

Engineering Trustworthy Secure Systems

RON ROSS
MICHAEL McEVILLEY
MARK WINSTEAD

PRE-RELEASE VERSION
Not For Public Distribution

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-160v1r1-draft>

Draft NIST Special Publication 800-160, Volume 1

Revision 1

Engineering Trustworthy Secure Systems

RON ROSS

*Computer Security Division
Information Technology Laboratory*

MICHAEL McEVILLEY

MARK WINSTEAD

*The MITRE Corporation
McLean, VA*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-160v1r1-draft>

January 2022



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
*James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce
for Standards and Technology & Director, National Institute of Standards and Technology*

AUTHORITY

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of the appropriate federal officials exercising policy authority over such systems. This guideline is consistent with requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, OMB Director, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-160, Vol. 1, Rev. 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-160, Vol. 1, Rev. 1, **207 pages** (January 2022)
CODEN: NSPUE2

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-160v1r1-draft>

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts, practices, and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review draft publications during the public comment periods and provide feedback to NIST. Many NIST publications, other than the ones noted above, are available at <https://csrc.nist.gov/publications>.

Public comment period: January 11, 2022 – February 25, 2022

Submit comments on this publication to: security-engineering@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA) [FOIA96].

40

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

41 The National Institute of Standards and Technology (NIST) Information Technology Laboratory
42 (ITL) promotes the U.S. economy and public welfare by providing technical leadership for the
43 Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference
44 data, proof of concept implementations, and technical analyses to advance the development
45 and productive use of information technology (IT). ITL's responsibilities include the development
46 of management, administrative, technical, and physical standards and guidelines for the cost-
47 effective security of other than national security-related information in federal information
48 systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach
49 efforts in information systems security and privacy and its collaborative activities with industry,
50 government, and academic organizations.

51

ABSTRACT

52 With the continuing frequency, intensity, and adverse consequences of cyber-attacks,
53 disruptions, hazards, and other threats to federal, state, and local governments, as well as
54 private sector organizations, the need for trustworthy secure systems has never been more
55 important to the long-term economic and national security interests of the United States.
56 Engineering-based solutions are essential to managing the complexity, dynamicity, and
57 interconnectedness of today's systems, as exemplified by cyber-physical systems and systems-
58 of-systems. This publication addresses the engineering-driven perspective and actions necessary
59 to develop more defensible and survivable systems, inclusive of the machine, physical, and
60 human components that compose those systems and the capabilities and services delivered by
61 those systems. This publication starts with and builds upon established international standards
62 for systems and software engineering by the International Organization for Standardization
63 (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and
64 Electronics Engineers (IEEE) and infuses systems security engineering methods, practices, and
65 techniques into those systems and software engineering activities. The objective is to address
66 security issues from a stakeholder protection needs, concerns, and requirements perspective
67 and to use established engineering processes to help ensure that such needs, concerns, and
68 requirements are addressed with appropriate fidelity and rigor throughout the system life cycle.

69

KEYWORDS

70 Assurance; developmental engineering; disposal; engineering trades; field engineering;
71 implementation; information security; information security policy; inspection; integration;
72 penetration testing; protection needs; requirements analysis; resilience; review; risk
73 assessment; risk management; risk treatment; security architecture; security authorization;
74 security design; security requirements; specifications; stakeholder; system of systems; system
75 component; system element; system life cycle; systems; systems engineering; systems security
76 engineering; trustworthiness; validation; verification.

77

ACKNOWLEDGMENTS

78 The authors gratefully acknowledge and appreciate the significant contributions from individuals
79 and organizations in the public and private sectors whose constructive comments improved the
80 overall quality, thoroughness, and usefulness of this publication. In particular, we wish to thank
81 Jeff Brewer, Ken Cureton, Jordan Denmark, Rick Dove, Holly Dunlap, Jim Foti, Michael Hankins,
82 Daryl Hild, M. Lee, Tom Llanso, Jimmie McEver, Perri Nejb, Cory Ocker, Daniel Patrick Pereira,
83 Victoria Pillitteri, Greg Ritter, Thom Schoeffling, Theresa Soloway, Gary Stoneburner, Gregory
84 Touhill, Isabel Van Wyk, Adam Williams, Drew Wilson, Carol Woody, William Young, and Michael
85 Zisa. Finally, the authors wish to thank the students participating in the various INCOSE tutorials
86 and MITRE Systems Security Engineering courses whose comments and insights help guide and
87 inform many of the proposed changes in this publication.

88

89

90

HISTORICAL CONTRIBUTIONS

The authors gratefully acknowledge the contributions of Janet Carrier Oren, one of the original coauthors of NIST Special Publication 800-160, Volume 1. The authors also wish to acknowledge the following organizations and individuals for their historic contributions to this publication:

Organizations: National Security Agency; Naval Postgraduate School; Department of Defense Office of Acquisition, Technology, and Logistics; Department of Homeland Security Science and Technology Office, Cyber Security Division; International Council on Systems Engineering, United States Air Force; Air Force Institute of Technology; Northrop Grumman Corporation; The MITRE Corporation; Lockheed Martin Corporation.

Individuals: Beth Abramowitz, Max Allway, Kristen Baldwin, Dawn Beyer, Debora Bodeau, Paul Clark, Keesha Crosby, Judith Dahmann, Kelley Dempsey, Holly Dunlap, Jennifer Fabius, Daniel Faigin, Jeanne Firey, Robin Gandhi, Rich Graubart, Kevin Greene, Richard Hale, Daryl Hild, Kesha Hill, Danny Holtzman, Cynthia Irvine, Brett Johnson, Ken Kepchar, Stephen Khou, Alvi Lim, Logan Mailloux, Dennis Mangsen, Doug Maughn, Rosalie McQuaid, Joseph Merklung, John Miller, Thuy Nguyen, Perri Nejb, Lisa Nordman, Dorian Pappas, Paul Popick, Roger Schell, Thom Schoeffling, Matthew Scholl, Peter Sell, Gary Stoneburner, Glenda Turner, Edward Yakabovicz, and William Young.

Finally, the authors respectfully acknowledge the seminal work in computer security that dates back to the 1960s. The vision, insights, and dedicated efforts of those early pioneers in computer security serve as the philosophical and technical foundation for the security principles, concepts, methods, and practices employed in this publication to address the critically important problem of engineering trustworthy secure systems.

91

NOTES TO REVIEWERS

92 This update to SP 800-160, Volume 1 provided an excellent opportunity to reflect on the past
93 five years of the publication's use by systems engineers and systems security engineers and to
94 apply targeted lessons learned during that timeframe. In particular, we focused on the following
95 strategic objectives which drove the majority of changes to the publication. These included:

- 96 • More strongly positioning Systems Security Engineering (SSE) as a sub-discipline of Systems
97 Engineering (SE)
- 98 • Emphasizing that the responsibility for engineering trustworthy secure systems is not
99 limited to security specialties and that the achievement of security outcomes must properly
100 align with SE outcomes
- 101 • Aligning SSE practices with safety practices and other disciplines that deal with the loss of
102 assets and the consequences of asset loss
- 103 • Focusing on the assurance of the correctness and effectiveness of the system's security
104 capability to achieve authorized and intended behaviors and outcomes and control adverse
105 effects and loss
- 106 • Emphasizing security roles and purpose to avoid inferring that SSE has responsibility for all
107 aspects of security outcomes and prescribing what the SSE role is or should be
- 108 • More closely aligning to international standards

109 Based on the strategic objectives above, the significant revisions and enhancements to NIST's
110 systems security engineering guidance include:

- 111 • A revised systems engineering and systems security engineering fundamentals section
112 ([Chapter Two](#)) with new guidance on organizational assets and asset loss
- 113 • Simplified and streamlined system life cycle processes, structure, and associated security
114 considerations ([Chapter Three](#))
- 115 • A revised section on security policy and requirements (new [Appendix C](#))
- 116 • A revised section on trustworthy secure design concepts for systems and system elements
117 (new [Appendix D](#))
- 118 • Enhanced security design principles presented in two distinct categories of trustworthiness
119 and loss control (new [Appendix E](#))
- 120 • A revised section on trustworthiness and assurance (new [Appendix F](#))
- 121 • Selected modifications to the system life cycle processes ([Chapter Three](#)) to ensure
122 consistency with ISO/IEC/IEEE 15288:202x
- 123 • Transitioning the content from two appendices, Summary of Systems Security Activities and
124 Tasks (formerly Appendix D) and Roles, Responsibilities, and Skills (formerly Appendix E) to
125 the NIST Systems Security Engineering web site

126 NIST is interested in your feedback on the specific changes made to the publication during this
127 update. This can include the organization and structure of the publication, the presentation of

128 the material, its ease of use, and the applicability of the technical content to current or planned
129 systems engineering initiatives.

130 Thank you for taking the time to review the draft publication. Your comments can be sent to
131 security-engineering@nist.gov using the comment template provided on the publication landing
132 page at <https://doi.org/10.6028/NIST.SP.800-160v1r1-draft>.

133 **Ron Ross**
134 *Project Leader,*
135 *Systems Security Engineering Project*

136

CALL FOR PATENT CLAIMS

137 This public review includes a call for information on essential patent claims (claims whose use
138 would be required for compliance with the guidance or requirements in this Information
139 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be
140 directly stated in this ITL Publication or by reference to another publication. This call includes
141 disclosure, where known, of the existence of pending U.S. or foreign patent applications relating
142 to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

143 ITL may require from the patent holder, or a party authorized to make assurances on its behalf,
144 in written or electronic form, either:

- 145 a) assurance in the form of a general disclaimer to the effect that such party does not hold
146 and does not currently intend holding any essential patent claim(s); or
- 147 b) assurance that a license to such essential patent claim(s) will be made available to
148 applicants desiring to utilize the license for the purpose of complying with the guidance
149 or requirements in this ITL draft publication either:
 - 150 i) under reasonable terms and conditions that are demonstrably free of any unfair
151 discrimination; or
 - 152 ii) without compensation and under reasonable terms and conditions that are
153 demonstrably free of any unfair discrimination.

154 Such assurance shall indicate that the patent holder (or third party authorized to make
155 assurances on its behalf) will include in any documents transferring ownership of patents
156 subject to the assurance, provisions sufficient to ensure that the commitments in the assurance
157 are binding on the transferee, and that the transferee will similarly include appropriate
158 provisions in the event of future transfers with the goal of binding each successor-in-interest.
159

160 The assurance shall also indicate that it is intended to be binding on successors-in-interest
161 regardless of whether such provisions are included in the relevant transfer documents.

162 ***Such statements should be addressed to:*** security-engineering@nist.gov.

163

TABLE OF CONTENTS

164 **CHAPTER ONE INTRODUCTION**..... 1

165 1.1 PURPOSE AND APPLICABILITY..... 2

166 1.2 TARGET AUDIENCE..... 4

167 1.3 HOW TO USE THIS PUBLICATION 5

168 1.4 ORGANIZATION OF THIS PUBLICATION..... 5

169 **CHAPTER TWO THE FUNDAMENTALS**..... 8

170 2.1 ENGINEERING FOUNDATIONS 8

171 2.2 SYSTEM CONCEPTS 12

172 2.2.1 Systems and System Structure 12

173 2.2.2 Interfacing, Enabling, and Interoperating Systems..... 14

174 2.3 SYSTEM SECURITY PERSPECTIVE 15

175 2.3.1 The Nature and Character of Systems 15

176 2.3.2 The Concept of Loss..... 16

177 2.3.3 The Concept of Security..... 18

178 2.3.4 The Concept of System Security 19

179 2.3.5 The Concept of Assets 20

180 2.3.6 Reasoning About Asset Loss 22

181 2.3.7 Protection Needs 26

182 2.3.8 System Security Viewpoints..... 29

183 2.4 DEMONSTRATING SYSTEM SECURITY 30

184 2.5 SYSTEMS SECURITY ENGINEERING FRAMEWORK 32

185 2.5.1 The Problem Context..... 34

186 2.5.2 The Solution Context 35

187 2.5.3 The Trustworthiness Context..... 36

188 **CHAPTER THREE SYSTEM LIFE CYCLE PROCESSES** 38

189 3.1 AGREEMENT PROCESSES 42

190 3.1.1 Acquisition 42

191 3.1.2 Supply 44

192 3.2 ORGANIZATIONAL PROJECT-ENABLING PROCESSES..... 46

193 3.2.1 Life Cycle Model Management 46

194 3.2.2 Infrastructure Management 48

195 3.2.3 Portfolio Management 49

196 3.2.4 Human Resource Management 51

197 3.2.5 Quality Management..... 52

198 3.2.6 Knowledge Management..... 53

199 3.3 TECHNICAL MANAGEMENT PROCESSES 55

200 3.3.1 Project Planning..... 55

201 3.3.2 Project Assessment and Control..... 57

202 3.3.3 Decision Management..... 60

203 3.3.4 Risk Management 61

204 3.3.5 Configuration Management 63

205 3.3.6 Information Management 66

206 3.3.7 Measurement 67

207 3.3.8 Quality Assurance 69

208 3.4 TECHNICAL PROCESSES..... 71

209 3.4.1 Business or Mission Analysis..... 71

210 3.4.2 Stakeholder Needs and Requirements Definition 73

211 3.4.3 System Requirements Definition 76

212 3.4.4 System Architecture Definition..... 78

213 3.4.5 Design Definition 81

214 3.4.6 System Analysis 83

215 3.4.7 Implementation..... 85

216	3.4.8 Integration	87
217	3.4.9 Verification	89
218	3.4.10 Transition	91
219	3.4.11 Validation	93
220	3.4.12 Operation	96
221	3.4.13 Maintenance	99
222	3.4.14 Disposal	101
223	REFERENCES	105
224	APPENDIX A GLOSSARY	119
225	APPENDIX B ACRONYMS	137
226	APPENDIX C SECURITY POLICY AND REQUIREMENTS	138
227	C.1 SECURITY POLICY	138
228	C.1.1 Rules	138
229	C.1.2 Scope of Control	138
230	C.2 REQUIREMENTS	139
231	C.2.1 Stakeholder Security Requirements	140
232	C.2.2 System Security Requirements	141
233	C.3 SYSTEM STATES—SECURE AND NON-SECURE	142
234	C.4 DISTINGUISHING REQUIREMENTS, POLICY, AND MECHANISMS	143
235	APPENDIX D TRUSTWORTHY SECURE DESIGN	145
236	D.1 DESIGN APPROACH FOR TRUSTWORTHY SYSTEMS	145
237	D.2 DESIGN FOR BEHAVIORS AND OUTCOMES	146
238	D.3 SECURITY DESIGN ORDER OF PRECEDENCE	148
239	D.4 FUNCTIONAL DESIGN CONSIDERATIONS	151
240	D.4.1 Roles for Security-Relevant Control	151
241	D.4.2 Essential Design Criteria for Mechanisms	152
242	D.4.3 Security Function Failure Analysis	153
243	D.4.4 Trade Space Considerations	154
244	APPENDIX E PRINCIPLES FOR TRUSTWORTHY SECURE DESIGN	156
245	E.1 TRUSTWORTHINESS DESIGN PRINCIPLES	157
246	E.1.1 Clear Abstractions	158
247	E.1.2 Commensurate Rigor	159
248	E.1.3 Commensurate Trustworthiness	159
249	E.1.4 Compositional Trustworthiness	160
250	E.1.5 Hierarchical Protection	160
251	E.1.6 Minimized Trusted Elements	160
252	E.1.7 Reduced Complexity	161
253	E.1.8 Self-Reliant Trustworthiness	162
254	E.1.9 Structured Decomposition and Composition	163
255	E.1.10 Substantiated Trustworthiness	163
256	E.1.11 Trustworthy System Control	164
257	E.2 LOSS CONTROL DESIGN PRINCIPLES	166
258	E.2.1 Anomaly Detection	166
259	E.2.2 Commensurate Protection	168
260	E.2.3 Commensurate Response	169
261	E.2.4 Continuous Protection	169
262	E.2.5 Defense In Depth	170
263	E.2.6 Distributed Privilege	171
264	E.2.7 Diversity (Dynamicity)	172
265	E.2.8 Domain Separation	173
266	E.2.9 Least Functionality	174
267	E.2.10 Least Persistence	174
268	E.2.11 Least Privilege	175
269	E.2.12 Least Sharing	175

270	E.2.13 Loss Margins	176
271	E.2.14 Mediated Access.....	177
272	E.2.15 Minimize Detectability.....	178
273	E.2.16 Protective Defaults	178
274	E.2.17 Protective Failure.....	178
275	E.2.18 Protective Recovery.....	179
276	E.2.19 Redundancy	179
277	APPENDIX F TRUSTWORTHINESS AND ASSURANCE	181
278	F.1 TRUST AND TRUSTWORTHINESS.....	181
279	F.1.1 Roles of Requirements in Trustworthiness	182
280	F.1.2 Design Considerations	182
281	F.2 ASSURANCE	183
282	F.2.1 Security Assurance Claims	184
283	F.2.2 Approaches to Assurance	185
284	F.2.3 Assurance Needs.....	187
285		

DISCLAIMER

This publication is intended to be used in conjunction with and as a supplement to **International Standard ISO/IEC/IEEE 15288, Systems and software engineering — System life cycle processes**. It is strongly recommended that organizations using this publication obtain the standard in order to fully understand the context of the security-related activities and tasks in each of the system life cycle processes. Content from the international standard that is referenced in this publication is used with permission from the Institute of Electrical and Electronics Engineers and is noted as follows: ***Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.***

The reprinted material has been updated to reflect any changes in the international standard.

291

PROLOGUE

292

293

294

295

“Providing satisfactory security controls in a computer system is in itself a system design problem. A combination of hardware, software, communications, physical, personnel and administrative-procedural safeguards is required for comprehensive security. In particular, software safeguards alone are not sufficient.”

296

297

**“Security Controls for Computer Systems,” (The Ware Report), Rand Corporation
Defense Science Board Task Force on Computer Security, February 1970**

298

299

300

“Mission assurance requires systems that behave with predictability and proportionality.”

General Michael Hayden

Former NSA and CIA Director, Syracuse University, October 2009

301

302

303

304

305

306

307

“In the past, it has been assumed that to show that a system is safe, it is sufficient to provide assurance that the process for identifying the hazards has been as comprehensive as possible, and that each identified hazard has one or more associated controls. While historically this approach has been used reasonably effectively to ensure that known risks are controlled, it has become increasingly apparent that evolution to a more holistic approach is needed as systems become more complex and the cost of designing, building, and operating them become more of an issue.”

Preface, NASA System Safety Handbook, Volume 1, November 2011

308

309

310

“This whole economic boom in cybersecurity seems largely to be a consequence of poor engineering.”

Carl Landwehr

Communications of the ACM, February 2015

311

312

313

314

“Cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace.”

315

316

317

“Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life.”

318

Executive Order (EO) on Improving the Nation’s Cybersecurity, May 2021

319

320

321

322

323

“[Systems] security engineering must be fundamental to systems engineering, not just a specialty discipline. Security concepts must be fundamental to [an] engineering education, and security proficiency must be fundamental in development teams. Security fundamentals must be clearly understood by stakeholders and effectively evaluated in a way that considers broad goals with security functions and outcomes.”

324

Security in the Future of Systems Engineering [FUSE21]

325

FOREWORD

326 On May 12, 2021, the President signed an *Executive Order (EO) on Improving the Nation’s*
327 *Cybersecurity* [[EO 14028](#)]. The Executive Order stated—

328 *“The United States faces persistent and increasingly sophisticated malicious cyber campaigns that*
329 *threaten the public sector, the private sector, and ultimately the American people’s security and*
330 *privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect,*
331 *and respond to these actions and actors.”*

332 The Executive Order further described the holistic nature of the cybersecurity challenges
333 confronting the Nation with computing technology embedded in every type of system from
334 general-purpose computing systems supporting businesses to cyber-physical systems controlling
335 the operations in power plants that provide electricity to the American people. The Federal
336 Government must bring to bear the full scope of its authorities and resources to protect and
337 secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope
338 of protection and security must include systems that process data (information technology [IT])
339 and those that run the vital machinery that ensures our safety (operational technology [OT]).

340 To achieve this overarching objective, we must:

- 341 • Identify stakeholder assets and protection needs and provide protection commensurate
342 with the criticality of those assets, needs, and the consequences of asset loss.
- 343 • Understand the modern threat space (i.e., adversary capabilities and intentions revealed by
344 the targeting actions of those adversaries).
- 345 • Increase understanding of the growing complexity of systems to effectively reason about,
346 manage, and address the uncertainty associated with that complexity.
- 347 • Adopt an engineering-based approach that addresses the principles of trustworthy secure
348 design and apply those principles throughout the system life cycle.

349 Building trustworthy, secure systems cannot occur in a vacuum with isolated stovepipes for
350 cyberspace, software, and information technology. Rather, it requires a holistic approach to
351 protection, broad-based thinking across all assets where loss could occur, and an understanding
352 of adversity, including how adversaries attack and compromise systems. As such, this
353 publication addresses considerations for the engineering-driven actions necessary to develop
354 defensible and survivable systems, including the components that compose and the services
355 that depend on those systems. The publication builds upon a set of international standards for
356 systems and software engineering published by the International Organization for
357 Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of
358 Electrical and Electronics Engineers (IEEE) and infuses systems security engineering techniques,
359 methods, and practices into those systems and software engineering activities. The overall
360 objective is to address security issues from a stakeholder requirements and protection needs
361 perspective and to use established engineering processes to ensure that such requirements and
362 needs are addressed with appropriate fidelity and rigor across the entire life cycle of the system.

363 Engineering trustworthy, secure systems is a significant undertaking that requires a substantial
364 investment in the requirements, architecture, and design of systems, components, applications,
365 and networks. A trustworthy system is a system that provides compelling evidence to support

366 claims that it meets its requirements to deliver the protection and performance needed by
367 stakeholders within their defined tolerance of risk. Introducing a disciplined, structured, and
368 standards-based set of systems security engineering activities and tasks provides an important
369 starting point and forcing function to initiate needed change.

370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386

“Some have a tendency to dismiss ideas that are older than x years, where x seems to be getting smaller and smaller as the pace of technology development continues to increase at an exponential rate. There is a tendency among some to think that cybersecurity is purely a technology problem – that if you just build the right widgets (device or piece of software), the problem will be solved. I call this the 'widget mentality.' Widgets are certainly important, but knowledge and deep understanding are essential. Indeed, developing widgets without an understanding of the nature of the problem and what constitutes a real solution to the problem is ineffective. *[It is important to understand]* ...the form of principles that underlie cybersecurity so that designers can understand what widgets to build, to what requirements they should build them, how they should be deployed and interconnected within cyberspace, and how to operate them when under attack.”

-- O. Sami Saydjari
Engineering Trustworthy Systems [Saydjari18]

387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408

THE POWER OF SCIENCE AND ENGINEERING

When crossing a bridge, we have a reasonable *expectation* that the bridge will not collapse and will get us to our destination without incident. For bridge builders, the focus is on equilibrium, static and dynamic loads, vibrations, and resonance. The science of *physics* combines with civil engineering principles and concepts to produce a product that we deem *trustworthy*, giving us a level of confidence that the bridge is fit-for-purpose.

For system developers, there are also fundamental principles and concepts that can be found in *mathematics, computational science, computer and electrical engineering, systems engineering, and software engineering* that when properly employed, provide the necessary and sufficient trustworthiness to give us that same level of confidence. Trustworthy secure systems cannot be achieved simply by applying best practices in cyber hygiene. Rather, it will take a significant and substantial investment in strengthening the underlying systems and system components by employing transdisciplinary systems engineering efforts guided and informed by well-defined security requirements and secure architectures and designs. Such efforts have been proven over time to produce sound engineering-based solutions to complex and challenging systems security problems. Only under those circumstances can we build systems that are adequately secure and exhibit a level of trustworthiness that is sufficient for the purpose for which the system was built.

HOW TO USE THIS PUBLICATION

This publication is intended to serve as a *reference* and *educational resource* for engineers and engineering specialties, architects, designers, and individuals involved in the development of trustworthy secure systems and system components. There is no expectation that all of the security considerations, system life cycle processes, design principles, or other technical content in this publication will be employed in systems engineering processes. Rather, the material can be applied selectively by organizations, individuals, or engineering teams to improve the security and trustworthiness of systems and system components.

410 CHAPTER ONE

411 INTRODUCTION

412 THE NEED FOR SYSTEMS ENGINEERING-BASED TRUSTWORTHY SECURE SYSTEMS

415 **T**he need for trustworthy secure systems¹ stems from the adverse effects associated with a
414 diverse set of stakeholder needs that are driven by mission, business, and other objectives
415 and concerns. The characteristics of these systems reflect a growth in the geographic size,
416 number, and types of components and technologies² that compose the systems; the complexity
417 and dynamicity in the behaviors and outcomes of the systems; and the increased dependence
418 that results in a range of consequences from major inconvenience to catastrophic loss due to
419 adversity³ within the global operating environment. Today's systems have the dimensions and
420 inherent complexity that require a disciplined and structured engineering approach to achieve
421 any expectation that the complexity can be effectively managed and that the systems can be
422 demonstrated to be trustworthy secure within the practical and feasible limits of human
423 capability and certainty.

424 Managing the complexity of systems and being able to claim that those systems are trustworthy
425 secure means that, first and foremost, there must be a level of confidence in the feasibility,
426 correctness-in-concept, philosophy, and design regarding the ability of a system to produce only
427 the intended behavior and outcomes. That basis provides the foundation to address security
428 concerns with sufficient confidence that the system functions only as intended while subjected
429 to a spectrum of adversity and to realistically bound those expectations with respect to
430 constraints and uncertainty. The failure to address this complexity will continue to leave the
431 Nation susceptible to the consequences of adversity with the potential for causing serious,
432 severe, or even catastrophic consequences.

433 *Security* is freedom from the conditions that can cause a loss of *assets* with unacceptable
434 consequences.⁴ The scope of security must be defined by stakeholders in terms of the assets to
435 which security applies and the consequences against which security is assessed.⁵

¹ A *system* is an arrangement of parts or elements that exhibit a behavior or meaning that the individual constituents do not [INCOSE19]. The elements that compose a system include hardware, software, data, humans, processes, procedures, facilities, materials, and naturally occurring entities [ISO 15288]. Examples of systems include financial systems, manufacturing systems, transportation distribution systems, logistics systems, vehicular systems, mobile devices, Internet of Things (IoT) devices, weapons systems, space systems, environmental control systems, communications systems, cyber-physical systems, and industrial control systems.

² The term *technology* is used in the broadest context in this publication to include computing, communications, and information technologies, as well as any mechanical, hydraulic, pneumatic, or structural components in systems that contain or are enabled by such technologies. This view of technology provides an increased recognition of the digital, computational, and electronic machine-based foundation of modern complex systems and the growing importance of the trustworthiness of that foundation in providing the system's functional capability and explicit interaction with its physical machine and human system elements.

³ The term *adversity* refers to those conditions that can cause a loss of assets (e.g., threats, attacks, vulnerabilities, hazards, disruptions, and exposures).

⁴ The phrasing used in this definition of *security* is intentional. [Anderson20] noted that "now that everything's acquiring connectivity, you can't have safety without security, and these ecosystems are emerging." Reflecting this observation, the security definition was chosen to achieve alignment with a prevailing *safety* definition.

⁵ Adapted from [NASA11].

436 *Systems engineering* provides the foundation for a disciplined and structured approach to
437 building trustworthy secure systems. Trustworthiness⁶ is defined in [Neumann04] as follows:

438 *By trustworthiness, we mean simply worthy of being trusted to fulfill whatever critical requirements*
439 *may be needed for a particular component, subsystem, system, network, application, mission,*
440 *enterprise, or other entity. Trustworthiness requirements might typically involve (for example)*
441 *attributes of security, reliability, performance, and survivability under a wide range of potential*
442 *adversities. Measures of trustworthiness are meaningful only to the extent that the requirements*
443 *are sufficiently complete and well defined, and can be accurately evaluated.*

444 *Systems security engineering* is considered a subdiscipline of systems engineering. It provides
445 considerations for the security-oriented activities and tasks that produce security outcomes as
446 part of every systems engineering process activity with emphasis on the appropriate level of
447 fidelity and rigor needed to achieve assurance and trustworthiness objectives. Systems security
448 engineering provides the needed complementary engineering capability that extends the notion
449 of trustworthiness to deliver trustworthy secure systems. Trustworthy secure systems are less
450 susceptible but not impervious to the effects of modern adversities. Such adversities come in
451 malicious and non-malicious forms and can emanate from a variety of sources including physical
452 and electronic. Adversities can include attacks from determined and capable adversaries, human
453 errors of omission or commission, accidents and incidents, component faults and failures, abuse
454 and misuse, and natural or human-made disasters.

455 **1.1 PURPOSE AND APPLICABILITY**

456 The purpose of this publication is:

- 457 • To provide a basis to formalize a discipline for systems security engineering in terms of its
458 principles, concepts, and activities
- 459 • To foster a common mindset to deliver security for any system, regardless of its purpose,
460 type, scope, size, complexity, or stage of the system life cycle
- 461 • To provide considerations and to demonstrate how systems security engineering principles,
462 concepts, and activities can be effectively applied to systems engineering activities
- 463 • To advance the field of systems security engineering as a discipline that can be applied and
464 studied
- 465 • To serve as a basis for the development of educational and training programs, including the
466 development of individual certifications and other professional assessment criteria

467 The considerations set forth in this publication are applicable to all federal systems other than
468 those systems designated as national security systems as defined in 44 U.S.C., Section 3542.⁷
469 These considerations have been broadly developed from a technical and technical management
470 perspective to complement similar considerations for national security systems and may be

⁶ *Trustworthiness* is not only about demonstrably meeting a set of requirements, but the requirements must also be complete, consistent, and correct. From a security perspective, a trustworthy system is a system that meets a set of well-defined requirements including security requirements.

⁷ [OMB M-19-03] states that increasing the trustworthiness of systems is a significant undertaking that requires a substantial investment in the requirements, architecture, design, and development of systems, system components, applications, and networks. The policy requires federal agencies to implement the systems security engineering principles, concepts, techniques, and system life cycle processes in this publication for all high value assets (HVA).

471 used for such systems with the approval of federal officials exercising policy authority over such
472 systems. State, local, and tribal governments, as well as private sector entities, are encouraged
473 to consider using the material in this publication, as appropriate.

474 The applicability statement is not meant to limit the technical and management application of
475 these considerations. That is, the security design principles, concepts, and techniques described
476 in this publication are part of a *trustworthy secure design* approach as described in [Appendix D](#)
477 and can be applied to any type of system, including:

478 • **New Systems**

479 The engineering effort includes such activities as concept exploration, preliminary or applied
480 research to refine the concepts and/or feasibility of technologies employed in a new system,
481 and an assessment of alternative solutions. This effort is initiated during the [concept](#) and
482 [development](#) stages of the system life cycle.

483 • **Dedicated or Special-Purpose Systems**

484 - *Security-dedicated or security-purposed systems*: The engineering effort delivers a
485 system that satisfies a security-dedicated need or provides a security-oriented purpose
486 and does so as a stand-alone system that may monitor or interact with other systems.
487 Such systems can include surveillance systems, physical protection systems, monitoring
488 systems, and security service provisioning systems.

489 - *High-confidence, dedicated-purpose systems*: The engineering effort delivers a system
490 that satisfies the need for real-time control of vehicles, industrial or utility processes, or
491 weapons, nuclear, and other special-purpose needs. Such systems may include multiple
492 operational states or modes with varying forms of manual, semi-manual, automated, or
493 autonomous modes. These systems have highly deterministic properties, strict timing
494 constraints and functional interlocks, and severe or catastrophic consequences of
495 failure.

496 • **System of Systems**

497 The engineering effort occurs across a set of constituent systems, each system with its own
498 stakeholders, primary purpose, and planned evolution. The composition of the constituent
499 systems into a *system of systems* [[Maier98](#)] produces a capability that would otherwise be
500 difficult or impractical to achieve. This effort can occur across a variety of system of systems
501 from a relatively informal, unplanned system of systems concept and evolution that
502 emerges over time via voluntary participation to a more formal execution with the most
503 formal being a system of systems concept that is directed, structured, and planned, and
504 achieved via a centrally managed engineering effort. Any resulting emergent behavior often
505 introduces opportunities and additional challenges for systems security engineering.

506 The design principles, concepts, and techniques can also be applied at any stage in the system
507 life cycle when an engineered approach is needed to achieve any of the following objectives:

508 • **System Modifications**

509 - *Reactive modifications to fielded systems*: The engineering effort occurs in response to
510 adversity that diminishes or prevents the system from achieving the design intent. This
511 effort can occur during the [production](#), [utilization](#), or [support](#) stages of the system life
512 cycle and may be performed concurrently with or independent of day-to-day system
513 operations.

- 514 - *Planned upgrades to fielded systems while continuing to sustain day-to-day operations:*
 515 The planned system upgrades may enhance an existing system capability, provide a new
 516 capability, or constitute a technology refresh of an existing capability. This effort occurs
 517 during the [production](#), [utilization](#), or [support](#) stages of the system life cycle.
- 518 - *Planned upgrades to fielded systems that result in new systems:* The engineering effort
 519 is carried out as if developing a new system with a system life cycle that is distinct from
 520 the life cycle of a fielded system. The upgrades are performed in a development
 521 environment that is independent of the fielded system.
- 522 • **System Evolution**
 523 The engineering effort involves migrating or adapting a system or system implementation
 524 from one operational environment or set of operating conditions to another operational
 525 environment or set of operating conditions.⁸
- 526 • **System Retirement**
 527 The engineering effort removes system functions or services and system elements from
 528 operation, including removal of the entire system, and may also include the transition of
 529 system functions and services to another system. The effort occurs during the [retirement](#)
 530 stage of the system life cycle and may be carried out while sustaining day-to-day operations.

531 1.2 TARGET AUDIENCE

532 This publication is intended for security engineering and other engineering professionals who
 533 accomplish the activities and tasks that are defined by the system life cycle processes described
 534 in [Chapter Three](#). The term [systems security engineer](#) is specifically used to include security
 535 professionals who perform the activities and tasks described in this publication. It may apply to
 536 an individual or a team of individuals from the same organization or different organizations.⁹
 537 This publication can also be used by professionals who perform other system life cycle activities
 538 or activities related to the education and/or training of systems engineers and systems security
 539 engineers. These include but are not limited to:

- 540 • Individuals with systems engineering, software engineering, architecture, design,
 541 development, and integration responsibilities
- 542 • Individuals with security governance, risk management, and oversight responsibilities
- 543 • Individuals with security verification, validation, testing, evaluation, auditing, assessment,
 544 inspection, and monitoring responsibilities
- 545 • Individuals with acquisition, budgeting, and project management responsibilities
- 546 • Individuals with system security administration, operations, maintenance, sustainment,
 547 logistics, and support responsibilities

⁸ Increasingly, there is a need to reuse or leverage system implementation successes within operational environments that are different from how they were originally designed and developed. This type of reuse or reimplementation of systems within other operational environments is more efficient and represents potential advantages in maximizing interoperability between various system implementations.

⁹ Systems security engineering activities and tasks can be applied to a mechanism, component, system element, system, system of systems, processes, or organizations. Regardless of the size or complexity of the entity, there is need for a transdisciplinary systems engineering team to deliver systems that are trustworthy and that satisfy the protection needs and concerns of stakeholders. The processes are intended to be tailored to facilitate effectiveness.

- 548 • Providers of technology products, systems, or services
- 549 • Academic institutions offering systems/computer/security engineering programs.

550
551
552
553
554
555
556
557

“Security is embedded in systems. Rather than two engineering groups designing two systems, one intended to protect the other, systems engineering specifies and designs a single system with security embedded in the system and its components.”

-- An Objective of Security in the Future of Systems Engineering [FUSE21]

558 1.3 HOW TO USE THIS PUBLICATION

559 Organizations using this guidance for their systems security engineering efforts can select and
560 employ some or all of the 30 [ISO 15288] processes and some or all of the security-related
561 activities and tasks defined for each process. There are process dependencies, and the
562 successful completion of some activities and tasks necessarily invokes other processes or
563 leverages the results of other processes. This publication is intended to be flexible in its
564 application in order to meet the diverse needs of organizations. It is *not* intended to provide a
565 recipe or roadmap for execution. Rather, it can be viewed as a catalog for achieving the security
566 outcomes of a systems engineering perspective on system life cycle processes – relying on the
567 experience and expertise of the engineering organization to determine what is correct for its
568 purpose.

569 The system life cycle processes can take advantage of any system or software development
570 methodology, including *waterfall*, *spiral*, *DevOps*, or *agile*. In addition, the processes can be
571 applied recursively, iteratively, concurrently, sequentially, or in parallel and to any system
572 regardless of its size, complexity, purpose, scope, environment of operation, or special nature.
573 The full extent of the application of the content in this publication is guided and informed by
574 stakeholder capability needs, protection needs, and concerns with particular attention paid to
575 considerations of cost, schedule, and performance.

576 1.4 ORGANIZATION OF THIS PUBLICATION

577 The remainder of this publication is organized as follows:

- 578 • [Chapter Two](#) provides an overview of the foundational concepts and principles of systems
579 engineering and the specialty discipline of systems security engineering. It presents the
580 basic concepts associated with a system; addresses the concepts of loss, security, protection
581 needs and assets; explains how system security is demonstrated using the concepts of
582 trustworthiness and assurance; and introduces a framework for implementing systems
583 security engineering.
- 584 • [Chapter Three](#) describes security considerations, contributions, and extensions to the
585 system life cycle processes defined in the international systems and software engineering
586 standard [ISO 15288]. Each of the system life cycle processes contains a set of security
587 enhancements that augment or extend the process outcomes, activities, and tasks defined
588 by the standard. The enhanced processes address system security as they are applied
589 throughout the system life cycle.

- 590 • The following sections provide additional information for the effective application of the
591 activities and tasks in this publication:
- 592 - [References](#)
 - 593 - [Appendix A](#): Glossary
 - 594 - [Appendix B](#): Acronyms
 - 595 - [Appendix C](#): Security Policy and Requirements
 - 596 - [Appendix D](#): Trustworthy Secure Design
 - 597 - [Appendix E](#): Principles for Trustworthy Secure Design
 - 598 - [Appendix F](#): Trustworthiness and Assurance
- 599

A SECURITY ENGINEERING FOCUS

This publication does not focus exclusively on cybersecurity but instead, addresses **security** more broadly. Given the scope of this publication, the following observations are relevant and worth noting:

“For the first few decades as a burgeoning discipline, cybersecurity has been dominated by the development of widgets to address some aspect of the problem. Systems have become increasingly complex and interconnected, creating even more attack opportunities, which in turn creates even more opportunities to create defensive widgets that will bring some value in detecting or preventing an aspect of the attack space. Eventually, this becomes a game of whack-a-mole in which a simulated mole pops up from one of many holes and the objective is to whack the mole before it pops back in its hole. The moles represent new attacks, and the holes represent a huge array of potential vulnerabilities—both known and as-yet-undiscovered.”

“Underlying [the discipline of] engineering is science. Sometimes engineering gets ahead of science, such as in bridge building, where the fundamentals of material science were not well understood. Many bridges were built; many fell down; some stayed up; designs of the ones that stayed up were copied. Eventually, for engineering to advance beyond some point, science must catch up with engineering. The science underlying cybersecurity [and more generally, security] engineering is complex and difficult. On the other hand, there is no time like the present to start, because it is both urgent and important to the future...”

-- O. Sami Saydjari
Engineering Trustworthy Systems [[Saydjari18](#)]

600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621

ENGINEERING-DRIVEN SOLUTIONS

The effectiveness of any engineering discipline first requires a thorough understanding of the problem and consideration of all feasible solutions before acting to solve the identified problem. To maximize the effectiveness of systems security engineering, the security requirements for the protection against asset loss must be driven by business, mission, and all other stakeholder asset loss concerns. The security requirements are defined and managed as a well-defined set of engineering requirements and cannot be addressed independently or after the fact.

In the context of systems security engineering, the term *protection* has a broad scope and is primarily focused on the concept of assets and asset loss. The protection capability provided by a system goes beyond prevention and aims to control the events, conditions, and consequences that constitute asset loss. It is achieved in the form of the specific capability and constraints on system architecture, design, function, implementation, construction, selection of technology, methods, and tools and must be “engineered in” as part of the system life cycle process.

Understanding stakeholder asset protection needs (including assets that they own and assets that they do not own but must protect) and expressing those needs through a set of well-defined security requirements is an investment in the organization’s mission and business success in the modern age of global commerce, powerful computing systems, and network connectivity.

622 CHAPTER TWO

623 THE FUNDAMENTALS

624 THE CONCEPTS ASSOCIATED WITH SYSTEMS AND SECURITY ENGINEERING

625 **T**his chapter provides the foundations of systems engineering and systems security
626 engineering; presents the basic concepts associated with a system, including system
627 structure, types of systems, and system of systems; offers a perspective on system
628 security that addresses the concepts of loss, security, protection needs, and assets; describes
629 how system security is demonstrated; and introduces a framework for implementing systems
630 security engineering.

631 2.1 ENGINEERING FOUNDATIONS

632 *Systems engineering* is a transdisciplinary and integrative approach to enabling the successful
633 realization, use, and retirement of engineered systems. It employs systems principles and
634 concepts, as well as scientific, technological, and management methods to achieve such systems
635 [[INCOSE](#)]. Systems engineering uses a collection of technical and non-technical system life cycle
636 processes with associated activities and tasks. The technical processes apply engineering
637 analysis and design principles to realize and deliver a system with the capability to satisfy
638 stakeholder needs and associated emergent properties.¹⁰ The non-technical processes provide
639 engineering management of all aspects of the engineering project, agreements between parties
640 involved in the project, and project-enabling support to facilitate execution of the project.

641 Systems engineering is *system-holistic* in nature, whereby the contributions across multiple
642 engineering and specialty disciplines are evaluated and balanced to produce a coherent
643 capability that is the *system*. Systems engineering applies both systems science and systems
644 thinking¹¹ to solve problems and balances the often-conflicting needs, priorities, and constraints
645 of performance, cost, schedule, and effectiveness to optimize the objectives for the solution
646 with an acceptable level of uncertainty. Systems engineering is *outcome-oriented* and leverages
647 a flexible set of engineering processes to realize a system while effectively managing complexity
648 and serving as the principal integrating mechanism for the technical, management, and support
649 activities related to the engineering effort. Finally, systems engineering is *data-* and *analytics-*
650 *driven* to ensure that all decisions and trades are guided and informed by data produced by
651 analyses conducted with an appropriate level of fidelity and rigor.

¹⁰ An *emergent property* is a property occurring, or emerging, due to interactions among entities within the system and often outside of the system. Emergent properties are typically qualitative in nature, subjective in their nature and assessment, and require consensus agreement based on evidentiary analysis and reasoning. Emergent properties may be anticipated or unanticipated and may be beneficial or detrimental. Emergent properties of systems include safety, security, survivability, maintainability, resilience, reliability, agility, and availability. INCOSE identifies specialty engineering disciplines within systems engineering that are necessary to deliver a complete system, some of which address one or more system emergent properties.

¹¹ *Systems science* is an interdisciplinary field that studies complex systems in nature, society, and science. It aims to develop interdisciplinary foundations that are applicable in a variety of areas, such as social sciences, engineering, biology, and medicine. *Systems thinking* is a discipline of examining wholes, interrelationships, and patterns [[SEBOK](#)].

652 Systems engineering efforts are complex, requiring close coordination between the *engineering*
653 *team* and stakeholders throughout the various stages of the system life cycle.¹² While systems
654 engineering is typically considered in terms of its developmental role as part of the acquisition
655 of a capability, systems engineering efforts and responsibilities do not end once a system
656 completes development and is transitioned to the environment of operation for day-to-day
657 operational use. Stakeholders responsible for the utilization, support, and retirement of a
658 system provide data to the systems engineering team on an ongoing basis. This data captures
659 their experiences, problems, and issues associated with the use and sustainment of the system.
660 Stakeholders also advise on enhancements and improvements made or that they wish to see
661 incorporated into system revisions. In addition, field engineering (also known as sustainment
662 engineering) provides on-site, full life cycle engineering support for operations, maintenance,
663 and sustainment organizations. Field engineering teams coexist with or are dispatched to
664 operational sites and maintenance depots to provide continuous systems engineering support.

665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688

ENGINEERING THE RIGHT SOLUTIONS FOR THE RIGHT REASONS

NASCAR is an organization that governs competition among race teams that engineer, operate, and sustain high-performance racecars designed to be extremely fast, able to operate in hostile racing environments, and able to protect the teams' most critical asset – the driver. These racecars are very different from the typical family car that carries your kids to school or makes the trip to the grocery store. Bigger, more powerful engines, larger tires, and additional safety features such as the head and neck safety (HANS) device are just a few items that result from the automobile engineering effort. In this example, the NASCAR team owner (the key stakeholder) wants to win races while also providing the safest possible vehicle for the driver in accordance with the rules, expectations, and constraints established by NASCAR. Based on those stakeholder objectives, NASCAR rules, the specific conditions anticipated on the racetrack, and the strategy for how the team decides to compete, a set of requirements that include performance and safety considerations are defined as part of the engineering process and subsequently, appropriate investments are made to produce a racecar that meets those requirements. While the typical NASCAR race car is more expensive than a family car, the additional expense is justified by the stakeholder mission and business objectives, strategy for competing, and willingness to preserve their most critical asset – the driver.

Knowing the value of your assets and engineering to protect against asset loss and the consequences of such loss – given all types of hazards, threats, and uncertainty – are the focal points of the systems security engineering discipline.

689 An important objective of systems engineering is to deliver systems deemed *trustworthy*.
690 Trustworthiness is the demonstrated worthiness of a system to be trusted to satisfy given
691 expectations. Claims of trustworthiness are meaningful only to the extent that the needs
692 expressed are accurate, comprehensive, and achievable [Neuman04]. Claims of trustworthiness
693 must include the needs that address adversity. Trustworthiness that is demonstrated only in the

¹² Nomenclature for stages of the system life cycle varies but often includes concept analysis; solution analysis; technology maturation; system design and development; engineering and manufacturing development; production and deployment; training, operations, and support; and retirement and disposal.

694 absence of adversity fails to account for the concerns of security and is inadequate. The
695 concepts of trust and trustworthiness are discussed in greater detail in [Section F.1](#).

696 Security is one of several emergent properties of a system. It shares the same issues and
697 challenges in its realization as every other emergent property of the system. Achieving security
698 objectives requires system security activities and considerations to be tightly integrated into all
699 system life cycle stages and the technical and non-technical processes¹³ of an engineering effort
700 – thus, the need for trustworthy secure engineering, or *systems security engineering*, as part of
701 demonstrating trustworthiness.

702 Systems security engineering is an integrative and transdisciplinary approach to enabling the
703 successful and secure realization, use, and retirement of engineered systems using systems,
704 security, and other principles and concepts, as well as scientific, technological, and management
705 methods. Systems security engineering ensures that these principles, concepts, methods, and
706 practices are applied during the entire system life cycle to achieve stakeholder objectives for the
707 protection of assets from all forms of adversity. It also helps to reduce system defects that can
708 lead to vulnerability and, as a result, reduces the effect that adversity can have on the system.

709 Finally, systems security engineering provides a sufficient base of *evidence* that supports claims
710 or assertions that the desired level of trustworthiness has been achieved – that is, a level of
711 trustworthiness such that the agreed-upon asset protection needs of stakeholders can be
712 satisfied on a continuous basis despite adversity.

713 As part of a transdisciplinary systems engineering effort to deliver a trustworthy secure system,
714 systems security engineering:

- 715 • Works with stakeholders to ensure that security objectives, protection needs/concerns,
716 security requirements, and associated validation methods are defined
- 717 • Defines system security requirements¹⁴ and associated verification methods
- 718 • Develops security views and viewpoints of the system architecture and design
- 719 • Identifies and assesses susceptibilities and vulnerabilities to life cycle hazards and
720 adversities
- 721 • Designs proactive and reactive features and functions encompassed within a balanced
722 strategy to control asset loss and associated loss consequences
- 723 • Provides security considerations to inform systems engineering efforts with the objective to
724 reduce errors, flaws, and weaknesses that may constitute a security vulnerability
- 725 • Performs system security analyses and interprets the results of system security-relevant
726 analyses in support of decision-making for engineering trades and risk management

¹³ These stages and processes should possess their own security objectives that support the security objectives.

¹⁴ When the term *system security requirement* is used in this publication, it is important to understand the context in which it is being used. For example, due to the complexity of system security, there are several types and purposes of system security requirements. See [Section 2.3.8](#) and [Appendix C](#).

- 727 • Identifies, quantifies, and evaluates the costs and benefits of security features and functions
728 and considerations to inform assessments of alternative solutions, engineering trade-offs,
729 and risk treatment¹⁵ decisions
- 730 • Demonstrates through evidence-based reasoning that security and trustworthiness claims
731 for the system have been satisfied
- 732 • Leverages multiple security and other specialties to address all feasible solutions

733 Systems security engineering is considered as a subdiscipline of systems engineering but is not
734 separate; it often overlaps other quality subdisciplines and leverages multiple *specialties* that
735 contribute to systems security engineering activities and tasks. These specialties include
736 computer security; communications security; transmission security; electronic emissions
737 security; anti-tamper protection; physical security; information, software, hardware, and supply
738 chain assurance; and technology specialties such as biometrics and cryptography. Systems
739 security engineering also leverages contributions from other enabling engineering disciplines
740 and specialties¹⁶ to analyze and manage system complexity, dynamicity, interconnectedness,
741 and susceptibility associated with hardware, software, and firmware-based technologies and
742 their development, manufacturing, handling, and distribution throughout the system life cycle.¹⁷
743 Figure 1 illustrates the relationship among systems engineering, systems security engineering,
744 and contributing security and other specialty engineering areas.

745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764

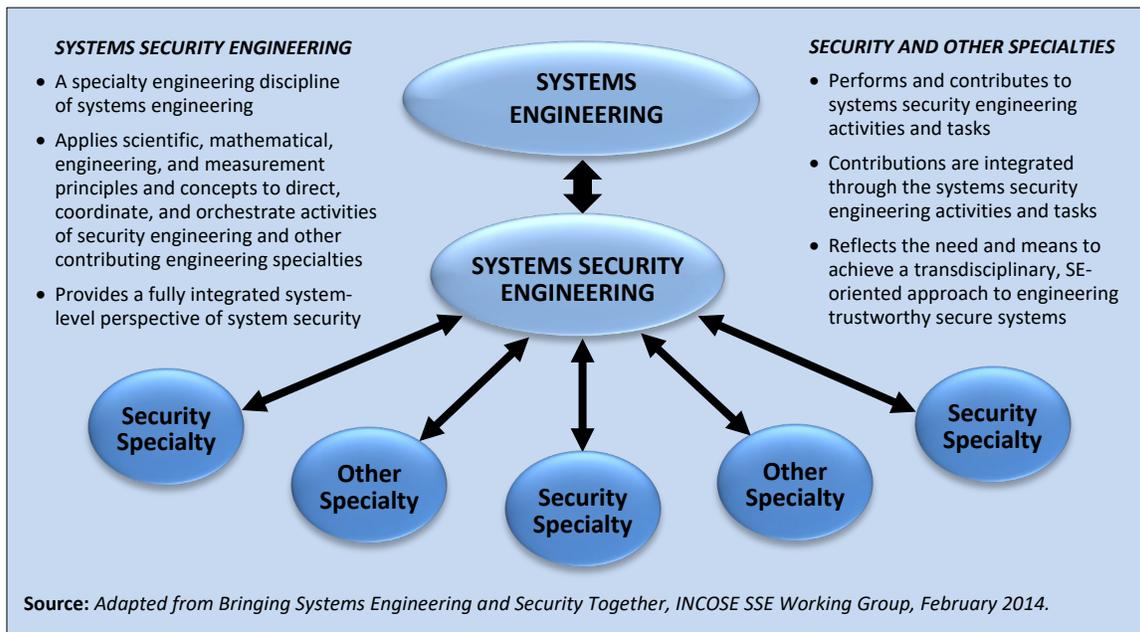


FIGURE 1: SYSTEMS ENGINEERING AND OTHER SPECIALTY ENGINEERING DISCIPLINES

¹⁵ The term *risk treatment* as defined in [ISO 73] is used in [ISO 15288].

¹⁶ Enabling engineering disciplines and specialties include reliability, availability, maintainability (RAM) engineering, software engineering, resilience engineering, and human factors engineering (ergonomics).

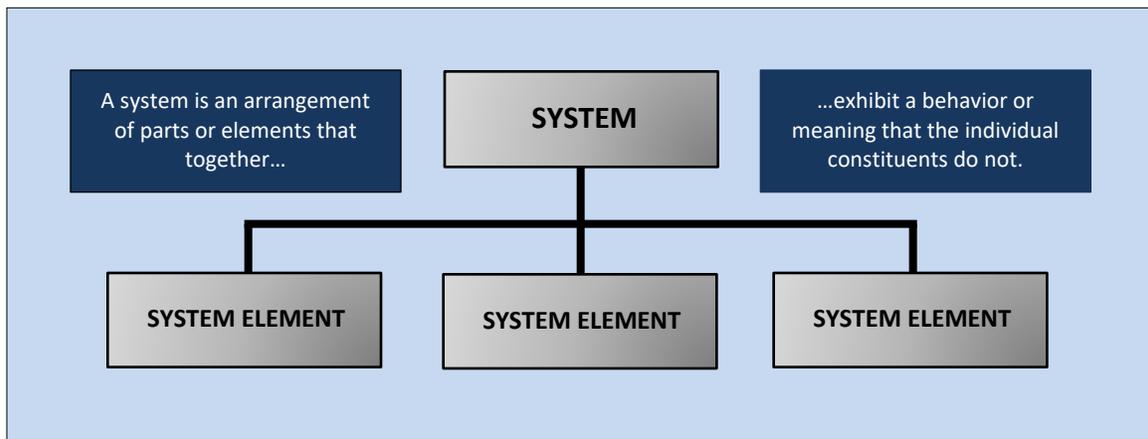
¹⁷ This includes assessment of supply chain risk when third-party and reuse considerations are part of the planned system.

765 2.2 SYSTEM CONCEPTS

766 Several system concepts are important to understand regarding the engineering of trustworthy
 767 secure systems. These include the basic definition of what constitutes a system, the structure of
 768 a system, the different categories of systems, and the concept of a system of systems.

769 2.2.1 Systems and System Structure

770 A *system* is an arrangement of parts or elements that together exhibit a behavior or meaning
 771 that the individual constituents do not.¹⁸ The properties of a system (i.e., attributes, qualities, or
 772 characteristics) emerge from the system's constituent parts or elements and their individual
 773 properties, as well as the relationships and interactions between and among the parts or
 774 elements, the system, and its environment [INCOSE19]. An *engineered system* is a system
 775 designed or adapted to interact with an anticipated operational environment to achieve one or
 776 more intended purposes while complying with applicable constraints [INCOSE19]. Figure 2
 777 shows the basic structure of a system including its constituent system elements.^{19 20}



793 **FIGURE 2: BASIC SYSTEM AND SYSTEM ELEMENT RELATIONSHIP**

794 Systems can include:

- 795 • Information technology (IT) systems (e.g., general purpose computing systems; command,
796 control, and communication systems; merchandising transaction, inventory, financial
797 management, and personnel systems)
- 798 • Internet of Things (IoT) devices (e.g., smart phones, tablets)

¹⁸ A system may be physical (composed of matter and energy), conceptual (composed of information or knowledge), or a combination of both.

¹⁹ A system element can be a discrete component, product, service, subsystem, system, infrastructure, or enterprise. System elements are implemented by hardware, software, and firmware that perform operations on information or data; physical structures, devices, and components in the environment of operation; and the people, processes, and procedures for operating, sustaining, and supporting the system elements.

²⁰ In addition to systems with active functions, there are passive systems (physical infrastructure) without such capability that need to exhibit trustworthiness. For example, the interstate highway system employs safety barriers such as Jersey walls (i.e., system elements) that contribute to the trustworthiness of the transportation system.

- Operational technology (OT) systems (e.g., Industrial Control Systems (ICS); Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS); Building Management and Building Automation Systems (BMS)/(BAS); weapons systems

The purpose of a system is to deliver a capability or part of a capability, that occurs as a service, function, operation, or a combination thereof. A capability can be delivered by a single system or the emergent combined results of a system of systems. The services, functions, and operations may directly or indirectly interact with, control, or monitor physical, mechanical, hydraulic, or pneumatic devices or other systems or capabilities, or it may provide the ability to create, manipulate, access, transmit, store, or share resources, such as data and information.

As shown in Figure 3, the relationship between system elements can be expressed in many forms (e.g., as hierarchies or networks). A system element may be considered a system (i.e., comprised of other system elements) before a complete set of system elements can be defined. In this manner, the appropriate system life cycle processes are applied recursively to a system of interest to resolve its structure to the point where understandable and manageable system elements can be implemented (i.e., developed, bought, or reused). Note that while the systems and system elements in Figure 3 may imply a hierarchical relationship, many systems are not hierarchical, such as networks and other distributed systems.

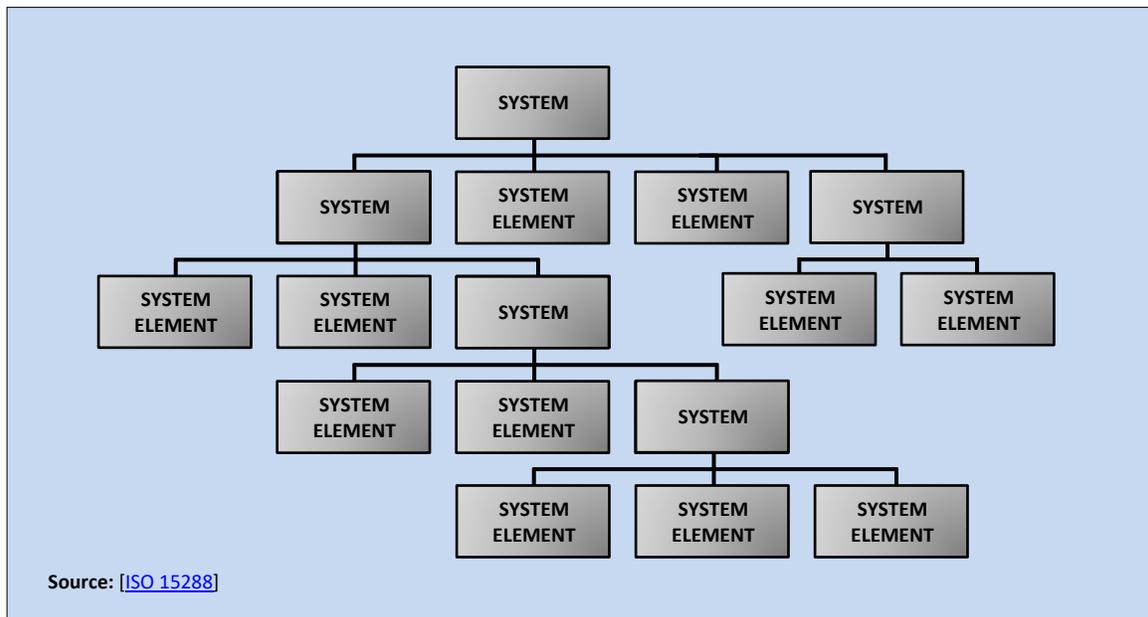


FIGURE 3: COMPLEX RELATIONSHIP AMONG SYSTEMS AND SYSTEM ELEMENTS

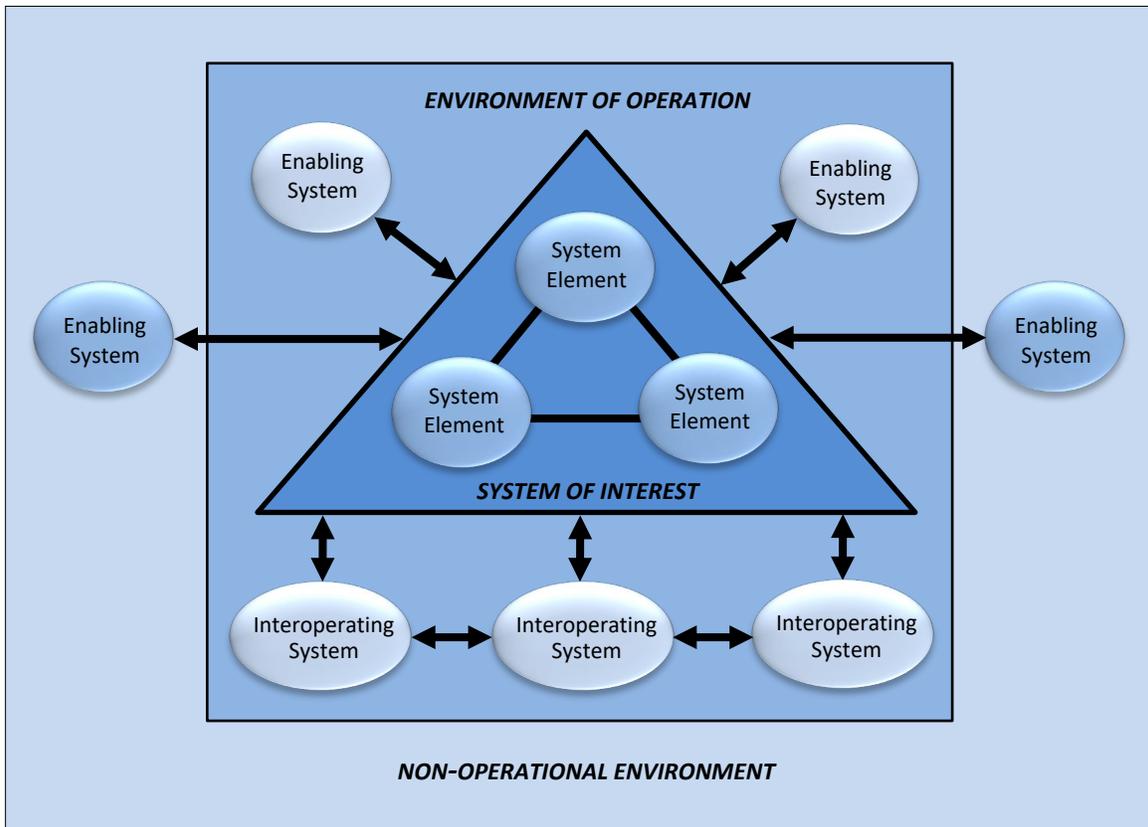
A *system of systems* is a set of systems and system elements interacting to provide a unique capability that none of the constituent systems can accomplish on its own. The elements of a system of systems are, by definition, systems themselves. A system of systems consists of a number of constituent systems plus any inter-system infrastructure, facilities, and processes necessary to enable the constituent systems to integrate or interoperate [\[ISO 21841\]](#). Often, a system may be a constituent system in two or more system of systems, further complicating the operational and managerial considerations and stakeholders.

