2026-06-29

System- og softwareudvikling – Begreber for systemrobusthed

Systems and software engineering – Systems resilience concepts

DANSK STANDARD
Danish Standards Association

Göteborg Plads 1
DK-2150 Nordhavn

Tel: +45 39 96 61 01
dansk.standard@ds.dk
www.ds.dk

DS/ISO/IEC 9837:2026

København
DS projekt: M388029
ICS: 01.040.35
ICS: 35.080

Første del af denne publikations betegnelse er:
DS/ISO/IEC, hvilket betyder, at det er en international standard, der har status som dansk standard.
IDT med: ISO/IEC 9837:2026

DS-publikationen er på engelsk.

I tilfælde af redaktionelle fejl i DS-publikationen kan der skrives til:
editorial-mistakes@ds.dk

ADVARSEL: DS-publikationer revideres over tid. Derudover kan sådanne publikationer ændres ved rettelsesblade og/eller tillæg. Der kan også udgives rettelsesblade, der udelukkende angår oversættelsen af en publikation. Det er derfor vigtigt at sikre sig, at man benytter en gældende udgave, medmindre fx lovgivning kræver andet. Den enkelte publikations status fremgår af https://webshop.ds.dk/. Her kan man desuden tilmelde sig en gratis notifikationsservice og følge en udgivet DS-publikations udvikling ved at klikke på "Følg".

En oversigt over forskellige DS-publikationstyper og -betegnelser findes her:
https://www.ds.dk/publikationstyper

In case of editorial errors in the DS publication, please write to:
editorial-mistakes@ds.dk

NOTICE: DS publications are revised over time. In addition, such publications may be altered by corrigenda and/or amendments. Also, corrigenda may be published solely in relation to the translation of a publication. It is therefore important to ensure that the edition used is valid, unless, for example, legislation requires otherwise. The status of each publication can be found at https://webshop.ds.dk/. Here you can also sign up for a free notification service and follow the progress of a published DS publication by clicking on "Follow".

An overview of different DS publication types and designations can be found here:
https://www.ds.dk/publikationstyper

International

ISO/IEC 9837

Systems and software engineering — Systems resilience concepts

Ingénierie des systèmes et du logiciel — Concepts de résilience des systèmes

First edition
2026-06

Reference number
ISO/IEC 9837:2026(en)

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

Published in Switzerland

ISO (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 7, *Software and systems engineering*.

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.

As the complexity of systems continues to increase and the list of capabilities required of those systems continues to grow, systems are expected to deliver those capabilities under various conditions, including adverse ones. Resilience is the quality characteristic that enables systems to achieve this. Broadly speaking, systems resilience involves the capabilities of systems to avoid, withstand, and recover from adversity. Resilience goals are realized through application of techniques during processes related to requirements, architecture, design or operations of a system.

This document focuses on establishing systems resilience concepts that form the basis for understanding, building and enhancing the resilience of systems. It also provides a resilience framework that includes fundamental objectives, means objectives and techniques for achieving systems resilience. It is compatible with a system engineering approach and with system life cycle processes.

This document serves as a foundation for other documents related to various aspects of systems resilience.

Systems and software engineering — Systems resilience concepts

1 Scope

This document establishes concepts for understanding and improving systems resilience. Systems resilience addresses the capabilities of systems under adversity.

This document is applicable to human-created systems that can be either physical or conceptual, or a combination of both. It applies to systems as defined in ISO/IEC/IEEE 15288, including services and products. It is not intended to apply to naturally occurring systems.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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 Systems resilience fundamentals

3.1.1
resilience
ability to provide required *capability* (3.1.2) in the face of *adversity* (3.1.3)

Note 1 to entry: Under adversity, what is required of a system can be distinct from the capability required during normal operation.

Note 2 to entry: Resilience includes the ability to anticipate and adapt to, resist or quickly recover from a potentially disruptive event.

[SOURCE: MITRE Technical Report MTR-190495, 2019,[23] modified — Notes to entry have been added.]

3.1.2
capability
ability to do something useful under a particular set of conditions

[SOURCE: ISO/IEC/IEEE 24641:2023, 3.1.3, modified — Note 1 to entry has been removed.]

3.1.3
adversity
anything that can degrade the required *capability* (3.1.2) of the system, directly or indirectly

Note 1 to entry: In contrast to risk, which is the effect of uncertainty on objectives (as defined in ISO/IEC/IEEE 15288:2023, 3.39), adversity can be anything actual or possible.

force, demand or influence on a system due to *adversity* (3.1.3) that directly affects the system

3.1.5
error recovery
detection, control, and correction of an internal discrepancy

3.1.6
fault
defect in a system or a representation of a system that if executed/activated can potentially result in an error

[SOURCE: ISO/IEC/IEEE 15026-1:2019,[1)] 3.4.6, modified — Note 1 to entry has been removed.]

3.2 Fundamental objectives

3.2.1
fundamental objective
end goal for achieving *resilience* (3.1.1)

Note 1 to entry: In this document, there are three fundamental objectives of resilience: *avoiding* (3.2.2), *withstanding* (3.2.4) and *recovering* (3.2.3) from *adversity* (3.1.3).

