



DRAFT International Standard

ISO/IEC DIS 9837

Systems and Software Engineering — Systems resilience concepts

ICS: 35.080; 01.040.35

ISO/IEC JTC 1/SC 7

Secretariat: **BIS**

Voting begins on:
2024-10-30

Voting terminates on:
2025-01-22

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 9837:2024(en)

© ISO/IEC 2024  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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

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

Published in Switzerland

Contents

Page

Foreword

iv

Introduction

v

1

Scope

1

2

Normative references

1

3

Terms and definitions

1

3.1

Systems resilience fundamentals

1

3.2

Fundamental objectives

2

3.3

Means objectives

2

3.4

Resilience techniques

4

4

Key resilience concepts and their relationships

7

4.1

The system context for systems resilience

7

4.2

Understanding resilience

8

4.3

Aspects of resilience

8

4.4

Relation of resilience to other system qualities

9

5

A resilience framework

10

5.1

Overview

10

5.2

Fundamental objectives layer

10

5.3

Means objectives layer

10

5.4

Resilience techniques layer

11

5.5

Resilience considerations during systems engineering life cycle activities

12

Bibliography

15

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

This document was prepared by Joint Technical Committee ISO/JTC 1/SC 7/WG 30.

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.

Introduction

As the complexity of systems continues to increase and the list of capabilities required of those systems continues to grow, the systems are expected to deliver those capabilities under various conditions, including adverse ones. Resilience is the quality characteristic that enables systems to achieve this.

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 systems engineering approach and systems 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. Broadly, systems resilience involves the capabilities of systems to avoid, withstand, and recover from adversity.

Adversities can be known or unknown and can arise in many ways, such as security threats, dangers affecting safety, financial and business impacts from external system disruptions, from internal system faults and defects, and from adverse effects of disclosure or loss of data and information. Resilience goals are realized through application of techniques during requirements, architecture, design or operations processes of a system.

This document is applicable to human-created systems that can be either physical or conceptual, or a combination of both. Systems include services and products. It is not intended to apply to naturally occurring systems.

NOTE “System” as used in this document follows the definition and scope of systems in ISO/IEC/IEEE 15288:2023.

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/ui>
- IEC Electropedia: available at <https://www.electropedia.org/>

NOTE For additional terms and definitions in the field of systems and software engineering, see ISO/IEC/IEEE 24765, which is published periodically as a “snapshot” of the SEVOCAB (Systems and software engineering — Vocabulary) database and is publicly accessible at <https://www.computer.org/sevocab>.

3.1 Systems resilience fundamentals

3.1.1 resilience

ability to provide required *capability* (3.1.2) when faced with *adversity* (3.1.3)

[SOURCE: ISO/IEC/IEEE 24641:2023, 3.1.28]

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.