

/ 15026-1— 2016

1

(ISO/IEC 15026-1:2013, IDT)



1 » () 2 22 « 3 26 2016 . 281-4 15026-1:2013 « 1. » (ISO/IEC 15026-1:2013 «Systems and software engineering — assurance — Part 1: Concepts and vocabulary», IDT). Systems and software 8 5 1.0—2012 (8). 1 (www.gost.)

© , 2016

,

П

1			1
2			1
2.1			1
2.2			1
3			1
3.1	,		2
3.2	•		2
3.3	•		3
3.4	,		4
3.5	,		4
4	,		
5			
5.1			
5.2	•••		•
5.3	••••		
5.4			
5.4 5.5			
	••••		
5.6 5.7			
5.8		45000	
6		/ 15026	
6.1	•••		
6.2			
6.3		/ 15026	
6.4			•
7	/ 15026		
7.1			
7.2			10
7.3			11
7.4			11
8	/ 15026		12
8.1			12
8.2			12
9	/ 15026		13
9.1			13
9.2			14
10			14
	()	
			16

```
( )
)
  1.
             2.
                                                           75 %
   15026-1
15026-1:2010.
   15026
 1.
 2.
 3.
4.
                                          15026
                  Std 1228—1994
                                   15026.
         15026-1
                              15026-4.
```

IV

1

Systems and software engineering. Systems and software assurance. Part 1 .Concepts and vocabulary

— 2017*—*06*—*01

1

,

() « » « ».

/ 15026 , .

2

2.1

, . / 15026

, / 12207 / 15288 -/ 25000. / 15026

.

2.2

/ 15026, : ,

.

3

, / 15026.

```
15026-1-2016
                                     15026
   3.1
   3.1.1
                                        (assurance):OcHoeaHne
   3.1.2
                                   (!1):
),
                                                                                      );
   3.1.3
                                                    (assurance
                                                                    ):
);
   3.1.4
                                                     |||| ):
                 25010 (99]
                                                                               [69]),
                                                                        , [64]
                                            60050-191 [631
   [ 60300-1:2003]
   3.2
   3.2.1
                    (process):
             15288:2008
                                    12207:2008]
   3.2.2
                                    (process view):OnncaHne
             15288:2008, D.3]
   3.2.3
                 (product):Pe3ynbTaT
```

```
2
                      9000:20051
         15288:2008
3.2.4 (system):KoM6kiHauMH
2
         15288:2008)
3.2.5
            ( 1
                            1):
                                                         ).
              29148:2011]
3.2.6
                         (system 1
                                      ):
         15288:2008]
3.3
3.3.1
                           (integrity 1
                        15026:1998.
3.3.2
                                      (integrity level requirements):
             15026:1998 (
                             3.3.1 3.3.2)
        1012:2004
3
```

```
15026-1-2016
3.4
3.4.1
                      (consequence):3<ixt>eKT (
                                                                                        ),
3.4.2
                                    (adverse
                                                           ):
3.4.3
                                                             (desirable (or positive) consequence):rioc-
3.4.4
              (error):
               (fault):
                                                                                                        )
3.4.5
3.4.6
                    ):
)
3.4.7
                   ( 1
                8
3.4.8
              ((
                  ):
3.4.9
                                 (systematicfailure):OTKa3,
               (8):
3.4.10
1
2
                                                                                   51.
3
           16085)
(
3.5
3.5.1
                      (organization):rpynna
2
                                                                                            ),
           15288:2008]
[ /
3.5.2
                                     (approval authority):4enoeeK (
),
2
```

```
15026-1—2016
3.5.3
                                        (design authority):4enoeeK
3.5.4
                                                         (integrity assurance
                                                                                       ):
                                              15026:1998,
4
            5
                                                                                              6
                                                                                              15026-2,
    15026-3
                          15026-4.
                                               7, 8
                                                                                     15026-4
                                            15026-2.
                                                                15026-3
5
5.1
                                                                                     15026.
5.2
             15026
                                                                                  ; 2)
                        , 1) 2).
              ),
```

```
/ 15026-1—2016
                                        , ) ,
                        ).
    5.3
    5.4
                                15288
                                                12207
                                                               15026
                                                               / 15026,
                   15026
    5.5
                                                                            15026.
( . 5.8)
                                                        25010
                                        9126-1,
                          / 18529
                                       / 25238.
       2382-14,
                  9241,
                          25010
                                                             25010
                                                                              [25], [64],
```

