INTERNATIONAL STANDARD

ISO/ IEC/IEEE 15026-2

Second edition
2022-11

Systems and software engineering — Systems and software assurance —

Part 2: Assurance case

Ingénierie du logiciel et des systèmes — Assurance du logiciel et des systèmes —

Partie 2: Cas d'assurance

Reference number
ISO/IEC/IEEE 15026-2:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Institute of Electrical and Electronics Engineers, Inc
3 Park Avenue, New York
NY 10016-5997, USA

Email: stds.ipr@ieee.org
Website: www.ieee.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 ISO/IEC documents should be noted. This document was drafted in accordance with the rules given in the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC 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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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*, in cooperation with the Systems and Software Engineering Standards Committee of the IEEE Computer Society, under the Partner Standards Development Organization cooperation agreement between ISO and IEEE.

This second edition cancels and replaces the first edition (ISO/IEC 15026-2:2011), which has been technically revised.

The main changes are as follows:

— Clause 2 of the previous edition was deleted.

— The title of Clause 5 of the previous edition was changed and became Clause 4 of this edition.

— Revised contents of Clause 6 can be found in Clause 5 of this edition.

— Clause 7 was deleted and its revised contents can be found in 4.2 and 5.2 of this edition.

A list of all parts in the ISO/IEC/IEEE 15026 series can be found on the ISO website.

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 purpose of this document is to define assurance case structure terminology, thereby improving consistency and comparability among instances of assurance cases and facilitating stakeholder communications, engineering decisions, and other uses of assurance cases.

This document does not place requirements on the quality of the contents but describes the structure and meaning of assurance cases with the necessary level of precision and detail so as to avoid inconsistent and subjective use of the terms.

Existing standards addressing different application areas and topics related to assurance cases possibly uses differing terminology and concepts when addressing common themes. This document is based on experience drawn from these specialized standards and guidelines.

While several notations and slightly varying terminologies are currently used in practice, this document does not require the use of any particular concrete representation including graphical representation. Likewise, it places no requirements on physical implementation of the data; in particular, it includes no requirements for redundancy or co-location.

Assurance cases are generally developed to support claims in areas such as safety, reliability, maintainability, human factors, operability, and security. They are applicable to any property of a system. These assurance cases are often called by more specific names, e.g. safety case or dependability case. ISO/IEC/IEEE 15026-1 provides concepts, terminology, background and a list of standards related to assurance cases.

This document uses the terminology and concepts consistent with ISO/IEC/IEEE 12207,[1] ISO/IEC/IEEE 15288,[5] and ISO/IEC/IEEE 15289.[6] This document does not presume or require that it is applied in conjunction with ISO/IEC/IEEE 12207[1] or ISO/IEC/IEEE 15288 [5].

Systems and software engineering — Systems and software assurance —

Part 2: Assurance case

1 Scope

This document specifies requirements for structure terminology of assurance cases.

This document is applicable for developing and maintaining assurance cases.

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/IEEE 15026-1, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC/IEEE 15026-1 and the following apply.

ISO, IEC and IEEE 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/

— IEEE Standards Dictionary Online: available at https://dictionary.ieee.org

NOTE For additional terms and definitions in the field of systems and software engineering, see ISO/IEC/IEEE 24765,[7] which is published periodically as a "snapshot" of the SEVOCAB (Systems and software Engineering Vocabulary) database and is publicly accessible at computer.org/sevocab.

3.1.1
assurance case
auditable artefact that provides a convincing and sound argument for a claim on the basis of tangible evidence under a given context

Note 1 to entry: An argument is valid if and only if it is necessary that if all of the premises are true, then the conclusion is true. An argument is sound if and only it is valid and contains only true premises.

3.1.2
assurance case report
auditable artefact that provides the claim of an *assurance case* (3.1.1) and a complete index of the argument and evidence of the assurance case such that the assurance case of interest can be assembled from the index

Note 1 to entry: An assurance case report is mapped to the report field [5.2 c)]. An assurance case report is an introduction to the assurance case. Its content varies from one case to another. For simple and/or small assurance cases a report can be superfluous. For larger or more complex assurance cases the report can include a system description, some of the argument and its supporting evidence e.g. the higher-level arguments and their supporting evidence.

Note 2 to entry: Assurance case reports are often issued as periodic updates to the assurance case at pre-agreed points such as at the end of a life cycle stage. They report on results of assurance activities done so far, an assessment of overall progress and a review of assurance activities' performance. Assurance case reports can be used at decision gates for stage exit/entry by suppliers and for project monitoring by acquirers.

3.1.3
basic assumption
assumption in a collection of claims shared by *assurance cases* (3.1.1) in a specific field

Note 1 to entry: Such a collection corresponds to a set of axioms in formal system in logic.

3.1.4
inference
reasoning step that derives a claim from a list of claims (premises) under a specified context

Note 1 to entry: The claim derived by inference is the conclusion, and the supported claims from which the inference derives the conclusion are the premises.

