FINAL
DRAFT

TECHNICAL SPECIFICATION

ISO/IEC DTS 22237-31

ISO/IEC JTC **1**/SC **39**

Secretariat: **ANSI**

Voting begins on:
2023-09-04

Voting terminates on:
2023-10-30

Information technology — Data centre facilities and infrastructures —

Part 31: Key performance indicators for resilience

Reference number
ISO/IEC DTS 22237-31:2023(E)

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

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take 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 and IEC 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 and https://patents.iec.ch. ISO and IEC 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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 39, *Sustainability, IT and data centres*.

A list of all parts in the ISO/IEC 22237 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

The various parts of the ISO/IEC 22237 series reference four qualitative Availability Classes as well as structural definitions to categorize different designs. The documents also refer to resilience criteria in order to improve structural requirements for a qualitative approach.

In order to meet the requirements necessary for evaluating or comparing different designs or to validate service level agreements (SLAs) for data centres, this document introduces quantitative metrics as key performance indicators (KPIs). The proposed KPIs cover resilience attributes, including dependability and fault tolerance metrics. The characteristics of aging of infrastructures are covered by reliability criteria.

Through the use of KPIs, the comparison of designs, functional elements and components of infrastructure designs becomes possible. In addition, it is possible to optimize data centre infrastructures (DCI) with holistic targets. It is recommended to use the KPIs of this document in combination with the efficiency and sustainability KPIs of the ISO/IEC 30134 series.

ISO/IEC 22237-1:2021, Annex A, demonstrates that a single KPI, such as Availability, is not sufficient to describe the complexity of a DCI. In recognition, this document has been developed in order to compare and value different designs with different Availability Classes of DCIs based on a set of selected KPIs.

Furthermore, the document has been created to establish KPIs for resilience of DCIs with defined resilience levels. The resilience objectives can vary depending on the outcome of the ISO/IEC 22237-1 risk analysis, the end user information technology equipment (ITE) process criticality, and the data centre type of business.

Using the different stages of a data centre design process, this document describes in which phases the application of KPIs for resilience is appropriate. With its assistance, data centre designers, planners and operators will be supported in defining resilience Levels, performing theoretical assessments and designing and operating DCIs which are able to meet SLAs.

Information technology — Data centre facilities and infrastructures —

Part 31: Key performance indicators for resilience

1 Scope

This document:

a) defines metrics as key performance indicators (KPIs) for resilience, dependability, fault tolerance and availability tolerance for data centres;

b) covers the data centre infrastructure (DCI) of power distribution and supply, and environmental control;

c) can be referred to for covering further infrastructures, e.g. telecommunications cabling;

d) defines the measurement and calculation of the KPIs and resilience levels (RLs);

e) targets maintainability, recoverability and vulnerability;

f) provides examples for calculating these KPIs for the purpose of analytical comparison of different DCIs.

This document does not apply to IT equipment, cloud services, software or business applications.

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/IEC 22237-1, *Information technology — Data centre facilities and infrastructures — Part 1: General concepts*

ISO/IEC 22237-3, *Information technology — Data centre facilities and infrastructures — Part 3: Power distribution*

ISO/IEC 22237-4, *Information technology — Data centre facilities and infrastructures — Part 4: Environmental control*

ISO/IEC 30134-1, *Information technology — Data centres — Key performance indicators — Part 1: Overview and general requirements*

IEC 61078, *Reliability block diagrams*

3 Terms and definitions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22237-1, ISO/IEC 22237-3, ISO/IEC 22237-4 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/

3.1.1
availability
ability to be in a state to perform as required

[SOURCE: IEC 60050-192:2015, 192-01-23, modified — Notes 1 and 2 to entry have been deleted.]

3.1.2
availability tolerance
ability to be in a state to perform as required with certain *failures* (3.1.8) present

3.1.3
dependability
ability to perform as and when required

Note 1 to entry: In this document, the term is used for the determination of data centre *reliability* (3.1.28), *availability* (3.1.1) and *failure rate* (3.1.9).

[SOURCE: IEC 60050-192:2015, 192-01-22, modified — Notes 1 and 2 to entry have been replaced by a new Note 1 to entry.]

3.1.4
double point of failure
DPoF
combination of two functional elements whose simultaneous *failures* (3.1.8) cause overall system *fault* (3.1.10)[SOURCE: IET, Journal of Engineering, Vol. 2019 Iss. 12, 99. 8419-8427][1]

3.1.5
double point of reduced availability
DPoRA
combination of two functional elements whose simultaneous *failures* (3.1.8) result in the violation of the *service level agreement (SLA)* (3.1.30)[SOURCE: IET, Journal of Engineering, Vol. 2019 Iss. 12, 99. 8419-8427][1]

3.1.6
down state
state of being unable to perform as required, due to *failures* (3.1.8) or *faults* (3.1.10)

Note 1 to entry: The state can be related to failures of items or faults at a specified *operation point (OP)* (3.1.21).