846 **2.2.2 Interfacing, Enabling, and Interoperating Systems**

847 *Interfacing systems* are systems that interact with the system of interest. Interfacing systems
 848 have an interface for exchanging data or information, energy, or other resources with the
 849 system of interest. An interfacing system exchanges resources with the system of interest during
 850 one or more stages of the system life cycle, such as a system that interfaces for maintenance
 851 purposes or a system used to develop the system of interest. The relationships with interfacing
 852 systems can be either bi-directional or one way. Interfacing systems have two specific subsets:
 853 *enabling systems* and *interoperating systems*.

- 854 • **Enabling systems** provide essential services required to create and sustain the system of
 855 interest. Examples of enabling systems include software development environments,
 856 production systems, training systems, maintenance systems.
- 857 • **Interoperating systems** interact with the system of interest for the purpose of jointly
 858 performing a function during the utilization and sustainment stages of the system life cycle.
 859 Interoperating systems often form a system of systems.

860 Figure 4 illustrates the relationship between the system of interest and its interfacing systems in
 861 both the environment of operation and non-operational (external) environment.



862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
FIGURE 4: SYSTEM OF INTEREST AND INTERFACING SYSTEMS

887 2.3 SYSTEM SECURITY PERSPECTIVE

888 Security, as the freedom from the conditions that cause loss of assets with unacceptable
889 consequences, must consider:

- 890 • The nature and characteristics of systems ([Section 2.3.1](#)) that inform defining conditions
- 891 • The nature and concept of loss ([Section 2.3.2](#))
- 892 • The concept and adequacy of security ([Section 2.3.3](#))
- 893 • The concept of assets ([Section 2.3.5](#)) and reasoning about asset loss ([Section 2.3.6](#))
- 894 • Protection needs ([Section 2.3.7](#)) and various security viewpoints ([Section 2.3.8](#))

895 2.3.1 The Nature and Character of Systems

896 The nature and characteristics of systems, their interrelationships with other systems, and their
897 role as part of a system of systems all impact security and efforts to achieve a secure system of
898 interest. The system characteristics that impact system security vary and can include:

- 899 • System type, function, and primary purpose²¹
- 900 • System technological, mechanical, physical, and human element characteristics
- 901 • Modes and states within which the system delivers its functions and services
- 902 • Criticality or importance of the system
- 903 • Ramifications of the failure of the system to meet its performance expectations, to function
904 correctly, to produce only the intended behaviors and outcomes, and to provide for its own
905 protection (i.e., self-protection)²²
- 906 • System concept for the delivery of a needed capability
- 907 • Approach to acquisition of the system, including the assets used in acquisition
- 908 • Value and sensitivity of assets entrusted to and used by the system
- 909 • Interfaces of the system of interest and systems that interact with the system of interest
910 through those interfaces

911 Each type of system has differences in terms of its distinct system characteristics and how those
912 characteristics impact the determination of *adequate security* ([Section 2.4](#)). For example, a
913 system of systems provides some unique security challenges given the difference in managerial
914 and operational governance compared to other systems. Constituent systems can and do
915 operate independently of one another to fulfill purposes that are distinct from the system of

²¹ Some systems are security-purposed systems dedicated to a specific security-oriented function. Such systems may be delivered as a fully independent security capability (e.g., surveillance system), incorporated as a system element within some system (e.g., cryptographic key management system), or attached to a system (e.g., sensor array on an aircraft).

²² As discussed in [Section D.2](#), a trustworthy secure system must allow only authorized and intended behaviors and outcomes. To the extent possible given constraints and practicality, *self-protection* is a required capability that enables the system to deliver the required stakeholder capabilities while also protecting their assets against loss and the consequences of loss.

916 interest. Managerially, the constituent systems are independent and interdependent. The
917 managing organizations retain some independence from others and often have their own goals
918 and stakeholders.

919 **2.3.2 The Concept of Loss**

920 Loss is the experience of having an asset²³ taken from one or destroyed or the failure to keep or
921 to continue to have an asset in a desired state or form.²⁴ The experience of loss is typically the
922 combination of a resultant adverse event or condition and the ramifications, consequences, or
923 impacts of the resultant adverse event or condition. The loss is determined and assessed
924 independent of the causal events and conditions (i.e., the triggering event, such as an error of
925 omission, or the exploitation event, such as an attack). Examples of resultant adverse events or
926 conditions and their ramifications, impacts, or consequences include:

- 927 1. **Adverse event or condition:** Data is stolen; it is no longer solely in the possession of the
928 owner or entities authorized by the owner.
929 **Ramification, impact, or consequence:** Market share and competitive advantage is taken
930 away because the data that was stolen provided detailed instructions for a precision
931 machining method that no other company possessed.
- 932 2. **Adverse event or condition:** Flat tire on a vehicle; it no longer supports the vehicle weight.
933 **Ramification, impact, or consequence:** One cannot drive the vehicle and needs alternate
934 transportation to get to work, the store, or go on vacation.

935 While the loss condition or event is negative relative to the intended norm, the effect of the loss
936 can be either neutral/inconsequential or negative/consequential.

937
938 Loss may occur because of a single or combination of intentional and unintentional causes,
939 events, and conditions. These may include the authorized or unauthorized use of the system;
940 intentional acts of disruption or subversion; human and machine faults, errors, and failures;
941 human acts of misuse and abuse; and the by-product of emergence, side-effects, and feature
942 interaction. These losses may be inconsequential to the mission or business objectives that are
943 supported by the system, meaning that the mission or business objectives are achieved despite
944 suffering an immediate or eventual loss.

945 The potential for loss suggests the need for *loss control objectives* that serve as the basis for
946 judgments about the effectiveness of protective measures taken to prevent and limit loss. This
947 includes the resultant adverse events and conditions and the ramifications of those adverse
948 events and conditions. The loss control objectives also serve as the basis to acquire evidence of
949 assurance that the system as designed, built, used, and sustained will adequately protect against
950 loss while achieving its design intent. The loss control objectives reflect an ideal to preserve the
951 characteristics of assets (i.e., state, condition, form, utility) to the extent practicable despite the
952 potential for those characteristics to be changed. The objectives accept uncertainty in the form
953 of limits to what can be done (i.e., not all losses can be avoided) and limits to the effectiveness
954 of what is done (i.e., anything that is done has its scope of effectiveness and set of potential
955 failure modes).

²³ An item of value to one or more stakeholders. See [Section 2.3.5](#).

²⁴ Adapted from the Merriam Webster definition of loss.

956 Due to uncertainty, it is not possible to guarantee that some form of loss cannot occur. There is
 957 a need to place an emphasis on protection against the effects of loss, including cascading or
 958 ripple events (i.e., the immediate effect of a loss is causing some additional unintended or
 959 undesired effect or compounding the situation, thereby causing additional losses to occur).
 960 Thus, holistically protecting against loss and the unintended or undesired effects of loss
 961 considers the full spectrum of possible loss across types of losses and loss effects associated
 962 with each asset class. This is important considering that all forms of adversity are not knowable.
 963 Therefore, focusing on effect rather than cause when protecting against loss is prudent.
 964
 965 The loss control objectives in Table 1 address the possibilities to control the potential for loss
 966 and the effects of loss given the limits of certainty, feasibility, and practicality. Collectively, the
 967 loss control objectives encompass the concerns attributed to security and to system safety,
 968 survivability, and resilience.

969

TABLE 1: LOSS CONTROL OBJECTIVES

LOSS CONTROL OBJECTIVE	DISCUSSION
LOSS PREVENTION <i>(Prevent the loss from occurring)</i>	<ul style="list-style-type: none"> • This is the case where a loss is totally avoided. That is, despite the presence of adversity: <ul style="list-style-type: none"> - The system continues to provide <i>only</i> the intended behavior and produces <i>only</i> the intended outcomes - The desired properties of the system and assets used by the system are retained - The assets continue to exist • Loss avoidance may be achieved by any combination of: <ul style="list-style-type: none"> - Preventing or removing the event or events that cause the loss (the loss never occurs) - Preventing or removing the condition or conditions that allow the loss to occur (the loss never occurs) - Not suffering an adverse effect despite the events or conditions (the loss never occurs) • Terms such as <i>avoid, continue, delay, divert, eliminate, harden, prevent, redirect, remove, tolerate,</i>²⁵ and <i>withstand</i> are typically used to characterize approaches to achieve this objective such that a loss does not occur despite the system being subjected to adversity
LOSS LIMITATION <i>(Limit the extent of the loss)</i>	<ul style="list-style-type: none"> • This covers cases where a loss can or has occurred, and the extent of loss is to be limited • The extent of loss can be limited in terms of any combination of the following: <ul style="list-style-type: none"> - Limited dispersion (e.g., migration, propagation, spreading, ripple, domino, or cascading effects) - Limited duration (e.g., milliseconds, minutes, hours, days) - Limited capacity (e.g., diminished utility, delivery of function, service, or capability) - Limited volume (e.g., bits or bytes of data/information) • Decisions to limit the extent of loss may require prioritizing what constitutes acceptable loss across a set of losses, whereby the objective to limit the loss for one asset requires accepting a loss of some other asset • The extreme case of loss limitation is to avoid destruction of the asset • Terms such as <i>tolerate, withstand, remove, continue, constrain, stop/halt, and restart</i> fall into this category in the case where the loss occurs and the system can, or enables the ability to, limit the effect of the loss

²⁵ The term *tolerate* refers to the objective of fault/failure tolerance, whereby adversity in the form of faults, errors, and failures is rendered inconsequential and does not alter or prevent the realization of authorized and intended system behavior and outcomes. That is, the faults, efforts, and failures are tolerated. As used in this publication, tolerate does not refer to a risk acceptance decision.

LOSS CONTROL OBJECTIVE	DISCUSSION
	<ul style="list-style-type: none"> • Loss recovery and loss delay are two means to limit loss: <ul style="list-style-type: none"> - <i>Loss Recovery</i>: Action is taken by the system or enabled by the system to recover (or allow the recovery of) some or all of its ability to function (i.e., behave, interact, produce outcomes) and to recover assets used by the system (e.g., re-imaging, reloading, or recreating information and data, including software in the system). The restoration of the asset, fully or partially, can limit the dispersion, duration, capacity, or volume of the loss. - <i>Loss Delay</i>: The loss event is avoided until the adverse effect is lessened or when a delay enables a more robust response or quicker recovery. • System and environmental conditions may be assumed to result in loss, but measures are taken to limit impacts • Terms such as <i>contain</i>, <i>recover</i>, <i>restore</i>, <i>reconstitute</i>, <i>reconfigure</i>, and <i>restart</i> are typically used to characterize approaches to achieving this objective

970

971 **2.3.3 The Concept of Security**

972 A system with freedom from those conditions that can cause a loss of assets with unacceptable
 973 consequences must provide the intended behaviors and outcomes (e.g., the intended system
 974 functionality) and avoid any unintended behaviors and outcomes that constitute a loss. The
 975 term *intended* has two cases, both of which must be satisfied:

- 976 • **Design intent:** As intended by the design
 977 • **User intent:** As intended by the user

978 A system that delivers a capability per the design intent but is inconsistent with the user intent
 979 constitutes a loss. For example, the loss of control of a vehicle might result from a failure in the
 980 vehicle’s steering control function (i.e., failure to meet the design intent) or through an attack
 981 that takes control away from the driver (i.e., failure to meet the user intent). The primary
 982 security objective is to ensure that only the intended behaviors and outcomes occur, both with
 983 the system and within the system.²⁶ Every security need and concern derive from this objective,
 984 which is based on the concept of *authorization* for what is and is not allowed.²⁷ As such, the
 985 primary security control objective is the enforcement of constraints in the form of rules for
 986 allowed and disallowed behaviors and outcomes. This security control objective – and one of
 987 the foundational principles of trustworthy secure design – is *Mediated Access*. If access is not
 988 mediated (i.e., controlled through the enforcement of constraints) in accordance with a set of
 989 non-conflicting rules, then there is no basis upon which to claim security is achieved.²⁸

²⁶ Behaviors are inclusive of interactions. Interactions of relevance include human-to-machine and machine-to-machine interactions. Human-to-machine interactions are typically transformed into machine-to-machine interactions, whereby a machine element operates on behalf of the human.

²⁷ An attacker seeks to produce unauthorized behaviors or outcomes. Attackers attempt to accomplish something that they are not authorized to accomplish, even if that behavior or outcome is authorized for some other entity.

²⁸ The *Reference Monitor Concept* (Section D.4.2) cites three properties of access mediation mechanisms: (1) always invoked, (2) tamper-proof, and (3) evaluable to substantiate claims of correctness of their implementation. While defined to explicitly address mediated access, the concepts apply equally to any mechanism that enforces constraints on state, behavior, or outcomes.

990 The rules for mediated access are stated in a set of security policies that reflect or are derived
991 from laws, directives, regulations, life cycle concepts,²⁹ requirements, or other specifically stated
992 stakeholder objectives. Each security policy includes a *scope of control* that establishes bounds
993 within which the policy applies. Security policy rules are stated in terms of subjects (active
994 entities), objects (passive entities), and the operations that the subject can perform or invoke on
995 the object.³⁰ The rules govern *subject-to-object* and *subject-to-subject* behaviors and outcomes.
996 The rules for each security policy must be accurate, consistent, compatible, and complete with
997 respect to stakeholder objectives for the scope of control.³¹ Inconsistency, incompatibility, or
998 incompleteness in the rules leads to gaps in security protection. It is equally important that the
999 security protection capabilities of the system are aligned with and can achieve the expectations
1000 of security policy.

1001 *Privileges*³² define the set of allowed and disallowed behavior and outcomes granted to a
1002 subject. Privileges are the basis for making mediated access decisions. A restrictive default
1003 practice for security policy enforcement is to design the enforcement mechanism to allow only
1004 what the policy explicitly allows and to deny everything else. For a system to be deemed
1005 trustworthy secure, there must be sufficient confidence that the system is capable of enforcing
1006 security policy on a continuous basis for the duration of the time that the security policy is in
1007 effect ([Appendix F](#), *Trustworthiness and Assurance*).

1008 Systems engineering must deal with optimizing across multiple objectives that are often in
1009 conflict with one another. Often, technologies do not (yet) exist to fully achieve objectives, or
1010 they are beyond the constraints of cost and schedule. Therefore, “best effort” is the most that
1011 can be practically expected. Given this reality, there is a need to judge best engineering efforts
1012 for security.

1013 **2.3.4 The Concept of System Security**

1014 The definition of security can be interpreted to capture what is meant by a secure system.

1015 *A secure system is a system that – for all of its identified states, modes, and transitions –*
1016 *ensures that only the authorized intended behaviors and outcomes occur, thereby providing*
1017 *freedom from those conditions, both intentionally/with malice and unintentionally/without*
1018 *malice, that can cause a loss of assets with unacceptable consequences.*

1019 This definition expresses an ideal that captures the three essential aspects of what it means to
1020 achieve security:

- 1021 • Enable the delivery of the required system capability despite intentional and unintentional
1022 forms of adversity.
- 1023 • Enforce constraints to ensure that only the desired behaviors and outcomes associated with
1024 the required system capability are realized while satisfying the first aspect.

²⁹ Life cycle concepts include operation, sustainment, evolution, maintenance, training, startup, and shutdown.

³⁰ Active entities exhibit behavior (e.g., a process in execution) while passive entities do not (e.g., data, file).

³¹ At the highest level of assurance, security policies are formally specified and verified.

³² Privileges are also referred to as authorizations or rights.

- 1025 • Enforce constraints based on a set of rules to ensure that only authorized human-to-
 1026 machine and machine-to-machine interactions and operations are allowed to occur while
 1027 satisfying the second aspect.

1028 For a system, *adequate security* is an evidence-based determination that achieves and optimizes
 1029 security performance against all other performance objectives and constraints. Judgments of
 1030 adequate security are driven by the stakeholder objectives, needs, and concerns associated with
 1031 the system. Adequate security has two elements:

- 1032 • Achieve the minimum acceptable threshold of security performance
 1033 • Maximize security performance to the extent that any additional increase in security
 1034 performance results in a degradation of some other aspect of system performance or
 1035 requires an unacceptable operational commitment

1036 Finally, adequate security is determined based on viewpoint, context, criticality, and priority and
 1037 may vary across mission or business operational objectives or across the states and modes of the
 1038 system as it exists (e.g., operation, storage, or transit).³³

1039 **2.3.5 The Concept of Assets**

1040 An asset is an item of value. There are many different types of assets. Assets are broadly
 1041 categorized as either *tangible* or *intangible*. Tangible assets include physical items, such as
 1042 hardware, computing platforms, or other technology components. Intangible assets include
 1043 humans, data, firmware, software, capabilities, functions, services, trademarks, intellectual
 1044 property, copyrights, patents, image, or reputation.³⁴ Within asset categories, assets can be
 1045 further identified and described in terms of common asset classes as illustrated in Table 2.

1046 Assets may also be considered as individual items or as an aggregate or group of items that
 1047 spans asset types or asset classes (e.g., personnel data, fire control function, environmental
 1048 sensor capability). This publication uses the term *asset of interest* to emphasize and establish
 1049 bounds on the scope of reasoning for a specific asset, asset type, or asset class.

1050

TABLE 2: COMMON ASSET CLASSES

ASSET CLASS	DESCRIPTION	LOSS PROTECTION CRITERIA
MATERIAL RESOURCES AND INFRASTRUCTURE	This asset class includes physical property (e.g., buildings, facilities, equipment) and physical resources (e.g., water, fuel). It also includes the basic physical and organizational structures and facilities (i.e., infrastructure) needed for an activity or the operation of an enterprise or society. ³⁵ An infrastructure ³⁶ may be comprised of assets in other	<i>Material resources</i> are protected from loss if they are not stolen, damaged, or destroyed or are able to function or be used as intended, as needed, and when needed. <i>Infrastructure</i> is protected from loss if it meets performance

³³ A system in storage or transit may have expectations to protect critical technologies contained within that system.

³⁴ Humans are perhaps the most important and valuable of all intangible assets. Safety explicitly considers the human asset, and that same consideration is equally applicable to security.

³⁵ Adapted from the Merriam Webster and Oxford definitions of *infrastructure*.

³⁶ There are 16 critical infrastructure sectors whose assets, systems, and networks – whether physical or virtual – are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof [CISA20].

ASSET CLASS	DESCRIPTION	LOSS PROTECTION CRITERIA
	<p>classes. For example, the National Airspace System (NAS) may be considered infrastructure that itself is a system and contains other elements that are forms of systems and infrastructures, such as Air Traffic Control, navigational aids, weather aids, airports, and the aircraft that maneuver within the NAS.</p>	<p>expectations while delivering only the authorized and intended capability and producing only the authorized and intended outcomes.</p>
<p>SYSTEM CAPABILITY</p>	<p>This asset class is the set of capabilities or services provided by the system. Generally, system capability is determined by: (1) the nature of the system (e.g., entertainment, vehicular, medical, financial, industrial, or recreational); and (2) the use of the system to achieve mission or business objectives.</p>	<p><i>System capability</i> is protected from loss if the system meets its performance expectations while delivering only the authorized and intended capability and producing only the authorized and intended outcomes.</p>
<p>HUMAN RESOURCES</p>	<p>This asset class includes personnel who are part of the system and personnel who are directly or indirectly involved with or affected by the system. The consequences of loss associated with the system may significantly change the importance of this asset class (e.g., the effect on personnel due to a failure of a guidance system in an aircraft is significantly different from the effect on personnel due to the breach of a system that compromises individual credit card information).</p>	<p><i>Human resources</i> are protected from loss if they are not injured, suffer illness, or killed.</p>
<p>INTELLECTUAL PROPERTY³⁷</p>	<p>This asset class includes trade secrets, recipes, technology,³⁸ and other items that constitute an advantage over competitors. The advantage is domain-specific and may be referred to as a competitive advantage, technological advantage, or combative advantage.</p>	<p><i>Intellectual property</i> is protected from loss if it is not stolen, corrupted, destroyed, copied, substituted in an unauthorized manner, or reverse-engineered in an unauthorized manner.</p>
<p>DATA AND INFORMATION</p>	<p>This asset class includes all types of data and information (aggregations of data) and all encodings and representations of data and information (e.g., digital, optical, audio, visual). There are general sensitivity classes of data and information that do not fall within the above categories, such as classified information, Controlled Unclassified Information (CUI), and unclassified data and information.</p>	<p><i>Data and information</i> are protected from loss due to unauthorized alteration, exfiltration, infiltration, and destruction.</p>
<p>DERIVATIVE NON-TANGIBLES</p>	<p>This asset class is comprised of derivative, non-tangible assets, such as image, reputation, and trust. These assets are defined, assessed, and affected – positively and negatively – by the success or failure to provide adequate protection for assets in the other classes.</p>	<p><i>Non-tangible assets</i> are protected from loss by ensuring the adequate protection of assets in the other classes.</p>

1051

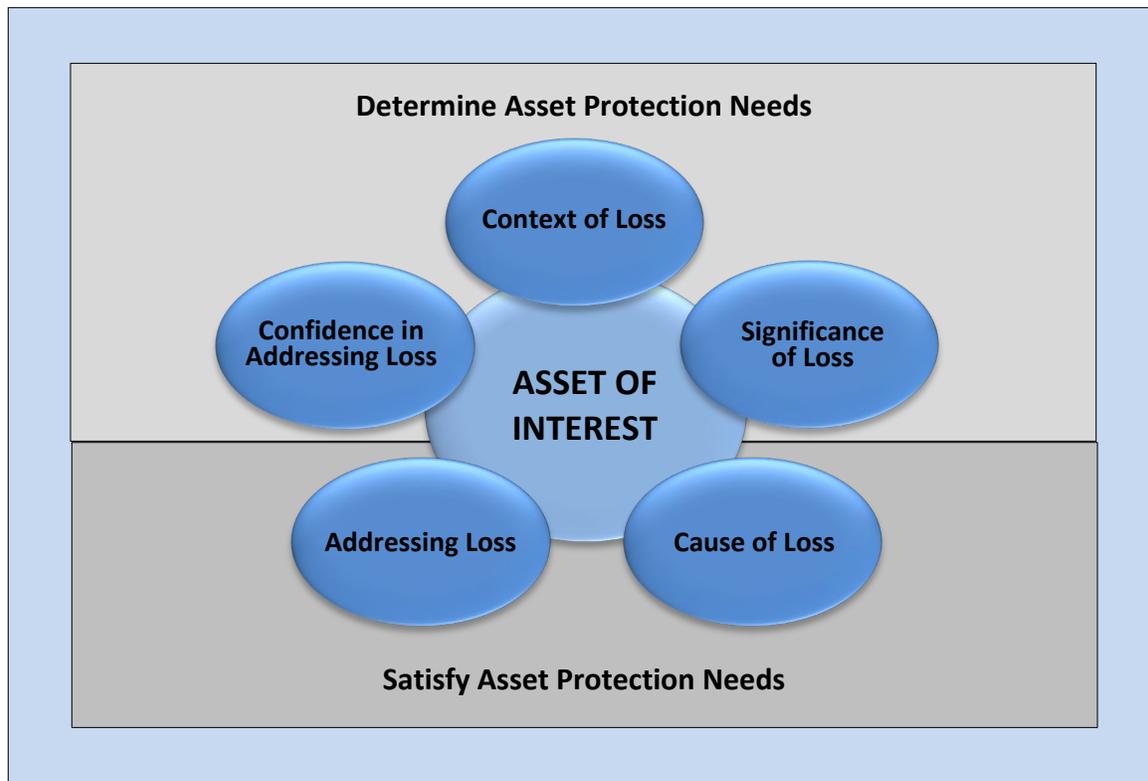
³⁷ The term *intellectual property* is defined as an output of a creative human thought process that has some intellectual or informational value [ISO 24765]. Examples include microcomputer design and computer programs.

³⁸ The term *technology* is defined as the application of scientific knowledge, tools, techniques, crafts, systems, or methods of organization to solve a problem or achieve an objective [ISO 16290].

1052 The *valuation* of an asset is a key input in decision-making about investments to protect an
 1053 asset. The valuation determination is made by stakeholders. For those cases where an asset is
 1054 associated with multiple stakeholders, there may be differing, contradictory, competing, or
 1055 conflicting concerns about the valuation of the asset. These differences are addressed as part of
 1056 discussions that resolve differences associated with agreements on needs, expectations, and
 1057 requirements. The valuation of an asset may be influenced by a variety of factors that include
 1058 the cost (i.e., monetary, time, material, human resources) to develop or acquire, the cost to
 1059 maintain, the cost to repair or replace, the cost if the asset is not repairable or replaceable, and
 1060 the importance of completing an objective.³⁹

1061 2.3.6 Reasoning About Asset Loss

1062 The elements of a structured approach for reasoning about assets and assets loss are shown in
 1063 Figure 5. The elements provide a comprehensive basis for decision-making about assets and
 1064 asset loss to determine the objectives for a secure system, optimize the protection capability of
 1065 the system, and make judgments on the suitability and effectiveness of the implemented
 1066 protections.⁴⁰ Each of these elements is discussed in greater detail below.



1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090

FIGURE 5: REASONING ABOUT ASSET PROTECTION

³⁹ The Department of Defense's *Mission Engineering Guide* [DOD 2020] relates asset protection to mission by using a mission objective of preserving a return on investment (ROI). Life, material, technological advantage, or other unintentional losses that occur while executing a mission may be considered a poor return on investment.

⁴⁰ The application of the asset reasoning approach works equally to reason about assets in terms of mission (i.e., mission-driven asset reasoning), organization (i.e., organization-driven asset reasoning), and enterprise (i.e., enterprise-driven asset reasoning).

1091 The elements are grouped into two objectives to facilitate reasoning about the *asset of interest*:

- 1092 • **OBJECTIVE 1:** *Determine* asset protection needs
- 1093 - **Context of Loss:** The scope and criteria that bounds reasoning about asset loss
- 1094 - **Significance of Loss:** The effect of asset loss (or adverse impact) based upon its
- 1095 valuation
- 1096 - **Confidence in Addressing Loss:** The assurance to be achieved based on claims-driven
- 1097 and evidence-based arguments about the effectiveness of what is done to address
- 1098 potential and actual loss
- 1099 • **OBJECTIVE 2:** *Satisfy* asset protection needs
- 1100 - **Cause of Loss:** The events, conditions, or circumstances that describe what has
- 1101 happened before and what can happen in the future and that constitute the potential
- 1102 for loss to occur
- 1103 - **Addressing Loss:** The various actions taken to exercise control over loss to the extent
- 1104 practicable. The control objectives are to prevent loss from occurring and to limit the
- 1105 extent and duration for those losses that do occur. Limiting loss includes recovery from
- 1106 loss to the extent practicable.

1107 The *asset of interest* is the asset class, asset type, or individual asset being addressed. Reasoning

1108 about loss is based on the asset of interest. Distinguishing the asset of interest from all other

1109 assets provides clarity in the interpretation of loss for the asset of interest and the associated

1110 judgments of suitability and effectiveness of protections employed. A focus on a specific asset

1111 class, type, or discrete element also enables precise traceability to requirements that support

1112 the analysis needed to determine the protection-relevant impact of changes to requirements.

1113

1114 The *context of loss* sets the boundary, scope, and time frame for the reasoning, analyses,

1115 assessments, and conclusions about the asset of interest. The context of loss also provides a

1116 basis to relate and trace asset dependencies and interactions and to group assets for protection.

1117 The context of loss time frame is particularly important because the asset of interest has a life

1118 cycle⁴¹ that is different from the system of interest.⁴² For example, the asset of interest may be

1119 created, configured, or modified outside of the scope of control of the system of interest yet be

1120 within the scope of the engineering effort. The asset of interest, once within the scope of

1121 control of the system of interest, may have differing protection needs associated with the state

1122 or mode of the system (e.g., the system operational mode protection may differ from the

1123 system training mode). Additionally, system life cycle assets ([Section 2.3.8](#)) may exist only within

1124 a development or production system and their associated supporting environments. The effect

1125 of the loss for these assets may transfer to a loss associated with the system of interest.

1126 Therefore, the context of loss includes the life cycle of the asset, the state and mode of the

1127 system, and other time-based periods or characteristics during which loss is addressed.

⁴¹ The lifetime of an asset may be different from the lifetime of the system. Assets may predate the system and may persist after the system's retirement from use. The significance of the loss of an asset can have ramifications that are independent of the system, system function, and business and mission objectives.

⁴² The asset life cycle is the same as the system life cycle when the asset of interest is the system of interest. The asset life cycle may be the same or shorter than the system life cycle for those assets created by the system of interest and only required while the system of interest is operating.

1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140

TIMEFRAME OF LOSS – AN EXAMPLE

A financial portfolio (an asset or collection of assets) with specific investment objectives and risk acceptance considerations may be created by a financial advisor for a client, funded by the client, and subsequently managed using multiple systems across one or more institutional investment firms throughout the portfolio's life cycle. Each asset of interest within the portfolio may have differing protection needs at different times depending on the type of asset, market conditions, regulatory jurisdiction, risk position, and other asset management factors that are imposed on the system.

1141 The *significance of loss* is the adverse effect on the asset of interest or the resultant adverse
1142 effect associated with the asset. The significance of loss is best described as an experience that
1143 is to be avoided, thereby warranting an investment to protect against it occurring and to
1144 minimize the extent of the adverse effect should it occur. The significance of loss is determined
1145 and assessed as an effects-based judgment. That is, it is determined without any consideration
1146 of how or why the loss occurs, the probability or likelihood of the loss occurring, and any intent
1147 or the absence of intent related to the loss.⁴³

1148 The *consequence of loss* simply answers the following question: "What are the ramifications,
1149 effects, and problems that result from suffering a loss of the asset of interest?" The significance
1150 of loss requires clarity in what loss means for the asset of interest. Examples of terms used to
1151 describe asset loss include ability, accessibility, accuracy, assurance, advantage (technological,
1152 competitive, combatant), capability, control, correctness, existence, investment, ownership,
1153 performance, possession, precision, quality, satisfaction, and time.

1154 *Confidence in addressing loss* ensures that protections have a body of objective evidence that
1155 demonstrates the effectiveness, sufficiency, and suitability of protective measures to satisfy
1156 asset protection needs. Confidence in addressing loss is cumulative. It begins with determining
1157 the loss concerns for the asset of interest and continuously builds as those concerns are better
1158 understood and addressed across the context of loss, the consequence of loss, the causes of
1159 loss, and how loss is addressed. The evidence basis that provides confidence is informed by
1160 verification and validation activities that occur throughout the life cycles of the assets and the
1161 system, including requirements elicitation and analysis. A key informing element to those
1162 activities is to ensure that the results contribute to the confidence sought.

1163 The *cause of loss*⁴⁴ is the individual or combination of events, conditions, and circumstances that
1164 result in some form of loss of an asset. The causes of asset loss constitute a continuum that

⁴³ Determining the consequence of loss is not a determination of risk.

⁴⁴ Many terms are used to describe the cause of asset loss. Some of these terms are specific to a community of interest or specialty field, while others span communities and specialties. There are also cases where the same term may be used differently across communities and specialty fields (e.g., the term *threat* has varying interpretations across communities, such as physical security, cybersecurity, commerce, law enforcement, industry, military combat operations, and military intelligence). The terms typically used as a synonym for the cause of asset loss include attack, breach, compromise, hazard, mishap, threat, violation, and vulnerability.

1165 includes intentional, unintentional, accidental, incidental, misuse, abuse, error, defect, fault,
 1166 weakness, and failure events and conditions. This continuum spans all human-based, machine-
 1167 based, physical-based, and nature-based drivers of loss. The following considerations apply to
 1168 reasoning about the causes of loss:

- 1169 • Single events and conditions that alone can produce the loss
- 1170 • Combinations, sequences, and aggregate events and conditions
- 1171 • Events and conditions that are desirable, intended, and even planned yet produce
 1172 unanticipated, unforeseen, and unpredictable results
- 1173 • Cascading and ripple events and conditions

1174 Finally, the causes of asset loss answer the questions: “How can loss occur, and how has loss
 1175 occurred in the past?” The purpose of determining how loss can occur does not ask the question
 1176 “What is likely or probable to happen?”⁴⁵

1177

1178

1179

1180

1181

1182

1183

1184

1185

1186

1187

1188

1189

1190

1191

1192

SIGNIFICANCE OF LOSS – AN EXAMPLE

The significance of loss due to a flat tire is determined and assessed without consideration of how or why the tire became flat (e.g., puncture, manufacturing defect, impact with curb or other object) and without any consideration of malicious intent (e.g., tire cut, valve stem loosened). Regardless of how or why the tire became flat, the significance of loss remains the same (e.g., loss of control if the vehicle is moving, inability to drive if the vehicle is stationary, time lost to replace or repair the tire to make the vehicle operable). The significance of loss due to a flat tire includes the inability to steer the vehicle, and the resultant adverse effect may be to impact some other object (i.e., a crash). The adverse effect of the loss of steering (loss of control) is specific, while the adverse effect of a crash is general (many other circumstances may result in a crash without any loss of the ability to steer the vehicle).

1193 *Addressing loss* occurs through the protective measures that enforce constraints to ensure that
 1194 only authorized and intended behaviors and outcomes of the system occur. These include:

- 1195 • Protective measures provided by the *machine* portion of the system (i.e., the system
 1196 architecture and design, the use of engineered features and devices within the architecture
 1197 and design)
- 1198 • Protective measures provided by the *human* portion of the system (i.e., personnel,
 1199 procedures, practices, the use of tools to support the human as a system element, and the
 1200 human role in designing and building the machine part of the system)
- 1201 • Protective measures provided by the *physical environment* (i.e., facility access points,
 1202 controlled access areas, physical monitoring, environmental controls, and fire suppression)

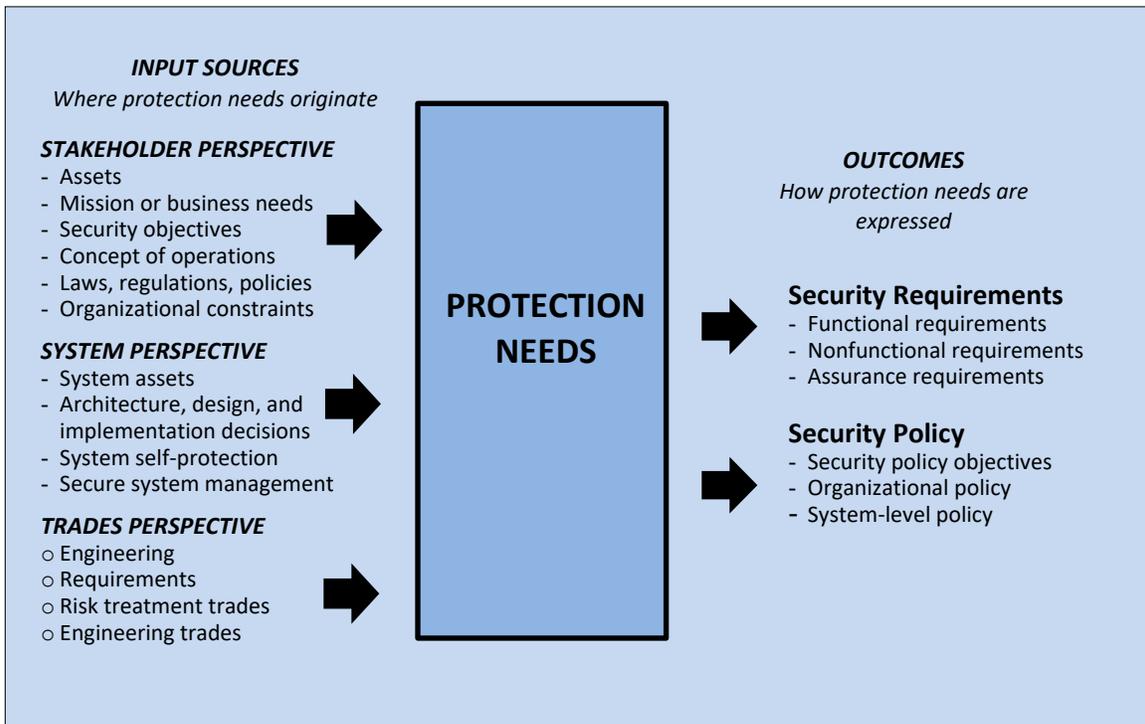
⁴⁵ This point distinguishes analysis of what can happen from a risk assessment that determines probability greater than zero and less than one that the adverse event will happen.

1203 The terminology used to describe means and methods includes configurations, controls,
 1204 countermeasures, features, inhibits, mechanisms, overrides, practices, procedures, processes,
 1205 safeguards, and techniques. These may be applied in accordance with governing policies,
 1206 regulations, laws, practices, standards, and techniques.

1207 **2.3.7 Protection Needs**

1208 Stakeholders have a need to achieve their mission or business objectives in a secure manner
 1209 that preserves assets and limits the extent of asset loss. Asset protection must be continuous,
 1210 thereby making it possible for stakeholders to have a realistic expectation of continuous success
 1211 in the ability of their systems to support and achieve their objectives.

1212
 1213 The scope and expectations for the protection of assets is foundational to achieving the design
 1214 intent for a trustworthy secure system. Protection needs typically correlate to the severity of
 1215 consequences associated with the loss of an asset. The protection needs are determined from
 1216 all needs, concerns, priorities, and constraints to protect and preserve stakeholder and system
 1217 assets. There are two perspectives for protection needs: (1) the *stakeholder* perspective; and (2)
 1218 the *system* perspective. Figure 6 illustrates the key input sources used to define protection
 1219 needs and the outputs derived from the specification of those needs.
 1220

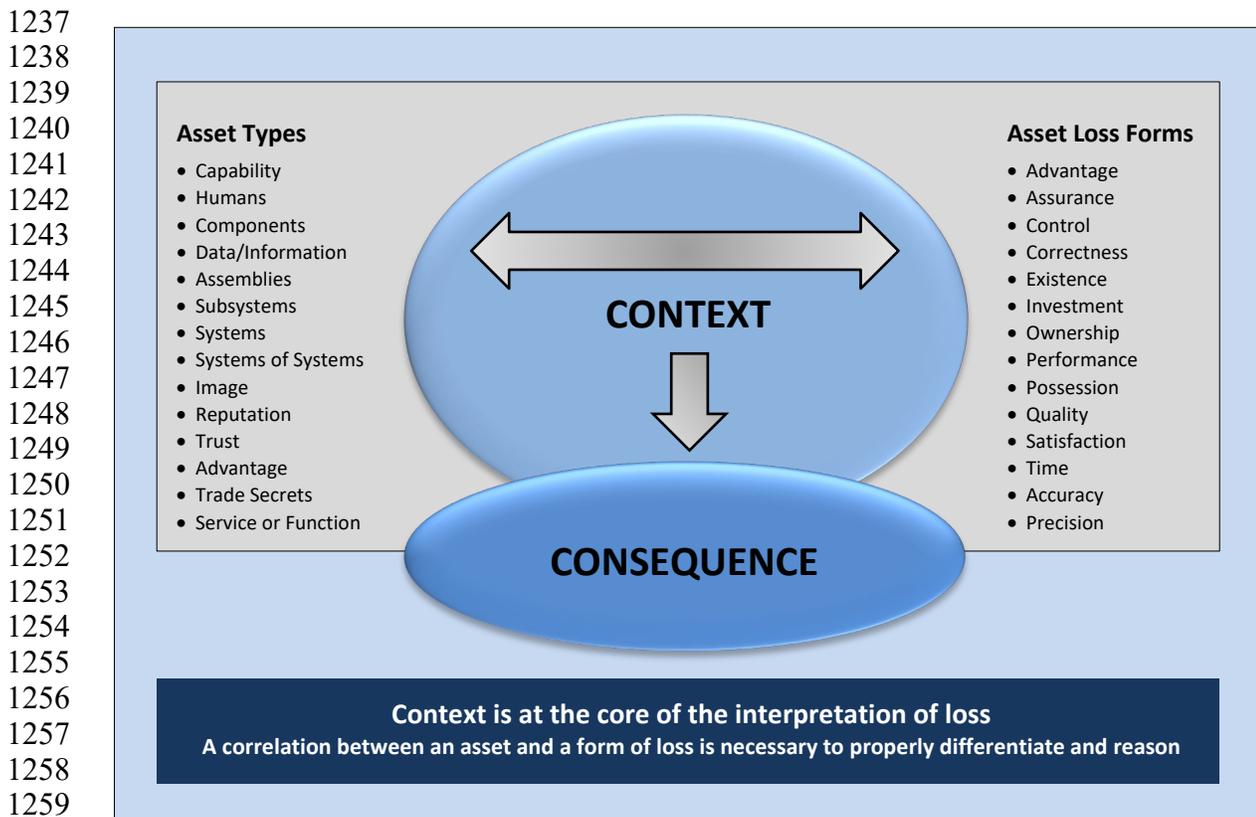


1221 **FIGURE 6: DEFINING PROTECTION NEEDS**

1222 The stakeholder perspective is based on the assets that belong to stakeholders. Therefore, those
 1223 stakeholders determine the protection needs. The system perspective is based on the assets
 1224 necessary for the system to function. These assets are determined by system design decisions

1225 and the criticality and priority⁴⁶ of the asset in providing or supporting the functions of the
 1226 system. Stakeholders are typically unaware of the existence of system assets and are not able to
 1227 make decisions about the protection needs for system assets. The protection of system assets is
 1228 an element of trustworthy secure system design.

1229
 1230 The purpose of establishing the *need for protection* is to decide what assets to protect and to
 1231 determine the priority given to such protection. This can be accomplished without considering a
 1232 cause or condition against which to protect. As shown in Figure 7, the need for protection is
 1233 derived from the relationship among the asset of interest, context of loss, type of loss, and the
 1234 consequences of loss. This approach establishes the need for protection that, once validated by
 1235 stakeholders across all assets of interest, provides the basis for developing security objectives
 1236 and requirements.⁴⁷



1260 **FIGURE 7: RELATIONSHIP AMONG ASSET, LOSS, AND CONSEQUENCE**

1261 Summarizing, the following considerations impact the identification of protection needs:

- 1262
- Assets have different classes and types

⁴⁶ Criticality and priority based on asset valuation is typically used in decisions on protection needs. An asset with higher criticality and priority would take precedence in providing protection should there be constraints that require making choices between the overall protection needs ([Section 2.3.7](#)).

⁴⁷ Requirements provide a formal and clear expression of the needs, concerns, priorities, and constraints to be satisfied for system function, operation, and maintenance. Each requirement is accompanied by verification methods for demonstrating that the requirement is satisfied. Requirements must be accurate, unambiguous, comprehensive, evaluable, and achievable.

- 1263 • Assets are associated with stakeholders and the system
- 1264 - Some assets are associated with stakeholders (i.e., stakeholder assets) and have a
- 1265 purpose, use, and existence that is independent of the system being designed
- 1266 - Some assets are associated with the system, are dependent on characteristics of the
- 1267 system design and behavior, and are typically unknown to stakeholders
- 1268 • Loss interpretation is dual-faceted
- 1269 - The effect on the asset of interest
- 1270 - The effect on those who value the asset of interest
- 1271 • Loss interpretation is temporal and state-based
- 1272 - Spans a continuum within and across asset types and classes
- 1273 - May change across the life cycle of the asset and the state in which the asset exists or is
- 1274 utilized
- 1275 • Asset-based judgments are subjective
- 1276 - Asset valuation
- 1277 - Asset loss ramifications
- 1278 - Asset protection suitability, effectiveness, and dependability

ASSET-BASED PROTECTION – ENGINEERING FOR SUCCESS

Don't focus on what is *likely* to happen. Instead, focus on what *can* happen, and be prepared. That is what systems security engineering means by adopting a proactive and reactive strategy ([Section D.2](#)) in the form of a *concept of secure function* that addresses the spectrum of asset loss and associated consequences. This means proactively planning and designing to prevent the loss of an asset that you are not willing to accept, to be able to minimize the consequences should such a loss occur, and to be in an informed position to reactively recover from the loss when it does happen.

- 1279
- 1280
- 1281 Protection needs are continuously reassessed and adjusted as variances, changes, and trades
- 1282 occur throughout the system life cycle. These include the maturation of the system design and
- 1283 life cycle concepts, improved understanding of the operational environment (e.g., a more
- 1284 thorough understanding of adversities), and changes in understanding the consequences of
- 1285 asset loss. Revisiting protection needs is a necessary part of the iterative nature of systems
- 1286 engineering and with it, systems security engineering—necessary to ensure completeness in
- 1287 understanding the problem space, exploring all feasible solutions, and engineering a trustworthy
- 1288 secure system.

1289 **2.3.8 System Security Viewpoints**

1290 The three predominant views of system security that support trustworthy secure design
1291 considerations for any system type, intended use, and consequence of system failure are *system*
1292 *function*, *security function*, and *life cycle assets*.

1293 Every system is delivered to satisfy stakeholder capability needs. These needs constitute the
1294 *system functions*. Securely satisfying stakeholder capability needs requires the enforcement of
1295 security-driven constraints that combine with the overall design of the system. The security-
1296 driven constraints are provided by the *security functions* of the system. These constraints focus
1297 on the avoidance (i.e., preferred outcome), reduction, and tolerance of susceptibilities, defects,
1298 weaknesses, and flaws in the system that may constitute a vulnerability that can be exploited or
1299 triggered. These vulnerabilities may be within the system's structure or within its behaviors,
1300 including vulnerabilities that counter, defeat, or minimize the ability of the security functions to
1301 effectively satisfy their design intent. Thus, the constraints also enable the synthesis of security
1302 functions into the system in a non-conflicting manner.

1303 *Security functions* are those functions of the system whose sole purpose is to satisfy objectives
1304 to control asset loss (including the loss of intended behavior and outcomes) and the associated
1305 consequences. Security functions are realized by the employment of engineered features and
1306 devices, generally referred to as controls, countermeasures, features, inhibits, mechanisms,
1307 overrides, safeguards, security controls, or security services. Security functions have both
1308 *passive* and *active* aspects:

- 1309 • Passive aspects of security functions do not exhibit behavior. They include the system
1310 architecture and design elements. The passive aspects are part of the system structure and
1311 require consideration in the architecture of the system. For example, the functional
1312 architecture may segment system functions (including security functions) into different
1313 subsystems, reducing the possibility of interference among functions as well as limiting the
1314 propagation of erroneous behavior. Passive aspects inherently reduce the susceptibility of
1315 the system to exposure, hazard, and vulnerability, thereby limiting if not eliminating the
1316 potential for loss scenarios. The employment of passive aspects generally enables greater
1317 confidence in the protection capability of the system.
- 1318 • Active aspects of security functions exhibit behavior (i.e., are functional in nature). The
1319 active aspects are employed or allocated within the system architecture, have a specific
1320 design, and have capabilities and limitations that affect their suitability and effectiveness
1321 relative to their intended use.

1322 *Life cycle assets* are those assets that are associated with the system but are not engineered into
1323 the system or delivered with the system. Their association with the system means that they can
1324 be the direct cause of loss or a conduit/means through which a loss can occur. Life cycle assets
1325 have several types:

- 1326 • Systems that interact with the system of interest in its environment of operation, including
1327 conceptual systems ([Section 2.2.1](#))
- 1328 • Intellectual property in various forms, including proprietary algorithms, technologies, and
1329 technology solutions
- 1330 • Data and information associated with the system

- 1331 • Developmental, manufacturing, fabrication, and production capabilities, systems, and
1332 environment systems and capabilities used to utilize, operate, and sustain the system⁴⁸

1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344

SECURITY FUNCTIONS – PASSIVE AND ACTIVE ASPECTS

As discussed in [Section D.3](#), *passive* security functions (i.e., structure) have certain advantages over *active* security functions due to their greater potential for assurance in achieving objectives. However, both types of functions are needed and are complementary (e.g., a good structure can increase the effectiveness of an active function). Passive and active aspects of security functions factor into trades, as discussed in [Section D.4.4](#). Active security functions also require additional hardware or loads on existing hardware, increasing demands for size, weight, and power (SWaP) and making active functions a challenge for SWaP-restricted systems (e.g., satellites).

1345

1346 2.4 DEMONSTRATING SYSTEM SECURITY

1347 The system security definition (i.e., freedom from those conditions that can cause a loss of
1348 assets with unacceptable consequences) brings an inherently context-sensitive and subjective
1349 nature to assertions or expectations about the system security objectives and the determination
1350 that those objectives have been achieved. The context sensitivity and subjectivity occur because
1351 no individual stakeholder can speak on behalf of all stakeholders regarding the ramifications or
1352 effects of the loss of stakeholder and system assets throughout the system life cycle.

1353 Moreover, system security, as an *emergent property* of the system, is an outcome that results
1354 from and is assessed in terms of the composed results of the system element parts. System
1355 security is not determined relative to an assessment of any one part or collection of parts
1356 without considering the whole.⁴⁹ Therefore, the requirements and associated verification and
1357 validation methods, while necessary, are not sufficient as the basis to deem a system secure.
1358 The requirements and the life cycle concepts informing those requirements must be shown to
1359 be comprehensive and sufficient. What is necessary is the means to address the emergent
1360 property of security across the subjective and often contradicting, competing, and conflicting
1361 needs and beliefs of stakeholders and to do so with a level of confidence that is commensurate
1362 with the asset loss consequences that are to be addressed ([Appendix F](#)).

1363 This is achieved through the type of diligent and targeted reasoning that forms the basis of
1364 assurance cases ([Appendix F](#)). The reasoning considers the system needs and capabilities,
1365 contributing system quantitative and qualitative factors, and how these capabilities and factors

⁴⁸ Examples include software and hardware development tools and suites; modeling and simulation environments and tools; maintenance and diagnostics devices, components, and suites; simulators and test-case scenario generators; and training systems. While these assets are not necessarily within the scope of engineering the system of interest, behaviors and outcomes of these systems have security implications that must be addressed in the secure design of the system of interest. The behaviors and outcomes to consider include how they might directly or indirectly enable, interface, interact, and interoperate with the system of interest.

⁴⁹ An individual function or mechanism can be verified and validated for correctness and for its specific quality and performance attributes. Those results inform the determination of system security but do not substitute for them.

1366 compose in the context of system security to produce an evidentiary base upon which analyses
1367 are conducted. These analyses, in turn, support substantiated and reasoned conclusions that
1368 serve as the basis for consensus among stakeholders.⁵⁰ The ultimate objective is to be able to
1369 claim with sufficient confidence or assurance that the system is *adequately secure* relative to all
1370 stakeholders' objectives, concerns, and associated constraints and to do so in a manner that is
1371 meaningful to stakeholders and that can be recorded, traced, and evolved as variances occur
1372 throughout the system life cycle. There will never be absolute assurance, however, because of
1373 the asymmetry in system security – that is, things can be declared insecure by observation, but
1374 there is no observation that allows one to declare an arbitrary system secure [Herley16].

1375 The scope of conditions relevant to security is specific to the stakeholder needs to be met by the
1376 system. This is also the case for the level of security to be considered acceptable. Absolute
1377 security is not expected to be attainable. Rather, a sufficient level of security is needed to fulfill
1378 protection need priorities. To be *adequately secure*,⁵¹ the system:

- 1379 • Is assessed to meet minimum tolerable levels of security, as determined by analysis,
1380 experience, or a combination of both. Below such levels the system is considered insecure.
- 1381 • Is as secure as reasonably practicable (ASARP); that is, incremental improvement in security
1382 would require an intolerable or disproportionate deterioration of meeting other system
1383 objectives such as those for system performance, would violate system constraints, or
1384 would require unacceptable concessions such as an unacceptable change in the way
1385 operations are performed.

1386 An adequately secure system does not necessarily preclude all of the conditions that can lead to
1387 undesirable consequences. The minimum tolerable levels of security and interpretations of “as
1388 secure as reasonably practicable” may not be fixed over the life of a system. The information
1389 gathered while the system is in use and the lessons learned may inform candidate modifications
1390 that raise the bar on either or both. Figure 8 illustrates the tradeoffs between system security
1391 and the cost, schedule, and technical performance of the system.

1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402

ADEQUATE SECURITY

No system can provide *absolute* security due to the limits of human certainty, the uncertainty that exists in the life cycle of every system, and the constraints of cost, schedule, performance, feasibility, and practicality. As such, trade-offs made routinely across contradictory, competing, and conflicting needs and constraints are optimized to achieve *adequate* security, which reflects a decision made by stakeholders.

⁵⁰ System security requirements development must be iterative with the involvement of stakeholders, regardless of the life cycle model used. Such development spans several life cycle processes as described in [Chapter Three](#). The iterative development of system security requirements is necessary to address the evolution and maturation of the system as it proceeds from concept to design and, subsequently, to its “as-built” forms.

⁵¹ The concept of *adequately secure* is an adaptation of the concept of *adequately safe* from [\[NASA14\]](#).

1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427

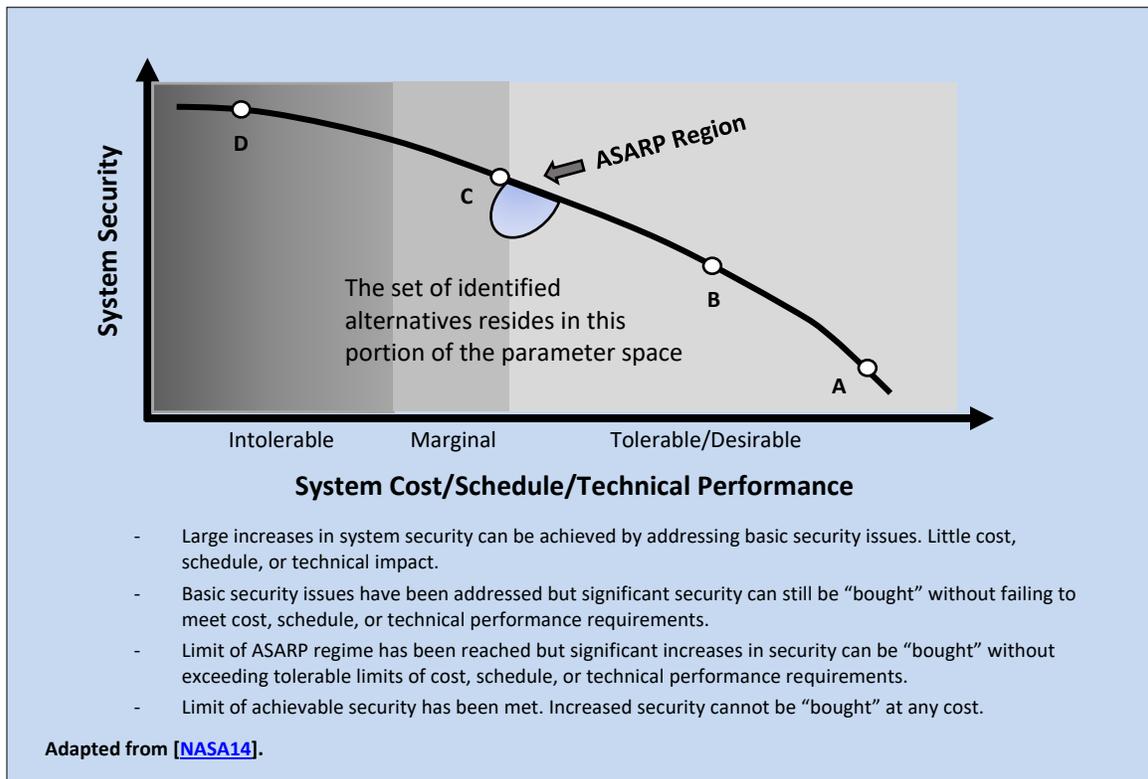


FIGURE 8: SYSTEM SECURITY AND COST/SCHEDULE/TECHNICAL PERFORMANCE

1428 2.5 SYSTEMS SECURITY ENGINEERING FRAMEWORK

1429 The *systems security engineering framework* [McEvilley15] provides a conceptual view of the key
1430 contexts within which systems security engineering activities are conducted. The framework
1431 defines, bounds, and focuses the systems security engineering technical and non-technical
1432 activities and tasks towards the achievement of stakeholder *security objectives* and presents a
1433 coherent, well-formed, evidence-based case that those objectives have been achieved.⁵² The
1434 framework is independent of system type and engineering or acquisition process model and is
1435 not to be interpreted as a sequence of flows or process steps but rather as a set of interacting
1436 contexts, each with its own checks and balances. The systems security engineering framework
1437 emphasizes an integrated, holistic security perspective across all stages of the system life cycle
1438 and is applied to satisfy the milestone objectives of each life cycle stage.

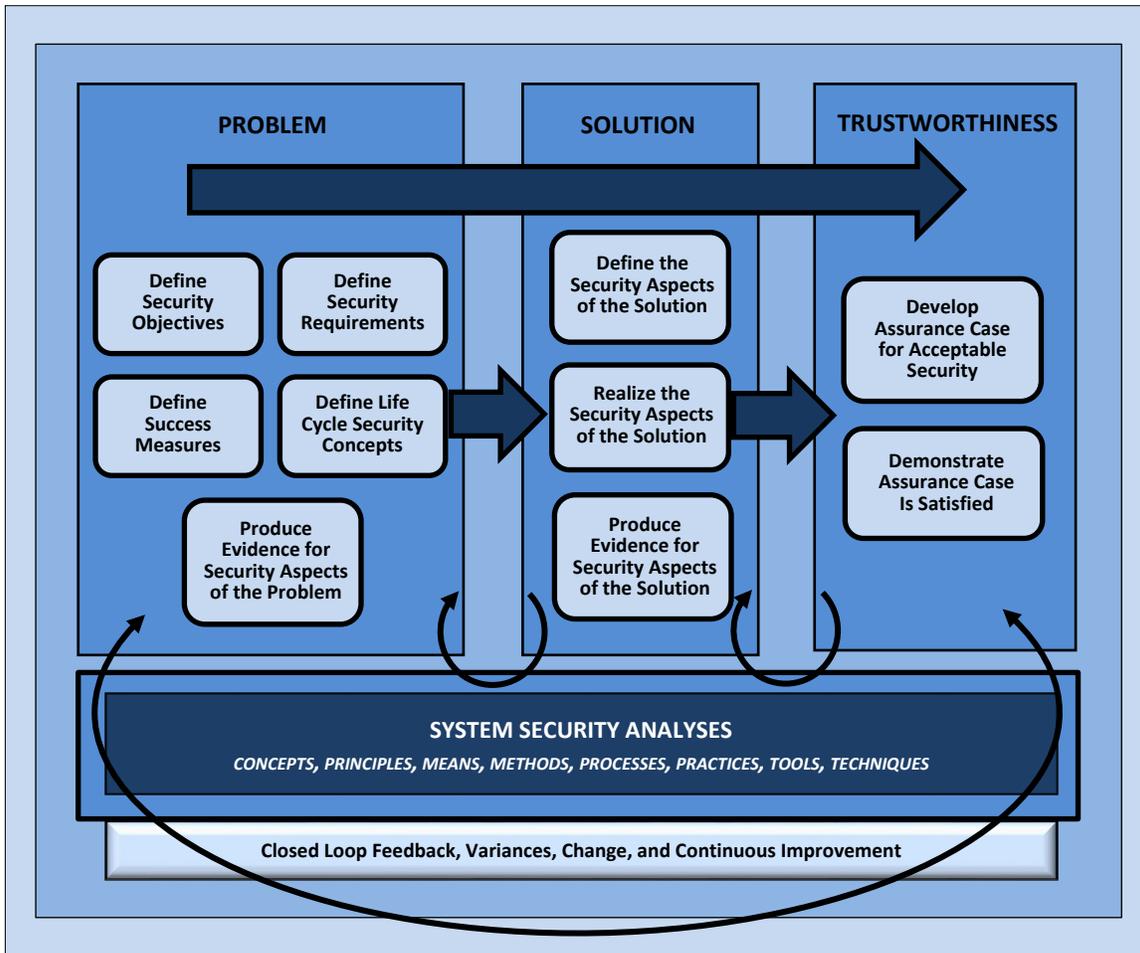
1439 The framework defines three contexts for conducting systems security engineering activities: (1)
1440 the *problem* context, (2) the *solution* context, (3) and the *trustworthiness* context. Establishing
1441 the three contexts helps to ensure that the engineering of a system is driven by a sufficiently
1442 complete understanding of the problem. This understanding is described in a set of stakeholder
1443 security objectives that reflect protection needs and security concerns instead of by security
1444 solutions brought forth in the absence of consideration of the entire problem space and its
1445 associated constraints. Moreover, there is explicit focus and a set of activities to demonstrate

⁵² Adapted from [NASA11].

1446 the worthiness of the solution in providing adequate security across competing and often
 1447 conflicting constraints. While the framework appears to follow a *sequential* execution across the
 1448 three contexts, it is actually implemented in an *iterative* manner within the stages of the system
 1449 life cycle and is guided and informed by system analyses ([Section 3.4.6](#)). The transition from
 1450 stage to stage in the life cycle is controlled by decision gates. Iteration facilitates refinement of
 1451 the problem statement, proposed solutions, and trustworthiness objectives.

1452 Figure 9 illustrates the systems security engineering framework and its key components.

1453
 1454
 1455
 1456
 1457
 1458
 1459
 1460
 1461
 1462
 1463
 1464
 1465
 1466
 1467
 1468
 1469
 1470
 1471
 1472
 1473
 1474
 1475
 1476
 1477
 1478
 1479



1480

FIGURE 9: SYSTEMS SECURITY ENGINEERING FRAMEWORK

1481 The contexts of the systems security engineering framework share a common foundational base
 1482 of *system security analyses*, including *system analyses* with security interpretations of resulting
 1483 data. System security analyses produce data to support engineering and stakeholder decision-
 1484 making. Such analyses are differentiated for application within the problem, solution, and
 1485 trustworthiness contexts and routinely employ concepts, principles, means, methods, processes,
 1486 practices, tools, and techniques. System security analyses:

- 1487 • Provide relevant data and technical interpretations of system issues from the system
 1488 security perspective

- 1489 • Are differentiated in their application to align with the scope and objectives of where they
1490 are applied within the systems security engineering framework
- 1491 • Are performed with a level of fidelity, rigor, and formality to produce data with a level of
1492 confidence that matches the assurance required by the stakeholders and engineering team
1493 (see [Appendix F](#))

1494 System security analyses address important topic areas related to systems security engineering.
1495 These areas include architecture, assurance, behavior, cost, criticality, design, effectiveness,
1496 emergence, exposure, fit-for-purpose, life cycle concepts, penetration resistance, performance
1497 (including security performance), protection needs, privacy, requirements, resilience, risk,
1498 strength of function, security objectives, threats, trades, uncertainty, vulnerability, verification,
1499 and validation.

1500 The systems security engineering framework includes a *closed loop feedback* for interactions
1501 among and between the three framework contexts and the requisite system security analyses to
1502 continuously identify and address variances as they are introduced into the engineering effort.
1503 The feedback loop also helps to achieve continuous process improvement for the system,
1504 including viewing the outputs of one life cycle phase (i.e., the “solution” to the phase) as the
1505 inputs to the next phase (i.e., the “problem” for the next phase).

1506 **2.5.1 The Problem Context**

1507 The *problem context* defines the basis for an acceptably and adequately secure system given the
1508 stakeholder’s mission, capability, performance needs and concerns; the constraints imposed by
1509 stakeholder concerns related to cost, schedule, performance, risk, and loss tolerance; and other
1510 constraints associated with life cycle concepts for the system. The problem context enables the
1511 engineering team to focus on acquiring as complete an understanding of the stakeholder
1512 problem as practical, exploring all feasible solution class options, and selecting the solution class
1513 option or options to be pursued. The problem context includes:

- 1514 • Determining life cycle security concepts⁵³
- 1515 • Defining security objectives
- 1516 • Defining security requirements
- 1517 • Determining measures of success

1518 The security objectives are foundational in that they establish and scope what it means to be
1519 *adequately secure* in terms of protection against asset loss and the consequences of such loss.