Note 2 to entry: There are special inferences called obvious inferences. See 5.3.4 EXAMPLE 2.

3.1.5
property
attribute of things

3.1.6
type
set of values, elements or items

3.1.7
undeveloped argument
placeholder argument to be replaced by a concrete argument

3.2 Abbreviated terms

CAE claims arguments evidence

GSN goal structuring notation

SACM structured assurance case metamodel

4 Use of assurance cases

4.1 Overview

Assurance that the system achieves certain objectives is particularly important when the system and its interaction with the environment are complex and evolving. Assurance cases make claims that concern selected properties of the system, and argue for the truth of those claims. While properties may be selected for any reason, the common reason of selection is that they are uncertain while high

confidence is demanded. An assurance case can be used to establish the values and the uncertainties associated with the claims. The assurance case presents arguments that support the claims. However, uncertainty can arise from a number of aspects of the argument including:

— the validity of the inference linking the claim to its supporting claims;

— the scope and relevance of applied context;

— the relevance and trustworthiness of the evidence supporting the claims.

The objective of the assurance case is to present a convincing argument along with specified ranges of validity or confidence levels. To be convincing, the argument needs to address the uncertainties in a balanced manner and assert that the arguments establish the claims only to the specified levels of validity and confidence. The readers of the assurance case form their conclusions regarding sufficiency of the evidence presented therein.

There are other sources of uncertainty; refer to 2:5.3.3 in Reference [9] for a more complete statement on uncertainties in arguments.

NOTE 1 The values and their uncertainties established for each claim by an assurance case can be non-numerical because not all claims are expressed in terms of numerically measurable property.

NOTE 2 The term "uncertainty" is used as a general term to cover "lack of certainty." See ISO/IEC/IEEE 15026-1:2019, 5.6. Different communities restrict the application of this term to limited usage, e.g. to predictions of future events, to physical measurements already made, or to unknowns; but in this document the term applies to any uncertainty.

Users of the assurance case can assess the truth of the top-level claim that the property of interest is realized in the product or service. The assessment can also cover the uncertainty in the truth of the claim. The assessment of the top-level claim and its support along with related uncertainties and consequences constitute a basis for rationally managing risk, establishing grounds for appropriate confidence, and aiding in decision making. Stakeholders can make better decisions about a system when the uncertainties of conclusions are understood and reduced. Assurance cases are developed for various audiences, taking into account the needs and characteristics of each audience. For example, an assurance case for service developers may differ from an assurance case for regulators, even if the underlying system of interest is one and the same.

NOTE 3 The text often refers to a single assurance case. However, a system can have multiple assurance cases.

The degree of validity and confidence level provided by the assurance case needs to be proportionate to the risk reduction required in the system of interest. Achieving an acceptable level of validity and confidence depend upon the complexities of the system, the technology involved in its construction, the developer's experience with the technology and the novelty of the assurance arguments used. It may also depend on the type of stakeholders concerned in the assurance case and the purpose of its use and the context of their evaluation.

NOTE 4 See ISO/IEC 15026-3[3] for more detailed discussion on this point.

An assurance case argues that interactions of a system with the intended environment of use, including the service it delivers, are as intended/specified. Consequently, the development of the assurance case should be integrated into the whole system life cycle, considering the environment.

NOTE 5 Selecting the top-level claim and the properties it involves is not restricted by this document. Top-level claims can be specified in stakeholder requirements, established by an approval authority for the system or product, or selected for reasons internal to the system.

NOTE 6 Limitations of a system's or product's assurance case are reflected in

— the guidance,

— transition, operations, and maintenance documentation,

— training,

— operator and user aids,

— data collection capabilities, or

— services included in or accompanying the system or product.

Assurance cases need to be maintained as the system evolves. This includes changes in the system design, its operational environment or its use, as these can impact the context and assumptions relied upon in the argument. Assurance cases should be initiated at the earliest life cycle stage of the system of interest and maintained through to its concluding life cycle stage. The system and its life cycle, as well as their environment, change after initial delivery. The technical processes can be changed because of the modifications needed after initial delivery. Also, useful evidence can be obtained after continued operation in production, especially in the case of dependability related claims. In both cases, the original assurance case should be modified or augmented.

NOTE 7 In the context of system life cycle process and software life cycle process, the maintenance activities are not only invoked during operation stage but also during other stages by agreement processes, technical management processes and technical processes. Assurance case maintenance follows the system maintenance life cycle. The milestone for assurance case acceptance and any modifications to the baseline assurance cases, thereby follows the governance of life cycle processes as provided by ISO/IEC/IEEE 15288 [5] and ISO/IEC/IEEE 12207. [1] ISO/IEC/IEEE 15026-4,[4] provides guideline for assurance activities as System Assurance process view and Software Assurance process view.

The truth of the claim should be assessed in a balanced way so as to remove unconscious bias by presenting, for instance, as much uncertainty as can be considered.

