International Standard

ISO 20682

Autonomous underwater vehicles — Risk and reliability

First edition
2026-02

Reference number
ISO 20682:2026(en)

© ISO 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO 2026

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**
4 Abbreviated terms ... **4**
5 Typical modules of AUVs ... **4**
5.1 General ... 4
5.2 Control ... 4
5.3 Sensors ... 4
5.4 Structure ... 5
5.5 Mechanical moving elements ... 5
5.6 Power ... 5
5.7 Navigation and communication ... 5
5.8 Product identification and traceability ... 6
6 Digital mission engineering ... **6**
6.1 General ... 6
6.2 Extreme mission ... 6
6.3 Simulation, verification and validation ... 7
6.3.1 General ... 7
6.3.2 Virtual testing ... 7
6.3.3 Maximum allowable uncertainties ... 7
7 Fault tree analysis ... **8**
7.1 General ... 8
7.2 Markov chain: state transition ... 9
8 Strategy for risk assessment and risk reduction ... **10**
8.1 General ... 10
8.2 Communication for safety ... 11
8.3 Hardware controls ... 11
8.4 Judgment ... 11
8.5 Reasonableness check ... 11
8.6 Search, rescue and recovery ... 12
8.7 Signal filtering ... 12
8.8 Dependability engineering ... 12
8.9 Safety case ... 12
Annex A (informative) **Reliability engineering mathematical background** ... **14**
Annex B (informative) **Design, verification and testing philosophy for AUVs** ... **18**
Annex C (informative) **Safety of autonomous land vehicles and applications for AUVs** ... **20**
Bibliography ... **21**

© ISO 2026 – All rights reserved

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 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 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. ISO 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.

This document was prepared by Technical Committee ISO/TC 8, *Ships and Marine Technology*, Subcommittee SC 13, *Marine Technology*.

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.

© ISO 2026 – All rights reserved

Introduction

Autonomous underwater vehicles (AUVs) are uncrewed vehicles. They rely on sensors, control units, and mechanical parts to manoeuvre and complete mostly pre-defined tasks in the ocean environment. A growing trend in underwater technology is to face the extreme environment, which refers to, for example, polar environments, rapid currents, extremely high temperatures due to underwater volcanoes, underwater oil plumes, etc. The side effect of using AUVs in extreme environments, however, is a higher risk and probability of failure. The capacity for uncrewed underwater vehicles to perform an extreme mission, which is to perform in an increased level of difficulty, is unknown. Usually, a team of experts employs the vehicle within a trial-and-error process to:

a) achieve the system identification, and

b) measure (most of the time qualitatively) the reliability of the AUV for a specific mission.

This document specifies how an AUV can carry out the actions described in a) and b). This document can therefore be used by the owners and operators of AUVs when designing missions. It should be noted that risk and reliability by nature are probabilistic. This document serves as a linkage between the capabilities of the vehicle and its intended mission, so as to avoid foreseeable undesired settings and circumstances. Despite this ability to foresee problems, faults and failures of the vehicle can be due to uniquely encountered states that have never been observed before. In such cases, dynamic risk analysis and online topic models can be used to expand the operational proficiency of an autonomous vehicle.

© ISO 2026 – All rights reserved

Autonomous underwater vehicles — Risk and reliability

1 Scope

This document specifies the risks and reliability of an autonomous underwater vehicle (AUV) in its underwater realm. It covers sensors, communication devices, and any other pieces and parts directly influencing the "digital mission" of the vehicle. This document does not cover the manufacturing or operation of the following items:

— autonomous underwater gliders (AUGs), as they use a narrowly modifiable set of operational commands;

— batteries for the use of AUVs;

— electrical motors for the use of AUVs.

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
abort
to terminate, in a controlled manner, a processing activity in a computer system because it is impossible, undesirable, or unsafe for an activity to proceed

3.2
availability
degree to which a system or resource is ready when needed

3.3
backout and recovery
activity conducted to bring the system back to a stable state, ending the accident life cycle

3.4
built-in test
test that can be designed into the system by various techniques regarding automation, software, and firmware, and considering the life cycle of the potential accident

3.5
burn-in test
accelerated production test that is designed to detect infant mortality, that is to flush out weaknesses within the component, device or subsystem

© ISO 2026 – All rights reserved

3.6
characteristic value
value of a parameter (either an action or a property of a member or a material) that has a specified probability of not being exceeded

Note 1 to entry: Action refers to external load applied to the vehicle, or an imposed deformation or acceleration.

[SOURCE: ISO 8930:2021, 3.2.2, modified — note to entry added to define the term “action” in this context.]