[122], [157] [40].

```
15026-1—2016
     5.5.1
                   »);
           1).
                                   ),
                                                       [135],
     5.6
                  15026
                                  15026
     5.7
                                                                                     [2], ,
                                                                                                  , [2],
[71] [14,
                 18, . 475—524]).
```

```
15026-1—2016
     5.8
[57], (54].
                                                                     »[150]<sup>1</sup>
                                                                            14620 [79],
                                                                                              19706 [81]
          25238 [121].
                                  16085 [91]
                                                   31000.
     6
                                                                      15026
     6.1
                15026
                                                15026
     6.2
                                    15026
                                                           15026
                          15026-4
                                15026-3
                                                                                                15026:1998,
                      15026-3
                                                                            15026-3
                                                                                                    15026-3
          8
```

```
/ 15026
 6.3
/ 15026
- / 15026-1 «
  / 15026-2 «
  / 15026-3 «
                   / 15026:1996);
   / 15026-4 «
   / 15026-2, / 15026-3
                          / 15026-4
   15026-4
   .
/ 15026-2
   15026-3
       15026-4
6.4
                15026
                                             15026-3
3 «
                      15026.
/ 15026
           / 15026.
```

```
/ 15026-1—2016
     7
                  / 15026
     7.1
                 15026-2
                RAM (
                                              »; (139], [142], [143], [146], [154], [155], [168]. [74], [22], [23], [24].
RAM
        [164]
    / 15026-2,
                                                15026.
(139, .5].
     1)
2)
  ).
                                                                                   25000,
                                               v.3.1
                                                               2» [30].
     7.2
                                    8
```

```
/ 15026-1—2016
a)
b)
c)
7.3
               ,
( . [139,
                             3,9.1)).
                                                                                           [150]
7.4
                                                              27
                          (ISMS)
                                                               , FIPS 140
     27002 «
                        / 27001 (
```

[139], [142]. [143], [22] [23].

11

BS 7799-2:2002).

```
15026-1—2016
                                                         )
                                                       )
                                                                                        (ISC)
                 SANS.
                    15026
8
8.1
          15026-3
             ( . 6.4).
                                          61508 «
                                                               » [70).
8.2
          15026
               61508 [70]
                                   31010,
                                                    1.0(2009-11-27) «
                                                               300-3-9
```

```
/ 15026-1—2016
                                              » (hazard)n « » (harm)
                               » (dangerous condition) «
                                                                           » (adverse
                                                       60300 «
consequence)
[64].
                                       , 014620 [79] —
 0 1 3849(78] —
                                                                          . 019706
                                                                      27005[1 ] —
                      / 25238[121] —
[81] —
                             , ŪK
                                       760760 [24] —
  .
/ 16085(91]
                    31000.
    9 / 15026
    9.1
            15026-4 «
             8
                                          15288 «
                           15288
                                             12207 «
             15288
                           12207
          12207
                                                                  12207
                          15288,
            24748 «
                                            24748
         24748-1
        15288
                                     12207.
             15026-4
                         15026-4
        15288
                         12207.
                        / 15288
                                              12207
                    16085
                                                              15939
             29148 «
             15289
            16326
```

```
15026-1—2016
          15026
9.2
                                                            [145].«
                                         ( .[140)
                                                                       ]).
                                                     [22,
                                                                                      ),
10
                                                                                   15026
                                                                   15026.
     15026,
```

/

15026.

/ 15026-1—2016

()