⁵³ The term *life cycle security concept* refers to the processes and activities associated with the system throughout the life cycle (from concept development through retirement) with specific security considerations. It is an extension of the *concept of operation* and includes the processes and activities related to development, prototyping, assessment of alternative solutions, training, logistics, maintenance, sustainment, evolution, modernization, disposal, and refurbishment. Each life cycle concept has one or more security considerations and constraints that must be fully integrated into the life cycle to ensure that the system security objectives can be met. Life cycle security concepts include those applied during acquisition and program management. Life cycle security concepts can affect such things as Requests for Information, Requests for Proposal, Statements of Work, source selections, development and test environments, operating environments, supply chains, supporting infrastructures, distribution, logistics, maintenance, training, clearances, and background checks.

1520 The security objectives have associated measures of success. The measures of success constitute
1521 specific and measurable criteria relative to operational performance measures and stakeholder
1522 concerns. Measures of success include both strength of protection and level of assurance or
1523 confidence in the protection capability that has been engineered. These measures influence the
1524 development of security requirements and assurance claims.

1525 Life cycle security concepts are the processes, methods, and procedures associated with the
1526 system throughout its life cycle and provide distinct contexts for interpretation of system
1527 security. These concepts also serve to scope and bound attention in addressing protection
1528 needs and for broader security-informing considerations and constraints. Protection needs are
1529 determined based on the security objectives, life cycle concepts, and stakeholder concerns. The
1530 protection needs are subsequently transformed into stakeholder security requirements and
1531 associated constraints, and the measures needed to validate that all requirements have been
1532 met. A well-defined and stakeholder-validated problem definition and context provides the
1533 foundation for all systems engineering and systems security engineering and supporting
1534 activities.

1535 The problem context may be interpreted within a life cycle phase as being informed by solutions
1536 from earlier life cycle stages, thereby providing a more accurate statement of the problem and
1537 its associated constraints. For example, the stakeholder requirements may be the “solution” of
1538 an early life cycle phase which then constrains activities completed in later life cycle stages.

1539 **2.5.2 The Solution Context**

1540 The *solution context* transforms stakeholder security requirements into derived requirements
1541 for the system, subsystem, or system element, as applicable. It also addresses the security
1542 architecture, design, and related aspects necessary to realize a system that satisfies those
1543 requirements and, lastly, produces sufficient evidence to demonstrate that those requirements
1544 have been satisfied.⁵⁴ The solution context is based on a balanced proactive and reactive system
1545 security protection strategy⁵⁵ that exercises control over events, conditions, asset loss, and the
1546 consequence of loss to the degree possible, practicable, and acceptable to stakeholders. The
1547 solution context includes:

- 1548 • Defining the security aspects of the solution
- 1549 • Realizing the security aspects of the solution
- 1550 • Producing evidence for the security aspects of the solution

1551 The security aspects of the solution include the development of a system protection strategy;
1552 allocated and derived security requirements; security architecture views and viewpoints;
1553 security design; security aspects, capabilities, and limitations in the system life cycle procedures;
1554 and security performance verification measures. The security aspects of the solution are realized

⁵⁴ Security constraints are transformed and incorporated into system design requirements with metadata-tagging to identify security relevance.

⁵⁵ The system security protection strategy is consistent with the overall *concept of secure function*. The concept of secure function, defined during the problem context, constitutes a strategy for a proactive and reactive protection capability throughout the system life cycle ([Section D.2](#)). The strategy has the objective to provide freedom from specific concerns associated with asset loss and loss consequences.

1555 during the implementation of the system design in accordance with the system architecture and
1556 in satisfaction of the security requirements. The evidence associated with the security aspects of
1557 the solution is obtained with a fidelity and rigor influenced by the level of assurance⁵⁶ targeted
1558 by the security objectives. Assurance evidence is obtained from standard systems engineering
1559 verification methods (e.g., analysis, demonstration, inspection, testing, and evaluation) and
1560 complementary validation methods applied against the stakeholder requirements. Application
1561 of the solution context may be interpreted to provide a part of the solution, constraining the
1562 next iteration of the problem context.

1563 **2.5.3 The Trustworthiness Context**

1564 The *trustworthiness context* is a decision-making context that provides an evidence-based
1565 demonstration, through reasoning, that the system of interest is deemed trustworthy based on
1566 a set of claims derived from security objectives. The trustworthiness context consists of:

- 1567 • Developing and maintaining the assurance case
- 1568 • Demonstrating that the assurance case is satisfied

1569 The trustworthiness context is grounded in the concept of an *assurance case*. An assurance case
1570 is a well-defined and structured set of arguments and a *body of evidence* showing that a system
1571 satisfies specific claims.⁵⁷ Assurance cases provide reasoned, auditable artifacts that support the
1572 contention that a top-level claim or set of claims is satisfied, including systematic argumentation
1573 and underlying evidence and explicit assumptions that support the claims [ISO 15026-2]. The
1574 claims may build from subclaims. For a given life cycle stage, one outcome may sufficiently
1575 satisfy a subclaim or set of subclaims, such as a subclaim that stakeholder requirements are
1576 sufficiently comprehensive to support an overall claim that the realized system is adequately
1577 secure.

1578 An assurance case is used to demonstrate that a system exhibits some complex emergent
1579 property, such as safety, security, resilience, reliability, or survivability. An effective security
1580 assurance case contains foundational security claims that are derived from stakeholder security
1581 objectives, credible and relevant evidence that substantiates the claims, and valid arguments
1582 that relate the various evidence to the supported security claims. The result provides a
1583 compelling statement that adequate security has been achieved and driven by stakeholder
1584 needs and expectations.

1585 Assurance cases typically include supporting information, such as assumptions, constraints, and
1586 any inferences that can affect the reasoning process. Subsequent to the development of the
1587 assurance case, analyses by subject-matter experts determine that all security claims are
1588 substantiated by the evidence produced and the arguments that relate the evidence to the
1589 claims. For maximum effectiveness, the assurance cases must be maintained in response to
1590 variances throughout the engineering effort.

1591 The specific form of an assurance case and the level of rigor and formality in acquiring the
1592 evidence required by the assurance case is a trade space consideration. It involves the target

⁵⁶ *Assurance* is the measure of confidence associated with a given requirement. As the level of assurance increases, so does the scope, depth, and rigor associated with the methods and analyses conducted ([Appendix F](#)).

⁵⁷ Software Engineering Institute, Carnegie Mellon University.

1593 (desired) level of assurance, the nature of the consequences for which assurance is sought, and
1594 the size and complexity of the dimensions that factor into the determination of trustworthiness.
1595 The assurance case is an *engineering construct* and must be managed accordingly to ensure that
1596 the effort expended to produce the evidence is justified by the need for that evidence in making
1597 the trustworthiness determination. The assurance claims are the key trustworthiness factor and
1598 are developed from the security objectives and associated measures of success, independent of
1599 the realization of the system and its supporting evidence.

1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611

SYSTEMS SECURITY ENGINEERING FRAMEWORK – WHY IT MATTERS

Establishing the problem, solution, and trustworthiness contexts as key components of a systems security engineering framework helps ensure that the *security* of a system is based on achieving a sufficiently complete understanding of the problem as defined by a set of stakeholder security objectives, security concerns, protection needs, and security requirements. This understanding is essential in order to develop effective security solutions – that is, a system that is sufficiently trustworthy and adequately secure to protect stakeholder’s assets in terms of loss and the associated consequences.

1612 CHAPTER THREE

1613 SYSTEM LIFE CYCLE PROCESSES

1614 SYSTEMS SECURITY IN SYSTEM LIFE CYCLE PROCESSES

1615 This chapter describes the considerations and contributions to the system life cycle
 1616 processes in [ISO 15288] to produce the behaviors and outcomes that are necessary to
 1617 achieve trustworthy secure systems. The system life cycle processes are grouped into the
 1618 following families: [Agreement Processes](#), [Organizational Project-Enabling Processes](#), [Technical](#)
 1619 [Management Processes](#), and [Technical Processes](#). Figure 10 lists the processes and illustrates
 1620 their application across the stages of the system life cycle.

1621

1622

1623

1624

1625

1626

1627

1628

1629

1630

1631

1632

1633

1634

1635

1636

1637

1638

1639

1640

1641

1642

1643

1644

1645

1646

1647

1648

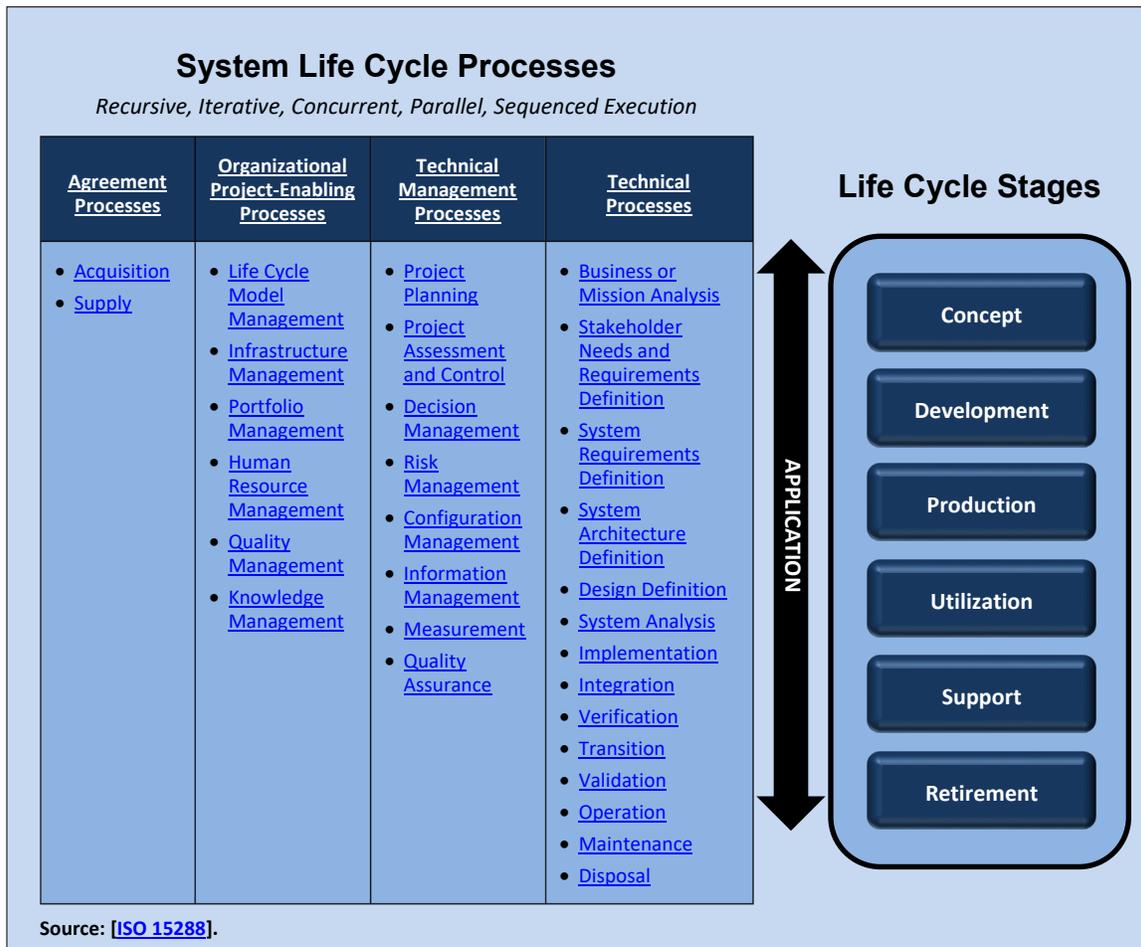


FIGURE 10: SYSTEM LIFE CYCLE PROCESSES AND LIFE CYCLE STAGES

1649 The security-related considerations and contributions to the system life cycle are provided as
 1650 systems security engineering tasks. The tasks are aligned with the engineering viewpoints of the
 1651 life cycle processes and are based on the foundational security and trust principles and concepts
 1652 described in [Chapter Two](#), [Appendix C](#), [Appendix D](#), [Appendix E](#), and [Appendix F](#). The tasks use
 1653 and leverage the principles, concepts, terms, and practices of systems engineering to facilitate
 1654 consistency in their application as part of a systems engineering effort.

1655 This publication is not intended to be prescriptive in nature. The processes, activities, and tasks
 1656 are to be applied as needed. They are not dependent on, oriented to, or presumed to be used in
 1657 any particular system development methodology. By design, the processes, activities, and tasks
 1658 can be applied concurrently, iteratively, or recursively: (1) at any level in the structural hierarchy
 1659 of a system, (2) with the appropriate fidelity and rigor, and (3) at any stage in the system life
 1660 cycle in accordance with acquisition, systems engineering, or other process models.⁵⁸ The
 1661 application of the processes, activities, or tasks relies on the skill, expertise, and experience of
 1662 the *practitioner*.

1663 The system life cycle processes are intended to be tailored to achieve optimized and efficient
 1664 results.⁵⁹ Tailoring can include:

- 1665 • Applying the system life cycle processes to an organization’s preferred development model
- 1666 • Ordering or sequencing the activities and tasks in the system life cycle processes
- 1667 • Accomplishing the outcomes in ways that do not strictly adhere to the presentation of the
 1668 processes in this publication
- 1669 • Supplementing the activities and tasks to achieve specific outcomes

1670 Tailoring may be motivated by the stage of the system life cycle; the size, scope, and complexity
 1671 of the system; specialized requirements; or the need to accommodate specific technologies,
 1672 methods, or techniques used to develop the system. Tailoring may be appropriate when the
 1673 activities of different processes overlap or interact in ways not defined in this publication.⁶⁰
 1674 Tailoring the system life cycle processes allows the engineering team to:

- 1675 • Optimize the application of the processes in response to technological, programmatic,
 1676 acquisition, process, procedural, system life cycle stage, or other objectives and constraints
- 1677 • Allow for concurrent application of the processes by sub-teams focused on different parts of
 1678 the same engineering effort
- 1679 • Facilitate the application of the processes to conform with a variety of system development
 1680 methodologies, processes, and models (e.g., agile, spiral, waterfall) that could be used on a
 1681 single engineering effort

⁵⁸ Systems engineering and system life cycle processes do not map explicitly to specific stages in the system life cycle. Rather, the processes may occur in one or more stages of the life cycle depending on the particular process and the conditions associated with the systems engineering effort. For example, the [Maintenance](#) process includes activities that plan the maintenance strategy such that it is possible to identify constraints on the system design necessitated by how the maintenance will be performed once the system is operational. Therefore, the *Maintenance Process* is conducted prior to or concurrent with the [Design Definition](#) process.

⁵⁹ Tailoring can occur as part of the project planning process at the start of the systems-engineering effort or in an ad hoc manner at any time during the engineering effort when situations and circumstances so dictate. Understanding the fundamentals of systems security engineering (i.e., the science underpinning the discipline) helps to inform the tailoring process whenever it occurs during the system life cycle. The INCOSE Systems Engineering Handbook provides additional guidance on how to tailor the systems engineering processes [[INCOSE14](#)].

⁶⁰ For example, the engineering team may need to initiate a system modification in a relatively short period to respond to a serious security incident. In this situation, the team may only informally consider each process rather than formally executing each process. It is essential that any system modifications continue to support stakeholder protection needs. Without a system-level perspective, modifications could fix one problem while introducing others.

- 1682 • Accommodate the need for unanticipated or other event-driven execution of processes to
1683 resolve issues and respond to changes that occur during the engineering effort

1684 While the life cycle processes from [\[ISO 15288\]](#) are addressed in terms of systems security
1685 engineering, the activities and tasks in this publication are neither a restatement of those
1686 processes nor do they constitute a one-for-one mapping to those processes. This publication
1687 focuses on specific contributions to the process, and the activities and tasks are titled to reflect
1688 the security contributions. In some cases, activities and tasks have been added to address the
1689 range of outcomes appropriate for the achievement of trustworthy, secure system objectives.

1690 The descriptions of the system life cycle processes assume that sufficient time, funding, and
1691 human and material resources are available to ensure a complete application of the processes
1692 within the systems engineering effort. The life cycle processes represent the “standard of
1693 excellence” within which appropriate tailoring is accomplished to achieve realistic, optimal, and
1694 cost-effective results within the constraints imposed on the engineering team.

1695 Each of the system life cycle processes contains a set of *activities* and *tasks* that produce a set of
1696 security-focused *outcomes*.⁶¹ These outcomes combine to deliver a system and corresponding
1697 body of evidence that serve as the basis to:

- 1698 • Substantiate the security and the trustworthiness of the system
- 1699 • Determine security risk across stakeholder concerns and with respect to the use of the
1700 system in support of mission or business objectives
- 1701 • Help stakeholders decide which operational constraints are necessary to mitigate security
1702 risk
- 1703 • Provide inputs to other processes associated with delivering the system
- 1704 • Support the system throughout the stages of its life cycle⁶²

1705 Each system life cycle process description has the following sections:

- 1706 • **Life Cycle Purpose:** Describes the goals of performing the process [\[ISO 15288\]](#).
- 1707 • **Security Purpose:** Establishes what the process achieves from the security standpoint.
- 1708 • **Security Outcomes:** Expresses the security-related observable results expected from the
1709 successful performance of the process and the data generated by the process.⁶³

⁶¹ Outcomes from the systems engineering processes inform other systems engineering processes and can also serve to inform processes external to the engineering effort, such as the organizational life cycle processes of stakeholders and certification, authorization, or regulatory processes.

⁶² The comprehensiveness, depth, fidelity, credibility, and relevance of the body of evidence are factors in helping to achieve the level of assurance sought by stakeholders. The objective is to have a body of evidence that is sufficient to convince stakeholders that their assurance needs are satisfied. The assurance level is an engineering trade space factor that must be planned for and executed with the appropriate fidelity and rigor. Assurance considerations can affect system cost and development schedule.

⁶³ The data and information generated during the execution of a process is not necessarily produced in the form of a document. Such data and information can be conveyed in the most effective manner as set forth by stakeholders or the engineering team. Data and information produced during a particular process may flow into a subsequent process or support other processes that are associated with the systems security engineering process.

- 1710 • **Security Activities:** Provides a set of cohesive security-related tasks that support
 1711 achievement of the security outcomes for the process. The tasks are accomplished
 1712 cooperatively within and across various roles of the organization, inclusive of systems
 1713 security engineering. While this publication focuses on the scope and responsibility of
 1714 systems security engineering, it is not the case that all aspects of every task are fulfilled by
 1715 systems security engineering.

1716 The following naming convention is established for the system life cycle processes. Each process
 1717 is identified by a two-character designation (e.g., BA is the official designation for the [Business](#)
 1718 [or Mission Analysis](#) process). Table 3 lists the system life cycle processes and their associated
 1719 two-character designators.

1720 **TABLE 3: PROCESS NAMES AND DESIGNATORS**

ID	PROCESS	ID	PROCESS
AQ	Acquisition	MS	Measurement
AR	System Architecture Definition	OP	Operation
BA	Business or Mission Analysis	PA	Project Assessment and Control
CM	Configuration Management	PL	Project Planning
DE	Design Definition	PM	Portfolio Management
DM	Decision Management	QA	Quality Assurance
DS	Disposal	QM	Quality Management
HR	Human Resource Management	RM	Risk Management
IF	Infrastructure Management	SA	System Analysis
IM	Information Management	SN	Stakeholder Needs and Requirements Definition
IN	Integration	SP	Supply
IP	Implementation	SR	System Requirements Definition
KM	Knowledge Management	TR	Transition
LM	Life Cycle Model Management	VA	Validation
MA	Maintenance	VE	Verification

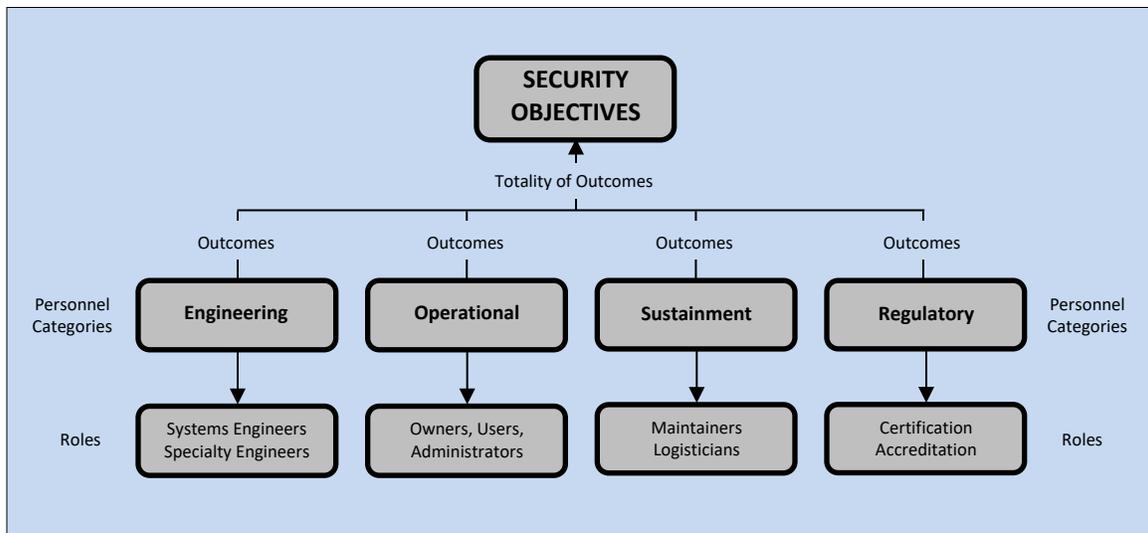
1721
 1722 The security activities and tasks in each system life cycle process are uniquely identified using a
 1723 two-character designation plus a numerical designation. For example, the first activity in the
 1724 [Stakeholder Needs and Requirements Definition](#) process is designated [SN-1](#). The first two tasks
 1725 within SN-1 are designated [SN-1.1](#) and [SN-1.2](#), respectively. The identification of the activities
 1726 and tasks within each system life cycle process provides for precise referencing and traceability
 1727 among the process elements. Task descriptions may contain a *notes* section that provides
 1728 additional information on considerations relevant to the successful execution of that task. A
 1729 *references* section provides a list of pertinent publications related to the activity and is a source
 1730 of content for additional information. Finally, a *related publications* section provides a list of
 1731 documents that are related to the topic being addressed in the activity. The remaining sections
 1732 in this chapter describe the security contributions, considerations, and outcomes for the 30
 1733 system life cycle processes defined in [\[ISO 15288\]](#).

1734 Finally, the outcomes described in this publication are achieved by personnel and machines.
 1735 Personnel conduct activities and tasks, such as those defined in the [\[ISO 15288\]](#) system life cycle
 1736 processes, to produce outcomes that achieve the defined security objectives. There is no single
 1737 personnel role that is responsible to produce all of the outcomes stated in the system life cycle

1738 processes (i.e., the life cycle processes are not role-specific). Thus, there may be multiple roles
 1739 that contribute to a specific outcome.

1740 This publication describes the engineering *considerations*, not the engineering responsibilities,
 1741 to produce the specified outcomes. Those responsibilities reside with the organizations using
 1742 the guidance in this publication. This facilitates maximum flexibility for organizations to define,
 1743 combine, and allocate responsibility to support the execution of the life cycle processes. There is
 1744 no expectation that any particular role or title is assigned any specific responsibility or possesses
 1745 any specific authority. Figure 11 provides an example of the types of personnel and roles that
 1746 support the system life cycle processes. Each personnel category has a scope of authority,
 1747 control, and responsibility and a variety of roles that collectively achieve the outcomes for the
 1748 category. Collectively, the outcomes produced across all categories achieve the defined security
 1749 objectives.

1750
 1751
 1752
 1753
 1754
 1755
 1756
 1757
 1758
 1759
 1760
 1761
 1762
 1763



1764 **FIGURE 11: TYPES OF PERSONNEL AND ROLES THAT SUPPORT LIFE CYCLE PROCESSES**

1765 **3.1 AGREEMENT PROCESSES**

1766 This section contains the *Agreement Processes* from [\[ISO 15288\]](#) with security-related
 1767 considerations and contributions.

1768 **3.1.1 Acquisition**

1769 The purpose of the *Acquisition* process is to obtain a product or service in accordance with the
 1770 acquirer's requirements.

1771 [\[ISO 15288\]](#) Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

1772 **3.1.1.1 Security Purpose**

- 1773 • To obtain a product or service in accordance with the acquirer's security requirements

1774 **3.1.1.2 Security Outcomes**

- 1775 • A request for supply includes security criteria.

- 1776 • One or more suppliers are selected that satisfy the security criteria.
- 1777 • An agreement containing security criteria is established between the acquirer and the
1778 supplier.
- 1779 • A product or service complying with the security criteria in the agreement is accepted.
- 1780 • The security aspects of acquirer obligations defined in the agreement are satisfied.

1781 3.1.1.3 Security Activities and Tasks

1782 AQ-1 PREPARE FOR THE ACQUISITION

1783 **AQ-1.1** Define the security aspects of the strategy for how the acquisition will be conducted.

1784 *Note:* This strategy describes or references the life cycle model, security risks and issues
1785 mitigation, a schedule of security-relevant milestones, protection of acquirer and supplier assets,
1786 and security-relevant selection criteria if the supplier is external to the acquiring organization. It
1787 also includes key security drivers and security-relevant characteristics of the acquisition, such as
1788 responsibilities and liabilities; specific models, methods, or processes; formality; level of
1789 criticality; and security's priority within relevant trade-off factors.

1790 **AQ-1.2** Prepare a request for a product or service that includes the security requirements.

1791 *Note:* The request includes security criteria for the business practices with which the supplier is
1792 to comply, a list of bidders with adequate security qualifications, and the security criteria that
1793 will be used to select the supplier.

1794 **References:** [\[ISO 15288, Section 6.1.1.3 a\)\]](#); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
1795 [15026-4\]](#); [\[ISO 27036-1\]](#); [\[ISO 27036-2\]](#); [\[ISO 27036-3\]](#).

1796 **Related Publications:** [\[ISO 12207, Section 6.1.1.3.1\]](#); [\[ISO 21827\]](#).

1797 AQ-2 ADVERTISE THE ACQUISITION AND SELECT THE SUPPLIER

1798 **AQ-2.1** Securely communicate the request for the supply of a product or service to potential
1799 suppliers.

1800 **AQ-2.2** Select one or more suppliers that meet the security criteria.

1801 **References:** [\[ISO 15288, Section 6.1.1.3 b\)\]](#); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
1802 [15026-4\]](#); [\[ISO 27036-1\]](#); [\[ISO 27036-2\]](#); [\[ISO 27036-3\]](#).

1803 **Related Publications:** [\[ISO 12207, Sections 6.1.1.3.2, 6.1.1.3.3\]](#); [\[ISO 21827\]](#).

1804 AQ-3 ESTABLISH AND MAINTAIN AN AGREEMENT

1805 **AQ-3.1** Develop and approve an agreement with the supplier that includes security acceptance
1806 criteria.

1807 *Note:* This agreement ranges in formality from a written contract to a verbal agreement.
1808 Appropriate to the level of formality, the agreement establishes security requirements, secure
1809 development and delivery milestones, security verification, security validation and security
1810 aspects of acceptance conditions, security aspects of process requirements (e.g., configuration
1811 management, risk management, and measurement), and security aspects of handling of data
1812 rights and intellectual property so that both parties of the agreement understand the basis for
1813 executing the agreement. The security aspects of the agreement also include application of all of
1814 the above to subcontractors and other supporting organizations to the supplier.

1815 **AQ-3.2** Identify necessary security-relevant changes to the agreement.

- 1816 **AQ-3.3** Evaluate the security impact of changes to the agreement.
- 1817 *Note:* The basis for the agreement change may or may not be security related. However, there
1818 may be security-related impact regardless of the basis for the change.
- 1819 **AQ-3.4** Update the security criteria in the agreement with the supplier, as necessary.
- 1820 **References:** [[ISO 15288](#), Section 6.1.1.3 c)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
1821 [15026-4](#)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].
- 1822 **Related Publications:** [[ISO 12207](#), Section 6.1.1.3.4]; [[ISO 21827](#)].
- 1823 **AQ-4** MONITOR THE AGREEMENTS
- 1824 **AQ-4.1** Assess the execution of the security aspects of the agreement.
- 1825 *Note:* This includes confirmation that all parties are meeting their security-relevant
1826 responsibilities according to the agreement.
- 1827 **AQ-4.2** Securely provide data needed by the supplier, and resolve issues in a timely manner.
- 1828 **References:** [[ISO 15288](#), Section 6.1.1.3 d)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].
- 1829 **Related Publications:** [[ISO 12207](#), Section 6.1.1.3.5]; [[ISO 21827](#)].
- 1830 **AQ-5** ACCEPT THE PRODUCT OR SERVICE
- 1831 **AQ-5.1** Confirm that the delivered product or service complies with the security aspects of the
1832 agreement.
- 1833 **AQ-5.2** Securely provide payment or other agreed consideration.
- 1834 **AQ-5.3** Accept the product or service from the supplier or other party, as directed by the
1835 security criteria in the agreement.
- 1836 **AQ-5.4** Close the agreement in accordance with agreement security criteria.
- 1837 **References:** [[ISO 15288](#), Section 6.1.1.3 e)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].
- 1838 **Related Publications:** [[ISO 12207](#), Section 6.1.1.3.6]; [[ISO 21827](#)].
- 1839 **3.1.2 Supply**
- 1840 The purpose of the *Supply* process is to provide an acquirer with a product or service that meets
1841 agreed requirements.
- 1842 [[ISO 15288](#)] Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.
- 1843 **3.1.2.1 Security Purpose**
- 1844 • To provide an acquirer with a product or service that meets agreed security requirements
- 1845 **3.1.2.2 Security Outcomes**
- 1846 • A response to the acquirer's request addresses the acquirer's security requirements.
- 1847 • An agreement established between the acquirer and supplier includes security
1848 requirements.
- 1849 • A product or service that satisfies the acquirer's security requirements is provided.
- 1850 • Supplier security obligations defined in the agreement are satisfied.

- 1851 • Responsibility for the acquired product or service, as directed by the agreement, is securely
1852 transferred.

1853 3.1.2.3 Security Activities and Tasks

1854 SP-1 PREPARE FOR THE SUPPLY

1855 **SP-1.1** Identify the security aspects of an acquirer's need for a product or service.

1856 **SP-1.2** Define the security aspects of the supply strategy.

1857 *Note:* This strategy describes or references the security aspects of the life cycle model, risks and
1858 issues mitigation, and a schedule of security-relevant milestones. It also includes key security-
1859 relevant drivers and characteristics of the acquisition such as responsibilities and liabilities,
1860 specific security-related models, security-relevant methods or processes, level of criticality,
1861 formality, and priority of relevant trade-off factors.

1862 **References:** [ISO 15288, Section 6.1.2.3 a)]; [ISO 15026-1]; [ISO 15026-2]; [ISO 15026-3]; [ISO
1863 15026-4]; [ISO 27036-1]; [ISO 27036-2]; [ISO 27036-3].

1864 **Related Publications:** [ISO 12207, Section 6.1.2.3.1]; [ISO 21827].

1865 SP-2 RESPOND TO A REQUEST FOR SUPPLY OF PRODUCTS OR SERVICES

1866 **SP-2.1** Evaluate a request for a product or service to determine the security-relevant feasibility
1867 and how to respond.

1868 **SP-2.2** Prepare a response that satisfies the security criteria in the solicitation.

1869 **References:** [ISO 15288, Section 6.1.2.3 b)]; [ISO 15026-1]; [ISO 15026-2]; [ISO 15026-3]; [ISO
1870 15026-4]; [ISO 27036-1]; [ISO 27036-2]; [ISO 27036-3].

1871 **Related Publications:** [ISO 12207, Section 6.1.2.3.2]; [ISO 21827].

1872 SP-3 ESTABLISH AND MAINTAIN AN AGREEMENT

1873 **SP-3.1** Negotiate and approve an agreement with the acquirer that includes security
1874 acceptance criteria.

1875 *Note 1:* This includes configuration management, risk reporting, reporting of security measures,
1876 and security measure analysis; security requirements; secure development; security verification;
1877 security validation; security acceptance procedures and criteria; regulatory body acceptance,
1878 authorization, and approval; procedures for transport, handling, delivery, and storage; security
1879 and privacy protections and restrictions on the use, dissemination, and destruction of data,
1880 information, and intellectual property; security-relevant exception-handling procedures and
1881 criteria; agreement change management procedures; and agreement termination procedures.

1882 *Note 2:* The security aspects of the agreement also include the application of all of the above to
1883 the plans for use of subcontractors.

1884 **SP-3.2** Identify necessary security-relevant changes to the agreement.

1885 **SP-3.3** Evaluate the security impact of necessary changes to the agreement.

1886 *Note:* The basis for the agreement change may or may not be security related. However, there
1887 may be security-related impact regardless of the basis for the change. A security-related
1888 evaluation of the needed change identifies any security relevance and determines impact in
1889 terms of plans, schedule, cost, technical capability, quality, assurance, and trustworthiness.

1890 **SP-3.4** Update the security criteria in the agreement with the acquirer, as necessary.

1891 **References:** [\[ISO 15288](#), Section 6.1.2.3 c)]; [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
1892 [15026-4\]](#); [\[ISO 27036-1\]](#); [\[ISO 27036-2\]](#); [\[ISO 27036-3\]](#).

1893 **Related Publications:** [\[ISO 12207](#), Section 6.1.2.3.3]; [\[ISO 21827\]](#).

1894 **SP-4 EXECUTE THE AGREEMENT**

1895 **SP-4.1** Execute the security aspects of the agreement according to established project plans.

1896 *Note:* A supplier sometimes adopts or agrees to use acquirer processes, including security-
1897 relevant processes.

1898 **SP-4.2** Assess the execution of the security aspects of the agreement.

1899 *Note:* This includes confirmation that all parties are meeting their security responsibilities
1900 according to the agreement.

1901 **References:** [\[ISO 15288](#), Section 6.1.2.3 d)]; [\[ISO 27036-1\]](#); [\[ISO 27036-2\]](#); [\[ISO 27036-3\]](#).

1902 **Related Publications:** [\[ISO 12207](#), Section 6.1.2.3.4]; [\[ISO 21827\]](#).

1903 **SP-5 DELIVER AND SUPPORT THE PRODUCT OR SERVICE**

1904 **SP-5.1** Deliver the product or service in accordance with the agreement security criteria.

1905 **SP-5.2** Provide security assistance to the acquirer, per the agreement.

1906 **SP-5.3** Securely accept and acknowledge payment or other agreed consideration.

1907 **SP-5.4** Transfer the product or service to the acquirer or other party as directed by the security
1908 requirements in the agreement.

1909 *Note:* This includes the transfer of hardware, software, and sensitive, proprietary, and classified
1910 information.

1911 **SP-5.5** Close the agreement in accordance with the agreement security criteria.

1912 **References:** [\[ISO 15288](#), Section 6.1.2.3 e)]; [\[ISO 27036-1\]](#); [\[ISO 27036-2\]](#); [\[ISO 27036-3\]](#).

1913 **Related Publications:** [\[ISO 12207](#), Section 6.1.2.3.5]; [\[ISO 21827\]](#).

1914 **3.2 ORGANIZATIONAL PROJECT-ENABLING PROCESSES**

1915 This section contains the *Organizational Project-Enabling Processes* from [\[ISO 15288\]](#) with
1916 security-related considerations and contributions.

1917 **3.2.1 Life Cycle Model Management**

1918 The purpose of the *Life Cycle Model Management* process is to define, maintain, and help
1919 ensure the availability of policies, life cycle processes, life cycle models, and procedures for use
1920 by the organization with respect to the scope of this International Standard.

1921 [\[ISO 15288\]](#) Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

1922 **3.2.1.1 Security Purpose**

- 1923 • To help ensure that security needs and considerations are incorporated in policies, life cycle
1924 processes, life cycle models, and procedures used by the organization

1925 **3.2.1.2 Security Outcomes**

- 1926 • Security considerations are captured in organizational policies and procedures for the
1927 management and deployment of life cycle models and processes.
- 1928 • Security roles, responsibility, accountability, and authority within life cycle policies,
1929 processes, models, and procedures are defined.
- 1930 • The selection of policies, life cycle processes, life cycle models, and procedures for use by
1931 the organization is informed by security needs and considerations.
- 1932 • Security needs and considerations for policies, life cycle processes, life cycle models, and
1933 procedures for use by the organization are assessed.
- 1934 • Prioritized security-relevant process, model, and procedure improvements are
1935 implemented.
- 1936 **3.2.1.3 Security Activities and Tasks**
- 1937 **LM-1 ESTABLISH THE LIFE CYCLE PROCESSES**
- 1938 **LM-1.1** Establish policies and procedures for process management and deployment that are
1939 consistent with the security aspects of organizational strategies.
- 1940 *Note:* The policies and procedures may be security focused, security based, or may have security-
1941 informing aspects.
- 1942 **LM-1.2** Establish the security aspects of the life cycle processes that implement the
1943 requirements of [\[ISO 15288\]](#) and that are consistent with organizational strategies.
- 1944 **LM-1.3** Define the security roles, responsibilities, accountabilities, and authorities to facilitate
1945 implementation of the security aspects of life cycle processes and the strategic
1946 management of life cycles.
- 1947 **LM-1.4** Define the security aspects of the criteria that control progression through the life cycle.
- 1948 *Note:* This includes security criteria for gates, checkpoints, and entry/exit criteria for milestones
1949 and decision points.
- 1950 **LM-1.5** Establish security criteria for the standard life cycle models for the organization,
1951 including criteria for outcomes for each stage.
- 1952 *Note:* The life cycle model comprises one or more stages, as needed, with each stage having
1953 security aspects to its purpose and outcomes. The model is assembled as a sequence of stages
1954 that overlap or iterate as appropriate for the scope of the system of interest, magnitude,
1955 complexity, changing needs, and opportunities (including protection needs and opportunities).
1956 The life cycle processes and activities are selected, tailored as appropriate, and employed in a
1957 stage to fulfill the security aspects of the purpose and outcomes of that stage.
- 1958 **References:** [\[ISO 15288\]](#), Section 6.2.1.3 a); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
1959 [15026-4\]](#).
- 1960 **Related Publications:** [\[ISO 12207\]](#), Section 6.2.1.3.1); [\[ISO 21827\]](#); [\[DoDD 8140.01\]](#).
- 1961 **LM-2 ASSESS THE LIFE CYCLE PROCESS**
- 1962 **LM-2.1** Monitor the security aspects of process execution across the organization.
- 1963 *Note:* This includes the analysis of process measures and the review of security-relevant trends
1964 with respect to strategic security criteria, feedback from the projects regarding the effectiveness

- 1965 and efficiency of the processes, and monitoring execution according to regulations and
1966 organizational policies.
- 1967 **LM-2.2** Conduct reviews of the security aspects of the life cycle models used by the projects.
- 1968 *Note:* This includes confirming the suitability, adequacy, and effectiveness of the life cycle models
1969 used by the project. The reviews should be conducted periodically and be event-driven, (e.g., at
1970 completions of large project milestones).
- 1971 **LM-2.3** Identify security-relevant improvement opportunities from assessment results.
- 1972 **References:** [[ISO 15288](#), Section 6.2.1.3 b)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
1973 [15026-4](#)].
- 1974 **Related Publications:** [[ISO 12207](#), Section 6.2.1.3.2]; [[ISO 21827](#)].
- 1975 **LM-3 IMPROVE THE PROCESS**
- 1976 **LM-3.1** Prioritize and plan for security-relevant improvement opportunities.
- 1977 **LM-3.2** Implement security improvement opportunities, and inform relevant stakeholders.
- 1978 *Note:* This includes regulatory, certification, accreditation, acceptance, and similar stakeholders.
- 1979 **References:** [[ISO 15288](#)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO 15026-4](#)].
- 1980 **Related Publications:** [[ISO 12207](#), Section 6.2.1.3.3]; [[ISO 21827](#)].
- 1981 **3.2.2 Infrastructure Management**
- 1982 The purpose of the *Infrastructure Management* process is to provide infrastructure and services
1983 to projects to support organization and project objectives throughout the life cycle.
- 1984 [[ISO 15288](#)] *Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.*
- 1985 **3.2.2.1 Security Purpose**
- 1986 • To define protection needs for the aspects of infrastructure and services that support
1987 organization and project objectives
- 1988 **3.2.2.2 Security Outcomes**
- 1989 • Protection needs for the infrastructure are defined.
- 1990 • Security capabilities and constraints of infrastructure elements are specified.
- 1991 • Infrastructure elements that satisfy infrastructure security specifications are obtained.
- 1992 • Secure infrastructure is available.
- 1993 • Prioritized infrastructure security-relevant improvements are implemented.
- 1994 **3.2.2.3 Security Activities and Tasks**
- 1995 **IF-1 ESTABLISH THE INFRASTRUCTURE**
- 1996 **IF-1.1** Define the infrastructure security protection needs.
- 1997 *Note:* The security aspects of infrastructure resource needs are considered in context with other
1998 projects and resources within the organization. Security constraints that influence and control
1999 the provision of infrastructure resources and services for the project are also defined.

2000 **IF-1.2** Identify, obtain, and provide the infrastructure resources and services that satisfy the
2001 security protection needs to securely implement and support projects.

2002 **References:** [ISO 15288, Section 6.2.2.3 a)]; [ISO 15026-1]; [ISO 15026-2]; [ISO 15026-3]; [ISO
2003 15026-4]; [ISO 27036-1]; [ISO 27036-2]; [ISO 27036-3].

2004 **Related Publications:** [ISO 12207, Sections 6.2.2.3.1, 6.2.2.3.2]; [ISO 21827].

2005 **IF-2** MAINTAIN THE INFRASTRUCTURE

2006 **IF-2.1** Evaluate the degree to which delivered infrastructure resources satisfy project
2007 protection needs.

2008 **IF-2.2** Identify and provide security improvements or changes to infrastructure resources as
2009 project requirements change.

2010 *Note:* Any mismatch between project security needs and the security provided by infrastructure
2011 resources may result in gaps in assurance.

2012 **References:** [ISO 15288, Section 6.2.2.3 b)]; [ISO 15026-1]; [ISO 15026-2]; [ISO 15026-3]; [ISO
2013 15026-4]; [ISO 27036-1]; [ISO 27036-2]; [ISO 27036-3].

2014 **Related Publications:** [ISO 12207, Section 6.2.2.3.3]; [ISO 21827].

2015 **3.2.3 Portfolio Management**

2016 The purpose of the *Portfolio Management* process is to initiate and sustain necessary, sufficient,
2017 and suitable projects in order to meet the strategic objectives of the organization.

2018 [ISO 15288] *Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.*

2019 **3.2.3.1 Security Purpose**

- 2020 • To identify security considerations for the projects that meet the strategic objectives of the
2021 organization

2022 **3.2.3.2 Security Outcomes**

- 2023 • Security aspects of strategic venture opportunities, investments, or necessities are
2024 prioritized.
- 2025 • Security aspects of projects are identified.
- 2026 • Resources and budgets for the security aspects of each project are allocated.
- 2027 • Project management responsibilities, accountability, and authorities for security are
2028 defined.
- 2029 • Projects that meet the security criteria in agreements and stakeholder security
2030 requirements are sustained.
- 2031 • Projects that do not meet the security criteria in agreements or do not satisfy stakeholder
2032 security requirements are redirected or terminated.
- 2033 • Projects that have completed the security aspects of agreements and that satisfy all
2034 stakeholder security requirements are closed.

2035 **3.2.3.3 Security Activities and Tasks**

- 2036 **PM-1** DEFINE AND AUTHORIZE PROJECTS
- 2037 **PM-1.1** Identify potential new or modified security capabilities or missions.
- 2038 *Note:* The organization strategy, concept of operations, or gap or opportunity analysis is
2039 reviewed to identify security-driven gaps, problems, or opportunities.
- 2040 **PM-1.2** Identify security aspects of potential new or modified capabilities or missions.
- 2041 *Note:* The organization strategy, concept of operations, or gap or opportunity analysis is
2042 reviewed to identify security-relevant gaps, problems, or opportunities.
- 2043 **PM-1.3** Prioritize, select, and establish new business opportunities, ventures, or undertakings
2044 with consideration for security objectives and concerns.
- 2045 **PM-1.4** Define the security aspects of projects, accountabilities, and authorities.
- 2046 *Note:* This includes project proprietary, sensitivity, and privacy criteria.
- 2047 **PM-1.5** Identify the security aspects of expected goals, objectives, and outcomes of each
2048 project.
- 2049 *Note:* This includes project proprietary, sensitivity, and privacy criteria.
- 2050 **PM-1.6** Identify and allocate resources for the achievement of the security aspects of project
2051 goals and objectives.
- 2052 **PM-1.7** Identify the security aspects of any multi-project interfaces and dependencies to be
2053 managed or supported by each project.
- 2054 *Note:* This includes interfaces and dependencies with enabling systems and services, as well as all
2055 associated data and information.
- 2056 **PM-1.8** Specify the security aspects of project reporting requirements, and review milestones
2057 that govern the execution of each project.
- 2058 **PM-1.9** Authorize each project to commence execution of project plans, including its security
2059 aspects.
- 2060 **References:** [\[ISO 15288\]](#), Section 6.2.3.3 a); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
2061 [15026-4\]](#).
- 2062 **Related Publications:** [\[ISO 12207\]](#), Section 6.2.3.3.1); [\[ISO 21827\]](#).
- 2063 **PM-2** EVALUATE THE PORTFOLIO OF PROJECTS
- 2064 **PM-2.1** Evaluate the security aspects of projects to confirm ongoing viability.
- 2065 *Note:* This includes the following:
- 2066 - The project is making progress towards achieving established security goals and objectives.
 - 2067 - The project is complying with project security directives.
 - 2068 - The project is being conducted according to security aspects of project life cycle policies,
2069 processes, and procedures.
 - 2070 - The project remains viable, as indicated by the continuing need for security services,
2071 practical secure product implementation, and acceptable security-driven investment
2072 benefits.
- 2073 **PM-2.2** Act to continue projects that are satisfactorily progressing in consideration of project
2074 security aspects.
- 2075 **PM-2.3** Act to redirect projects that can be expected to progress satisfactorily with appropriate
2076 security-informed redirection.

- 2112 **HR-2.2** Obtain security-relevant training, education, or mentoring resources.
- 2113 **HR-2.3** Provide planned security-relevant skills development.
- 2114 **HR-2.4** Maintain records of security-relevant skills development.
- 2115 **References:** [[ISO 15288](#), Section 6.2.4.3 b)].
- 2116 **Related Publications:** [[ISO 12207](#), Section 6.2.4.3.2]; [[ISO 21827](#)]; [[ISO 27034-1](#)]; [[DoDD](#)
2117 [8140.01](#)].
- 2118 **HR-3 ACQUIRE AND PROVIDE SKILLS**
- 2119 **HR-3.1** Obtain qualified personnel when security-relevant skill deficits are identified.
- 2120 **HR-3.2** Maintain and manage the pool of security-skilled personnel necessary to staff ongoing
2121 projects.
- 2122 **HR-3.3** Make personnel assignments based on security-relevant project and staff development
2123 needs.
- 2124 **HR-3.4** Motivate security-skilled personnel (e.g., through career development and reward
2125 mechanisms).
- 2126 **HR-3.5** Resolve the security aspects of personnel conflicts across or within projects.
- 2127 *Note:* Conflicts across or within projects may include personnel capacity, availability, qualification
2128 conflicts, and personality conflicts.
- 2129 **References:** [[ISO 15288](#)] 15288, Section 6.2.4.3 c).
- 2130 **Related Publications:** [[ISO 12207](#), Section 6.2.4.3.3]; [[SP 800-181](#)].
- 2131 **3.2.5 Quality Management**
- 2132 The purpose of the *Quality Management* process is to assure that products, services, and
2133 implementations of the quality management process meet organizational and project quality
2134 objectives and achieve customer satisfaction.
- 2135 [[ISO 15288](#)] Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.
- 2136 **3.2.5.1 Security Purpose**
- 2137 • To define organizational and project security quality objectives and the criteria used to
2138 determine that products, services, and implementations of the *Quality Management*
2139 process meet those security objectives
- 2140 **3.2.5.2 Security Outcomes**
- 2141 • Organizational security quality management policies, standards, and procedures are defined
2142 and implemented.
- 2143 • Security quality evaluation criteria and methods are established.
- 2144 • Resources and information are provided to projects to support the operation and
2145 monitoring of project security quality assurance activities.
- 2146 • Security aspects of quality evaluation results are analyzed.

- 2147 • Security quality management policies and procedures are improved based on project and
2148 organization results.

2149 3.2.5.3 Security Activities and Tasks

2150 QM-1 PLAN QUALITY MANAGEMENT

2151 **QM-1.1** Establish the security aspects of quality management policies, standards, and
2152 procedures.

2153 **QM-1.2** Define responsibilities and authority for the implementation of security quality
2154 management.

2155 **QM-1.3** Define security quality evaluation criteria and methods.

2156 **QM-1.4** Provide resources, data, and information for security quality management.

2157 **References:** [[ISO 15288](#), Section 6.2.5.3 a)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
2158 [15026-4](#)]; [[ISO 9001](#)].

2159 **Related Publications:** [[ISO 12207](#), Section 6.2.5.3.1].

2160 QM-2 ASSESS QUALITY MANAGEMENT

2161 **QM-2.1** Gather and analyze quality assurance evaluation results in accordance with the defined
2162 security quality evaluation criteria.

2163 **QM-2.2** Assess customer satisfaction.

2164 *Note:* The satisfaction focuses on security for the systems security efforts.

2165 **QM-2.3** Conduct periodic reviews of project quality assurance activities for compliance with the
2166 security quality management policies, standards, and procedures.

2167 **QM-2.4** Monitor the status of security quality improvements on processes, products, and
2168 services.

2169 **References:** [[ISO 15288](#), Section 6.2.5.3 b)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
2170 [15026-4](#)]; [[ISO 9001](#)].

2171 **Related Publications:** [[ISO 12207](#), Section 6.2.5.3.1].

2172 QM-3 PERFORM QUALITY MANAGEMENT CORRECTIVE AND PREVENTIVE ACTIONS

2173 **QM-3.1** Plan corrective actions when security quality management objectives are not achieved.

2174 **QM-3.2** Plan preventive actions when there is a sufficient risk that security quality management
2175 objectives will not be achieved.

2176 **QM-3.3** Monitor the security aspects of corrective and preventive actions to completion and
2177 inform stakeholders.

2178 **References:** [[ISO 15288](#), Section 6.2.5.3 c)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
2179 [15026-4](#)]; [[ISO 9001](#)].

2180 **Related Publications:** [[ISO 12207](#)], Section 6.2.5.3.2].

2181 3.2.6 Knowledge Management

2182 The purpose of the *Knowledge Management* process is to create the capability and assets that
2183 enable the organization to exploit opportunities to reapply existing knowledge.

2184 [\[ISO 15288\]](#) Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

2185 3.2.6.1 Security Purpose

- 2186 • To enable the organization to exploit opportunities to reapply existing security knowledge

2187 3.2.6.2 Security Outcomes

- 2188 • A taxonomy for the application of security-relevant knowledge assets is identified.
- 2189 • Organizational security knowledge, skills, and knowledge assets are organized.
- 2190 • Organizational security knowledge, skills, and knowledge assets are available.
- 2191 • Organizational security knowledge, skills, and knowledge assets are communicated across
- 2192 the organization.
- 2193 • Security knowledge management usage data is analyzed.

2194 3.2.6.3 Security Activities and Tasks

2195 **KM-1** PLAN KNOWLEDGE MANAGEMENT

2196 **KM-1.1** Define the security aspects of the knowledge management strategy.

2197 *Note:* The security aspects of the knowledge management strategy generally include:

- 2198 - Identifying security knowledge domains and technologies and their potential for the
- 2199 reapplication of knowledge
- 2200 - Plans for obtaining and maintaining security knowledge, skills, and security knowledge assets
- 2201 for their useful life
- 2202 - Characterization of the types of security knowledge, security skills, and security knowledge
- 2203 assets to be collected and maintained
- 2204 - Criteria for accepting, qualifying, and retiring security knowledge, security skills, and security
- 2205 knowledge assets
- 2206 - Procedures for controlling changes to the security knowledge, security skills, and security
- 2207 knowledge assets
- 2208 - Plans, mechanisms, and procedures for protection, control, and access to classified or
- 2209 sensitive data and information
- 2210 - Mechanisms for secure storage and secure retrieval

2211 **KM-1.2** Identify the security knowledge, skills, and knowledge assets to be managed.

2212 **KM-1.3** Identify projects that can benefit from the application of the security knowledge, skills,

2213 and knowledge assets.

2214 **References:** [\[ISO 15288\]](#), Section 6.2.6.3 a)].

2215 **Related Publications:** [\[ISO 12207\]](#), Section 6.2.4.3.4); [\[ISO 21827\]](#); [\[SP 800-181\]](#); [\[DoDD 8140.01\]](#).

2216 **KM-2** SHARE KNOWLEDGE AND SKILLS THROUGHOUT THE ORGANIZATION

2217 **KM-2.1** Establish and maintain a classification for capturing and sharing security knowledge and

2218 skills.

2219 *Note:* This classification includes security expert, common security, and security domains

2220 knowledge and skills, as well as lessons learned.

2221 **KM-2.2** Capture or acquire security knowledge and skills.

- 2222 **KM-2.3** Make security knowledge and skills accessible across the organization.
- 2223 **References:** [\[ISO 15288\]](#), Section 6.2.6.3 b)].
- 2224 **Related Publications:** [\[ISO 12207\]](#), Section 6.2.4.3.4); [\[ISO 21827\]](#).
- 2225 **KM-3** SHARE KNOWLEDGE ASSETS THROUGHOUT THE ORGANIZATION
- 2226 **KM-3.1** Establish a taxonomy to organize security knowledge assets.
- 2227 *Note:* The taxonomy includes the following:
- 2228 - Definition of the boundaries of security domains and their relationships to one another
- 2229 - Definition of the boundaries of security-related domains (e.g., safety) and their relationships
- 2230 to one another
- 2231 - Domain models that capture essential common and different security-relevant features,
- 2232 capabilities, concepts, and functions
- 2233 **KM-3.2** Develop or acquire security knowledge assets.
- 2234 *Note:* Security knowledge assets include system elements or their representations (e.g., reusable
- 2235 code libraries, security reference architectures), architecture or design elements (e.g., security
- 2236 architecture or security design patterns), processes, security criteria, or other technical
- 2237 information (e.g., training materials) related to security domain knowledge and lessons learned.
- 2238 **KM-3.3** Make all knowledge assets securely accessible to the organization.
- 2239 **References:** [\[ISO 15288\]](#), Section 6.2.6.3 c)]; [\[ISO 42010\]](#).
- 2240 **Related Publications:** [\[ISO 12207\]](#), Section 6.2.4.3.4); [\[ISO 21827\]](#).
- 2241 **KM-4** MANAGE KNOWLEDGE, SKILLS, AND KNOWLEDGE ASSETS
- 2242 **KM-4.1** Maintain security knowledge, skills, and knowledge assets.
- 2243 **KM-4.2** Monitor and record the use of security knowledge, skills, and knowledge assets.
- 2244 **KM-4.3** Periodically reassess the currency of the security aspects of technology and market
- 2245 needs of the security knowledge assets.
- 2246 **References:** [\[ISO 15288\]](#), Section 6.2.6.3 d)].
- 2247 **Related Publications:** [\[ISO 12207\]](#), Section 6.2.4.3.4); [\[ISO 21827\]](#).

2248 **3.3 TECHNICAL MANAGEMENT PROCESSES**

2249 This section contains the *Technical Management Processes* from [\[ISO 15288\]](#) with security-

2250 related considerations and contributions.

2251 **3.3.1 Project Planning**

2252 The purpose of the *Project Planning* process is to produce and coordinate effective and

2253 workable plans.

2254 [\[ISO 15288\]](#) *Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.*

2255 **3.3.1.1 Security Purpose**

- 2256 • To determine and coordinate the security aspects of effective and workable plans

2257 **3.3.1.2 Security Outcomes**

- 2258 • Security objectives, security-specific plans, and the security aspects of other plans are
2259 defined.
- 2260 • Security-relevant roles, responsibilities, accountabilities, and authorities within the project
2261 are defined.
- 2262 • Security aspects of performance and achievement criteria are defined.
- 2263 • The resources and services necessary to achieve the security objectives are committed.
- 2264 • Plans for the execution of the security aspects of the project are activated.

2265 3.3.1.3 Security Activities and Tasks

2266 PL-1 DEFINE THE PROJECT

2267 **PL-1.1** Identify the security aspects of project objectives and constraints.

2268 *Note:* Objectives and constraints include strategic security, assurance, and trustworthiness goals,
2269 as well as loss thresholds and regulatory concerns. Each security-relevant objective is identified
2270 with a level of detail that permits selection, tailoring, and implementation of the appropriate
2271 processes and activities.

2272 **PL-1.2** Define the security aspects of the project scope as established in agreements.

2273 *Note:* This includes the relevant activities required to satisfy security aspects of decision criteria
2274 and complete the project successfully.

2275 **PL-1.3** Define and maintain security views of the project life cycle model that are comprised of
2276 stages using the defined life cycle models of the organization.

2277 **PL-1.4** Establish appropriate security aspects of the breakdown structures.

2278 *Note:* Each security-relevant element of a breakdown structure is described with a level of detail
2279 that is consistent with identified security risks and required visibility.

2280 **PL-1.5** Define and maintain the security aspects of processes that will be applied on the
2281 project.

2282 **References:** [[ISO 15288](#), Section 6.3.1.3 a)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
2283 [15026-4](#)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)]; [[ISO 24748-1](#)].

2284 **Related Publications:** [[ISO 12207](#), Section 6.3.1.3.1]; [[ISO 21827](#)].

2285 PL-2 PLAN PROJECT AND TECHNICAL MANAGEMENT

2286 **PL-2.1** Define and maintain the security aspects of a project schedule based on management
2287 and technical objectives and work estimates.

2288 *Note:* This includes security aspects that impact the definition of the duration, relationship,
2289 dependencies, and sequence of activities; achievement milestones; resources employed; reviews
2290 (including security subject matter expertise employed); and schedule reserves for security risk
2291 management necessary to achieve timely completion of the project.

2292 **PL-2.2** Define the security aspects of achievement criteria for the life cycle decision gates,
2293 delivery dates, and major dependencies on external inputs and outputs.

2294 *Note:* This includes criteria defined by regulatory, certification, evaluation, and other approval
2295 authorities.

2296 **PL-2.3** Define the security aspects of project performance criteria.

- 2297 **PL-2.4** Define the security-related project costs, and plan the budget.
- 2298 **PL-2.5** Define the security-relevant roles, responsibilities, accountabilities, and authorities.
- 2299 *Note:* This includes defining the project organization, staff acquisitions, and development of staff
 2300 security-relevant skills. Authorities include, as appropriate, the legally responsible roles and
 2301 individuals. These security-relevant authorities include security design authorization, security test
 2302 and operation authorization, and the award of certification, accreditation, or authorization.
- 2303 **PL-2.6** Define the security aspects of infrastructure and services required.
- 2304 *Note:* This includes defining the capacity needed for security infrastructure and services, its
 2305 availability, and its allocation to project tasks. Security infrastructure includes facilities (e.g.,
 2306 Sensitive Compartmented Information Facilities [SCIFs] and isolated networks), specific strength
 2307 of mechanism mediated access, cross-domain solutions, tools, communication, and information
 2308 technology assets.
- 2309 **PL-2.7** Plan the security aspects of acquiring materials and enabling system services supplied
 2310 from outside of the project.
- 2311 **PL-2.8** Generate and communicate a plan for the security aspects of project and technical
 2312 management and execution, including security reviews that address security
 2313 considerations.
- 2314 *Note:* Security considerations and the planning to address those considerations are captured in a
 2315 Systems Engineering Management Plan, Software Engineering Management Plans, and similar
 2316 plans.
- 2317 **References:** [[ISO 15288](#), Section 6.3.1.3 b)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
 2318 [15026-4](#)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].
- 2319 **Related Publications:** [[ISO 12207](#), Section 6.3.1.3.2]; [[ISO 21827](#)].
- 2320 **PL-3** ACTIVATE THE PROJECT
- 2321 **PL-3.1** Obtain authorization for the security aspects of the project.
- 2322 **PL-3.2** Submit requests and obtain commitments for the necessary resources to perform the
 2323 security aspects of the project.
- 2324 **PL-3.3** Implement the security aspects of project plans.
- 2325 **References:** [[ISO 15288](#), Section 6.3.1.3 c)].
- 2326 **Related Publications:** [[ISO 12207](#), Section 6.3.1.3.3]; [[ISO 21827](#)].
- 2327 **3.3.2 Project Assessment and Control**
- 2328 The purpose of the *Project Assessment and Control* process is to assess if the plans are aligned
 2329 and feasible; determine the status of the project, technical, and process performance; and
 2330 direct execution to help ensure that the performance is within projected budgets according to
 2331 plans and schedules to satisfy technical objectives.
- 2332 [[ISO 15288](#)] Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.
- 2333 **3.3.2.1 Security Purpose**
- 2334 • To assess if the security aspects of plans and security plans are aligned and feasible
- 2335 • To determine the state of the project, technical, and process security performance

- 2336 • To direct execution to help ensure that the security performance is within projected budgets
2337 according to plans and schedules to satisfy security and other technical objectives

2338 3.3.2.2 Security Outcomes

- 2339 • Security aspects of performance measures or assessment results are available.
- 2340 • Adequacy of security-relevant roles, responsibilities, accountabilities, authorities, and
2341 resources is assessed.
- 2342 • Security aspects of technical progress reviews are performed.
- 2343 • Deviations in the security aspects of project performance from plans are analyzed.
- 2344 • Affected stakeholders are informed of the security aspects of project status.
- 2345 • Corrective action is directed when project performance or achievement is not meeting
2346 security-relevant targets.
- 2347 • Security aspects of project replanning are initiated as necessary.
- 2348 • Security aspects of project action to progress (or not) from one scheduled milestone or
2349 event to the next is authorized.

2350 3.3.2.3 Security Activities and Tasks

2351 PA-1 PLAN FOR PROJECT ASSESSMENT AND CONTROL

2352 PA-1.1 Define the security aspects of the project assessment and control strategy.

2353 *Note 1:* This includes the planned security assessment methods and time frames as well as
2354 necessary security management and technical reviews.

2355 *Note 2:* Expectations of regulatory, certification, and authorization entities inform the security
2356 aspects of the project assessment and control strategy.

2357 **References:** [\[ISO 15288, Section 6.3.2.3 a\)\]](#); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
2358 [15026-4\]](#).

2359 **Related Publications:** [\[ISO 21827\]](#).

2360 PA-2 ASSESS THE PROJECT

2361 PA-2.1 Assess the alignment of the security aspects of project objectives and plans with the
2362 project context.

2363 PA-2.2 Assess the security aspects of the management and technical plans against objectives to
2364 determine adequacy and feasibility.

