TECHNICAL SPECIFICATION

ISO/IEC TS 22237-31

First edition
2023-12

Information technology — Data centre facilities and infrastructures —

Part 31: Key performance indicators for resilience

Technologie de l'information — Installation et infrastructures de centres de traitement de données —

Partie 31: Indicateurs clés de performance pour la résilience

Reference number
ISO/IEC TS 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 for validating 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, $t + \Delta t$) and the duration of this interval, Δt, when Δt 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 — Original 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 $\boldsymbol{x}$
e	exponential PDF
$f(t)$	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

$S(\boldsymbol{x}_{\mathrm{E}})$ environmental control success function

$S(\boldsymbol{x}_{\mathrm{OP}})$ overall success function

$S(\boldsymbol{x}_{\mathrm{P}})$ power and distribution success function

t_{MDT} mean down time

t_{MTBF} mean time between failures

t_{MTBM} mean time between maintenance

t_{MTTR} mean time to restoration

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

α confidence rate;

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

χ^2 chi-square distribution function law with two degrees of freedom;

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, $S(\boldsymbol{x}_{\mathrm{E}})=1$, 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: $S(\boldsymbol{x}_{\mathrm{E}})=0$. The cause of the failure can be planned or unplanned.

A failure or the combination of failures which lead to $S(\boldsymbol{x}_{\mathrm{OP}})=0$ 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]);
- the maximum time interval of loss of the environmental control (see ISO/IEC 22237-4);
- the maximum time of fault of the entire DCI.

c) Define the maximum accepted failure rate at the OP deemed as faults during the time interval of reporting.

d) Define the set of KPIs depending on the resilience objective, for example:

- dependability requirements (reliability, availability, failure rate);
- fault tolerance requirements (number of SPoF, number of DPoF);
- availability tolerance requirements (number of SPoRA, number of DPoRA).

The definitions of resilience objectives can be made by making the provisions of 6.6 mandatory during nominal operation (NRL) and during reduced operation (RRL).

5.1.4 Phase 3 — System specifications

Phase 3 defines the target specifications for all infrastructures. The output of the specifications shall be validated in accordance with the objectives of Phase 2.

5.1.5 Phase 4 — Design proposal

Phase 4 offers several options for a design proposal. This phase requires the following.

a) Compare/optimize different designs through the application of KPIs for resilience.

b) Approve compliance of the designs for the defined requirements.

5.1.6 Phase 6 — Functional design

Phase 6 offers the functional design. This phase requires the following.

a) Approve the functional design through the application of KPIs for resilience.

5.1.7 Phase 8 — Final design and project plan

During Phase 8 the designer defines volume and/or pieces for all items of the DCI. To meet the resilience objectives, the definitions made in previous phases shall be taken into account, by the help of the applied KPIs of resilience.

5.1.8 Phase 10 — Construction

Phase 10 includes supervision and acceptance verification of the DCI, until it is put into service. The Resilience objectives shall be taken into account during the following.

a) Factory acceptance tests (FATs).

b) Equipment transportation and installation on site.

c) Commissioning tests, such as functional performance tests (FPT) and integrated system tests (IST);

d) Failure simulations on functional elements;

e) Failure simulations on the entire DCI.

The outcome of this phase is deeper knowledge of the resilience properties of the DCI.

5.1.9 Phase 11 — Operation

Phase 11 describes the handover to the owner for operation. This phase requires the following.

a) Approve compliance of the DCI for the assumptions of the KPIs used.

b) Monitor the defined KPIs of resilience during operation.

c) Approve compliance of the DCI for the defined requirements in case of planned interruptions, times for logistics, response times.

d) Review and, if required, recalculate the KPIs for Resilience of the DCI.

5.2 Documentation during operation

5.2.1 General

Documentation of metrics and causes are the basis for optimization of resilience during operation. In order to be able to monitor aspects of resilience, the organization shall document the following metrics.

a) MTBF and MTTR of the utility supply.

b) MTBF, MTTR, MTBM and MDT data of the functional elements or components.

c) Causes for failures and/or faults.

d) Causes and scope of restoration.

For evaluation and documentation of failures, the Failure Mode Effects and Criticality Analysis (FMECA) is applicable. See Annex D.

5.3 Documentation of resilience level

5.3.1 General

In order to evaluate KPIs for resilience, the following information shall be provided.

a) The resilience model of the DCI.

b) The OPs studied and their load assumptions.

c) The MTBF, MTTR, MTBM and MDT data of the functional elements or components.

d) The number of SPoF and DPoF.

e) If applicable, the number of SPoRA and DPoRA.

f) The calculation method.

Periods of runtime shall be documented on an annual basis, where 1 a = 8 760 h.

The recalculation of the resilience KPIs is required after an incident that involves structural modifications as well as modifications on functional elements. Structural change requires the review and, if necessary, the revision of the resilience model.

5.3.2 Requirements

Cause and duration of violations of the resilience level shall be documented to calculate the past reliability, past availability, and past failure rate.

5.4 Documentation of dependability

5.4.1 Requirements

In general, reliability, availability and failure rate shall be reported at a minimum of four and a maximum of six decimal places. The chosen OP and the load assumption of the DCI shall always be quoted alongside documented values.

To gauge the availability KPI, a corresponding NRL shall be defined.

5.4.2 Recommendations

To distinguish between calculated availabilities, i.e. the inherent availability, the operational availability, and the measured past availability of a data centre in operation, the measurement of A_p (past availability) should be documented in percentage terms. This is also applicable to the measurement of the past reliability, R_p, and the past failure rate, λ_p.

A reduced resilience level (RRL) during periods of planned reconstruction, adaptation or renewal should be defined.

To avoid rounding errors, the data of the system's items should be used at least one order of magnitude higher than the KPIs to be calculated.

5.5 Documentation of fault tolerance

5.5.1 Requirements

The number of SPoF and DPoF shall be documented as integers; see Formulae (14) and (15). Based on the resilience model of the DCI, the KPIs of SPoF and DPoF shall be calculated.

5.6 Documentation of availability tolerance

5.6.1 Requirements

The number of SPoRA and DPoRA shall be documented as integers; see Formulae (16) and (17).

The RRL, as a condition of planned maintenance, shall be defined. Based on the resilience model of the DCI, the operational availability for all cases of SPoF and DPoF shall be calculated. The number of violations of $A_{o,RRL}$ in cases of SPoF gives the number of SPoRA, and in case of DPoF gives the number of DPoRA.

5.6.2 Recommendations

Comparing DCI models in terms of the number of SPoRA and DPoRA allows deeper insights into the resilience characteristics than are acheivable using the number of SPoF and DPoF. Particularly for the optimization and/or comparison of different DCIs, these KPIs are crucial.

6 Determination of KPIs for resilience

6.1 General

ISO/IEC 22237-1 gives a qualitative availability classification, starting with class 1 for low availability and going up to class 4 for high availability. Furthermore, ISO/IEC 22237-1 uses the term "resilience" to specify the coherence between fault tolerance, determined by the number and the design of supply paths, and the data centre availability.

The ISO/IEC 22237 series opens the possibility to combine different Availability Classes in the paths of power supply distribution and environmental control. Asymmetric infrastructure designs are possible, where supply or distribution paths can be different from each other. Different design goals, such as high energy efficiency or minimizing life cycle cost, can lead to very different results.

The design and/or operation of data centres is often contracted by an SLA. SLAs can be limited to the availability for a defined infrastructure service. Occasionally SLAs do not take into account aspects such as reliability, failure rate, fault tolerance and/or reduced availability under constraints. In order to be able to include additional aspects in quantitative considerations, definitions of resilience levels (RLs) under different conditions of operation are introduced.

The validation of RLs and the evaluation and comparison of different designs of data centres rely on meaningful metrics. As shown in 6.2, a variety of metrics is required to describe DCIs in quantitative ways, since each metric focuses on specific properties. This document gives KPIs as dependability metrics as well as tolerance metrics to calculate the reliability, availability, failure rate, fault tolerance and availability tolerance of DCIs.