.1

15026-4:2012	IDT	/ 15026-4—2016 «
		. 4. »
- : 		-

- [1] Abran ., & Moore J.W. (Executive editors); Pierre Bourque, Robert Dupuis, Leonard Tripp (Editors). Guide to the Software Engineering Body of Knowledge. 2004 Edition. Los Alamitos. California; IEEE Computer Society. Feb. 16.2004. Available at http://www.swebok.org
- [2] Adamski A., & Westrum R. Requisite imagination: The fine art of anticipating what might go wrong. In: (55), pp. 193—220,2003
- [3] Adelard. The Adelard Safety Case Development Manual. Available at http://www.adelard.com/web/hnav/resources/ascad
- [4] Alexander I *Systems Engineering Isn't Just Software.* 2001. Available at http://easyweb.easynet.co.uk/-iany/consultancy/systems_engineering/se_isnljust_sw.htm.
- [5] Allen J.H., Barum S.. Ellison R.J.. Megraw G.. Mead N.R. Software Security Engineering: A Guide for Project Managers. Addison-Wesley. 2008
- [6] 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. U.S. Nuclear Regulatory Commission: Office of Inspection and Enforcement, 1987
- [7] Anderson J.P. Computer Security Technology Planning Study Volume I, ESDTR-73-51, Vol. I, Electronic Systems Division. Air Force Systems Command. Hanscom Field. Bedford. MA 01730, Oct 1972.
- [8] Anderson R.J. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley and Sons. Second Edition. 2008
- [9] 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
- [10] Armstrong J.M., & Paynter S.P. *The Deconstruction of Safety Arguments through Adversarial Counter-argument.*School of Computing Science. Newcastle University CS-TR-832.2004
- [11] Atchison 8., Lindsay P., Tombs D. A Case Study in Software Safety Assurance Using Formal Methods. Technical Report No. 99—31. Sept. 1999
- [12] ATSIN Number 17 Issued 9. Lapsesand Mistakes. Air Traffic Services Information Notice, Safety Regulation Group, ATS Standards Department. UK Civil Aviation Authority. August 2002
- [13] Bahill A.T., & Gissing B. Re-evaluating Systems Engineering Concepts Using Systems Thinking. *IEEE Trans. Syst. Man Cybem. C.* 1998 November. 28 (4) pp. 516—527
- [14] BergC.J. High-Assurance Design: Architecting SecureandReliable Enterprise Applications. Addison Wesley,2006
- [15] Bernstein Lawrence. & Yuhas . M. Trustworthy Systems through Quantitative Software Engineering. Wiley-IEEE Computer Society Press, 2005. About reliability not security
- [16] Bishop M..& Engle S. *The Software AssuranceCBKandUniversity Curricula.* Proceedings of the 10th Colloquium for Information Systems Security Education, 2006
- [17] Bishop M. Computer Security: Art and Practice. Addison-Wesley, 2003
- [18] Bishop P., & Bloomfield R. *A Methodology for Safety Case Development.* Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-critical Systems Symposium, Birmingham. 1998
- [19] Bishop P., & Bloomfield R. The SHIP Safety Case Approach. SafeComp95. Belgirate. Italy. Oct 1995
- [20] Buehner M.J.. & Cheng P.W. Causal Learning. In: *The Cambridge Handbook of Thinking and Reasoning,* (Morrison R.. & Holyoak K.J. eds.). Cambridge University Press. 2005, pp. 143—68.
- [21] Cannon J.C. Privacy. Addison Wesley. 2005
- [22] CAP 670 Air Traffic Services Safely Requirements. UK Civil Aviation Authority Safety Regulation Group. 2012
- [23] CAP 730 Safety Management Systems for Air Traffic Management. A Guide to Implementation. UK Civil Aviation Authority Safety Regulation Group, 12 September 2002
- [24] CAP 760 Guidance on the Conduct of Hazard Identification, Risk Assessmentand the Production of Safety Cases For Aerodrome Operators and Air Traffic Service Providers. 10 December 2010
- [25] Chung L. et al. Non-Functional Requirements in Software Engineering. Kluwer. 1999
- [26] Clark D.D., & Wilson D.R. *A Comparison of Commercial and Military Computer Security Policies*, Proc, of the 1987 IEEE Symposium on Security and Privacy. IEEE. pp. 184—196.1987
- [27] CNSS. National Information Assurance Glossary, CNSS Instruction No. 4009, 26 April 2010. Available at http://www.cnss.gov/full-index.html
- [28] Committee on Information Systems Trustworthiness. *Trust in Cyberspace, Computer Science and Telecommunications Board.* National Research Council. 1999