4.2 Application of this document

Application of this document supports use of assurance cases by providing for the following.

a) An assurance case having the structure specified by Clause 5 is provided as an artefact or collection of artefacts of the system.

NOTE As an artefact of the system, the assurance case is generally constructed with the system and maintained as the system is maintained.

b) A logical mapping between the assurance case and the structure specified by Clause 5 is provided as a part of the assurance case. [5.3.6 f)]

c) Records documenting the fulfilment of the requirements of this document are produced and provided as a part of the assurance case [5.3.6 g)].

5 Structure of assurance cases

5.1 General

Subclause 5.2 defines the structure of assurance cases by means of a record type that has three fields. 5.3 defines the types that are used in 5.2.

A mechanism shall be provided that helps ensure that each identifier refers to an unambiguously defined value of some type, is an explicitly declared parameter, or is a generally accepted term.

The Appendix D to Reference [10] gives the basis for the approach taken in this clause.

Examples of each structure are provided in Annex A, and a more complex example is given in Annex B. Annex C is a comparison of this document and three community standards GSN, SACM and CAE in terms of mapping the structure terminology in the former to the terms in the latter.

5.2 Top-level structure

An assurance case is a record that has three fields: main field, evidence field and report field.

a) Main field

A supported claim (5.3.5).

NOTE An assurance case is incomplete if its main field contains an undeveloped argument (3.1.7).

b) Evidence field

A set of evidence items (5.3.2).

c) Report field

A narrative introduction (5.3.6). Its assurance goal field (5.3.6 d)) corresponds to the top-level claim of the main field. The contents of the report field constitute the assurance case report (3.1.2).

5.3 Description of types

5.3.1 Context type

The context type is the type of list whose elements are:

a) the definition of a term or identifier;

b) a basic assumption (3.1.3) on the terms defined in the assurance case; or

c) a reference to a document concerning the system of interest.

NOTE 1 Contexts can be used to define identifiers specific to the assurance case that refer to, e.g. evidence items, other components of the assurance case, the system of interest and its components, and the environment of the system of interest.

NOTE 2 When multiple local definitions for an identifier are allowed, the mechanism required in 5.2 enforces proper scoping rules to help ensure that each occurrence of the identifier refers to a unique local definition.

EXAMPLE 1

A definition of "tolerability targets" for each identified hazard can be given in a context.

EXAMPLE 2

A reference to the system requirements specification can be specified in a context.

5.3.2 Evidence type

The evidence type is the record type which has the following four fields. An element of evidence type is called an evidence item:

NOTE 1 An evidence item is an available body of facts or information that support an assertion of truth of a claim.

NOTE 2 Evidence can be a document that demonstrates a redundancy requirement has been physically implemented in a component. It can also be operator and training manuals.

a) An artefact consisting of tangible data or information which includes the following:

1) description of items produced by the life cycle processes of the system of interest, such as contracts and design descriptions;

2) reports provided by the activities of the system of interest, as listed in ISO/IEC/IEEE 15289:2019, 7.6;

3) record provided by the activities of the system of interest, as listed in ISO/IEC/IEEE 15289:2019, 9.3;

4) authoritative documents such as laws, standards and scientific documents on established theory, history, and observations;

b) scope of applicability of the evidence;

c) uncertainty, including the credibility of its source (e.g. authenticity, trustworthiness, and competence) and the measurement accuracy;

d) assumptions associated with the evidence.

NOTE 3 An evidence item can exist independently of the assurance case before its construction, or can be newly created or collected for the purpose of constructing the assurance case. A description of preparation for collecting an evidence item, such as field data, can be another evidence item. An evidence item is to support a claim in the assurance case, as indicated in the definition of argument type (5.3.5).

NOTE 4 The artefact can become quite large. In such cases, the artefact is organized, located, and presented to be understandable to those who review, approve, or directly use it.

NOTE 5 When evidence items are created in developing the assurance case, it is more convenient for them to be managed independently of the arguments.

NOTE 6 Multiple assumptions in d) are taken as their conjunction.

NOTE 7 Evidence and claims are related by supported claim. Additional explanation can be given in a context of that supported claim.

5.3.3 Claim type

The claim type is the type of claim as defined by ISO/IEC/IEEE 15026-1:2019, 3.1.4.

NOTE There are different ways of stating claims: by the probability of the claim being false, or the probability of a situation invalidating the claim occurring or, by the duration for which the claim is valid.

EXAMPLE 1

Failure rate of the memory board is less than 10^{-3} failures per year. (This is an example of limitation on the value of the property associated with the claim. See Note 2 to entry of ISO/IEC/IEEE 15026-1:2019, 3.1.4).

EXAMPLE 2

The certificate for authentication is valid until 2020-12-31. (This is an example of limitations on duration of the claim's validity associated with the claim. See Note 2 to entry of ISO/IEC/IEEE 15026-1:2019, 3.1.4).