2365 PA-2.3 Assess the security aspects of the project and technical status against appropriate plans
2366 to determine actual and projected cost, schedule, and performance variances.

2367 PA-2.4 Assess the adequacy of the security-relevant roles, responsibilities, accountabilities, and
2368 authorities.

2369 *Note:* This includes assessment of the adequacy of personnel competencies to perform project
2370 roles and accomplish project tasks.

2371 PA-2.5 Assess the security aspects of resource adequacy and availability.

- 2372 **PA-2.6** Assess progress using measured security achievement and security aspects of milestone
2373 completion.
- 2374 *Note:* This includes collecting and evaluating security-relevant data for labor, material, service
2375 costs, and technical performance, as well as other technical data about security objectives. These
2376 are compared against security-relevant measures of achievement. This includes conducting
2377 effectiveness assessments to determine the adequacy of the evolving system to security
2378 requirements.
- 2379 **PA-2.7** Conduct required management and technical reviews, audits, and inspections relevant
2380 to the security aspects of the project.
- 2381 *Note:* The reviews, audits, and inspections are formal or informal and are conducted to
2382 determine the security-relevant readiness to proceed to the next stage or milestone, to help
2383 ensure project and technical security objectives are being met, or to solicit feedback from
2384 stakeholders with security concerns.
- 2385 **PA-2.8** Monitor the security aspects of critical processes and new technologies.
- 2386 *Note:* This includes identifying and evaluating technology maturity from a security perspective, as
2387 well as the feasibility of technology insertion for satisfying security objectives.
- 2388 **PA-2.9** Make recommendations based on security measurement results and other security-
2389 relevant project information.
- 2390 *Note:* Measurement results are analyzed to identify security-relevant deviations, variations, or
2391 undesirable trends from planned values and to make security-relevant recommendations for
2392 corrective, preventive, adaptive, additive, or perfective actions.
- 2393 **PA-2.10** Record and provide security status and security findings from the assessment tasks.
- 2394 **PA-2.11** Monitor the security aspects of process execution within the project.
- 2395 *Note:* This includes an analysis of process security measures and a review of security-relevant
2396 trends with respect to project objectives.
- 2397 **References:** [[ISO 15288](#), Section 6.3.2.3 b)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
2398 [15026-4](#)].
- 2399 **Related Publications:** [[ISO 12207](#), Sections 6.3.2.3.1, 6.3.2.3.3]; [[ISO 21827](#)].
- 2400 **PA-3** CONTROL THE PROJECT
- 2401 **PA-3.1** Initiate the actions needed to address identified security issues.
- 2402 **PA-3.2** Initiate the necessary security aspects of project replanning.
- 2403 *Note:* Replanning is initiated when the security aspects of project objectives or constraints have
2404 changed or when security-relevant planning assumptions are shown to be invalid.
- 2405 **PA-3.3** Initiate necessary change actions when there is a contractual change to cost, time, or
2406 quality due to the security impact of an acquirer or supplier request.
- 2407 *Note:* The security impact is not necessarily obvious in the case where the request is not security-
2408 driven or security-oriented.
- 2409 **PA-3.4** Recommend that the project proceed toward the next milestone or event, if justified,
2410 based on the achievement of security-relevant milestones or event criteria.
- 2411 **References:** [[ISO 15288](#), Section 6.3.2.3 c)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].
- 2412 **Related Publications:** [[ISO 12207](#)] 12207, Sections 6.3.2.3.2, 6.3.2.3.4]; [[ISO 21827](#)].

2413 3.3.3 Decision Management

2414 The purpose of the *Decision Management* process is to provide a structured, analytical
 2415 framework for objectively identifying, characterizing, and evaluating a set of alternatives for a
 2416 decision at any point in the life cycle and select the most beneficial course of action.

2417 [\[ISO 15288\]](#) Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

2418 3.3.3.1 Security Purpose

2419 • To identify, analyze, characterize, and evaluate the security aspects of alternatives for a
 2420 decision

2421 • To recommend the most beneficial course of security-informed action

2422 3.3.3.2 Security Outcomes

2423 • Security aspects of decisions requiring alternative analysis are identified.

2424 • Security aspects of alternative courses of action are identified and evaluated.

2425 • A preferred security-informed course of action is selected.

2426 • Security aspects of a resolution, of the decision rationale, and of the assumptions are
 2427 identified.

2428 3.3.3.3 Security Activities and Tasks

2429 DM-1 PREPARE FOR DECISIONS

2430 **DM-1.1** Define the security aspects of the decision management strategy.

2431 *Note:* A decision management strategy includes the identification of security-relevant roles,
 2432 responsibilities, accountabilities, and authorities. It includes the identification of security-specific
 2433 decision categories and a prioritization scheme. Security-related decisions often arise as a result
 2434 of a security effectiveness assessment, a technical trade-off, a security-related problem needing
 2435 to be solved, an action needed as a response to security risk that exceeds the acceptable
 2436 threshold, or a new opportunity.

2437 **DM-1.2** Identify the security aspects of the circumstances and need for a decision.

2438 **DM-1.3** Identify stakeholders with relevant security expertise to support decision-making
 2439 efforts.

2440 **References:** [\[ISO 15288\]](#), Section 6.3.3.3 a)].

2441 **Related Publications:** [\[ISO 12207\]](#), Section 6.3.3.3.1]; [\[ISO 21827\]](#).

2442 DM-2 ANALYZE THE DECISION INFORMATION

2443 **DM-2.1** Select and declare the security aspects of the decision management strategy for each
 2444 decision.

2445 *Note:* This includes the security-related level of rigor and the data and system analysis needed.

2446 **DM-2.2** Determine the desired security outcomes and the measurable security attributes of
 2447 selection criteria.

2448 *Note:* The desired value for all quantifiable security criteria and the threshold value(s) beyond
 2449 which the attribute will be unsatisfactory are determined.

- 2450 **DM-2.3** Identify the security aspects of the trade space and alternatives.
- 2451 *Note:* If a large number of alternatives exist, security aspects are to qualitatively screen in order
2452 to reduce alternatives to a manageable number for further detailed system analysis.
- 2453 **DM-2.4** Evaluate each alternative against the security criteria.
- 2454 **References:** [[ISO 15288](#), Section 6.3.3.3 b)].
- 2455 **Related Publications:** [[ISO 12207](#), Section 6.3.3.3.2]; [[ISO 21827](#)].
- 2456 **DM-3** MAKE AND MANAGE DECISIONS
- 2457 **DM-3.1** Determine the preferred alternative for each security-informed and security-based
2458 decision.
- 2459 **DM-3.2** Record the security-informed or security-based resolution, decision rationale, and
2460 assumptions.
- 2461 **DM-3.3** Record, track, evaluate, and report the security aspects of security-informed and
2462 security-based decisions.
- 2463 *Note:* Security aspects of problems or opportunities and the alternative courses of action that
2464 will resolve their outcome – including those with security impacts – are recorded, categorized,
2465 and reported.
- 2466 **References:** [[ISO 15288](#), Section 6.3.3.3 c)].
- 2467 **Related Publications:** [[ISO 12207](#), Section 6.3.3.3.3]; [[ISO 21827](#)].
- 2468 **3.3.4 Risk Management**
- 2469 The purpose of the *Risk Management* process is to identify, analyze, treat, and monitor the risks
2470 continually.
- 2471 [[ISO 15288](#)] *Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.*
- 2472 **3.3.4.1 Security Purpose**
- 2473 • To continually identify, analyze, treat, and monitor the risks associated with the uncertainty
2474 of achieving security objectives and the effects of security protection efforts on achieving
2475 system objectives
- 2476 **3.3.4.2 Security Outcomes**
- 2477 • Security-related risks are identified.
- 2478 • Security-related risks are analyzed.
- 2479 • Security-related risk treatments are selected.
- 2480 • Appropriate security-related risk treatments are implemented.
- 2481 • Security-related risks are evaluated on an ongoing basis to assess changes in status and
2482 progress in treatment.
- 2483 • Security-related risks are recorded and maintained in the risk profile.
- 2484 **3.3.4.3 Security Activities and Tasks**
- 2485 **RM-1** PLAN RISK MANAGEMENT

- 2486 **RM-1.1** Define the security aspects of the risk management strategy.
- 2487 *Note 1:* The nature of security risk includes intentional and unintentional casual events,
2488 considerations of the intended behaviors and outcomes, functions (security and other functions),
2489 and the potential effects of security risk realization. Casual events may be combinations of
2490 events in the operational environment and events in the system environment.
- 2491 *Note 2:* The security aspects scope of the risk management process, risk management approach,
2492 risk criteria, measures, parameters, rating scale, and treatment alternatives are defined. This
2493 includes security aspects of the risk management process at all levels of the supply chain (e.g.,
2494 suppliers, subcontractors) and how they are incorporated into the project risk management
2495 process.
- 2496 *Note 3:* The strategy can also include those security-relevant issues (e.g., risks with likelihood of
2497 occurrence of 1) and opportunities within scope and approach. Opportunity aspects include
2498 opportunity criteria, measures, parameters, rating scale, and treatment alternatives.
- 2499 **RM-1.2** Define and record the security context of the risk management process.
- 2500 *Note 1:* This includes the identification of security-relevant stakeholders and descriptions of their
2501 perspectives, risk categories, and technical and managerial objectives, assumptions, and
2502 constraints.
- 2503 *Note 2:* Security opportunities provide potential benefits for the system or project. Security
2504 contexts consider the security impact of not pursuing an opportunity and the security risk of not
2505 achieving the effects provided by the opportunity.
- 2506 **References:** [[ISO 15288](#), Section 6.3.4.3 a)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
2507 [15026-4](#)]; [[ISO 16085](#)]; [[ISO 31000](#)].
- 2508 **Related Publications:** [[ISO 12207](#), Section 6.3.4.3.1]; [[ISO 21827](#)].
- 2509 **RM-2** MANAGE THE RISK PROFILE
- 2510 **RM-2.1** Define and record the security risk thresholds and conditions.
- 2511 *Note:* The security risk thresholds define the levels at which the appropriate treatment strategies
2512 are considered.
- 2513 **RM-2.2** Establish and maintain the security aspects of the risk profile.
- 2514 *Note:* The risk profile records each security risk and opportunity including a description of the
2515 security risk or opportunity, a record of the risk or opportunity parameters, the priority based on
2516 risk or opportunity criteria, and the risk or opportunity current state, treatment, and contingency
2517 strategy. The risk profile is updated when there are changes in an individual security risk or
2518 opportunity state.
- 2519 **RM-2.3** Provide the security aspects of the relevant risk profile to stakeholders.
- 2520 *Note:* The frequency of communicating the risk profile and its security aspects is determined by
2521 project planning.
- 2522 **References:** [[ISO 15288](#), Section 6.3.4.3 b)]; [[ISO 31000](#)]; [[ISO 16085](#)].
- 2523 **Related Publications:** [[ISO 12207](#), Section 6.3.4.3.2]; [[ISO 21827](#)].
- 2524 **RM-3** ANALYZE RISK
- 2525 **RM-3.1** Identify security risks in the categories described in the risk management context.
- 2526 *Note:* Security risks are commonly identified through various security and other analyses, such as
2527 safety, assurance, producibility, and performance analyses; technology, architecture, integration,

2528 and readiness assessments; measurement reports; and trade-off studies. Additionally, security
 2529 risks are often identified through the analysis of measures associated with system security goals
 2530 (e.g., security-relevant Measures of Effectiveness or Measures of Performance).

2531 **RM-3.2** Measure each identified security risk.

2532 *Note:* A common risk measurement is the likelihood of occurrence and consequences as well as
 2533 the levels of confidence with those measures.

2534 **RM-3.3** Evaluate each security risk against its risk thresholds.

2535 **RM-3.4** Define and record recommended treatment strategies and measures for each security-
 2536 relevant risk that exceeds its risk threshold.

2537 **References:** [ISO 15288, Section 6.3.4.3 c)]; [ISO 15026-1]; [ISO 15026-2]; [ISO 15026-3]; [ISO
 2538 15026-4]; [ISO 31000]; [ISO 16085].

2539 **Related Publications:** [ISO 12207, Section 6.3.4.3.3]; [ISO 21827].

2540 **RM-4** TREAT RISKS THAT EXCEED THEIR RISK THRESHOLD

2541 **RM-4.1** Identify recommended alternatives for security risk treatment.

2542 **RM-4.2** Define measures for determining the effectiveness of security risk treatments.

2543 **RM-4.3** Implement selected security risk treatments.

2544 *Note:* The implemented alternative should be the one for which the security-relevant
 2545 stakeholders determine the actions taken will make a security-relevant risk acceptable.

2546 **RM-4.4** Coordinate management action for selected security risk treatments.

2547 **References:** [ISO 15288, Section 6.3.4.3 d)]; [ISO 31000]; [ISO 16085].

2548 **Related Publications:** [ISO 12207, Section 6.3.4.3.4]; [ISO 21827].

2549 **RM-5** MONITOR RISK

2550 **RM-5.1** Continually monitor all security-relevant risks and the security risk management
 2551 context.

2552 *Note:* Changes with security-relevant risks and their treatments may prompt reevaluation. The
 2553 initial treatment plans for a security-relevant risk may include preplanned additional actions
 2554 when risk increases or insufficiently decreases despite treatment.

2555 **RM-5.2** Implement and monitor measures to evaluate the effectiveness of security-relevant risk
 2556 treatments.

2557 **RM-5.3** Continually monitor for the emergence of new security-relevant risks and sources of risk
 2558 throughout the life cycle.

2559 *Note:* This includes monitoring known changes in adversities.

2560 **References:** [ISO 15288, Section 6.3.4.3 e)]; [ISO 15026-1]; [ISO 15026-2]; [ISO 15026-3]; [ISO
 2561 15026-4]; [ISO 31000]; [ISO 16085].

2562 **Related Publications:** [ISO 12207, Section 6.3.4.3.5]; [ISO 21827].

2563 3.3.5 Configuration Management

2564 The purpose of the *Configuration Management* process is to manage system and system
 2565 elements and configurations over the life cycle.

2566 [ISO 15288] Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

2567 **3.3.5.1 Security Purpose**

- 2568 • To incorporate security considerations to securely manage system and system elements and
2569 configurations over the life cycle

2570 **3.3.5.2 Security Outcomes**

- 2571 • System element configurations are securely managed.
2572 • Security aspects of configuration baselines are established.
2573 • Changes to items under configuration management are securely controlled.
2574 • Security aspects of configuration status information are available.
2575 • Security aspects of required configuration audits are completed.
2576 • Security aspects of system releases are approved.

2577 **3.3.5.3 Security Activities and Tasks**

2578 **CM-1 PREPARE FOR CONFIGURATION MANAGEMENT**

2579 **CM-1.1** Define a secure configuration management strategy.

2580 *Note:* These include:

- 2581 - Security-relevant roles, responsibilities, accountabilities, and authorities
2582 - Criteria for the secure management of changes to items under configuration management,
2583 including dispositions, access, release, and control
2584 - Security considerations, criteria, and constraints for the locations, conditions, and
2585 environment of storage
2586 - Criteria or events for commencing secure configuration control and securely maintaining
2587 baselines of evolving configurations
2588 - Security aspects of the audit strategy and the responsibilities for assessing continual integrity
2589 and security of the configuration definition information
2590 - Criteria and constraints for secure change management, planned configuration control
2591 boards and security configuration control boards, regulatory and emergency change
2592 requests, and procedures for secure change management
2593 - Secure coordination among stakeholders, acquirers, suppliers, supply chain, and other
2594 interacting organizations

2595 **CM-1.2** Define the secure archive and retrieval approach for configuration items, configuration
2596 management artifacts, and data.

2597 *Note:* This includes rules governing secure retention, access, and use.

2598 **References:** [[ISO 15288](#), Section 6.3.5.3 a)]; [[ISO 10007](#)]; [[IEEE 828](#)]; [[EIA 649C](#)].

2599 **Related Publications:** [[ISO 12207](#), Sections 6.3.5.3.1, 7.2.2.3.1]; [[ISO 21827](#)].

2600 **CM-2 PERFORM CONFIGURATION IDENTIFICATION**

2601 **CM-2.1** Identify the security aspects of system elements and artifacts that need to be under
2602 configuration management.

2603 **CM-2.2** Identify the security aspects of the configuration data to be managed.

2604 **CM-2.3** Establish the security aspects of identifiers for items under configuration management.

- 2605 **CM-2.4** Define the security aspects of baselines through the life cycle.
- 2606 **CM-2.5** Obtain applicable stakeholder agreement of the security aspects to establish a baseline.
- 2607 **CM-2.6** Approve and track security aspects of system or system element releases.
- 2608 *Note 1:* The security aspects of a release are security-relevant considerations of authorization of
 2609 the use of a system or system element for a specific purpose with or without security-relevant
 2610 restrictions. Examples are releases for tests or operational use.
- 2611 *Note 2:* Releases generally include a set of changes made through the Technical Processes.
 2612 Release approval generally includes acceptance of the verified and validated changes and any
 2613 impacts to security of the changes.
- 2614 **References:** [[ISO 15288](#), Section 6.3.5.3 b)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].
- 2615 **Related Publications:** [[ISO 12207](#), Sections 6.3.5.3.2, 7.2.2.3.2]; [[ISO 21827](#)].
- 2616 **CM-3** PERFORM CONFIGURATION CHANGE MANAGEMENT
- 2617 **CM-3.1** Identify and record the security aspects of requests for change and requests for
 2618 variance.
- 2619 *Note 1:* This includes requests for deviation, waiver, or concession.
- 2620 *Note 2:* Change or variance can be based on reasons other than security or without an obvious
 2621 relevance to security.
- 2622 **CM-3.2** Determine the security aspects of action to coordinate, evaluate, and disposition
 2623 requests for change or requests for variance.
- 2624 *Note:* The security aspects identified are coordinated and evaluated across all impacted
 2625 performance and effectiveness evaluation criteria, as well as the criteria of project plans, cost,
 2626 benefits, risks, quality, and schedule.
- 2627 **CM-3.3** Submit requests for security review and approval.
- 2628 *Note:* Control boards may or may not be security focused. For a non-security control board
 2629 activity, security should be reviewed to verify that there are no security aspects to a request.
- 2630 **CM-3.4** Track and manage the security aspects of approved changes to the baseline, requests
 2631 for change, and requests for variance.
- 2632 **References:** [[ISO 15288](#), Section 6.3.5.3 c)].
- 2633 **Related Publications:** [[ISO 12207](#), Sections 6.3.5.3.2, 7.2.2.3.3]; [[ISO 21827](#)].
- 2634 **CM-4** PERFORM CONFIGURATION STATUS ACCOUNTING
- 2635 **CM-4.1** Develop and maintain security-relevant configuration management status information
 2636 for system elements, baselines, approved changes, and releases.
- 2637 *Note:* The information includes security certification, accreditation, authorization, or approval
 2638 decisions for a system, system element, baseline, or release.
- 2639 **CM-4.2** Capture, store, and report security-relevant configuration management data.
- 2640 **References:** [[ISO 15288](#), Section 6.3.5.3 d)].
- 2641 **Related Publications:** [[ISO 12207](#), Section 7.2.2.3.4]; [[ISO 21827](#)].
- 2642 **CM-5** PERFORM CONFIGURATION EVALUATION

- 2643 **CM-5.1** Identify the need for secure configuration and configuration management verification
2644 activities and audits.
- 2645 **CM-5.2** Verify that the product or service configuration meets the security-relevant
2646 configuration requirements.
- 2647 *Note:* This is performed by comparing security requirements, constraints, and waivers (variances)
2648 with the results of formal verification activities.
- 2649 **CM-5.3** Monitor the secure incorporation of approved configuration changes.
- 2650 **CM-5.4** Perform configuration and configuration management security verification activities and
2651 audits to establish the security aspects of product baselines.
- 2652 *Note:* This includes the security aspects of the functional configuration audit (FCA) that are
2653 focused on functional and performance capabilities and the security aspects of the physical
2654 configuration audit (PCA) that are focused on system conformance to operational and
2655 configuration information items.
- 2656 **CM-5.5** Record the security aspects of the configuration management audit and other
2657 configuration evaluation results and disposition action items.
- 2658 **References:** [[ISO 15288](#), Section 6.3.5.3 e)].
- 2659 **Related Publications:** [[ISO 12207](#), Section 7.2.2.3.5]; [[ISO 21827](#)].

2660 **3.3.6 Information Management**

2661 The purpose of the *Information Management* process is to generate, obtain, confirm, transform,
2662 retain, retrieve, disseminate, and dispose of information to designated stakeholders.

2663 [[ISO 15288](#)] *Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.*

2664 **3.3.6.1 Security Purpose**

- 2665 • To address the security aspects of information management

2666 **3.3.6.2 Security Outcomes**

- 2667 • Security-relevant information to be managed is identified.
- 2668 • Security protections for information are identified.
- 2669 • Security aspects of information representations are defined.
- 2670 • Information is securely managed.
- 2671 • Security aspects of information status are identified.
- 2672 • Information is available to designated stakeholders in a secure manner.

2673 **3.3.6.3 Security Activities and Tasks**

2674 **IM-1** PREPARE FOR INFORMATION MANAGEMENT

2675 **IM-1.1** Define the security aspects of the strategy for information management.

2676 *Note:* The security aspects include stakeholder, technical, and other information. These aspects
2677 address security, privacy, and intellectual property concerns.

2678 **IM-1.2** Define the security aspects of the items of information that will be managed.

- 2679 **IM-1.3** Designate authorities and responsibilities for the security aspects of information
2680 management.
- 2681 *Note:* Due regard is paid to legislation, security, and privacy (e.g., ownership, agreement
2682 restrictions, rights of access, data rights, and intellectual property). Where restrictions or
2683 constraints apply, information is identified accordingly. Staff with knowledge of such items of
2684 information are informed of their security-relevant obligations and responsibilities.
- 2685 **IM-1.4** Define the security aspects of the content, formats, structure, and strengths of
2686 protection for information items.
- 2687 *Note 1:* The security aspects apply to information while at rest (i.e., persistent or non-persistent
2688 storage) and while in transit between a source/point of origin and destination.
- 2689 *Note 2:* The security aspects are informed by criteria in applicable laws, policies, directives,
2690 regulations, and patents.
- 2691 **IM-1.5** Define the security aspects of information maintenance actions.
- 2692 **References:** [[ISO 15288](#), Section 6.3.6.3 a)].
- 2693 **Related Publications:** [[ISO 12207](#), Section 6.3.6.3.1]; [[ISO 21827](#)].
- 2694 **IM-2** PERFORM INFORMATION MANAGEMENT
- 2695 **IM-2.1** Securely obtain, develop, or transform the identified information items.
- 2696 **IM-2.2** Securely maintain information items and their storage records, and record the security
2697 status of information.
- 2698 **IM-2.3** Securely publish, distribute, or provide access to information and information items to
2699 designated stakeholders.
- 2700 **IM-2.4** Securely archive designated information.
- 2701 *Note:* The media, location, and protection of the information are selected in accordance with the
2702 specified storage and retrieval periods, agreements, legislation, and organizational security
2703 policy.
- 2704 **IM-2.5** Securely dispose of unwanted, invalid, or unvalidated information.
- 2705 **References:** [[ISO 15288](#), Section 6.3.6.3 b)].
- 2706 **Related Publications:** [[ISO 12207](#), Section 6.3.6.3.2]; [[ISO 21827](#)].
- 2707 **3.3.7 Measurement**
- 2708 The purpose of the *Measurement* process is to collect, analyze, and report objective data and
2709 information to support effective management and demonstrate the quality of the products,
2710 services, and processes.
- 2711 [[ISO 15288](#)] Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.
- 2712 **3.3.7.1 Security Purpose**
- 2713 • To collect, analyze, and report security-relevant data and information to support effective
2714 management and demonstrate the quality of the products, services, and processes
- 2715 **3.3.7.2 Security Outcomes**
- 2716 • Security-relevant information needs are identified.

- 2717 • An appropriate set of security measures are identified or developed based on security-
2718 relevant information needs and information security protection needs.
- 2719 • Required data is securely managed.
- 2720 • Security-relevant data is analyzed and the results interpreted.
- 2721 • Measurement results provide objective information that supports security-relevant
2722 decisions.

2723 3.3.7.3 Security Activities and Tasks

2724 MS-1 PREPARE FOR MEASUREMENT

2725 MS-1.1 Define the security aspects of the measurement strategy.

2726 MS-1.2 Describe the characteristics of the organization that are relevant to security
2727 measurement.

2728 MS-1.3 Identify and prioritize security-relevant information needs.

2729 *Note:* The needs are based on protection objectives, identified security risks, and other security-
2730 relevant items related to project decisions.

2731 MS-1.4 Select and specify measures that satisfy security-relevant information needs.

2732 MS-1.5 Define procedures for the collection, analysis, access, and reporting of security-relevant
2733 data.

2734 MS-1.6 Define security-relevant criteria for evaluating the information items and the
2735 measurement process.

2736 *Note:* All criteria for a security-relevant information item are security-relevant.

2737 MS-1.7 Identify the security aspects for enabling the systems or services needed to support
2738 measurement.

2739 MS-1.8 Identify and plan for enabling the systems or services needed to support the security
2740 aspects of measurement.

2741 MS-1.9 Obtain or acquire access to the security aspects of enabling systems or services to be
2742 used in measurement.

2743 **References:** [[ISO 15288](#), Section 6.3.7.3 a)]; [[ISO 9001](#)]; [[ISO 15939](#)].

2744 **Related Publications:** [[ISO 12207](#), Section 6.3.7.3.1].

2745 MS-2 PERFORM MEASUREMENT

2746 MS-2.1 Integrate procedures for the generation, collection, analysis, and reporting of security-
2747 relevant data into the relevant processes.

2748 MS-2.2 Integrate procedures for the secure generation, collection, analysis, and reporting of
2749 data into the relevant processes.

2750 MS-2.3 Collect, store, and verify security-relevant data.

2751 MS-2.4 Securely collect, store, and verify data.

2752 MS-2.5 Analyze security-relevant data, and develop security-relevant information items.

2753 MS-2.6 Record security measurement results and inform the measurement users.

2754 *Note:* Security measurement results are provided to stakeholders and project personnel to
 2755 support decision-making, risk management, and to initiate corrective actions and improvements.

2756 **References:** [\[ISO 15288\]](#), Section 6.3.7.3 b)); [\[ISO 9001\]](#); [\[ISO 15939\]](#).

2757 **Related Publications:** [\[ISO 12207\]](#), Sections 6.3.7.3.2, 6.3.7.3.3].

2758 3.3.8 Quality Assurance

2759 The purpose of the *Quality Assurance* process is to help ensure the effective application of the
 2760 organization's *Quality Management* process to the project.

2761 [\[ISO 15288\]](#) Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

2762 3.3.8.1 Security Purpose

- 2763 • To help ensure the effective application of the organization's *Quality Management* process
 2764 to the security aspects of the project

2765 3.3.8.2 Security Outcomes

- 2766 • Security aspects of quality assurance procedures, including security criteria and methods for
 2767 quality assurance evaluations, are implemented.
- 2768 • Evaluations of the products, services, and processes of the project are performed in a
 2769 manner consistent with security quality management policies, procedures, and
 2770 requirements.
- 2771 • Security results of evaluations are provided to relevant stakeholders.
- 2772 • Security-relevant incidents are resolved.
- 2773 • Prioritized security-relevant problems are treated.

2774 3.3.8.3 Security Activities and Tasks

2775 QA-1 PREPARE FOR QUALITY ASSURANCE

2776 **QA-1.1** Define the security aspects of the quality assurance strategy.

2777 *Note:* The security aspects are informed by and consistent with the quality management policies,
 2778 objectives, and procedures and include:

- 2779 - Project security quality assurance procedures
- 2780 - Security roles, responsibilities, accountabilities, and authorities
- 2781 - Security activities appropriate to each life cycle process
- 2782 - Security activities appropriate to each supplier (including subcontractors)
- 2783 - Required security-oriented verification, validation, monitoring, measurement, inspection,
 2784 and test activities specific to the product or service
- 2785 - Security criteria for product or service acceptance

2786 **QA-1.2** Establish the independence of security quality assurance from other life cycle processes.

2787 **References:** [\[ISO 15288\]](#), Section 6.3.8.3 a)); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
 2788 [15026-4\]](#); [\[ISO 15408-1\]](#); [\[ISO 15408-2\]](#); [\[ISO 15408-3\]](#).

2789 **Related Publications:** [\[ISO 12207\]](#), Section 7.2.3.3.1].

- 2790 **QA-2** PERFORM PRODUCT OR SERVICE EVALUATIONS
- 2791 **QA-2.1** Evaluate products and services for conformance to established security criteria,
2792 contracts, standards, and regulations.
- 2793 **QA-2.2** Perform the security aspects of verification and validation on the outputs of the life
2794 cycle processes to determine conformance to specified requirements.
- 2795 **References:** [[ISO 15288](#), Section 6.3.8.3 b)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
2796 [15026-4](#)].
- 2797 **Related Publications:** [[ISO 12207](#), Section 7.2.3.3.2].
- 2798 **QA-3** PERFORM PROCESS EVALUATIONS
- 2799 **QA-3.1** Evaluate project life cycle processes for conformance to established security quality
2800 criteria.
- 2801 **QA-3.2** Evaluate tools and environments that support or automate the process for conformance
2802 to established security quality criteria.
- 2803 **QA-3.3** Evaluate supplier processes for conformance to process security requirements.
- 2804 *Note:* Consider items such as the security aspects of development environments, process
2805 measures that suppliers are required to provide, or a risk process that suppliers are required to
2806 use.
- 2807 **References:** [[ISO 15288](#), Section 6.3.8.3 c)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
2808 [15026-4](#)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].
- 2809 **Related Publications:** [[ISO 12207](#), Section 7.2.3.3.3].
- 2810 **QA-4** MANAGE QUALITY ASSURANCE RECORDS AND REPORTS
- 2811 **QA-4.1** Create records and reports related to the security aspects of quality assurance activities.
- 2812 **QA-4.2** Securely maintain, store, and distribute records and reports.
- 2813 **QA-4.3** Identify the security aspects of incidents and problems associated with product, service,
2814 and process evaluations.
- 2815 **References:** [[ISO 15288](#), Section 6.3.8.3 d)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
2816 [15026-4](#)].
- 2817 **Related Publications:** [[ISO 12207](#), Section 7.2.3.3.4].
- 2818 **QA-5** TREAT INCIDENTS AND PROBLEMS
- 2819 **QA-5.1** Record, analyze, and classify the security aspects of incidents.
- 2820 *Note:* Incidents are grouped (classified) by criteria such as type, scope, and effect.
- 2821 **QA-5.2** Resolve the security aspects of incidents, or elevate the security aspects of incidents to
2822 problems.
- 2823 **QA-5.3** Record, analyze, and classify the security aspects of problems.
- 2824 **QA-5.4** Track the security aspects of the prioritization and implementation of problem
2825 treatment.
- 2826 *Note:* This includes both security-driven problem treatment and the security aspects of general
2827 problem treatment.
- 2828 **QA-5.5** Note and analyze the security aspects of incidents and problems.

2829 **QA-5.6** Inform stakeholders of the status of the security aspects of incidents and problems.

2830 **QA-5.7** Track the security aspects of incidents and problems to closure.

2831 **References:** [ISO 15288, Section 6.3.8.3 e)]; [ISO 15026-1]; [ISO 15026-2]; [ISO 15026-3]; [ISO
2832 15026-4]; [ISO 24748-1].

2833 **Related Publications:** None.

2834 **3.4 TECHNICAL PROCESSES**

2835 This section contains the *Technical Processes* from [ISO 15288] with security-related
2836 considerations and contributions.

2837 **3.4.1 Business or Mission Analysis**

2838 The purpose of the *Business or Mission Analysis* process is to define the overall strategic
2839 problem or opportunity, characterize the solution space, and determine potential solution
2840 class(es) that can address a problem or take advantage of an opportunity.

2841 [ISO 15288] Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

2842 **3.4.1.1 Security Purpose**

- 2843 • To define the security aspects related to the strategic problems or opportunities
- 2844 • To identify the security objectives, concerns, and constraints that inform the potential
2845 solution classes

2846 **3.4.1.2 Security Outcomes**

- 2847 • Security aspects of the strategic problem or opportunity space are defined.
- 2848 • Security aspects of the solution space are characterized.
- 2849 • The definition of the preliminary operational concepts and other concepts in the life cycle
2850 stages are informed by the security aspects of the problem or opportunity space.
- 2851 • Alternative solution classes are analyzed considering identified security aspects.
- 2852 • Selection of the preferred alternative solution class(es) is informed by the security aspects
2853 of the solution space.
- 2854 • Enabling systems or services needed for the security aspects of business or mission analysis
2855 are available.
- 2856 • Traceability of the security aspects of the strategic problems and opportunities to the
2857 preferred alternative solution classes is established.

2858 **3.4.1.3 Security Activities and Tasks**

2859 **BA-1** PREPARE FOR BUSINESS OR MISSION ANALYSIS

2860 **BA-1.1** Identify the security aspects for enabling systems or services needed to support
2861 business or mission analysis.

2862 **BA-1.2** Identify and plan for enabling systems or services needed to support the security
2863 aspects of business or mission analysis.

- 2864 **BA-1.3** Obtain or acquire access to the security aspects of enabling systems or services to be
2865 used in business or mission analysis.
- 2866 **References:** [\[ISO 15288, Section 6.4.1.3 a\)\]](#).
- 2867 **Related Publications:** None.
- 2868 **BA-2** DEFINE THE PROBLEM OR OPPORTUNITY SPACE
- 2869 **BA-2.1** Analyze the problems or opportunities in the context of the security-relevant trade
2870 space factors.
- 2871 *Note:* The security-relevant trade space factors are analyzed within the context of all factors,
2872 including factors related to loss tolerances. The results of the analyses inform decisions on the
2873 suitability and feasibility of alternative options to be pursued.
- 2874 **BA-2.2** Define the security aspects of the mission, business, or operational problem or
2875 opportunity to be addressed by the solution class(es).
- 2876 *Note:* Information is elicited from stakeholders to acquire an understanding of the mission,
2877 business, or operational problem or opportunity from a system security perspective. Security
2878 aspects include security objectives, concerns, and constraints.
- 2879 **References:** [\[ISO 15288, Section 6.4.1.3 b\)\]](#); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
2880 [15026-4\]](#).
- 2881 **Related Publications:** None.
- 2882 **BA-3** CHARACTERIZE THE SOLUTION SPACE
- 2883 **BA-3.1** Define the security aspects of the preliminary operational concepts and other concepts
2884 in life cycle stages.
- 2885 *Note 1:* Security operational concepts include modes of secure operation, security-related
2886 operational scenarios and use cases, and secure usage within a mission area or line of business.
- 2887 *Note 2:* Security aspects are integrated into the life cycle concepts and used to support feasibility
2888 analysis and the evaluation of candidate alternative solution classes.
- 2889 **BA-3.2** Identify the security aspects of the alternative solution classes.
- 2890 **References:** [\[ISO 15288, Section 6.4.1.3 c\)\]](#); [\[ISO 42010\]](#); [\[ISO 24748-1\]](#).
- 2891 **Related Publications:** None.
- 2892 **BA-4** EVALUATE ALTERNATIVE SOLUTION CLASSES
- 2893 **BA-4.1** Assess each alternative solution class while considering the identified security aspects.
- 2894 **BA-4.2** Select the preferred alternative solution class (or classes) based on the identified
2895 security aspects, trade space factors, and other criteria defined by the organization.
- 2896 **BA-4.3** Provide security-relevant feedback to strategic level life cycle concepts to reflect the
2897 selected solution class(es).
- 2898 **References:** [\[ISO 15288, Section 6.4.1.3 d\)\]](#); [\[ISO 42010\]](#); [\[ISO 24748-1\]](#).
- 2899 **Related Publications:** None.
- 2900 **BA-5** MANAGE THE BUSINESS OR MISSION ANALYSIS
- 2901 **BA-5.1** Maintain traceability of the security aspects of business or mission analysis.

2902 *Note:* Bidirectional traceability is maintained between identified security aspects and supporting
 2903 security data associated with the problems and opportunities, proposed solution class or classes,
 2904 and organizational strategy.

2905 **BA-5.2** Provide the security-relevant artifacts that have been selected for baselines.

2906 **References:** [\[ISO 15288\]](#), Section 6.4.1.3 e); [\[ISO 42010\]](#); [\[ISO 24748-1\]](#).

2907 **Related Publications:** None.

2908 **3.4.2 Stakeholder Needs and Requirements Definition**

2909 The purpose of the *Stakeholder Needs and Requirements Definition* process is to define the
 2910 stakeholder requirements for a system that can provide the capabilities needed by users and
 2911 other stakeholders in a defined environment.

2912 [\[ISO 15288\]](#) Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

2913 **3.4.2.1 Security Purpose**

- 2914 • To identify the protection needs associated with the stakeholder needs and requirements
- 2915 for a system that can protect the capabilities needed by users and other stakeholders in a
- 2916 defined environment

2917 **3.4.2.2 Security Outcomes**

- 2918 • Security-relevant stakeholders of the system are identified.
- 2919 • Security concerns of stakeholders are identified.
- 2920 • Required characteristics and context for the secure use of capabilities for system life cycle
- 2921 concepts in system life cycle stages are defined.
- 2922 • Stakeholder assets and asset classes are identified.
- 2923 • Adversity presented by the environment is characterized.
- 2924 • Asset protection priorities are determined.
- 2925 • Stakeholder protection needs are defined.
- 2926 • Security-driven and security-informed constraints on a system are identified.
- 2927 • Prioritized stakeholder protection needs are transformed into stakeholder requirements.
- 2928 • Security-oriented performance measures and quality characteristics are defined.
- 2929 • Stakeholder agreement that their protection needs and expectations are adequately
- 2930 reflected in the requirements is achieved.
- 2931 • Enabling systems or services needed for the security aspects of stakeholder needs and
- 2932 requirements definition are available.
- 2933 • Traceability of stakeholder requirements to stakeholders and their protection needs is
- 2934 established.

2935 **3.4.2.3 Security Activities and Tasks**

2936 **SN-1** PREPARE FOR STAKEHOLDER NEEDS AND REQUIREMENTS DEFINITION

- 2937 **SN-1.1** Identify the stakeholders and their security concerns.
- 2938 *Note 1:* All stakeholders have security concerns, whether implicit or explicit.
- 2939 *Note 2:* This includes stakeholders who represent milestone decision authority, regulatory,
2940 certification, authorization, acceptance, and similar organizations with specific security-related
2941 decision-making authority and responsibilities.
- 2942 **SN-1.2** Define the stakeholder protection needs and requirements definition strategy.
- 2943 *Note:* The strategy includes addressing how consensus about protection needs and requirements
2944 is to be achieved among stakeholders with opposing interests.
- 2945 **SN-1.3** Identify the security aspects for enabling systems or services needed to support
2946 stakeholder needs and requirements definition.
- 2947 **SN-1.4** Identify and plan for enabling systems or services needed to support the security
2948 aspects of stakeholder needs and requirements definition.
- 2949 **SN-1.5** Obtain or acquire access to the security aspects of enabling systems or services to be
2950 used in stakeholder needs and requirements definition.
- 2951 **References:** [[ISO 15288](#), Section 6.4.2.3 a)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
2952 [15026-4](#)].
- 2953 **Related Publications:** [[ISO 12207](#), Section 6.4.1.3.1]; [[ISO 21827](#)].
- 2954 **SN-2** DEVELOP THE OPERATIONAL AND OTHER LIFE CYCLE CONCEPTS
- 2955 **SN-2.1** Define a representative set of scenarios to identify required protection capabilities and
2956 security measures that correspond to anticipated operational and other life cycle
2957 concepts.
- 2958 *Note:* The scenarios reflect how the system is intended to behave in the intended operational
2959 environments. Scenarios also help to identify security-driven changes to life cycle concepts.
- 2960 **SN-2.2** Characterize the security aspects of the operational environments and the intended
2961 users.
- 2962 *Note 1:* This includes distinguishing what is and is not known about adversity within the
2963 operational environments.
- 2964 *Note 2:* This includes the trust expectations for users to address insider threat concerns. If a user
2965 security aspect cannot be obtained or there is uncertainty about the trust of users, it will
2966 significantly drive design and the operational procedure to complement the design.
- 2967 **SN-2.3** Identify the interactions among entities (e.g., personnel, enabling and other interfacing
2968 systems) and the system and security-related factors affecting the interactions.
- 2969 *Note:* The interactions among entities and the system and the factors affecting the interactions
2970 need to be understood to inform engineering efforts. Factors influencing the interactions include
2971 the environment of the system of interest and any system of systems the system of interest
2972 belongs to, as well as the characterization of the entities with which the system interacts.
- 2973 **SN-2.4** Identify the security-related constraints on a system solution.
- 2974 **References:** [[ISO 15288](#), Section 6.4.2.3 c)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
2975 [15026-4](#)]; [[ISO 18152](#)]; [[ISO 25060](#)]; [[ISO 25063](#)]; [[ISO 29148](#)].
- 2976 **Related Publications:** [[ISO 9241](#)]; [[ISO 21827](#)]; [[ISO 25010](#)].
- 2977 **SN-3** DEFINE STAKEHOLDER NEEDS

- 2978 **SN-3.1** Define the rules capturing authorized and intended interactions, behaviors, and
 2979 outcomes.
- 2980 *Note:* The life cycle concepts and their context inform the rules.
- 2981 **SN-3.2** Identify stakeholder assets and asset classes.
- 2982 **SN-3.3** Identify loss concerns for each identified asset and each asset class.
- 2983 **SN-3.4** Prioritize assets based on the adverse consequence of asset loss.
- 2984 **SN-3.5** Determine adversities present in the environment.
- 2985 *Note:* Environments that expose the system to potential adversities can include test, operational,
 2986 maintenance, and logistical environments. The adversities need to be avoided when possible and
 2987 protected against otherwise.
- 2988 **SN-3.6** Identify stakeholder protection needs.
- 2989 **SN-3.7** Prioritize and down-select the stakeholder protection needs.
- 2990 **SN-3.8** Record the stakeholder protection needs and rationale.
- 2991 **References:** [[ISO 15288](#), Section 6.4.2.3 b)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
 2992 [15026-4](#)]; [[ISO 25063](#)].
- 2993 **Related Publications:** [[ISO 21827](#)]; [[ISO 18152](#)]; [[ISO 25010](#)].
- 2994 **SN-4** TRANSFORM STAKEHOLDER NEEDS INTO STAKEHOLDER REQUIREMENTS
- 2995 **SN-4.1** Identify the security-related constraints on a system solution.
- 2996 **SN-4.2** Define stakeholder requirements in a manner consistent with security aspects and
 2997 protection needs.
- 2998 **References:** [[ISO 15288](#), Section 6.4.2.3 d)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
 2999 [15026-4](#)]; [[ISO 25030](#)].
- 3000 **Related Publications:** [[ISO 12207](#), Section 6.4.1.3.2]; [[ISO 21827](#)]; [[ISO 15408-1](#)]; [[ISO 15408-2](#)];
 3001 [ISO 15408-3](#)]; [[ISO 27034-1](#)].
- 3002 **SN-5** ANALYZE STAKEHOLDER NEEDS AND REQUIREMENTS
- 3003 **SN-5.1** Analyze the set of stakeholder requirements with respect to the protection needs.
- 3004 *Note:* The stakeholder requirements are analyzed to determine if the protection needs are
 3005 accurately and comprehensively expressed in both individual requirements and the set of
 3006 requirements. Potential analysis characteristics include that the requirements: (1) are necessary,
 3007 complete, succinct, and implementation-free, and (2) comprehensively address the protection
 3008 needs.
- 3009 **SN-5.2** Define security-relevant performance and assurance measures that enable the
 3010 assessment of technical achievement and their relative criticality.
- 3011 *Note:* Determining the relative criticality of measures captures technical achievements and reflects
 3012 stakeholder priorities.
- 3013 **SN-5.3** Provide feedback to applicable stakeholders from the analyzed requirements to validate
 3014 that their protection needs and expectations have been adequately captured and
 3015 expressed.
- 3016 **SN-5.4** Resolve stakeholder requirements issues related to protection needs.

3017 *Note:* Any change to stakeholder requirements signifies a need to reassess protection needs and
 3018 determine if any subsequent changes are required.

3019 **References:** [[ISO 15288](#), Section 6.4.2.3 e)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
 3020 [15026-4](#)]; [[ISO 15939](#)]; [[ISO 29148](#)]; [[INCOSE10](#)].

3021 **Related Publications:** [[ISO 12207](#), Section 6.4.1.3.3]; [[ISO 21827](#)].

3022 **SN-6** MANAGE THE STAKEHOLDER NEEDS AND REQUIREMENTS DEFINITION

3023 **SN-6.1** Obtain explicit agreement that the stakeholder requirements satisfactorily address
 3024 protection needs.

3025 **SN-6.2** Record asset protection data.

3026 **SN-6.3** Maintain traceability between stakeholder protection needs and stakeholder
 3027 requirements.

3028 **SN-6.4** Provide the security-relevant artifacts that have been selected for baselines.

3029 **References:** [[ISO 15288](#), Section 6.4.2.3 f)].

3030 **Related Publications:** [[ISO 12207](#), Sections 6.4.1.3.4, 6.4.1.3.5]; [[ISO 21827](#)].

3031 **3.4.3 System Requirements Definition**

3032 The purpose of the *System Requirements Definition* process is to transform the stakeholder,
 3033 user-oriented view of desired capabilities into a technical view of a solution that meets the
 3034 operational needs of the user.

3035 [[ISO 15288](#)] Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

3036 **3.4.3.1 Security Purpose**

- 3037 • To provide an accurate and complete representation of stakeholder protection needs (as
 3038 expressed in the stakeholder requirements) in the system requirements

3039 **3.4.3.2 Security Outcomes**

- 3040 • Security aspects of the system description – including system interfaces, functions, and
 3041 boundaries for a system solution – are defined.
- 3042 • Security-relevant system requirements and security-driven design constraints are defined.
- 3043 • Security performance measures are defined.
- 3044 • Security aspects of the system requirements are analyzed.
- 3045 • Enabling systems or services needed for the security aspects of the system requirements
 3046 definition are available.
- 3047 • Traceability of the security aspects of system requirements and associated security-relevant
 3048 constraints to stakeholder requirements is established.

3049 **3.4.3.3 Security Activities and Tasks**

3050 **SR-1** PREPARE FOR SYSTEM REQUIREMENTS DEFINITION

3051 **SR-1.1** Define the security aspects of the intended behavior and outcomes at the functional
 3052 boundary of the system.

- 3053 *Note:* The intended behavior and security properties to be realized at the functional boundary
 3054 consider the characteristics of the capability provided or used, the characteristics of the entities
 3055 that interact with the system of interest at the functional boundary, and the associated
 3056 assurance needs.
- 3057 **SR-1.2** Define the security domains of the system and their correlation to the functional
 3058 boundaries of the system.
- 3059 **SR-1.3** Define the security aspects of the system requirements definition strategy.
- 3060 **SR-1.4** Identify the security aspects for enabling systems or services needed to support system
 3061 requirements definition.
- 3062 **SR-1.5** Identify and plan for enabling systems or services needed to support the security
 3063 aspects of system requirements definition.
- 3064 **SR-1.6** Obtain or acquire access to the security aspects of enabling systems or services to be
 3065 used in system requirements definition.
- 3066 **References:** [\[ISO 15288, Section 6.4.3.3 a\)\]](#); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
 3067 [15026-4\]](#).
- 3068 **Related Publications:** [\[ISO 21827\]](#).
- 3069 **SR-2** DEFINE SYSTEM REQUIREMENTS
- 3070 **SR-2.1** Define each security function that the system is required to perform.
- 3071 *Note:* Security functions are defined for all system states, modes, and conditions of system
 3072 operation and use, including the associated transitions between system states and modes.
 3073 Security functions include those oriented to delivery of capability and the ability of the system to
 3074 execute while preserving its inherent security characteristics.
- 3075 **SR-2.2** Define the security aspects of each function that the system is required to perform.
- 3076 *Note:* This includes the need for other system functions to be non-interfering (see [D.4.1](#)).
- 3077 **SR-2.3** Define necessary security-driven implementation constraints.
- 3078 *Note:* Security-driven constraints on the system are from adversity, uncertainty, and risk,
 3079 considering performance objectives and assurance needs. These constraints are informed by
 3080 stakeholder requirements, the system architecture definition, and solution limitations across the
 3081 life cycle.
- 3082 **SR-2.4** Define necessary constraints on security implementation.
- 3083 *Note:* Constraints on security implementation are to satisfy expectations for non-security
 3084 capability and performance.
- 3085 **SR-2.5** Define system security requirements and rationale.
- 3086 *Note:* System security requirements include security capability and functional requirements,
 3087 security performance and effectiveness requirements, security assurance requirements, and
 3088 implementation constraints (SR-2.3 and SR-2.4 outcomes expressed as requirements).
- 3089 **SR-2.6** Apply security metadata to the system security requirements.
- 3090 *Note:* Metadata enables identification and traceability to support analysis of completeness and
 3091 consistency to determine security impact when requirements change.
- 3092 **References:** [\[ISO 15288, Section 6.4.3.3 b\)\]](#); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
 3093 [15026-4\]](#); [\[ISO 27036-1\]](#); [\[ISO 27036-2\]](#); [\[ISO 27036-3\]](#); [\[ISO 29148\]](#); [\[ISO 25030\]](#).

- 3094 **Related Publications:** [[ISO 12207](#), Section 6.4.2.3.1]; [[ISO 15408-1](#)]; [[ISO 15408-2](#)]; [[ISO 15408-3](#)]; [[ISO 21827](#)]; [[ISO 27034-1](#)].
- 3095
- 3096 **SR-3 ANALYZE SYSTEM REQUIREMENTS**
- 3097 **SR-3.1** Analyze the complete set of system requirements in consideration of security concerns.
- 3098 *Note:* Requirements are analyzed to ensure that individual and combinations of requirements
- 3099 fully and properly capture security protection and security-constraint considerations. Rationale is
- 3100 captured to support analysis conclusions and provides a basis to conclude that the analysis has
- 3101 the proper perspective and is fully aware of assumptions made. See [Appendix C](#).
- 3102 **SR-3.2** Define security-driven performance and assurance measures that enable the
- 3103 assessment of technical achievement.
- 3104 **SR-3.3** Provide feedback from the analyzed system requirements to applicable stakeholders for
- 3105 security-relevant reviews.
- 3106 **SR-3.4** Resolve system requirements security issues.
- 3107 **References:** [[ISO 15288](#), Section 6.4.3.3 c)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
- 3108 [15026-4](#)]; [[ISO 15939](#)]; [[ISO 29148](#)]; [[INCOSE10](#)].
- 3109 **Related Publications:** [[ISO 12207](#), Section 6.4.2.3.2]; [[ISO 21827](#)].
- 3110 **SR-4 MANAGE THE SYSTEM REQUIREMENTS**
- 3111 **SR-4.1** Obtain explicit agreement that system requirements express protection needs.
- 3112 **SR-4.2** Record key security-related system requirement decisions and the rationale.
- 3113 **SR-4.3** Maintain traceability of system requirements to their security-relevant aspects.
- 3114 *Note:* The traceability of system requirements to protection needs; stakeholder requirements;
- 3115 architecture elements; interface definitions; analysis results; verification methods; and all
- 3116 allocated, decomposed, and *derived requirements* (in their system, system element, security
- 3117 protection, and security-driven constraint forms); risk and loss tolerance; and assurance and
- 3118 trustworthiness objectives is maintained.
- 3119 **SR-4.4** Provide the security-relevant artifacts that have been selected for baselines.
- 3120 **References:** [[ISO 15288](#), Section 6.4.3.3 d)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
- 3121 [15026-4](#)].
- 3122 **Related Publications:** [[ISO 21827](#)].
- 3123 **3.4.4 System Architecture Definition**
- 3124 The purpose of the *System Architecture Definition* process is to generate system architecture
- 3125 alternatives, to select one or more alternative(s) that frame stakeholder concerns and meet
- 3126 system requirements, and to express this in a set of consistent views and models.
- 3127 [[ISO 15288](#)] Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.
- 3128 **3.4.4.1 Security Purpose**
- 3129 • To generate the architectural concepts and properties of system architecture alternatives
- 3130 for the system protection capability that frame stakeholder protection concerns and meet
- 3131 system requirements
- 3132 • To express them in a set of consistent views and models

- 3133 • To provide the security aspects used to select one or more architecture alternatives
- 3134 **3.4.4.2 Security Outcomes**
- 3135 • The problem space is refined with respect to key stakeholder security concerns.
- 3136 • Alignment of the architecture with applicable security policies, directives, objectives, and
3137 constraints is achieved.
- 3138 • Concepts, properties, characteristics, behaviors, functions, and constraints that are
3139 significant to security-relevant architecture decisions about the system are allocated to
3140 architectural entities.
- 3141 • Identified stakeholder protection concerns are addressed by the system architecture.
- 3142 • Traceability of the security aspects of system architecture elements to key architecturally
3143 relevant stakeholder and system requirements is established.
- 3144 • Security aspects of architecture views and models of the system are developed.
- 3145 • Security aspects of system elements, their interactions, and their interfaces are defined.
- 3146 **3.4.4.3 Security Activities and Tasks**
- 3147 **AR-1 PREPARE FOR SYSTEM ARCHITECTURE DEFINITION**
- 3148 **AR-1.1** Define the security aspects of the system architecture definition strategy.
- 3149 **AR-1.2** Identify the set of existing security-relevant architectures or reference architectures that
3150 may have direct applicability and are to be used as guiding oversight.
- 3151 **AR-1.3** Establish the security aspects of the architecture description framework(s), viewpoints,
3152 and modeling templates to be used throughout the system architecture definition
3153 effort.
- 3154 **AR-1.4** Establish security-specific viewpoints and modeling templates to be used throughout
3155 the system architecture definition effort.
- 3156 **AR-1.5** Determine the security evaluation objectives and criteria with respect to the concerns of
3157 key stakeholders.
- 3158 **AR-1.6** Determine security evaluation methods and integrate with evaluation objectives and
3159 criteria.
- 3160 **AR-1.7** Collect and review security evaluation-related information.
- 3161 **AR-1.8** Identify the security aspects for enabling systems or services needed to support system
3162 architecture definition.
- 3163 **AR-1.9** Identify and plan for enabling systems or services needed to support the security
3164 aspects of system architecture definition.
- 3165 **AR-1.10** Obtain or acquire access to the security aspects of enabling systems or services to be
3166 used in system architecture definition.
- 3167 **References:** [[ISO 15288](#), Section 6.4.4.3 a)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
3168 [15026-4](#)]; [[ISO 42010](#)]; [[ISO 42020](#)].
- 3169 **Related Publications:** [[ISO 21827](#)].
- 3170 **AR-2 CREATE THE SYSTEM ARCHITECTURE CANDIDATE(S)**

- 3171 **AR-2.1** Establish the security aspects of architecture objectives and critical success criteria.
- 3172 **AR-2.2** Synthesize potential trustworthy secure solution(s) in the solution space.
- 3173 **AR-2.3** Characterize aspects of trustworthy secure solutions and the trade space.
- 3174 **AR-2.4** Formulate trustworthy secure candidate architecture(s).
- 3175 **AR-2.5** Capture trustworthy secure architecture concepts and properties.
- 3176 **AR-2.6** Relate the candidate architecture(s) to other architectures and relevant affected entities
3177 to help ensure the consistency of trustworthy secure architecture concepts and
3178 properties.
- 3179 **AR-2.7** Coordinate the secure use of the candidate architecture(s) by intended users.
- 3180 **AR-2.8** Develop the security aspects of the models and views of the candidate architecture(s).
- 3181 *Note:* The following are typical considerations to define the security aspects of the system
3182 context and boundaries in terms of interfaces and interactions between entities:
- 3183 - Definition of the system security context and security boundaries in terms of interfaces and
3184 interactions with external entities
 - 3185 - The identification of architectural entities and relationships between entities that address
3186 key stakeholder protection concerns and system security requirements
 - 3187 - The allocation of security concepts, security properties, security characteristics, secure
3188 behaviors, security functions, or security constraints that are significant to architecture
3189 decisions of the system to architectural entities
 - 3190 - Composition of views from the models in accordance with identified viewpoints to express
3191 how the architecture addresses stakeholder protection concerns and meets stakeholder and
3192 system security requirements
 - 3193 - Harmonization of the architecture models and views
- 3194 **AR-2.9** Coordinate secure use of the architecture by intended users.
- 3195 **References:** [[ISO 15288](#), Section 6.4.4.3 a)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
3196 [15026-4](#)]; [[ISO 42010](#)]; [[ISO 42020](#)].
- 3197 **Related Publications:** [[ISO 21827](#)].
- 3198 **AR-3** EVALUATE THE SYSTEM ARCHITECTURE CANDIDATE(S)
- 3199 **AR-3.1** Analyze trustworthy secure architecture concepts and properties, and assess the value
3200 of the architecture in meeting stakeholder security protection concerns.
- 3201 **AR-3.2** Characterize the candidate architecture(s) based on trustworthy secure analysis results.
- 3202 **AR-3.3** Formulate security-relevant evaluation findings and recommendations.
- 3203 **AR-3.4** Capture and communicate security-relevant evaluation results.
- 3204 **AR-3.5** Relate the architecture to the other architectures and to relevant affected entities to
3205 help ensure consistency in the trustworthy secure system architecture.
- 3206 **References:** [[ISO 15288](#), Section 6.4.4.3 c)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
3207 [15026-4](#)]; [[ISO 42010](#)]; [[ISO 42020](#)].
- 3208 **Related Publications:** [[ISO 21827](#)].
- 3209 **AR-4** MANAGE THE RESULTS OF SYSTEM ARCHITECTURE DEFINITION
- 3210 **AR-4.1** Obtain agreement on the security aspects of the architecture.

- 3246 **DE-1.4** Determine the necessary security and trustworthiness categories of system
3247 characteristics represented in the design.
- 3248 *Note:* Such characteristics include applying foundational security design principles and concepts
3249 with the necessary rigor to achieve target levels of assurance.
- 3250 **DE-1.5** Define the principles for trustworthy secure evolution of the system design.
- 3251 **DE-1.6** Identify the security aspects for enabling systems or services needed to support design
3252 definition.
- 3253 **DE-1.7** Identify and plan for enabling systems or services needed to support the security
3254 aspects of design definition.
- 3255 **DE-1.8** Obtain or acquire access to the security aspects of enabling systems or services to be
3256 used in design definition.
- 3257 **References:** [\[ISO 15288, Section 6.4.5.3 a\)\]](#); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
3258 [15026-4\]](#).
- 3259 **Related Publications:** [\[ISO 21827\]](#).
- 3260 **DE-2** CREATE THE SYSTEM DESIGN
- 3261 **DE-2.1** Allocate security requirements to system elements.
- 3262 *Note:* This allocates the security aspects of architecture, behavior, and constraints to the system
3263 design.
- 3264 **DE-2.2** Transform security-relevant architectural entities and relationships into design
3265 elements.
- 3266 **DE-2.3** Transform secure architectural characteristics into trustworthy secure design
3267 characteristics.
- 3268 *Note 1:* The transformation applies the architectural, trust, and security design principles in
3269 successively finer-grained contexts to express the security design characteristics for the
3270 constituent components of architectural entities. Security design characteristics apply to security
3271 functional capabilities.
- 3272 *Note 2:* The characteristics include or reflect the expected level of assurance.
- 3273 **DE-2.4** Define the necessary trustworthy secure design enablers.
- 3274 *Note:* Trustworthy secure design enablers include standards, specifications, patterns, models for
3275 security policy, security protocols, strength of mechanism, cryptographic algorithms, adversarial
3276 threat actors, and functional behaviors and interactions.
- 3277 **DE-2.5** Examine trustworthy secure design alternatives.
- 3278 *Note:* Assess the feasibility of each design alternative to minimize susceptibility, exposure,
3279 vulnerability, and hazard based on the allocation of system characteristics.
- 3280 **DE-2.6** Refine or define the security aspects of interfaces between system elements and with
3281 external entities.
- 3282 *Note:* The details of the defined interfaces are refined to capture additional details provided by
3283 the security aspects of the design. In addition, the interfaces, interconnections, behavior, and
3284 interactions for components within the system of interest are identified, as are the security and
3285 security-driven design constraints applied on all interfaces, interactions, and behavior between
3286 components of the system of interest.
- 3287 **DE-2.7** Develop the security aspects of design artifacts.

3288 *Note:* Design artifacts include general and security-specific specifications, data sheets, databases,
3289 and documents.

3290 **DE-2.8** Capture the security aspects of the design.

3291 **References:** [ISO 15288, Section 6.4.5.3 b)]; [ISO 15026-1]; [ISO 15026-2]; [ISO 15026-3]; [ISO
3292 15026-4].

3293 **Related Publications:** [ISO 12207, Sections 6.4.3.3.1, 7.1.4.3.1]; [ISO 27034-1]; [ISO 15408-1];
3294 [ISO 15408-2]; [ISO 15408-3]; [ISO 21827].

3295 **DE-3** EVALUTE THE SYSTEM DESIGN

3296 **DE-3.1** Analyze each system design alternative against criteria developed from expected
3297 trustworthy secure design properties and characteristics.

3298 **DE-3.2** Assess each system design alternative for how well it meets stakeholder protection
3299 needs and the security aspects of the system requirements.

3300 **DE-3.3** Combine the security analyses and assessments in the overall evaluation to select a
3301 preferred design solution.

3302 **References:** [ISO 15288, Section 6.4.5.3 c)]; [ISO 15026-1]; [ISO 15026-2]; [ISO 15026-3]; [ISO
3303 15026-4].

3304 **Related Publications:** [ISO 12207, Section 6.4.3.3.2]; [ISO 27034-1]; [ISO 21827].

3305 **DE-4** MANAGE THE RESULTS OF DESIGN DEFINITION

3306 **DE-4.1** Obtain agreement on the security aspects of the design.

3307 **DE-4.2** Map the trustworthy secure design characteristics to the system elements.

3308 **DE-4.3** Record the trustworthy secure design decisions and the rationale.

3309 **DE-4.4** Maintain traceability of the security aspects of the system design.

3310 *Note:* Traceability is maintained between the trustworthy secure design characteristics and the
3311 security architectural entities, system element requirements, interface definitions, analysis
3312 results, and verification and validation methods or techniques.

3313 **DE-4.5** Provide the security-relevant artifacts that have been selected for baselines.

3314 **References:** [ISO 15288, Section 6.4.5.3 d)].

3315 **Related Publications:** [ISO 15408-1]; [ISO 15408-2]; [ISO 15408-3]; [ISO 21827].

3316 **3.4.6 System Analysis**

3317 The purpose of the *System Analysis* process is to provide a rigorous basis of data and
3318 information for technical understanding to aid decision-making and technical assessments
3319 across the life cycle.