- (29] Committee on National Security Systems (CNSS) Instruction 4009; National Information Assurance (IA) Glossary. Revised May 2003. Available at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
- (30] Common Criteria Recognition Arrangement (CCRA). Common Criteria v 3.1 Revision 2. NIAP September 2007. Available at http://www.commoncriteriaportal.org
- (31] Common Weaknesses Enumeration. MITRE. 2012. Available at http://cwe. mitre.org
- (32] Cooke N.J., Gorman J.C., Winner J. L. Team Cogitation. In:(43), pp. 239—268
- (33] Courtois P.-J. Justifying the Dependability of Computer-based Systems: With Applications in Nuclear Engineering. Springer, 2008
- (34] Cranor L., & Garfinkel S. Security and Usability: Designing Secure Systems that People Can Use. O'Reilly, 2005
- (35] Dayton-Johnson. Jeff. Natural disasters and adaptive capacity. OECD Development Centre Research programme on: Market Access, Capacity Building and Competitiveness. Working Paper No. 237 DEV/DOC(2004)06, August 2004
- (36] 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 http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.
- (37] Department of Defense Strategic Defense Initiative Organization. Trusted Software Development Methodology, SDI-S-SD-91-000007, vol. 1.17 June 1992
- (38] Department of Homeland Security National Cyber Security Division's "Build Security In' (BSI) web site, 2012, http://buildsecurityin.us-cert.gov
- (39] Dependability Research Group. Safety Cases. University of Virginia, Available at: http://dependability.cs.virginia.edu/info/Safety_Cases
- (40] Despotou G.. & Kelly T. Extending the Safety Case Concept to Address Dependability. Proceedings of the 22nd International System Safety Conference. 2004
- (41] Dowd M.. McDonald J.. Schuh J. *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*. Addison-Wesley, 2006
- (42] Dunbar K.. & Fugelsang J. Scientific Thinking and Reasoning. In: (59). pp.705—727
- (43] Durso F.T., Nickerson R.S., Dumais S.T., Lewandowsky S., Perfect T.J. eds. *Handbook of Applied Cognition* 2nd edition. Wiley, 2007
- (44] Ellsworth P.C. Legal Reasoning. In: (59). p. 685—704
- (45] Ericsson K.A.. Charness N.. Feltovich P.J., Hoffman R.R. eds. *The Cambridge Handbook of Expertise and Expert Performance*. Cambridge University Press. 2006
- (46] Fenton N.. Littlewood B., Neil M., Strigini L., Sutcliffe A., Wright D. Assessing dependability of safety critical systems using diverse evidence. *IEEProc. Softw.* 1998 145(1)pp. 35—39
- (47] Gasser M. Building a Secure Computer System. Van Nostrand Reinhold. 1988. Available at http://deke.ruc.edu.cn/wshi/readings/cs02.pdf
- (48] Gray J.W. *Probabilistic Interference*. Proceedings of the IEEE Symposium on Research in Security and Privacy. IEEE, pp.170—179,1990
- (49] Greenwell W.. Strunk E.. Knight J. *Failure Analysis and the Safety-Case Lifecycle*. IFIP Working Conference on Human Error, Safety and System Development (HESSD) Toulouse, France. Aug 2004
- (50] 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
- (51] Hall A.. & Chapman R. Correctness by Construction: Developing a Commercial Secure System. *IEEE* Softw.2002 Jan/Feb, 19(1)pp. 18—25
- (52] Herrmann D.S. Software Safety and Reliability. IEEE Computer Society Press, 1999
- (53] Hoglund G.. & McGraw G. Exploiting Software: How to break code. Addison-Wesley, 2004
- (54] HollnagelE., Woods D.D., Leveson N. eds. Resilience Engineering: Concepts and Precepts. Ashgale PubCo, 2006
- (55] Hollnagel E. ed. Handbook of cognitive task design. Lawrence Erlbaum Associates. 2003
- (56] Hollnagel E. Human Error: Trick or Treat? In: (43], pp.219—238
- (57] Hollnagel E. Barriers and Accident Prevention. Ashgate, 2004
- (58] Hollnagel E. Human Factors: From Liability to Asset. Presentation, 2007. Available at www.vtt. fi/liitetiedostot/muut/Hollnagel.pdf
- (59] Holyoak K.J., & Morrison R.G. eds. *The Cambridge Handbook of Thinking and Reasoning.* Cambridge University Press. 2005