EXAMPLE 3

Probability of occurrence of a specific hazard in a year is less than 10^{-3}. (This is an example of condition-related uncertainty. See Note 2 to entry of ISO/IEC/IEEE 15026-1:2019, 3.1.4).

EXAMPLE 4

The code coverage of the software testing is 99 % but the correctness of remaining 1 % is reviewed by the supplier. (This is an example of limitations on the uncertainty of the property value meeting its limitations. See Note 2 to entry of ISO/IEC/IEEE 15026-1:2019, 3.1.4).

EXAMPLE 5

All hazards are considered appropriately managed by safety panel.

5.3.4 Inference type

The inference type is the type of inference (3.1.4).

NOTE An inference combines the supported claims to form an argument (5.3.5).

EXAMPLE 1

An instance of logical inference rule can be an inference. The instances of premises of the inference rule are the premises of the inference and the instance of conclusion of the inference rule is the conclusion of the inference.

EXAMPLE 2

There are special inferences called obvious inferences. The obvious inference can be used when readers are expected to agree with the obviousness. The explicit mention of the obvious inference clarifies the assumptions.

An inference can be universal, like a logical inference rule, or can be specific to the assurance case. Justifications for inferences may be given in a context (5.3.1).

5.3.5 Supported claim type and argument type

The supported claim type and argument type are record types that are mutually recursively defined as follows.

A supported claim consists of

a) a claim C (5.3.3),

b) an argument A that supports a), and

c) a possibly empty list of contexts (5.3.1).

Contexts in the list c) applies to a) and b).

An argument A that supports a claim C is either

d) an undeveloped argument (3.1.7), or

e) a pair consisting of

   1) a possibly empty list of contexts (5.3.1), and

   2) either

      i) an inference *R* (5.3.4) with a list of supported claims SC_1, SC_2, SC_3 ... SC_n, where R derives C from the set of claims of SC_1, SC_2, SC_3 ... SC_n, or

      ii) a reference to an evidence item (5.3.2) that supports the truth of C.

A supported claim is incomplete if it contains undeveloped arguments.

Contexts in e) 1) applies to e) 2) i) and e) 2) ii).

NOTE 1 It is possible that the assurance case writer wishes to concentrate on some parts of assurance case leaving other parts undeveloped for the time being. Undeveloped argument makes explicit that it is left undeveloped.

NOTE 2 A variety of methods can be used to construct an argument. These methods, including the tools used, vary in their applicability, power, resulting accuracy and uncertainty, and ease of use.

NOTE 3 Claims, evidence, and arguments can have uncertainty specified in the context.

EXAMPLE

Figure 1 depicts an example supported claim SC using goal structuring notation (GSN).[11] SC consists of claim C, argument A that supports C, and the empty list of contexts. A is the pair consisting of the empty list of contexts and inference R with the list of supported claims SC_1, SC_2 and SC_3.

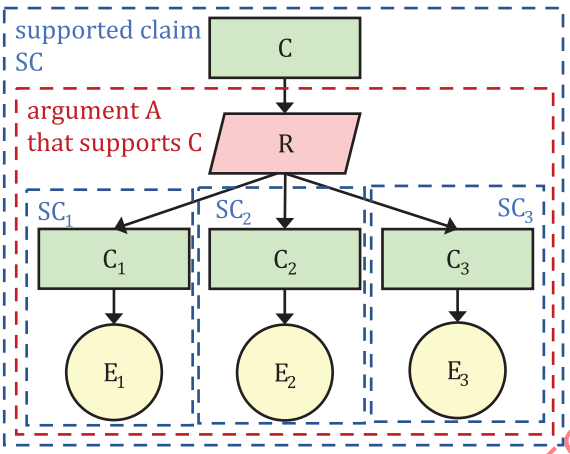

Figure 1 — Example of a supported claim

5.3.6 Narrative introduction type

The narrative introduction type is the record type that has the following fields:

a) description of the system and service;

b) description of the environment in which the system and service are used;

c) description of the system life cycle;

NOTE 1 Descriptions of the transition and disposal process are important in c),

d) the top-level claim of the assurance case together with a discussion of its uncertainty;

NOTE 2 The top-level claim represents the goal of assurance activity.

e) description of all changes relevant to the assurance goal that are made to the previous version of the system or are planned for the next version;

f) an unambiguous mapping between elements of the assurance case and the structure provided by this document that either covers the whole structure or is accompanied by a documented justification for not covering the whole, possibly with information augmenting the assurance case for the purpose of clarifying the mapping;

NOTE 3 If uncertainty is not explicitly specified in a claim, then the mapping can augment it by stating that the uncertainty is negligible.

g) records documenting the fulfilment of the requirements of this document.

NOTE 4 Different parts of an assurance case typically involve different technical fields with different, possibly conflicting, terminologies and notations. The mapping can be supplied with augmenting information for translation among them in order to integrate those parts into the whole structure as specified in this document.

NOTE 5 Narrative can be used in a number of areas, such as an executive summary of findings and conclusions as well as to expand on certain points.