[SOURCE: IEC 60050-192:2015, 192-02-20]

3.1.7
event
something that happens and leads to one or more *failures* (3.1.8) or *faults* (3.1.10)

3.1.8
failure
<of an item> loss of ability to perform as required

Note 1 to entry: In this context it is irrelevant if the cause was planned or unplanned.

[SOURCE: IEC 60050-192:2015, 192-03-01, modified — Notes 1 to 3 to entry have been replaced by Note 1 to entry.]

3.1.9
failure rate
limit of the ratio of the conditional probability that the instant of time, *T*, of a *failure* (3.1.8) of a product falls within a given *time interval* (3.1.35) (*t, t* + Δ*t*) and the duration of this interval, Δ*t*, when Δ*t* tends towards zero, given that the item is in an *up state* (3.1.36) at the start of the time interval

[SOURCE: IEC 60050-192:2015, 821-12-21]

3.1.10
fault
inability to perform as required, due to an internal state

Note 1 to entry: Opposite of success. In the context of the expected *resilience level (RL)* (3.1.26), at a specified *operation point (OP)* (3.1.21).

[SOURCE: IEC 60050-192:2015, 192-04-01]

3.1.11
fault tolerance
ability to continue functioning with certain *faults* (3.1.10) present

[SOURCE: IEC 60050-192:2015, 192-10-09]

3.1.12
information technology equipment
ITE
equipment providing data storage, processing and transport services together with equipment dedicated to providing direct connection to core and/or access networks

3.1.13
infrastructure
technical systems providing the functional capability of the data centre

Note 1 to entry: Examples are power distribution, environmental control, telecommunications cabling, physical security

[SOURCE: ISO/IEC 22237-1:2021, 3.1.21, modified — "telecommunications cabling" has been added to the list in Note 1 to entry.]

3.1.14
inherent availability
availability (3.1.1) provided by the design under ideal conditions of operation and maintenance

[SOURCE: IEC 60050-192:2015, 192-08-02]

3.1.15
mean down time
MDT
average downtime caused by scheduled and unscheduled maintenance, including any logistics time (expectations including detection time, diagnostic time, spare part delivery time, repair time)

[SOURCE: IEEE Std. 493-2007]

3.1.16
mean operating time between failures
MTBF
expectation of the duration of the operating time between *failures* (3.1.8)

Note 1 to entry: Mean operating time between failures should only be applied to repairable items. For non-repairable items, see *mean operating time to failure* (3.1.17).

Note 2 to entry: The term “mean time between failures” (MTBF) is used synonymously in this document.

[SOURCE: IEC 60050-192:2015, 192-05-13]

3.1.17
mean operating time to failure
expectation of the operating time to *failure* (3.1.8)

Note 1 to entry: In the case of non-repairable items with an exponential distribution of operating times to failure, i.e. a constant *failure rate* (3.1.9), the mean operating time to failure is numerically equal to the reciprocal of the failure rate. This is also true for repairable items if after restoration they can be considered to be "as-good-as-new".

Note 2 to entry: The term “mean time to failures” (MTTF) is used synonymously in this document.

[SOURCE: IEC 60050-192:2015, 192-05-11]

3.1.18
mean time between maintenance
MTBM
average time between all maintenance *events* (3.1.7), scheduled and unscheduled, and also includes any associated logistics time

[SOURCE: IEEE Std. 493-2007]

3.1.19
mean time to restoration
mean time to replace or repair a failed component

Note 1 to entry: Logistics time associated with the repair, such as parts acquisitions or crew mobilization, are not included.

[SOURCE: IEEE Std. 493-2007]

3.1.20
normal resilience level
NRL
resilience level (3.1.26) mandatory during nominal operation

3.1.21
operation point
OP
point of reference for which calculation of *resilience level* (3.1.26) is performed

Note 1 to entry: This can be an individual *socket* (3.1.33) taking into account the entire data centre infrastructure (DCI) or certain defined parts of the *infrastructure* (3.1.13). The documentation of the referenced operation point (OP) is required for any key performance indicator (KPI).

3.1.22
operational availability
availability (3.1.1) experienced under actual conditions of operation and maintenance

[SOURCE: IEC 60050-192:2015, 192-08-03, modified — Note 1 to entry has been deleted.]

3.1.23
past availability
availability (3.1.1) measured during a period of 1 year

Note 1 to entry: For the purposes of this document, 1 year equals 8 760 hours.