- [60] Howard ., & LeBlanc D.C. Writing Secure Code. Microsoft Press, Second Edition, 2002
- [61] Howard .» & Lipner S. The Security Development Lifecycle. Microsoft Press, 2006
- [62] Howell C. Assurance Cases for Security Workshop (follow-on workshop of the 2004 Symposium on Dependable Systems and Networks), June, 2005
- [63] I EC 60050-191, International Electrotechnical Vocabulary, Chapter 191: Dependability and Quality of Service
- [64] IEC 60300 Dependability management [several parts)
- [65] IEC 60300-3-15 ed 1.0 (2009-06) Dependability management Part 3-15 Application guide Engineering of system dependability
- [66] IEC 60300-3-2 ed 2.0(2004-11), Dependability management Part 3-2: Application guide Collection of dependability data from the field
- [67] IEC 60812 ed 2.0 (2006-01), Analysis techniques for system reliability Procedure for failure mode and effects analysis (FMEA)
- [68] IEC 61025ed 2.0 (2006-12), Fault tree analysis (FTA)
- [69] IEC 61078 ed 2.0 (2006-01), Analysis techniques for dependability Reliability block diagram and Boolean methods
- [70] \text{\text{\text{EC61503ed2.G}, Functional safety of electrical/electronic/programmable electronic safety-related systems[several parts]}
- [71] IEC 61508-7 ed 2.0 (2010-04), Functional safety of electrical/electronic/programmable electronic safety-related systems Part 7: Overview of techniques and measures
- [72] IEC 61511 ed 1.0. Functional safety Safety instrumented systems for the process industry sector [several parts]
- [73] [IEC] 61882 ed 1.0 (2001 -05). Hazard and operability studies (HAZOP studies) Application guide
- [74] IEC CD 62741 ed 1.0, Reliability of systems, equipment, and components. Guide to the demonstration of dependability requirements. The dependability case
- [75] Std IEEE 1228-1994, IEEE Standard for Software Safety Plans
- [76] International Council on Systems Engineering INCOSE. Guide to Systems Engineering Body of Knowledge (G2SEBoK). Available at http://g2sebok.incose.org/
- 77] ISO 12100:2010. Safety of machinery General principles for design Risk assessment and risk reduction
- [78] IS013849, Safety of machinery Safety-related parts of control systems [three parts]
- [79] IS014620, Space systems Safety requirements [three parts]
- [80] ISO 14625:2007, Space systems—Ground support equipment for use at launch, landing or retrieval sites General requirements
- [81] IS019706:2011, Guidelines for assessing the fire threat to people
- [82] ISO 20282, Ease of operation of everyday products [four parts]
- [83] ISO 2394:1998, General principles on reliability for structures
- [84] ISO 28003:2007, Security management systems for the supply chain Requirements for bodies providing audit and certification of supply chain security management systems
- [85] ISO 9241-400:2007, Ergonomics of human system interaction Part 400: Principles and requirements for physical input devices
- [86] ISO/IEC 12207:2008, Systems and software engineering Software life cycle processes
- [87] ISO/IEC 15288:2008, Systems and software engineering System life cycle processes
- [88] ISO/IEC 15408, Information technology— Security techniques Evaluation criteria for IT security [three parts]
- [89] ISO/IEC TR15443. Information technology Security techniques Security assurance framework [two parts]
- [90] ISO/IEC 15939:2007, Systems and software engineering Measurement process
- [91] ISO/IEC 16085:2006, Systems and software engineering Life cycle processes Risk Management
- [92] ISO/IEC/IEEE 16326:2009, Systems and software engineering Life cycle management Project management
- [93] ISO/IEC 18014, Information technology— Security techniques— Time-stamping services [three parts]
- [94] ISO/IEC 18028, Information technology Security techniques IT network security [many parts]
- [95] ISO/IEC 19770, Information technology— Software Asset Management [two parts]
- [96] ISO/IEC 21827:2008, Information technology—Security techniques Systems Security Engineering Capability Maturity Model® (SSE-CMM®)
- [97] ISO/IEC 2382-14:1997, Information technology— Vocabulary Part 14: Reliability, maintainability and availability