3320 [ISO 15288] Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

3321 **3.4.6.1 Security Purpose**

- 3322 • To produce a rigorous basis of data and information for the technical understanding of
3323 security aspects to aid decision-making and technical assessments across the life cycle

3324 **3.4.6.2 Security Outcomes**

- 3325 • Security aspects of system analysis needs are identified.
- 3326 • Security aspects of system analysis assumptions and results are validated.
- 3327 • System analysis results provided for all decisions or technical assessment needs include
3328 security aspects.
- 3329 • Enabling systems or services for the security aspects of system analysis are available.
- 3330 • Traceability of the security aspects of the system analysis results is established.

3331 3.4.6.3 Security Activities and Tasks

3332 SA-1 PREPARE FOR SYSTEM ANALYSIS

3333 SA-1.1 Define the security aspects of the system analysis strategy.

3334 SA-1.2 Identify the security aspects of the problem or question that require system analysis.

3335 *Note:* The problem or question may not be driven by or have obvious security consideration or
3336 aspects.

3337 SA-1.3 Identify the security-relevant stakeholders of the system analysis.

3338 SA-1.4 Define the scope, objectives, level of fidelity, level of rigor, and level of assurance for the
3339 security aspects of system analysis.

3340 SA-1.5 Select the methods to address the security aspects of system analysis.

3341 SA-1.6 Identify the security aspects for enabling systems or services needed to support system
3342 analysis.

3343 SA-1.7 Identify and plan for enabling systems or services needed to support the security
3344 aspects of system analysis.

3345 SA-1.8 Obtain or acquire access to the security aspects of enabling systems or services to be
3346 used in system analysis.

3347 SA-1.9 Identify and validate security-relevant assumptions.

3348 *Note 1:* This includes assumptions derived from the limits of certainty: what is known, what is
3349 insufficiently known, and what is unknown.

3350 *Note 2:* Assumptions that cannot be validated represent uncertainty and potential risk.

3351 SA-1.10 Plan for and collect the data and inputs needed for the security aspects of the analysis.

3352 **References:** [[ISO 15288](#), Section 6.4.6.3 a)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
3353 [15026-4](#)].

3354 **Related Publications:** [[ISO 21827](#)].

3355 SA-2 PERFORM SYSTEM ANALYSIS

3356 SA-2.1 Apply the selected analysis methods to perform the required security-relevant aspects
3357 of system analysis.

3358 SA-2.2 Review analysis results for security-relevant quality and validity.

3359 *Note:* The results are coordinated with associated and previously completed security-relevant
3360 analyses. Trustworthiness of the results is determined with the review.

- 3396 *Note 1:* These aspects apply to all system elements that are acquired new, built new, or reused
 3397 (with or without modification). If the strategy is reuse, then the project needs to determine the
 3398 extent, source, suitability, and trustworthiness for the purpose of the reused system elements.
 3399 The implementation strategy includes procedures, fabrication processes, tools and equipment,
 3400 tolerances, and verification uncertainties, which may introduce weaknesses and vulnerabilities.
 3401 In the case of repeated system element implementation (e.g., mass production, replacement
 3402 system elements), the procedures and fabrication processes are defined to achieve consistent
 3403 and repeatable trustworthy producibility.
- 3404 *Note 2:* The security aspects are informed by the targeted level of assurance, security verification
 3405 uncertainties, and security concerns associated with implementation-related logistics, supply,
 3406 and distribution of components.
- 3407 **IP-1.2** Identify security-relevant constraints and objectives from implementation in the system
 3408 security requirements, architecture and design characteristics, or implementation
 3409 techniques.
- 3410 **IP-1.3** Identify the security aspects for enabling systems, services, and materials needed to
 3411 support implementation.
- 3412 **IP-1.4** Identify and plan for enabling systems, services, and materials needed to support the
 3413 security aspects of implementation.
- 3414 **IP-1.5** Obtain or acquire access to the security aspects of enabling systems, services, and
 3415 materials to be used in implementation.
- 3416 **References:** [[ISO 15288](#), Section 6.4.7.3 a)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
 3417 [15026-4](#)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].
- 3418 **Related Publications:** None.
- 3419 **IP-2** PERFORM IMPLEMENTATION
- 3420 **IP-2.1** Realize or adapt system elements in accordance with the security aspects of the
 3421 implementation strategy and implementation procedures, as well as security-relevant
 3422 constraints.
- 3423 *Note:* System elements can include:
- 3424 - *Hardware and Software:* Hardware and software elements are either acquired or fabricated.
 3425 Custom hardware fabrication and software development enable insight into the details of
 3426 design and implementation. These insights often translate to increased assurance.
 3427 Acquired hardware and software elements may not provide the opportunity to achieve the
 3428 same insight into design and implementation and may offer more functionality and
 3429 capability than required. The limits of what can be known about the internals of the
 3430 elements translate to a level of uncertainty about vulnerability and to the maximum
 3431 assurance that can be achieved.
 - 3432 - *Firmware:* Firmware exhibits properties of hardware and software. Firmware elements may
 3433 be acquired or may be developed to realize the software aspects and then fabricated to
 3434 realize the physical form of the hardware aspects. Firmware elements, therefore, adhere to
 3435 the security implementation considerations of both hardware and software elements.
 - 3436 - *Services:* System elements implemented by obtaining or leasing services are subject to the
 3437 same criteria used to acquire hardware, firmware, and software but must also address
 3438 security considerations associated with utilization and support resources.
 - 3439 - *Utilization and Support Resources:* The security considerations of services acquired or leased
 3440 must account for the specific roles and responsibilities of individuals of the service/lease

- 3441 provider and their ability to account for all of the security requirements and constraints
 3442 associated with the delivery, utilization, and sustainment of the service or capability being
 3443 leased.
- 3444 **IP-2.2** Place the system element in a secure state for future use, as needed.
- 3445 *Note:* This includes protection of the element while stored and in transit, as well as the packaging
 3446 and labeling of the element.
- 3447 **IP-2.3** Record objective evidence that system elements meet the system security
 3448 requirements.
- 3449 **References:** [\[ISO 15288, Section 6.4.7.3 b\)\]](#); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
 3450 [15026-4\]](#); [\[ISO 27036-1\]](#); [\[ISO 27036-2\]](#); [\[ISO 27036-3\]](#).
- 3451 **Related Publications:** [\[ISO 12207, Section 7.1.5.3.1\]](#); [\[ISO 27034-1\]](#).
- 3452 **IP-3** MANAGE RESULTS OF IMPLEMENTATION
- 3453 **IP-3.1** Record the security aspects of implementation results and any anomalies encountered.
- 3454 **IP-3.2** Maintain traceability of the security aspects of implemented system elements.
- 3455 *Note:* Bidirectional traceability of the security aspects of the implemented system elements to
 3456 the system security requirements, the security views of the architecture, the security design, and
 3457 the security interface requirements is maintained.
- 3458 **IP-3.3** Provide the security-relevant artifacts that have been selected for baselines.
- 3459 **References:** [\[ISO 15288, Section 6.4.7.3 c\)\]](#); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
 3460 [15026-4\]](#).
- 3461 **Related Publications:** None.
- 3462 **3.4.8 Integration**
- 3463 The purpose of the *Integration* process is to synthesize a set of system elements into a
 3464 realized system that satisfies the system requirements.
- 3465 [\[ISO 15288\]](#) Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.
- 3466 **3.4.8.1 Security Purpose**
- 3467 • To synthesize a set of system elements into a realized trustworthy secure system that
 3468 satisfies the system requirements
- 3469 **3.4.8.2 Security Outcomes**
- 3470 • Security-relevant integration constraints that influence requirements, architecture, design,
 3471 or interfaces and interactions are identified.
- 3472 • Approaches and checkpoints for the correct secure activation of the identified interfaces
 3473 and system functions to an initial or established secure state are developed.
- 3474 • Enabling systems or services for the security aspects of integration are available.
- 3475 • A trustworthy secure system composed of implemented system elements is integrated.
- 3476 • Security aspects of system external interfaces (system to external environment) and system
 3477 internal interfaces (between implemented system elements) are checked.

- 3478 • Security aspects of integration results and anomalies are identified.
- 3479 • Traceability of the security aspects of the integrated system elements is established.

3480 3.4.8.3 Security Activities and Tasks

3481 IN-1 PREPARE FOR INTEGRATION

3482 **IN-1.1** Identify and define checkpoints for the correct secure activation and integrity of the
3483 interfaces and the selected system functions as the system elements are synthesized.

3484 **IN-1.2** Define the security aspects of the integration strategy.

3485 *Note:* Integration is performed to achieve trustworthy secure results using aspects such as secure
3486 assembly sequences and checkpoints for the system elements based on established priorities
3487 while minimizing integration time and cost and providing appropriate risk treatments.

3488 **IN-1.3** Identify the security-relevant constraints and objectives from integration to be
3489 incorporated in the system requirements, architecture, or design.

3490 **IN-1.4** Identify the security aspects for enabling systems, services, and materials needed to
3491 support to support integration.

3492 **IN-1.5** Identify and plan for enabling systems, services, and materials needed to support the
3493 security aspects of integration.

3494 **IN-1.6** Obtain or acquire access to the security aspects of enabling systems, services, and
3495 materials to be used in integration.

3496 **References:** [[ISO 15288](#), Section 6.4.8.3 a)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
3497 [15026-4](#)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].

3498 **Related Publications:** [[ISO 21827](#)].

3499 IN-2 PERFORM INTEGRATION

3500 **IN-2.1** Check interface availability and conformance of the interfaces in accordance with the
3501 security aspects of interface definitions and integration schedules.

3502 **IN-2.2** Perform actions to address any security-related conformance or availability issues.

3503 **IN-2.3** Securely combine the implemented system elements in accordance with planned
3504 sequences.

3505 **IN-2.4** Securely integrate system element configurations until the complete system is securely
3506 synthesized.

3507 **IN-2.5** Check for the expected results of interfaces, interconnections, selected functions, and
3508 security characteristics.

3509 **References:** [[ISO 15288](#), Section 6.4.8.3 b)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].

3510 **Related Publications:** [[ISO 12207](#), Sections 6.4.5.3.2, 7.1.6.3.1]; [[ISO 27034-1](#)]; [[ISO 21827](#)].

3511 IN-3 MANAGE RESULTS OF INTEGRATION

3512 **IN-3.1** Record the security aspects of integration results and any anomalies encountered.

3513 *Note:* Anomaly analyses determine corrective actions that possibly affect the protection
3514 capability of the system and the level of assurance that can be obtained.

3515 **IN-3.2** Maintain traceability of the security aspects of integrated system elements.

3516 *Note:* Bidirectional traceability of the security aspects of the integrated system elements to the
 3517 system security requirements, security views of the architecture, security design, and security
 3518 interface requirements is maintained. Traceability provides evidence that supports assurance
 3519 and trustworthiness claims.

3520 **IN-3.3** Provide the security-relevant artifacts that have been selected for baselines.

3521 **References:** [\[ISO 15288](#), Section 6.4.8.3 c)]; [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
 3522 [15026-4\]](#).

3523 **Related Publications:** [\[ISO 21827\]](#).

3524 **3.4.9 Verification**

3525 The purpose of the *Verification* process is to provide objective evidence that a system,
 3526 system element, or artifact fulfills its specified requirements and characteristics.

3527 [\[ISO 15288\]](#) Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

3528 **3.4.9.1 Security Purpose**

- 3529 • To provide objective evidence that a system, system element, or artifact (e.g., system
 3530 requirements, architecture description, or design description) fulfills its specified security
 3531 requirements and characteristics
- 3532 • To identify security-relevant anomalies⁶⁴ in any artifact, implemented system elements, or
 3533 life cycle processes, and provide the necessary information to determine the resolution of
 3534 such anomalies

3535 **3.4.9.2 Security Outcomes**

- 3536 • Security-relevant verification constraints that influence requirements, architecture, or
 3537 design are identified.
- 3538 • Enabling systems or services for the security aspects of verification are available.
- 3539 • Security aspects of the system, system element, or artifact are verified.
- 3540 • Security-relevant data that provides information for corrective actions is reported.
- 3541 • Objective evidence that the realized system fulfills the security requirements and security
 3542 aspects of the architecture and design is provided.
- 3543 • Security aspects of verification results and anomalies are identified.
- 3544 • Traceability of the security aspects of the verified system elements is established.

3545 **3.4.9.3 Security Activities and Tasks**

3546 **VE-1** PREPARE FOR VERIFICATION

3547 **VE-1.1** Identify the security aspects within the verification scope and corresponding security
 3548 verification actions.

3549 *Note:* Scope includes system, system elements, information items or artifacts that will be verified
 3550 against applicable requirements, security characteristics, or other security properties. Each

⁶⁴ Anomalies include behaviors and outcomes observed but not specified.

- 3551 verification action description includes what will be verified (e.g., actual system, model, mock-up,
3552 prototype, procedure, plan, or other document), the verification method (including any adversity
3553 emulation), and the expected result as defined by the success criteria. The security criteria may
3554 reflect considerations of strength of function/mechanism, resistance to tamper, misuse or abuse,
3555 penetration resistance, level of assurance, absence of flaws, weaknesses, and the absence of
3556 unspecified behavior and outcomes.
- 3557 **VE-1.2** Identify the constraints that can potentially limit the feasibility of the security-focused
3558 verification actions.
- 3559 *Note:* Constraints include technical feasibility; the availability of qualified personnel and
3560 verification enablers; the availability of sufficient, relevant, and credible threat data; technology
3561 employed (including adversity emulation); the size and complexity of the system element or
3562 artifact; and the cost and time allotted for the verification.
- 3563 **VE-1.3** Select appropriate security verification methods and the associated success criteria for
3564 each security verification action.
- 3565 *Note:* The methods and techniques are selected to provide the evidence required to achieve the
3566 expected results with the desired level of assurance.
- 3567 **VE-1.4** Define the security aspects of the verification strategy.
- 3568 *Note:* This includes the approach used to incorporate security considerations into all verification
3569 actions, considering trade-offs between scope, depth, and rigor needed for the desired level of
3570 assurance and the given constraints.
- 3571 **VE-1.5** Identify the security-relevant constraints and objectives that result from the security
3572 aspects of the verification strategy to be incorporated into the system requirements,
3573 architecture, and design.
- 3574 **VE-1.6** Identify the security aspects for enabling systems or services needed to support
3575 verification.
- 3576 **VE-1.7** Identify and plan for enabling systems or services needed to support the security
3577 aspects of verification.
- 3578 **VE-1.8** Obtain or acquire access to the security aspects of enabling systems or services to be
3579 used in verification.
- 3580 **References:** [\[ISO 15288](#), Section 6.4.9.3 a)]; [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
3581 [15026-4](#) [\[ISO 29119-1\]](#); [\[ISO 29119-2\]](#); [\[ISO 29119-3\]](#); [\[ISO 29119-4\]](#); [\[ISO 29148\]](#)].
- 3582 **Related Publications:** [\[ISO 12207](#), Section 7.2.4.3.1]; [\[ISO 21827\]](#)].
- 3583 **VE-2** PERFORM VERIFICATION
- 3584 **VE-2.1** Define the security aspects of the verification procedures, each supporting one or a set
3585 of verification actions.
- 3586 *Note:* The procedures identify the security purpose of verification, the success criteria (expected
3587 results), the verification method to be applied, the necessary enabling systems (e.g., facilities,
3588 equipment, etc.), and the environmental conditions to perform each verification procedure (e.g.,
3589 resources, qualified personnel, adversity emulations, etc.).
- 3590 **VE-2.2** Perform security verification procedures.
- 3591 **References:** [\[ISO 15288](#), Section 6.4.9.3 b)].
- 3592 **Related Publications:** [\[ISO 12207](#), Sections 6.4.6.3.1, 7.1.7.3.1, 7.2.4.3.2]; [\[ISO 27034-1\]](#); [\[ISO](#)
3593 [21827\]](#)].

3594 **VE-3** MANAGE RESULTS OF VERIFICATION3595 **VE-3.1** Record the security aspects of verification results and any anomalies encountered.3596 **VE-3.2** Obtain agreement from the approval authority that the system, system element, or
3597 artifact meets the specified system security requirements.3598 *Note:* There may be multiple approval authorities with security-related responsibilities.3599 **VE-3.3** Maintain traceability of the security aspects of verification.3600 *Note:* Bidirectional traceability is maintained between the verified security aspects of system
3601 elements and the system security requirements, architecture, design, and interface
3602 requirements. This traceability includes verification results or evidence, such as security-relevant
3603 anomalies, deviations, or requirement satisfaction.3604 **VE-3.4** Provide the security-relevant artifacts that have been selected for baselines.3605 **References:** [[ISO 15288](#), Section 6.4.9.3 c)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
3606 [15026-4](#)]; [[ISO 27034-1](#)].3607 **Related Publications:** [[ISO 21827](#)].3608 **3.4.10 Transition**3609 The purpose of the *Transition* process is to establish a capability for a system to provide
3610 services specified by stakeholder requirements in the operational environment.3611 [[ISO 15288](#)] Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.3612 **3.4.10.1 Security Purpose**

- 3613 • To preserve the system's verified security characteristics during the orderly and planned
-
- 3614 transition of the system to be operable in the intended environment, which may be a new
-
- 3615 or changed environment

3616 **3.4.10.2 Security Outcomes**

- 3617 • Security-relevant transition constraints that influence system requirements, architecture, or
-
- 3618 design are identified.
-
- 3619 • Enabling systems or services for the security aspects of transition are available.
-
- 3620 • The prepared site satisfies security criteria.
-
- 3621 • The system is installed in its operational environment and is capable of delivering its
-
- 3622 specified functions in a trustworthy secure manner.
-
- 3623 • Operators, users, and other stakeholders necessary to the system utilization and support are
-
- 3624 trained in the system's security capabilities, mechanisms, and features.
-
- 3625 • Security-relevant transition results and anomalies are identified.
-
- 3626 • The installed system is activated and ready for trustworthy secure operation.
-
- 3627 • Traceability of the security aspects of the transitioned elements is established.

3628 **3.4.10.3 Security Activities and Tasks**3629 **TR-1** PREPARE FOR TRANSITION

- 3630 **TR-1.1** Define the security aspects of the transition strategy.
- 3631 *Note:* The transition strategy includes all security-relevant activities, from site delivery and
 3632 installation through deployment and commissioning of the system, as well as all security-relevant
 3633 stakeholders, including human operators. The strategy also includes security roles and
 3634 responsibilities, facilities security considerations, secure shipping and receiving, contingency back
 3635 out plans, security training, security aspects of installation acceptance demonstration tasks,
 3636 secure operational readiness reviews, secure operations commencement, transition security
 3637 success criteria, rights of secure access, data rights, and integration with other plans. System
 3638 commissioning is considered along with the secure decommissioning of the old system when one
 3639 exists. In this case, the Transition and Disposal processes are used concurrently.
- 3640 **TR-1.2** Identify and define any security-relevant facility or site changes needed.
- 3641 **TR-1.3** Identify the security-relevant constraints and objectives from the security aspects of
 3642 transition to be incorporated into the system requirements, architecture, and design.
- 3643 **TR-1.4** Identify and arrange the security training of operators, users, and other stakeholders
 3644 necessary to the system utilization and support.
- 3645 **TR-1.5** Identify the security aspects for enabling systems or services needed to support
 3646 transition.
- 3647 **TR-1.6** Identify and plan for enabling systems or services needed to support the security
 3648 aspects of transition.
- 3649 **TR-1.7** Obtain or acquire access to the security aspects of enabling systems or services to be
 3650 used in transition.
- 3651 **TR-1.8** Identify security aspects, and arrange for the secure shipping and receiving of system
 3652 elements and enabling systems.
- 3653 **References:** [\[ISO 15288](#), Section 6.4.10.3 a)]; [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
 3654 [15026-4\]](#).
- 3655 **Related Publications:** None.
- 3656 **TR-2** PERFORM TRANSITION
- 3657 **TR-2.1** Prepare the site of operation in accordance with secure installation requirements.
- 3658 **TR-2.2** Securely deliver the system for installation at the correct location and time.
- 3659 *Note:* Secure delivery considers the various forms, means, and methods that accomplish end-to-
 3660 end transport of system elements to ensure that system elements are not tampered with during
 3661 transport. Items and packages are delivered to the intended recipient and only to the intended
 3662 recipient, which may mean shipping with more lead time to account for additional security.
- 3663 **TR-2.3** Install the system in its operational environment in accordance with the secure
 3664 installation strategy, and establish secure interconnections to its environment.
- 3665 **TR-2.4** Demonstrate trustworthy secure system installation.
- 3666 *Note:* The installation and connection procedures are to be properly verified to provide
 3667 confidence that the intended system configuration across all system modes and states is
 3668 achieved. This includes completion of the acceptance tests defined in agreements. These tests
 3669 include security aspects associated with physical connections between the system and the
 3670 environment.
- 3671 **TR-2.5** Provide security training for the operators, users, and other stakeholders necessary for
 3672 system utilization and support.

- 3673 **TR-2.6** Perform security activation and checkout of the system.
- 3674 *Note:* Security activation and checkout shows that the system can initialize to its initial secure
3675 operational state for all defined modes of operation and accounts for all interconnections to
3676 other systems across physical, virtual, and wireless interfaces.
- 3677 **TR-2.7** Demonstrate that the installed system is capable of delivering its required functions in a
3678 trustworthy secure manner.
- 3679 **TR-2.8** Demonstrate that the security functions provided by the system and the effects of the
3680 security functions are sustainable by enabling systems.
- 3681 **TR-2.9** Review the security trustworthiness of the system for operational readiness.
- 3682 *Note:* The results of installation, operational, and enabling system checkouts are reviewed to
3683 determine if the security performance and effectiveness are sufficient to justify operational use.
- 3684 **TR-2.10** Commission the system for secure operation.
- 3685 *Note:* This includes providing security support to users and operators at the time of the system
3686 commissioning.
- 3687 **References:** [[ISO 15288](#), Section 6.4.10.3 b)].
- 3688 **Related Publications:** [[ISO 12207](#), Sections 6.4.7.3.1, 6.4.8.3.1, 6.4.9.3.2].
- 3689 **TR-3** MANAGE RESULTS OF TRANSITION
- 3690 **TR-3.1** Record the security aspects of transition results and any anomalies encountered.
- 3691 **TR-3.2** Record the security aspects of operational incidents and problems, and track their
3692 resolution.
- 3693 **TR-3.3** Maintain traceability of the security aspects of transitioned system elements.
- 3694 *Note:* Bidirectional traceability is maintained between all identified security aspects and
3695 supporting data associated with the transition strategy and the system requirements, system
3696 architecture, and system design.
- 3697 **TR-3.4** Provide the security-relevant artifacts that have been selected for baselines.
- 3698 **References:** [[ISO 15288](#), Section 6.4.10.3 c)].
- 3699 **Related Publications:** None.
- 3700 **3.4.11 Validation**
- 3701 The purpose of the *Validation* process is to provide objective evidence that the system, when
3702 in use, fulfills its business or mission objectives and stakeholder requirements, achieving its
3703 intended use in its intended operational environment.
- 3704 [[ISO 15288](#)] Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.
- 3705 **3.4.11.1 Security Purpose**
- 3706 • To provide objective evidence that the system, when in use, fulfills the protection needs
3707 associated with its business or mission objectives and the stakeholder requirements,
3708 achieving its intended use in its intended operational environment in a trustworthy secure
3709 manner

3710 3.4.11.2 Security Outcomes

- 3711 • Security validation criteria are defined.
- 3712 • The availability of security services required by stakeholders is confirmed.
- 3713 • Security-relevant validation constraints that influence system requirements, architecture, or
3714 design are identified.
- 3715 • Security aspects of the system, system element, or artifact are validated.
- 3716 • Enabling systems or services for the security aspects of validation are available.
- 3717 • Security-focused validation results and anomalies are identified.
- 3718 • Objective evidence of the successful validation of security aspects is provided.
- 3719 • Traceability of the validated security aspects of the system, system elements, and artifacts is
3720 established.

3721 3.4.11.3 Security Activities and Tasks

3722 VA-1 PREPARE FOR VALIDATION

3723 VA-1.1 Identify the security aspects within the validation scope and corresponding security
3724 validation actions.

3725 *Note:* The security aspects of validation focus on the stakeholders' protection needs, concerns,
3726 and associated stakeholder security requirements. The scope includes system elements, the
3727 entire system, or any artifact that impacts the stakeholder's confidence in the system and the
3728 decision to accept the system as being trustworthy for its intended use.

3729 VA-1.2 Identify the constraints that can potentially limit the feasibility of the security validation
3730 actions.

3731 *Note:* Constraints may include the level of assurance and the availability of business or mission
3732 stakeholders to support validation activities; the availability of sufficient, relevant, and credible
3733 threat data; the limits on conducting validation activities in actual operational conditions across
3734 all business and mission modes and associated system states and modes; technology employed;
3735 the size and complexity of the system element or artifact; and the cost and time allotted for
3736 validation activities.

3737 VA-1.3 Select appropriate security validation methods and the associated success criteria for
3738 each security validation action.

3739 *Note:* Adversity emulation, including penetration testing and emulating abuse and misuse, is
3740 included.

3741 VA-1.4 Develop the security aspects of the validation strategy.

3742 *Note:* The security aspects of the validation strategy address the approach to incorporate
3743 security considerations into all validation actions, considering trade-offs between scope, depth,
3744 and rigor needed for the desired level of assurance and the given constraints.

3745 VA-1.5 Identify the security-relevant system constraints that result from the security aspects of
3746 the validation strategy to be incorporated in the stakeholder protection needs and the
3747 requirements transformed from those needs.

- 3748 *Note:* These constraints are associated with the clarity and accuracy of the expression of needs
 3749 and requirements in order to achieve the desired level of assurance with certainty and
 3750 repeatability.
- 3751 **VA-1.6** Identify the security aspects for enabling systems or services needed to support
 3752 validation.
- 3753 **VA-1.7** Identify and plan for enabling systems or services to support the security aspects of
 3754 validation.
- 3755 **VA-1.8** Obtain or acquire access to the security aspects of enabling systems or services to be
 3756 used to support validation.
- 3757 **References:** [[ISO 15288](#), Section 6.4.11.3 a)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
 3758 [15026-4](#)].
- 3759 **Related Publications:** [[ISO 12207](#), Section 7.2.5.3.1]; [[ISO 21827](#)].
- 3760 **VA-2** PERFORM VALIDATION
- 3761 **VA-2.1** Define the security aspects of the validation procedures, each supporting one or a set of
 3762 validation actions.
- 3763 *Note:* This includes the identification of the validation methods or techniques to be employed,
 3764 the qualifications of individuals conducting the validation, and any specialized equipment that
 3765 may be needed, such as what may be required to emulate environmental adversities.
- 3766 **VA-2.2** Perform security validation procedures.
- 3767 *Note 1:* Security-focused validation actions from the execution of validation procedures
 3768 contribute to demonstrating that the system is sufficiently trustworthy.
- 3769 *Note 2:* The performance of a security-focused validation action consists of capturing a result
 3770 from the execution of the procedure, comparing the obtained result with the expected result,
 3771 deducing the degree of compliance of the element, and deciding about the acceptability of
 3772 compliance if uncertainty remains.
- 3773 **References:** [[ISO 15288](#), Section 6.4.11.3 b)].
- 3774 **Related Publications:** [[ISO 12207](#), Sections 6.4.8.3.1, 7.2.5.3.2]; [[ISO 21827](#)].
- 3775 **VA-3** MANAGE RESULTS OF VALIDATION
- 3776 **VA-3.1** Record the security aspects of validation results and any anomalies encountered.
- 3777 *Note:* The recorded validation results include nonconformance issues, anomalies, or problems
 3778 that are potentially security related. These results inform the analyses to determine causes and
 3779 enable corrective or improvement actions. Corrective actions may affect the security aspects of
 3780 the system architecture definition, design definition, system security requirements and
 3781 associated constraints, the level of assurance that can be obtained, and/or the implementation
 3782 strategy, including its security aspects.
- 3783 **VA-3.2** Record the security characteristics of operational incidents and problems, and track
 3784 their resolution.
- 3785 *Note:* Incidents that occur in the operational environment of the system are recorded and
 3786 subsequently correlated to validation activities and results. This is an important feedback loop
 3787 for continuous improvement in the engineering of trustworthy secure systems.
- 3788 **VA-3.3** Obtain agreement that security validation criteria have been met.
- 3789 **VA-3.4** Maintain traceability of the security aspects of validation.

3790 *Note:* Bidirectional traceability of the security aspects of validated system elements to
 3791 stakeholder protection needs, security concerns, and security requirements is maintained.
 3792 Traceability demonstrates completeness of the validation process and provides evidence that
 3793 supports assurance and trustworthiness claims.

3794 **VA-3.5** Provide the security-relevant artifacts that have been selected for baselines.

3795 **References:** [\[ISO 15288](#), Section 6.4.11.3 c)]; [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
 3796 [15026-4\]](#).

3797 **Related Publications:** [\[ISO 21827\]](#).

3798 **3.4.12 Operation**

3799 The purpose of the *Operation* process is to use the system to deliver its services.

3800 [\[ISO 15288\]](#) Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

3801 **3.4.12.1 Security Purpose**

3802 • To inform the security aspects of the requirements and constraints to securely operate the
 3803 system and monitor the security aspects of products, services, and operator-system
 3804 performance

3805 • To identify and analyze security-relevant operational anomalies

3806 **3.4.12.2 Security Outcomes**

3807 • Security aspects of operation constraints that influence system requirements, architecture,
 3808 or design are identified.

3809 • Enabling systems, services, and material for the security aspects of operation are available.

3810 • Trained and qualified personnel who can securely operate the system are available.

3811 • System products or services that meet stakeholder security requirements are delivered.

3812 • Security aspects of system performance during operation are monitored.

3813 • Security support to stakeholders is provided.

3814 **3.4.12.3 Security Activities and Tasks**

3815 **OP-1** PREPARE FOR OPERATION

3816 **OP-1.1** Define the security aspects of the operation strategy.

3817 *Note 1:* This includes the approach to enable the continuous secure operation and use of the
 3818 system and its security services, as well as the provision of support to operations elements to
 3819 address anomalies identified during operation and use of the system. It also includes:

3820 - The capacity, availability, schedule considerations, and security of products or services as
 3821 they are introduced, routinely operated, and disposed (including contingency operations)

3822 - The human resources strategy and security qualification requirements for personnel
 3823 including all associated security-related training and personnel compliance requirements

3824 - The security aspects of release and re-acceptance criteria and schedules of the system to
 3825 permit modifications that sustain the security aspects of existing or enhanced products or
 3826 services

- 3827 - The approach to implement the operational modes in the System Operational Concept,
3828 including normal and contingency operations
- 3829 - The secure approaches for contingency, degraded, alternative, training, and other modes of
3830 operation, as well as transition within and between modes while considering resilience in
3831 the face of adversity
- 3832 - Measures for operation that will provide security insights into performance levels
- 3833 - The approach to achieve situational awareness to determine security-relevant consequences

3834 *Note 2:* This includes planning for securely starting the system, halting the system, shutting down
3835 the system, operating the system in a training mode, secure implementation of work-around
3836 procedures to restore operation, performing back-out and restore operations, operating in any
3837 degraded mode, or alternative modes for special conditions. If needed, the operator performs
3838 the necessary steps to enter into contingency operations and possibly power down the system.
3839 Contingency operations are performed in accordance with pre-established procedures for such
3840 an event.

3841 *Note 3:* There may be a need to plan for certain modes of operation for which security functions
3842 and services are reduced or eliminated to achieve more critical system functions and services or
3843 to carry out certain maintenance or periodic testing. Predetermined procedures for entering and
3844 exiting such modes would be followed.

3845 **OP-1.2** Identify the constraints and objectives that result from the security aspects of operation
3846 to be incorporated into the system requirements, architecture, and design.

3847 **OP-1.3** Identify the security aspects for enabling systems and services needed to support
3848 operation.

3849 **OP-1.4** Identify and plan for enabling systems or services needed to support the security
3850 aspects of operation.

3851 **OP-1.5** Obtain or acquire access to the security aspects of enabling systems or services to be
3852 used in operation.

3853 **OP-1.6** Identify or define security training and qualification requirements to sustain the
3854 workforce needed for secure system operation.

3855 *Note:* Security qualification and training includes role and function-oriented competency,
3856 proficiency, certification, and other criteria to securely operate and use the system in all of its
3857 defined modes or states.

3858 **OP-1.7** Assign trained and qualified personnel needed for secure system operation.

3859 **References:** [[ISO 15288](#), Section 6.4.12.3 a)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].

3860 **Related Publications:** [[ISO 12207](#), Section 6.4.9.3.1]; [[ISO 21827](#)].

3861 **OP-2** PERFORM OPERATION

3862 **OP-2.1** Securely use the system in its intended operational environment.

3863 **OP-2.2** Apply materials and other resources as required to securely operate the system and
3864 sustain its product and service capabilities.

3865 *Note 1:* Materials and resources are provided by logistical actions. Logistics is discussed as part
3866 of the maintenance process.

3867 *Note 2:* Operational personnel may perform system modification and support activities, such as
3868 software updates.

3869 **OP-2.3** Monitor system operations for deviations from intended behavior and outcomes.

- 3870 *Note:* This includes managing adherence to the operation strategy and operational procedures
3871 (the operations conducted by personnel) and monitoring that the system is operated in a secure
3872 manner and compliant with regulations, procedures, and directives. This also includes monitoring
3873 for anomalies that may not be directly observable as system behavior and may or may not be
3874 obviously security relevant.
- 3875 **OP-2.4** Use the measures defined in the strategy, and analyze them to confirm that system
3876 security performance is within acceptable parameters.
- 3877 *Note:* System monitoring includes reviewing whether the performance is within established
3878 security-relevant thresholds, periodic instrument readings are acceptable, and service and
3879 response times are acceptable. Operator feedback and suggestions are useful input for
3880 improving the security aspects of system operational performance.
- 3881 **OP-2.5** Identify and record when system security or service performance is not within
3882 acceptable parameters.
- 3883 **References:** [[ISO 15288](#), Section 6.4.12.3 b)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
3884 [15026-4](#)].
- 3885 **Related Publications:** [[ISO 12207](#), Section 6.4.9.3.3]; [[ISO 21827](#)].
- 3886 **OP-3** MANAGE RESULTS OF OPERATION
- 3887 **OP-3.1** Record the results of secure operations and any anomalies encountered.
- 3888 *Note:* Anomalies include those associated with the operation strategy, the operation of enabling
3889 systems, the execution of the operation, and incorrect system definition, all of which may be due
3890 to security issues or may result in security issues.
- 3891 **OP-3.2** Record the security aspects of operational incidents and problems, and track their
3892 resolution.
- 3893 **OP-3.3** Maintain traceability of the security aspects of the operation elements.
- 3894 **OP-3.4** Provide the security-relevant artifacts that have been selected for baselines.
- 3895 **References:** [[ISO 15288](#), Section 6.4.12.3 c)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
3896 [15026-4](#)].
- 3897 **Related Publications:** [[ISO 21827](#)].
- 3898 **OP-4** SUPPORT STAKEHOLDERS
- 3899 **OP-4.1** Provide security assistance and consultation to stakeholders as requested.
- 3900 *Note:* Assistance and consultation includes the provision or recommendation of sources for
3901 security-relevant training, security aspects of documentation, vulnerability resolution, security
3902 reporting (including cyber security), and other security-relevant support services that enable
3903 effective and secure use of the product or service.
- 3904 **OP-4.2** Record and monitor requests and subsequent actions for security support.
- 3905 **OP-4.3** Determine the degree to which the security aspects of delivered products and services
3906 satisfy the needs of stakeholders.
- 3907 **References:** [[ISO 15288](#), Section 6.4.12.3 d)].
- 3908 **Related Publications:** [[ISO 12207](#), Sections 6.4.9.3.4, 6.4.9.3.5]; [[ISO 21827](#)].

3909 **3.4.13 Maintenance**

3910 The purpose of the *Maintenance* process is to sustain the capability of the system to provide
3911 a product or service.

3912 [\[ISO 15288\]](#) Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

3913 **3.4.13.1 Security Purpose**

- 3914 • To establish the security aspects of requirements and constraints to securely sustain the
3915 capability of the system to provide a product or service

3916 *Note:* Secure sustainment includes all maintenance and logistics activities for the packaging,
3917 handling, storage, and transportation of replacement system elements.

3918 **3.4.13.2 Security Outcomes**

- 3919 • Security aspects of maintenance and logistics constraints that influence system
3920 requirements, architecture, or design are identified.
- 3921 • Enabling systems or services needed for the security aspects of system maintenance and
3922 logistics are available.
- 3923 • Replacement, repaired, or modified system elements are securely made available.
- 3924 • The need for required security-relevant maintenance and logistics actions is reported.
- 3925 • Security-relevant failures and life cycle data, including associated costs, are determined.

3926 **3.4.13.3 Security Activities and Tasks**3927 **MA-1 PREPARE FOR MAINTENANCE AND LOGISTICS**

3928 **MA-1.1** Define the security aspects of the maintenance strategy.

3929 *Note:* The maintenance strategy seeks to preserve the secure capability and performance of the
3930 delivered system. The security aspects of the maintenance strategy generally include:

- 3931 - The secure transition of the system and system elements into a secure maintenance mode
3932 or state, as well as the secure transition back to operation.
- 3933 - An approach to help ensure that sourced materials and system elements that do not meet
3934 specified quality, origin, and functionality (e.g., counterfeit) are not introduced into the
3935 system.
- 3936 - The skill and personnel levels required to effect repairs, replacements, and restoration
3937 accounting for maintenance staff requirements and any relevant legislation regarding health,
3938 safety, security, and the environment.
- 3939 - Maintenance measures that provide insight into the security aspects of performance levels,
3940 effectiveness, and efficiency.

3941 **MA-1.2** Define the security aspects of the logistics strategy.

3942 *Note:* The logistics strategy defines the specific security considerations required to perform
3943 logistics throughout the life cycle. This generally includes:

- 3944 - Acquisition logistics to help ensure that security implications are considered early during the
3945 development stage.
- 3946 - Operations logistics to help ensure that the necessary material and resources, in the right
3947 quantity and quality, are securely made available at the right place and time throughout the

- 3948 utilization and support stages; considerations for securely making material and resources
 3949 available include identification and marking, packaging, distribution, handling, and
 3950 provisioning.
- 3951 - The security criteria for storage locations and conditions, as well as the number and type of
 3952 replacement system security-specific elements, their anticipated replacement rate, and their
 3953 storage life and renewal frequency.
- 3954 **MA-1.3** Identify the security-relevant constraints and objectives that result from the security
 3955 aspects of maintenance and logistics to be incorporated into the system requirements,
 3956 architecture, and design.
- 3957 **MA-1.4** Identify trade-offs such that the security aspects of the system and associated
 3958 maintenance and logistics actions result in a solution that is trustworthy, secure,
 3959 affordable, operable, supportable, and sustainable.
- 3960 *Note:* The cost of secure maintenance and logistics should be considered within the lifetime cost
 3961 of the system.
- 3962 **MA-1.5** Identify the security aspects for enabling systems, products, and services needed to
 3963 support maintenance and logistics.
- 3964 **MA-1.6** Identify and plan for enabling systems, products, and services needed to support the
 3965 security aspects of maintenance and logistics.
- 3966 **MA-1.7** Obtain or acquire access to the security aspects of enabling systems, products, and
 3967 services to be used in maintenance and logistics.
- 3968 **References:** [\[ISO 15288, Section 6.4.13.3 a\)\]](#); [\[ISO 15026-1\]](#); [\[ISO 15026-2\]](#); [\[ISO 15026-3\]](#); [\[ISO](#)
 3969 [15026-4\]](#); [\[ISO 27036-1\]](#); [\[ISO 27036-2\]](#); [\[ISO 27036-3\]](#).
- 3970 **Related Publications:** [\[ISO 12207, Section 6.4.10.3.1\]](#); [\[ISO 21827\]](#).
- 3971 **MA-2** PERFORM MAINTENANCE
- 3972 *Note:* The need to perform maintenance may be driven by the need to address explicit security issues,
 3973 incidents, or failures. All maintenance actions must be accomplished in a secure manner with the
 3974 understanding that some actions may have a direct effect on the security posture of the system.
- 3975 **MA-2.1** Monitor and review stakeholder requirements and incident and problem reports to
 3976 identify security-relevant corrective, preventive, adaptive, additive, or perfective
 3977 maintenance needs.
- 3978 *Note:* Security-relevant maintenance needs include those needs that are direct (e.g., an
 3979 identified security incident) or indirect (e.g., considerations to securely address a maintenance
 3980 need).
- 3981 **MA-2.2** Record the security aspects of maintenance incidents and problems, and track their
 3982 secure resolution.
- 3983 **MA-2.3** Analyze the impact of changes introduced by maintenance actions on the security
 3984 aspects of the system and system elements.
- 3985 **MA-2.4** Upon encountering faults that cause a system failure, securely restore the system to
 3986 secure operational status.
- 3987 *Note:* Secure restoration means that the maintenance action itself does not worsen the secure
 3988 state or condition of the system.
- 3989 **MA-2.5** Securely correct anomalies (e.g., defects, errors, and faults), and replace or upgrade
 3990 system elements.

- 3991 **MA-2.6** Perform preventive maintenance by securely replacing or servicing system elements
3992 prior to failure.
- 3993 **MA-2.7** Securely perform adaptive, additive, or perfective maintenance as required.
- 3994 **References:** [[ISO 15288](#), Section 6.4.13.3 b)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
3995 [15026-4](#)].
- 3996 **Related Publications:** [[ISO 12207](#), Sections 6.4.10.3.2, 6.4.10.3.3, 6.4.10.3.4, 6.4.10.3.5]; [[ISO](#)
3997 [21827](#)].
- 3998 **MA-3** PERFORM LOGISTICS SUPPORT
- 3999 **MA-3.1** Perform the security aspects of acquisition logistics.
- 4000 **MA-3.2** Perform the security aspects of operational logistics.
- 4001 **MA-3.3** Implement mechanisms for the secure logistics needed during the life cycle.
- 4002 *Note 1:* These mechanisms enable secure packaging, handling, storage, and transportation.
- 4003 *Note 2:* These mechanisms aid in the prevention and detection of counterfeits, tampering,
4004 substitution, and redirection.
- 4005 **MA-3.4** Confirm that the security aspects of logistics actions are implemented.
- 4006 *Note:* The security aspects of logistics actions satisfy both logistics protection concerns and the
4007 need to meet repair rates, replenishment levels, and planned schedules.
- 4008 **References:** [[ISO 15288](#), Section 6.4.13.3 c)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO 15026-3](#)]; [[ISO](#)
4009 [15026-4](#)]; [[ISO 27036-1](#)]; [[ISO 27036-2](#)]; [[ISO 27036-3](#)].
- 4010 **Related Publications:** [[ISO 21827](#)].
- 4011 **MA-4** MANAGE RESULTS OF MAINTENANCE AND LOGISTICS
- 4012 **MA-4.1** Record the security aspects of maintenance and logistics results and any anomalies
4013 encountered.
- 4014 **MA-4.2** Record maintenance and logistics security incidents and problems, and track their
4015 secure resolution.
- 4016 **MA-4.3** Identify and record the security-relevant trends of incidents, problems, and
4017 maintenance and logistics actions.
- 4018 **MA-4.4** Maintain traceability of the security aspects of maintenance and logistics.
- 4019 **MA-4.5** Provide security-relevant artifacts that have been selected for baselines.
- 4020 **MA-4.6** Monitor customer satisfaction with the security aspects of the system, maintenance,
4021 and logistics.
- 4022 **References:** [[ISO 15288](#), Section 6.4.13.3 d)]; [[ISO 10004](#)]; [[ISO 15026-1](#)]; [[ISO 15026-2](#)]; [[ISO](#)
4023 [15026-3](#)]; [[ISO 15026-4](#)].
- 4024 **Related Publications:** [[ISO 21827](#)].
- 4025 **3.4.14 Disposal**
- 4026 The purpose of the *Disposal* process is to end the existence of a system element or system
4027 for a specified intended use, appropriately handle replaced or retired elements and any
4028 waste products, and properly attend to identified critical disposal needs (e.g., per an
4029 agreement, per organizational policy, or for environmental, legal, safety, or security aspects).

4030 [\[ISO 15288\]](#) Reprinted with permission from IEEE, Copyright IEEE 2015, All rights reserved.

4031 **3.4.14.1 Security Purpose**

- 4032 • To provide the aspects needed to securely end the existence of a system element or system
- 4033 for a specified intended use and securely preserve or destroy the associated data and
- 4034 information

4035 **3.4.14.2 Security Outcomes**

- 4036 • Secure disposal constraints that influence system requirements, architecture, design, and
- 4037 implementation are identified.
- 4038 • Enabling systems or services for the security aspects of disposal are available.
- 4039 • System elements or waste products are destroyed, stored, reclaimed, or recycled in
- 4040 accordance with safety and security requirements.
- 4041 • The environment is securely returned to its original secure or an agreed-upon secure state.
- 4042 • Records of the security aspects of disposal actions and analysis are available.

4043 **3.4.14.3 Security Activities and Tasks**

4044 **DS-1 PREPARE FOR DISPOSAL**

4045 **DS-1.1** Define the security aspects of the disposal strategy.

4046 *Note:* The security aspects address securely terminating system functions and services,
 4047 transforming the system and environment into an acceptable secure state, addressing security
 4048 concerns, and transitioning the system and system elements for future use. The disposal strategy
 4049 determines approaches, schedules, resources, specific considerations of secure disposal, and the
 4050 effectiveness and completeness of secure disposal and disposition actions.

- 4051 - *Permanent termination of system functions and delivery of services:* The security aspects
- 4052 address the removal, decommissioning, or destruction of the associated system elements
- 4053 while preserving the security posture of any remaining functions and services.
- 4054 - *Transform the system and environment into an acceptable state:* The security aspects
- 4055 address any alterations made to the system, its operation, and the environment to ensure
- 4056 that stakeholder protection needs and concerns are addressed by the remaining portions of
- 4057 the system and the functions and services it provides. When the entire system is removed,
- 4058 the security aspects address alterations to the environment to return it to its original or
- 4059 agreed-upon secure state.
- 4060 - *Address security concerns for material, data, and information:* The security aspects address
- 4061 protections for sensitive components, technology, information, and data removed from
- 4062 service, dismantled, stored, prepared for reuse, or destroyed. The aspects may include the
- 4063 duration of protection level/state, downgrades, releasability, and criteria that define
- 4064 authorized access and use during the storage period. The protection needs for disposal are
- 4065 defined by stakeholders and agreements and may be subject to regulatory requirements,
- 4066 expectations, and constraints.
- 4067 - *Transition the system and system elements for future use:* The security aspects address the
- 4068 transition of the system or system elements for future use in a modified or adapted form,
- 4069 including legacy migration and return to service. The security aspects may include
- 4070 constraints, limitations, or other criteria to enable recovery of the systems' functions and
- 4071 services within a specified time period or to ensure security-oriented interoperability with

- 4072 future enabling systems and other systems. These aspects may also include periodic
 4073 inspections to account for the security posture and return-to-service readiness of stored
 4074 system elements, associated data and information, and all supporting operations and
 4075 sustainment support materials. The security aspects apply to all system functions and
 4076 services and are not limited to only security protection-oriented functions and services of
 4077 the system.
- 4078 **DS-1.2** Identify the security-relevant constraints and objectives of disposal on the system
 4079 requirements, architecture and design characteristics, and implementation techniques.
- 4080 **DS-1.3** Identify the security aspects for enabling systems or services needed to support
 4081 disposal.
- 4082 **DS-1.4** Identify and plan for enabling systems or services needed to support the security
 4083 aspects of disposal.
- 4084 **DS-1.5** Obtain or acquire access to the security aspects of enabling systems or services to be
 4085 used in disposal.
- 4086 **DS-1.6** Specify security criteria for containment facilities, storage locations, inspection, and
 4087 storage periods (if the system is to be stored).
- 4088 **DS-1.7** Define the security aspects of preventive methods to preclude disposed elements and
 4089 materials that should not be repurposed, reclaimed, or reused from re-entering the
 4090 supply chain.
- 4091 **References:** [[ISO 15288](#), Section 6.4.14.3 a)].
- 4092 **Related Publications:** [[ISO 12207](#), Section 6.4.11.3.1]; [[ISO 21827](#)].
- 4093 **DS-2** PERFORM DISPOSAL
- 4094 **DS-2.1** Securely deactivate the system or system element to prepare it for secure removal from
 4095 operation.
- 4096 *Note:* Deactivation is accomplished to preserve the security posture of the system.
- 4097 **DS-2.2** Securely remove the system, system element, or waste material from use or production
 4098 for appropriate secure disposition and action.
- 4099 **DS-2.3** Securely withdraw impacted operating staff from the system or system element, and
 4100 record relevant secure operation knowledge.
- 4101 **DS-2.4** Securely disassemble the system or system element into manageable elements to
 4102 facilitate its secure removal for reuse, recycling, reconditioning, overhaul, archiving, or
 4103 destruction.
- 4104 *Note:* Secure disassembly preserves the security characteristics of the system elements that are
 4105 not removed.
- 4106 **DS-2.5** Securely handle system elements and their parts that are not intended for reuse in a
 4107 manner that will help ensure that they do not get back into the supply chain.
- 4108 **DS-2.6** Conduct secure sanitization and destruction of the system elements and life cycle
 4109 artifacts.
- 4110 *Note 1:* Governing agreements, laws, and regulations determine the appropriate means to
 4111 sanitize and destroy data, information, and systems elements that contain data and information,
 4112 as well as retention periods before sanitization and destruction can occur.
- 4113 *Note 2:* Sanitization and destruction techniques include clearing, purging, cryptographic erase,
 4114 physical modification, and physical destruction.

- 4115 *Note 3:* Sanitization and destruction techniques and methods may be specific to data,
4116 information, and system element type.
- 4117 **References:** [[ISO 15288](#), Section 6.4.14.3 b)].
- 4118 **Related Publications:** [[ISO 12207](#), Section 6.4.11.3.2]; [[ISO 21827](#)].
- 4119 **DS-3** FINALIZE THE DISPOSAL
- 4120 **DS-3.1** Confirm that no detrimental security factors exist following disposal.
- 4121 **DS-3.2** Return the environment to its original secure state or to a secure state specified by
4122 agreement.
- 4123 **DS-3.3** Securely archive data and information gathered through the lifetime of the system to
4124 permit audits and reviews in the event of long-term hazards to health, safety, security,
4125 and the environment and to permit future system creators and users to securely build a
4126 knowledge base from past experiences.
- 4127 **DS-3.4** Provide security-relevant artifacts that have been selected for baselines.
- 4128 **References:** [[ISO 15288](#), Section 6.4.14.3 c)].
- 4129 **Related Publications:** [[ISO 21827](#)].

4130

REFERENCES

4131

KEY REFERENCES RELATED TO SYSTEMS SECURITY ENGINEERING

LAWS AND EXECUTIVE ORDERS

- [EGOV] E-Government Act [incl. FISMA] (P.L. 107-347), December 2002.
<https://www.govinfo.gov/app/details/PLAW-107publ347>
- [EO 14028] Executive Order 14028 (2021), *Improving the Nation's Cybersecurity*. (The White House, Washington, DC), May 12, 2021.
<https://www.federalregister.gov/d/2021-10460>
- [FISMA] Federal Information Security Modernization Act (P.L. 113-283), December 2014.
<https://www.govinfo.gov/app/details/PLAW-113publ283>
- [FOIA96] Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996.
<https://www.govinfo.gov/app/details/PLAW-104publ231>

POLICIES, DIRECTIVES, AND INSTRUCTIONS

- [CNSSI 4009] Committee on National Security Systems Instruction (CNSSI) No. 4009, *Committee on National Security Systems (CNSS) Glossary*, April 2015.
<https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
- [DODD 8140.01] Department of Defense (DoD) Directive 8140.01, *Cyberspace Workforce Management*, October 2020.
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.PDF?ver=si7QmZONMCW2tStUt4ws3Q%3D%3D>
- [OMB A-130] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 2016.
<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf>
- [OMB M-19-03] Office of Management and Budget (2018) Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program. (The White House, Washington, DC), OMB Memorandum M-19-03, December 2018.
<https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf>

STANDARDS AND GUIDELINES

- [ANSI G-043B] American National Standards Institute (ANSI)/American Institute of Aeronautics and Astronautics (AIAA) G-043B-2018, *Guide To The Preparation Of Operational Concept Documents*, April/May 2018.
<https://webstore.ansi.org/Standards/AIAA/ANSIAIAA043B2018>
- [EIA 649C] Electronic Industries Alliance (EIA) 649C, *Configuration Management Standard*, February 2019.
<https://www.sae.org/standards/content/eia649c>
- [GSNCS18] Goal Structuring Notation Community Standard, Version 2, The Assurance Case Working Group, January 2018.
<https://scsc.uk/r141B:1?t=1>
- [IEEE 610.12] Institute of Electrical and Electronics Engineers (IEEE) Std. 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology*, December 1990.
https://standards.ieee.org/standard/610_12-1990.html
- [IEEE 828] Institute of Electrical and Electronics Engineers (IEEE) Std. 828-2012, *IEEE Standard for Configuration Management in Systems and Software Engineering*, IEEE Computer Society, March 2012.
<https://standards.ieee.org/standard/828-2012.html>
- [ISO 73] International Organization for Standardization (ISO) Guide 73:2009, *Risk management – Vocabulary*, November 2009.
<https://www.iso.org/standard/44651.html>
- [ISO 7498-2] International Organization for Standardization (ISO) ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*, February 1989.
<https://www.iso.org/standard/14256.html>
- [ISO 9000] International Organization for Standardization (ISO) 9000:2015, *Quality management systems – Fundamentals and vocabulary*, September 2015.
<https://www.iso.org/standard/45481.html>
- [ISO 9001] International Organization for Standardization (ISO) 9001:2015, *Quality management systems – Requirements*, September 2015.
<https://www.iso.org/standard/62085.html>
- [ISO 9241] International Organization for Standardization (ISO) 9241-210:2010, *Ergonomics of human-system interaction – Part 210: Human-centered design for interactive systems*, March 2010.
<https://www.iso.org/standard/52075.html>
- [ISO 10004] International Organization for Standardization (ISO) 10004:2018, *Quality management – Customer satisfaction – Guidelines for monitoring and managing*, August 2018.
<https://www.iso.org/standard/71582.html>

- [ISO 10007] International Organization for Standardization (ISO) 10007:2003, *Quality management systems – Guidelines for configuration management*, March 2017.
<https://www.iso.org/standard/70400.html>
- [ISO 12207] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 12207:2008, *Systems and software engineering – Software life cycle processes*, November 2017.
<https://www.iso.org/standard/63712.html>
- [ISO 13008] International Organization for Standardization (ISO) 13008:2012, *Information and documentation — Digital records conversion and migration process*, June 2012.
<https://www.iso.org/standard/52326.html>
- [ISO 14258] International Organization for Standardization (ISO) 14258:1998, *Industrial automation systems — Concepts and rules for enterprise models*, September 1998.
<https://www.iso.org/standard/24020.html>
- [ISO 15026-1] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15026-1:2019, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*, March 2019.
<https://www.iso.org/standard/73567.html>
- [ISO 15026-2] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15026-2:2011, *Systems and software engineering -- Systems and software assurance -- Part 2: Assurance case*, February 2011.
<https://www.iso.org/standard/80625.html>
- [ISO 15026-3] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15026-3:2015, *Systems and software engineering -- Systems and software assurance -- Part 3: System integrity levels*, November 2015.
<https://www.iso.org/standard/64842.html>
- [ISO 15026-4] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15026-4:2012, *Systems and software engineering -- Systems and software assurance -- Part 4: Assurance in the life cycle*, October 2012.
<https://www.iso.org/standard/59927.html>
- [ISO 15288] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, *Systems and software engineering — Systems life cycle processes*, May 2015.
<https://www.iso.org/standard/63711.html>

- [ISO 15408-1] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*.
<https://www.iso.org/standard/72891.html>
- [ISO 15408-2] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408-2:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*.
<https://www.iso.org/standard/72892.html>
- [ISO 15408-3] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408-3:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*.
<https://www.iso.org/standard/46413.html>
- [ISO 15939] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15939:2017, *Systems and software engineering — Measurement process*, May 2017.
<https://www.iso.org/standard/71197.html>
- [ISO 16085] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 16085:2021, *Systems and software engineering — Life cycle processes — Risk management*, January 2021.
<https://www.iso.org/standard/74371.html>
- [ISO 16290] International Organization for Standardization (ISO) 16290:2013, *Space systems — Definition of the Technology Readiness Levels (TRLs) and their criteria of assessment*, November 2013.
<https://www.iso.org/standard/56064.html>
- [ISO 18152] International Organization for Standardization/Technical Specification (ISO/TS) 18152:2010, *Ergonomics of human-system interaction — Specification for the process assessment of human-system issues*, June 2010.
<https://www.iso.org/standard/56174.html>
- [ISO 18307] International Organization for Standardization/Technical Report (ISO/TR) 18307:2001, *Health informatics — Interoperability and compatibility in messaging and communication standards — Key characteristics*, December 2001.
<https://www.iso.org/standard/33396.html>

- [ISO 19014] International Organization for Standardization (ISO) 19014:2020, *Earth-moving machinery — Functional safety — Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system*, July 2020.
<https://www.iso.org/standard/70718.html>
- [ISO 21827] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 21827:2008, *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)*, October 2008.
<https://www.iso.org/standard/44716.html>
- [ISO 21839] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 21839:2019, *Systems and software engineering — System of systems (SoS) considerations in life cycle stages of a system*, July 2019.
<https://www.iso.org/standard/71955.html>
- [ISO 21840] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 21840:2019, *Systems and software engineering — Guidelines for the utilization of ISO/IEC/IEEE 15288 in the context of system of systems (SoS)*, December 2019.
<https://www.iso.org/standard/71956.html>
- [ISO 21841] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 21841:2019, *Systems and software engineering — Taxonomy of systems of systems*, July 2019.
<https://www.iso.org/standard/71957.html>
- [ISO 24748-1] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) TR 24748-1:2010, *Systems and software engineering — Life cycle management — Part 1: Guide for life cycle management*, October 2010.
<https://www.iso.org/standard/50502.html>
- [ISO 24748-6] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) TR 24748-6:2016, *Systems and software engineering — Life cycle management — Part 6: System integration engineering*, December 2016.
<https://www.iso.org/standard/66433.html>
- [ISO 24765] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 24765:2017, *Systems and software engineering — Vocabulary*, September 2017.
<https://www.iso.org/standard/71952.html>

- [ISO 24774] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 24774:2021, *Systems and software engineering — Life cycle management — Specification for process description*, May 2021.
<https://www.iso.org/standard/78981.html>
- [ISO 25010] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 25010:2011, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*, March 2011.
<https://www.iso.org/standard/35733.html>
- [ISO 25030] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 25030:2019, *Software Engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Quality Requirements*, August 2019.
<https://www.iso.org/standard/72116.html>
- [ISO 25060] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) TR 25060:2010, *Systems and software engineering — Systems and software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for usability: General framework for usability-related information*, July 2010.
<https://www.iso.org/standard/35786.html>
- [ISO 25063] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 25063:2014, *Systems and software engineering – Systems and software product Quality Requirements and Evaluation (SQuaRE) – Common Industry Format (CIF) for usability: Context of use description*, March 2014.
<https://www.iso.org/standard/35789.html>
- [ISO 27001] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013, *Information technology -- Security techniques -- Information security management systems -- Requirements*, September 2013.
<https://www.iso.org/standard/54534.html>
- [ISO 27002] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002:2013, *Information technology -- Security techniques -- Code of practice for information security controls*, September 2013.
<https://www.iso.org/standard/54533.html>

- [ISO 27034-1] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27034-1:2011, *Information technology — Security techniques — Application security — Part 1: Overview and concepts*, November 2011.
<https://www.iso.org/standard/44378.html>
- [ISO 27036-1] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27036-1:2014, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*, April 2014.
<https://www.iso.org/standard/59648.html>
- [ISO 27036-2] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27036-2:2014, *Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements*, August 2014.
<https://www.iso.org/standard/82060.html>
- [ISO 27036-3] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27036-3:2013, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security*, November 2013.
<https://www.iso.org/standard/59688.html>
- [ISO 29110-1] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) TR 29110-1:2016, *Systems and software engineering — Lifecycle profiles for Very Small Entities (VSEs) — Part 1: Overview*, June 2016.
<https://www.iso.org/standard/62711.html>
- [ISO 29119-1] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 29119-1:2013, *Software Testing: Concepts and Definitions*, September 2013.
<https://www.iso.org/standard/45142.html>
- [ISO 29119-2] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 29119-2:2013, *Software Testing: Test Processes*, September 2013.
<https://www.iso.org/standard/56736.html>
- [ISO 29119-3] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 29119-3:2013, *Software Testing: Test Documentation*, September 2013.
<https://www.iso.org/standard/56737.html>
- [ISO 29119-4] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 29119-4:2014, *Software Testing: Test Techniques*, December 2015.
<https://www.iso.org/standard/60245.html>

- [ISO 29148] International Organization for Standardization /International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 29148:2018, *Systems and software engineering — Life cycle processes – Requirements engineering*, November 2018.
<https://www.iso.org/standard/72089.html>
- [ISO 31000] International Organization for Standardization (ISO) 31000:2018, *Risk management – Guidelines*, February 2018.
<https://www.iso.org/standard/65694.html>
- [ISO 42010] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers (IEEE), ISO/IEC/IEEE 42010, *Systems and Software Engineering — Architecture description*, December 2011.
<https://www.iso.org/standard/50508.html>
- [ISO 42020] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers (IEEE), ISO/IEC/IEEE 42020:2019, *Software, systems and enterprise — Architecture processes*, July 2019.
<https://www.iso.org/standard/68982.html>
- [MILSTD-882E] Department of Defense Standard Practice, *System Safety*, MIL-STD-882E, May 2012.
- [SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
<https://doi.org/10.6028/NIST.SP.800-30r1>
- [SP 800-160v2] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau and R. McQuaid (2021) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-160 Volume 2, Revision 1.
<https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final>
- [SP 800-181] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel G. Witte (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-181 Revision 1.
<https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final>
- [TCSEC85] Department of Defense (DoD) Standard 5200.28-STD, *Trusted Computer System Evaluation Criteria*, December 1985.
<https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf>

