

This document reviews many technical documents to summarize the current state of the art understanding of degrading faults in industry standards and technical publications.

NOTE Terminology in the referenced publications and standards is not always aligned to terms and definitions of the ISO 26262 series. When referencing publications and standards, the terminology of the referenced work is used.

5.2 Degrading faults in industry standards

5.2.1 JEDEC JEP122H[4]

The JEDEC Solid State Technology Association is a semiconductor industry trade association and standardization body. JEDEC has over 300 companies as members and publishes electronics standards on a wide variety of topics.

JEDEC JEP122H is the latest revision on JEDEC's standard for "Failure Mechanisms and Models for Semiconductor Devices," last updated in 2016. The standard describes eighteen different failure mechanisms, classifying them as being related to the die front end of line (FEoL), die back end of line (BEoL), or packaging. Models are provided for estimating the rates of degradation per failure mode. The information provided in JEP122H is validated by a team of reliability experts from the SEMATECH/ISMI Reliability Council and supported by extensive references to technical publications.

The die FEoL failure mechanisms described by the JEP122H include:

— time dependent dielectric breakdown (TDDB) due to gate oxide breakdown;

— hot carrier Injection (HCI);

— negative bias temperature instability (NBTI);

— surface inversion due to mobile ions;

— floating gate non-volatile memory (NVM) data retention;

— localized charge trapping NVM data retention;

— phase change memory (PCM) NVM data retention.

The die BEoL failure mechanisms described by JEP122H include:

— TDDB due to ILD/low-k/mobile Cu ions;

— aluminium electromigration (EM);

— copper EM;

— aluminium and copper corrosion;

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

— aluminium stress migration (SM);

— copper SM.

The packaging failure mechanisms described in JEP122H include:

— fatigue failures due to temperature cycling and thermal shock;

— interfacial failures due to temperature cycling and thermal shock;

— intermetallic and oxidation failure due to high temperature;

— tin whiskers;

— ion mobility kinetics due to component cleanliness.

5.3 Degrading faults in technical publications

5.3.1 Advanced CMOS Reliability Update: Sub 20 nm FinFET Assessment[5]

Reference [5] was published by Sandia National Laboratories, a research organization of the United States Department of Energy, in 2020. The purpose of the report is to document the most critical failure modes impacting advanced semiconductor technologies using FinFET technology. FinFET based semiconductors are used for most current generation SoCs (system on chip devices), dGPUs (discrete graphics processing units), and DRAMs (dynamic random-access memories) which are used in infotainment, ADAS (advanced driver assistance systems), and ADS (automated driving system) applications. While the use of FinFET transistors enables smaller process geometries (e.g. <20 nm feature size) and faster processing, it also changes the failure mode susceptibility characteristics compared to more traditional planar transistor technologies found in 28 nm and larger process technologies.

The report provides details for the following failure modes:

— die related failure modes:

  — bias temperature instability (BTI);

  — dielectric integrity;

  — HCI;

  — BEoL, EM and stress voiding;

  — middle end of line (MEoL) concerns (also known as middle of line, or MoL);

— packaging and package-die interaction;

— integrated die design and process reliability – electrostatic discharge (ESD);

— radiation effects:

  — total ionizing dose (TID);

  — displacement damage;

  — COTS electronics and radiation effects.

The die and packaging related failure modes discussed can generally be argued to manifest as random degrading faults before becoming intermittent or permanent faults. The ESD and radiation effects can generally be argued to be systematic or transient in nature.

Also of interest is the section on reliability degradation and its impact on circuit/system performance. This section focuses on “soft” logic failures which manifest before “hard” physical failures of the

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

semiconductor devices. As most of the degradation mechanisms discussed result in parameter degradation, it is suggested that statistical methods can be used to predict circuit failures.

5.3.2 Circuit-Based Reliability Consideration in FinFET Technology[6]

Reference [6] is authored by four experts from Taiwan Semiconductor Manufacturing Company (TSMC) in 2017 to describe the primary reliability failure modes of concern for FinFET based process technologies and to present a model for estimating reliability. Comparisons are made between the performance of 28 nm planar technologies versus 16 nm and 7 nm FinFET technologies.