- (98] ISO/IEC 25000:2005, Software Engineering Software product Quality Requirements and Evaluation (SQuaRE) Guide to SQuaRE
- (99] ISO/IEC 25010:2011, Systems and software engineering Systems and software product Quality Requirements and Evaluation (SQuaRE) System and software quality models
- (100] ISO/IEC 25012:2008, Software engineering Software product Quality Requirements and Evaluation (SQuaRE) Data quality model
- (101] \SOIIEC25Q20:2Q07. Softwareengineering —Softwareproduct QualityRequirementsandEvaluation(SQuaRE)— Measurement reference model and guide
- (102] ISO/IEC 25030:2007, Software engineering Software product Quality Requirements and Evaluation (SQuaRE) Quality requirements
- (103] ISO/IEC 25040:2011, Systems and software engineering Systems and software Quality Requirements and Evaluation (SQuaRE) Evaluation process
- (104] ISO/IEC 25051:2006, Software engineering Software product Quality Requirements and Evaluation (SQuaRE) Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing
- (105] ISO/IEC 26702:2007, Systems engineering Application and management of the systems engineering process
- (106] ISO/IEC 27000:2012, Information technology—Security techniques Information security management systems Overview and vocabulary
- (107] ISO/IEC 27001:2013, Information technology—Security techniques Information security management systems Requirements
- (108] ISO/IEC 27002:2013, Information technology Security techniques Code of practice for information security controls
- (109] ISO/IEC 27004:2009, Information technology Security techniques Information security management Measurement
- (110] ISO/IEC 27005:2011, Information technology Security techniques Information security risk management
- (111] ISO/IEC 27006:2011, Information technology Security techniques Requirements for bodies providing audit and certification of information security management systems
- (112] ISO/IEC 27011:2008, Information technology—Security techniques Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- (113] ISO/IEC/IEEE 42010:2011, Systems and software engineering Architecture Description
- (114] ISO/IEC 90003:2004, Software engineering Guidelines for the application of ISO 9001:2000 to computer software
- (115] ISO/IEC TR 15446:2009, Information technology— Security techniques Guide for the production of Protection Profiles and Security Targets
- (116] ISO/IEC TR 19791:2010, Information technology Security techniques Security assessment of operational systems
- (117] ISO/IEC TR 24748-1:2010. Systems and software engineering Life cycle management Part 1: Guide for life cycle management
- (118] ISO/TR 16982:2002, Ergonomics of human-system interaction Usability methods supporting human-centred design
- (119] ISO/TR 18529:2000, Ergonomics Ergonomics of human-system interaction Human-centred lifecycle process descriptions
- (120] ISO/TR 27809:2007, Health informatics Measures for ensuring patient safety of health software
- (121] ISO/TS 25238:2007, Health informatics Classification of safety risks from health software
- (122] Kazman R.. Asundi J., Klein M. *Making Architecture Design Decisions: An Economic Approach, SEI-2002-TR-035.*Software Engineering Institute. Carnegie Mellon University, 2002
- (123] Kazman R., Klein M., Clements P. ATAM: Method for Architecture Evaluating the Quality Attributes of a Software Architecture. Technical Report CMU/SEI-200-TR004. Software Engineering Institute. Carnegie Mellon University, 2000
- (124] Hetty T. Arguing Safety— A Systematic Approach to Managing Safety Cases. DoctorialThesis University of York: Department of Computer Science. Sept 1998
- (125] Hetty 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
- (126] 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

- [127] Ladkin . The Pre-Implementation Safety Case for RVSM in European Airspace is Flawed. 29 Aug 2002. Available al http://www.rvs.uni-bielefeld.de/publications/Reports/SCflawed-pa per.html
- [128] Landwehr C. Computer Security. IJIS. 2001,1 pp. 3—13
- [129] Lautieri S., Cooper D., Jackson D. SafSec: Commonalities Between Safety and Security Assurance. Proceedings of the Thirteenth Safety Critical Systems Symposium Southampton, 2005
- [130] LeBoeuf R.A., & Shafir E.B. Decision Making. In: [59], pp.243—266
- [131] Leveson N. A Systems-Theorelic Approach to Safety in Software-Intensive Systems. IEEE Trans. Dependable Sec. Comput. 2004,1 (1) pp. 66—86
- [132] Lipner S.. & Howard M. *The Trustworthy Computing Security Development Lifecycle*, Microsoft. 2005. Available at http://msdn.microsoft.com/en-us/library/ms995349.aspx
- [133] Maguire R. Safety Cases abd Safety Reports: Meaning. Motivation and Management. Ashgate. 2006
- [134] McDermid J. Software Safety: Where's the Evidence? 6th Australian Workshop on Industrial Experience with Safety Critical Systems and Software (SCS'01), Brisbane. 2001
- [135] McGraw G. Software Security: Building Security In. Addison Wesley. 2006
- [136] McLean J. Security Models. In: Encyclopedia of Software Engineering. (Marciniak J. ed.). Wiley. 1994
- [137] Meier J.D.. Mackman A., Vasireddy S.. Dunner M., Escamilla R.. Murukan A. *Improving Web Application Security:*Threats and Countermeasures, Microsoft. 2004. Available at:

 http://download.microsoft.eom/download/d/8/c/d8c02f31-64af-438ca9f4-e31acb8e3333/Threats_Countermeasur