OTHER PUBLICATIONS

- [Adcock20] Adcock R, Jackson S, Singer J, Hybertson D, "Principles of Systems Thinking," Stevens Institute of Technology, May 2020.
https://www.sebokwiki.org/wiki/Principles_of_Systems_Thinking
- [Anderson72] Anderson J, *Computer Security Technology Planning Study*, Technical Report ESD-TR-73- 51, Air Force Electronic Systems Division, Hanscom AFB, October 1972.
<https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande72a.pdf>
- [Anderson20] Anderson R, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd Edition, Wiley, December 2020.
- [Ball03] Ball RE, "The Fundamentals of Aircraft Combat Survivability Analysis and Design", 2nd Edition. AIAA Education Series, 2003.
<https://arc.aiaa.org/doi/book/10.2514/4.862519>
- [Benjamin14] Benjamin A, et al., "Developing Probabilistic Safety Performance Margins for Unknown and Underappreciated Risks," PSAM-12 International Conf. on Probabilistic Safety and Management, June 2014.
- [Bieder20] Bieder C, *The Coupling of Safety and Security - Exploring Interrelations in Theory and Practice*, Springer, 2020.
<https://link.springer.com/book/10.1007%2F978-3-030-47229-0>
- [Bryant20] Bryant WD, Ball RE, "Developing the Fundamentals of Aircraft Cyber Combat Survivability: Part 2," *Joint Aircraft Survivability Program Office, Aircraft Survivability Journal*, Spring 2020
- [CISA20] Critical Infrastructure Sectors, Department of Homeland Security Cybersecurity and Infrastructure Security Agency.
<https://www.cisa.gov/critical-infrastructure-sectors>
- [DOD 2007] Department of Defense, MIL-HDBK-454B, *General Guidelines for Electronic Equipment*, April 2007.
https://www.dla.mil/Portals/104/documents/landAndMaritime/v/va/pSMC/documents/IM_MIL_HDBK_454B_151030.pdf
- [DOD 2020] Department of Defense, MIL-HDBK-454B, *Mission Engineering Guide*, November 2020.
https://ac.cto.mil/wp-content/uploads/2020/12/MEG-v40_20201130_shm.pdf
- [DODI 5200] Department of Defense Instruction (DoDI) 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," October 2020.
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520039p.pdf>

- [DSB 2013] Department of Defense Science Board Task Force Report, *Resilient Military Systems and the Advanced Cyber Threat*, January 2013.
<https://dsb.cto.mil/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf>
- [DSB 2017] Department of Defense Science Board, *Task Force on Cyber Deterrence*, February 2017.
https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf
- [FUSE21] Dove R, Willett K, McDermott T, Dunlap H, MacNamara DP, Ocker C. "Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundational Concepts" *INCOSE International Symposium*, July 2021.
- [Herley16] Herley C, *Unfalsifiability of Security Claims*, Microsoft Research, Proceedings of the National Academy of Sciences, April 2016.
- [INCOSE] International Council On Systems Engineering, *What Is Systems Engineering?*
<https://www.incose.org/systems-engineering>
- [INCOSE05] Roedler G, Jones C, *Technical Measurement*, International Council on Systems Engineering, INCOSE TP-2003-020-01, December 2005.
<https://www.incose.org/docs/default-source/ProductsPublications/technical-measurement-guide---dec-2005.pdf?sfvrsn=4&sfvrsn=4>
- [INCOSE10] Systems Engineering Measurement Primer, International Council On Systems Engineering INCOSE TP-2010-005-02, November 2010.
<https://www.incose.org/docs/default-source/ProductsPublications/systems-engineering-measurement-primer---december-2010.pdf>
- [INCOSE14] System Engineering Handbook—A Guide for System Engineering Life Cycle Processes and Activities, International Council on Systems Engineering, INCOSE TP-2003-002-04, July 2015.
- [INCOSE19] Sillitto H, Martin J, McKinney D, Griego R, Dori D, Krob D, Godfrey P, Arnold E, Jackson L, INCOSE-TP-2020-002-06, *Systems Engineering and System Definitions*, July 2019.
https://www.incose.org/docs/default-source/default-document-library/incose-se-definitions-tp-2020-002-06.pdf?sfvrsn=b1049bc6_0
- [INCOSE20] Guide for Writing Requirements, International Council On Systems Engineering, INCOSE TP-2010-006-03, July 2019.
<https://connect.incose.org/Pages/Product-Details.aspx?ProductCode=TechGuideWR2019Soft>

- [Jackson13] Jackson S, Ferris T, “Resilience Principles for Engineered Systems,” *Systems Engineering*, Vol. 16, No. 2, July 2013.
<https://onlinelibrary.wiley.com/doi/abs/10.1002/sys.21228>
- [Lampson73] Lampson BW, “A Note on the Confinement Problem,” *Communications of the ACM* 16, 10, pp. 613-615, October 1973.
<https://dl.acm.org/doi/10.1145/362375.362389>
- [Leveson11] Leveson NG, “Engineering a Safer World – Systems Thinking Applied to Safety,” Chapter 14, MIT Press, ISBN 978-0-262-01662-9, 2011.
<https://direct.mit.edu/books/book/2908/Engineering-a-Safer-WorldSystems-Thinking-Applied>
- [Maier98] Maier M, “Architecting Principles for Systems-of-Systems,” The Aerospace Corporation, 1998.
<https://onlinelibrary.wiley.com/doi/abs/10.1002/%28SICI%291520-6858%281998%291%3A4%3C267%3A%3AAID-SYS3%3E3.0.CO%3B2-D>
- [McEvilley15] McEvilley M, “Towards a Notional Framework for Systems Security Engineering,” The MITRE Corporation, NDIA 18th Annual Systems Engineering Conference, October 2015.
- [MITRE21] Hild D, McEvilley M, Winstead M, “Principles for Trustworthy Design of Cyber-Physical Systems,” MITRE Technical Report, MTR210263, June 2021.
- [Moller08] Moller N, Hansson SO, “Principles of Engineering Safety: Risk and Uncertainty Reduction,” *Reliability Engineering & System Safety*, Vol. 93, No. 6, June 2008.
- [NASA07] National Aeronautics and Space Administration (NASA), *Systems Engineering Handbook*, NASA/SP-2007-6105, Revision 1, December 2007.
https://www.nasa.gov/sites/default/files/atoms/files/nasa_systems_engineering_handbook.pdf
- [NASA11] National Aeronautics and Space Administration (NASA), *System Safety Handbook Volume 1: System Safety Framework and Concepts for Implementation*, NASA/SP-2010-580, Version 1.0, November 2011.
<https://ntrs.nasa.gov/api/citations/20120003291/downloads/20120003291.pdf>
- [NASA14] National Aeronautics and Space Administration (NASA), *System Safety Handbook Volume 2: System Safety Concepts, Guidelines, and Implementation Examples*, NASA/SP-2014-612, Version 1.0, November 2014.
<https://ntrs.nasa.gov/api/citations/20150015500/downloads/20150015500.pdf>

- [NASA17] Rinehart DJ, Knight JC, and Rowanhill J, "Understanding What it Means for Assurance Cases to Work," NASA/CR-2017-219582, April 2017.
<https://catalog.libraries.psu.edu/catalog/20766348>
- [NASA19] National Aeronautics and Space Administration (NASA), *Advocate: Assurance Case Automation Toolset*, January 2019.
<https://ti.arc.nasa.gov/tech/rse/research/advocate>
- [Neumann00] Neumann P, "Practical Architectures for Survivable Systems and Networks," Technical Report, Final Report, Phase Two, Project 1688, SRI International, Menlo Park, California, June 2000.
<http://www.csl.sri.com/neumann/survivability.html>
- [Neumann04] Neumann P, "Principled Assuredly Trustworthy Composable Architectures," CDRL A001 Final Report, SRI International, Menlo Park, CA, December 28, 2004.
<http://www.csl.sri.com/users/neumann/chats4.pdf>
- [Neumann17] Neumann P, "Fundamental Trustworthiness Principles," 2017.
- [NICE Framework] Cybersecurity and Infrastructure Security Agency (CISA), *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*.
<https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework>
- [NICE RC] National Initiative for Cybersecurity Education (NICE) Framework Resource Center
<https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center>
- [Levin07] Levin T, Irvine C, Benzel T, Bhaskara G, Clark P, and Nguyen T, *Design Principles and Guidelines for Security*, Technical Report NPS-CS-07-014, Naval Postgraduate School, November 2007.
<https://nps.edu/web/c3o/technical-reports>
- [Pagani04] Pagani LP, "On the Quantification of Safety Margins," PhD Dissertation, Massachusetts Institute of Technology, September 2004.
- [Popek74] Popek G, "The Principle of Kernel Design," in 1974 NCC, AFIPS Cong. Proc., Vol. 43.
- [Saleh14] Saleh JH, Marais KB, and Favaro FM, "System safety principles: A multidisciplinary engineering perspective," *Journal of Loss Prevention in the Process Industries*, Vol. 29, 2014.
- [Saltzer75] Saltzer JH, Schroeder MD, "The Protection of Information in Computer Systems," in *Proceedings of the IEEE* Vol. 63, No. 9, September 1975.
<https://www.cs.virginia.edu/~evans/cs551/saltzer>

- [Saltzer09] Saltzer JH, Kaashoek MF, "Principles of Computer System Design," 2009.
https://ocw.mit.edu/resources/res-6-004-principles-of-computer-system-design-an-introduction-spring-2009/online-textbook/readings_open_5_0.pdf
- [Saydjari18] Saydjari OS, *Engineering Trustworthy Systems: Get Cybersecurity Design Right the First Time*, McGraw-Hill, August 2018.
<https://books.apple.com/us/book/engineering-trustworthy-systems-get-cybersecurity-design/id1413527360>
- [Schroeder72] Schroeder MD, "Cooperation of mutually suspicious subsystems in a computer utility," Ph.D. dissertation, M.I.T., Cambridge, Mass., 1972
<https://web.mit.edu/~saltzer/www/publications/TRs+TMs/Multics/TR-104.pdf>
- [Schroeder77] Schroeder MD, Clark DD, and Saltzer JH, "The Multics Kernel Design Project," in *Proceedings of Sixth ACM Symposium on Operating Systems Principles*, 1977.
<https://web.mit.edu/Saltzer/www/publications/rfc/csr-rfc-140.pdf>
- [SEBoK] BKCASE Editorial Board (2019) The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 2.0, ed Cloutier RJ (The Trustees of the Stevens Institute of Technology, Hoboken, NJ). BKCASE is managed and maintained by the Stevens Institute of Technology Systems Engineering Research Center, the International Council on Systems Engineering, and the Institute of Electrical and Electronics Engineers Computer Society.
[https://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_\(SEBoK\)](https://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK))
- [Sheard18] Sheard S, Konrad M, Weinstock C, and Nichols W, "A Complexity Measure for System Safety Assurance," in *INCOSE International Symposium*, Adelaide Australia, 2018.
<https://onlinelibrary.wiley.com/doi/abs/10.1002/j.2334-5837.2017.00373.x>
- [Simovici08] Simovici DA, Djeraba C, "Partially Ordered Sets," *Mathematical Tools for Data Mining: Set Theory, Partial Orders, Combinatorics*, Springer, 2008.
- [Smith12] Smith RE, "A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles," *IEEE Security & Privacy*, Vol. 10, No. 6, November/December 2012.
- [Snyder15] Snyder D, Powers JD, Bodine-Baron E, Fox B, Kendrick L, Powell MH, "Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles," Rand Corporation, 2015.
https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf

- [Uchenick05] Uchenick GM, Vanfleet WM, "Multiple Independent Levels of Safety and Security: High Assurance Architecture for MSLS/MLS," *IEEE Military Communications Conference*, 2005, pp. 610-614 Vol. 1.
- [Young14] Young W, Leveson NG, "An Integrated Approach to Safety and Security based on Systems Theory," *Communications of the ACM*. Volume 57, Issue 2, 2014, pp. 31-35.
<https://dl.acm.org/doi/10.1145/2556938>

4132

4133 **APPENDIX A**4134 **GLOSSARY**

4135 COMMON TERMS AND DEFINITIONS

4136 Appendix A provides definitions for the engineering and security terminology used within
4137 Special Publication 800-160, Volume 1.

abstraction [ISO 24765]	View of an object that focuses on the information relevant to a particular purpose and ignores the remainder of the information.
acquirer [ISO 15288]	Stakeholder that acquires or procures a product or service from a supplier.
acquisition [ISO 15288]	Process of obtaining a system, product, or service.
activity [ISO 15288]	Set of cohesive tasks of a process.
adequate security (systems)	Meets minimum tolerable levels of security, as determined by analysis, experience, or a combination of both; and is as secure as reasonably practicable (i.e., incremental improvement in security would require an intolerable or disproportionate deterioration of meeting other system objectives such as those for system performance, or would violate system constraints).
adverse consequence [ISO 15026-1]	An undesirable consequence associated with a loss.
adversity	The conditions that can cause a loss of assets (e.g., threats, attacks, vulnerabilities, hazards, disruptions, and exposures).
agreement [ISO 15288]	Mutual acknowledgement of terms and conditions under which a working relationship is conducted (e.g., memorandum of agreement or contract).
anomaly [ISO 24765]	Condition that deviates from expectations, based on requirements specifications, design documents, user documents, or standards, or from someone's perceptions or experiences.
anti-tamper [DODI 5200]	Systems engineering activities intended to prevent or delay exploitation of critical program information in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering. See <i>tampering</i> .

architecture [ISO 42010]	Fundamental concepts or properties related to a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution. Refer to <i>security architecture</i> .
architecture (system) [ISO 42010]	Fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution.
architecture description [ISO 42010]	A work product used to express an architecture.
architecture framework [ISO 42010]	Conventions, principles, and practices for the description of architectures established within a specific domain of application and/or community of stakeholders.
architecture view [ISO 42010]	A work product expressing the architecture of a system from the perspective of specific system concerns.
architecture viewpoint [ISO 42010]	A work product establishing the conventions for the construction, interpretation, and use of architecture views to frame specific system concerns.
artifact [ISO 19014]	Work products that are produced and used during a project to capture and convey information, (e.g., models, source code).
asset [ISO 24765]	Anything that has value to a person or organization. <i>Note 1:</i> Assets have interrelated characteristics that include value, criticality, and the degree to which they are relied upon to achieve organizational mission/business objectives. From these characteristics, appropriate protections are to be engineered into solutions employed by the organization. <i>Note 2:</i> An asset may be tangible (e.g., physical item such as hardware, software, firmware, computing platform, network device, or other technology components) or intangible (e.g., information, data, trademark, copyright, patent, intellectual property, image, or reputation).
assurance [ISO 15026-1]	Grounds for justified confidence that a claim has been or will be achieved. <i>Note 1:</i> Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated. <i>Note 2:</i> Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims.
assurance case [ISO 15026-1]	A reasoned, auditable artifact created that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s).

assurance evidence	The information upon which decisions regarding assurance, trustworthiness, and risk of the solution are substantiated. <i>Note:</i> Assurance evidence is specific to an agreed-to set of claims. The security perspective focuses on assurance evidence for security-relevant claims whereas other engineering disciplines may have their own focus (e.g., safety).
availability [ISO 7498-2]	Property of being accessible and usable on demand by an authorized entity.
baseline [IEEE 828]	Formally approved version of a configuration item, regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle. <i>Note:</i> The engineering process generates many artifacts that are maintained as a baseline over the course of the engineering effort and after its completion. The configuration control processes of the engineering effort manage baselined artifacts. Examples include stakeholder requirements baseline, system requirements baseline, architecture/design baseline, and configuration baseline.
behavior [ISO 14258] adapted]	The way an entity functions as an action, reaction, or interaction. How a system element, system, or system of systems acts, reacts, and interacts.
body of evidence	The totality of evidence used to substantiate trust, trustworthiness, and risk relative to the system.
claim [ISO 15026-1]	A true-false statement about the limitations on the values of an unambiguously defined property called the claim's property; and limitations on the uncertainty of the property's values falling within these limitations during the claim's duration of applicability under stated conditions.
complex system [INCOSE19]	A system in which there are non-trivial relationships between cause and effect: each effect may be due to multiple causes; each cause may contribute to multiple effects; causes and effects may be related as feedback loops, both positive and negative; and cause-effect chains are cyclic and highly entangled rather than linear and separable.
component	See <i>system element</i> .

<p>concept of operations [ANSI G043B]</p>	<p>Verbal and graphic statement, in broad outline, of an organization’s assumptions or intent in regard to an operation or series of operations of new, modified, or existing organizational systems.</p> <p><i>Note 1:</i> The concept of operations frequently is embodied in long-range strategic plans and annual operational plans. In the latter case, the concept of operations in the plan covers a series of connected operations to be carried out simultaneously or in succession to achieve an organizational performance objective.</p> <p><i>Note 2:</i> The concept of operations provides the basis for bounding the operating space, system capabilities, interfaces, and operating environment.</p>
<p>concept of secure function</p>	<p>A strategy for achievement of secure system function that embodies proactive and reactive protection capability of the system.</p> <p><i>Note 1:</i> This strategy strives to prevent, minimize, or detect the events and conditions that can lead to the loss of an asset and the resultant adverse impact; prevent, minimize, or detect the loss of an asset or adverse asset impact; continuously deliver system capability at some acceptable level despite the impact of threats or uncertainty; and recover from an adverse asset impact to restore full system capability or to recover to some acceptable level of system capability.</p> <p><i>Note 2:</i> The concept of secure function is adapted from historical and other secure system concepts such as <i>Philosophy of Protection</i>, <i>Theory of Design and Operation</i>, and <i>Theory of Compliance</i>.</p>
<p>concern [ISO 42020]</p>	<p>Matter of interest or importance to a stakeholder.</p>
<p>concern (system) [ISO 42010]</p>	<p>Interest in a system relevant to one or more of its stakeholders.</p>
<p>configuration item [ISO 15288]</p>	<p>Item or aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process.</p>
<p>consequence [ISO 15026-1]</p>	<p>Effect (change or non-change), usually associated with an event or condition or with the system and usually allowed, facilitated, caused, prevented, changed, or contributed to by the event, condition, or system.</p>
<p>constraints [ISO 29148]</p>	<p>Limitation on the system, its design, or its implementation or on the process used to develop or modify a system.</p> <p>Limitation that restricts the design solution, implementation, or execution of the system.</p> <p><i>Note:</i> A constraint is a factor that is imposed on the solution by force or compulsion and may limit or modify the design.</p>

criticality [CNSSI 4009]	An attribute assigned to an asset that reflects its relative importance or necessity in achieving or contributing to the achievement of stated goals.
customer [ISO 9000]	Organization or person that receives a product.
cyber-physical system [ISO 21840 adapted]	A system integrating computation with physical processes whose behavior is defined by both the computational (digital and other forms) and the physical parts of the system.
derived requirement [ISO 29148]	<p>A requirement deduced or inferred from the collection and organization of requirements into a particular system configuration and solution.</p> <p><i>Note 1:</i> The next higher-level requirement is referred to as a “parent” requirement while the derived requirement from this parent is called a “child” requirement.</p> <p><i>Note 2:</i> A derived requirement is typically identified during the elicitation of stakeholder requirements, requirements analysis, trade studies or validation.</p>
design [ISO 24765]	Process to define the architecture, system elements, interfaces, and other characteristics of a system or system element.
[ISO 15288]	<p>Result of the process to be consistent with the selected architecture, system elements, interfaces, and other characteristics of a system or system element.</p> <p><i>Note 1:</i> Information, including specification of system elements and their relationships, that is sufficiently complete to support a compliant implementation of the architecture.</p> <p><i>Note 2:</i> Design provides the detailed implementation-level physical structure, behavior, temporal relationships, and other attributes of system elements.</p>
design characteristics [ISO 24765]	Design attributes or distinguishing features that pertain to a measurable description of a product or service.
design margin [NASA07]	The margin allocated during design based on assessments of uncertainty and unknowns. This margin is often consumed as the design matures.

domain [ISO 24765 adapted]	<p>A set of elements, data, resources, and functions that share a commonality in combinations of: (1) roles supported, (2) rules governing their use, and (3) protection needs.</p> <p><i>Note:</i> Security domains may reflect one or any combination of the following: capability, functional, or service distinctions; data flow and control flow associated with capability, functional, or service distinctions; data and information sensitivity; data and information security; or administrative, management, operational, or jurisdictional authority. Security domains that are defined in the context of one or more of the above items, reflect a protection-focused partitioning of the system that translates to relationships driven by trust concerns.</p>
emergence	<p>The behaviors and outcomes that result from how individual system elements compose to form the system as a whole.</p> <p><i>Note:</i> The behavior and outcomes produced by the system are not those of the individual system elements that comprise the system. Rather, the emergent system behavior and outcomes, or properties, result from the composition of multiple system elements.</p>
enabling system [ISO 15288]	<p>System that supports a system of interest during its life cycle stages but does not necessarily contribute directly to its function during operation.</p>
engineered system [INCOSE19]	<p>A system designed or adapted to interact with an anticipated operational environment to achieve one or more intended purposes while complying with applicable constraints.</p>
engineering team	<p>The individuals on the systems engineering team with security responsibilities, systems security engineers that are part of the systems engineering team, or a combination thereof.</p>
environment [ISO 42010]	<p>Context determining the setting and circumstances of all influences upon a system.</p>
event [ISO 73]	<p>Occurrence or change of a particular set of circumstances.</p>
evidence	<p>Grounds for belief or disbelief; data on which to base proof or to establish truth or falsehood.</p> <p><i>Note 1:</i> Evidence can be objective or subjective. Evidence is obtained through measurement, the results of analyses, experience, and the observation of behavior over time.</p> <p><i>Note 2:</i> The security perspective places focus on credible evidence used to obtain assurance, substantiate trustworthiness, and assess risk.</p>
facility [ISO 15288]	<p>Physical means or equipment for facilitating the performance of an action, e.g., buildings, instruments, tools.</p>

incident [ISO 15288]	Anomalous or unexpected event, set of events, condition, or situation at any time during the life cycle of a project, product, service, or system.
information item [ISO 24748-6]	Separately identifiable body of information that is produced, stored, and delivered for human use.
information system [Egov]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Refer to <i>system</i> .
interface [ISO 15288]	Wherever two or more logical, physical, or both, system elements or software system elements meet and act on or communicate with each other.
interoperating system [ISO 15288]	System that exchanges information with the system of interest and uses the information that has been exchanged.
integrity [ISO 13008]	Quality of being complete and unaltered.
life cycle [ISO 15288]	Evolution of a system, product, service, project or other human-made entity from conception through retirement.
life cycle model [ISO 15288]	Framework of processes and activities concerned with the life cycle that may be organized into stages, which also acts as a common reference for communication and understanding.
life cycle security concepts	The processes, methods, and procedures associated with the system throughout its life cycle and provides distinct contexts for the interpretation of system security. Life cycle security concepts apply during program management, development, engineering, acquisition, manufacturing, fabrication, production, operations, sustainment, training, and retirement.
likelihood [ISO 73]	Chance of something happening.
margin [MITRE21]	A spare amount or measure or degree allowed or given for contingencies or special situations. The allowances carried to account for uncertainties and risks. See also <i>design margin</i> and <i>operational margin</i> .

mechanism	<p>A process or system that is used to produce a particular result.</p> <p>The fundamental processes involved in or responsible for an action, reaction, or other natural phenomenon.</p> <p>A natural or established process by which something takes place or is brought about.</p> <p>Refer to <i>security mechanism</i>.</p> <p><i>Note:</i> A mechanism can be technology- or nontechnology-based (e.g., apparatus, device, instrument, procedure, process, system, operation, method, technique, means, or medium).</p>
module [ISO 24765]	<p>Program unit that is discrete and identifiable with respect to compiling, combining with other units, and loading.</p> <p>Discrete and identifiable element with a well-defined interface and well-defined purpose or role whose effect is described as relations among inputs, outputs, and retained state.</p>
monitoring [ISO 73]	<p>Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.</p>
operational concept [ANSI G043B]	<p>Verbal and graphic statement of an organization's assumptions or intent in regard to an operation or series of operations of a specific system or a related set of specific new, existing, or modified systems.</p> <p><i>Note:</i> The operational concept is designed to give an overall picture of the operations using one or more specific systems, or set of related systems, in the organization's operational environment from the users' and operators' perspectives. See also concept of operations.</p>
operational environment	<p>Context determining the setting and circumstance of all influences upon a delivered system.</p> <p><i>Note:</i> Operational environments include physical (e.g., land, air, maritime, space) and cyberspace contexts.</p>
operational margin [NASA11] [INCOSE19]	<p>The margin that is designed in explicitly to provide space between the worst normal operating condition and the point at which failure occurs (derives from physical design margin).</p>

operator [ISO 15288]	Individual or organization that performs the operations of a system. <i>Note 1:</i> The role of operator and the role of user can be vested, simultaneously or sequentially, in the same individual or organization. <i>Note 2:</i> An individual operator combined with knowledge, skills, and procedures can be considered as an element of the system. <i>Note 3:</i> An operator may perform operations on a system that is operated, or of a system that is operated, depending on whether or not operating instructions are placed within the system boundary.
organization [ISO 9000] [ISO 15288]	Group of people and facilities with an arrangement of responsibilities, authorities and relationships. <i>Note:</i> An identified part of an organization (even as small as a single individual) or an identified group of organizations can be regarded as an organization if it has responsibilities, authorities and relationships. A body of persons organized for some specific purpose, such as a club, union, corporation, or society, is an organization.
outcome [ISO 18307]	Result of the performance (or non-performance) of a function or process(es).
party [ISO 15288]	Organization entering into an agreement.
penetration testing [CNSSI 4009]	A test methodology intended to circumvent the security function of a system. <i>Note:</i> Penetration testing may leverage system documentation (e.g., system design, source code, manuals) and is conducted within specific constraints. Some penetration test methods use brute force techniques.
problem [ISO 15288]	Difficulty, uncertainty, or otherwise realized and undesirable event, set of events, condition, or situation that requires investigation and corrective action.
process [ISO 9000]	Set of interrelated or interacting activities which transforms inputs into outputs. A program in execution.
process purpose [ISO 15288]	High-level objective of performing the process and the likely outcomes of effective implementation of the process. <i>Note:</i> The purpose of implementing the process is to provide benefits to the stakeholders.
process outcome [ISO 12207]	Observable result of the successful achievement of the process purpose.

product [ISO 9000]	Result of a process. <i>Note:</i> There are four agreed generic product categories: hardware (e.g., engine mechanical part); software (e.g., computer program); services (e.g., transport); and processed materials (e.g., lubricant). Hardware and processed materials are generally tangible products, while software or services are generally intangible.
project [ISO 15288]	Endeavor with defined start and finish criteria undertaken to create a product or service in accordance with specified resources and requirements. <i>Note:</i> A project is sometimes viewed as a unique process comprising co-coordinated and controlled activities and composed of activities from the Technical Management and Technical Processes defined in this document.
protection needs	Informal statement or expression of the stakeholder security requirements focused on protecting information, systems, and services associated with mission/business functions throughout the system life cycle. <i>Note:</i> Requirements elicitation and security analyses transform the protection needs into a formalized statement of stakeholder security requirements that are managed as part of the validated stakeholder requirements baseline.
qualification [ISO 12207]	Process of demonstrating whether an entity is capable of fulfilling specified requirements.
quality assurance [ISO 9000]	Part of quality management focused on providing confidence that quality requirements will be fulfilled.
quality characteristic [ISO 9000]	Inherent characteristic of a product, process, or system related to a requirement. <i>Note:</i> Critical quality characteristics commonly include those related to health, safety, security, assurance, reliability, availability, and supportability.
quality management [ISO 9000]	Coordinated activities to direct and control an organization with regard to quality.
requirement [ISO 29148] [IEEE 610.12, adapted]	Statement that translates or expresses a need and its associated constraints and conditions. A condition or capability that must be met or possessed by a system or system element to satisfy a contract, standard, specification, or other formally imposed documents.
requirements engineering [ISO 29148]	An interdisciplinary function that mediates between the domains of the acquirer and supplier to establish and maintain the requirements to be met by the system, software or service of interest. <i>Note:</i> Requirements engineering is concerned with discovering, eliciting, developing, analyzing, verifying, validating, managing, communicating, and documenting requirements.

resource [ISO 15288]	Asset that is utilized or consumed during the execution of a process. <i>Note 1:</i> Includes diverse entities such as funding, personnel, facilities, capital equipment, tools and utilities such as power, water, fuel, and communication infrastructures. <i>Note 2:</i> Resources include those that are reusable, renewable or consumable.
retirement [ISO 15288]	Withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system.
risk [ISO 73]	Effect of uncertainty on objectives. <i>Note 1:</i> An effect is a deviation from the expected, positive or negative. A positive effect is also known as an opportunity. <i>Note 2:</i> Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). <i>Note 3:</i> Risk is often characterized by reference to potential events and consequences, or a combination of these. <i>Note 4:</i> Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. <i>Note 5:</i> Uncertainty is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood.
risk analysis [ISO 73]	Process to comprehend the nature of risk and to determine the level of risk.
risk assessment [ISO 73]	Overall process of risk identification, risk analysis, and risk evaluation.
risk criteria [ISO 73]	Terms of reference against which the significance of a risk is evaluated.
risk evaluation [ISO 73]	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.
risk identification [ISO 73]	Process of finding, recognizing, and describing risks.
risk management [ISO 73]	Coordinated activities to direct and control an organization with regard to risk.
risk tolerance [ISO 73]	The organization or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives. <i>Note:</i> Risk tolerance can be influenced by legal or regulatory requirements.

risk treatment [ISO 73]	Process to modify risk.
safety [ISO 12207]	Expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered.
security	Freedom from those conditions that can cause loss of assets with unacceptable consequences.
security architecture	<p>A set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected.</p> <p><i>Note:</i> The security architecture reflects security domains, the placement of security-relevant elements within the security domains, the interconnections and trust relationships between the security-relevant elements, and the behavior and interactions between the security-relevant elements. The security architecture, similar to the system architecture, may be expressed at different levels of abstraction and with different scopes.</p>
security control [OMB A-130]	A mechanism designed to address needs as specified by a set of security requirements.
security domain [CNSSI 4009]	<p>A domain within which behaviors, interactions, and outcomes occur and that is defined by a governing security policy.</p> <p><i>Note:</i> A security domain is defined by rules for users, processes, systems, and services that apply to activity within the domain and activity with similar entities in other domains.</p>
security function	The capability provided by the system or a system element. The capability may be expressed generally as a concept or specified precisely in requirements.
security mechanism [CNSSI 4009]	<p>A method, tool, or procedure that is the realization of security requirements.</p> <p><i>Note 1:</i> A security mechanism exists in machine, technology, human, and physical forms.</p> <p><i>Note 2:</i> A security mechanism reflects security and trust principles.</p> <p><i>Note 3:</i> A security mechanism may enforce security policy and therefore must have capabilities consistent with the intent of the security policy.</p>

security policy [CNSSI 4009]	<p>A set of rules that governs all aspects of security-relevant system and system element behavior.</p> <p><i>Note 1:</i> System elements include technology, machine, and human, elements.</p> <p><i>Note 2:</i> Rules can be stated at very high levels (e.g., an organizational policy defines acceptable behavior of employees in performing their mission/business functions) or at very low levels (e.g., an operating system policy that defines acceptable behavior of executing processes and use of resources by those processes).</p>
security relevance	<p>The functions or constraints that are relied upon to, directly or indirectly, to meet protection needs.</p> <p><i>Note:</i> the term <i>security relevance</i> has been used to differentiate the role of system functions that singularly or in combination, exhibit behavior, produce an outcome, or provide a capability to enforce authorized and intended system behavior or outcomes.</p>
security requirement	<p>A requirement that has security relevance.</p>
security risk [ISO 73] adapted]	<p>The effect of uncertainty on objectives pertaining to asset loss and the associated consequences.</p> <p><i>Note:</i> [ISO 73] defines risk as the effect of uncertainty on objectives. Furthermore, risk can be either positive or negative.</p>
security service [CNSSI 4009]	<p>A security capability of function provided by an entity.</p>
security specification	<p>The requirements for the security-relevant portion of the system.</p> <p><i>Note:</i> The security specification may be provided as a separate document or may be captured with a broader specification.</p>
service [ISO 15288]	<p>Performance of activities, work, or duties.</p> <p><i>Note 1:</i> A service is self-contained, coherent, discrete, and can be composed of other services.</p> <p><i>Note 2:</i> A service is generally an intangible product.</p>
specification [IEEE 610.12]	<p>A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system or component and often the procedures for determining whether these provisions have been satisfied.</p> <p>Refer to <i>security specification</i>.</p>
stage [ISO 15288]	<p>Period within the life cycle of an entity that relates to the state of its description or realization.</p> <p><i>Note 1:</i> As used in this document, stages relate to major progress and achievement milestones of the entity through its life cycle.</p> <p><i>Note 2:</i> Stages often overlap.</p>

stakeholder [ISO 15288]	Individual or organization having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations.
stakeholder (system) [ISO 42010]	Individual, team, organization, or classes thereof, having an interest in a system.
strength of function	<p>Criterion expressing the minimum efforts assumed necessary to defeat the specified security behavior of an implemented security function by directly attacking its underlying security mechanisms.</p> <p><i>Note 1:</i> Strength of function has as a prerequisite that assumes that the underlying security mechanisms are correctly implemented. The concept of strength of functions may be equally applied to services or other capability-based abstraction provided by security mechanisms.</p> <p><i>Note 2:</i> The term robustness combines the concepts of assurance of correct implementation with strength of function to provide finer granularity in determining the trustworthiness of a system.</p>
susceptibility	The inability to avoid adversity.
supplier [ISO 15288]	<p>Organization or an individual that enters into an agreement with the acquirer for the supply of a product or service.</p> <p><i>Note 1:</i> Other terms commonly used for supplier are contractor, producer, seller, or vendor.</p> <p><i>Note 2:</i> The acquirer and the supplier sometimes are part of the 1 same organization.</p>
system [INCOSE19] [ISO 15288]	<p>An arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not. Systems can be <i>physical</i> or <i>conceptual</i>, or a combination of both.</p> <p><i>Note 1:</i> A system is sometimes considered as a product or as the services it provides.</p> <p><i>Note 2:</i> In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun (e.g., aircraft system). Alternatively, the word “system” is substituted simply by a context-dependent synonym (e.g., aircraft), though this potentially obscures a system principles perspective).</p> <p><i>Note 3:</i> A complete system includes all of the associated equipment, facilities, material, computer programs, services, firmware, technical documentation, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment.</p>
system element [ISO 15288]	<p>Member of a set of elements that constitute a system.</p> <p><i>Note:</i> A system element is a discrete part of a system that can be implemented to fulfill specified requirements.</p>
system of interest [ISO 15288]	System whose life cycle is under consideration.

system of systems [INCOSE14] [ISO 21839]	<p>System of interest whose system elements are themselves systems; typically, these entail large-scale interdisciplinary problems with multiple, heterogeneous, distributed systems.</p> <p>Set of systems or system elements that interact to provide a unique capability that none of the constituent systems can accomplish on its own.</p>
system context	<p>The specific system elements, boundaries, interconnections, interactions, and environment of operation that define a system.</p>
system life cycle [IEEE 610.12]	<p>The period of time that begins when a system is conceived and ends when the system is no longer available for use.</p> <p>Refer to <i>life cycle stages</i>.</p>
system security requirement	<p>System requirement that has security relevance. System security requirements define the protection capabilities provided by the system, the performance and behavioral characteristics exhibited by the system, and the evidence used to determine that the system security requirements have been satisfied.</p> <p><i>Note 1:</i> Due to the complexity of system security, there are several types and purposes of system security requirements. These include: (1) structural security requirements that express the passive aspects of the protection capability provided by the system architecture, and (2) functional security requirements that express the active aspects of the protection capability provided by the engineered features and devices (e.g., security mechanisms, inhibits, controls, safeguards, overrides, and countermeasures).</p> <p><i>Note 2:</i> Each system security requirement is expressed in a manner that makes verification possible via analysis, observation, test, inspection, measurement, or other defined and achievable means.</p>
systems engineering [INCOSE19] [ISO 24765]	<p>A transdisciplinary and integrative approach to enable the successful realization, use, and retirement of engineered systems, using systems principles and concepts, and scientific, technological, and management methods.</p> <p>Interdisciplinary approach governing the total technical and managerial effort required to transform a set of stakeholder needs, expectations, and constraints into a solution and to support that solution throughout its life.</p>
systems security engineer	<p>Individual that practices the discipline of systems security engineering, regardless of their formal title. Additionally, the term <i>systems security engineer</i> refers to multiple individuals operating on the same team or cooperating teams.</p>

systems security engineering	A transdisciplinary and integrative approach to enable the successful secure realization, use, and retirement of engineered systems, using systems, security, and other principles and concepts, as well as scientific, technological, and management methods. Systems security engineering is a subdiscipline of systems engineering.
tampering [CNSSI 4009]	An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.
task [ISO 15288]	Required, recommended, or permissible action, intended to contribute to the achievement of one or more outcomes of a process.
threat [CNSSI 4009]	<p>An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss.</p> <p><i>Note:</i> The specific causes of asset loss, and for which the consequences of asset loss are assessed, can arise from a variety of conditions and events related to adversity, typically referred to as disruptions, hazards, or threats. Regardless of the specific term used, the basis of asset loss constitutes all forms of intentional, unintentional, accidental, incidental, misuse, abuse, error, weakness, defect, fault, and/or failure events and associated conditions.</p>
traceability [ISO 29110-1]	Discernible association among two or more logical entities, such as requirements, system elements, verifications, or tasks.
traceability analysis	<p>The analysis of the relationships between two or more products of the development process conducted to determine that objectives have been met or that the effort represented by the products is completed.</p> <p><i>Note:</i> A requirements traceability analysis demonstrates that all system security requirements have been traced to and are justified by at least one stakeholder security requirement, and that each stakeholder security requirement is satisfied by at least one system security requirement.</p>

traceability matrix[\[IEEE 610.12\]](#)

A matrix that records the relationship between two or more products of the development process (e.g., a matrix that records the relationship between the requirements and the design of a given software component).

Note 1: A traceability matrix can record the relationship between a set of requirements and one or more products of the development process and can be used to demonstrate completeness and coverage of an activity or analysis based upon the requirements contained in the matrix.

Note 2: A traceability matrix may be conveyed as a set of matrices representing requirements at different levels of decomposition. Such a traceability matrix enables the tracing of requirements stated in their most abstract form (e.g., statement of stakeholder requirements) through decomposition steps that result in the implementation that satisfies the requirements.

trade-off[\[ISO 15288\]](#)

Decision-making actions that select from various requirements and alternative solutions on the basis of net benefit to the stakeholders.

trade-off analysis

Determining the effect of decreasing one or more key factors and simultaneously increasing one or more other key factors in a decision, design, or project.

trust[\[MITRE21\]](#)

A belief that an entity meets certain expectations and therefore can be relied upon.

Note: The term belief implies that trust may be granted to an entity whether the entity is trustworthy or not.

trust relationship

An agreed upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets.

Note: This refers to trust relationships between system elements implemented by hardware, firmware, and software.

trustworthiness[\[Neumann04\]](#)

Worthy of being trusted to fulfill whatever critical requirements may be needed for a particular component, subsystem, system, network, application, mission, enterprise, or other entity.

Note: From a security perspective, a trustworthy system is a system that meets specific security requirements in addition to meeting other critical requirements.

trustworthy

The degree to which the security behavior of a component is demonstrably compliant with its stated requirements.

user[\[ISO 25010\]](#)

Individual or group that interacts with a system or benefits from a system during its utilization.

Note: The role of user and the role of operator are sometimes vested, simultaneously or sequentially, in the same individual or organization.

validation [ISO 9000]	Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled. <i>Note:</i> A system is able to accomplish its intended use, goals and objectives (i.e., meet stakeholder requirements) in the intended operational environment. The right system was built.
verification [ISO 9000]	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. <i>Note:</i> Verification is a set of activities that compares a system or system element against the required characteristics. This includes, but is not limited to, specified requirements, design description, and the system itself. The system was built right.
verification and validation [IEEE 610.12]	The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements.
view [ISO 24774]	Representation of a whole system from the perspective of a related set of concerns. <i>Note:</i> A view can cover the entire system being examined or only a part of that system.
viewpoint [ISO 24774]	Specification of the conventions for constructing and using a view.
vulnerability	A weakness that can be exploited or triggered to produce an adverse effect. The inability to withstand adversity. <i>Note:</i> Vulnerability can exist in anywhere throughout the life cycle of a system, such as in the CONOPS, procedures, processes, requirements, design, implementation, utilization, and sustainment of the system.

4139 **APPENDIX B**4140 **ACRONYMS**

4141 COMMON ABBREVIATIONS

CNSS	Committee on National Security Systems
DoD	Department of Defense
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INCOSE	International Council on Systems Engineering
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
NDI	Non-Developmental Item
SecDOP	Security Design Order of Precedence
SSE	Systems Security Engineering

4142

4143 APPENDIX C

4144 SECURITY POLICY AND REQUIREMENTS

4145 CRITICAL ELEMENTS FOR BUILDING TRUSTWORTHY SECURE SYSTEMS

4146 This appendix addresses security requirements and policy considerations in support of
4147 [Chapter Three](#), [Appendix D](#), and [Appendix E](#) but is not a complete tutorial on either. This
4148 appendix also discusses the rules and scope of control for security policy ([Section C.1](#));
4149 stakeholder and system security requirements ([Section C.2](#)); secure and non-secure system
4150 states and modes ([Section C.3](#)); and the relationship among security requirements, policy, and
4151 mechanisms ([Section C.4](#)).

4152 C.1 SECURITY POLICY

4153 A security policy is a set of rules ([Section C.1.1](#)) that governs behavior within a defined scope of
4154 control ([Section C.1.2](#)). The term *security policy* is used in different ways including: (1) *security*
4155 *policy objectives*, (2) *organizational security policy*, and (3) *system security policy*. Security
4156 policies have a variety of contexts, authorities, scopes, and purposes as described in Section
4157 C.1.2, and typically form hierarchical relationships (e.g., security policy objectives subsume
4158 organizational security policy, which in turn subsumes system security policy).⁶⁵

4159 C.1.1 Rules

4160 Security policy rules are stated in terms of subjects (i.e., active entities), objects (i.e., passive
4161 entities), and the operations that subjects can perform or invoke on objects.⁶⁶ The rules for each
4162 security policy govern *subject-to-object* behaviors and outcomes. The rules must be accurate,
4163 consistent, compatible, and complete with respect to stakeholder objectives for the defined
4164 scope of control. Otherwise, gaps in the desired governed behavior will occur.

4165 C.1.2 Scope of Control

4166 Security policies reflect and are derived from laws, directives, regulations, life cycle concepts,⁶⁷
4167 requirements, or stakeholder objectives. Each security policy includes a *scope of control* that
4168 establishes the bounds within which the policy applies. Security policy objectives, organizational
4169 security policy, and system security policy typically have a specific scope of applicability as
4170 follows:

- 4171 • **Security Policy (Protection) Objectives:** Policy objectives capture what is to be achieved or a
4172 preferred state. Security policy objectives include assets⁶⁸ to be protected, a statement of
4173 intent to protect the assets within the specific scope of stakeholder responsibility, and the
4174 scope of protections. Security policy objectives are the basis for the derivation of all other
4175 security policy forms.

⁶⁵ Note that *policy*, at the organization and system level, may be plural in practice and captured across multiple entities for management purposes.

⁶⁶ Active entities exhibit behavior (e.g., a process in execution) while passive entities do not (e.g., data, file).

⁶⁷ Life cycle concepts include operation, sustainment, evolution, maintenance, training, startup, and shutdown.

⁶⁸ Implicitly or explicitly.

- 4176 • **Organizational Security Policy:** Organizational policy is the set of rules⁶⁹ that regulate how
4177 an organization achieves its objectives. To be meaningful, the rules provide individuals with
4178 a reasonable ability to determine whether their actions either violate or comply with the
4179 policy. Organizational security policy defines the behavior of individuals in performing their
4180 missions and business functions and is used for the development of processes and
4181 procedures.
- 4182 • **System Security Policy:** System security policy specifies what the security capability of the
4183 system is expected to do. It is the set of restrictions and properties that specifies how a
4184 system enforces or contributes to the enforcement of an organizational security policy.

4185 Security policy goes through an iterative refinement process that decomposes an abstract
4186 statement of security policy into more specific statements of security policy. This occurs in
4187 parallel with security requirements allocation and the decomposition of requirements as the
4188 system design matures. Figure C-1 illustrates security policy allocation across the organization.

4189
4190
4191
4192
4193
4194
4195
4196
4197
4198
4199
4200
4201
4202
4203

4204

4205
4206

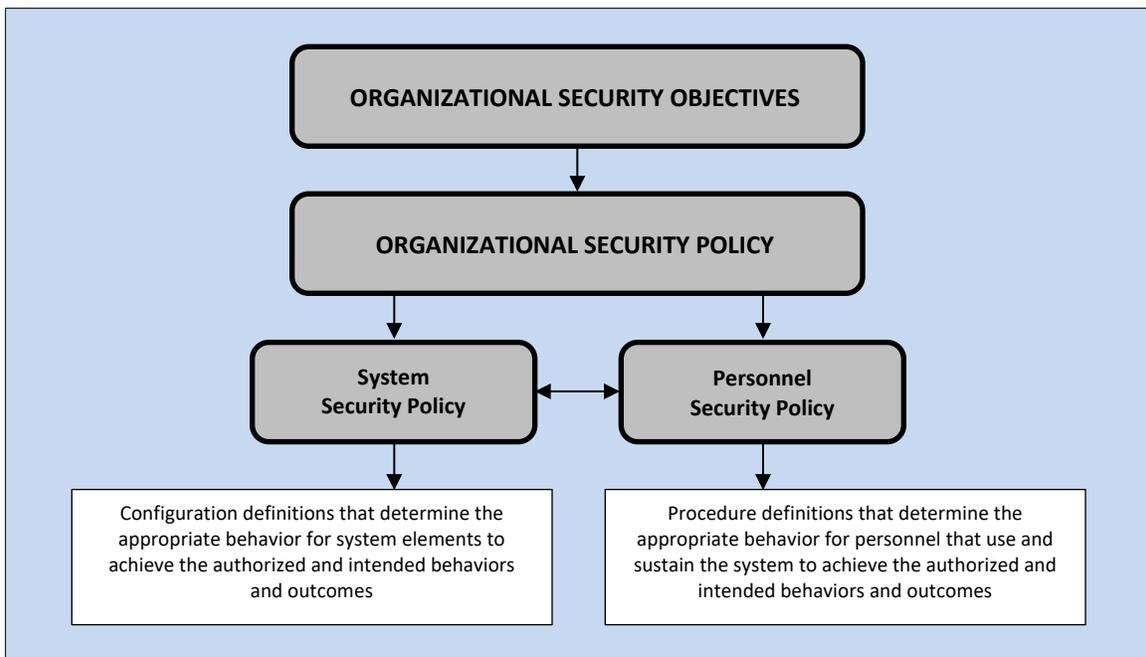


FIGURE C-1: ALLOCATION OF SECURITY POLICY RESPONSIBILITIES

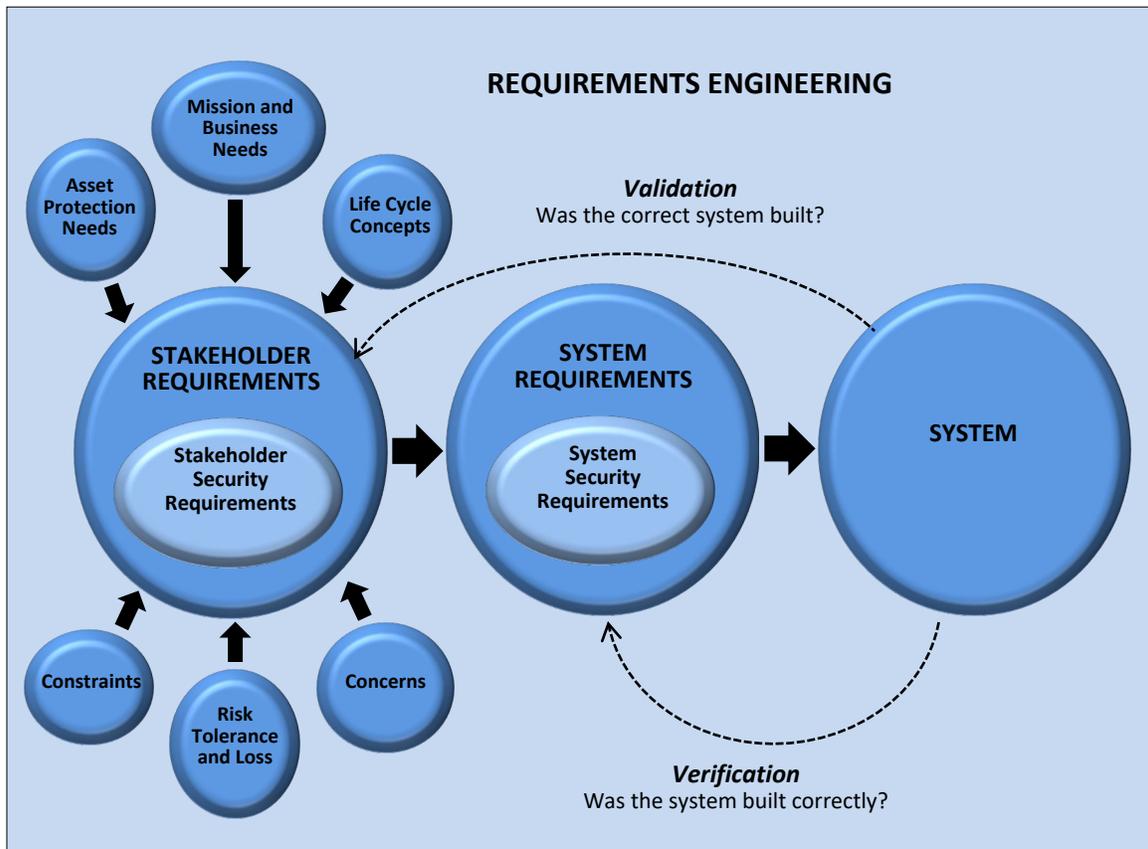
4207 C.2 REQUIREMENTS

4208 A *requirement* is a statement that translates or expresses a specific need and its associated
4209 constraints and conditions [ISO 29148].⁷⁰ *Security requirements* translate or express protection
4210 needs (Section 2.3.7), associated constraints, and associated conditions. The constraints also
4211 reflect concerns about the system functions, system architecture, and design to ensure that
4212 they are specified in a manner that avoids and reduces susceptibilities, defects, flaws, and
4213 weaknesses (Section 2.3.8) and is consistent with the needs of active security functions.

⁶⁹ The rules may be captured in laws and practices.

⁷⁰ General requirements and definition processes are described in sources such as [ISO 29148] and [INCOSSE20].

4214 Requirements can be categorized as: (1) *stakeholder requirements* that address the need to be
 4215 satisfied in a design-independent manner; and (2) *system requirements* that express the specific
 4216 solution that will be delivered (design-dependent manner). Figure C-2 illustrates the two types
 4217 of requirements and their relationship to the verification and validation of the system.



4218
 4219

FIGURE C-2: STAKEHOLDER AND SYSTEM REQUIREMENTS

4220 Security requirements and security-relevant constraints and conditions on other requirements
 4221 are informed by various items, such as those pictured in Figure C-3.

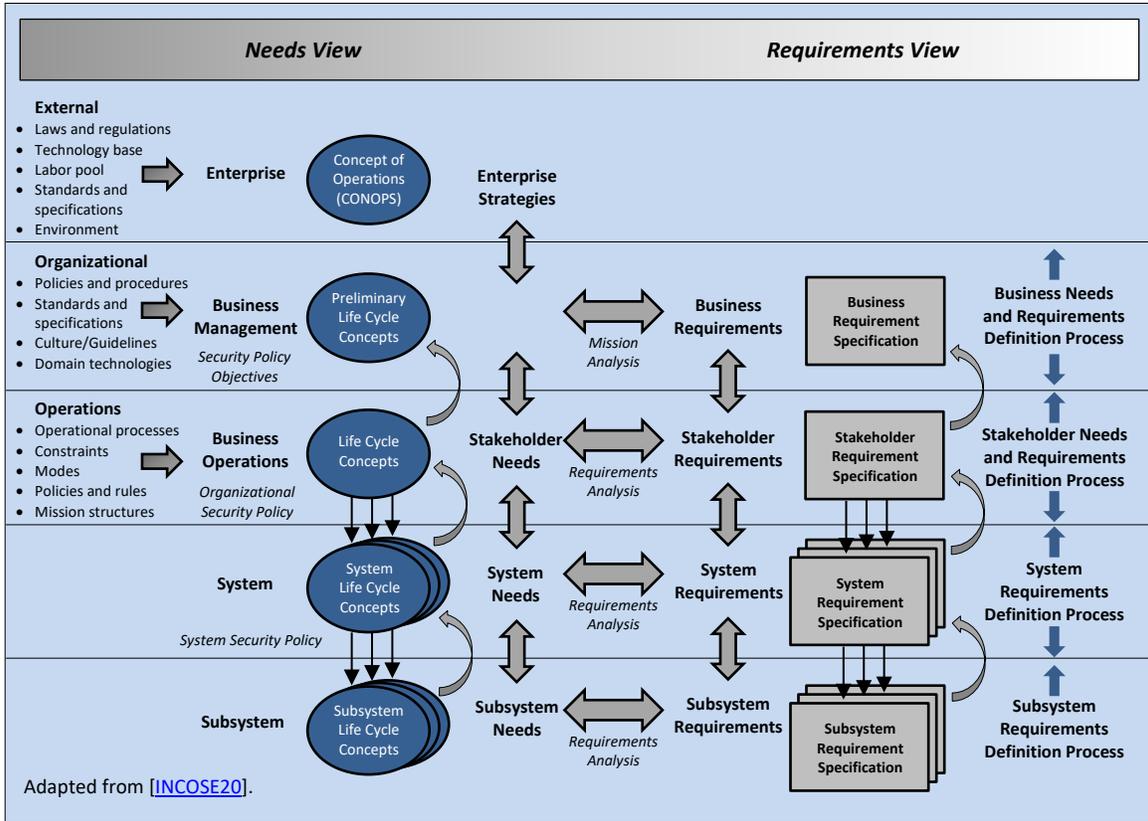
4222 C.2.1 Stakeholder Security Requirements

4223 *Stakeholder security requirements* are those stakeholder requirements that are security
 4224 relevant. Stakeholder security requirements specify:

- 4225 • The protection needed for the mission or business, data, information, processes, functions,
 4226 humans, and system assets
- 4227 • The roles, responsibilities, and security-relevant actions of individuals who perform and
 4228 support the mission or business processes
- 4229 • The interactions between the security-relevant solution elements
- 4230 • The assurance that is to be obtained in the security solution

4231 Systems security considerations within activities and tasks (such as those described in [Chapter](#)
 4232 [Three](#)) provide the security perspective to ensure that the appropriate stakeholder security
 4233 requirements are included in the stakeholder requirements and that the stakeholder security
 4234 requirements are consistent with all other stakeholder requirements.

4235
 4236
 4237
 4238
 4239
 4240
 4241
 4242
 4243
 4244
 4245
 4246
 4247
 4248
 4249
 4250
 4251
 4252
 4253
 4254
 4255
 4256
 4257
 4258



4259 **FIGURE C-3: ENTITIES THAT AFFECT SECURITY REQUIREMENT DEVELOPMENT**

4260 **C.2.2 System Security Requirements**

4261 System requirements specify the technical view of a system or solution that meets the specified
 4262 stakeholder needs. The system requirements are a transformation of the validated stakeholder
 4263 requirements. System requirements specify what the system or solution must do to satisfy the
 4264 stakeholder requirements. *System security requirements* are those system requirements that
 4265 are security relevant. These requirements define:

- 4266
- 4267 • The protection capabilities provided by the security solution
 - 4268 • The performance and behavioral characteristics exhibited by the security solution
 - 4269 • Assurance processes, procedures, and techniques
 - 4270 • Constraints on the system and the processes, methods, and tools used to realize the system
 - The evidence required to determine the system security requirements have been satisfied⁷¹

⁷¹ Each system security requirement is expressed in a manner that makes verification possible via observation, analysis, test, inspection, measurement, or other defined and achievable means.

4271 Due to the complexity of system security, there are several types and purposes of system
4272 security requirements. These include: (1) *structural security requirements* that express the
4273 passive aspects of the protection capability provided by the system architecture, and (2)
4274 *functional security requirements* that express the active aspects of the protection capability
4275 provided by engineered features and devices (e.g., security mechanisms, controls, safeguards,
4276 inhibits, overrides, and countermeasures). The decomposition of system security requirements
4277 is accomplished as part of the system requirements decomposition and is to be consistent with
4278 the different levels of hierarchical abstraction and forms of the system requirements.

4279 **C.3 SYSTEM STATES—SECURE AND NON-SECURE**

4280 Systems once implemented will have states which may be secure or nonsecure. Policy and
4281 requirements reflect these states. In [Section 2.3.4](#), the definition of security was interpreted to
4282 capture what is meant by a secure system:

4283 *A secure system is a system that – for all of its identified states, modes, and transitions –*
4284 *ensures that only the authorized intended behaviors and outcomes occur, thereby providing*
4285 *freedom from those conditions, both intentionally/with malice and unintentionally/without*
4286 *malice, that can cause a loss of assets with unacceptable consequences.*

4287 This interpretation expresses an **ideal** that captures the essential aspects of what it means to
4288 achieve system security. These aspects include:

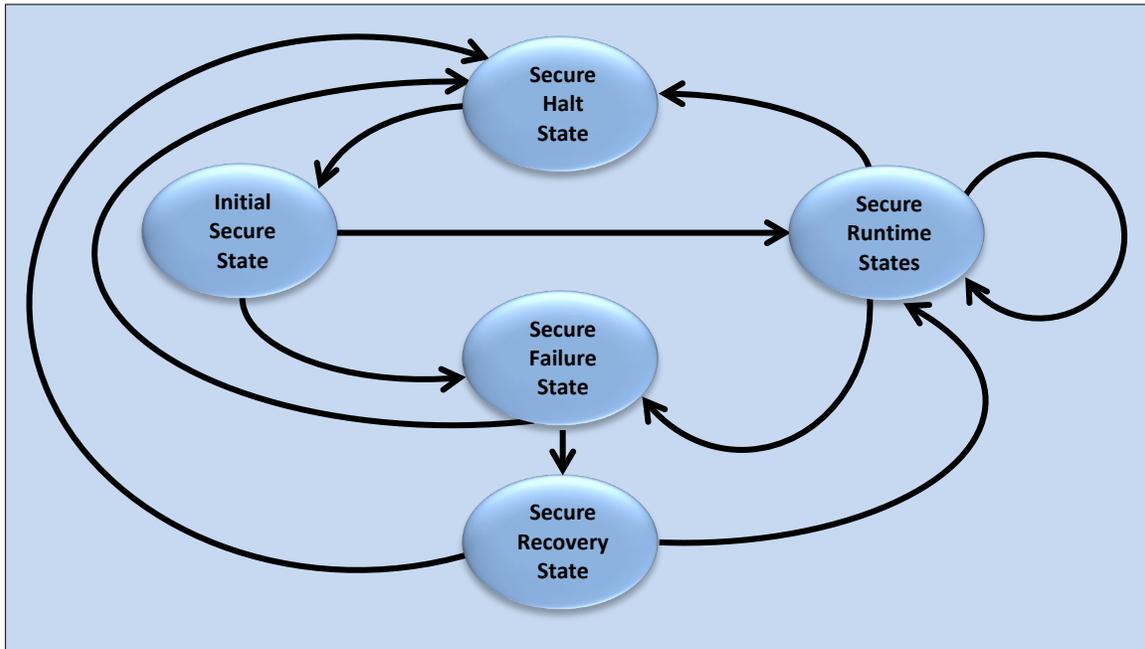
- 4289 • Enabling the delivery of the required capability despite intentional and unintentional forms
4290 of adversity.
- 4291 • Enforcing constraints to ensure that only the desired behaviors and outcomes associated
4292 with the required capability are realized while satisfying the first aspect.
- 4293 • Enforcing constraints based on a set of rules to ensure that only authorized human-to-
4294 machine and machine-to-machine interactions and operations are allowed to occur while
4295 satisfying the second aspect.

4296 The system security policy and system requirements reflect that the set of all possible system
4297 states may be partitioned into the set of secure states (i.e., what states are allowed) and the set
4298 of nonsecure states (i.e., what states are not allowed). A secure system is, therefore, a system
4299 that begins execution in a secure state and cannot transition to a nonsecure state. That is, every
4300 state transition results in the same secure state or another secure state. Each state transition
4301 must also be secure. Figure C-4 illustrates these “idealized” secure system state transitions.

4302 While it is theoretically possible to engineer such an idealized system, it is impractical to do so.
4303 Therefore, security policies and requirements should include additional states and supporting
4304 state transitions that reflect the key principles of [Protective Failure](#) and [Protective Recovery](#).
4305 Protective failure requires the ability to: (1) detect that the system is in a nonsecure state, and
4306 (2) detect a transition that will place the system into a nonsecure state to avoid the propagation
4307 of new failure.

4308 Protective failure calls for responsive and corrective actions. It includes transitioning to a secure
4309 halt state with a protected recovery to allow for continuation of operations in a reconstituted,
4310 reconfigured, or alternative secure operational mode. Other stakeholder objectives may also
4311 necessitate the continuation of operations in a less-than-fully-secure state. The policy and

4312 requirements should reflect such necessities. Protective recovery requires the ability to effect
 4313 reactive, responsive, or corrective action to securely transition from a nonsecure state to a
 4314 secure state (or a less insecure state). The secure state achieved after completion of protective
 4315 recovery actions includes those actions that limit or prevent any further state transition and
 4316 those that constitute some type of degraded mode, operation, or capability.
 4317



4318

FIGURE C-4: IDEALIZED SECURE SYSTEM STATE TRANSITIONS

4319 C.4 DISTINGUISHING REQUIREMENTS, POLICY, AND MECHANISMS

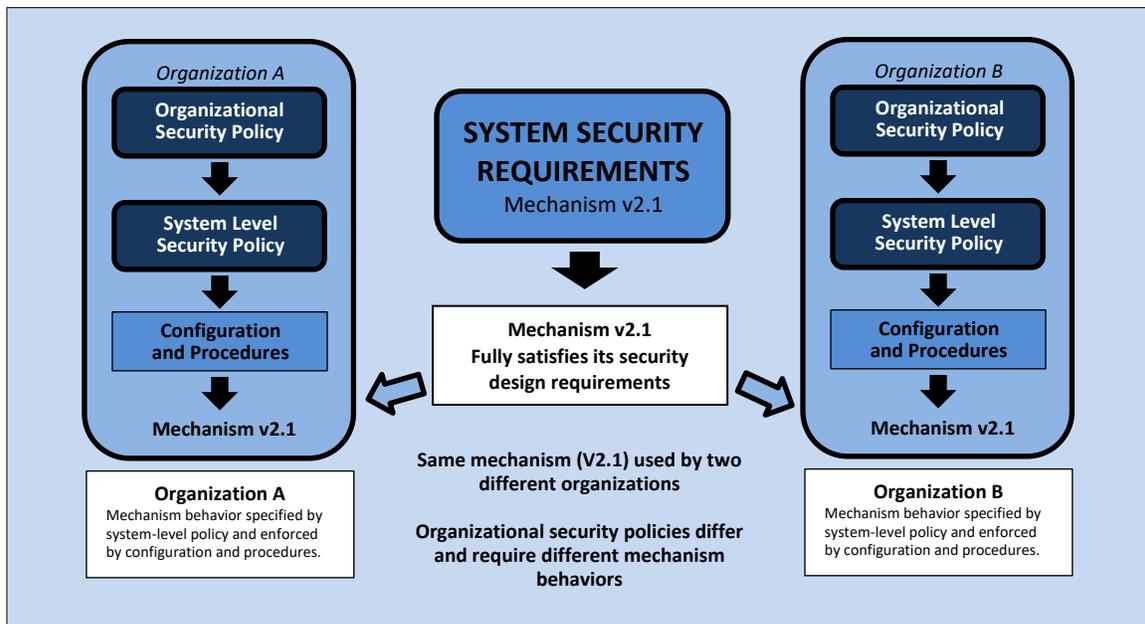
4320 The terms *requirements*, *policy*, and *mechanisms* are often used in abstract manners that allow
 4321 them to be considered as synonyms. However, when used in the context of the engineering of
 4322 trustworthy secure systems, these terms are distinct in their meaning and importance to
 4323 specifying, realizing, utilizing, and sustaining systems in a trustworthy secure manner.