The authors highlight several new reliability concerns including bias temperature instability (BTI), stress-induced leakage currents (SILCs), self-heating effects (SHEs), and time dependent junction degradation (TDJD). Models are proposed to estimate the reliability impacts of these mechanisms, based on a combination of simulation and reliability testing.

5.3.3 Intermittent Faults and Effects on Reliability of Integrated Circuits[7]

Reference [7] is authored by a reliability expert from AMD in 2008 and studies intermittent faults. An experiment was conducted using more than 250 servers (from pre-2008) to provide over 300 server years of operational data. Identified memory single bit errors were analysed for root cause, and the findings documented. The rates of occurrence of the errors introduced by these faults can vary from one design to another and one technology to another.

Failure modes discussed in this paper include ultra-thin oxide breakdown, soft breakdown (SBD), EM voids, barrier layer material (BLM) cracks, and crosstalk as sources of intermittent faults. It is noted that these intermittent faults can be detected by monitoring the Vmin (voltage minimum) thresholds necessary for correct operation. Mitigations are discussed in terms of systematic avoidance, screening at manufacturing test, and online fault detection in application including failure prediction.

6 Literature survey on predictive maintenance

6.1 General

This document reviews many technical documents to summarize the current state of the art understanding of predictive maintenance in industry standards and technical publication. Additional application domain specific standards are in development (e.g. IEC 63270[8]).

NOTE Terminology in the referenced publications and standards is not always aligned to the terms and definitions of the ISO 26262 series. When referencing publications and standards, the terminology of the referenced work is used.

6.2 Predictive maintenance in industry standards

6.2.1 IEC 61508[9]

IEC 61508 is a basic safety publication for functional safety which was the original basis for the ISO 26262 series. The 2010 edition of the standard includes guidance on the use of fault forecasting, maintenance, and supervisory actions supported by artificial intelligence (AI) systems.

6.2.2 IEEE Std 1856[3]

IEEE Std 1856 provides an industry-independent approach to the use of predictive maintenance and similar techniques. This standard is intended to be applied at many different levels of design abstraction and is not specific to semiconductor technologies. This standard applies the terms “prognostics” and “Prognostics and Health Management (PHM)” interchangeably with predictive methods. The standard is primarily focused on estimating the remaining useful life (RUL) after a fault is detected, rather than the method by which the fault is detected.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

IEEE Std 1856 provides a lifecycle model for PHM as illustrated in Figure 1:

— the product is initially deployed without faults;

— an off-nominal behaviour (fault) is detected;

— a failure occurs.

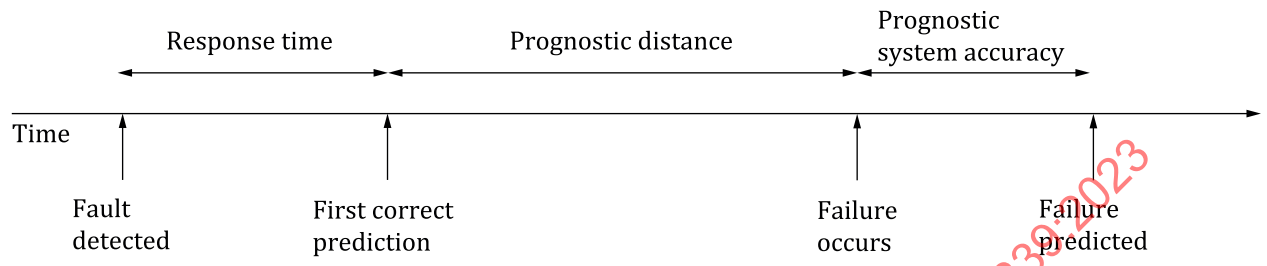


Figure 1 — IEEE Std 1856-2017 lifecycle model for prognostics

The IEEE Std 1856 model introduces three metrics, which when used together can be used to compare the effectiveness of different PHM approaches:

— the response time for the predictive algorithm, defined as the time between first fault detection and first correct prediction of RUL;

— the prognostic distance, defined as the time between the correct prediction and the occurrence of a failure;

— the prognostic system accuracy, defined as the difference between the predicted failure time and the actual failure time.