 es.pdf
- [138] Merkow M.S., & Breithaupt J. Computer Security Assurance Using the Common Criteria. Thompson Delamr Learning, 2005
- [139] Ministry of Defence. Defence Standard 00-42 Issue 2, Reliability and Maintainability (R&M) Assurance Guidance. Part 3. R&M Case. 6 June 2003
- [140] Ministry Of Defence. Defence Standard 00-55 (PART lyissue 2. Requirements for Safety Related Software in Defence Equipment Part 1: Requirements. 21 August 1997
- [141] Ministry of Defence. Defence Standard 00-55 (PART 2)/Issue 2. Requirements for Safety Related Software in Defence Equipment Part 2: Guidance. 21 August 1997
- [142] Ministry of Defence. Interim Defence Standard 00-56. Safely Management Requirements for Defence Systems Part 1: Requirements, 17 December 2004
- [143] Ministry of Defence. Interim Defence Standard 00-56, Safely Management Requirements for Defence Systems Part 2: Guidance on Establishing a Means of Complying with Part 1,17 December 2004
- [144] Moore A., Klinker E., Mihelcic D. Howto Construct Formal Arguments that Persuade Certifiers. In: *Industrial Strength Formal Methods in Practice*. Academic Press. 1999
- [145] National Aeronautics and Space Administration (NASA) Software Assurance Guidebook. September 1989 (NASA-GB-A201). Available at http://www.hq.nasa.gov/office/codeq/doctree/ nasa_gb_a201 .pdf
- [146] National Offshore Petroleum Safety Authority. Safety case. [Online Documents [cited on: 20 Jun 2012] Available at http://www.nopsema.gov.au/safety/safety-case/
- [147] National Research Council (NRC) Computer Science and Telecommunications Board. (CSTB). Cybersecurity Today and Tomorrow: Pay Now or Pay Later. National Academies Press, 2002. Available al http://www.nap.edu/topics.php? topic=320&start=10
- [148] National Security Agency, The Information Systems Security Engineering Process (IATF) v3.1.2002
- [149] Naval Research Laboratory. *Handbook for the Computer Security Certification of Trusted Systems.* US Naval Research Laboratory. 1995
- [150] NDIA System Assurance Committee. Engineering for System Assurance. National Defense Industrial Association, USA, 2008
- [151] NIST. Federal Information Processing Standards Publication (FIPS PUB) 200: Minimum Security Requirements for Federal Information and Information Systems. March 2006. Available at http://csrc.nist.gov/publicalions/fips/fips200/FIPS-200-final-march.pdf
- [152] NIST. NIST Special Publication 800-27, Rev A: Engineering Principles for Information Technology Security (A Baseline for Achieving Security). Revision A, June 2004. Available at http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf
- [153] NIST. NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security, December 2001. Available at http://csrc.nist.gov/publications/ nistpubs/800-33/sp800-33.pdf