Data centres are usually designed for a long service life, e.g. in the range of ten or more years. The continuous operation can be supported by predictive maintenance. To determine how an infrastructure will age, the use of the reliability KPI as a function of time can be helpful. By performing a reliability analysis, worn functional elements can be identified and replaced. Additionally, with the help of a reliability analysis, it is possible to prepare strategies in order to renew functional elements or supply paths in product life cycle management according to ISO/IEC TS 22237-7.

6.2 Structuring of the KPIs for resilience

6.2.1 General

Figure 1 summarizes the KPIs for resilience covered by this document.

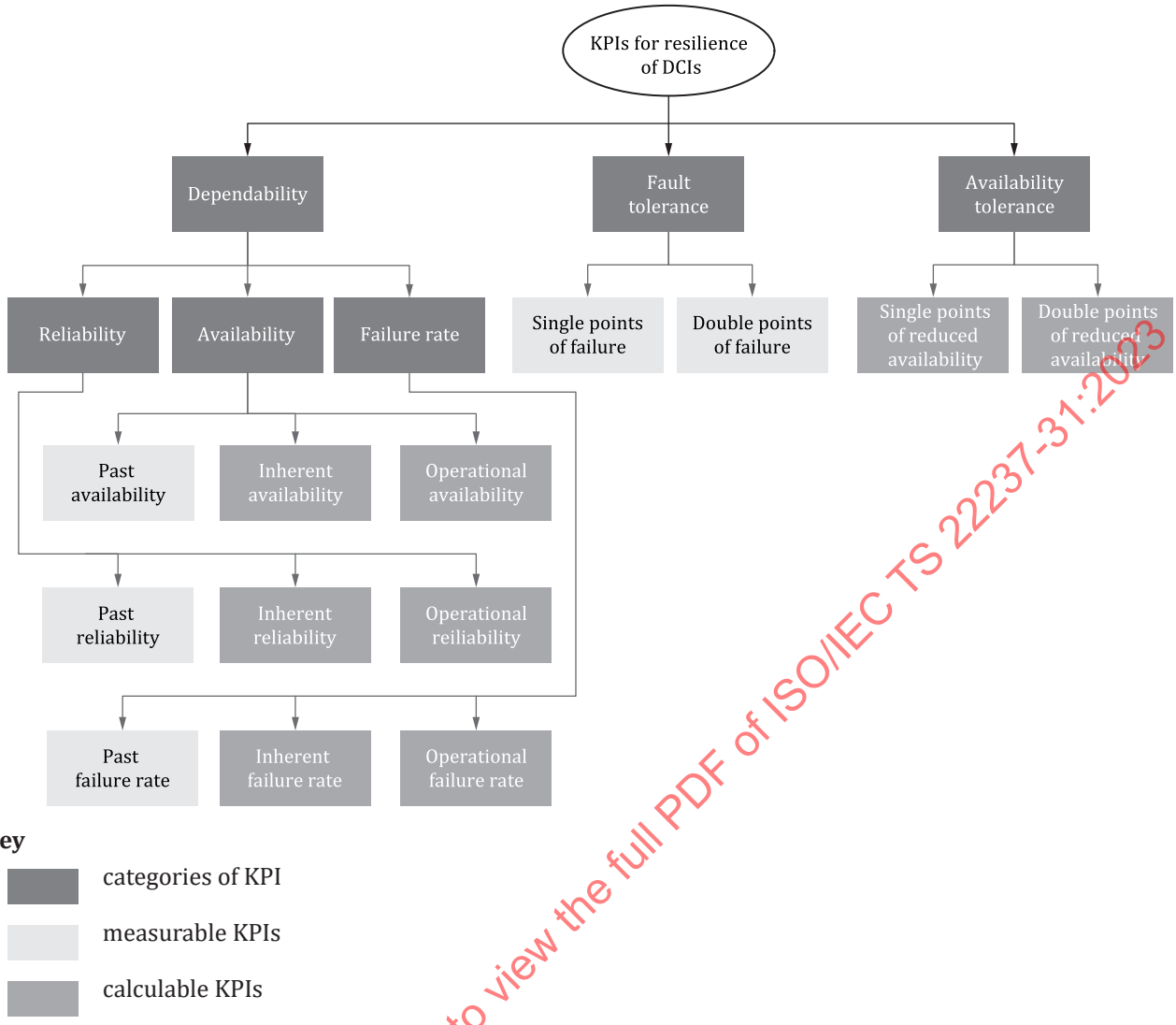

Figure 1 — KPIs for resilience of DCIs

6.2.2 KPIs

6.2.2.1 Categories

KPIs for resilience of DCIs are divided into three categories:

a) dependability,

b) fault tolerance, and

c) availability tolerance.

The category of dependability is defined by the characteristics of the functional elements of the DCI. For this purpose, dependability is subdivided into reliability, availability and failure rate.

6.2.2.2 Reliability

The category of reliability includes the following KPIs:

1) past reliability, R_p, which can be measured and calculated by using historical data [see Formula (5)];

2) inherent reliability, R_i, which can be calculated by using the metric failure rate λ_i [see Formula (6)];

3) operational reliability, R_o, which can be calculated by using the metric failure rate λ_o [see Formula (7)].

6.2.2.3 Availability

The category of availability includes the following KPIs:

1) past availability, A_p, which can be measured and calculated by using historical data [see Formulae (8)];

2) inherent availability, A_i, which can be calculated by using MTBF and MTTR of the associated functional elements of the DCI [see Formula (9)];

3) operational availability, A_o, which can be calculated by using MTBM and MDT of the associated functional elements of the DCI [see Formula (10)].

6.2.3 Failure rate

The category of failure rate includes the following KPIs:

1) past failure rate, λ_p, which can be measured and calculated by historical data [see Formula (11)];

2) inherent failure rate, λ_i, which can be calculated by using the metric MTBF [see Formula (12)].

3) operational failure rate, λ_o, which can be calculated by using the metric MTBM [see Formula (13)].

6.2.3.1 Fault tolerance

The category of fault tolerance includes the following KPIs:

1) single points of failure (SPoF), which can be determined by analysing the DCI. For the mathematical definition of SPoF, see Formula (14);

2) double points of failure (DPoF), which can also be determined by analysing the DCI. For the mathematical definition of DPoF, see Formula (15).

6.2.3.2 Availability tolerance

The category of availability tolerance includes the following KPIs:

1) single points of reduced availability (SPoRA), which can be calculated by using A_o and SPoF. For the mathematical definition of SPoRA, see Formula (16);

2) double points of reduced availability (DPoRA), which can be calculated by using A_o and DPoF. For the mathematical definition of DPoRA, see Formula (17).

Application of the proposed KPIs is possible in every phase of the design and/or operation of a data centre. For effectiveness, the integration into the process phases of ISO/IEC 22237-1 is recommended.

The application of KPIs for resilience of DCIs is in reference to the OP specified. Thus, the specified OP and the load assumption at the DCI shall always be provided when reporting KPIs.

6.2.4 Metrics

Metrics serve as the quantitative indicator data for the calculation of particular KPIs. The metrics shown in Figure 1 are explained in the following list. The explanations refer to the descriptions provided in of IEEE 493-2007:[4]

1) MTBF The mean operating time between consecutive failures of a component.

2) MTTR The mean time to replace or repair a failed component. Logistics time associated with the repair, such as parts acquisitions, crew mobilization, are not included. The metric can be estimated by dividing the summation of repair times by the number of repairs

3) MTBM The average time between all maintenance events, scheduled and unscheduled, and also including any associated logistics time.

4) MDT The average down time caused by scheduled and unscheduled maintenance, including any logistics time.

In order to establish a comparability of calculation results, it is recommended to use a standardized metric database, for example, IEEE 493-2007, Annex Q.[4]

Vendor-specific metrics can be used to evaluate different functional elements and/or components for the purpose of decision making.

For optimization purposes, especially in the phase of data centre operation, it is recommended to compare the standardized data (or manufacturer data) with data from self-collected statistics.