NOTE Prognostic system accuracy can be positive (failure occurs before prediction) or negative (failure occurs after prediction).

In IEEE Std 1856-2017, Annex A, the standard provides additional guidance. The content on levels of PHM implementation closely matches the ISO 26262 series approach of performing analysis on multiple levels of design hierarchy: device, component, assembly, sub-system, system, and system of systems.

6.3 Predictive maintenance in technical publications

6.3.1 A Survey of Online Failure Prediction Methods[10]

Reference [10] is a literature survey compiled by three researchers from Humboldt University in Berlin in 2010. It is intended to provide a picture of the state of the art in online failure prediction methods as of 2010. Some of the key information included in this document is:

— a lifecycle approach based on the progression of faults to errors to failures which is largely compatible with the ISO 26262 series;

— a definition of nine metrics to evaluate predictive methods, with focus on precision and recall;

— a taxonomy of failure prediction methods which introduces twenty-two categories;

— a review and classification of forty-seven different implementations defined in technical publications into the twenty-two categories.

6.3.2 An Odometer for CPUs[11]

Reference [11] is an article published in the IEEE Spectrum magazine in 2011. It provides a simplified introduction to the topic of degrading faults and introduces one possible detection mechanism. The

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

description of silicon aging mechanisms includes HCI, BTI, and oxide breakdown. A degradation detection mechanism is described which uses the comparison of two ring oscillators (one run in normal conditions, the other under stress conditions).

6.3.3 Circuit Failure Prediction for Robust System Design in Scaled CMOS [12]

Reference [12] is one of many papers on the subject written by Professor Mitra, director of the Stanford University Robust Systems Group. The work focuses on the detection of faults before they can generate errors or failures of a system. Mitra separates the product lifecycle into early life, useful life, and end of life according to a bathtub curve model and emphasizes the need to address the semiconductor physics dominant in each lifecycle phase to maximize the effectiveness of fault detection and error prediction.

The NBTI degrading failure mode is considered a dominant degrading failure mode and prime candidate for predictive mechanisms. In addition, methods which can provide self-repair of NBTI based degradation are discussed. Mitra introduces an online test mechanism, CASP (Concurrent Autonomous chip self-test using Stored Patterns) as one possible mechanism for detection and prediction.

6.3.4 A Circuit Failure Prediction Mechanism (DART) for High Field Reliability [13]

Reference [13] considers the impact of degrading fault mechanisms such as channel hot carrier (CHC), NBTI, and TDDB on timing parameters in a semiconductor device. A mitigation strategy is proposed, and its effectiveness is evaluated using a performance index called DART:

— degrade factors – as many types of degradation as possible are considered;

— accuracy – predicted degradation is as accurate as possible;

— report and repair – sufficient information is reported to enable mitigation during usage;

— test coverage – high detection of degrading faults is achieved.

Also of interest is data showing that the same timing parameter can be impacted by different degrading fault mechanisms, which have different rates of degradation. Understanding this impact can be crucial for defining test intervals and accurately predicting RUL.

6.3.5 Predicting Remediations for Hardware Failures in Large-Scale Datacenters [14]

Reference [14] provides a system level view of predictive maintenance which is data driven rather than based on physics of individual failure mechanisms at a component level. This machine learning based approach is focused on predicting the necessary repair action based upon detected faults. The RUL of the system is defined based on the class of repair which is predicted rather than by the understanding of specific degradation characteristics. Data are presented showing the effectiveness of this approach as implemented at large scale in Facebook's datacentres.