Annex A
(informative)

Examples of supported claims and arguments

This annex provides examples of supported claims and arguments (5.3.5). In each example, a), b), c), d), e) 1), e) 2) i) and e) 2) ii) denotes the field of supported claim and argument. The expression {*a*, *b*, *c*, ...} denotes the set consisting of *a*, *b*, *c*, ... The symbol ∅ denotes an empty set.

A GSN diagram is attached to each example.

EXAMPLE 1

SC_1 is a supported claim and A_1 is an argument. They are given by the following fields. Figure A.1 depicts them.

SC_1 claim a): C_1 argument b): A_1 contexts c): ∅

A_1 contexts e) 1): ∅ reference to evidence item e) 2) ii): E_1

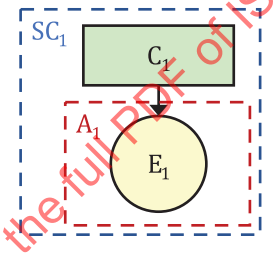

Figure A.1

EXAMPLE 2

SC_1 and SC_2 are supported claims and A_1 and A_2 are arguments. They are given by the following fields. Figure A.2 depicts them.

SC_1 claim a): C_1 argument b): A_1 contexts c): ∅

A_1 contexts e) 1): ∅ inference e) 2) i): R_1 with {SC_2}

SC_2 claim a): C_2 argument b): A_2 contexts c): ∅

A_2 contexts e) 1): ∅ reference to evidence item e) 2) ii): E_1

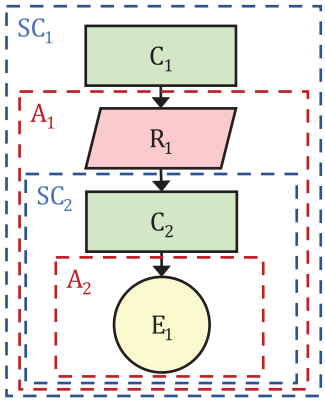

Figure A.2

EXAMPLE 3

SC_1, SC_2 and SC_3 are supported claims and A_1, A_2 and A_3 are arguments. They are given by the following fields. Figure A.3 depicts them.

SC_1	claim a): C_1	argument b): A_1	contexts c): ∅
A_1	contexts e) 1): ∅	inference e) 2) i): R_1 with {SC_2, SC_3}	
SC_2	claim a): C_2	argument b): A_2	contexts c): ∅
A_2	contexts e) 1): ∅	reference to evidence item e) 2) ii): E_1	
SC_3	claim a): C_3	argument b): A_3	contexts c): ∅
A_3	contexts e) 1): ∅	reference to evidence item e) 2) ii): E_2	

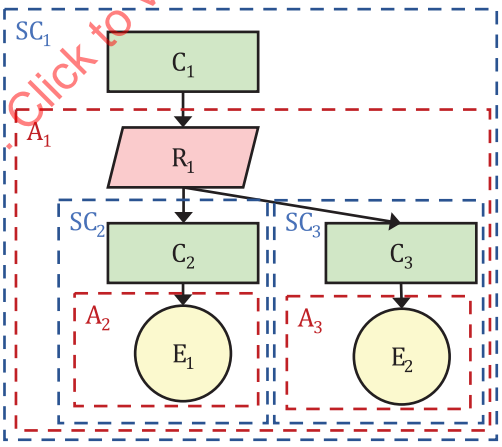

Figure A.3

EXAMPLE 4

SC_1, SC_2 and SC_3 are supported claims and A_1, A_2 and A_3 are arguments. They are given by the following fields. Figure A.4 depicts them.

SC_1	claim a): C_1	argument b): A_1	contexts c): ∅

A_1 contexts e) 1): ∅ inference e) 2) i): R_1 with {SC_2, SC_3}

SC_2 claim a): C_2 argument b): A_2 contexts c): ∅

A_2 contexts e) 1): ∅ reference to evidence item e) 2) ii): E_1

SC_3 claim a): C_3 argument b): A_3 contexts c): ∅

A_3 undeveloped argument d)

The supported claim SC_1 is incomplete since its sub-supported claim SC_3 is undeveloped.

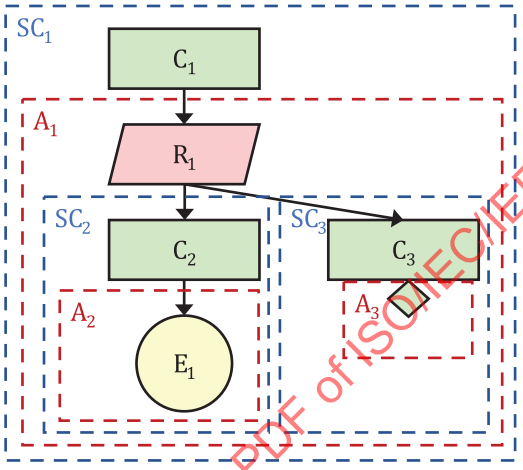

Figure A.4

EXAMPLE 5

SC_1, SC_2 and SC_3 are supported claims and A_1, A_2 and A_3 are arguments. They are given by the following fields. Figure A.5 depicts them.