6.3 Dependability

6.3.1 Provided KPIs

Dependability provides metrics which are essential in the design, operation, and optimization of data centres. The following probability metrics are covered by this document as KPIs:

a) past reliability, R_p;

b) operational reliability, R_o;

c) inherent reliability, R_i;

d) past availability, A_p;

e) operational availability, A_o;

f) inherent availability, A_i.

Reliability and availability are probability metrics measured with the range $0 < x < 1$, where a higher value indicates a better performance.

In general, availability depends on the time. The KPIs A_p, A_o, and A_o are asymptotic values, and sufficient for practical application. An example of calculating the instantaneous availability using the Markov technique as another method is shown in IEC 61078.

The failure rate, λ, measures the frequency at which an item fails. It is expressed in failures per item of time. The following failure rates are covered by this document:

g) past failure rate, λ_p;

h) inherent failure rate, λ_i;

i) operational failure rate, λ_o.

A failure rate of $\lambda = 0$ expresses that there is no failure in the given time interval.

6.3.2 Reliability

6.3.2.1 General

Reliability is a probability value defined as the ability to perform as required, without failure, for the given time interval t, considering the failure rate. For the comparison of reliability considerations, periods of multiples of 8 760 h (1 a) shall be used.

Reliability can be calculated for devices, functional elements and supply paths, as well as for the system success function $S(\boldsymbol{x}_{\mathrm{OP}})$. If the underlying probability distribution of failures is known, then the system reliability in a time interval $[0;T]$ can be calculated according to Formula (3):[4]

$$R(t)=\int_0^T f(t)dt \tag{3}$$

where

$R(t)$ is the reliability of a system in time interval $[0;T]$;

$f(t)$ is the probability density function (PDF).

Assuming an exponential PDF and a constant failure rate, the reliability calculates according to Formula (4):

$$R(t)=e^{-t\lambda} \tag{4}$$

where

t time interval $[0;T]$;

λ failure rate.

If a PDF is known which better meets the characteristics of a particular target, this function may be used.

6.3.2.2 Past reliability

Past reliability, R_{p}, is defined as the ability to perform as required, without failure, for the given time interval, t, considering the past failure rate, λ_{p}, as shown in Formula (5):

$$R_{\mathrm{p}}=e^{-t\lambda_{\mathrm{p}}} \tag{5}$$

where

t time interval $[0;T]$;

λ_{p} past failure rate.

6.3.2.3 Inherent reliability

Inherent reliability, R_{i}, is defined as the ability to perform as required, without failure, for the given time interval, t, considering the inherent failure rate, λ_{i}, as shown in Formula (6):

$$R_{\mathrm{i}}=e^{-t\lambda_{\mathrm{i}}} \tag{6}$$

where

t time interval $[0;T]$;

$\lambda_i = 1/t_{MTBF}$

6.3.2.4 Operational reliability

Operational reliability, R_o, is defined as the ability to perform as required, without failure, for the given time interval t considering the operational failure rate, λ_o, as shown in Formula (7):

$$R_o = e^{-t\,\lambda_o} \tag{7}$$

where

t time interval $[0;T]$;

$\lambda_o = 1/t_{MTBM}$

6.3.3 Availability

6.3.3.1 Past availability

The past availability, A_p, can be calculated for past time intervals of data centre operation in which the time interval, t, of the service success function $S(\boldsymbol{x}_{OP})$ was measured, as shown in as shown in Formula (8). For the comparison of past availability values, an interval of 8 760 h (1 a) shall be documented.

$$A_p = \frac{t_{S(x(OP))=1}}{t_{S(x(OP))=1} + t_{S(x(OP))=0}} \tag{8}$$

where

$t_{S(x(OP))=1}$ is the period of successful operation (the service at the OP is up);

$t_{S(x(OP))=0}$ is the period of non-successful operation (fault, the service at the OP is down).

By multiplying by 100 %, a percentage notation is obtained.

6.3.3.2 Inherent availability

The inherent availability, A_i, is a probability value defined as availability provided by the design under ideal conditions for operation and maintenance, as shown in Formula (9):

$$A_i = \frac{t_{MTBF}}{t_{MTBF} + t_{MTTR}} \tag{9}$$

where

t_{MTBF} is the mean time between failures;

t_{MTTR} is the mean time to restoration.

As MTBF and MTTR are defined as constant values, the resulting A_i is also not a function of time. The inherent availability can be calculated for devices, functional elements and supply paths as well as for the system success function $S(\boldsymbol{x}_{OP})$.

6.3.3.3 Operational availability

The operational availability, A_o, is a probability value, defined as availability experienced under actual conditions of operation and maintenance, as shown in Formula (10):

$$A_o = \frac{t_{MTBM}}{t_{MTBM} + t_{MDT}} \tag{10}$$

where

t_{MTBM} is the mean time between maintenance;

t_{MDT} Is the mean down time.

As MTBM and MDT are defined as constant values, the resulting A_o is also not a function of time. The operational availability can be calculated for devices, functional elements and supply paths as well as for the system success function $S(\boldsymbol{x}_{OP})$.

6.3.4 Failure rate

6.3.4.1 General

The failure rate expresses the limit of the ratio of the conditional probability that the instant of time, T, of a failure of a product falls within a given time interval $(t, t+\Delta t)$ and the duration of this interval, Δt, when Δt tends towards zero, given that the item is in an up state at the start of the time interval.

6.3.4.2 Past failure rate

The past failure rate, λ_p, can be measured by counting the number of failures per time interval as shown in Formula (11):

$$\lambda_p = N_f / t \tag{11}$$

where

N_f is the number of failures during time interval t;

t is the time interval $[0;T]$.

For comparability, multiples of a year's (8 760 h) time span should be used.

6.3.4.3 Inherent failure rate

The inherent failure rate, λ_i, is the reciprocal of the MTBF, as shown in Formula (12):

$$\lambda_i = 1 / t_{MTBF} \tag{12}$$

6.3.4.4 Operational failure rate

The operational failure rate, λ_o, is the reciprocal of the MTBM, as shown in Formula (13):

$$\lambda_o = 1 / t_{MTBM} \tag{13}$$

6.3.4.5 Confidence interval of failure rate

Methods for determining the confidence interval of the failure rate within the considered time interval can be distinguished in:

a) estimations with failures;

b) estimations without failures.

Depending on the data situation, statistical methods are applicable for the determination. Examples are given in Annex E. Reference is made to further literature such as IEC 60300 and IEC 60605-4.

6.4 Fault tolerance

6.4.1 General

Fault tolerance is introduced to specify how the DCI reacts in the event of failures. A failure in this context can be an unplanned service violation or a planned maintenance event. The following KPIs are covered by this document, according to the mathematical definitions in Reference [1]:

a) number of single points of failure (SPoF);

b) number of double points of failure (DPoF).

A lower value indicates a better fault tolerance.

Examples for calculating the KPIs for SPof and DPoF are given in Annex A, by using the method of RBD in accordance with IEC 61078.

6.4.2 Single point of failure (SPoF)

The functional element $x_{m(i)}$ marks an SPoF of the mth DCI if its failure leads to overall infrastructure service failure. Thus, $N_{\mathrm{SPoF}(m)}$ encompasses all those elements $x_{m(i)}$ whose single failure, $x_{m(i)}=0$, results in $S_m(\boldsymbol{x}_m)=0$, as shown in Formula (14):

$$N_{\mathrm{SPoF}(m)}=\left|\left\{x_{m(i)}\in X_m\left|\begin{array}{c}(S_m(\boldsymbol{x}_m)=0)\cap\\ \left(\bar{x}_{m(i)}\prod_{l=1,\,l\neq i}^{N}x_{m(l)}=1\right)\end{array}\right.\right\}\right| \tag{14}$$

The number $N_{\mathrm{SPoF}(m)}$ indicates the number of SPoFs within DCIs determined by the vector $\boldsymbol{x}$.