6.3.6 Improving Analog Functional Safety Using Data-Driven Anomaly Detection [15]

Reference [15] provides an example implementation of predictive maintenance in a functional safety context. The authors developed a recurrent neural network (RNN) for predicting errors based on detecting faults using multiple sensor technologies. This approach is data driven, meaning that it identifies potential errors based on data patterns without an understanding of the underlying physics of failure. The focus of this mechanism is predicting whether a fault will result in an error, rather than predicting the remaining useful lifetime after a fault is detected.

7 Degrading faults and the ISO 26262 series

7.1 Understanding the lifecycle of degrading faults

Figure 2 illustrates an example lifecycle of a degrading fault.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

The lifecycle is broken up into three phases following a bathtub curve reliability model (refer to ISO 26262-11:2018, 4.6.1.5): infant mortality, useful life, and end of life, along an X axis representing time. The vertical dashed lines represent the changes in lifecycle phases.

The Y axis represents a voltage margin for an element. The horizontal dashed line is the minimum voltage margin needed for correct operation. If the voltage margin drops below this limit, malfunctioning behaviour can be induced when the element is stimulated.

NOTE 1 The choice of voltage margin as the critical parameter for degradation is only for illustrative purposes.

NOTE 2 The curve shown in Figure 2 is one example and can be different depending on the process technology uses and the critical parameter monitored.

The solid curve represents the element's expected voltage margin degradation over time when no fault is present. During the infant mortality phase the element is newly manufactured and has sufficient voltage margin to operate properly unless a degrading fault is present. Additional permanent faults can be present which are largely removed from the population during manufacturing test. As the element is exposed to wear and stress, the voltage margin decreases. As the element enters the end-of-life phase, it has exceeded its expected lifespan. Once the voltage margin decreases beyond the minimum operating threshold, the element begins to exhibit malfunctions when stimulated.

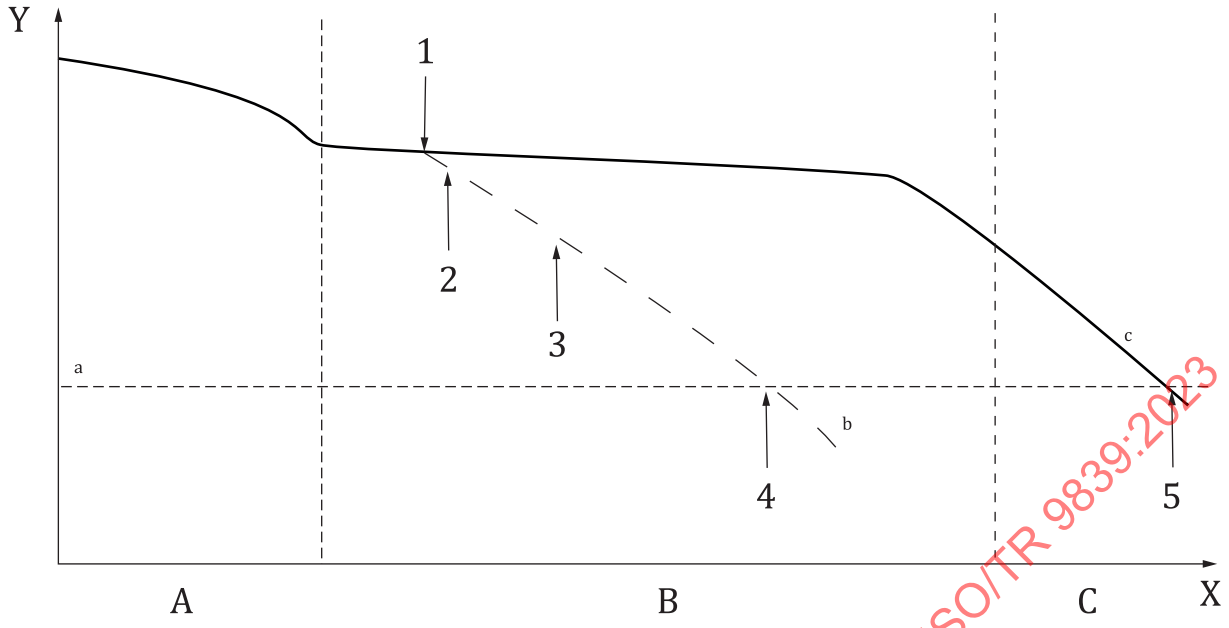
NOTE 3 An element which is used beyond its expected lifespan can exhibit malfunctions without the presence of a random hardware fault.

