International Standard

ISO/IEC/IEEE 15026-1

Second edition
2025-12

Systems and software engineering — Systems and software assurance —

Part 1: Vocabulary and concepts

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

Partie 1: Vocabulaire et concepts

Reference number
ISO/IEC/IEEE 15026-1:2025(en)

COPYRIGHT PROTECTED DOCUMENT

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

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
3.1 Terms related to assurance ... 1
3.2 Terms related to system life cycles ... 4
3.3 Terms related to integrity level ... 6
3.4 Terms related to risks and dependability ... 7
4 Basic concepts ... **10**
4.1 General ... 10
4.2 Assurance ... 10
4.3 Stakeholders ... 11
4.4 System and product ... 11
4.5 Property ... 11
4.5.1 General ... 11
4.5.2 Properties as behaviours ... 12
4.6 Uncertainty and confidence ... 12
4.7 Conditions and initiating events ... 12
4.8 Consequences ... 13
5 Using multiple parts of the ISO/IEC/IEEE 15026 series ... **13**
5.1 General ... 13
5.2 Initial usage guidance ... 13
5.3 Relationships among parts of the ISO/IEC/IEEE 15026 series ... 14
5.4 Authorities ... 14
6 The ISO/IEC/IEEE 15026 series and the assurance case ... **14**
6.1 General ... 14
6.2 Justification of method of reasoning ... 15
6.3 Means of obtaining and managing evidence ... 16
6.4 Certifications and accreditations ... 16
7 The ISO/IEC/IEEE 15026 series and integrity levels ... **16**
7.1 General ... 16
7.2 Risk analysis ... 17
8 The ISO/IEC/IEEE 15026 series and the life cycle ... **17**
8.1 General ... 17
8.2 Assurance activities in the life cycle ... 18
Bibliography ... **19**
IEEE notices and abstract ... **25**

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).

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.

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*, 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/IEEE 15026-1:2019), which has been technically revised.

The main changes are as follows:

— definitions of terms introduced in other parts of the ISO/IEC/IEEE 15026 series have been added or modified;

— definitions of terms whose definitions were sourced from ISO/IEC 15288 and ISO/IEC/IEEE 24774 have been updated.

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

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

Software and systems assurance and closely related fields share concepts but have different vocabularies and perspectives. This document provides an unambiguous use of vocabulary for systems and software assurance and a unifying set of underlying concepts across these various fields. It provides a basis for elaboration, discussion and recording agreement and rationale regarding concepts and the vocabulary used uniformly across the ISO/IEC/IEEE 15026 series.

Clause 4 covers basic concepts such as assurance, stakeholders, systems and products, property, uncertainty and confidence, conditions and initial events, and consequence. Clause 5 covers some issues of which users of ISO/IEC/IEEE 15026-2, ISO/IEC/IEEE 15026-3 and ISO/IEC/IEEE 15026-4 should be initially aware (5.2). Clause 6, Clause 7 and Clause 8 cover concepts relevant to users of ISO/IEC/IEEE 15026-2, ISO/IEC/IEEE 15026-3 and ISO/IEC/IEEE 15026-4, respectively; also, users of one of these parts can benefit from the clauses for other parts.

The essential concepts introduced by the ISO/IEC/IEEE 15026 series are the claims in an assurance case and the support of claims in terms of argument and evidence. These claims are in the context of assurance for properties of systems and software within life cycle processes for the system or software product.

Potential users of the ISO/IEC/IEEE 15026 series are developers and maintainers of assurance cases and those who wish to develop, sustain, evaluate or acquire a system that possesses requirements for specific properties in such a way as to be more certain of those properties and their requirements. The ISO/IEC/IEEE 15026 series uses concepts and vocabulary consistent with ISO/IEC/IEEE 12207 and ISO/IEC/IEEE 15288 and generally consistent with the standards on Systems and software Quality Requirements and Evaluation (SQuaRE) developed by JTC 1/SC 7, but the concepts and vocabulary provided by the ISO/IEC/IEEE 15026 series can differ from those to which the potential user is accustomed. This document attempts to clarify these differences.

The ISO/IEC/IEEE 15026 series is made up of the following parts.