6.4.3 Double point of failure (DPoF)

Two functional elements $\{x_{m(i)},x_{m(j)}\}$ mark a DPoF of the mth DCI if its simultaneous failure leads to overall infrastructure service failure. Thus, $N_{\mathrm{DPoF}(m)}$ encompasses all those element sets $\{x_{m(i)},x_{m(j)}\}$ whose double failure $x_{m(i)}=0$ and $x_{m(j)}=0$ results in $S_m(\boldsymbol{x}_m)=0$, as shown in Formula (15):

$$N_{\mathrm{DPoF}(m)}=\left|\left\{\{x_{m(i)},x_{m(j)}\}\subset X_m\left|\begin{array}{c}(S_m(\boldsymbol{x}_m)=0)\cap\\ \left(\bar{x}_{m(i)}\bar{x}_{m(j)}\prod_{l=1,\,l\neq i,j}^{N}x_{m(l)}=1\right)\end{array}\right.\right\}\right| \tag{15}$$

The number $N_{\mathrm{DPoF}(m)}$ indicates the number of DPoFs within DCIs determined by the vector $\boldsymbol{x}$.

6.5 Availability tolerance

6.5.1 General

Availability tolerance is introduced to specify how the DCI reacts in case of failures. A failure in this context can be an unplanned service violation or a planned maintenance event. The following KPIs are covered by this document, according to the mathematical definitions in Reference [1]:

a) number of single points of reduced availability (SPoRA);

b) number of double points of reduced availability (DPoRA).

A lower value indicates a better availability tolerance.

Examples for calculating the KPIs for SPoRA and DPoRA are given in Annex A, by using the method of RBD in accordance with IEC 61078.

6.5.2 Single point of reduced availability (SPoRA)

The functional element $x_{m(i)}$ marks an SPoRA of the mth DCI if its failure leads to a violation of the required operational availability, $A_{\mathrm{o,req}}$. Thus, $N_{\mathrm{SPoRA}(m)}$ encompasses all those elements $x_{m(i)}$ whose single failure, $x_{m(i)}=0$, violates the required operational availability $A_{\mathrm{o}}(D_m(\boldsymbol{x}_m))<A_{\mathrm{o,req}}$ including the elements where $A_{\mathrm{o}}(D_m(\boldsymbol{x}_m))=0$, as shown in Formula (16):

$$N_{\mathrm{SPoRA}(m)}=\left|\left\{x_{m(i)}\in X_m \;\middle|\; \begin{pmatrix} A_{\mathrm{o}}(D_m(\boldsymbol{x}_m))<A_{\mathrm{o,req}} \end{pmatrix}\cap \left(\bar{x}_{m(i)}\prod_{l=1,\,l\neq i}^{N} x_{m(l)}=1\right)\right\}\right| \tag{16}$$

With the number of SPoRA, the operational availability and single fault tolerance of a DCI can be expressed in one single KPI. A lower number of SPoRA expresses a more resilient DCI from the perspective of single faults. By comparing the number of SPoRA, the resilience of different designs can be evaluated and used for optimization.

6.5.3 Double point of reduced availability (DPoRA)

Two functional elements $\{x_{m(i)},x_{m(j)}\}$ mark a DPoRA of the mth DCI if its simultaneous failure leads to a violation of the required operational availability. Thus, $N_{\mathrm{DPoRA}(m)}$ encompasses those element sets $\{x_{m(i)},x_{m(j)}\}$ whose double failure $x_{m(i)}=0$ and $x_{m(j)}=0$ results in reduced availability, $A_{\mathrm{o}}(D_m(\boldsymbol{x}_m))<A_{\mathrm{o,req}}$, including the element sets where $A_{\mathrm{o}}(D_m(\boldsymbol{x}_m))=0$, as shown in Formula (17):

$$N_{\mathrm{DPoRA}(m)}=\left|\left\{\{x_{m(i)},x_{m(j)}\}\subset X_m \;\middle|\; \begin{pmatrix} A_{\mathrm{o}}(D_m(\boldsymbol{x}_m))<A_{\mathrm{o,req}} \end{pmatrix}\cap \left(\bar{x}_{m(i)}\bar{x}_{m(j)}\prod_{l=1,\,l\neq i,j}^{N} x_{m(l)}=1\right)\right\}\right| \tag{17}$$

With the number of DPoRA, the operational availability and double fault tolerance of a DCI can be expressed in one single KPI. A lower number of DPoRA expresses a more resilient DCI from the perspective of double failures.

By comparing the number of DPoRA, the resilience can be evaluated and used for optimization. DPoRA is meaningful for more complex designs with higher requirements, such as those of the availability classes 3 and 4.

6.6 Resilience level (RL)

6.6.1 General

To specify the objectives of DCIs, it can be helpful to use a standardized definition scheme. For that reason, the resilience level (RL) supports enumeration of the attributes of a defined service. To specify the RL of DCIs, the following characteristics shall be defined.

a) The reporting time interval in years.

b) The maximum of accepted events of service violation per reporting time interval.

c) The maximum of accepted down time per reporting time interval.

If an SLA for design and/or operation of the DCI is given, relevant details shall be taken into account in the RL definition.

It is recommended to specify different RLs for different operational conditions of the DCI. Subclause 6.6.2 shows examples for RLs during operation at NRL, and 6.6.3 adds examples during operation at RRL.

RL considerations can be required at different OPs of the DCI. Different OPs can have different service requirements for different infrastructures (see 5.1.3). The requirements for the service quality of an OP to different infrastructures shall be taken into account.

6.6.2 Operation at normal resilience level

Operation at normal resilience level, when all functional elements are in the up state, is referred to as NRL. NRL specifies the minimum operational availability that can be expected in accordance with the operational design parameters of the DCI.

Examples of NRL definitions of different availability classes are shown in Table 1. Including the number of SPoF and availability, Table 1 combines different aspects of resilience, such as fault tolerance and availability considerations.

The 1st column of Table 1 shows a recommendation on which availability class could be able to fulfil the particular NRL at a specific OP. Capital letters have been used to clarify which infrastructures the definition applies to. The letter "P" stands for "Power" and the letter "E" stands for "Environmental Control". The 2nd column shows the maximum number of SPoF allowed in the DCI design for the specified infrastructures. Both columns represent aspects of the DCI design.

Starting with the 3rd column, availability aspects are targeted. The 3rd column represents the reporting time interval in years. The 4th column represents the maximum accepted number of faults per reporting interval. The 5th column represents the maximum accepted downtime per service violation.

The NRL itself is defined by the four numbers of columns 2 to 5, separated by semicolons — see the 6th column of Table 1 for reference. The last column shows the resulting NRL operational availability value, $A_{o,NRL}$, which has been calculated using the columns 3 to 5.

Table 1 — Examples of definitions of operation at normal resilience level

Availability class	Maximum number of single points of failure (SPoF)	Reporting time interval (years)	Maximum accepted number of faults per reporting interval	Maximum accepted down time per service violation (h)	Operation at normal resilience level (NRL)	Calculated operational availability, $A_{\text{o NRL}}$
1	2	3	4	5	6	7
AC1(P,E)	15	5	20	36	15; [5; 20; 36]	0,983 8
	20	10	40	36	20; [10; 40; 36]	0,983 8
	20	10	60	24	20; [10; 60; 24]	0,983 8
AC2(P,E)	10	5	10	36	10; [5; 10; 36]	0,991 8
	5	10	20	36	5; [10; 20; 36]	0,991 8
	10	10	30	24	10; [10; 30; 24]	0,991 8
AC3(P,E)	2	5	1	12	2; [5; 1; 12]	0,999 7
	2	10	2	12	2; [10; 2; 12]	0,999 7
	1	10	2	12	1; [10; 2; 12]	0,999 7
	0	15	4	10	0; [15; 4; 10]	0,999 7
AC4(P,E)	0	10	1	12	0; [10; 1; 12]	0,999 9
	0	10	2	6	0; [10; 2; 6]	0,999 9
	0	15	1	18	0; [15; 1; 18]	0,999 9
	0	15	2	9	0; [15; 2; 9]	0,999 9
	0	20	1	24	0; [20; 1; 24]	0,999 9

To give an example using the data from Table 1 (see 8th row), an NRL of $(2;[10,2,12])$ expresses the following:

— The first digit, "2", indicates that this AC3 design is not free of SPoFs in accordance with ISO/IEC 22237-1:2021, Table B.1.