The dashed curve represents voltage margin degradation in the presence of a degrading fault. The observable degradation accelerates unexpectedly, to the point that it crosses the minimum voltage threshold for correct operation during the useful life phase. Once the threshold is crossed, the element will cause errors or failures if stimulated. If a safety mechanism is present, it is possible to detect the degrading fault before it can cause an error or failure.

NOTE 4 The effectiveness of a predictive maintenance safety mechanism to detect abnormal degradation is dependent on attributes such as the time of measurement and multiple measurements to establish the rate of degradation and to distinguish it from normal degradation.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved



Key

X time
Y voltage margin
A infant mortality phase
B useful life phase
C end of life phase
1 degrading fault occurs
2 degrading fault observable
3 degrading fault detected
4 fault causes error or failure if stimulated
5 normal end of life
a Minimum voltage for correct operation.
b Unexpected voltage degradation (fault present).
c Normal voltage degradation (no fault present).

Figure 2 — Example degrading fault lifecycle

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

Figure 3 illustrates the lifecycle model for non-degrading faults as described in ISO 26262-1. This lifecycle has element level and item level considerations. As described in ISO 26262-10:2018, 4.3, the relationship between faults, errors, and failures can be established at multiple levels of design hierarchy. A failure at the element level can be perceived as a fault at the item level.

In Figure 3 a fault is first occurring at an element level. The fault handling time interval (FHTI) is the sum of the fault detection time interval (FDTI) and the fault reaction time interval (FRTI). The time between the occurrence of the fault and when it can result in malfunctioning behaviour at the item level leading to a hazardous event if not mitigated is the maximum FHTI that can be specified for a safety mechanism to support the functional safety concept. A fault at an element level can occur and be detected before it can result in malfunctioning behaviour at the item level.

EXAMPLE 1 A periodic test of memory executing within the maximum FHTI can detect a fault before it is stimulated during normal usage.

© ISO 2023 – All rights reserved

The fault tolerant time interval (FTTI) is the time between a fault at the item level and malfunctioning behaviour resulting in a hazardous event if not mitigated. Faults, errors and failures are seen at different levels of hierarchy at different times, as illustrated in ISO 26262-10:2018, Figure 5.

EXAMPLE 2 Communication is lost to a sensor module.

Figure 3 differs from ISO 26262-1:2018, Figure 5. ISO 26262-1:2018, Figure 5 illustrates a scenario in which the fault at the element level immediately causes a fault resulting in malfunctioning behaviour at the item level. Not all faults at the element level will result in an immediate malfunctioning behaviour at the item level. As such Figure 3 provides a more generalized view of the relationship between FHTI and FTTI as compared to ISO 26262-1:2018, Figure 5.

So long as the fault is detected and responded in time to prevent the occurrence of a hazardous event, then the fault is sufficiently mitigated.