— ISO/IEC/IEEE 15026-1 explains concepts and terms as a basis for all parts of the ISO/IEC/IEEE 15026 series.

— ISO/IEC/IEEE 15026-2 includes requirements on the structure of the assurance case.

— ISO/IEC/IEEE 15026-3 relates integrity levels to the assurance case and includes requirements for their use with and without an assurance case.

— ISO/IEC/IEEE 15026-4 provides guidance and recommendations for assurance of a selected claim about the system-of-interest by achieving the claim and showing the achievement. The guidance and recommendations are given in a system assurance process view on top of ISO/IEC/IEEE 15288 and a software assurance process view on top of ISO/IEC/IEEE 12207.

The assurance case is relevant to a greater or lesser extent in all parts of the ISO/IEC/IEEE 15026 series, although ISO/IEC/IEEE 15026-4 discusses achieving the claim and showing the achievement of the claim whether or not such “showing” is contained in an artefact specifically called an “assurance case”.

ISO/IEC/IEEE 15026-2 concentrates on the contents and structure of the assurance case. ISO/IEC/IEEE 15026-3 relates integrity levels and assurance cases by describing how integrity levels and assurance cases can work together, especially in the definition of specifications for integrity levels or by using integrity levels within a portion of an assurance case. This relationship is governed by the degree of risk and dependencies in the system.

ISO/IEC/IEEE 15026-4 includes assurance-related guidance and recommendations for activities across the life cycle processes including activities that extend beyond those directly related to an assurance case, e.g. project planning for assurance-related considerations.

Systems and software engineering — Systems and software assurance —

Part 1: Vocabulary and concepts

1 Scope

This document defines assurance-related terms and establishes an organized set of concepts to form a basis for shared understanding in the field of assurance. It benefits users of ISO/IEC/IEEE 15026-2, ISO/IEC/IEEE 15026-3 and ISO/IEC/IEEE 15026-4.

Vocabulary and concepts for assurance of a service being operated and managed on an ongoing basis is not covered in this document.

While essential to assurance practice, details regarding exactly how to measure, demonstrate or analyse particular properties are not covered.

2 Normative references

There are no normative references in this document.

Bibliography

[1] IEC 31010, *Risk management — Risk assessment techniques*

[2] IEC 60050-192:2015, *International electrotechnical vocabulary — Part 192: Dependability*

[3] IEC 60300 (all parts), *Dependability management*

[4] IEC 60812, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*

[5] IEC 61025, *Fault tree analysis (FTA)*

[6] IEC 61078, *Reliability block diagrams*

[7] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[8] IEC 61511 (all parts), *Functional safety — Safety instrumented systems for the process industry sector*

[9] IEC 61882, *Hazard and operability studies (HAZOP studies) — Application guide*

[10] IEC 62741, *Reliability of systems, equipment, and components. Guide to the demonstration of dependability requirements. The dependability case*

[11] IEEE Std 1012-2024, *IEEE Standard for System, Software, and Hardware Verification and Validation*

[12] IEEE 1633-2016, *IEEE Recommended Practice on Software Reliability*

[13] ISO 12100, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

[14] ISO 13849 (all parts), *Safety of machinery — Safety-related parts of control systems*

[15] ISO 14620 (all parts), *Space systems — Safety requirements*

[16] ISO 14625, *Space systems — Ground support equipment for use at launch, landing or retrieval sites — General requirements*

[17] ISO 14971, *Medical devices — Application of risk management to medical devices*

[18] ISO 19706, *Guidelines for assessing the fire threat to people*

[19] ISO 20282-1:2006, *Ease of operation of everyday products — Part 1: Design requirements for context of use and user characteristics*

[20] ISO/TS 20282-2:2013, *Usability of consumer products and products for public use Part 2: Summative test method*

[21] ISO 2394, *General principles on reliability for structures*

[22] ISO 28003, *Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems*

[23] ISO 31000, *Risk management — Guidelines*

[24] ISO 31073:2022, *Risk management — Vocabulary*

[25] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[26] ISO 9241 (all parts), *— Ergonomics of human-system interaction*

[27] ISO/IEC 15408-1, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security, Part 1: Introduction and general model*