— The numbers in square brackets indicate that over a reporting period of 10 years, only 2 fault events would be allowed, with a maximum accepted duration of service violation of 12 hours per event.

The resulting operational availability is shown in the 6th column of Table 1. In this example, the calculation of $A_{\text{o,NRL}}$ is as shown in Formula (18):

$$A_{\text{o,NRL}}(2;[10;2;12]) = \frac{10\times 8760}{10\times 8760 + 2\times 12} = 0,999\,7 \tag{18}$$

The availability class as well as the number of SPoF are design characteristic of the DCI. For this reason, they are not part of the calculation of the $A_{\text{o,NRL}}$. In cases of design validation and/or comparison, it can also be useful to specify the NRL inherent availability, $A_{\text{i,NRL}}$, in addition to or instead of $A_{\text{o,NRL}}$.

For holistic resilience evaluation and/or optimization, the calculations of the KPIs N_{DPoF}, N_{SPoRA}, and N_{DPoRA} are recommended.

The event of service success refers to the OP specified. Thus, the specified $S(\boldsymbol{x}_{\text{OP}})$ and the load assumption at the DCI shall be provided when reporting NRL.

6.6.3 Operation at reduced resilience level

Due to the long lifetime of data centres, maintenance (including failure and recovery to nominal operation) can be required on several occasions. Planned maintenance events allow adequate preparations. However, functional contingencies are often unavoidable, with the result that the

expected availability cannot be guaranteed. Especially for data centres of availability class 3 and 4, the particular $A_{o,RRL}$ definitions become important.

Therefore, it is recommended to determine a DCI operation of RRL during a limited period of planned maintenance. Examples of RRL are shown in Table 2. The requirements for RRL can be lower than those for NRL. This can result in a lower operational availability, $A_{o,RRL}$, during such limited periods of time.

Table 2 — Examples of definitions of operation at reduced resilience level

Availa-bilty class (AC)	Maximum number of single points of failure (SPoF)	Reporting time interval (years)	Maximum accepted number of faults per reporting interval	Maximum accepted down time per service violation (h)	Operation at Reduced Resilience Level (RRL)	Calculated Operational Availability $A_{o,RRL}$
1	2	3	4	5	6	7
AC3(P,E)	5	5	5	4	5; [5; 4; 5]	0,999 5
	6	10	20	2	10; [20; 2; 6]	0,999 5
	5	15	15	4	15; [15; 4; 5]	0,999 5
AC4(P,E)	3	10	10	3	10; [10; 3; 3]	0,999 7
	5	15	30	2	15; [30; 2; 5]	0,999 5
	4	20	20	3	20; [20; 3; 4]	0,999 7

The event of service violation is in reference to the OP chosen. Thus, specified $S(\boldsymbol{x}_{OP})$ and the load assumption at the DCI shall be provided when reporting RRL.

The number of SPoF is a design characteristic of the DCI. For this reason, it is not a factor in the calculation for the operational availability value $A_{o,RRL}$. The resulting operational availability is shown in the 6th column of Table 2. For the example in the 2nd row of Table 2, $A_{o,RRL}$ calculates as shown in Formula (19):

$$A_{o,RRL}(6;[10;20;2]) = \frac{10\times 8760}{10\times 8760 + 20\times 2} = 0,999\,5 \tag{19}$$

In preparation for a period of reduced operation, the calculations for the KPIs N_{DPoF}, N_{SPoRA} and N_{DPoRA} are recommended.

6.7 Application to data centre infrastructures

6.7.1 Methodology and analysis considerations

6.7.1.1 General

Depending on the scope of a resilience analysis, the availability and reliability calculation considering failure sequences of single events and multiple events and more can be covered. For this purpose, various statistical methods are applicable, such as:

a) IEC 60812, Failure modes and effects analysis (FMEA and FMECA);

b) IEC 61025, Fault tree analysis (FTA);

c) IEC 61078, Reliability block diagrams (RBD);

d) IEC 61165, Application of Markov techniques;

e) IEC 62551, Petri net techniques.

The use of these methods requires experience in their application, as well as sufficient technical understanding of the particular DCI. This encompasses the determination of the OP, the adequate resilience modelling, the selection of the applicable KPIs in relation to the required RL and/or SLAs, and the resilience data of the functional elements. Specialized software tools can be helpful to support the application.

6.7.1.2 Resilience data

Depending on the objective of the analysis and the applicable resilience data, the following aspects should be taken into account.

a) The required functional elements depending on the OP definition (power system, environmental, auxiliary supply, monitoring and control systems, fire detection and extinction systems, etc.).

b) The functional elements failure modes.

c) The functional elements failure rates.

d) Planned maintenance events (with and without power down of devices).

e) Unplanned maintenance events (detection time, reconfiguration time, lock out time, diagnostic time, logistics time, repair time).

f) Common cause failure modes:

   1) architecture of the system (common auxiliary systems, no compartmentalization);

   2) environment (fire, flood, lightning impact, extreme outside temperature, extreme adverse weather, etc.);

   3) human errors (equipment or system design errors, PLC or protection relay configuration errors, installation errors or maintenance errors).

g) Time to restoration on various aspects:

   1) skills of on-site operators;

   2) emergency procedures;

   3) manufacturer maintenance contracts;

   4) spare parts management, agreed delivery times, time for logistics.

For the purpose of numerical resilience analysis, component databases such as IEEE 493-2007, Annex Q[4] are available. This component database includes a set of items and dependability data for application to resilience models.

6.7.2 Analysis process

A typical process for performing resilience analysis of DCIs is described by the phase diagram of Figure 2.

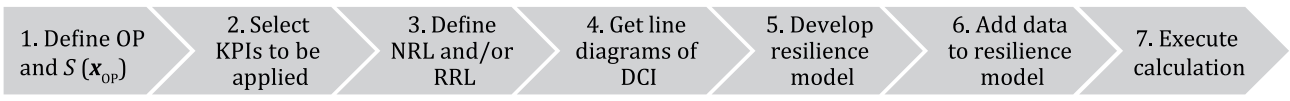

Figure 2 — Phase diagram of resilience analysis

Explanation of the seven phases of Figure 2:

1) The infrastructure service definition, including the system success function $S(\boldsymbol{x}_{\mathrm{OP}})$, is discussed in 4.2.

2) For the selection of KPIs to be calculated, Figure 1 can be used.

3) The definition of NRL, and RRL if required, is discussed in 6.6.

4) The line diagrams of the infrastructures to guarantee the system success function $S(\boldsymbol{x}_{\mathrm{OP}})$ are generally made available with the planners and, if necessary, with the operators of the DCI.

5) Based on the line diagrams, the resilience model is developed.

6) Dependability data are to be added to every item of the resilience model. For the comparability of analysis results, standards shall be preferred as dependability data sources. Depending on the task of the analysis, other sources such as manufacturer data or user specific data could be used; see 6.7.1.2.

7) For the analysis of less complex infrastructure models, a spreadsheet tool can be used. If the interdependencies of the DCIs and/or the models to analyse are more complex, third-party tools can be incorporated.

To be able to compare the calculation results of resilience analysis for different DCIs, it is necessary for the analysis methods used, as well as the applied dependability data, to be equivalent.

6.7.3 Method of reliability block diagrams (RBD)

A method for calculating the resilience KPIs covered in this document is given by IEC 61078. This method, involving reliability block diagram (RBD) models, is applicable to DCIs because of the following capabilities.

a) With the aid of block symbols, the system success function at the OP $S(\boldsymbol{x}_{\mathrm{OP}})$ of the DCI can be modelled.

b) RBD models are helpful for displaying and analysing the dependencies between the functional elements, and different DCIs.

c) When evaluating the calculation results, the extension to higher orders of multiple failure combinations can be considered and extended to double or multiple site infrastructures if required.

d) With the help of success paths, failure sequences can be analysed.

e) When evaluating the calculation results, the extension to common cause failures can be considered.