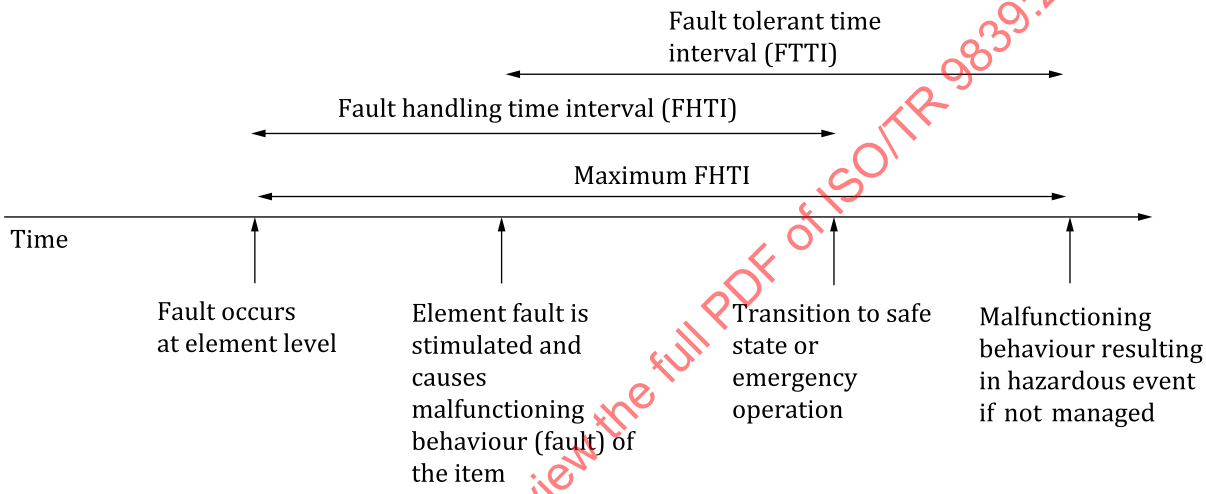


Figure 3 — ISO 26262 lifecycle model for non-degrading faults

Figure 4 maps the lifecycle of a degrading fault from Figure 2 onto the non-degrading fault model presented in Figure 3. The time between the occurrence of the degrading fault and the time when it will generate an error or failure if stimulated is the maximum degrading fault handling time interval (DFHTI) can be specified for a predictive maintenance safety mechanism to support the functional safety concept. Like the FHTI, the DFHTI can be broken into a degrading fault detection time interval (DFDTI) and a degrading fault reaction time interval (DFRTI).

The same criterion for effective mitigation applied to non-degrading faults applies to degrading faults. If a degrading fault is detected and handled before a hazardous event occurs, the degrading fault is sufficiently mitigated.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

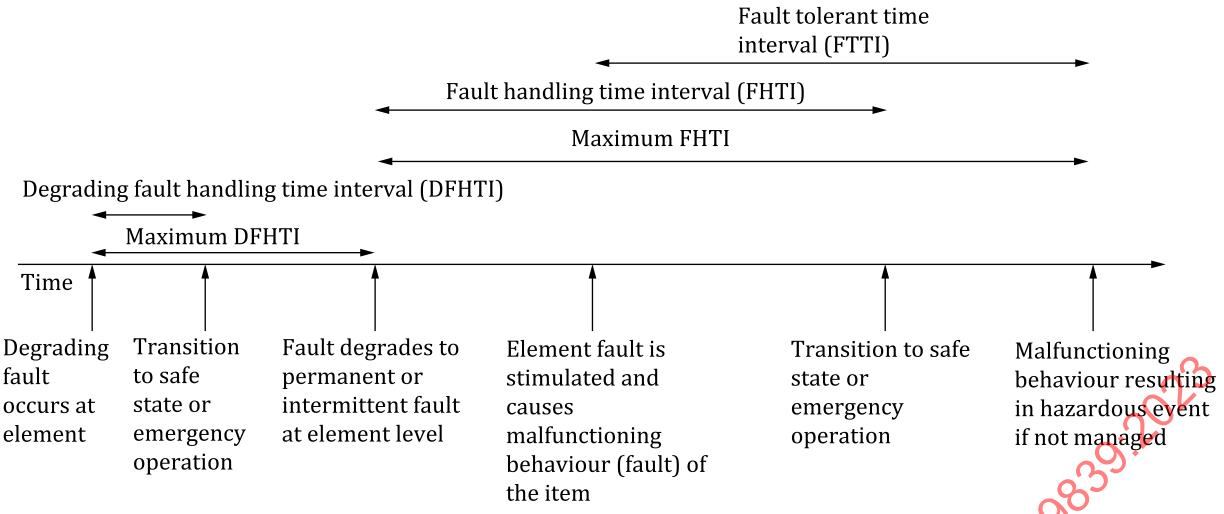


Figure 4 — Lifecycle model for degrading faults

7.2 Classification of degrading faults

The root cause of a hardware fault can be either systematic or random in nature. The same consideration applies to degrading faults.