[28] ISO/IEC 18014 (all parts), *Information security — Time-stamping services*

[29] ISO/IEC 19770 (all parts), *Information technology — IT asset management*

[30] ISO/IEC 21827:2008, *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)*

[31] ISO/IEC 2382:2015, *Information technology — Vocabulary*

[32] ISO/IEC 25000, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE*

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

[34] ISO/IEC 25012, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model*

[35] ISO/IEC 25020, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality measurement framework*

[36] ISO/IEC 25030, *Systems and software engineering — Systems and software quality requirements and evaluation (SQuaRE) — Quality requirements framework*

[37] ISO/IEC 25040, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality evaluation framework*

[38] ISO/IEC 25051, *Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing*

[39] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[40] ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[41] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

[42] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

[43] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[44] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[45] ISO/IEC 27006-1, *Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General*

[46] ISO/IEC 27011, *Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations*

[47] ISO/IEC 27033 (all parts), *— Information technology – Network security*

[48] ISO/IEC/IEEE 90003, *Software engineering — Guidelines for the application of ISO 9001:2008 to computer software*

[49] ISO/IEC Guide 51:2014, *Safety aspects — Guidelines for their inclusion in standards*

[50] ISO/IEC/TR 15443 (all parts), *Information technology — Security techniques — Security assurance framework*

[51] ISO/IEC/IEEE 12207:2017, *Systems and software engineering — Software life cycle processes*

[52] ISO/IEC/IEEE 15026-2, *Systems and software engineering — Systems and software assurance — Part 2: Assurance case*

[53] ISO/IEC/IEEE 15026-3, *Systems and software engineering — Systems and software assurance — Part 3: System integrity levels*

[54] ISO/IEC/IEEE 15026-4, *Systems and software engineering — Systems and software assurance — Part 4: Assurance in the life cycle*

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

[56] ISO/IEC/IEEE 15289, *Systems and software engineering — Content of life-cycle information items (documentation)*

[57] ISO/IEC/IEEE 15939, *Systems and software engineering — Measurement process*

[58] ISO/IEC/IEEE 16085, *Systems and software engineering — Life cycle processes — Risk management*

[59] ISO/IEC/IEEE 16326, *Systems and software engineering — Life cycle processes — Project management*

[60] ISO/IEC/IEEE 24748 (all parts), *Systems and software engineering — Life cycle management*

[61] ISO/IEC/IEEE 24774:2021, *Systems and software engineering — Life cycle management — Specification for process description*

[62] ISO/IEC/IEEE 29148:2018, *Systems and software engineering — Life cycle processes — Requirements engineering*

[63] ISO/IEC/IEEE 42010, *Software, systems and enterprise — Architecture description*

[64] ISO/IEC/TR 15446, *Information technology — Security techniques — Guidance for the production of protection profiles and security targets*

[65] Adelard. The Adelard Safety Case Development Manual. Available at https://www.adelard.com/web/hnav/resources/ascad

[66] Altman W., Ankrum T., Brach W. Improving Quality and the Assurance of Quality in the Design and Construction of Nuclear Power Plants: A Report to Congress. NUREG 1055, U.S. Nuclear Regulatory Commission: Office of Inspection and Enforcement, 1987, https://www.nrc.gov/docs/ML0630/ML063000293.pdf

[67] Ankrum T.S., Kromholz A.H. “Structured Assurance Cases: Three Common Standards,” Ninth IEEE International Symposium on High-Assurance Systems Engineering (HASE'05), pp. 99-108, 2005

[68] Armstrong, J.M. and Paynter S.P. The Deconstruction of Safety Arguments through Adversarial Counter-argument. School of Computing Science, Newcastle University CS-TR-832, 2004

[69] Atchison B., Lindsay P., Tombs D. A Case Study in Software Safety Assurance Using Formal Methods. Technical Report No. 99-31. Sept. 1999

[70] Berg C.J. High-Assurance Design: Architecting Secure and Reliable Enterprise Applications. Addison Wesley, 2006

[71] Bernstein, Lawrence and C. M. Yuhas. Trustworthy Systems through Quantitative Software Engineering. Wiley-IEEE Computer Society Press, 2005. About reliability not security