3.2.2
avoiding
eliminating or reducing exposure to *adversity* (3.1.3)

3.2.3
recovering
replenishing lost *capability* (3.1.2) after degradation

Note 1 to entry: The degree of recovery can be less than, the same as, or greater than the degree of degradation.

3.2.4
withstanding
resisting degradation of *capability* (3.1.2) when stressed

3.3 Means objectives

3.3.1
means objective
objective which enables the achievement of other objectives

Note 1 to entry: Means objectives are used to achieve *fundamental objectives* (3.2.1) or other means objectives.

Note 2 to entry: A means objective can be implemented through one or more *resilience techniques* (3.4.1).

Note 3 to entry: Means objectives are named by noun phrases in this document. Some names are based on the approach that is provided, such as *preparation* (3.3.9), *prevention* (3.3.10), *rearchitecting* (3.3.11) and *redeployment* (3.3.12). Some names are based on the outcome achieved, such as *agility* (3.3.3), *integrity* (3.3.8), *robustness* (3.3.13) and *situational awareness* (3.3.15).

EXAMPLE *Anticipation* (3.3.4) is a means objective used to achieve the *fundamental objectives* (3.2.1) of *avoiding* (3.2.2), *withstanding* (3.2.4) and *recovering* (3.2.3) from *adversity* (3.1.3).

1) Cancelled and replaced by ISO/IEC/IEEE 15026-1:2025.

acting to reduce the effectiveness of *adversities* (3.1.3)

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience,[25] modified — removed "number and".]

3.3.3
agility
ability of a system to adapt to deliver required *capability* (3.1.2) in unpredictably evolving conditions

3.3.4
anticipation
establishing awareness of the nature of potential *adversities* (3.1.3), their likely consequences and appropriate responses, prior to the adversity stressing the system

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience,[25] modified — added "establishing".]

3.3.5
damage control
limiting the propagation of malfunction within a system

3.3.6
evolution
modifying a system to address changes over time due to *adversity* (3.1.3) or emergent needs

3.3.7
graceful degradation
ability of a system to transition to acceptable states after damage

Note 1 to entry: See also *fail soft* (3.4.17).

3.3.8
integrity
means by which a system remains complete and unaltered under *adversity* (3.1.3)

3.3.9
preparation
developing and maintaining courses of action that address predicted *adversity* (3.1.3)

3.3.10
prevention
precluding the realization of *adversity* (3.1.3)

3.3.11
rearchitecting
modifying an architecture

3.3.12
redeployment
putting system *capabilities* (3.1.2) into operation following *stress* (3.1.4)

3.3.13
robustness
means to enable a system to function correctly in the presence of invalid inputs or stressful environmental conditions

3.3.14
service continuity
means to deliver required *capability* (3.1.2) under *stress* (3.1.4)

perception of elements in the environment, and a comprehension of their meaning, and could include a projection of the future status of perceived elements and the risk associated with that status

Note 1 to entry: Situational awareness of the environment is complemented by *resilience modelling* (3.4.36) of the internal elements of the system.

[SOURCE: ISO 17757:2019, 3.1.23, modified — Note 1 to entry has been added.]

3.4 Resilience techniques

3.4.1
resilience technique
method to realize a *means objective* (3.3.1)

Note 1 to entry: A resilience technique can contribute to the realization of one or more means objectives.

Note 2 to entry: Resilience techniques are named by noun phrases in this document. Some names are derived from the ability provided by the technique, such as *absorption* (3.4.2), *dynamic repositioning* (3.4.16), *forward recovery* (3.4.19), and *replacement* (3.4.35). Other names are derived from the outcome achieved by application of the resilience technique, such as *fail soft* (3.4.17), *human-in-the-loop* (3.4.20), *safe state* (3.4.38), and *self-modelling* (3.4.40).

3.4.2
absorption
withstanding (3.2.4) *stress* (3.1.4) without unacceptable degradation in the system's *capability* (3.1.2)

3.4.3
adaptive response
dynamic reaction to limit or avoid consequences of an adverse situation

Note 1 to entry: An adaptive response can occur before or after *adversity* (3.1.3) stresses the system.

3.4.4
anomaly detection
discovering salient irregularities or abnormalities in the system or in its environment to enable effective response action

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience,[25] modified — removed "in a timely manner" and replaced "that enables" with "to enable".]

3.4.5
boundary enforcement
implementing process, temporal and spatial limits intended to protect the system

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience[25]]

3.4.6
buffering
reducing degradation due to *stress* (3.1.4) by means of excess capacity

3.4.7
coordinated defence
using multiple, synergistic mechanisms to protect required *capability* (3.1.2)

3.4.8
deception
confusing and thus impeding an adversary

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience[25]]

hierarchical deployment of different levels of diverse equipment and procedures (known as barriers) to prevent the escalation of *faults* (3.1.6) to a hazardous condition

[SOURCE: ISO 1709:2018, 3.12]

3.4.10
detection avoidance
reducing an adversary's awareness of the system

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience[25]]

3.4.11
disaggregation
dispersing missions, functions, subsystems or components across multiple systems or subsystems

3.4.12
distributed privilege
requiring multiple authorized entities to act in a coordinated manner before a system function is allowed to proceed

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience[25]]

3.4.13
diversification
using a heterogeneous set of resources to minimize common vulnerabilities and common mode failures

Note 1 to entry: Resources include technologies, data sources, processing locations, equipment locations, supply chains and communications paths.