Systematic faults, including degrading faults, are primarily addressed by avoidance measures such as robust processes and detection before a product is deployed to the field.

Random hardware faults, including degrading faults, are considered in the calculation of the relative hardware metrics (SPFM, LFM) and the probabilistic metrics (PMHF or EEC). When a fault has been classified as a random hardware fault, it can further be classified as safe, single-point, residual, or multiple-point (perceived, detected, or latent). ISO 26262-10:2018, 8.1 and Figure 10 can assist in the classification of random hardware faults. This guidance is the same for all types of random hardware faults.

ISO 26262 random hardware metrics are not only focused on the permanent fault model. The ISO 26262 series considers all relevant fault models. ISO 26262-5:2018, 8.4.7 b) NOTE 2 states that transient faults are considered when shown to be relevant. Degrading faults can also be considered if shown to be relevant.

7.3 Quantifying degrading fault base failure rate

ISO 26262-5:2018, 8.4.3 provides three options for establishing the base failure rate (BFR)of relevant faults. These methods can be used to establish BFRs for random degrading faults.

Two strategies are identified to quantify the failure rate due to degrading faults. One is to estimate the failure rate for degrading faults in addition to the failure rates for other types of faults. The other is to consider the failure rate of degrading faults as a subset of the failure rate for permanent or intermittent faults.

EXAMPLE A set of failures is initially classified as resulting from permanent faults. With additional data, it is established that some of the failures are the result of degrading faults, which were perceived as permanent after sufficient degradation had occurred.

7.3.1 Industry standards and models

ISO 26262-5:2018, 8.4.3 a) provides the options of using hardware part data from a recognized industry source. Multiple examples of such sources are provided in ISO 26262-5:2018, 8.4.3 a) EXAMPLE 1.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

Currently there are no identified industry sources which provide models or handbook data for calculating the BFR due to degrading faults. JEDEC JEP122H[4] provides acceleration models which can be used to estimate the degradation of certain degrading faults (e.g. HCI, NBTI) but does not provide estimation of the rate of occurrence.

7.3.2 Field data

ISO 26262-5:2018, 8.4.3 b) provides the option of using statistics based on field returns to establish a BFR for a given failure mode. It is suggested in ISO 26262-5:2018, 8.4.3 b) NOTE 5 that such arguments can be calculated as described in ISO 26262-8:2018, Clause 14.

Reliability experiments or field data can apply a statistical approach. The data collected by such an approach can apply a 70 % confidence level using a chi-square distribution as described in ISO 26262-8:2018, 14.4.5.2.4. JEDEC JESD85A[16] provides examples of calculating such a distribution for experimental test results.

7.3.3 Expert judgement

ISO 26262-5:2018, 8.4.3 c) provides the option of using expert judgement to establish the BFR. This can be done with a combination of approaches including field data, testing, reliability analyses and simulation as per ISO 26262-5:2018, 8.4.3 c) NOTE 6.

EXAMPLE An application of expert judgement can include a combination of establishing a BFR using reliability testing and estimating degradation rate using JEDEC JEP122H[4] or a simulation based on physics of failure models following JEDEC JESD91B[17].

8 Applying predictive maintenance

8.1 Diagnostic coverage (DC) evaluation for predictive mechanisms

ISO 26262-5:2018 does not include normative requirements for establishing the DC of safety mechanisms. ISO 26262-5:2018, Annex D (and by extension ISO 26262-11:2018 for semiconductors) can be used as the starting point for evaluating DC. The DC is supported with a proper rationale. Neither source directly considers predictive maintenance.

Many predictive maintenance safety mechanisms are built upon existing classes of safety mechanisms. Existing guidance can be considered as a starting point for establishing a DC claim.