[72] Bishop M., Engle S. The Software Assurance CBK and University Curricula. Proceedings of the 10th Colloquium for Information Systems Security Education, 2006

[73] Bishop, P. and Bloomfield, R. The SHIP Safety Case Approach. SafeComp95, Belgirate, Italy. Oct 1995

[74] Bishop P., Bloomfield R. A Methodology for Safety Case Development. Industrial Perspectives of Safety-critical Systems. In Proceedings of the Sixth Safety-critical Systems Symposium, Birmingham. 1998

[75] CAP 760 Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases for Aerodrome Operators and Air Traffic Service Providers, 10 December 2010

[76] Chung L. et al. Non-Functional Requirements in Software Engineering. Kluwer, 1999

[77] CNSS. National Information Assurance Glossary, CNSS Instruction No. 4009, 26 April 2010. Available at https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf

[78] Committee on Information Systems Trustworthiness. Trust in Cyberspace, Computer Science and Telecommunications Board. National Research Council, 1999

[79] Common C.R.A. (CCRA). Common Criteria v3.1 Revision 2. NIAP September 2007. Available at https://www.commoncriteriaportal.org/.

[80] Courtois P.-J. Justifying the Dependability of Computer-based Systems: With Applications in Nuclear Engineering. Springer, 2008

[81] Department of Defense Directive 8500.1 (6 February 2003). Information Assurance (IA), Washington, DC: US Department of Defense, ASD(NII)/DoD CIO, April 23, 2007. Available at https://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

[82] Department of Defense Strategic Defense Initiative Organization. Trusted Software Development Methodology, SDI-S-SD-91-000007, vol. 1, 17 June 1992

[83] Dependability Research Group. Safety Cases. University of Virginia, Available at: https://web.archive.org/web/20131229153301/[3)]

[84] Despotou G., Kelly T. Extending the Safety Case Concept to Address Dependability, Proceedings of the 22nd International System Safety Conference, 2004

[85] Fenton N., Littlewood B., Neil M., Strigini L., Sutcliffe A., Wright D. Assessing dependability of safety critical systems using diverse evidence. IEE Proc. Softw. 1998 145 (1) pp. 35–39

[86] Greenwell W.S., Knight J.C., Pease J.J. A Taxonomy of Fallacies in System Safety Arguments. 24th International System Safety Conference, Albuquerque, NM, August 2006

[87] Kelly T. Arguing Safety — A Systematic Approach to Managing Safety Cases. Doctorial Thesis — University of York: Department of Computer Science. Sept 1998

[88] Kelly T. Reviewing Assurance Arguments — A Step-by-Step Approach. Workshop on Assurance Cases for Security: The Metrics Challenge, International Conference on Dependable Systems and Networks, 2007

[89] Kelly T., Weaver R. The Goal Structuring Notation — A Safety Argument Notation. Workshop on Assurance Cases: Best Practices, Possible Obstacles, and Future Opportunities, Florence, Italy. July 2004

[90] Ladkin P. The Pre-Implementation Safety Case for RVSM in European Airspace is Flawed. 29 Aug 2002. Available at http://www.rvs.uni-bielefeld.de/publications/Reports/SCflawed-paper.html

[91] Lautieri S., Cooper D., Jackson D. SafSec: Commonalities Between Safety and Security Assurance. Proceedings of the Thirteenth Safety Critical Systems Symposium — Southampton, 2005

[92] Lipner S., Howard M. The Trustworthy Computing Security Development Lifecycle, Microsoft, 2005. Available at https://msdn.microsoft.com/en-us/library/ms995349.aspx

[93] Maguire R. Safety Cases and Safety Reports: Meaning, Motivation and Management. Ashgate, 2006

3) http://dependability.cs.virginia.edu/info/safety_cases

[94] McDermid J. Software Safety: Where's the Evidence? 6th Australian Workshop on Industrial Experience with Safety Critical Systems and Software (SCS '01), Brisbane. 2001

[95] Merkow M.S., Breithaupt J. Computer Security Assurance Using the Common Criteria. Thompson Delmar Learning, 2005