SC_1 claim a): C_1 argument b): A_1 contexts c): {X_1}

A_1 contexts e) 1): {X_2} inference e) 2) i): R_1 with {SC_2, SC_3}

SC_2 claim a): C_2 argument b): A_2 contexts c): ∅

A_2 contexts e) 1): ∅ reference to evidence item e) 2) ii): E_1

SC_3 claim a): C_3 argument b): A_3 contexts c): ∅

A_3 contexts e) 1): ∅ reference to evidence item e) 2) ii): E_2

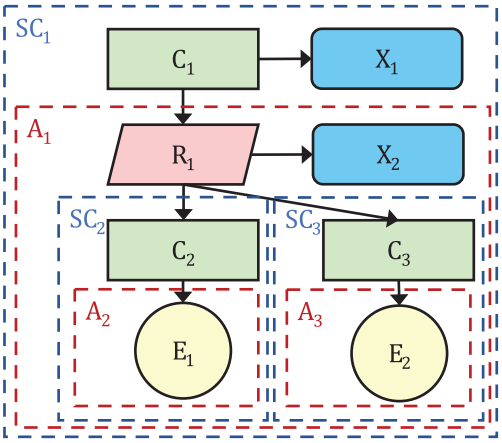

Figure A.5

Annex B
(informative)

An example of top-level structure of assurance cases

B.1 General

This annex provides an example of top-level structure (5.2) of assurance cases; namely, examples of a) main field, b) evidence field and c) report field. Figure B.1 depicts the example using GSN[11].

An assurance case has three fields: a) main field, b) evidence field and c) report field.

In the example, a), b), c), d), e) 1), e) 2) i) and e) 2) ii) denote the field of supported claim and argument. The expression {a, b, c, ...} denotes the set consisting of a, b, c, ... The symbol ∅ denotes an empty set.

NOTE This example assurance case is adapted from Reference [11], p.14.