Examples for resilience analysis by using RBD method are given in Annexes A, B, and C.

6.7.4 Method of Failure Mode Effects and Criticality Analysis

A common method in reliability management is Failure Mode Effects and Criticality Analysis (FMECA). The failure sequence modelling shall include all events from the failure occurrence till the system get back to its normal state. For this purpose, FMECA considers:

a) failure detection;

b) reaction of the protection, automation and/or control systems;

c) failure consequences;

d) failure isolation and/or reconfiguration;

e) restoration and/or repair.

An example of a FMECA analysis is given in Annex D.

Annex A
(informative)

Resilience analysis for DCIs

Annex A provides a basic example of a dependability calculation. Figure A.1 shows an example of a block diagram of a simplified DCI according to availability class 2 (AC2). If subsystems are to be formed as a reliability block diagram (RBD) of a DCI, the following should be considered:

a) compartmentalization of functional elements;

b) isolation of failures by safety and protective devices;

c) logical and systemic dependencies.

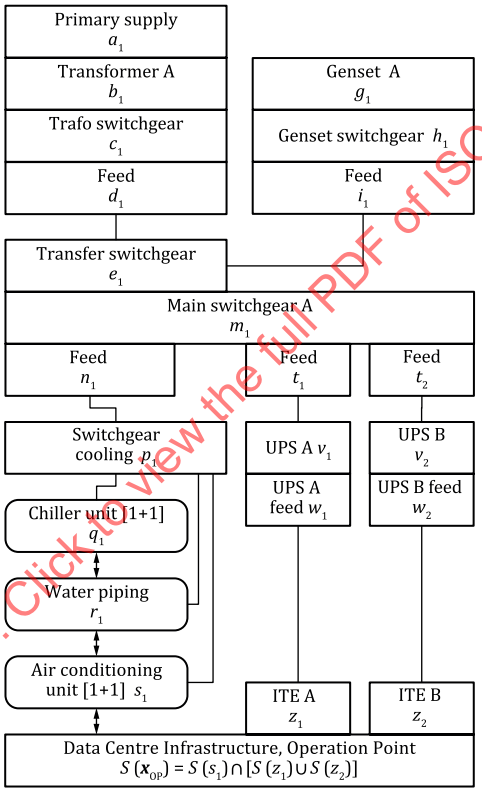

Figure A.1 — Example RBD of a simplified DCI according to AC2 (P,E)

The RBD of Figure A.1 consists of 22 subsystems, denoted by a_1 to z_2. The success of the DCI at the OP of Figure A.1 is given by the success function of Formula (A.1).

$$\begin{aligned} S(\boldsymbol{x}_{\mathrm{OP}})_{\text{Annex A, AC2(P,E)}} = {} & g_1\, h_1\, i_1\, e_1\, m_1\, t_1\, v_1\, w_1\, z_1\, n_1\, p_1\, q_1\, r_1\, s_1 \cup \\ & g_1\, h_1\, i_1\, e_1\, m_1\, t_2\, v_2\, w_2\, z_2\, n_1\, p_1\, q_1\, r_1\, s_1 \cup \\ & a_1\, b_1\, c_1\, d_1\, e_1\, m_1\, t_1\, v_1\, w_1\, z_1\, n_1\, p_1\, q_1\, r_1\, s_1 \cup \\ & a_1\, b_1\, c_1\, d_1\, e_1\, m_1\, t_2\, v_2\, w_2\, z_2\, n_1\, p_1\, q_1\, r_1\, s_1 \end{aligned} \tag{A.1}$$

Overall, four system success paths (SSPs) are required to describe the success function. Note that the order of the Boolean variables inside an SSP can be chosen arbitrarily. Likewise, the order of the SSPs

can be chosen arbitrarily. For some practical reasons, it is recommended to start with the shortest paths.

To calculate the dependability values, the terms of Formula (A.1) shall be mutually exclusive. For more information, see IEC 61078. Applying methods of multi-variable inversion (MVI) to Formula (A.1), Formula (A.2) results.

$$
\begin{aligned}
D(\boldsymbol{x}_{\mathrm{OP}})_{\text{Annex A, AC2(P,E)}} = {} & g_1\, h_1\, i_1\, e_1\, m_1\, t_1\, v_1\, w_1\, z_1\, n_1\, p_1\, q_1\, r_1\, s_1 \cup \\
& g_1\, h_1\, i_1\, e_1\, m_1\, n_1\, p_1\, q_1\, r_1\, s_1\, t_2\, v_2\, w_2\, z_2\, \overline{t_1\, v_1\, w_1\, z_1} \cup \\
& a_1\, b_1\, c_1\, d_1\, e_1\, m_1\, n_1\, p_1\, q_1\, r_1\, s_1\, t_2\, v_2\, w_2\, z_2\, \overline{g_1\, h_1\, i_1} \cup \\
& a_1\, b_1\, c_1\, d_1\, e_1\, m_1\, t_1\, v_1\, w_1\, z_1\, n_1\, p_1\, q_1\, r_1\, s_1\, \overline{g_1\, h_1\, i_1}\, \overline{t_2\, v_2\, w_2\, z_2}
\end{aligned}
\tag{A.2}
$$

With the premise of systemic independence, the Boolean variables of Formula (A.2) can be replaced by dependability data. For this purpose, the dependability data for the components of Table A.1 are used.

A valuable source for the dependability data of components is IEEE Std. 493.[4] Note that functional elements usually consist of multiple items of IEEE Std. 493-2007, Annex Q. In that case, components can be grouped to subsystems. Where additional attributes exist, such as dimensions or redundancies, they must be taken into account. For the calculation of $R(t)$ Formula (4) is used.

Table A.1 — Dependability for the functional elements of the example AC2

Boolean variable	Description	Redundancy	$R(t)$ $t = 8\,760$ h	A_i	A_o
a_i	Supply MV	—	0,712 898 90	0,999 972 89	0,999 680 37
b_i	Transformer	—	0,991 153 00	0,999 997 16	0,999 879 92
c_i	Transformer switchgear	—	0,990 554 80	0,999 992 10	0,999 455 60
d_i	Feed	—	0,997 390 09	0,999 999 79	0,999 954 20
e_i	Transfer switchgear	—	0,966 513 34	0,999 993 94	0,999 764 26
g_i	Genset LV	—	0,882 614 90	0,999 742 25	0,997 355 30
h_i	Genset switchgear	—	0,990 554 80	0,999 992 10	0,999 455 60
i_i	Feed	—	0,997 390 09	0,999 999 79	0,999 954 20
m_i	Main switchgear	—	0,990 554 80	0,999 992 10	0,999 455 60
n_i	Feed	—	0,997 402 67	0,999 999 83	0,999 954 24
p_i	Switchgear cooling	—	0,990 554 80	0,999 992 10	0,999 455 60
q_i	Chiller	1+1	0,971 846 33	0,999 999 94	0,999 988 99
r_i	Water piping	—	0,990 233 81	0,999 998 04	0,994 760 28
s_i	Air conditioning	1+1	0,995 144 86	0,999 999 99	0,999 999 53
t_i	Feed	—	0,997 402 67	0,999 999 83	0,999 954 24
v_i	UPS	—	0,924 677 54	0,999 662 67	0,998 081 20
w_i	UPS feed	—	0,987 982 01	0,999 991 93	0,999 409 87
z_i	ITE switchgear	—	0,989 606 86	0,999 991 90	0,999 253 74

For comparison reasons, Figure A.2 shows a more complex block diagram as an example of a DCI of availability class 4 (AC4).