- [154] Process Framework O.P.E.N. Safety Cases. (Online Document cited on: 20 Jun 2012] Available at: http://www.opfro.org/index.html? Components/WorkProducts/SafetySet/SafetySet. html-Contents
- [155] OPSI. The Offshore Installations (Safely Case) Regulations 2005. [Online Document cited on: 20 June 2012]. Available at http://www.opsi.gov.uk/si/si2005/20053117.htm
- [156] Park J.. Montrose B.. Froscher J. Tools for Information Security Assurance Arguments. DARPA Information Survivability Conference & Exposition II. 2001. DISCEX'01. Proceedings, 2001
- [157] Petroski H. Design Paradigms. Cambridge University Press. 1994
- [158] Prasad D. Dependable Systems Integration using Measurement Theory and Decision Analysis, PhD Thesis, Department of Computer Science. University of York. UK. 1998
- [159] psm Safety & Security TWO. Security Measurement. Nov. 2004
- [160] Pullum L.L. Software Fault Tolerance. Artech House, 2001
- (161] Randell B.. & Koutny M. Failures: Their Definition, Modelling and Analysis. School of Computing Science. Newcastle University CS-TR NO 994. Dec. 2006 Randell 8. & Rushby J.M. Distributed Secure Systems: Then and Now. CS-TR No 1052 School of Computing Science, Newcastle University, Oct. 2007
- [162] RechtinE. Systems Architecting of Organizations: Why Eagles Can't Swim. CRC Press, Boca Raton. FL. 2000
- [163] Redwine S.T. Jr. ed. Software Assurance: A Guide to the Common Body of Knowledge to Produce. Acquire, and Sustain Secure Software Version 1.1. US Department of Homeland Security, September 2006
- [164] 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
- [165] Redwine S.T. Jr.. & Davis N. eds. Processes for Producing Secure Software: Towards Secure Software. Vols. I and II. Washington, D.C.: National Cyber Security Partnership, 2004. Available at http://www.cigital.com/papers/download/secure_software_process.pdf
- [166] Ross K.G.. Shafer J. L., Klein G. Professional Judgements and Naturalistic Decision Making'. In: [45], pp. 403—420
- [167] Ross R. et al. Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53, Aug 2009. Available at http://csrc.nist.gov/publications/nistpubs/80053-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
- [168] SAE JA1000, Reliability Program Standard, SAE International, June 1998. Available at http://www.sae.org
- [169] SaltzerJ.H.. & Schroeder M.D. Theprotection of information in computer systems. *Proc. IEEE.* 1975,63 (9), pp. 1278—1308. Available at: http://cap-lore.com/CapTheory/ProtInf/
- [170] Seminal Papers History of Computer Security Project, University of California Davis Computer Security Laboratory. Available at: http://seclab.cs. ucdavis.edu/projects/history/seminal.html
- [171] Serene. "Safety argument". (Online Document] [cited on: 13 Feb 2007] Available at: http://www2.dcs.qmul.ac.uk/-norman/SERENE_Help/sereneSafety_argument.htm
- [172] Severson K. Yucca Mountain Safety Case Focus of NWTRB September Meeting. United States Nuclear Waste Technical Review Board. Aug. 2006
- [173] SieckW.R., & Klein G. Decision making. In: [43]. pp. 195—218
- [174] Software and Systems Engineering Vocabulary (sevocab). Availableatwww.computer.org/sevocab
- [175] Sommerville I. Software Engineering. Pearson Education. Eighth Edition. 2006
- [176] Stoneburner G., Hayden C., Feringa A. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A. NIST Special Publication 800-27 Rev A. June 2004
- [177] StoreyN. Safety-Critical Computer Systems. Addison Wesley, 1996
- [178] Strunk E., & Knight J. *The Essential Synthesis of Problem Frames and Assurance Cases.* IWAAPF'06. Shanghai. China. May 2006
- [179] Swiderski F.. & Snyder W. Threat Modeling. Microsoft Press. 2004
- [180] U.S. NRC. "Quality Assurance Case Studies at Construction Projects"
- [181] Vanfleet W.M. et al. MILS: "Architecture for High Assurance Embedded Computing," Crosstalk, August, 2005
- [182] Viega J.. & McGraw G. Building Secure Software: How to Avoid Security Problems the Right Way. Addison Wesley. Reading, MA, 2001
- [183] Walker V.R. Risk Regulation and the 'Faces' of Uncertainty, *Risk: Health. Safety and Environment,* pp. 27—38. Winter 1998
- [184] WareW.H. Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security. The RAND Corporation. Santa Monica. CA (Feb. 1970)

/ 15026-1—2016

- [185] WeaverR. The Safety of Software Constructing and Assuring Arguments. Doctorial Thesis— University of York: Department of Computer Science. 2003
- [186] Weaver R.. Fenn J.. Kelly T. *A Pragmatic Approach to Reasoning about the Assurance of Safety Arguments*. 8lh Australian Workshop on Safety Critical Systems and Software (SCS'03), Canberra. 2003
- [187] Whittaker J.A., & Thompson H.H. How to Break Software Security: Effective Techniques for Security Testing. Pearson Education, 2004
- [188] Williams J., & Schaefer M. Pretty Good Assurance. Proceedings of the New Security Paradigms Workshop. IEEE Computer Society Press. 1995
- [189] Williams J.R., & Jelen G.F. A Framework for Reasoning about Assurance, Document Number ATR 97043, Area Systems. Inc., 23 April 1998
- [190] YatesJ.F.,&Tschirhart M.D. Decision-Making Expertise. In: [45], pp. 421—438
- [191] Yee K.-P. User interaction design for securesystems. Proceedingsof the4th International Conference on Information and Communications Security, Springer-Verlag, LNCS 2513.2002

$006.34 \hbox{:} 004.05 \hbox{:} 004.052 \hbox{:} 006.354$

35.080