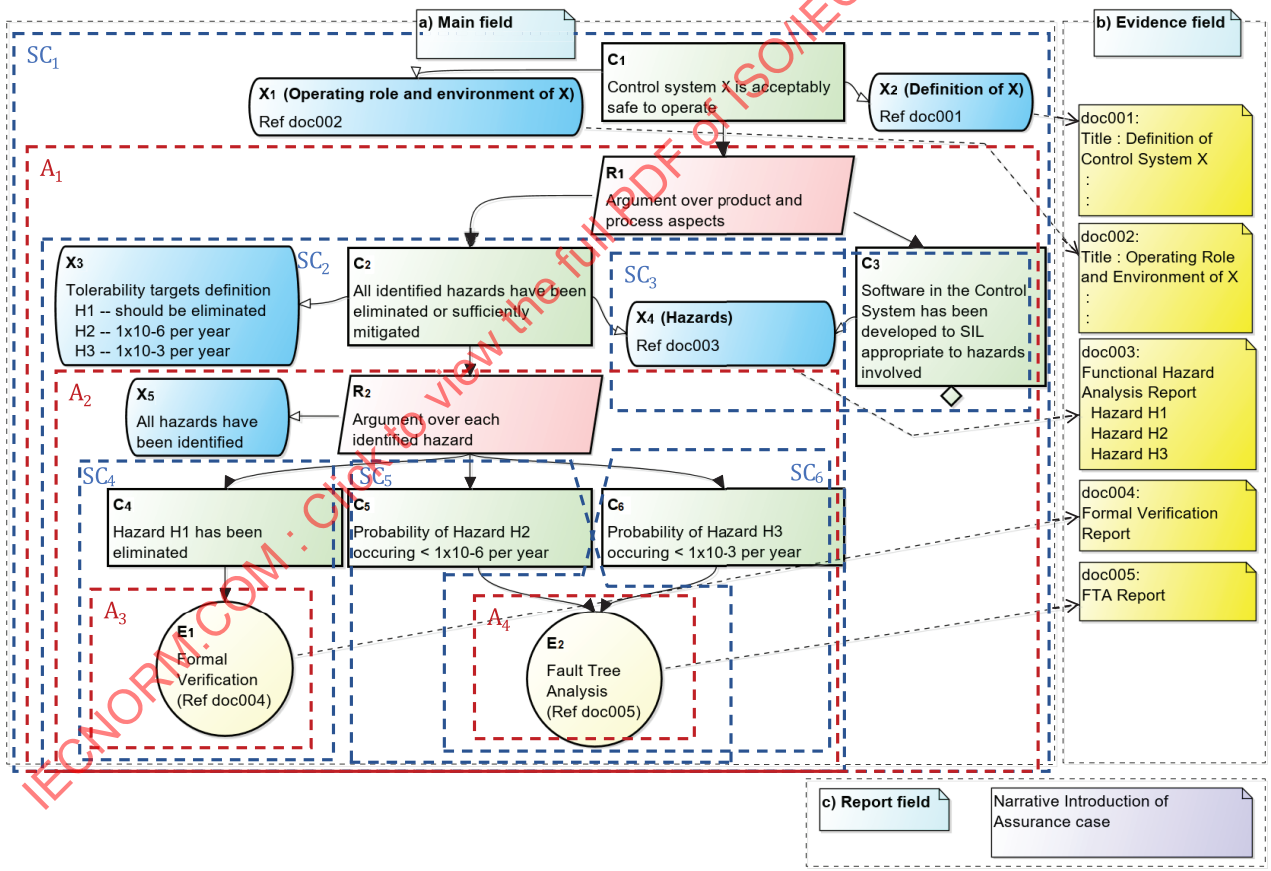

Figure B.1 — Example assurance case

B.2 Main field

The value of the main field is supported claim SC_1. SC_1 and its components are given by the following field values.

Supported claim

SC_1 a): C_1

b) A_1

c) $\{X_1, X_2\}$

SC_2 a) C_2

b) A_2

c) $\{X_3, X_4\}$

SC_3 a) C_3

b) undeveloped argument

c) $\{X_4\}$

SC_4 a) C_4

b) A_3

c) ∅

SC_5 a) C_5

b) A_4

c) ∅

SC_6 a) C_6

b) A_4

c) ∅

Argument

A_1 e) 1) ∅

e) 2) i) R_1

A_2 e) 1) $\{X_5\}$

e) 2) i) R_2

A_3 e) 1) ∅

e) 2) ii) E_1

A_4 e) 1) ∅

e) 2) ii) E_2

Claim

C_1 "Control system X is acceptably safe to operate."

C_2 "All identified hazards have been eliminated or sufficiently mitigated."

C_3 "Software in the Control System has been developed to SIL appropriate to hazards involved."

C_4 "Hazard H_1 has been eliminated."

C_5 "Probability of hazard H_2 occurring is less than $1*10^{-6}$."

C_6 "Probability of hazard H_3 occurring is less than $1*10^{-3}$."

Context

X_1 Operating role and context of X (reference to doc002)

X_2 Definition of the system X (reference to doc001)

X_3 Tolerability targets definition.
H_1 — should be eliminated
H_2 — 1×10^{-6} per year
H_3 — 1×10^{-6} per year

X_4 Hazards identified from FHA (reference to doc003)

X_5 "All hazards have been identified."

Inference

R_1 Argument over product and process aspects, which derives C_1 from $\{SC_2, SC_3\}$

R_2 Argument over each identified hazard, which derives C_2 from $\{SC_4, SC_5, SC_6\}$

Reference to evidence item

E_1 Formal verification report (reference to doc004)

E_2 Fault tree analysis report (reference to doc005)

B.3 Evidence field

The value of the evidence field is the set of five evidence items doc001, doc002, doc003, doc004 and doc005 that are referred to in the main field.

— doc001 Definition of control system X (referred to in the context X_2)

— doc002 Operating role and environment of X (referred to in the context X_1)

— doc003 Functional hazard analysis report (referred to in the context X_4)

— doc004 Formal verification report (referred to by E_1)

— doc005 FTA report (referred to by E_2)

These can be selections from information item contents as provided in ISO/IEC/IEEE 15289.[6] They include, but are not limited to, concept of operations, service level agreement, system requirement specification, system architecture description, as well as problem report and incident report.

B.4 Report field

In the report field, there is a narrative introduction of the assurance case which conforms to the narrative introduction type (5.3.6).

Annex C
(informative)

Comparison of terminology

C.1 General

This annex compares terminology used in this document and in the following documents.

— goal structuring notation (GSN)[11]

— structured assurance case metamodel (SACM™)[12]

— CAE Framework[13],[14]

See Table C.1.

Double quotes are used to mark terms defined in GSN, SACM and CAE.

The structure terminology provided in this document is covered by that of GSN, but not vice versa. For instance, modules and parameters are not covered. Also, the concepts of arguments and argumentation in this document differ from those in GSN. The overview given in this annex addresses only the GSN core notation and has limited ability to represent the GSN extensions necessary to apply best practice in argumentation.

Table C.1 provides a simple association that is expanded upon in the following subclauses. This relationship for GSN is only to the core notation and extensions to GSN are not addressed. GSN and CAE offer concrete representation notations, SACM is a metamodel. Mappings of the metamodels underpinning GSN and CAE notations to the SACM are available.