[96] National Aeronautics and Space Administration (NASA)). Software Assurance Guidebook. September 1989 (assurance and software safety standard, NASA-GB-A201).STD-8739.8B. Available at http://www.hq.nasa.gov/office/codeq/doctree/nasa_gb_a201.pdf[4)]

[97] National Offshore Petroleum Safety Authority. Safety cases and validation. Online Documents cited on 20 Jun 2012. Available at https://www.nopsema.gov.au/offshore-industry/safety/safety-cases-and-validation

[98] NDIA System Assurance Committee. Engineering for System Assurance. National Defense Industrial Association, USA, 2008. Available at https://www.ndia.org/-/media/sites/ndia/meetings-and-events/divisions/systems-engineering/sse-committee/systems-assurance-guidebook.pdf

[99] OPSI. The Offshore Installations (Safety Case) Regulations 2005. [Online Document cited on: 20 June 2012] Available at http://www.opsi.gov.uk/si/si2005/20053117.htm

[100] Park J., Montrose B., Froscher J. Tools for Information Security Assurance Arguments. DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings, 2001

[101] Randell, B., and Koutny, M. Failures: Their Definition, Modelling and Analysis. School of Computing Science, Newcastle University CS-TR NO 994, Dec 2006; Randell, B., and Rushby, J.M. Distributed Secure Systems: Then and Now. CS-TR No 1052 School of Computing Science, Newcastle University, Oct 2007

[102] Redwine S.T. Jr. The Quality of Assurance Cases. Workshop on Assurance Cases for Security: The Metrics Challenge, International Conference on Dependable Systems and Networks, 2007

[103] Severson K. Yucca Mountain Safety Case Focus of NWTRB September Meeting. United States Nuclear Waste Technical Review Board. Aug 2006

[104] Software and Systems Engineering Vocabulary (sevocab). Available at www.computer.org/sevocab

[105] Stanford Encyclopedia of Philosophy. "Properties", Available at: https://plato.stanford.edu/entries/properties/, substantive revision 2016-02-17

[106] Strunk, E. and Knight, J. The Essential Synthesis of Problem Frames and Assurance Cases. IWAAPF'06, Shanghai, China. May 2006

[107] Swiderski F., Snyder W. Threat Modeling. Microsoft Press, 2004

[108] The Assurance Case Working Group (ACWG). Goal Structuring Notation Community Standard (Version 3), Version 3 of the Goal Structuring Notation (GSN) Standard. [SCSC-141C], Safety-Critical Systems Club, May 2021, available at https://scsc.uk/r141C:1

[109] U.S. NRC. "Quality Assurance Case Studies at Construction Projects."

[110] Vanfleet, W.M., et al. "MILS: Architecture for High Assurance Embedded Computing," Crosstalk, August, 2005

[111] Walker, V.R. Risk Regulation and the 'Faces' of Uncertainty, Risk: Health, Safety and Environment. p. 27-38, Winter 1998

[112] Washizaki H., ed. Guide to the Software Engineering Body of Knowledge (SWEBOK Guide), Version 4.0, IEEE Computer Society, 2024; www.swebok.org Abran A., Moore J.W. (Executive editors); Pierre Bourque, Robert Dupuis, Leonard Tripp (Editors). Guide to the Software Engineering Body of

4) https://standards.nasa.gov/standard/NASA/NASA-STD-87398

Knowledge. 2004 Edition. Los Alamitos, California: IEEE Computer Society, Feb. 16, 2004. Available at http://www.swebok.org

[113] Weaver R. The Safety of Software — Constructing and Assuring Arguments. Doctorial Thesis — University of York: Department of Computer Science. 2003

[114] Weaver R., Fenn J., Kelly T. A Pragmatic Approach to Reasoning about the Assurance of Safety Arguments. 8th Australian Workshop on Safety Critical Systems and Software (SCS'03), Canberra. 2003

[115] Williams J., Schaefer M. Pretty Good Assurance. Proceedings of the New Security Paradigms Workshop. IEEE Computer Society Press. 1995

[116] Williams, J.R., Jelen G.F. A Framework for Reasoning about Assurance, Document Number ATR 97043, Arca Systems, Inc., 23 April 1998