EXAMPLE ISO 26262-5:2018, Table D.5 suggests that a test pattern can typically achieve high DC for analogue I/O. The same test pattern when used for fault detection in a predictive maintenance safety mechanism can assume similar DC as an initial DC claim.

Guidance which is provided to establish and justify the DC of an arbitrary safety mechanism not found in ISO 26262-5:2018, Annex D or ISO 26262-11:2018 can be applied to predictive mechanisms. Analytical arguments, expert judgement and experiments (including simulation and fault injection) are possible sources for data to support a DC claim for a predictive mechanism.

8.2 Considering random hardware metrics

8.2.1 Impacting the SPFM and LFM

For a safety mechanism to provide a detection benefit considered in the SPFM, the ISO 26262 series provides some constraints in ISO 26262-5:2018, 7.4.3.3. Similar consideration for the LFM is provided in ISO 26262-5:2018, 7.4.3.4. In both cases the primary requirements can be summarized as:

— the safety mechanism must detect and achieve or maintain a safe state or transition to emergency operation within the FTTI or FHTI for SPFM or the MPFDTI for LFM;

— the DC with respect to residual faults or latent faults, respectively, is established.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved

The approach can be extended to degrading faults by considering the DFHTI in addition to the FTTI and FHTI for calculating the SPFM. So long as the fault is detected and responded in time to prevent the occurrence of a hazardous event, then the fault is sufficiently mitigated.

In calculating the SPFM and LFM including degrading faults and predictive mechanisms, several aspects are considered if relevant to the safety concept:

— the confidence in the computed RUL and the maximum DFHTI;

— the ratio of the BFR of degrading faults as compared to permanent, transient and intermittent faults; and

— the classification of degrading faults according to ISO 26262-10:2018, Clause 8 and Figure 10.

False positive detections do not impact the metric calculation but can impact the rate of field returns.

Per ISO 26262-5:2018, 6.4.2, the relevant characteristics of the safety mechanism are included in the safety requirements and verified according to ISO 26262-5:2018, 6.4.9.

EXAMPLE The maximum DFHTI is one possible relevant characteristic.

Annex A provides one integrated approach to handling degrading faults with predictive maintenance.

8.2.2 Application as a dedicated measure

An alternative approach is to apply predictive maintenance as a dedicated measure for mitigating degrading faults. Dedicated measures can be used to argue that the probability of occurrence of faults is sufficiently low, such that:

— single point faults are acceptable per ISO 26262-5:2018, 9.4.1.2 and ISO 26262-5:2018, 9.4.3.5 or

— residual faults with less than 90 % DC are acceptable per ISO 26262-5:2018, 9.4.1.3 and ISO 26262-5:2018, 9.4.3.6 or

— a rationale can be created for how safety goals can be achieved despite PMHF targets not being met (ISO 26262-5:2018, 9.4.2.4 NOTE 6).

ISO 26262:2018 does not include any requirements for dedicated measures similar to those present for safety mechanisms. ISO 26262-5:2018, 9.4.1.2 NOTE 2 provides examples of dedicated measures which are typically implemented as design or production measures rather than online measures.

8.3 Considering RUL prediction

The ISO 26262 series does not have any metrics defined related to the prediction of RUL. RUL is of interest in the current state of the art for two scenarios.

— The average age of vehicles in the field continues to rise, many of which can be operating beyond the original designed lifetime of their safety related elements. Understanding when a safety related element is no longer trustworthy can provide drivers guidance to replace worn out elements before they are exposed to hazards.

— New applications using new technologies, such as autonomous driving, can have less confidence in operational profiles than more established applications using legacy technologies. In addition, fully autonomous vehicles cannot rely on a human driver for fallback operation and can take more appropriate actions if the RUL of primary and backup systems is known.

The metrics from the IEEE Std 1856 [3] can be used to compare the performance for different predictive maintenance solutions. The IEEE Std 1856 response time can illustrate the speed of prediction after the first detection of a fault. Some solutions consider multiple fault detections before the RUL can be predicted.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 9839:2023

© ISO 2023 – All rights reserved