4324 The security policy states the behavior that is necessary to achieve a secure condition, whereas
 4325 a security mechanism is a means to achieve the necessary behavior. The distinction between
 4326 security policy and security mechanism extends to differentiating security requirements from
 4327 security policy. Security requirements specify the capability, behavior, and quality attributes
 4328 exhibited and possessed by security mechanisms as well as constraints on each. Security policy
 4329 specifies how the security mechanisms must behave in some operational context and the
 4330 constraints on those behaviors. From the system standpoint, a human is a system element and
 4331 may serve as a security mechanism. Therefore, the human is expected to behave as stated by
 4332 relevant security policy and security requirements.

4333 Requirements, policies, and mechanisms have an important dependency relationship. System
 4334 security requirements specify the capabilities and behaviors that a security mechanism is able to
 4335 provide. A security policy specifies the particular aspects that a mechanism must enforce to
 4336 achieve organizational objectives. This means that a secure system cannot be achieved if the

4337 security requirements do not fully specify the minimal capability necessary to enforce the
 4338 security policy. It also means that the satisfaction of requirements alone does not result in a
 4339 secure system. Verification and validation activities must be accomplished separately and
 4340 coordinated to ensure the individual and combined correctness and effectiveness of the
 4341 requirements and policy.

4342 Figure C-5 illustrates the significance of the consistency relationship that must be maintained
 4343 across interacting security requirements, security policy, and security mechanisms.



4344
 4345

FIGURE C-5: RELATIONSHIP BETWEEN MECHANISMS AND SECURITY POLICY ENFORCEMENT

4346 Any security mechanism that fully satisfies its system security requirements may be deemed
 4347 capable of enforcing the security policy that is defined for two different organizations. Each
 4348 organization will use the same mechanism and configure it to behave in a manner that enforces
 4349 the rules of their organizational security policy. However, if the organizations were to switch
 4350 mechanisms and keep the same configuration of the mechanism, they would achieve uncertain
 4351 results (unless their security policy objectives required the exact same configuration of the
 4352 mechanism). From this, the following conclusions may be drawn:

- 4353
- 4354 • Requirements determine the capability for security mechanisms
 - 4355 • Security policy determines the behavior that is deemed “secure” behavior
 - 4356 • For a mechanism to be deemed secure, the requirements for the capability of the
 4357 mechanism must be consistent with the security policy enforcement rules; the mechanism
 4358 must satisfy the security requirements; and the mechanism must be configured to behave in
 a manner defined by the organizational security policy.

4359 **APPENDIX D**4360 **TRUSTWORTHY SECURE DESIGN**

4361 FOUNDATIONAL CONCEPTS FOR THE TRUSTWORTHY SECURE DESIGN OF SYSTEMS

4362 **T**his appendix discusses the approach and considerations for application of the elements of
4363 a trustworthy secure system design. This includes a discussion of the system’s authorized
4364 and intended behaviors and outcomes, the security design order of precedence, and the
4365 functional design and trade space considerations.

4366 A principled and effective system design is necessary for trustworthiness. The principled basis
4367 and the effectiveness of the design is supported by evidence, thereby making the resultant
4368 system trustworthy. The trustworthy secure design concepts described in this appendix provide
4369 a balanced and integrated approach that optimally protects against asset loss.

4370 The content in this appendix is supplemented by an in-depth discussion of the principles for
4371 trustworthy secure design in [Appendix E](#) and the concepts of trustworthiness and assurance in
4372 [Appendix F](#). The application of the principles should be planned for, appropriately scoped, and
4373 revisited throughout the system life cycle and engineering effort. The principles provide a sound
4374 basis for reasoning about a system and permit a demonstration of system trustworthiness
4375 through *assurance* based on relevant and credible evidence.

4376 **D.1 DESIGN APPROACH FOR TRUSTWORTHY SYSTEMS**

4377 The design approach for engineering trustworthy secure systems is intended to establish and
4378 maintain the ability to deliver system capabilities at an acceptable level of performance⁷² while
4379 minimizing the occurrence and extent of loss. The approach provides a system structure for
4380 optimal employment of the tactical engineered features and devices.^{73 74} The system design
4381 must provide the intended behaviors and outcomes, avoid the unintended behaviors and
4382 outcomes, prevent loss, and limit loss when it occurs. A trustworthy secure design includes a
4383 margin⁷⁵ and a situational awareness capability⁷⁶ to account for the unknowns and uncertainty
4384 inherent in the system and its operational environment, as well as related adversity.

⁷² An acceptable level of performance lies between the minimum threshold of acceptability and the objective of maximum performance. The level of acceptable performance may vary across operational or system states and modes (e.g., patrolling in clear weather versus severe weather conditions), may vary across contingency conditions (e.g., normal, degraded), and may be subject to operational priorities (e.g., search and rescue, manhunt).

⁷³ The term *tactics* refers to a specific means to accomplish an action. Tactics focus on *how* to accomplish the action (e.g., using engineered features and devices, including security controls, to react to a threat). This is in contrast to the term *strategy*, which takes a broader view and focuses on *what* to accomplish (e.g., a design approach for trustworthy secure systems) [Young14].

⁷⁴ [Snyder15] postulates that “poor systems security engineering is very difficult to mitigate by overlaying security controls, whereas security controls overlaid on a sound, secure design can be quite effective.”

⁷⁵ The term *margin* refers to a spare amount, measure, or degree allowed or given for contingencies or special situations. The allowances are carried to account for uncertainties and risks. In general, there are two types of margins used in systems engineering: *design margin* and *operational margin*. See the design principle of [Loss Margins](#).

⁷⁶ A *situational awareness* capability includes detecting pending and actual failure (e.g., by crossing the threshold of the margins that have been established). See the design principle of [Anomaly Detection](#).

4385 The design approach includes the following elements:⁷⁷

- 4386 • Define the intended behaviors and outcomes for the system.⁷⁸
- 4387 • Identify the system states and conditions that reflect the intended behaviors and outcomes.
- 4388 • Identify the system states and conditions that potentially lead to loss in the system.
- 4389 • Engineer to prevent loss to the extent practicable (preferred), and limit the loss that does
- 4390 occur (where, when, and to the extent necessary and practicable).

4391 Iterate the above elements to address how the functions that serve to prevent or limit loss may
4392 fail due to intentional or unintentional reasons.

4393 Figure D-1 illustrates the steps in the design approach in the context of the *Systems Security*
4394 *Engineering Framework* described in [Section 2.5](#).

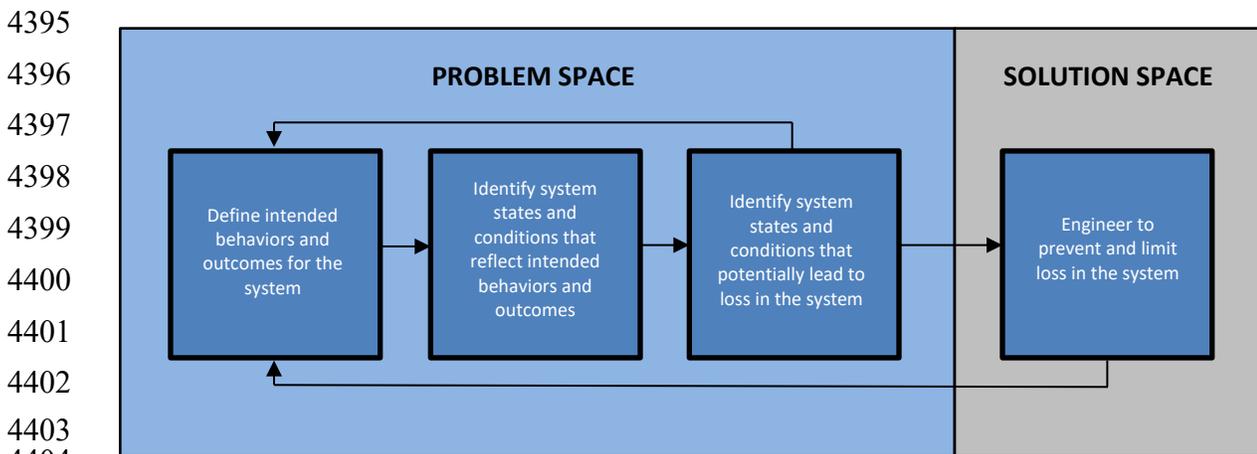


FIGURE D-1: DESIGN APPROACH IN A SYSTEMS SECURITY ENGINEERING FRAMEWORK

4406 D.2 DESIGN FOR BEHAVIORS AND OUTCOMES

4407 A system is to deliver the required capability at a specified level of performance. The system
4408 capability is reflected in its behaviors and outcomes. The design goal is to provide capabilities
4409 that are authorized and intended. However, the system can also deliver a capability that is not
4410 authorized or intended. This possibility exists due to the concept of *emergence*. Emergence
4411 refers to the behaviors and outcomes that result from how individual system elements compose
4412 to form the system as a whole. That is, the behavior and outcomes produced by the system are
4413 not those of the individual system elements that comprise the system. Rather, the emergent
4414 system behavior and outcomes, or properties, result from the composition of multiple system
4415 elements (see trustworthy secure design principle [Structured Decomposition and Composition](#)
4416 and [Figure 4](#)).

⁷⁷ These steps are useful in applying a *system control* concept for any loss-relevant emergent property (e.g., safety, security, resilience).

⁷⁸ This flow iterates through systems engineering as the system is decomposed. Subsequent iterations of this same approach would apply within the elements that comprise the system of interest (i.e., the subsystems, assemblies, and components).

4417 Additionally, while the emergent system properties sought are desired and productive, there are
4418 emergent properties that are not desired or productive. Such properties can produce unknown,
4419 unforeseen, or adverse effects. The engineering of trustworthy secure systems seeks to deliver
4420 only the desired and productive emergent properties of the system because trustworthiness
4421 judgments are based on the expectation that the system can satisfy the stated capability needs.
4422 To achieve this, the design must address emergence at all levels of system abstraction in terms
4423 of how the system is decomposed into its constituent elements and how those elements
4424 compose to produce the system (see the design principle of [Compositional Trustworthiness](#)).
4425
4426

SECURITY AS AN EMERGENT SYSTEM PROPERTY

The objective of security as an emergent system property is to achieve *only* the authorized and intended system behaviors and outcomes. This requires a fundamental understanding of how individual system elements are composed into the system as a whole. Systems are designed from that basis of understanding to limit the emergent behaviors and outcomes that are not specified (including desired unspecified and undesired unspecified behaviors and outcomes).

4435
4436
4437 Both *proactive* and *reactive* aspects are considered as part of an integrated and balanced
4438 engineering approach to defining the authorized and intended behaviors and outcomes needed
4439 to address protection needs. The proactive aspect of the engineering effort addresses actions
4440 taken to prevent and limit loss before the event occurs, while the reactive aspect addresses
4441 actions taken to limit loss and its effects once an event has occurred. The proactive aspect
4442 recognizes the conditions where loss may occur and addresses the scenarios before loss occurs.
4443 If the loss does occur, the results are limited due to actions taken in advance. It is independent
4444 of any specific knowledge of attacks and attacker objectives and is focused on what is possible in
4445 the system's life cycle.

4446 The reactive aspect of the engineering effort recognizes that new, unanticipated, and otherwise
4447 unforeseen adverse consequences will occur despite the proactive planning and institution of
4448 means and methods to control loss and the extent of its consequences. The reactive aspect
4449 enables informed operational decision-making once the system is in use and a loss condition
4450 occurs, proactively giving operations the ability to deal with the loss condition and to better deal
4451 with the loss. The reactive aspect complements the proactive aspect by providing an informed
4452 basis and means for an external entity (e.g., a human operator or system of systems) to act
4453 when failures occur. In essence, the reactive aspect is a proactive engineering activity about
4454 providing a *reactive capability*.

4455 The proactive and reactive aspects must be balanced across all assets, stakeholders, concerns,
4456 and objectives. Achieving such balance requires that security objectives be established and that
4457 requirements elicitation and analysis be conducted to unambiguously and clearly ascertain the
4458 scope of security in terms of addressing failure and the associated consequences in its proactive
4459 and reactive aspects. Figure D-2 illustrates the balanced design strategy for achieving
4460 trustworthy secure systems.

4461
 4462
 4463
 4464
 4465
 4466
 4467
 4468
 4469
 4470
 4471
 4472
 4473
 4474
 4475
 4476
 4477
 4478
 4479
 4480
 4481
 4482
 4483
 4484
 4485
 4486
 4487
 4488
 4489
 4490
 4491
 4492
 4493
 4494
 4495
 4496
 4497
 4498
 4499

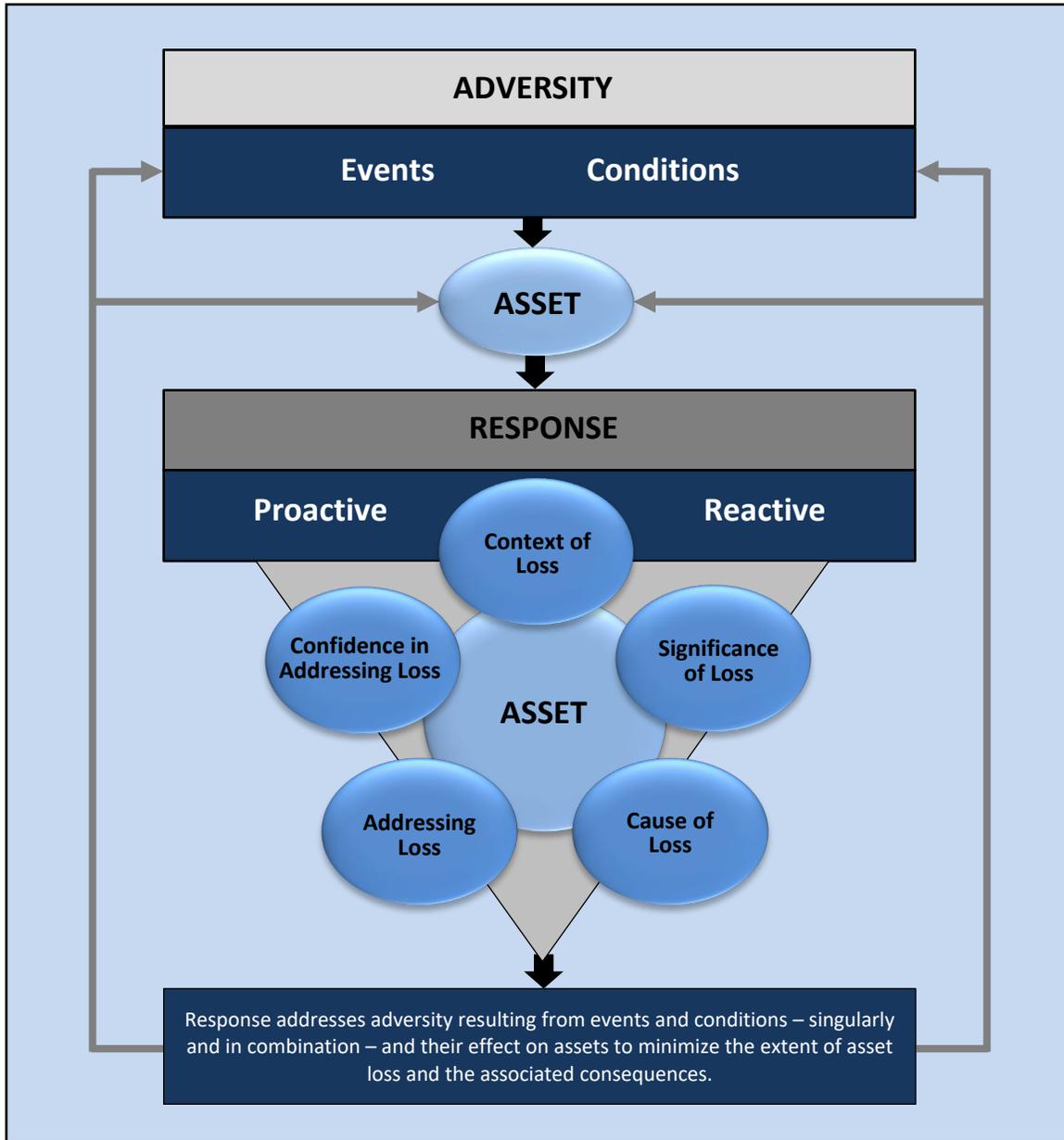


FIGURE D-2: BALANCED DESIGN STRATEGY FOR ACHIEVING TRUSTWORTHY SECURE SYSTEMS

4500 D.3 SECURITY DESIGN ORDER OF PRECEDENCE

4501 The security design order of precedence (SecDOP)⁷⁹ is part of a design approach that uses
 4502 passive architectural features to provide the structure for the employment of engineered
 4503 features and devices. SecDOP reflects a design goal to eliminate the design basis for loss
 4504 potential. Using a principled and assured engineering approach, the SecDOP eliminates
 4505 susceptibility, hazard, and vulnerability to the extent practicable, thereby eliminating the

⁷⁹ The *security design order of precedence* is inspired by the *System Safety Design Order of Precedence*, an optimized design approach for system safety described in [MILSTD-882E].

4506 associated risk. For those cases in which susceptibility, hazard, or vulnerability cannot be
4507 eliminated, the SecDOP reduces the loss potential (e.g., occurrence, impact) to the lowest
4508 acceptable level within the constraints of cost, schedule, and performance. The SecDOP
4509 identifies the design options and lists those options in order of decreasing effectiveness, thus
4510 enabling a maximized return on investment.

4511 The SecDOP acts as follows:

4512 1. **Eliminate the potential for loss through design selection.**

4513 Susceptibility, hazard, and vulnerability are eliminated by selecting a design or material
4514 alternative that completely removes the susceptibility, hazard, and vulnerability and thus
4515 prevents loss.

4516 *Example:* The design selected for a *system function of interest* minimizes the number of
4517 interfaces to other systems (i.e., external interfaces) and the number of internal interfaces
4518 (i.e., interfaces with no connection to other systems). The minimization of interfaces (both
4519 external and internal) is determined in consideration of the interface needs of *all system*
4520 *functions* and results in an across-the-board optimization that does not overly constrain the
4521 design for the *system function of interest*. That is, the design results in less susceptibility,
4522 hazard, and vulnerability than a design that incorporates additional and unnecessary
4523 internal and external interfaces.

4524 *Note:* The design selection to control loss is accomplished to accommodate the need for
4525 mechanisms that provide mediated access and trusted communication as these engineered
4526 features and devices are necessary for a secure system.

4527 2. **Reduce the potential for loss through design alteration.**

4528 If adopting an alternative design or material to eliminate susceptibility, hazard, and
4529 vulnerability is not feasible, consider design changes or material selection that would reduce
4530 the frequency, potential, severity, and/or extent of loss caused by the susceptibility, hazard,
4531 or vulnerability.

4532 *Example:* The selected design for the *system function of interest* has susceptibility, hazard,
4533 and vulnerability due to the system-level design trades made to satisfy the requirements for
4534 *all system functions*, emergence, and the limits of certainty. In response to these conditions,
4535 the design might consider functional domains, defense-in-depth layering, redundancy, and
4536 other approaches to further reduce susceptibility, hazard, and vulnerability.

4537 *Note:* The design alteration to control loss is accomplished to accommodate the need for
4538 mechanisms that provide mediated access and trusted communication, as these engineered
4539 features and devices are necessary for a secure system.

4540 3. **Incorporate engineered features or devices to control the potential for loss.**

4541 If preventing, limiting, or reducing the potential for loss through design alteration and
4542 material selection is not feasible or adequate, employ engineered features and devices to
4543 control loss associated with susceptibility, hazard, and vulnerability. In general, engineered
4544 features actively disrupt the loss scenario sequence and interactions, and devices reduce the
4545 potential, severity, and extent of loss.

4546 There are two general types of engineered features and devices employed to address the
4547 potential for loss associated with the *system function of interest*:

4548 - *Mandatory security features and devices:* Mandatory security features and devices are those
 4549 that apply foundational security principles for the interfaces. For example, each interface
 4550 must have mediated access to control access to and use of the capability and data provided
 4551 by the interface.

4552 - *Function-specific features and devices:* Function-specific security features and devices
 4553 protect against a loss associated with the design's ability to meet functional requirements
 4554 and performance parameters. Engineered features such as redundant data and control
 4555 flows and redundant system elements can supplement the design selection to achieve the
 4556 required protection. The system may also have engineered features that enable external
 4557 entities to intervene into the system to address the potential, severity, or extent of loss.

4558 **4. Provide visibility and feedback to external entities.**

4559 If design alteration, material selection, and engineered features and devices are not feasible
 4560 or do not adequately lower the frequency, potential, severity, or extent of loss caused by
 4561 the susceptibility, hazard, or vulnerability, employ engineered detection and feedback
 4562 systems and warning devices to alert external entities to the presence of a susceptible,
 4563 hazardous, or vulnerable condition; the occurrence of an event that will lead to a loss; or an
 4564 actual loss event. External entities include operational personnel, monitoring systems, or
 4565 other systems capable of responding.

4566 *Example:* Engineered anomaly detection features can be used to provide situational
 4567 awareness data and warnings to system users.

4568 *Note:* The visibility provided is not of value if the external entities are not able to respond
 4569 appropriately. For example, personnel should have appropriate training and standard
 4570 operating procedures for loss.

4571 **5. Incorporate signage, procedures, training, and proper equipment.**

4572 Incorporate procedures, training, signage, and proper equipment where design alternatives,
 4573 design changes, and engineered features and devices are not feasible and warning devices
 4574 cannot adequately lessen the potential, severity, or extent of loss caused by the hazard,
 4575 susceptibility, or vulnerability. Procedures and training include appropriate warnings and
 4576 cautions and may prescribe the use of equipment. For critical losses, the use of signage,
 4577 procedures, training, and equipment as the only means to reduce the potential, severity, or
 4578 extent of loss should be avoided.

4579 *Example:* Procedures and training materials address proper use of the *system function of*
 4580 *interest*, as well as the use of mediated access functions, redundant capabilities, and
 4581 warning systems, including all relevant cautions and warnings.

TRUSTWORTHY SECURE DESIGN

Trustworthy secure design is a means to optimally satisfy the requirements that form the basis for achieving system security objectives across competing and conflicting stakeholder capability needs, concerns, and constraints.

4582

4583 D.4 FUNCTIONAL DESIGN CONSIDERATIONS

4584 This section describes the functional design considerations for trustworthy secure systems.
4585 These include assured functions that provide control enforcement, control decision, and control
4586 infrastructure; the design criteria for mechanisms; security function failure analysis; and trade
4587 space considerations.

4588 D.4.1 Roles for Security-Relevant Control

4589 Historically, from the perspective of secure system design and evaluation, the term *security*
4590 *relevance* has been used to differentiate the role of system functions that singularly or in
4591 combination exhibit behavior, produce an outcome, or provide a capability to enforce
4592 authorized and intended system behavior or outcomes. This includes those authorized
4593 behaviors and outcomes associated with protective failure and protective recovery in the event
4594 of loss. However, from the perspective of the views of security ([Section 2.3.8](#)) and the possibility
4595 of loss due to weaknesses and defects in any system function, all functions have loss- related
4596 concerns and, thus, protection concerns. The active protection functions enforce or contribute
4597 to the control or influence of the behaviors and outcomes of the system or system elements,
4598 and all functions have the potential to influence behaviors and outcomes beyond themselves
4599 and their host system elements. Therefore, protection control functions may be characterized
4600 and analyzed by using the following designations:

- 4601 • **Protection Control Decision Functions:** These functions make authorization decisions or
4602 take other actions for protection control enforcement functions. For example, a protection
4603 control decision function is a function that decides to grant or deny access to a resource
4604 based on a request, possibly from a protection control enforcement function.
- 4605 • **Protection Control Enforcement Functions:** These functions enforce a constraint to ensure
4606 that the system or system element exhibits only authorized and intended behaviors or
4607 outcomes. For example, a protection control enforcement function enforces a decision to
4608 grant or deny access to a resource.
- 4609 • **Protection Control Infrastructure Functions:** These functions support and help protection
4610 control enforcement and control decision functions fulfill their purposes. The functions also
4611 provide data or services or perform operations upon which protection control enforcement
4612 and decision functions depend. For example, a protection control infrastructure function
4613 includes secure storage, secure communication, and anomaly detection mechanisms.

4614 Other functions, some of which may be control functions for other purposes besides protection,
4615 can potentially adversely affect the correct operation of the protection control enforcement,
4616 decision, and infrastructure functions. For the purposes of secure design and evaluation, these
4617 functions are designated *other system functions*. Ideally, these functions should be non-
4618 interfering functions. The objective for non-interference may be achieved through assurance
4619 with constraints on the requirements, architecture, design, and use of these functions.

4620 All system functions can be mapped to one or more of the functions listed above for the
4621 purpose of secure design and evaluation. The importance of the distinction is to guide and
4622 inform a principled design to limit interference among functions with confidence. Such
4623 confidence can be achieved by employing [Trustworthy System Control](#), applying the design
4624 criteria described in [Section D.4.2](#), and optimally placing a function in the system architecture to

4625 limit the side effects and interactions that may interfere with the protection control decision,
4626 protection control enforcement, and control infrastructure functions.

4627 System analyses can also determine the extent to which functions may interfere with other
4628 functions and inform uncertainty that impacts confidence and needed actions for assurance. For
4629 example, to satisfy a size or form-factor constraint, a system function may occupy the same
4630 privilege domain as control enforcement, control decision, or control infrastructure functions,
4631 thereby elevating the privilege of that system function. If the size or form-factor constraint does
4632 not exist, it would be prudent to employ that system function elsewhere to avoid giving the
4633 function elevated privilege. This would increase the assurance that the enforcement, decision,
4634 and infrastructure functions are isolated from the other parts of the system and would not be
4635 adversely impacted by their behavior or provide an avenue for attack.

4636 **D.4.2 Essential Design Criteria for Mechanisms**

4637 To effectively achieve the objectives of trustworthy secure design, engineered features and
4638 devices – often known as *mechanisms* – must satisfy four essential design criteria. They must be
4639 non-bypassable, evaluable, always invoked, and tamper-proof [Uchenick05]. In general, the
4640 design for any control function that provides protection should adhere to those criteria.⁸⁰ A brief
4641 description of the essential design criteria is provided in Table D-1.

4642

TABLE D-1: ESSENTIAL DESIGN CRITERIA FOR MECHANISMS

ESSENTIAL DESIGN CRITERIA	DESCRIPTION
NON-BYPASSABLE	The mechanism must not be circumventable.
EVALUATABLE	The mechanism must be sufficiently small and simple enough to be assessed to produce adequate confidence in the protection provided, the constraint (or control objective) enforced, and the correct implementation of the mechanism. The assessment includes the analysis and testing needed.
ALWAYS INVOKED	The protection provided by a mechanism or feature that is not always invoked is not continuous and therefore, a loss may occur while the mechanism or feature is suspended or turned off.
TAMPER-PROOF	The mechanism or feature and the data that the mechanism or feature depends on cannot be modified in an unauthorized manner.

4643

4644 The design criteria described above are based on the *generalized reference monitor concept*.
4645 The reference monitor concept⁸¹ is an abstract model of the necessary and sufficient properties
4646 that must be achieved by any mechanism that performs an access mediation control function
4647 [Levin07] [Anderson72]. The reference monitor concept is a foundational access control concept
4648 for assured system design. It is defined as a trustworthy abstract machine that mediates all

⁸⁰ The argument that any control function should be non-bypassable, evaluable, always invoked, and tamper-proof follows from an in-depth examination of Systems Theoretic Process Analysis (STPA) as described in [Leveson11], specifically the discussions on why controls may fail and how to address failure.

⁸¹ The *reference monitor concept* is described in the [Trustworthy System Control](#) principle in [Appendix E](#).

4649 accesses to objects by subjects [TCSEC85]. As a concept for an abstract machine, the reference
 4650 monitor does not address any specific implementation. A reference validation mechanism,
 4651 which includes a combination of hardware and software, realizes the reference monitor concept
 4652 to provide the access mediation foundation for a trustworthy secure system.

4653 The generalized reference monitor concept and the four essential design criteria can be used
 4654 effectively as the design basis for individual system elements, collections of elements, networks,
 4655 and systems where intentional and unintentional adversity can prevent the realization of a loss
 4656 control objective. The reference monitor concept also drives the need for rigor in engineering
 4657 activities commensurate with the trust to be placed in the system or its constituent system
 4658 elements.⁸² The concept describes an *abstract model* of the necessary properties that must be
 4659 realized by any mechanism that claims to achieve a constraint or set of constraints and the basis
 4660 for determining the extent to which the properties are satisfied. A mechanism that achieves
 4661 successful constraint has two parts: (1) a means to decide whether to constrain or not constrain,
 4662 and (2) the enforcement of the decision. Enforcement of the decision must sufficiently:

- 4663 • Enforce constraints to achieve only the authorized and intended system behaviors and
 4664 outcomes
- 4665 • Provide self-protection against targeted attacks on the mechanism enforcing the decision
 4666 (including the application of the essential design criteria)
- 4667 • Be absent of self-induced emergent, erroneous, unsafe, and non-assured control actions

4668 The protection characteristics for mechanisms must account for but not be dependent on
 4669 having detailed knowledge of the capability, means, and methods of an adversary.

4670

THE SCIENCE BEHIND THE SECURITY

“Each of these [design] requirements [for mechanisms] is significant, for without them, the mechanism cannot be considered secure. The [need to be tamper-proof] is obvious, since if the reference validation mechanism can be tampered with, its validity is destroyed, as is any hope of achieving security through it. The [third] requirement of always invoking the reference validation mechanism simply states that if the reference validation is (or must be) suspended for some group of programs, then those programs must be considered part of the security apparatus and be [tamper-proof and evaluable]. The [evaluable] requirement is equally important. It states that because the reference validation mechanism is the security mechanism in the system, it must be possible to ascertain that it works correctly in all cases and is always invoked. If this cannot be achieved, then there is no way to know that the reference validation correctly takes place in all cases, and therefore there is no basis for certifying a system as secure.”

-- James P. Anderson
The Anderson Report [Anderson72]

4685

D.4.3 Security Function Failure Analysis

4687 The design principle of [Protective Failure](#) states that a failure of a particular system element
 4688 should neither result in an unacceptable loss nor invoke another loss scenario. The failure of a

⁸² Conceptually, the reference monitor concept can be extended to any control function that is to enforce a system constraint [MITRE21].

4689 security function is of special concern, given the need for security functions to always be
4690 invoked and operating correctly. Consequently, failure analyses must be performed during
4691 system design to determine the impacts of function failure on the system capabilities, including
4692 the protection capability relative to the resulting consequences of such failure and the needed
4693 assurance of the protection capability.

4694 Failure analyses consider the assets that may be impacted by security function failure and the
4695 associated loss consequences. Failure analyses also consider the function allocation to system
4696 elements and the way the system function and element combination interacts with other
4697 system function and element combinations, independent of specific events and conditions that
4698 might lead to the failure. The principles for trustworthy secure design in [Appendix E](#) serve to
4699 guide and inform the analyses.

4700 The outcomes of the security function failure analyses also drive assurance levels and objectives,
4701 as well as the fidelity and rigor of architecture, design, and implementation methods employed
4702 to achieve those objectives. Assurance considerations are discussed in [Appendix F](#).

4703 **D.4.4 Trade Space Considerations**

4704 System design involves a number of trade space decisions. These decisions may be informed by
4705 criticality or priority of an asset, costs, and benefits of an approach. Decision-making about
4706 protecting the various assets includes determining the criticality (e.g., assessing the positive
4707 effect in achieving objectives and the negative effect if there is some loss associated with the
4708 asset) and priority (i.e., relative ranking of equally critical assets) of each asset. The criticality
4709 and priority based on *valuation* are used in investment decisions on the type, rigor, and
4710 expected effectiveness of protection.

4711 The *costs* associated with a trustworthy secure design approach include the cost to acquire,
4712 develop, integrate, operate, and sustain the security features; the cost of the security features
4713 and functions in terms of their system performance impact; the cost of security services used by
4714 the system; the cost of developing and managing life cycle documentation and training; and the
4715 cost of obtaining and maintaining the target level of assurance.

4716 The cost of analysis to substantiate the trustworthiness claims of certain design choices is also
4717 an important trade space factor. Given two equally effective design options, the more attractive
4718 of the two options may be the one that has a lower relative cost to obtain the assurance needed
4719 to demonstrate satisfaction of trustworthiness claims. In all cases, the cost of system security
4720 must be assessed at the system level and consider trustworthiness objectives and the cost that
4721 is driven by the assurance activities necessary to achieve the trustworthiness objectives.

4722 Trustworthiness design principles such as [Commensurate Rigor](#) and [Commensurate](#)
4723 [Trustworthiness](#) inform the trade space analysis.

4724 The benefits derived from a trustworthy secure design approach are determined by its
4725 effectiveness in providing the required protection capability, the trustworthiness that can be
4726 placed on it, and the loss potential associated with it, given the value, criticality, exposure, and
4727 importance of the assets protected. It may be the case that an *optimal balance* between cost
4728 and benefit is realized through the use of a less costly combination of engineering activities and
4729 system features and functions rather than the use of a single cost-prohibitive activity or security

4730 feature or function. It may also be the case that the adverse performance impact on the system
4731 may preclude some security options.

“Retroactive cybersecurity design is a Sisyphean task.”

-- **O. Sami Saydjari**
Engineering Trustworthy Systems [[Saydjari18](#)]

4732 APPENDIX E

4733 PRINCIPLES FOR TRUSTWORTHY SECURE DESIGN

4734 FOUNDATIONS FOR ENGINEERING TRUSTWORTHY SECURE SYSTEMS⁸³

4735 This section describes a set of principles that serve as the foundation for engineering
4736 trustworthy secure systems. The principles for trustworthy secure design are applied to
4737 control the adversity⁸⁴ that might occur as a direct or indirect result of the system
4738 delivering a specified capability at a specified level of performance. The principles represent
4739 research, development, and application experience starting with the early incorporation of
4740 security mechanisms for trusted operating systems to today's fully networked, distributed,
4741 mobile, and virtual computing components, environments, and systems. The principles are
4742 intended to be universally applicable across this broad range of systems, as well as new systems
4743 as they emerge and mature.

4744 The principles for trustworthy secure design provide a basis for reasoning about a system. As
4745 reasoning tools, the inherent suitability of the principles in a particular situation will depend on
4746 the judgment of the practitioner. Engineering judgment must be exercised in the application of
4747 the principles for trustworthy secure systems.⁸⁵ The principles should not be applied as "rules"
4748 to be complied with, nor should they be prioritized, sequenced, or ordered for prescriptive
4749 application, or used individually or in groups as a basis for making judgments of conformance.
4750 Principles are subject to various priorities and constraints that may restrict or preclude their
4751 application. At times, these principles may be in conflict with other principles and must be
4752 deconflicted. In practice, the principles can be satisfied or implemented in various and perhaps
4753 equally effective ways. Within the system life cycle, the applicability of a particular principle may
4754 change due to evolving requirements, protection needs, priorities, or constraints; architecture
4755 and design decisions and trade-offs; or changes in the risk acceptance threshold.

KEY SECURITY OBJECTIVE

An important objective for security is the reduction in uncertainty regarding the occurrence and effects of adverse events. Reducing the uncertainty of adverse events is achieved by eliminating hazards, susceptibility, and vulnerability to the extent possible. Where elimination cannot occur, their effects must be controlled. Applying the design principles for trustworthy secure systems is a part of the means to achieve both the elimination and the control of the hazards, susceptibility, and vulnerability that lead to adverse events [MITRE21].

⁸³ NIST acknowledges and appreciates the contributions of the Naval Postgraduate School Center for Information Systems Security Studies and Research and The MITRE Corporation in providing content for this appendix. The content was guided and informed by the research reports of the principal investigators from those organizations [Levin07] [MITRE21].

⁸⁴ The term *adversity* refers to the conditions that can cause a loss of assets (e.g., threats, attacks, vulnerabilities, hazards, disruptions, and exposures).

⁸⁵ Engineering judgment considerations for the application of the principles for trustworthy secure systems is described in [MITRE21].

4767 The principles for trustworthy secure design are representative of the practices of the safety,
 4768 security, survivability, and resilience communities and the specialty engineering disciplines
 4769 associated with those communities. Collectively, the goals of these practices represent the “end
 4770 objectives” that the system must satisfy for trustworthy control of adverse effects. The concepts
 4771 and theorems from the disciplines of computer science, systems engineering, control systems,
 4772 fault/failure tolerance, software engineering, computer engineering, and mathematics – as
 4773 employed across the communities and specialties – constitute the means to achieve the end
 4774 objectives. The application of the principles should be planned for, appropriately scoped, and
 4775 revisited throughout the system life cycle and engineering effort.

4776 The principles for trustworthy secure design are listed in Table E-1. The principles are divided
 4777 into two categories: (1) *trustworthiness* design principles, and (2) *loss control* design principles.

4778

TABLE E-1: PRINCIPLES FOR TRUSTWORTHY SECURE DESIGN

PRINCIPLES FOR TRUSTWORTHY SECURE DESIGN	
TRUSTWORTHINESS DESIGN PRINCIPLES	LOSS CONTROL DESIGN PRINCIPLES (Cont.)
Clear Abstractions	Defense In Depth
Commensurate Rigor	Distributed Privilege
Commensurate Trustworthiness	Diversity (Dynamicity)
Compositional Trustworthiness	Domain Separation
Hierarchical Protection	Least Functionality
Minimized Trusted Elements	Least Persistence
Reduced Complexity	Least Privilege
Self-Reliant Trustworthiness	Least Sharing
Structured Composition and Decomposition	Loss Margins
Substantiated Trustworthiness	Mediated Access
Trustworthy System Control	Minimize Detectability
LOSS CONTROL DESIGN PRINCIPLES	Protective Defaults
Anomaly Detection	Protective Failure
Commensurate Protection	Protective Recovery
Commensurate Response	Redundancy
Continuous Protection	

4779

4780 **E.1 TRUSTWORTHINESS DESIGN PRINCIPLES**

4781 *Trustworthiness design principles* are based on the historical meaning of trustworthiness and
 4782 trust and their use as the basis for the design of secure systems. In particular, [Neumann04]
 4783 defines the terms *trustworthiness* and *trust* as follows:

- 4784 • **Trustworthiness:** The demonstrated worthiness of an entity to be trusted based on
 4785 evidence that supports a claim or judgment of being trustworthy.
- 4786 • **Trust:** A belief that an entity *can* be trusted. (Implies that trust may be granted to an entity
 4787 whether the entity is trustworthy or not).

4788 Trustworthiness is a cross-cutting objective in the design of systems due to the consequences of
4789 the failure of systems to behave and produce outcomes only as authorized and intended. The
4790 terms *trust* and *trusted* are used to mean “the decision is made to trust because the required
4791 trustworthiness is demonstrated.” Trustworthiness is associated with one of the essential design
4792 criteria and the reference monitor concept ([Section D.4.2](#)). A protection mechanism or feature
4793 must be evaluable (i.e., the mechanism must be sufficiently small and simple enough to be
4794 assessed to produce adequate confidence in the protection provided, the constraint or control
4795 objective enforced, and the correct implementation of the mechanism).

4796 Trustworthiness design principles are fundamental to managing complexity and otherwise aid in
4797 understanding the engineered system. The principles are necessary to achieve loss control
4798 objectives given the complexity in understanding loss in context (based on how the system is
4799 intended to be utilized and sustained). Complexity increases analysis workloads and reduces
4800 confidence in that analysis. Complexity also increases the costs and difficulty of performing
4801 systems analyses for loss. That is, systems may be too complex to be analyzed for adequate
4802 assurance [[Sheard18](#)].

4803 The trustworthiness design principles include:

- 4804 • [Clear Abstractions](#)
- 4805 • [Commensurate Rigor](#)
- 4806 • [Commensurate Trustworthiness](#)
- 4807 • [Compositional Trustworthiness](#)
- 4808 • [Hierarchical Protection](#)
- 4809 • [Minimized Trusted Elements](#)
- 4810 • [Reduced Complexity](#)
- 4811 • [Self-Reliant Trustworthiness](#)
- 4812 • [Structured Decomposition and Composition](#)
- 4813 • [Substantiated Trustworthiness](#)
- 4814 • [Trustworthy System Control](#)

4815 **E.1.1 Clear Abstractions**

4816 **PRINCIPLE:** *The abstractions used to characterize the system are simple, well-defined, accurate,*
4817 *precise, necessary, and sufficient.*

4818 *Note:* Abstractions can help manage the complexity of the system [[ISO 24765](#)]. Clarity in the
4819 abstract representations of the system helps to facilitate an accurate understanding of the
4820 system and how the system functions to deliver the required capability. Clear abstractions also
4821 reduce the potential for misunderstanding or misinterpretation of what is represented by the
4822 abstraction. Applying the principle of clear abstractions means that a system has simple, well-
4823 defined interfaces and functions that provide a consistent and intuitive view of the data and
4824 how it is managed. The elegance (e.g., accuracy, precision, simplicity, necessity, sufficiency) of
4825 the system interfaces – combined with a precise definition of the functional behavior of the
4826 interfaces – promotes ease of analysis, inspection, and testing, as well as the correct and secure

4827 use of the system. Examples that reflect the application of this principle include avoidance of
4828 redundant, unused interfaces; information hiding;⁸⁶ and avoidance of semantic overloading of
4829 interfaces or their parameters (e.g., not using one function to provide different functionality,
4830 depending on how it is used).

4831 It is important to ensure that the appropriate rigor is applied in the development of system
4832 abstractions during design. Clarity in the abstract representation of the system requires the use
4833 of well-defined syntax and semantics with elaboration as needed to ensure the representations
4834 are well-defined, precise, necessary, and sufficient. Clear abstractions promote confidence in
4835 analysis, verification, and the correct use of the system. Abstractions can be achieved through
4836 the use of models, including Systems Modeling Languages.

4837 **REFERENCES:** [[ISO 24765](#)]; [[Schroeder77](#)]; [[Neumann04](#)]; [[Levin07](#)].

4838 **E.1.2 Commensurate Rigor**

4839 **PRINCIPLE:** *The rigor associated with the conduct of an engineering activity provides the*
4840 *confidence required to address the most significant adverse effect that can occur.*

4841 *Note:* Rigor determines the scope, depth, and detail of an engineering activity. Rigor is a means
4842 to provide confidence in the results of a completed engineering activity. Generally, an increase
4843 in rigor translates into an increase in confidence in the results of the activity. Further, increased
4844 confidence reduces the uncertainty that can also reduce risk or provide a better understanding
4845 of what to address to achieve risk reduction. The relationship between rigor and the criticality of
4846 data and information used to make decisions is recognized by systems analysis practice [[ISO](#)
4847 [15288](#)].

4848 The principle of commensurate rigor helps to ensure that the concept of rigor is included as an
4849 equal factor in the trade space of capability, adverse effect, cost, and schedule in the planning
4850 and conduct of engineering activities, method and tool selection, and personnel selection. An
4851 increase in rigor may translate into an increase in the cost of personnel, methods, and tools
4852 required to complete rigorous engineering activities or an increase in schedule to accomplish
4853 the activities with the expected rigor. Any increased cost that may occur can be justified by
4854 acquiring confidence about system performance to limit loss while also addressing the system's
4855 ability to deliver the capability. Therefore, the rigor associated with an engineering activity
4856 should be commensurate to the significance of the most adverse effect associated with the
4857 activity.

4858 **REFERENCES:** [[ISO 15288](#)]; [[Neumann04](#)].

4859 **E.1.3 Commensurate Trustworthiness**

4860 **PRINCIPLE:** *A system element is trustworthy to a level commensurate with the most significant*
4861 *adverse effect that results from a failure of that element.*

4862 *Note:* A trusted element continuously exhibits properties of trust for the duration of the time
4863 that it is depended upon by other system elements. The degree of trustworthiness needed for a
4864 trusted element is determined by those entities that depend on the element. Some basis is

⁸⁶ The term *information hiding*, also called representation-independent programming, is a design discipline to ensure that the internal representation of information in one system component is not visible to another system component invoking or calling the first component, such that the published abstraction is not influenced by how the data may be managed internally.

4865 required to support decisions about trust and trustworthiness. The basis includes expressing the
4866 trust that is to be placed in a system element, expressing the trustworthiness that is exhibited
4867 by the element, and comparing the trustworthiness of different system elements. This principle
4868 is particularly relevant when considering systems and elements in which there are complex
4869 chains of trust dependencies.

4870 **REFERENCES:** [[Schroeder77](#)]; [[Neumann04](#)].

4871 **E.1.4 Compositional Trustworthiness**

4872 **PRINCIPLE:** *The system design is trustworthy for each aggregate composition of interacting*
4873 *system elements.*

4874 *Note:* The trustworthiness of an aggregate of composed system elements cannot be assumed
4875 based on the trustworthiness assertions of each element in the aggregate. Further, the
4876 trustworthiness of an aggregate of composed trustworthy system elements cannot be assumed
4877 to be equal to the trustworthiness of the least trustworthy element in the aggregate. By
4878 definition, a system is a combination of interacting system elements. Each system function
4879 results from the emergent behavior of a composed set of system elements. Likewise, the
4880 trustworthiness of a composed set of elements is an emergent property of the composition.
4881 Therefore, the trustworthiness of the composed set of system elements (i.e., aggregate) for a
4882 given system function must be determined by treating the aggregate as a single discrete
4883 element. The compositional trustworthiness principle addresses how an argument can be made
4884 for system-level trustworthiness given how the constituent elements of the system compose to
4885 form the system and do so by adhering to the composition principles.

4886 **REFERENCES:** [[ISO 15288](#)]; [[Neumann00](#)]; [[Neumann04](#)]; [[Leveson11](#)].

4887 **E.1.5 Hierarchical Protection**

4888 **PRINCIPLE:** *A system element need not be protected from more trustworthy elements.*

4889 *Note:* Hierarchical protection is a simplifying assumption for trade decisions to help determine
4890 where emphasis is placed in providing protection and the extent of the protection effectiveness.
4891 The simplifying assumption introduces susceptibilities to system elements that are dependent
4892 on more trustworthy elements. The assumption relies on validated trust assertions about the
4893 more trustworthy element and acceptable uncertainty associated with behavior outside of the
4894 scope of the validated trust assertions. For example, systems may include a human element,
4895 which is often the more trustworthy element. The assertions of the trusted human are violated
4896 for the malicious insider threat. The extent to which any element is considered trustworthy has
4897 limits, and beyond those limits, the element should not be assumed to remain trustworthy. In
4898 the degenerate case of the most trustworthy system element, it must protect itself from all
4899 other elements. For example, if an operating system kernel is deemed the most trustworthy
4900 component in a system, then it must protect itself from the less trustworthy applications it
4901 supports. However, the applications do not need to protect themselves from the operating
4902 system kernel.

4903 **REFERENCES:** [[Neumann04](#)]; [[Smith12](#)]

4904 **E.1.6 Minimized Trusted Elements**

4905 **PRINCIPLE:** *A system has as few trusted system elements as practicable.*

4906 *Note:* Minimizing trusted system elements is a cost-benefit trade space consideration employed
4907 for the functional allocation of trust within the system. The need for trust is tied to the function
4908 provided by a system element, and that need is independent of any distribution of trust across
4909 multiple elements in the architecture. The trade decision is, therefore, how best to allocate trust
4910 to system elements given the functions they provide and how the elements are best distributed
4911 throughout the architecture where there is justified need for the distribution. The minimization
4912 of trusted system elements is one of several considerations in making that decision.

4913 Trusted elements are generally costlier to construct due to increased rigor in engineering
4914 processes and activities. They also require more analysis to qualify their trustworthiness.
4915 Minimizing the number of trusted system elements reduces the cost of analysis (i.e., decreases
4916 the size, scope, and complexity of the analysis). When the minimization of trusted system
4917 elements considers the principle of [Commensurate Protection](#), the cost-effectiveness of the
4918 analysis is also ensured (i.e., cost of the analysis is justified by the extent of trust required).

4919 Historically, the analysis of interactions between trusted system elements and untrusted system
4920 elements is one of the most important aspects of the trust-based verification of system security
4921 performance. If these interactions are unnecessarily complex, the security of the system will
4922 also be more difficult to ascertain than one whose internal trust relationships are simple and
4923 elegantly constructed. In general, fewer trusted components will result in fewer internal trust
4924 relationships and a simpler system.

4925 **REFERENCES:** [[Schroeder77](#)]; [[Neumann04](#)]; [[Smith12](#)]; [[Saltzer09](#)].

4926 **E.1.7 Reduced Complexity**

4927 **PRINCIPLE:** *The system design is as simple as practicable.*

4928 *Note:* Many engineered systems are complex. Complexity can be found in the system structure,
4929 interfaces, dependencies, data and control flows, and the system's interaction with its external
4930 environment. Some degree of complexity in the system design is inherent, unavoidable, and
4931 must be accepted. The objective is to ensure that the design reflects the extent to which
4932 complexity can be reasonably minimized (i.e., avoid unnecessary complexity). Simplicity in the
4933 system design reduces complexity, allows for increased confidence in the ability to understand
4934 the design, and is less prone to error. A simpler design is less prone to erroneous interpretation
4935 during system analysis, system implementation, and system verification [[Moller08](#)]. Reduced
4936 complexity contributes to confidence in the technical understanding of the design, enabling
4937 more informed trade decisions. It also facilitates the identification of vulnerabilities and the
4938 verification of the correctness and completeness of system security functions.

4939 Complexity is impacted by how the system is decomposed into constituent elements, aggregates
4940 of elements (e.g., subsystems, assemblies), and the composition of those elements to comprise
4941 the system. Identifying and assessing loss scenarios, susceptibilities, and vulnerabilities is made
4942 more difficult by complexity. Thus, reducing complexity helps to facilitate the identification and
4943 assessment of loss scenarios, hazards, susceptibility, and vulnerability to all forms of adversity.
4944 Finally, any conclusion about the correctness, completeness, and existence of vulnerabilities in
4945 systems or system elements can be reached with a higher degree of assurance in contrast to
4946 conclusions reached in situations where the system design is inherently more complex. The
4947 principle of reduced complexity may also be referred to as the principle of simplification or least
4948 common mechanism.

4949 **REFERENCES:** [[Saltzer75](#)]; [[Neumann04](#)]; [[Jackson13](#)]; [[Saleh14](#)]; [[Moller08](#)].

4950 **E.1.8 Self-Reliant Trustworthiness**

4951 **PRINCIPLE:** *The trustworthiness of a system element is achieved with minimal dependence on*
4952 *other elements.*

4953 *Note:* In the ideal case, the trustworthiness of a system element occurs when the claim of
4954 trustworthiness is not dependent on protection from another element. If an element is
4955 dependent on some other element to satisfy its trustworthiness claims, then that element's
4956 trustworthiness is susceptible to any loss or degradation of the protection capability provided by
4957 the other element. The considerations for the extent to which a system element exhibits self-
4958 reliant trustworthiness include:

- 4959 • The trustworthiness objective for the capability
- 4960 • The trustworthiness of the system element in providing the capability
- 4961 • The extent to which the capability provided by a system element is dependent on another
4962 element
- 4963 • The extent to which the trustworthiness associated with a capability is dependent on
4964 another system element

4965 An argument for self-reliant trustworthiness can be applied at the discrete system element
4966 level, at the level of an aggregate of elements, at the system level, or at the system of systems
4967 level. In all cases, the distinction between the capability provided and the trustworthiness
4968 responsibility for that capability must be preserved (e.g., self-reliant trustworthiness cannot be
4969 claimed if the protection assertions for trust are allocated to and therefore dependent on some
4970 other entity). Likewise, when a capability is distributed across multiple system elements, self-
4971 reliant trustworthiness requires that the trust expectations for the capability are properly
4972 allocated across the elements that comprise the distributed capability.

4973 The judgment that a system element is self-reliantly trustworthy is based on the element's
4974 ability to satisfy a specific set of requirements and associated assumptions. An element that is
4975 self-reliantly trustworthy for one set of requirements and assumptions is not necessarily self-
4976 reliantly trustworthy for other sets of requirements and assumptions. Any change in the
4977 requirement, the satisfaction of the requirement, or in the assumptions associated with the
4978 requirement requires reassessment to determine that the element remains self-reliantly
4979 trustworthy.

4980 **REFERENCES:** [[Neumann04](#)].

4981
4982
4983
4984
4985
4986
4987

*"System components [elements] are self-protective. System componentry is augmented, upgraded,
and replaced over time by methods and personnel that cannot be unequivocally trusted."*

-- An Objective of the Security in the Future of Systems Engineering [[FUSE21](#)]

4988 **E.1.9 Structured Decomposition and Composition**

4989 **PRINCIPLE:** *System complexity is managed through the structured decomposition of the system*
4990 *and the structured composition of the constituent elements to deliver the required capability.*

4991 *Note:* The structured decomposition of the system and the subsequent composition of the
4992 constituent system elements are guided and informed by the concepts of modularity, layering,
4993 and partially ordered dependencies. Modularity is the system design technique to “divide and
4994 conquer” – that is, sub-divide the system into smaller, well-defined cohesive components and
4995 assemblies that are referred to as modules. Modularity serves to isolate functions and data
4996 structures into well-defined logical units. Modular decomposition can include the allocation of
4997 policies to systems in a network, the allocation of system policies to layers, the separation of
4998 system applications into processes with distinct address spaces, and the separation of processes
4999 into subjects with distinct privileges based on hardware-supported privilege domains. Modular
5000 design may also extend to consider trust, trustworthiness, privilege, and policy.

5001 Layering is the grouping of modules into a relational structure with well-defined interfaces,
5002 function, data, and control flow so that the dependencies graph among layers is linearly or
5003 partially ordered such that higher layers are dependent only on lower layers [Neumann04].
5004 Partially ordered dependencies among modules (e.g., if module A depends on module B, then
5005 module B cannot depend on module A) and system layering contribute significantly to system
5006 design simplicity and coherence. While a partial ordering of all functions and processes may not
5007 be possible, the inherent problems of circularity can be more easily managed if the circular
5008 dependencies are constrained to occur within layers and minimized within each layer. Partially
5009 ordered dependencies also facilitate system testing and analysis and enable a strong form of
5010 loose coupling (i.e., minimizing interdependencies among modules).

5011 Modularity and layering are effective in managing the complexity of the composed system. They
5012 provide the means to decompose the system into discrete and aggregate elements to better
5013 comprehend the system in terms of its structure, flows, relationships, and how the system
5014 delivers the required capability. The structured composition of the constituent elements must
5015 also adhere to the principle of [Compositional Trustworthiness](#) to provide a basis to support
5016 claims about how the system is composed based on the application of modularity, layering, and
5017 partially ordered dependencies to achieve authorized and intended behaviors and outcomes.

5018 **REFERENCES:** [Saltzer75]; [Schroeder77]; [Neumann04]; [Simovici08]; [Adcock20].

5019 **E.1.10 Substantiated Trustworthiness**

5020 **PRINCIPLE:** *System trustworthiness judgments are based on evidence that demonstrates the*
5021 *criteria for trustworthiness have been satisfied.*

5022 *Note:* Trustworthiness should not be assumed but rather substantiated through evidence that
5023 clearly enables determination of the extent to which an entity is worth being trusted. This helps
5024 to ensure that an entity is never trusted beyond the extent to which it is worthy of trust. The
5025 approach to substantiated trustworthiness requires commensurate rigor with cautious mistrust
5026 (i.e., system elements are assumed to be guilty until they are proven innocent).⁸⁷ Substantiated
5027 trustworthiness is characterized by a design mentality in which all components involved in the

⁸⁷ Adapted from a statement made by John Rushby, SRI International, about the need for software to be treated as “guilty until proven innocent” at a Layered Assurance Workshop (LAW).

5028 design context (i.e., a system element and the elements with which it interacts) are treated with
5029 a mutually suspicious mindset [[Schroeder77](#)][[Neumann04](#)]. Such mutual suspicion reflects
5030 cautious distrust – the feeling or thought that something undesired, unwanted, or unexpected is
5031 possible or can happen. The design for every system element should reflect a lack of trust in
5032 interacting elements or itself. This suspicion assumes element non-performance and addresses
5033 the following two cases:

- 5034 • **Interacting element suspicion (mutual suspicion):** The design for the system element-of-
5035 interest is based on the non-performance of the elements it interacts with and how their
5036 non-performance can influence the behavior and outcomes produced by the element-of-
5037 interest. Mutual suspicion may also be referred to as zero trust.⁸⁸ Designing to mutual
5038 suspicion is reinforced by applying the principle of [Least Privilege](#) to all entities (so an
5039 element executes with only the privileges needed, mitigating harm that may be created)
5040 while applying the principle of [Least Persistence](#) so that each element is minimally exposed.
- 5041 • **Self-suspicion:** The design for the system element-of-interest must consider its own non-
5042 performance independent of any external influence. Designing to self-suspicion may involve
5043 self-monitoring and built-in actions, including built-in testing at the initiation of the element.

5044 This approach forces the system designer to assume things will not go right and to rigorously
5045 seek evidence that demonstrates the effectiveness of the design when things go wrong.

5046 Considerations for system element non-performance include:

- 5047 • The expectation that design elements will behave and produce outcomes that are
5048 inconsistent with their design intent
- 5049 • The constraints, assumptions, and preconditions associated with achieving threshold
5050 performance
- 5051 • Intentional and unintentional events and conditions, typically referred to by terms like fault,
5052 error, failure, and compromise

5053 **REFERENCES:** [[Neumann04](#)]; [[Levin07](#)]; [[Schroeder72](#)].

5054 **E.1.11 Trustworthy System Control**

5055 **PRINCIPLE:** *The design for system control functions conforms to the properties of the generalized*
5056 *reference monitor.*

5057 *Note:* The trustworthy system control principle reflects the generalization of the reference
5058 monitor concept to provide a uniform design assurance basis for trustworthy system control
5059 mechanisms or constraint-enforcing mechanisms that compose to provide system control
5060 functions. The reference monitor concept ([Section D.4.2](#)) is a foundational access control
5061 concept for secure system design. It is defined as a trustworthy abstract machine that mediates
5062 all accesses to objects by subjects [[TCSEC85](#)]. As a concept for an abstract machine, the
5063 reference monitor does not address any specific implementation. A reference validation
5064 mechanism, a combination of hardware and software, realizes the reference monitor concept to
5065 provide the access mediation foundation for a secure system [[Anderson72](#)].

⁸⁸ *Zero trust* means only that an entity is not trusted; zero trust does not mean that the entity is not trustworthy. The term *zero trust* is not to be confused with Zero Trust Architecture (ZTA).

5066 The reference monitor concept has three criteria that provide design assurance of its realization
5067 as a reference validation mechanism:

- 5068 • The reference validation mechanism must be tamper-proof, ensuring that its integrity and
5069 validity is not destroyed.
- 5070 • The reference validation mechanism must always be invoked, and if it cannot be, then the
5071 group of programs for which it provides validation services must be considered part of the
5072 reference validation mechanism and be subject to the first and third requirements.
- 5073 • The reference validation mechanism must be subject to rigorous analysis and tests, the
5074 completeness of which can be assured (with the purpose of ascertaining that the reference
5075 validation mechanism works correctly in all cases).

5076 For trustworthy system control, a fourth criterion of non-bypassability is added ([Section D.4.2](#)).
5077 Successful achievement of the criterion will prevent the interference of outside entities on a
5078 protection mechanism or controller. More specifically:

- 5079 • A protection mechanism or feature should not be circumventable (i.e., the mechanism
5080 should be non-bypassable).
- 5081 • A protection mechanism or feature should be evaluatable (i.e., sufficiently small and simple
5082 enough to be assessed to produce adequate confidence in the protection provided, the
5083 constraint or control objective enforced, and the correct implementation of the mechanism
5084 [see [Reduced Complexity](#)]).
- 5085 • A protection mechanism or feature is always invoked, providing continuous protection.
- 5086 • A protection mechanism or feature must be tamper-proof (i.e., neither the protection
5087 functions nor the data that the functions depend on can be modified without authorization).

5088 Trustworthy system control also uses *protective control*. Protective control encompasses
5089 control, safety, and security concepts to establish a system capability that sufficiently:

- 5090 • Enforces constraints to achieve only the authorized and intended system behaviors and
5091 outcomes
- 5092 • Provides self-protection against targeted attack on the system
- 5093 • Is absent of self-induced emergent, erroneous, unsafe, and non-secure control actions

5094 The notion of protective control underlies the loss control objectives and transforms the
5095 approach for design to not be dependent on having detailed knowledge of the capability,
5096 means, and methods of an adversary. This design approach can be employed in attack-
5097 dependent or attack-independent manners based on the limits of certainty for what is known
5098 with confidence about the adversary.

5099 Trustworthy system control serves well as the design basis for individual system elements,
5100 collections of elements, networks, and systems where intentional and unintentional adversity
5101 can prevent the achievement of the loss control objectives. The principle also drives the need
5102 for rigor in engineering activities commensurate to the trust placed in the system elements.

5103 **REFERENCES:** [[Levin07](#)]; [[Anderson72](#)]; [[TCSEC85](#)]; [[Uchenick05](#)].

5104 E.2 LOSS CONTROL DESIGN PRINCIPLES

5105 *Loss control design principles* are applied in combination with the trustworthiness principles to
5106 yield trustworthy control over the system behavior and outcomes, deliver the required system
5107 capability, and protect against loss. The loss control design principles include:

- 5108 • [Anomaly Detection](#)
- 5109 • [Commensurate Protection](#)
- 5110 • [Commensurate Response](#)
- 5111 • [Continuous Protection](#)
- 5112 • [Defense In Depth](#)
- 5113 • [Distributed Privilege](#)
- 5114 • [Diversity \(Dynamicity\)](#)
- 5115 • [Domain Separation](#)
- 5116 • [Least Functionality](#)
- 5117 • [Least Persistence](#)
- 5118 • [Least Privilege](#)
- 5119 • [Least Sharing](#)
- 5120 • [Loss Margins](#)
- 5121 • [Mediated Access](#)
- 5122 • [Minimize Detectability](#)
- 5123 • [Protective Defaults](#)
- 5124 • [Protective Failure](#)
- 5125 • [Protective Recovery](#)
- 5126 • [Redundancy](#)

5127 E.2.1 Anomaly Detection

5128 **PRINCIPLE:** *Any salient anomaly in the system or in its environment is detected in a timely*
5129 *manner that enables effective response action.*

5130 *Note:* The purpose of anomaly detection is to identify the need to take corrective action to
5131 address a loss condition that has occurred or that will occur if conditions that affect the system
5132 behavior are allowed to persist. Anomaly detection is critical to achieving the loss control
5133 objectives to prevent and limit loss and its adverse effects. The detection of such anomalies
5134 requires monitoring system behaviors and outcomes to confirm that they have not deviated
5135 from the design intent. It also requires monitoring conditions in the environment to identify or
5136 forecast those conditions that can cause an anomaly in the system if corrective action is not
5137 taken. The “timely manner” aspect of anomaly detection reflects the urgency to detect
5138 emerging loss conditions as early as possible. Early detection increases response action options,
5139 such as graduated response options, and ensures that response actions have sufficient time to

5140 have an effect. When the determination of response involves humans in the loop, early
5141 detection enables a more reasoned judgment of appropriate response.