3.1.24
reduced resilience level
RRL
resilience level (3.1.26) mandatory during reduced operation in case of one or more *failures* (3.1.8)

3.1.25
resilience
ability to withstand and reduce the magnitude and/or duration of disruptive *events* (3.1.7), including the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event[SOURCE: IEEE Task Force on Definition and Quantification of Resilience, PES-TR65:2018-04][2]

3.1.26
resilience level
enumeration of attributes for the determination of *resilience* (3.1.25) aspects of a defined service at a defined *operation point (OP)* (3.1.21)

3.1.27
redundancy
<in a system> provision of more than one means for performing a function

Note 1 to entry: In a data centre, redundancy can be achieved by duplication of devices, functional elements, and/or supply paths.

[SOURCE: IEC 60050-192:2015, 192-10-02, modified — Note 1 to entry has been replaced by a new Note 1 to entry.]

3.1.28
reliability
ability to perform as required, without *failure* (3.1.8), for a mean *time interval* (3.1.35), under given conditions

[SOURCE: IEC 60050-192:2015, 192-01-24, modified — Notes 1 to 3 to entry have been deleted.]

3.1.29
resilience model
representation ***x*** of the data centre infrastructure (DCI) that shows all required subsystems, components and items as well as their systemic interdependencies

3.1.30
service level agreement
SLA
agreement defining the content and quality of the service to be delivered and the timescale in which it is to be delivered

[SOURCE: ISO/IEC TS 22237-7:2018, 3.1.20]

3.1.31
single point of failure
SPoF
functional element whose *failure* (3.1.8) causes overall system *fault* (3.1.10)[SOURCE: IET, Journal of Engineering, Vol. 2019 Iss. 12, 99. 8419-8427][1]

3.1.32
single point of reduced availability
SPoRA
functional element whose *failure* (3.1.8) results in the violation of the *service level agreement (SLA)* (3.1.30)[SOURCE: IET, Journal of Engineering, Vol. 2019 Iss. 12, 99. 8419-8427][1]

3.1.33
socket
connection enabling supply of power to attached equipment

Note 1 to entry: This can be a de-mateable or a hardwired connection.

[SOURCE: ISO/IEC 22237-3:2021, 3.1.26]

3.1.34
system success path
infrastructural path, consisting of a minimum of functional elements, to express the success of the *infrastructure* (3.1.13) system at the *operation point (OP)* (3.1.21) to be in the *up state* (3.1.36)

Note 1 to entry: Each functional element can consist of one or more devices.

3.1.35
time interval
part of the time axis limited by two instants

[SOURCE: IEC 60050-192:2015, 113-01-10]

3.1.36
up state
state of being able to perform as required

Note 1 to entry: The state can be related to items or to a specified *operation point (OP)* (3.1.21).

[SOURCE: IEC 60050-192:2015, 192-02-01]

3.2 Symbols and abbreviated terms

3.2.1 Symbols

For the purposes of this document, the symbols given in ISO/IEC 22237-1, ISO/IEC 30134-1 and the following apply.

A_i	inherent availability
A_o	operational availability
$A_{o,NRL}$	normal resilience level operational availability
$A_{o,req}$	required operational availability
$A_{o,RRL}$	reduced resilience level operational availability
A_p	past availability
$D(\boldsymbol{x})$	disjoint sum of system success paths of $\boldsymbol{x}$
Δt	duration of time interval
λ_i	inherent failure rate
λ_{mean}	mean failure rate
λ_o	operational failure rate
λ_p	past failure rate
$f(t)$	probability density function (PDF)
N_f	number of failures during time interval t
N_x	number of x
$R(t)$	reliability in time interval t
R_i	inherent reliability

R_o	operational reliability
R_p	past reliability
$S(\boldsymbol{x})$	success, $\boldsymbol{x}$ is in the up state
$S(\boldsymbol{x}_E)$	environmental control success function
$S(\boldsymbol{x}_{OP})$	overall success function
$S(\boldsymbol{x}_P)$	power and distribution success function
t_x	time interval of x
T	instant of time
$\boldsymbol{x}_m$	vector of elements of $x_{m(i)}$ of the mth DCI
$x_{m(i)}$	functional element x of the mth DCI with the index i
X_m	set of all functional elements x of the mth DCI

3.2.2 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 22237-1, ISO/IEC 30134-1 and the following apply.