3.4.14
domain separation
physically or logically isolating system elements with distinctly different protection needs

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience,[25] modified — "items" has been replaced with "system elements".]

3.4.15
drift correction
preventive action to keep system operation within the boundaries of acceptable performance

3.4.16
dynamic repositioning
relocation of system functionality or components

3.4.17
fail soft
technique to enable prioritized, gradual termination of affected functions, in the case of a *fault* (3.1.6), or when failure is imminent

[SOURCE: IEC 60050:2015:192-10-07, modified — "capable of" has been replaced with "technique to enable".]

3.4.18
fault tolerance
technique to continue functioning with certain *faults* (3.1.6) present

[SOURCE: IEC 60050:2015:192-10-09, modified — "ability" has been replaced with "technique".]

error recovery (3.1.5) in which a system, program, database, or other system resource is restored to a new, not previously occupied state in which it can perform required functions

[SOURCE: IEC 60050:2015:192-10-18]

3.4.20
human-in-the-loop
including persons as part of a system for adaptive *capability* (3.1.2)

3.4.21
least functionality
technique by which each element of the system has the ability to accomplish its required functions, but no more

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience,[25] modified — replaced "when" with "technique by which".]

3.4.22
least persistence
technique by which system elements are available, accessible and able to fulfil their design intent only for the time they are needed

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience,[25] modified — replaced "when" with "technique by which".]

3.4.23
least privilege
technique by which system elements are allocated authorizations that are necessary to accomplish their specified functions, but not more

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience,[25] modified — replaced "when" with "technique by which".]

3.4.24
least sharing
technique by which system resources are accessible by multiple system elements only when necessary, and among as few system elements as possible

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience,[25] modified — replaced "when" with "technique by which".]

3.4.25
loose coupling
technique by which dependencies between elements of a system are intentionally reduced to limit the potential for propagation of damage

3.4.26
maintainability
technique by which a system has the ability to be retained in, or restored to, a state to perform as required

3.4.27
mediated access
controlling the ability to use system elements

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience,[25] modified — removed "access and".]

3.4.28
modularity
technique by which a system is composed of discrete elements such that a change to one element has minimal impact on other components

technique by which a system assumes a condition in which it is acceptable to make no changes while awaiting stakeholder evaluation of possible changes

3.4.30
non-persistence
retaining information, services, and connectivity or functions for a limited time, thereby reducing an adversary's opportunity to exploit vulnerabilities and establish a persistent foothold

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience[25]]

3.4.31
privilege restriction
restricting authorization assigned to entities by an authority

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience[25]]

3.4.32
protective default
technique by which a predetermined configuration of a system safeguards its effectiveness

3.4.33
protective recovery
ensuring that recovery of a system element does not result in, nor lead to, unacceptable loss

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience[25]]

3.4.34
redundancy
technique by which a system has more than one means at a given time for providing required *capability* (3.1.2)

3.4.35
replacement
changing parts of an existing item to regain its functionality

[SOURCE: ISO 20887:2020, 3.32, modified — replaced "change of" with "changing".]

3.4.36
resilience modelling
developing and maintaining useful representations of required system *capabilities* (3.1.2), how those capabilities are generated, the system environment, and the potential for degradation due to *adversity* (3.1.3)

3.4.37
resilience monitoring
gathering, fusing and analysing data to identify vulnerabilities, adverse conditions and system degradation and evaluating the efficacy of system countermeasures

3.4.38
safe state
technique to achieve a state without critical or catastrophic consequences

3.4.39
segmentation
technique by which system elements are separated, logically or physically, to limit the spread of damage

3.4.40
self-modelling
providing a system with a model of itself to enable it to achieve *resilience* (3.1.1)

Note 1 to entry: A system provided with a model of itself can use that model to adapt to *adversities* (3.1.3).

providing the ability to ensure that system components have not been corrupted

[SOURCE: SEBoK, v. 2.11, Taxonomy for Achieving Resilience[25]]

3.4.42
substitution
use of system elements from an alternate source or with differences in form or function to provide or restore *capability* (3.1.2)

3.4.43
system reconfiguration
technique to change the location or functionality of system elements, in the event of failure or external disturbance, to enable the system to continue operation

[SOURCE: IEC 60050:2015, 192-10-15, modified — "process" has been replaced with "technique".]

3.4.44
tolerance
technique to provide *capability* (3.1.2) despite the effects of *stress* (3.1.4) on the system

3.4.45
virtualization
use of digital entities to represent a system, allowing for *redundancy* (3.4.34) and simultaneous use of physical system resources