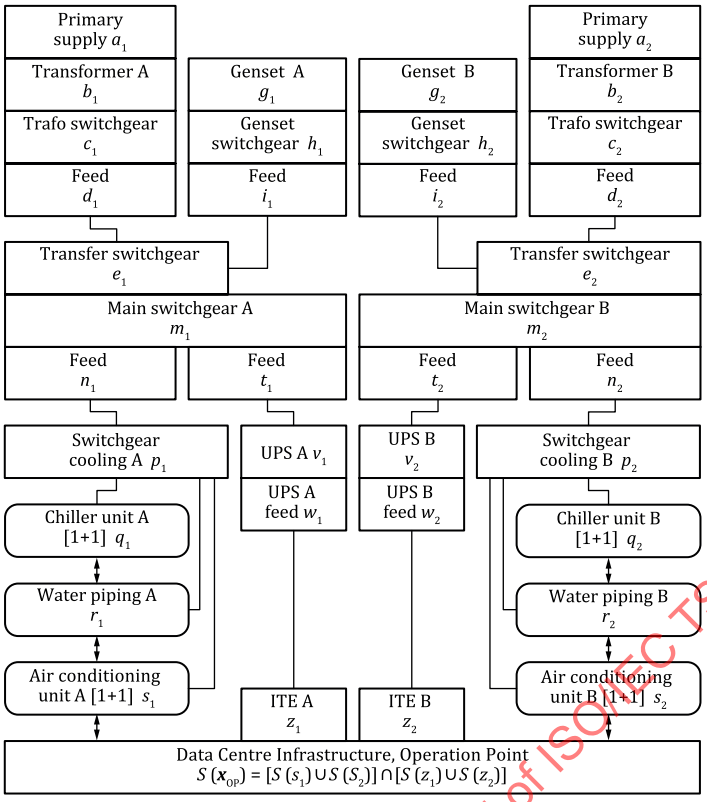

Figure A.2 — Example RBD of a simplified DCI according to AC4 (P,E)

The RBD of Figure A.2 consists of 36 subsystems, denoted by a_1 to z_2. The success of the DCI at the OP of Figure A.2 is given by the success function of Formula (A.3).

$$
\begin{aligned}
S(\boldsymbol{x}_{\mathrm{OP}})_{\text{Annex A, AC4(P,E)}} = {} & g_1\, h_1\, i_1\, e_1\, m_1\, t_1\, v_1\, w_1\, z_1\, n_1\, p_1\, q_1\, r_1\, s_1 \cup \\
& g_2\, h_2\, i_2\, e_2\, m_2\, t_2\, v_2\, w_2\, z_2\, n_2\, p_2\, q_2\, r_2\, s_2 \cup \\
& a_1\, b_1\, c_1\, d_1\, e_1\, m_1\, t_1\, v_1\, w_1\, z_1\, n_1\, p_1\, q_1\, r_1\, s_1 \cup \\
& a_2\, b_2\, c_2\, d_2\, e_2\, m_2\, t_2\, v_2\, w_2\, z_2\, n_2\, p_2\, q_2\, r_2\, s_2 \cup \\
& g_1\, h_1\, i_1\, e_1\, m_1\, t_1\, v_1\, w_1\, z_1\, g_2\, h_2\, i_2\, e_2\, m_2\, n_2\, p_2\, q_2\, r_2\, s_2 \cup \\
& g_2\, h_2\, i_2\, e_2\, m_2\, t_2\, v_2\, w_2\, z_2\, g_1\, h_1\, i_1\, e_1\, m_1\, n_1\, p_1\, q_1\, r_1\, s_1 \cup \\
& g_2\, h_2\, i_2\, e_2\, m_2\, t_2\, v_2\, w_2\, z_2\, a_1\, b_1\, c_1\, d_1\, e_1\, m_1\, n_1\, p_1\, q_1\, r_1\, s_1 \cup \\
& g_1\, h_1\, i_1\, e_1\, m_1\, t_1\, v_1\, w_1\, z_1\, a_2\, b_2\, c_2\, d_2\, e_2\, m_2\, n_2\, p_2\, q_2\, r_2\, s_2 \cup \\
& a_2\, b_2\, c_2\, d_2\, e_2\, m_2\, t_2\, v_2\, w_2\, z_2\, g_1\, h_1\, i_1\, e_1\, m_1\, n_1\, p_1\, q_1\, r_1\, s_1 \cup \\
& a_1\, b_1\, c_1\, d_1\, e_1\, m_1\, t_1\, v_1\, w_1\, z_1\, g_2\, h_2\, i_2\, e_2\, m_2\, n_2\, p_2\, q_2\, r_2\, s_2 \cup \\
& a_2\, b_2\, c_2\, d_2\, e_2\, m_2\, t_2\, v_2\, w_2\, z_2\, a_1\, b_1\, c_1\, d_1\, e_1\, m_1\, n_1\, p_1\, q_1\, r_1\, s_1 \cup \\
& a_1\, b_1\, c_1\, d_1\, e_1\, m_1\, t_1\, v_1\, w_1\, z_1\, a_2\, b_2\, c_2\, d_2\, e_2\, m_2\, n_2\, p_2\, q_2\, r_2\, s_2
\end{aligned}
\tag{A.3}
$$

Overall, 12 SSPs are required to describe the success function. To compute the disjoint sum $D(\boldsymbol{x}_{\mathrm{OP}})_{\text{Annex A, AC4(P,E)}}$ from Formula (A.3), a third-party tool was used.

Considering the entire DCI, Table A.2 corresponds to NRL. Using the same methodology and applying the dependability data of Table A.1 to the disjoint success functions $D(\boldsymbol{x}_{\mathrm{OP}})_{\text{Annex A, AC2(P,E)}}$ and $D(\boldsymbol{x}_{\mathrm{OP}})_{\text{Annex A, AC4(P,E)}}$, the resilience analysis for the RBDs of Figures A.1 and A.2 gives the results listed in Table A.2.

Table A.2 — Resilience calculation results of simplified DCI examples

DCI example Annex A	Level of resilience	Number of functional elements	Number of SSPs	$R(t)$ $t = 8\,760$ h	A_i	A_o	Number of SPoF	Number of DPoF
AC2 (P,E)	NRL	22	4	0,862 433	0,999 976	0,993 372	5	125
AC4 (P,E)	NRL	36	12	0,961 531	0,999 999	0,999 940	0	57

The following Table A.3 shows the counted DPoFs of example AC2 (P,E).