3.7
code calibration
determination of the reliability elements in a given code format in order to reach the reliability target

3.8
command
control signal or a request from a terminal for the performance of an operation or execution of a particular program

3.9
design value
value to be used in the deterministic design procedure, i.e. *characteristic value* (3.6) multiplied by the safety factor

3.10
deterministic method
calculation method in which the basic variables are treated as non-random

3.11
design point
most probable outcome of the basic variables when *failure* (3.16) occurs

Note 1 to entry: The design point is the point on the limit-state surface with the highest probability density.

3.12
digital mission engineering
modelling of things that move through space in six degrees of freedom (DoF) and time, involving sensors and information transfer

Note 1 to entry: The term was originally coined in assisting the successful conduction of outer space missions.

3.13
error
discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition

3.14
fail-operational
design of a subsystem or device in a way that it can continue operation despite the occurrence of a discrete malfunction

3.15
fail-safe
characteristic of a system whereby any malfunction affecting the system safety will cause the system to revert to a state that is known to be within acceptable risk parameters

3.16
fail-soft
characteristic of a system that continues to provide partial operational capability in the event of a certain malfunction

© ISO 2026 – All rights reserved

3.17
failure
inadvertent termination of a capability of a functional unit to perform its required operation

3.18
fault
inadvertent condition that causes a function to fail to perform in a required (appropriate) manner

3.19
node
point where one or more functional units interconnect, or the representation of a state or an event by means of a point in a diagram

Note 1 to entry: In a tree structure, a node is a point at which subordinate items of data and information originate.

3.20
normal operation
conditions that arise from the intended use and application of the vehicle, including associated condition and integrity monitoring, maintenance, and repair

Note 1 to entry: Normal operations include steady manoeuvring over the full range of design speeds, as well as possible abrupt turns and stopping.

[SOURCE: ISO 16708:2006, 3.28, modified — “pipeline” has been changed to “vehicle” for the use of this document.]

3.21
redundancy
existence in a system of more than one means of accomplishing a given function

3.22
reliability
ability of a system to perform its required functions under stated conditions for a specified period of time

Note 1 to entry: A reliable system is no total assurance of acceptable risk.

3.23
safety case
structured argument backed by evidence

3.24
sensor
device that converts measurable elements of a physical process into data that is meaningful to a computer

3.25
system effectiveness
function of availability, dependability, and capability:

$$P(E) = P(A) \cdot P(D) \cdot P(C)$$

3.26
unit
lowest level of hardware assembly for which acceptance and qualification tests are required

[SOURCE: ISO 19683:2017, 3.4]

3.27
validation
checking of data for correctness or compliance with applicable standards, rules, and conventions

© ISO 2026 – All rights reserved

3.28
verification
act of determining whether an operation has been accomplished correctly

4 Abbreviated terms

AUV	autonomous underwater vehicle
COTS	commercial-off-the-shelf
GPS	Global Positioning System
Dgps	differential GPS
MTBF	Mean Time to Failure
SaFAD	Safety First for Automated Driving
SOTIF	Safety of the Intended Functionality

5 Typical modules of AUVs

5.1 General

AUVs have been employed in the subsea industry for the past few decades. They have shown effective performance in alignment with the emerging trends in science and technology. More rapid production and versatile utilization of these vehicles is foreseen in the future because they have both a robust design and an adaptive performance. Typical modules of a modern AUV are described in 5.2 to 5.8.

NOTE The major subsystems of an AUV include the propulsion system, navigation system, communication system, power system, security detection system and sensor system.[1]

5.2 Control

The control unit has the most direct involvement in the fault incident. Although it is not physically engaged with the AUV mission, the control module of the vehicle shall correctly receive inputs from and send commands to other units.

5.3 Sensors

For this document, the sensors gather every input that must be known for either data acquisition or control purposes of the vehicle. For data acquisition, where data are gathered for subsequent analysis and processing of the mission conditions, a fault incident is not critically detrimental to the mission. At a later time, the operator decides to either replicate or interpolate and extrapolate the missing part of the data. Where data are used as input to the control module, a sensor fault means one or both of the following.

a) Data input is completely interrupted in a way that one or many of the input parameters are completely missing. Depending on the input-output relations, that is the parametric response, the vehicle is susceptible to either incremental or immediate malfunction. Based on such a response, the autonomous vehicle decides on how to abort the mission. In other words, mission abort is a definite result, while the vehicle can hinder abort if this helps to avoid a more severe failure (i.e. fail-soft).

b) Data input is a parasitic intermittent signal. Two scenarios can be imagined:

   1) signal disturbance sustains at a level that does not invoke an emergency action (i.e. fail-operational);

   2) signal disturbance excites an increasing level of errors that interfere with mission integrity (i.e. fail-safe).

© ISO 2026 – All rights reserved