CBEMA	Computer Business Equipment Manufacturers Association
DCI	data centre infrastructure (infrastructure residing within a data centre)
DPoF	double point of failure
DPoRA	double point of reduced availability
FAT	factory acceptance test
FMECA	Failure Mode Effects and Criticality Analysis
ITE	information technology equipment
KPI	key performance indicator
MDT	mean down time
MTBF	mean operating time between failures
MTBM	mean time between maintenance
MTTF	mean time to failure
MTTR	mean time to restoration
NRL	normal resilience level
OP	operation point
PDF	probability density function
RBD	reliability block diagram

RL	resilience level
RRL	reduced resilience level
SLA	service level agreement
SPoF	single point of failure
SPoRA	single point of reduced availability
SSP	system success path

4 Area of application

4.1 General

The KPIs for resilience, including the dependability, fault tolerance and availability tolerance KPIs, as specified in this document are associated with the following DCIs of the ISO/IEC 22237 series:

a) ISO/IEC 22237-3: Power supply and distribution;

b) ISO/IEC 22237-4: Environmental control.

The application can be extended to additional infrastructures, e.g. ISO/IEC TS 22237-5 (telecommunications cabling infrastructure).

4.2 DCI service definition

To determine system success at the operation point (OP), it is required to define the relevant DCI. In general, the overall success function $S(\boldsymbol{x}_{\mathrm{OP}})$ is represented by a certain number, N, of successes of infrastructures inside the DCI as shown in the Formula (1):

$$S(\boldsymbol{x}_{\mathrm{OP}}) = \bigcap_{m=1}^{N} S(\boldsymbol{x}_m) \tag{1}$$

The success $S(\boldsymbol{x}_m)$ of the enumerated infrastructures $\boldsymbol{x}_m$ is connected by the $\cap$ operator. In general, these infrastructures are not mutually exclusive, because the functions depend on each other. Functional dependencies shall be taken into account in the calculations.

To operate the information technology equipment (ITE) within the permitted parameters, the service success requires:

— adequate service quality of the power supply and distribution, fed by the sockets;

— adequate service quality of the cooling by the environmental control.

The DCI is represented by the vector $\boldsymbol{x}$, which refers to Formula (1). The operation of the DCI is considered to be successful if power supply and distribution $S(\boldsymbol{x}_{\mathrm{P}})$ and environmental control $S(\boldsymbol{x}_{\mathrm{E}})$ are by themselves operating successfully at the specified OP. Formula (2) defines the system success function as follows:

$$S(\boldsymbol{x}_{\mathrm{OP}}) = S(\boldsymbol{x}_{\mathrm{P}}) \cap S(\boldsymbol{x}_{\mathrm{E}}) \tag{2}$$

The operation of the power supply and distribution system is deemed successful, $S(\boldsymbol{x}_{\mathrm{P}}) = 1$, if the infrastructure provides the required power quality to the specific socket defined as OP. A violation of the power quality, as required by the ITE at a specific socket, is defined as a failure: $S(\boldsymbol{x}_{\mathrm{P}}) = 0$. The cause of the failure can be planned or unplanned.

The operation of the environmental control system is deemed successful, $S(x_E)=1$, if the environmental requirements of the ITE at the specified socket defined as OP are satisfied. A violation of the environmental conditions of a specific functional element or device is defined as a failure: $S(x_E)=0$. The cause of the failure can be planned or unplanned.

A failure or the combination of failures which lead to $S(x_{OP})=0$ is deemed as fault. For calculation purposes using Formula (2), the following criteria shall be taken into account.

a) The power and cooling capacity of the entire DCI shall be specified.

b) The OP shall be selected in relation to the outcome of the risk analysis.

c) The specified power and cooling capacity shall be given for the selected OP.

d) The service quality of power supply and distribution and environmental control at the selected OP shall be represented by the DCI model.

The selection of the OP depends on the specific task. In general, the OPs with the highest requirements of service quality are of relevance.

5 Resilience considerations as part of the life cycle

5.1 Implementation in the design process

5.1.1 General

According to ISO/IEC 22237-1, the data centre design process is split into 11 project phases. The resilience of the DCI can be managed all along the life cycle, from the strategy phase (1) until the operation phase (11). In particular, the usage of the KPIs for resilience covers the following of these phases.

5.1.2 Phase 1 — Strategy

Phase 1 is for information collection in order to define the project objectives. This phase requires the following.

a) Gather the requirements, for example, SLAs.

b) Decide about application of resilience KPIs for design.

c) Decide about application of resilience KPIs for operation.

d) Define the DCI services for application of KPIs for resilience.

5.1.3 Phase 2 — Objectives

Phase 2 is handled by the owner to convert the strategy into objectives. This phase requires the definition of the resilience objectives according to the risk analysis respective to SLAs.

a) Define the OP, for example: protected/non-protected sockets, server racks, rack rows, etc.

b) Define the maximum accepted downtime at the OP, for example:

— the maximum time interval of loss of the power supply (see ISO/IEC 22237-3);

— the maximum time interval of loss of the power distribution (see ISO/IEC 22237-3);

— supply boundary that ITE can tolerate without experiencing unexpected shutdowns or malfunctions (see Reference [3]);