Table A.3 — DPoF Resilience calculation results of simplified DCI examples

No.	DPoF	No.	DPoF	No.	DPoF	No.	DPoF	No.	DPoF
1	$[g_1, m_1]$	26	$[i_1, a_1]$	51	$[m_1, z_2]$	76	$[v_1, r_1]$	101	$[p_1, b_1]$
2	$[g_1, a_1]$	27	$[i_1, m_1]$	52	$[m_1, v_1]$	77	$[w_1, z_2]$	102	$[p_1, z_1]$
3	$[g_1, r_1]$	28	$[e_1, v_1]$	53	$[m_1, d_1]$	78	$[w_1, w_2]$	103	$[p_1, z_2]$
4	$[g_1, n_1]$	29	$[e_1, z_2]$	54	$[m_1, c_1]$	79	$[w_1, t_2]$	104	$[p_1, v_2]$
5	$[g_1, e_1]$	30	$[e_1, d_1]$	55	$[m_1, p_1]$	80	$[w_1, p_1]$	105	$[p_1, a_1]$
6	$[g_1, p_1]$	31	$[e_1, b_1]$	56	$[m_1, w_1]$	81	$[w_1, n_1]$	106	$[p_1, c_1]$
7	$[g_1, d_1]$	32	$[e_1, c_1]$	57	$[m_1, a_1]$	82	$[w_1, r_1]$	107	$[p_1, p_1]$
8	$[g_1, c_1]$	33	$[e_1, v_2]$	58	$[m_1, r_1]$	83	$[w_1, v_2]$	108	$[p_1, s_1]$
9	$[g_1, b_1]$	34	$[e_1, r_1]$	59	$[m_1, w_2]$	84	$[n_1, z_1]$	109	$[r_1, w_2]$
10	$[h_1, n_1]$	35	$[e_1, t_2]$	60	$[m_1, b_1]$	85	$[n_1, c_1]$	110	$[r_1, z_1]$
11	$[h_1, p_1]$	36	$[e_1, p_2]$	61	$[m_1, q_1]$	86	$[n_1, z_2]$	111	$[r_1, v_2]$
12	$[h_1, m_1]$	37	$[e_1, w_2]$	62	$[m_1, s_1]$	87	$[n_1, b_1]$	112	$[r_1, b_1]$
13	$[h_1, d_1]$	38	$[e_1, a_1]$	63	$[t_1, t_2]$	88	$[n_1, a_1]$	113	$[r_1, z_2]$
14	$[h_1, b_1]$	39	$[e_1, t_1]$	64	$[t_1, n_2]$	89	$[n_1, t_2]$	114	$[r_1, d_1]$
15	$[h_1, r_1]$	40	$[e_1, n_1]$	65	$[t_1, w_2]$	90	$[n_1, r_1]$	115	$[r_1, t_2]$
16	$[h_1, e_1]$	41	$[e_1, z_1]$	66	$[t_1, v_2]$	91	$[n_1, p_1]$	116	$[r_1, c_1]$
17	$[h_1, a_1]$	42	$[e_1, m_1]$	67	$[t_1, p_1]$	92	$[n_1, v_2]$	117	$[r_1, a_1]$
18	$[h_1, c_1]$	43	$[e_1, w_1]$	68	$[t_1, z_2]$	93	$[n_1, w_2]$	118	$[r_1, q_1]$
19	$[i_1, n_1]$	44	$[e_1, q_1]$	69	$[t_1, r_1]$	94	$[n_1, d_1]$	119	$[r_1, s_1]$
20	$[i_1, r_1]$	45	$[e_1, s_1]$	70	$[v_1, z_1]$	95	$[n_1, q_1]$	120	$[z_1, v_2]$
21	$[i_1, p_1]$	46	$[m_1, z_1]$	71	$[v_1, w_2]$	96	$[n_1, s_1]$	121	$[z_1, w_2]$
22	$[i_1, c_1]$	47	$[m_1, v_2]$	72	$[v_1, n_1]$	97	$[p_1, r_1]$	122	$[z_1, z_2]$
23	$[i_1, d_1]$	48	$[m_1, t_2]$	73	$[v_1, t_2]$	98	$[p_1, t_2]$	123	$[z_1, t_2]$
24	$[i_1, b_1]$	49	$[m_1, n_1]$	74	$[v_1, p_1]$	99	$[p_1, d_1]$	124	$[q_1]$
25	$[i_1, e_1]$	50	$[m_1, t_1]$	75	$[v_1, v_2]$	100	$[p_1, w_2]$	125	$[s_1]$

Note that $N+M$ redundant subsystems are not DPoF safe, if $M<2$. In example AC2(P,E) this applies to q_1 and s_1 which are $1+1$ redundant and therefore only SPoF safe.

Both examples shown here are simplified in order to be able to follow the calculation of the KPIs. DCI models for real data centres shall include all required functional elements, as well as the interdependencies between the functional elements, such as:

1) air conditioning of the rooms in which there are UPSs, main switchgears, and/or generator sets;

2) pumps and piping for the fuel tanks;

3) control equipment for electrical and/or environmental control systems;

4) water supply, pumps, piping and storage for adiabatic cooling systems;

5) systems for switching between different supply paths;

6) feedback of switching states;

7) redundancies of functional elements and/or components.

Note that the effort for calculation can rise exponentially with the complexity of the DCI. Further information on the method of calculation can be found in Reference [1].

Annex B
(informative)

SPoF Analysis for DCIs

Annex B explains the KPI of the number of SPoF by graphical illustrations with the help of RBDs. For this purpose, the SSPs of the AC2 (P,E) RBD of Annex A, shown in Figure A.1, is used. All four possible SSPs are depicted in Figures B.1 to B.4.

Blocks which are members of a particular SSP are marked by bold lines. Blocks which are not members of a particular SSP are given by dashed lines.

In this example, the five shaded blocks are required in all possible SSPs. Thus, each of these blocks represent a SPoF. In other words, the system is not completely fault-tolerant, because the number of SPoF is greater than zero.

The calculation of the total number of SPoF is possible by application of Formula (14).

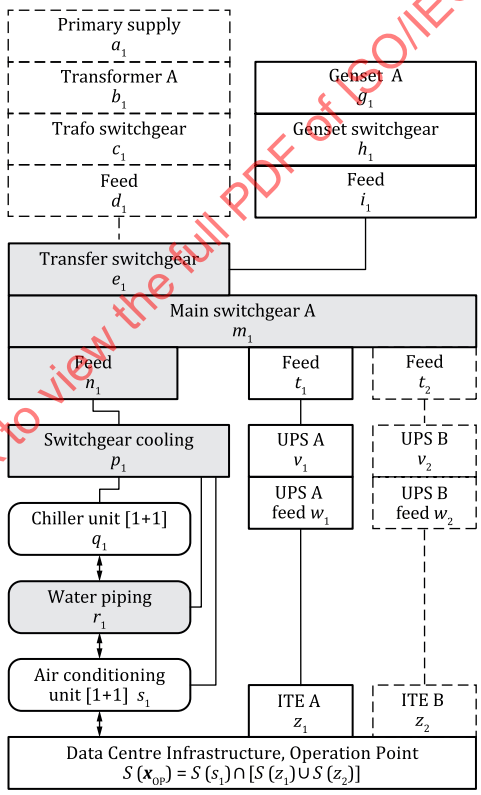

Figure B.1 — 1st SSP of Figure A.1

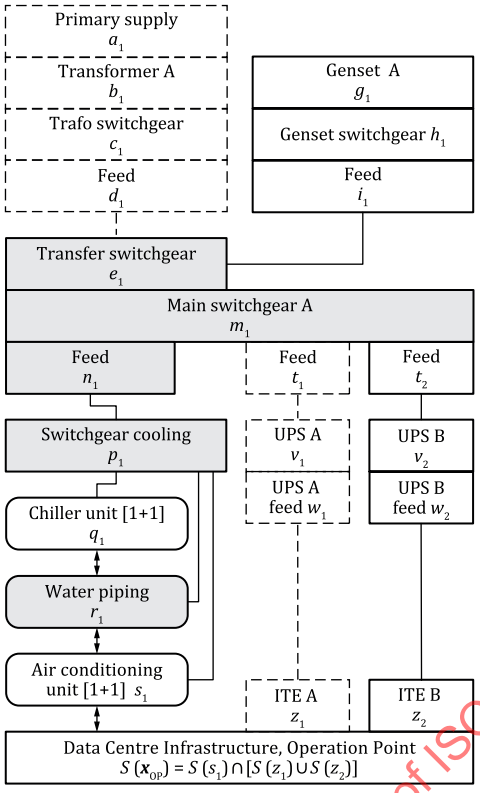

Figure B.2 — 2nd SSP of Figure A.1

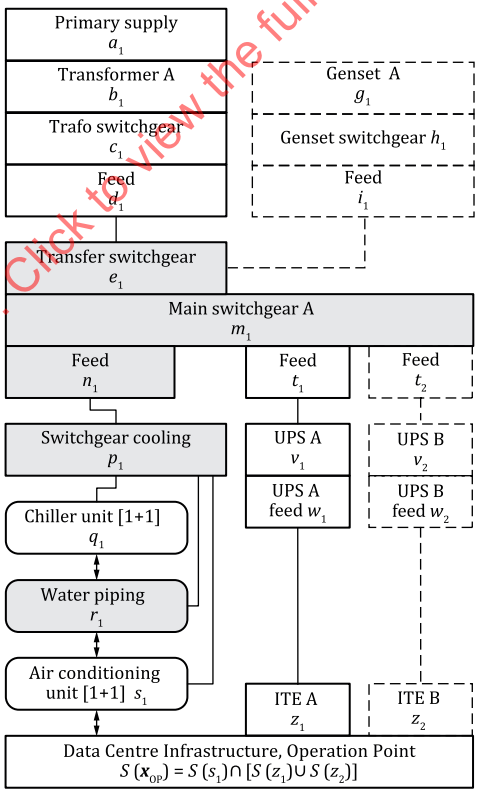

Figure B.3 — 3rd SSP of Figure A.1