International Standard

ISO/IEC 9837

First edition
2026-06

Systems and software engineering — Systems resilience concepts

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

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

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 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.

Introduction

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.

Bibliography

[1] IEC 60050-192:2015, *International Electrotechnical Vocabulary (IEV) — Part 192: Dependability*

[2] IEC 60300-1, *Dependability management — Part 1: Guidance for management and application*

[3] IEC 62853, *Open systems dependability*

[4] IEEE 982-2024, *IEEE Standard for Measures of the Software Aspects of Dependability*

[5] ISO 1709:2018, *Nuclear energy — Fissile materials — Principles of criticality safety in storing, handling and processing*

[6] ISO 14620-1:2018, *Space systems — Safety requirements — Part 1: System safety*

[7] ISO 17757:2019, *Earth-moving machinery and mining — Autonomous and semi-autonomous machine system safety*

[8] ISO 20887:2020, *Sustainability in buildings and civil engineering works — Design for disassembly and adaptability — Principles, requirements and guidance*

[9] ISO 22301:2019, *Security and resilience — Business continuity management systems — Requirements*

[10] ISO/IEC 25010, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model*

[11] ISO/IEC/TS 25011:2017, *Information technology — Systems and software Quality Requirements and Evaluation (SQuaRE) — Service quality models*

[12] ISO/IEC 25023, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement of system and software product quality*

[13] ISO/IEC 27031, *Cybersecurity — Information and communication technology readiness for business continuity*

[14] ISO/IEC/TS 5723:2022, *Trustworthiness — Vocabulary*

[15] ISO/IEC/IEEE 15026-1:2019[2)], *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

[16] ISO/IEC/IEEE 15288:2023, *Systems and software engineering — System life cycle processes*

[17] ISO/IEC/IEEE 24641:2023, *Systems and Software engineering — Methods and tools for model-based systems and software engineering*

[18] ISO/IEC/IEEE 24765, *Systems and software engineering — Vocabulary*

[19] NIST SP 800-160, *Vol. 2 Rev. 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*

[20] Bodeau, D., et al. Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, The MITRE Corporation, 2015

[21] Boehm B., Chen C., Srisopha K., Shi L. The Key Roles of Maintainability in an Ontology for System Qualities. INCOSE International Symposium, 26(1), 2026–2040, 2016

[22] Brtis J.S. How to Think About Resilience in a DoD Context, MITRE Technical Report MTR-160138, 2016

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

[23] Brtis J.S., McEvilley M.A. Systems Engineering for Resilience, MITRE Technical Report MTR-190495, The MITRE Corporation, 2019

[24] Brtis, J.S., McEvilley, M.A., Unifying Loss-Driven Systems Engineering Activities, INCOSE INSIGHT Magazine, December 2020, Wiley

[25] Brtis J.S., Jackson S., Cureton K. System Resilience, in SEBoK Editorial Board. 2024. *The Guide to the Systems Engineering Body of Knowledge (SEBoK)*, v. 2.11, N. Hutchison (Editor in Chief). Hoboken, NJ: The Trustees of the Stevens Institute of Technology [2025-05-05]. Available from: www.sebokwiki.org

[26] Clemen, R., Reilly, T., Making Hard Decisions with DecisionTools, Cengage Learning, 2014

[27] Keeney, R., Value-Focused Thinking, Harvard University Press, 1992

[28] Vlacheas, P., Stavroulaki, V., Demestichas, P., Cadzow, S., Gorniak, S., Ikonomou, D., Ontology and taxonomies of resilience. European Network and Information Security Agency (ENISA). Heraklion, Greece, 2011

[29] Walden, D.D. et al. (editors), Systems Engineering Handbook: A Guide for System Life Cycle Process and Activities (5th ed.). San Diego, CA: International Council on Systems Engineering. Published by John Wiley & Sons, Inc. 2023

[30] Westrum, R., A Typology of Resilience Situations, chapter 5 of Resilience Engineering Concepts and Precepts, E. Hollnagel, D.D. Woods, N. Leveson (editors), Ashgate, 2006

[31] Winstead, M., Hild, D., McEvilley, M. Principles of Trustworthy Design of Cyber-Physical Systems, MITRE Technical Report #210263, 2021