Table C.1 — Comparison of terminology

No.	This document	GSN[11]	SACM[12]	CAE[13],[14]
1	Context	Context	ArtifactReference	N/A
		Justification	Claim (assertionDeclaration: axiomatic)	
		Assumption	Claim (assertionDeclaration: assumed)	
2	Evidence item	Evidence item	Artifact	Evidence
3	Claim	Goal	Claim (assertionDeclaration: asserted, needsSupport)	Claim
4	Inference	Strategy	ArgumentReasoning	Argument
5	Argument	N/A	N/A	N/A
6	Supported Claim	Argument	ArgumentPackage	N/A
7	Narrative introduction	N/A	N/A	N/A
8	Reference to an evidence item	Solution	ArtifactReference	N/A

C.2 Context (5.3.1)

C.2.1 GSN

A context can be represented as a "context", "assumption", or "justification" of GSN, depending on the nature of the context (subclauses 0:4.5, 0:4.6, 0:4.7, 1:2.1.4 and 1:2.2.7—1:2.2.19 of Reference [11]).

The GSN makes a semantic differentiation between these types of contextual elements in addition to the symbolic differences.

NOTE See also C.7 for the conceptual differences GSN uses for 'Argument' and its treatment of evidence items.

C.2.2 SACM

A context can be represented as an "ArtifactReference" or a "Claim" with "assertionDeclaration" set to "assumed" or to "axiomatic". Either way, it should be associated with a "Claim" or an "AssertedInference" to which the context is added by an "AssertedContext". Contextual information for the whole assurance case, e.g. definition of terms, can be included in a "TerminologyPackage" contained in an "AssuranceCasePackage" (subclauses 11.9, 11.11, 11.14, 11.16, 10.4, and 9.2 of Reference [12]).

C.2.3 CAE

The concept of a context has no named counterpart in CAE. "Other" node type (See 3.1.5 of Reference [15] for example of its usage) can be used for contexts. Contextual information can also be contained in a "claim"[13] and in a "side-warrant"[14].

C.3 Evidence item (5.3.2)

C.3.1 GSN

An evidence item itself has no representation in GSN notation. A "solution" containing a reference to an evidence item is used instead (subclauses 1:2.1.4 and 1:2.2.7—1:2.2.9 of Reference [11]). "Evidence" is explained as "information or objective artefacts being offered in support of one or more claims" in the glossary of Reference [11]. While assurance cases defined in this document can contain evidence items themselves (5.2 b) evidence field), "goal structures" in GSN can contain only references to them.

NOTE See also C.7 for the conceptual differences GSN uses for argument and its treatment of evidence items.

C.3.2 SACM

An evidence item can be represented as an "Artifact" associated with a "Claim" by an "AssertedEvidence." (subclauses 12.7, 11.11, 11.15 of Reference [12]).

C.3.3 CAE

An evidence item itself has no representation in CAE notation. An "evidence" in CAE is a reference to the evidence item[13].

C.4 Claim (5.3.3)

C.4.1 GSN

A claim is represented as a "goal" (subclause 1:2.1.4 and 1:2.3 of Reference [11]).

C.4.2 SACM

A claim can be represented as a "Claim" of SACM. Its attribute "assertionDeclaration" should be set either to "asserted" if the argument supporting it does not contain an undeveloped argument, or to "needsSupport" otherwise (subclauses 11.11, 11.8 of Reference [12]).

C.4.3 CAE

A claim can be represented as a "Claim" of CAE[13].

C.5 Inference (5.3.4)

C.5.1 GSN

An inference can be represented as a "strategy" (subclause 1:2.1.4 and 1:2.2.3—1:2.2.6 of Reference [11]). A strategy is an optional element in GSN. Its presence does not modify the semantics of the argument. It is only provided for clarity and its omission implies an obvious inference (3.1.4).

C.5.2 SACM

An inference can be represented as an "ArgumentReasoning" associated with an "AssertedInference" (subclauses 11.12, 11.14 of Reference [12]).

C.5.3 CAE

An inference can be represented as an "Argument" of CAE[13].

C.6 Supported claim (5.3.5)

C.6.1 GSN

The concept of a supported claim has no named counterpart in the core GSN. A supported claim corresponds to that part of an overall goal structure consisting of a "goal" and all the elements reachable from it through links "SupportedBy" and "InContextOf" (See Reference [11]).

C.6.2 SACM

The concept of a supported claim has no named counterpart in SACM. A supported claim corresponds to a collection of elements consisting of a "Claim" and all the elements reachable from it through "AssertedRelationship"s. Such a collection can be represented using the more general concept of an "ArgumentPackage" (subclause 11.4 of Reference [12]).

C.6.3 CAE

The concept of a supported claim has no named counterpart in CAE. A supported claim corresponds to that part of an overall CAE structure consisting of a "claim" and all the elements supporting it.

C.7 Argument (5.3.5)

The concept of an argument in this document has no named counterpart in GSN, SACM nor CAE. In particular, argument in the sense of this document is different from "argument" in GSN. Similarly to how a supported claim corresponds to that part of goal structure in GSN that is headed by a "goal", the concept of an argument in this document corresponds to that part of goal structure headed by a "strategy" etc. In CAE, an argument can be represented as that part of a structure headed by "argument".