5142 Anomaly detection can be implemented at varying levels of abstraction (e.g., system, sub-
5143 system, assembly, function, mechanism) and may occur in periodic, aperiodic, or event-driven
5144 manners. The basis for anomaly detection within the system is the expectation that the system
5145 behaviors, outcomes, and interactions produced are expected to remain consistent, adhere to
5146 some norm, or are deterministic across all system states and modes. The types of anomalies
5147 include those associated with the results of system behavior; state consistency; continuity of
5148 function; integrity, correctness, and trustworthiness of system elements; system configuration;
5149 and the abuse or misuse of the system.

5150 The basis for anomaly detection in the environment differs from that in the system because the
5151 environment is not within the control of the system. The environment presents a wide range of
5152 adversity to the system, and the system is designed to achieve its design intent within defined
5153 bounds of environmental conditions. Those bounds can be treated as the “norm” for anomaly
5154 detection, whereby environmental conditions that are trending beyond the norm or that reflect
5155 conditions outside of the norm may result in an adverse effect on the system, thus requiring a
5156 planned response to prepare for an impending difficulty or crisis.

5157 Anomaly detection requires capturing data to support all intended response actions for a
5158 detected anomaly, including attribution-related data. Consequently, the rigor in data describing
5159 the anomaly must be commensurate with the consequences of the loss scenarios associated
5160 with the anomaly and of wrong responses in addressing the detected anomaly. The responses
5161 taken will often rely on attribution to uniquely identifiable entities that may be responsible for
5162 undesired actions, behaviors, or outcomes. For non-human entities, corrective actions may
5163 include component replacements, repairs, or other corrections. For human entities, these may
5164 include training, remediation, or disciplinary actions. Wrongful attribution may have undesired
5165 consequences, such as the cost of unnecessarily repairing the wrong system element while an
5166 undesired condition persists or the wrongful termination of an individual. Attribution rigor is
5167 driven by the needed proof that an entity is responsible for an anomaly. Three aspects of
5168 anomaly detection are necessary to provide criteria for an appropriate response action or set of
5169 actions:

- 5170 • **Basis for Correctness:** A system model provides a basis against which actual behavior and
5171 outcomes can be compared to confidently enable conclusions that an anomaly exists or to
5172 determine or forecast that an anomaly is about to occur. System models includes normal,
5173 contingency, degraded, and other system states/modes of operation and account for the
5174 adversity to which the system is subjected.
- 5175 • **Data Collection:** Systems capture self-awareness data in the form of health, status, test, and
5176 other data indicative of actual behavior and outcomes, including traceability to support
5177 attribution. Terms for data collection include instrumentation, monitoring, logging, auditing,
5178 self-tests, and built-in tests.
- 5179 • **Data Interpretation:** The interpretation of data allows for conclusions of unacceptable or
5180 suspicious events that have happened (e.g., halt or failure condition), that are progressing
5181 (e.g., approaching a threshold of failure condition), or that can be expected to happen (i.e.,
5182 in the absence of change, the failure condition will occur), including tracing to responsible
5183 entities to inform appropriate responses to events.

5184 Caution must be taken with the use of design features that may hinder anomaly detection.
5185 Poorly designed lines of defense for defense in depth have been found to conceal emerging
5186 dangerous system states and conditions, especially from human observers [Saleh14]. The
5187 system design must minimize the difference between estimated system states and conditions
5188 and actual system states and conditions.

5189 There are two approaches to anomaly detection:

- 5190 • **Self-Anomaly Detection:** An entity has no dependency on another entity to detect an
5191 anomaly within the scope of its intended design. Self-anomaly detection usually involves an
5192 axiomatic or environmentally enforced assumption about its integrity. Typically, trusted
5193 elements have the capability for self-anomaly detection. This means that at the highest level
5194 of trustworthiness, an entity must be able to assess its internal state and functionality to a
5195 meaningful extent at various stages of execution. The detected anomalies must correlate to
5196 the trustworthiness assumptions placed on the entity.
- 5197 • **Dependent Anomaly Detection:** An entity-of-interest is dependent on another entity for
5198 some or all anomalies that are detected. When an entity-of-interest relies on another entity
5199 for any portion of the assessment, that entity must be at least as trustworthy as the entity-
5200 of-interest.

5201 **REFERENCES:** [Schroeder77]; [Smith12]; [Saleh14].

“System and component behaviors are monitored for anomalous operation. Adversaries innovate new attack methods to evade known-pattern detection screening. System and component behavior outside of normal expectations is a method-agnostic telltale.”

-- An Objective of the Security in the Future of Systems Engineering [FUSE21]

5202

5203 E.2.2 Commensurate Protection

5204 **PRINCIPLE:** *The strength and type of protection provided to a system element is commensurate*
5205 *with the most significant adverse effect that results from a failure of that element.*

5206 *Note:* The strength and effectiveness of the protection for a system element must be
5207 proportional to the need. As the need increases, the protection of that element should also
5208 increase to the same degree. Need is derived from the most significant adverse effect associated
5209 with the system element or the trust that is placed in the element. The protection can come in
5210 the form of the system element’s own self-protection, from protections provided by the system
5211 architecture, or from protection provided by other elements. The needed strength of protection
5212 is independent of these design choices (or others, such as distributed versus centralized design),
5213 a concept sometimes referred to as *secure distributed composition* [Neumann04]. Furthermore,
5214 confidence in the effectiveness of the protections provided to a system element should also
5215 increase commensurate to the need. This is addressed by the principle of *Commensurate Rigor*.

5216 **REFERENCES:** [Neumann04]; [Levin07].

5217 **E.2.3 Commensurate Response**

5218 **PRINCIPLE:** *The system design matches the aggressiveness of an engineered response action's*
5219 *effect to the needed immediacy to control the effects of each loss scenario.*

5220 *Note:* The selected response to a detected anomaly should consider three factors to determine
5221 the effect that the response has on the loss and the system:

- 5222 • The expected effectiveness and aggressiveness of the response to directly address the
5223 anomaly and to prevent or limit the loss
- 5224 • The direct, residual, or side-effect of the response on the system
- 5225 • The opportunities that remain to take some other response action should the selected
5226 response fail to achieve the intended result

5227 The response can be achieved by any combination of *fully manual, semi-automated, fully*
5228 *automated, or autonomous* means. However, the response action is distinct from the
5229 determination that a response is necessary and from the notification or signaling that invokes
5230 the response action.

5231 A commensurate response requires consideration of the *response-effect-consequence*
5232 relationship associated with a specific loss. Ideally, for any given need for a response, a single
5233 action taken will be effective to resolve the loss concern and will have no associated adverse
5234 effect. Practically, due to complexity and the limits of certainty, the response action may not
5235 have the desired effect, may compound the problem, or may cause another problem. The
5236 balance required is one that determines if, when, and how a response action should be taken to
5237 be initially more aggressive or initially less aggressive. The severity of the problem and the time
5238 available for an effective response typically dictates a strategy for a continuum of responses,
5239 characterized by two extremes:

- 5240 • **Graduated Response:** A graduated response is initially the least aggressive or impactful
5241 action possible to prevent the loss from continuing or escalating and does so with
5242 consideration of the possible side effects associated with the response action. The
5243 graduated response allows for taking increasingly more aggressive action should the loss
5244 situation persist or escalate.
- 5245 • **Ungraduated Response:** An ungraduated response is the most aggressive and most
5246 impactful action possible to prevent the loss from continuing or escalating and does so
5247 without consideration of the possible side effects associated with the response action. The
5248 ungraduated response recognizes the severity of the loss as justifying the most aggressive
5249 action, even if that option provides no alternatives should it fail to have the intended or
5250 desired effect or if it causes other losses to occur.

5251 Without early observability of possible loss, the option for a graduated response may not exist.
5252 Commensurate response is aided by early detection, which in turn increases the options for a
5253 graduated response.

5254 **REFERENCES:** [[Saleh14](#)].

5255 **E.2.4 Continuous Protection**

5256 **PRINCIPLE:** *The protection provided for a system element must be effective and uninterrupted*
5257 *during the time that the protection is required.*

5258 *Note:* The protection capability must be uninterrupted across all relevant system states, modes,
 5259 and transitions for there to be assurance that the system can be effective in delivering the
 5260 required capability while controlling loss. Continuous protection requires adherence to the
 5261 following principles:

- 5262 • **Trustworthy System Control:** Every controlled action is constrained by the mechanism, and
 5263 the mechanism is able to protect itself from tampering. Sufficient assurance of the
 5264 correctness and completeness of the mechanism can be ascertained from analysis and
 5265 testing.
- 5266 • **Protective Failure and Protective Recovery:** A protective state is preserved during error,
 5267 fault, failure, and successful attack, as well as during the recovery of assets or of recovery to
 5268 normal, degraded, or alternative operational modes.

5269 Continuous protection applies to all configurations, states, and modes of the system, as well as
 5270 the transitions between those configurations, states, and modes. The system design must
 5271 ensure that protections are coordinated and composed in a non-conflicting and mutually
 5272 supportive manner across the non-behavioral aspects of the system structure and the
 5273 behavioral aspects of system function and data flow.

5274 While the design for continuous protection applies for the entire time that the protection is
 5275 required, there may be cases where, by design, protection capability is intentionally disabled
 5276 (e.g., Battleshort⁸⁹ intentional override). The intentional disabling/override of protection is an
 5277 exception case and, therefore, does not violate this principle. That is, the principle of [Continuous](#)
 5278 [Protection](#) applies only for the entirety of time that the protection is required and not knowingly
 5279 and intentionally disabled.⁹⁰

5280 **REFERENCES:** [[Levin07](#)].

5281 **E.2.5 Defense In Depth**

5282 **PRINCIPLE:** *Loss is prevented or minimized by employing multiple coordinated mechanisms.*

5283 *Note:* The coordinated deployment of multiple protective mechanisms for a system helps to
 5284 avoid single points of failure. The principle of defense in depth has several pillars:

- 5285 • Multiple lines of defenses or barriers should be placed along loss scenario sequences.
- 5286 • Loss control should not rely on a single defensive element.
- 5287 • The successive barriers should be diverse in nature and include technical, operational, and
 5288 organizational barriers.

5289 Defense in depth requires the employment of coordinated mechanisms (active) within an
 5290 architectural structure (passive) that achieves the *depth* characteristic.⁹¹ Ideally, the initial lines
 5291 of defense prevent loss, while subsequent lines of defense block loss scenario escalation and/or

⁸⁹ Battleshort is a switch used to bypass normal interlocks in mission-critical equipment (e.g., equipment that must not be shut down or the mission function will fail) during battle conditions [[DOD 2007](#)].

⁹⁰ However, the inclusion of a capability for intentionally disabling/overriding protection requires additional control features and devices and associated analysis for the enforcement of constraints to prevent the inadvertent actuation of the override capability.

⁹¹ While the elaboration is limited to the machine, defense in depth may involve the combination of technical, operational, and organizational elements.

5292 contain loss and potential consequences when needed. A defense-in-depth strategy examines
5293 loss scenarios for those points of opportunity to prevent or contain loss. It also leverages the
5294 opportunities to use active or passive mechanisms or constraints to meet loss control objectives.

5295 The coordination of the multiple defense-in-depth mechanisms (i.e., combinations of structural,
5296 data, and control flow coordination) in conjunction with other design principles (e.g., [Anomaly](#)
5297 [Detection](#), [Commensurate Response](#)) reflects a design strategy to satisfy the loss control
5298 objectives.

5299 While defense in depth distributes the protection capability to many components, a defense-in-
5300 depth strategy may also consider a distributed composition to a line of defense. A protection
5301 capability provided by a single system component is a potential single point of failure or
5302 bottleneck to system performance. It may also raise other concerns. A distributed composition
5303 of a defense layer may provide additional options within the coordination of layers.

5304 Defense in depth is, in part, a form of the principle of [Protective Failure](#). It helps satisfy the
5305 objective that a failure of a system element should not result in an unacceptable loss. However,
5306 it does not satisfy the objective that a failure of a system element should not invoke another
5307 loss scenario.

5308 **REFERENCES:** [[Neumann04](#)]; [[Levin07](#)]; [[Jackson13](#)]; [[Saleh14](#)].

5309 **E.2.6 Distributed Privilege**

5310 **PRINCIPLE:** *Multiple authorized entities act in a coordinated manner before an operation on the*
5311 *system is allowed to occur.*

5312 *Note:* Distributed privilege⁹² is a means to prevent a single authorized entity from performing an
5313 erroneous action, whether or not that action is performed with intent. Distributed privilege
5314 requires that an erroneous action can only be performed if multiple entities agree to do so, for
5315 either legitimate (e.g., override of the protection in extreme cases) or illegitimate purposes (e.g.,
5316 collusion to intentionally take improper action). In the case of an attack on an operation,
5317 distributed privilege forces the adversary to target all of the entities to whom privilege is
5318 distributed.

5319 Distributed privilege separates, divides, or in some other manner distributes the privileges
5320 required to perform an operation among multiple entities. The distribution of privilege includes
5321 a set of rules, conditions, and constraints that describe how multiple entities must interact
5322 through positive actions before a requested operation can proceed and be completed. The
5323 rules, conditions, and constraints may reflect combinations of the following, all of which require
5324 that multiple conditions be met for the operation to proceed:

- 5325 • **Simultaneous Actions:** Multiple different authorized entities execute a command within a
5326 specified time window.
- 5327 • **Sequenced Actions:** Multiple different entities interact within a linear sequence of actions
5328 where each successive action is enabled only by the successful completion of a prior action.
- 5329 • **Parallel Actions:** Multiple entities execute sequences concurrently, and success is achieved
5330 either by a consensus of the results of each concurrent action or by voting among the
5331 participants.

⁹² [[Saltzer75](#)] originally named this the *separation of privilege*. It is also equivalent to separation of duty.

5332 **REFERENCES:** [\[Saltzer75\]](#); [\[Levin07\]](#).

5333 **E.2.7 Diversity (Dynamicity)**

5334 **PRINCIPLE:** *The system design delivers the required capability through structural, behavioral, or*
5335 *data or control flow variation.*

5336 *Note:* A system design that incorporates diversity helps to avoid common mode failures and
5337 introduces unpredictability to adversaries, thus complicating the planning and execution of
5338 where, when, and how to target their attacks. While the system behaviors that result from a
5339 design may be unpredictable from the viewpoint of the adversary, the design itself must be
5340 predictable and verifiable in achieving only the intended outcomes. The options for diversity
5341 include variety in the system structural and architectural design elements, the system functional
5342 and behavioral elements, the interfaces and interconnections between interfaces, the data and
5343 control flow, and the technology and component selection. Diversity can reside in:

- 5344 • *Fixed or static characteristics of the system* (e.g., multiple instances of a system element,
5345 multiple communication channels)
- 5346 • *Variable or dynamic characteristics of the system* (e.g., reconfiguration, relocation, refresh
5347 of system elements; random routing of data over different communication channels from
5348 source to destination; the ability to change aspects of the system behavior, structure, data,
5349 or configuration in a random but nonetheless verifiable manner)

5350 Any design approach that includes diversity in structure, configuration, communications,
5351 protocols, and similar or dissimilar system elements (e.g., N-version, heterogeneity) increases
5352 uncertainty due to the increased complexity of the design and the behaviors and outcomes that
5353 stem from emergent effects, side-effects, and feature interaction. This drives the need for
5354 confidence that the design approach will deliver only the authorized and intended functional
5355 behavior, produce only the authorized and intended outcomes, and do so in a manner that
5356 allows for control over side-effects, emergence, and feature interaction.

5357 Diversity options include intentionally designed regular or irregular changes in the system (e.g.,
5358 implementing the concept of dynamicity).⁹³ This results in unpredictability and uncertainty to
5359 adversaries – complicating their attack planning – and can provide required performance
5360 despite other adversity. Dynamic change may refer to either shifting the target or shifting the
5361 behaviors of a target in performing its activities.

5362 The uncertainty and diminished predictability associated with the employment of diversity and
5363 dynamicity in design can be problematic where it impedes or prevents having confidence that
5364 the system will function and produce outcomes only as authorized and intended. It is important
5365 to differentiate where the uncertainty lies: (1) uncertainty in how the system achieves an end
5366 objective (i.e., the means to an end) or (2) uncertainty that an objective will be achieved (i.e.,
5367 achieving the end). A design that employs diversity and dynamicity must be based on acquiring
5368 confidence that the system will produce only the desired results despite uncertainty in knowing

⁹³ A design incorporating *dynamicity* can serve many purposes: (1) it complicates the attack planning of an adversary, (2) it reduces the potential for non-adversarial adversity to have an effect on the system, (3) it provides the capability and margin to deliver a required capability while reducing actual losses, and (4) it protects against the effects of an attack. An example of dynamicity is frequency hopping with wireless communications, which complicates the interception and jamming of signals.

5369 exactly how the desired results are achieved. This constitutes a design trade that is specific to
5370 diversity- and dynamicity-based designs. Diversity may have a cost (e.g., hardware, software,
5371 maintenance, training, assurance) greater than the value or effectiveness that it provides.

5372 **REFERENCES:** [[Schroeder77](#)]; [[Jackson13](#)]; [[Moller08](#)].

5373 **E.2.8 Domain Separation**

5374 **PRINCIPLE:** *Domains with distinctly different protection needs are physically or logically*
5375 *separated.*

5376 *Note:* The separation of domains enables enhanced control and, therefore, protection of system
5377 function and the flow of data. Control relative to separated domains limits the extent to which
5378 an entity or domain is influenced by or is able to influence some other entity or domain, thereby
5379 enhancing the protection of a domain. This is achieved through the control of information flow
5380 and data between domains as well as control over the use of a system capability between
5381 domains.

5382 The differing protection needs that are used to define domains may be thought of in terms of
5383 protecting the domain from influence by external entities (i.e., susceptibility) and protecting
5384 external entities from erroneous behavior that occurs within the domain (i.e., containment).
5385 This distinction may include separating critical functions from less critical functions, such as
5386 separating the flight control functions of a transport aircraft from the environmental control
5387 functions that maintain a safe environment for the cargo and passengers being transported.

5388 Historically, domain separation has been used to enforce the separation of roles or privileges
5389 (i.e., least privilege). For example, a system may separate an “administrative” or “supervisor”
5390 domain from “user” domains. The administrative domain is accessible only by system
5391 administrators with appropriate privileges, and distinctly administrative functions may only be
5392 executed by administrators from the administrative domain. Similarly, data intended to only be
5393 accessed by administrators and administrative functions (e.g., system configurations) is stored
5394 and accessed only within that domain, ensuring needed protection of the data.

5395 Domain separation requires a domain to be contained within its own protected subsystem so
5396 that elements of the domain are only directly accessible by procedures or functions of the
5397 protected subsystem. The concept of isolation enables the implementation of domain
5398 separation. Isolation limits the extent to which one domain can influence or can be influenced
5399 by other entities. The challenge is that the system elements within domains must at times
5400 interact with other elements and the environment to deliver a capability. Every interface that
5401 results from design decisions can diminish domain separation while achieving requirements for
5402 a system capability. External requests for resources or functions within protected subsystems
5403 are arbitrated at these interfaces. Firewall, data diodes, and cross-domain solutions (CDS) are
5404 examples of mechanisms that enable varying degrees of control over the interactions between
5405 separated domains.

5406 Encryption is another mechanism often used to provide domain separation. For example,
5407 communication between distinct subsystems within a domain may be encrypted with a key that
5408 is known only to the subsystems within the domain. Where a common storage module or
5409 subsystem is used for multiple domains, encryption may be used to limit information access to
5410 the domain that owns the key to decrypt.

5411 **REFERENCES:** [[Smith12](#)]; [[Levin07](#)].

5412 E.2.9 Least Functionality

5413 **PRINCIPLE:** *Each system element has the capability to accomplish its required functions but no*
5414 *more.*

5415 *Note:* Susceptibility and vulnerability increase unnecessarily when a system element provides
5416 more functionality than is needed to achieve its intended purpose. Least functionality reduces
5417 the potential for susceptibility and vulnerability and also reduces the scope of analysis of the
5418 system element’s trustworthiness and loss potential. The strictest interpretation of least
5419 functionality is to prohibit any system element functions that are not required. Where that is
5420 not possible or practical, the unnecessary functions of the system element should be disabled,
5421 disarmed, or put into a “safe” mode that prevents the functions from being used. In all other
5422 cases, mediated access can be used to prevent access to and use of the unneeded functions. An
5423 example of when it may not be possible or practical to avoid unnecessary functions is the use of
5424 commercial off-the-shelf (COTS) components. COTS components typically contain functions
5425 beyond those required to fulfill its intended purpose. In such cases, the components should be
5426 configured to enable only the functions that are required to fulfill its purpose and prohibit or
5427 restrict functions that are not required to fulfill its purpose.

5428 **REFERENCES:** [[Neumann04](#)]; [[Levin07](#)].

5429 E.2.10 Least Persistence

5430 **PRINCIPLE:** *System elements and other resources are available, accessible, and able to fulfill their*
5431 *design intent only for the time for which they are needed.*

5432 *Note:* Least persistence reduces susceptibility. It limits the extent to which functions, resources,
5433 data, and information remain present, accessible, and usable when not required, thereby
5434 reducing the opportunity for their inadvertent or unauthorized use, modification, or activation.
5435 The broadest interpretation of least persistence is to not install, instantiate, or apply power to
5436 system elements and resources until needed and to completely remove system elements or
5437 power from elements and resources when they are no longer required. Where that condition is
5438 not possible or practical, those system elements and resources should be fully disabled,
5439 disarmed, or put into safe mode to prevent their ability to function or to be used. At a minimum,
5440 [Mediated Access](#) should include constraints on the time and duration of their use.

5441 Three conditions must be satisfied for an active system element or resource to be usable, with
5442 two of these conditions applying to non-active elements or resources:

- 5443 • **Presence (active and non-active):** The system element or resource must be installed,
5444 loaded, residing in memory (software), and configured.
- 5445 • **Accessible (active and non-active):** The system element or resource can be invoked,
5446 interacted with, or operated on.
- 5447 • **Able to Function (active):** The system element or resource must be able to execute (i.e.,
5448 powered on, enabled, or armed) to deliver a service or perform a function.

5449 Least persistence is reflected in concepts such as sanitizing, erasing, clearing memory and
5450 storage locations; disabling, removing, and disconnecting network ports, system interfaces, and
5451 the services provided by system interfaces; powering off and unplugging hardware when not
5452 needed; and instantiating software just before needed and de-instantiating after it is no longer
5453 needed. Least persistence has added benefits that include simplifying the processes of:

- 5454 • Cleansing the system element to remove corrupted aspects or side effects
- 5455 • Re-establishing the system element to a known state (i.e., a refresh)
- 5456 • Minimizing the period of time in which system elements are exposed to the environment, to
5457 attack, and to erroneous behavior

5458 Where system elements or resources are removed and then restored as needed, there must be
5459 a trusted representation of the system element and a trusted ability to instantiate that system
5460 element within the time constraints for its use.

5461 **REFERENCES:** [[SP 800-160v2](#)].

5462 **E.2.11 Least Privilege**

5463 **PRINCIPLE:** *Each system element is allocated privileges that are necessary to accomplish its*
5464 *specified functions but no more.*

5465 *Note:* System elements can be implemented by entities such as hardware, firmware, software,
5466 and personnel. By design, the system must be able to limit the scope of a system element's
5467 actions. This has two desirable effects: (1) the impact of a failure, corruption, or misuse of the
5468 element is minimized, and (2) the analysis of the system element is simplified. A design driven
5469 by least privilege considerations results in a sufficiently fine granularity of privilege
5470 decomposition and the ability for the fine-grained allocation of privileges to human and machine
5471 elements. The application of the principle of least privilege means allocating the minimum
5472 (separate) privileges necessary to a system element according to the extent to which that
5473 element has a need to perform some function. This could include a need know, modify, delete,
5474 use, configure, authorize, start/enable, or stop/disable [[Schroeder77](#)]. In addition to its
5475 manifestations at the system interface, least privilege can also be used as a guide for the
5476 internal structure of the system itself, such as how to employ [Domain Separation](#). One aspect of
5477 internal least privilege is to construct modules so that only the system elements encapsulated
5478 by the module are directly accessed or operated upon by the functions within the module.
5479 Elements external to a module that may be affected by the module's operation are indirectly
5480 accessed through interaction with the module that contains those elements.

5481 **REFERENCES:** [[Neumann04](#)]; [[Levin07](#)]; [[Saltzer75](#)]; [[Scroeder77](#)].

5482 **E.2.12 Least Sharing⁹⁴**

5483 **PRINCIPLE:** *System resources are shared among system elements only when necessary and*
5484 *among as few elements as possible.*

5485 *Note:* Sharing via common mechanism and other means can increase the susceptibility of
5486 system resources (e.g., data, information, system variables, interfaces, functions, services) to
5487 unauthorized access, disclosure, use, or modification and can adversely affect the capabilities
5488 provided by the system. According to [[Saltzer75](#)], "Every shared mechanism (especially one
5489 involving shared variables) represents a potential information path between users and must be
5490 designed with great care to be sure it does not unintentionally compromise security." A design

⁹⁴ The historically well-known security design principle, *least common mechanism*, is an instance of least sharing. The principle of least common mechanism is described in [[Popek74](#)].

5491 that employs least sharing helps to reduce the adverse consequences that can result from
5492 sharing system functions, state, resources, and variables among different system elements. A
5493 system element that corrupts a shared state or shared variables has the potential to corrupt
5494 other elements whose behavior is dependent on the state. Minimized sharing also helps to
5495 simplify the design and implementation [[Lampson73](#)].

5496 There are two criteria that provide the basis for the application of the principle of least sharing:
5497 (1) share only if absolutely necessary, and (2) minimize sharing if allowed. The first criterion is a
5498 trade decision that factors in the cost and benefit of sharing resources against the increased
5499 exposure that results from the sharing. The second criterion is a constraint on the extent of
5500 sharing.

5501 **REFERENCES:** [[Popek74](#)]; [[Saltzer75](#)]; [[Lampson73](#)]; [[Neumann04](#)] [[Levin07](#)].

5502 **E.2.13 Loss Margins**

5503 **PRINCIPLE:** *The system is designed to operate in a state space sufficiently distanced below the*
5504 *threshold at which loss occurs.*

5505 *Note:* Margins refer to the difference between a conservative threshold at which the system is
5506 expected to operate while subjected to adversity and the point at which the adversity results in
5507 failure. Loss margins are created by engineered features put in place to maintain operational
5508 conditions and the associated adversity level at some distance (i.e., conservative threshold)
5509 from the estimated critical adversity threshold or loss-triggering threshold. Loss margins also
5510 allow for increased time to detect the need for a response action (see [Anomaly Detection](#)), to
5511 determine what the response action should be (see [Commensurate Response](#)), and to complete
5512 the selected response action. When there is uncertainty about the effectiveness of the response
5513 action, loss margins need to allow time to evaluate response effectiveness, determine any
5514 additional actions needed, and complete any selected actions.

5515 Uncertainty may derive from the environment of operation, the design and realization of the
5516 system, the utilization and sustainment of the system, and the adversity presenting itself to the
5517 system. Loss margins are effective in addressing uncertainty about how and when a loss-
5518 triggering event occurs. Specifically, loss margins are effective in addressing uncertainty
5519 associated with:

- 5520 • Intelligently designed and executed attacks, including attacks that persist and evolve over
5521 time
- 5522 • Unknown, unquantified, and underappreciated susceptibilities, threats, hazards,
5523 vulnerabilities, and associated risks

5524 For designs that incorporate loss margins, uncertainty about adversity makes determining the
5525 loss-triggering thresholds difficult. Loss margins for design should be determined with a balance
5526 between certainty (i.e., what has happened and can happen again) and uncertainty (i.e., what
5527 has not happened but can happen, or what has happened but can also happen in a different
5528 way). Loss scenarios that include loss escalation and an estimation of the critical threshold for
5529 loss occurrence are helpful in making design decisions that incorporate loss margins. Loss
5530 scenarios also help to determine the limits of adversity-driven decisions due to uncertainty in
5531 knowledge about the adversity (i.e., the adversity is insufficiently known or understood or is just
5532 unknown).

5533 Sensitivity analyses must inform the determination of loss margins. Other factors for computing
5534 loss margins include system complexity, the use of newer technology or older technology in new
5535 ways, and the degree of new environments being introduced. An additional factor is the ability
5536 to complete comprehensive and effective testing. Limitations on system test coverage and
5537 effectiveness for all actual, simulated, or emulated adversity necessitate larger margins to
5538 account for the remaining uncertainty. The size of the margin may be reduced with time as
5539 unknown and underappreciated loss scenarios are uncovered and corrected, or the size may
5540 need to be increased over time as a malicious adversity capability matures in sophistication.

5541 **REFERENCES:** [[Saleh14](#)]; [[Moller08](#)]; [[NASA11](#)]; [[NASA14](#)]; [[Benjamin14](#)]; [[Pagani04](#)].

5542 **E.2.14 Mediated Access**

5543 **PRINCIPLE:** *All access to and operations on system elements are mediated.*

5544 *Note:* Mediated access is a foundational principle in the design of secure systems. The purpose
5545 of mediated access is to achieve the following:

- 5546 • Place limits on access to and use of the system
- 5547 • Reduce the possibility of loss escalation
- 5548 • Reduce the extent to which loss escalates and propagates

5549 Mediated access is based on the interaction between an entity and a target system element and
5550 has two aspects:

- 5551 • **Access to the System Element:** The requesting entity only has authorized access to a target
5552 system element.
- 5553 • **Use of the System Element:** The requesting entity is only allowed to perform authorized
5554 operations on the target system element.

5555 Mediated access has two parts: (1) a policy-based access mediation decision and (2) the
5556 enforcement of the access mediation decision. The access mediation decision may include
5557 conditional constraints that further restrict access (e.g., role, time of day, system state or mode,
5558 or duration of operation). If access is not sufficiently mediated, there is no possibility of limiting
5559 how system elements (including human and machine elements) interact to ensure that only
5560 authorized behaviors and intended outcomes result.

5561 Mediated access is achieved by an access mediation control mechanism. Seminal computer
5562 security work defined the *reference validation mechanism* as the generalized form of any
5563 mechanism that is an implementation of the reference monitor concept ([Section D.4.2](#)). The
5564 reference monitor provides the design assurance basis for demonstrating the trustworthiness of
5565 a mediated access control mechanism. The essential design criteria ([Section D.4.2](#)) provide a
5566 refinement to extend the generalized reference monitor concept. Mediated access may enforce
5567 the constraints described in the principles of [Distributed Privilege](#), [Least Privilege](#), and [Least](#)
5568 [Sharing](#).

5569 Efficiently mediated access refers to using a *least common mechanism* for mediating access.
5570 Mediating access is often the predominant security function within a secure system and may
5571 result in performance bottle necks if not designed and implemented correctly. The use of least
5572 common mechanism is one means to help reduce bottle necks [[Levin07](#)].

5573 **REFERENCES:** [[Saltzer75](#)]; [[Neumann04](#)]; [[Levin07](#)]; [[Neumann17](#)]; [[Anderson72](#)]; [[Saleh14](#)].

5574 E.2.15 Minimize Detectability

5575 **PRINCIPLE:** *The design of the system minimizes the detectability of the system as much as*
5576 *practicable.*

5577 *Note:* A system that is not discoverable, observable, or trackable by an adversarial threat or
5578 exposed to such a threat is less prone to a targeted attack. Minimizing detectability drives
5579 engineering design decisions to eliminate or reduce exposures such as unnecessary interfaces,
5580 access points, footprints, and emanations, thereby reducing susceptibility to adversarial threat
5581 actions. Interfaces and access points have the effect of exposing the system to intentional
5582 adversity (i.e., attacks) and non-intentional adversity (i.e., faults, errors, incidents, accidents).
5583 Yet interfaces and access points are necessary to compose system elements to deliver required
5584 capabilities, and some duplication of interfaces and access points is needed to avoid single
5585 points of failure. System design must balance the need for interfaces with the susceptibility that
5586 results from the interface being exposed, discovered, and observed. Every interface, whether
5587 internal or external, constitutes an exposure that must be considered.

5588 Minimizing detectability reduces the ability of an adversary to observe and discover information
5589 about the system to craft and execute attacks. This includes detection of a system's location,
5590 presence, and movement (e.g., due to emissions, signatures, or footprints). There are various
5591 ways that a system may be detectable, including heat emission, electronic magnetic (EM)
5592 emissions, sound, vibrations, reflecting radar waves or light, or the response to stimulus (e.g., a
5593 response to an Internet Control Message Protocol [ICMP] echo request or "ping"). There are
5594 specific forms or means to minimize detectability, including camouflage, stealth, low probability
5595 of intercept/low probability of detect (LPI/LPD) waveforms (for radios), and frequency hopping.

5596 **REFERENCES:** [[Bryant20](#)]; [[Ball03](#)]; [[SP 800-160v2](#)].

5597 E.2.16 Protective Defaults

5598 **PRINCIPLE:** *The default configuration of the system provides maximum protection effectiveness.*

5599 *Note:* The configuration of the system includes the parameters for system functions, data,
5600 interfaces, and resources that determine how the system behaves and the outcomes it
5601 produces. Protective defaults guarantee that the "as shipped" system configuration and
5602 parameters prioritize the achievement of loss control objectives over the ability to deliver a
5603 required system capability and performance without dependence on human intervention.
5604 Protective defaults require conscientious action to establish the system configuration and
5605 parameters that deliver the required capability and performance in a manner that provides
5606 [Commensurate Protection](#) against loss. Protective default configurations for systems include
5607 constituent subsystems, components, and mechanisms. The principles of Protective Failure,
5608 Protective Recovery, and Continuous Protection parallel this principle to provide the ability to
5609 detect and recover from failure.

5610 **REFERENCES:** [[Saltzer75](#)]; [[Neumann04](#)]; [[Levin07](#)].

5611 E.2.17 Protective Failure

5612 **PRINCIPLE:** *A failure of a system element neither results in an unacceptable loss nor invokes*
5613 *another loss scenario.*

5614 *Note:* Protective failure is the aspect of continuous protection that ensures that a protection
 5615 capability is not interrupted during a failure and that the effect of the failure is constrained. Two
 5616 aspects of protective failure must be satisfied to achieve the intended effect:

- 5617 • **Avoid Single Points of Failure:** The failure of a single system element should not lead to
 5618 unacceptable loss. Unacceptable loss should only occur in the case of multiple independent
 5619 malfunctions – a safety principle known as *single failure criterion*. The principle of [Defense in](#)
 5620 [Depth](#) can help achieve this aspect of protective failure.
- 5621 • **Avoid Propagation of New Failure:** If unmitigated, failures in the system can result in
 5622 propagating, cascading, or rippling effects on the system. These effects can be addressed if
 5623 the remaining protections remain effective to prevent the originating failure from causing
 5624 additional failures. The principle of [Defense in Depth](#) does not address the propagation of
 5625 failure by invoking a new loss scenario and, therefore, does not help achieve this aspect of
 5626 protective failure without additional analysis.

5627 Protective failure applies to discrete system elements, aggregates of system elements, and the
 5628 systems abstraction. Protective failure seeks to limit the effect of a failure to the extent
 5629 practicable and, in doing so, minimize the introduction of new loss possibilities. Protective
 5630 failure is able to limit the extent to which a failure is able to advance loss scenarios associated
 5631 with the failure, including cascading losses; trigger a different loss scenario; or create a new loss
 5632 scenario. Efforts to avoid or limit failures may themselves degrade system performance, a form
 5633 of failure. Thus, system designers may need to consider trade spaces between possible adverse
 5634 effects and system performance.

5635 **REFERENCES:** [[Neumann04](#)]; [[Jackson13](#)]; [[Saleh14](#)]; [[Moller08](#)]; [[Levin07](#)].

5636 **E.2.18 Protective Recovery**

5637 **PRINCIPLE:** *The recovery of a system element does not result in nor lead to unacceptable loss.*

5638 *Note:* Protective recovery is an aspect of [Continuous Protection](#) that ensures that a protection
 5639 capability is not interrupted during recovery from actual or impending failure. Protective
 5640 recovery is applied to discrete system elements, aggregates of system elements, and the
 5641 system. To the extent practicable, any recovery from impending or actual failure to resume
 5642 normal, degraded, contingency or alternative operation, or the recovery of other asset losses
 5643 should not (1) advance the loss scenario that is the target of the recovery, (2) trigger other loss
 5644 scenarios, or (3) create new loss scenarios. The practicable aspect of this principle recognizes
 5645 that for some recovery efforts to be successful, they may degrade system performance, which is
 5646 a form of loss. Protective recovery is an aspect of the response strategy for the system. Thus,
 5647 graduated and ungraduated considerations of [Commensurate Response](#) apply to best suit
 5648 expediency in the need for a protective recovery.

5649 **REFERENCES:** [[Schroeder77](#)]; [[Neumann04](#)]; [[NASA11](#)]; [[Levin07](#)].

5650 **E.2.19 Redundancy**

5651 **PRINCIPLE:** *The system design delivers the required capability by the replication of system*
 5652 *functions or elements.*

5653 *Note:* Redundancy employs multiples of the same system elements, data and control flows, or
 5654 paths to avoid single points of failure. Redundancy requires a strategy for how multiple system
 5655 elements are used individually or in combination (e.g., load-balancing, fail-over, concurrently,

5656 backup, voting, agreement, consensus). Redundant solutions are susceptible to common mode
5657 failure (i.e., a single event that results in the same or equivalent elements failing in the same
5658 manner). The cause of the failure may occur with or without intent. *Diversity* is a means to
5659 address the concerns of common mode failure.

5660 **REFERENCES:** [[Schroeder77](#)]; [[Neumann04](#)]; [[Jackson13](#)]; [[Moller08](#)].

5661
5662

APPLICATION OF DESIGN PRINCIPLES TO COMMERCIAL PRODUCTS

For commercial products to be trustworthy commensurate with their criticality, security design principles should be selected and applied appropriately throughout the products' system life cycle. Each design principle must be assessed for its relevance, applicability, and validity. The security design principles described in this appendix have been demonstrated by industry in past work and have previously been codified into national and international standards and guidance documents, including the Department of Defense *Trusted Computer System Evaluation Criteria (TCSEC)* and ISO/IEC 15408, *Common Criteria for Information Technology Security Evaluation*.

Many commercial products have been designed, developed and evaluated against specifications from those standards and guidelines up to and including the highest levels of assurance (e.g., TCSEC Class A1 and Class B3). These products represent use cases of trustworthy components and systems that have been verified to be highly resistant to penetration from determined adversaries and, in the case of TCSEC Class A1, distinguished by substantially dealing with the problem of subversion of security mechanisms. To merit the trust of consumers, commercial products must demonstrate – in a manner that can be independently verified – that the security design principles articulated in this appendix have been applied to produce components and systems that are both sound and logically coherent with respect to security.

5663 APPENDIX F

5664 TRUSTWORTHINESS AND ASSURANCE

5665 REDUCING UNCERTAINTY AND BUILDING CONFIDENCE IN THE SYSTEM

5666 The determination that a system⁹⁵ is trustworthy is based on the concept of *assurance*.
 5667 Assurance is the grounds for *justified confidence* that a claim or set of claims has been or
 5668 will be achieved [[ISO 15026-1](#)]. Justified confidence is derived from objective evidence that
 5669 reduces uncertainty to an acceptable level and in doing so, reduces risk.⁹⁶ Evidence is acquired
 5670 through the application of rigorous engineering verification methods.⁹⁷ The evidence must be
 5671 relevant, accurate, credible, and of sufficient quantity to enable reasoned conclusions and
 5672 consensus among subject-matter experts that the claims are satisfied. The relationship between
 5673 evidence and claims can be represented in various ways. These approaches are discussed in
 5674 [Section F.2](#).

5675
5676
5677
5678 *“The trust we place in our digital infrastructure should be proportional to how trustworthy and
 5679 transparent that infrastructure is and to the consequences we will incur if that trust is misplaced.”*

5680 -- *Executive Order (EO) on Improving the Nation’s Cybersecurity* [[EO 14028](#)]
 5681 May 2021

5682
5683
5684
5685 F.1 TRUST AND TRUSTWORTHINESS

5686 The concepts of *trust* and *trustworthiness* are foundational to trustworthy secure design, the
 5687 decisions made to grant trust, and the extent to which trust is granted based on *demonstrated*
 5688 trustworthiness. Trust is a belief that an entity meets certain expectations, and therefore, can
 5689 be relied upon. The terms *belief* and *can* imply that trust may be granted to an entity whether
 5690 the entity is trustworthy or not. A trustworthy entity is one for which sufficient evidence exists
 5691 to support its claimed trustworthiness. Thus, trustworthiness is the demonstrated ability and,
 5692 therefore, worthiness of an entity to be trusted to satisfy expectations. Trustworthiness, being
 5693 something demonstrated, is based on evidence that supports a claim or judgment of an entity
 5694 being worthy to be trusted [[Schroeder77](#)] [[Neumann04](#)] [[Levin07](#)].

5695 Trust in an entity can occur without a basis for or knowledge of the entity’s trustworthiness.
 5696 Trust may occur because: (1) there is no alternative (e.g., an individual trusts the components
 5697 involved in an Internet transaction without knowing anything about the components), (2) the
 5698 need for trustworthiness is not realized and occurs de facto, or (3) other reasons [[Neumann17](#)].

⁹⁵ As discussed in [Chapter Two](#), a *system of interest* can be a system, sub-system, component, system of systems, network, as well as an infrastructure.

⁹⁶ [Section F.2](#) describes the relationship between uncertainty and risk.

⁹⁷ Verification methods include demonstration, inspection, analysis, and testing. These verification methods support decision-making throughout the system life cycle, including decisions for major reviews and for system acceptance, approval, or authorization. Additionally, there are other types of validation activities, such as the validation of requirements prior to their incorporation into a configuration-controlled requirements baseline.

5699 Since trust is not necessarily based on a judgment of trustworthiness, the decision to trust an
5700 entity should consider the consequences, effects, and impacts of trust *expectations* not being
5701 fulfilled because of non-performance, whether due to failure, deficiency, or incompetence.
5702 Ideally, the criteria to grant trust is used to determine the trustworthiness of an entity. Trust
5703 that is granted without establishing the required trustworthiness is a significant contributor to
5704 risk.

5705 **F.1.1 Roles of Requirements in Trustworthiness**

5706 Trustworthiness judgments are based on criteria that express the need to trust. This need must
5707 be transformed into requirements in the same way that capability, performance, security, and
5708 other needs are transformed into requirements. The trustworthiness judgments are meaningful
5709 only to the extent that the trustworthiness-relevant requirements accurately reflect the
5710 problem, accurately define the solution, and can be verified as being satisfied by the solution.
5711 Trustworthiness requirements about security derive from the protection needs, priorities,
5712 constraints, and concerns associated with the ability of the system to achieve authorized and
5713 intended behaviors and outcomes, deal with adversity, and control loss. The requirements also
5714 address the measures used to assess trustworthiness and the evidentiary data required to
5715 substantiate conclusions about trustworthiness and granting trust based on trustworthiness.
5716 The discipline of *requirements engineering* provides the methods, processes, techniques, and
5717 tools for this to occur.

5718

5719

5720

5721

5722

5723

5724

5725

5726

5727

5728

"A meaningful claim of trustworthiness cannot be based on an isolated demonstration that the system contains protection capability assumed to be effective or sufficient. Instead, conclusions about protection capability must have their basis on evidence that the system was properly specified, designed, and implemented with the rigor needed to deliver system-level function, in a manner deemed to be trustworthy and secure." [Neumann04]

5728 **F.1.2 Design Considerations**

5729 The design for a trustworthy secure system requires the rigorous application of principled
5730 engineering concepts and methods supported by evidence that provides assurance that all
5731 security-related claims about the system are satisfied ([Section F.2](#)).⁹⁸ There are several
5732 considerations that apply to achieving trustworthiness in system design:

5733 • **Composition**

5734 Trustworthiness judgments themselves are compositional. They must align with how the set
5735 of composed elements provides a system capability. The way the system is composed from
5736 its system elements must include the application of the design principle of [Compositional](#)
5737 [Trustworthiness](#) coupled with the principle of [Structured Decomposition and Composition](#) to
5738 the extent practical.

⁹⁸ Constraints and claims are expressed in terms of functional correctness, strength of function, concerns for asset loss and consequences, and the protection capability derived from adherence to standards or from the use of specific processes, procedures, or methods.

- 5739
- **States, Modes, and Transitions**
- 5740 Ideally, the implemented system design will result in a system that continually remains in
 5741 secure states and modes, with secure transitions between states and modes. Realistically,
 5742 the system will have insecure and indeterminant (unknown if secure or insecure) systems
 5743 states and modes. The design must account for these cases and provide the capability to
 5744 transition from insecure states and modes to secure states and modes (see [Protective](#)
 5745 [Recovery](#)). In short, the system design must account for behaviors and outcomes that
 5746 comprise secure, insecure, and indeterminant states, modes, and transitions.
- **Failure Propagation**
- 5747 All systems fail. When a failure occurs, it should not trigger or invoke some other failure
 5748 scenario or create a new failure scenario (see [Protective Failure](#)). Design without single
 5749 points of failures (see [Redundancy](#)), including not having common mode failures (see
 5750 [Diversity](#)), can isolate system element failures while providing required system capabilities.
 5751 Additionally, the response to failure should not lead to loss or other failures (see [Protective](#)
 5752 [Recovery](#)).
- **Anomaly Detection**
- 5753 [Anomaly Detection](#) provides situational awareness that allows the system to make decisions
 5754 and provide recommendations for corrective action to account for actual and potential
 5755 deviations from the accepted norms.
- **Trades**
- 5756 Not every system element may have trustworthiness that is sufficient for its intended
 5757 purpose. A deficiency in trustworthiness can result from:
- Technical feasibility and practicality issues
 - Cost and schedule issues of what is feasible and practical
 - Limits of certainty (i.e., what is not known, what cannot be known, and what is
 5758 underappreciated [known or could be known but dismissed prematurely])
- 5759 The *trade space* is the application of the combined set of trustworthiness and loss control
 5760 principles that provides a basis for making the necessary design decisions to maximize the
 5761 trustworthiness of individual system elements and the trustworthiness of aggregates of
 5762 elements that must be trusted. For example, in addressing the feasibility and practicality of
 5763 cost and schedule issues described above, the design principle of minimizing the number of
 5764 system elements that must be trusted (see [Minimized Trusted Elements](#)) is applied. This
 5765 reduces the size and scope of the effort, and potentially reduces the expense to generate
 5766 evidence of trustworthiness.

5773 F.2 ASSURANCE

5774 Assurance is the grounds for justified confidence that a claim or set of claims has been or will be
 5775 achieved [[ISO 15026-1](#)]. Assurance is a complex and multi-dimensional property of the system
 5776 that builds over time. Assurance must be planned, established, and maintained in alignment
 5777 with the system throughout the system life cycle.

5778 Judgments of adequate security should be based on the level of confidence in the ability of the
5779 system to protect itself against asset loss and the associated consequences across all forms of
5780 adversity.⁹⁹ It cannot be based solely on individual efforts, such as the demonstration of
5781 compliance, functional testing, or adversarial penetration tests. Judgments include what the
5782 system cannot do, will not do, or cannot be forced to do. These judgments of non-behavior must
5783 be grounded in sufficient confidence in the system’s ability to correctly deliver its intended
5784 function in the presence and absence of adversity and to do so when used in accordance with its
5785 design intent.

5786 The needed evidentiary basis for such judgments derives from well-formed and comprehensive
5787 evidence-producing activities that address the requirements, design, properties, capabilities,
5788 vulnerabilities, and effectiveness of security functions. Testing is one of several verification
5789 activities. The evidence acquired from these activities informs reasoning by qualified subject-
5790 matter experts to interpret the evidence to substantiate the assurance claims made while
5791 considering other emergent properties that the system may possess.

VENEER SECURITY

Veneer security is security functionality provided without corresponding assurance so that the functionality only **appears** to protect resources when, in fact, it does not. Veneer security results in a false sense of security and, in fact, increases risk due to the uncertainty about the behavior and outcomes produced by the security functionality in the presence and absence of adversity. Veneer security must be avoided [Saydjari18].

Compliance is a form of “veneer security.” While compliance may have an important *informing* role in judgments of trustworthiness, compliance-based judgments – like other forms of veneer security – do not suffice as the sole evidentiary basis for assurance and the associated judgments of trustworthiness.

5808 F.2.1 Security Assurance Claims

5809 From a security perspective, a top-level claim addresses freedom from the conditions that cause
5810 asset loss and the associated consequences by ensuring the system achieves only authorized
5811 and intended system behaviors and outcomes. Supporting claims include the completeness and
5812 accuracy of stakeholder and system requirements, a sound approach to design, the proper
5813 implementation of the design, and the proper use and maintenance of the system.

5814 When applied to security, the top-level claim is that the *system* will adequately contribute to
5815 freedom from the conditions that cause asset loss and the associated consequences. The top-
5816 level security claim decomposes into claims about the design, implementation, requirements,
5817 methods, and adversities in a structured manner that demonstrates that the design adequately
5818 contributes to ensuring only authorized and intended system behaviors and outcomes.

⁹⁹ The term adversity refers to those conditions that can cause a loss of assets (e.g., threats, attacks, vulnerabilities, hazards, disruptions, and exposures).

5819 Security assurance claims reflect the desired attributes of a trustworthy secure system.
 5820 These claims are derived from concerns about the completeness and accuracy of
 5821 stakeholder and system requirements,¹⁰⁰ enforcement of the security policy, proper
 5822 implementation of the design, proper maintenance of the system, the usability of the
 5823 system,¹⁰¹ and the avoidance, minimization, and mitigation of defects, errors, and
 5824 vulnerabilities.¹⁰² There may also be other claims involving the ability to exhibit
 5825 predictable behavior while operating in secure states in the presence and absence of
 5826 adversity and the ability to recover from an insecure state. Claims can be expressed in
 5827 terms of functional correctness, strength of function, and the protection capability
 5828 derived from the adherence to standards and/or from the use of specific processes,
 5829 procedures, and methods.

5831
 5832

LEARNING FROM SAFETY

The NASA System Safety Handbook [[NASA11](#)] describes the relevant *claims* to be met in terms of the top-level claim that the system is adequately safe with *subclaims*, including the system is designed to be as safe as reasonably practicable, built to be as safe as reasonably practicable, and operated as safely as reasonably practicable.

5833
 5834
 5835
 5836
 5837

5838 F.2.2 Approaches to Assurance

5839 There are three general approaches to assurance. These approaches vary based on type of
 5840 evidence, how the evidence is acquired, the strength of the judgments made based on the
 5841 evidence, and the extent to which the assurance matches decision-making needs. From weakest
 5842 to strongest, the assurance approaches are *axiomatic*, *analytic*, and *synthetic*.

- 5843 • **Axiomatic Assurance** (assurance by assertion) is based on beliefs accepted on faith in an
 5844 artifact or process. The beliefs are often accepted because they are not contradicted by
 5845 experiment or demonstration. Axiomatic assurance is not suited to complex scenarios.
- 5846 - Demonstration of conformance and compliance are types of axiomatic assurance. While
 5847 useful, they are not well-suited as the sole basis of assurance for complex scenarios.

¹⁰⁰ Claims are not expressed solely as a restatement of the security functional and performance requirements. Doing so only provides assurance that the security requirements are satisfied with the implicit assumption that the requirements are correct, provide adequate coverage, and accurately reflect stakeholder needs and concerns.

¹⁰¹ [[Anderson20](#)] observes that most system failures have a human component, and that assurance must consider human frailty. Furthermore, [[Leveson11](#)] notes that operator behavior is a product of the environment (including its systems) in which it occurs.

¹⁰² Not all vulnerabilities can be mitigated to an acceptable level. There are three classes of vulnerabilities in systems: (1) vulnerabilities whose existence is known and either eliminated or made to be inconsequential, (2) vulnerabilities whose existence is known but that are not sufficiently mitigated, and (3) unknown vulnerabilities that constitute an element of uncertainty. That is, the fact that the vulnerability has not been identified should not give increased confidence that the vulnerability does not exist. Determining the effect of vulnerabilities that are in the delivered system and the risk posed by those vulnerabilities and accepting that there is uncertainty about the existence of a vulnerability that will only become known over time are important aspects that are addressed by assurance.

- 5848
- 5849
- 5850
- 5851
- 5852
- 5853
- 5854
- **Analytic Assurance** (assurance by test and analysis) derives from testing or reasoning to justify conclusions about properties of interest. Belief is relocated from an artifact or process to trust in some method of analysis. The feasibility of establishing an analytic basis depends on the amount of work involved in performing the analysis and on the soundness of any assumptions underlying that analysis. Analytic methods are most relevant in a model that spans *all* relevant uses and *all* interfaces to the environment. That is, the model must not ignore too many details.
- 5855
- Testing demonstrates the presence but not the absence of errors and vulnerabilities.
- 5856
- Testing and analyses will have *uncertainty* that cannot be ignored, especially when they lack comprehensiveness. Uncertainty contributes to risk.
- 5857
- 5858
- **Synthetic Assurance** (assurance by structured reasoning) derives from the method of composition of the “components of assurance” (i.e., the assurance derives from the manner of *synthesis* of the constituent parts). It requires that assurance be a consideration at every step of design and implementation, from the smallest components to the final subsystem realization.
- 5859
- 5860
- 5861
- 5862
- The assurance case described in [[ISO 15026-2](#)] is an example of structured reasoning (also see [Section 2.5.3](#)). Structured reasoning serves to fill the gaps associated with the axiomatic and analytic assurance approaches. Since synthetic assurance is based on expert judgment of available evidence, it is not complete. However, synthetic assurance does further reduce uncertainty and thus reduces risk.
- 5863
- 5864
- 5865
- 5866
- 5867

5868

5869

5870

ASSURANCE CASE

An *assurance case* is a reasoned, auditable artifact that is created to support the contention that a top-level claim is satisfied. The assurance case includes systematic argumentation, evidence, and explicit assumptions that support the claim.

An assurance case contains the following elements [[ISO 15026-2](#)]:

- One or more claims about properties
- Arguments that logically link the evidence and any assumptions
- A body of evidence
- Justification of the choice of a top-level claim and the method of reasoning

[[NASA17](#)] found that assurance cases have numerous advantages over other means for obtaining confidence, such as in the areas of comprehension, informing needed allocation responsibilities, information organization, and robust due diligence. These advantages were larger in areas with otherwise insufficient methods to achieve high assurance. Additionally, assurance cases were determined to be more efficient for complex and novel systems, as well as systems in need of high assurance.

Many formalizations and tools for building assurance cases have been developed in recent years, including the Goal Structuring Notation (GSN) [[GSNCS18](#)] and NASA’s AdvoCATE: Assurance Case Automation Toolset [[NASA19](#)].

5888

5889

5890

5891 Assurance in the system depends on the *quality* of the evidence used in arguments that
 5892 demonstrate that claims about the system are satisfied. Assurance evidence can be obtained
 5893 directly through measurement, testing, observation, or inspection. It can also be obtained
 5894 indirectly through analysis, including the analysis of data obtained from measurement, testing,
 5895 observation, or inspection. Evidence must have sufficient quality in accuracy, credibility,
 5896 relevance, rigor, and quantity. The accuracy, credibility, and relevance of evidence should be
 5897 confirmed prior to its use. For example, some evidence can support arguments for strength of
 5898 function, others for negative requirements (i.e., what will not happen), and still other evidence
 5899 for qualitative properties.

5900 F.2.3 Assurance Needs

5901 Assurance is a need that is engineered and satisfied similar to the need to engineer the system
 5902 capability to satisfy capability needs. Assurance needs for trustworthy secure systems are
 5903 grounded in the concerns of loss and adverse effects due to intentional and unintentional
 5904 adversity (see the design principles of [Commensurate Rigor](#), [Commensurate Trustworthiness](#),
 5905 and [Substantiated Trustworthiness](#)). Assurance needs include the evidence-basis for reasoning,
 5906 the degree of rigor to acquire and interpret the evidence, and the selection of the methods,
 5907 tools, and processes used throughout the system life cycle. Like capability and performance
 5908 needs, assurance needs, expectations, priorities, and constraints should be expressed as system
 5909 requirements and achieved, tracked, and maintained within *systems engineering* as such.

5910
5911
5912
5913
5914
5915
5916
5917
5918
5919
5920
5921
5922

CONFIDENCE MAY BE NEGATIVE

Confidence that is obtained through analysis is not necessarily positive. Assurance evidence can support a compelling argument that counters a stated claim, as well as a conclusion that there is insufficient confidence to support a trustworthiness decision. That is, the system or some part of the system is not sufficiently trustworthy and should *not* be trusted relative to its specified function without further action to establish a sufficiently credible and reasoned evidence base for its use. Alternatively, a risk analysis and risk treatment may be performed [[ISO 16085](#)].

5923 Assurance needs determine the type of evidence and the rigor associated with the activities,
 5924 methods, and tools used to acquire the evidence to satisfy the following cases:

- 5925 • **What is done:** The realization of the design for a secure system
- 5926 • **The means to accomplish what is done:** The methods, processes, and tools employed
 5927 (driven by rigor and assurance objectives) to realize the design for a secure system
- 5928 • **The results of what is done:** The substantiated effectiveness of the realized design of the
 5929 secure system

5930 Assurance needs can vary and constitute a *trade space* that must be managed similar to how
 5931 capability and performance needs can vary. The degree of rigor is the primary means of varying
 5932 assurance. As shown in Figure F-1, a direct relationship exists between the degree of rigor and

5933 assurance and the stakeholder’s assessment of the effects of asset loss. The assurance trade
 5934 space includes the following considerations:

- 5935 • Cost, schedule, and performance
- 5936 • Architecture and design decisions
- 5937 • Selection of technology and solutions
- 5938 • Selection and employment of methods and tools
- 5939 • Qualifications necessary for subject-matter experts

5940 Requirements analysis across stakeholder and system requirements determines the *threshold*
 5941 degree of rigor that is required. When a system cannot practicably meet the needed degrees of
 5942 rigor, stakeholders should have a means to determine if they will accept the associated risk.
 5943

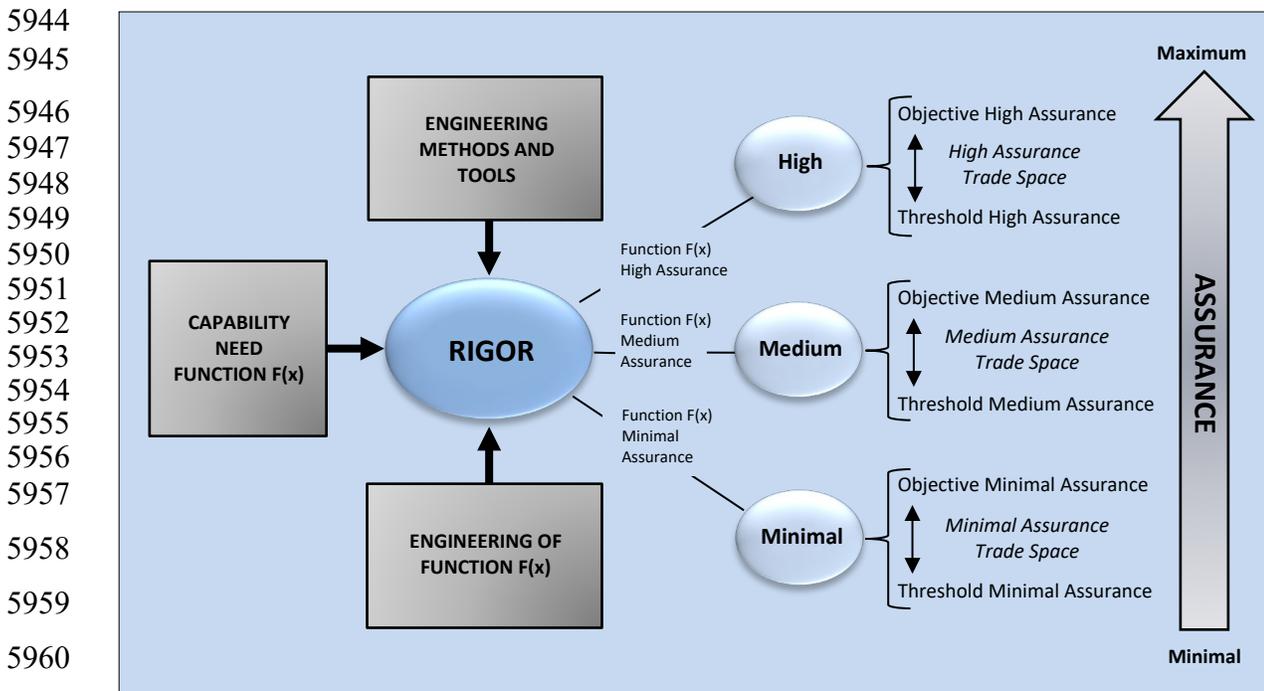


FIGURE F-1: ASSURANCE AND DEGREE OF RIGOR IN REALIZING A CAPABILITY NEED

5963 The highest levels of rigor across systems often requires formal methods—techniques that
 5964 model systems as mathematical entities to enable rigorous verification of the system’s
 5965 properties through mathematical proofs. Formal methods depend on formal specifications (i.e.,
 5966 statements in a language whose vocabulary, syntax, and semantics are formally defined) and a
 5967 variety of models including a formal security policy model (i.e., a mathematically rigorous
 5968 specification of a system's security policy [Appendix C]).

5969 Due to the cost and complexity associated with formal methods, such methods are typically
 5970 limited to engineering efforts where only the highest levels of assurance are needed, such as the
 5971 formal modeling, specification, and verification of security policy and the implementation that
 5972 enforces the policy (Section D.4.2). In this case, the security policy model is verified as complete

5973 for its scope of control and as self-consistent. The verified security policy model then serves as a
5974 foundation to verify the models of the design and implementation of the mechanisms providing
5975 for decision-making and the enforcement of those decisions.

5976

DOES DEFENSE IN DEPTH INCREASE TRUSTWORTHINESS?

[Levin07] noted:

“The notion of defense in depth describes security derived from the application of multiple mechanisms (e.g., to create a series of barriers against an attack by an adversary). However, there is no theoretical basis to assume that defense in depth, in and of itself, could imply a level of trustworthiness greater than that of the individual security components. Without a sound security architecture and supporting theory, the nonconstructive nature of these approaches renders them equivalent to temporary patches.”

Moreover, [Saleh14] notes that poorly designed *defense in depth* layering can actually conceal emerging dangerous system states and conditions. For more information on the proper use of the principle for trustworthy secure design, [Defense In Depth](#), see [Appendix E](#).