



SafSec: Integration of Safety & Security Certification

SafSec Methodology: Standard

S.P1199.50.2
Issue: 3.1
Status: Definitive
2nd November 2006

Originator

Brian Dobbins and Samantha Lautieri

Approver

Martin Fawley (Line Manager)

John Harvey (Safety Manager)

Mark Suitters (MoD DPA FBG 3d)

Copies to:

Client
Mark Suitters MoD DPA FBG 3d

Praxis High Integrity Systems
project file



Contents

1	Background	4
1.1	Foreword	4
1.2	Introduction	5
2	Scope and References	6
2.1	Scope	6
2.2	Limitations	6
2.3	Reading this Standard	6
2.4	Normative References	7
2.5	Terms and Definitions	8
2.6	Symbols and Abbreviated Terms	13
3	Explanatory model	14
3.1	Concepts and Terminology	14
3.2	Establishing Sufficient Dependability	19
3.3	GSN Structure	21
4	Requirements	23
4.1	G1: System is demonstrably dependable	23
4.2	G2: Sufficient losses are identified and mitigated	24
4.3	G3: DSs are defined that mitigate all the identified losses	29
4.4	G4: Causal analysis is sound	30
4.5	G5: Sufficient losses are identified	31
4.6	G6: The causal basis of the identified losses is established	31
4.7	G7: All identified losses and other significant causal steps have associated severity and likelihoods defined	32
4.8	G8: Each DS is sound	33
4.9	G9: DSs are realisable specifications	34
4.10	G10: Appropriate Assurance Requirements defined for each DS	35
4.11	G11: Causal analysis reflects the aggregate effects of DSs	35
4.12	G12: A statement exists that explains how DSs mitigate losses	36
4.13	G13: DSs are together sufficient to achieve mitigation	36
4.14	G14: Actual system is shown to meet all DSs	37
4.15	G15: Actual system is complete	37
4.16	G16: Evidence relates to actual system	39
4.17	G17: Evidence shows that the system meets the DSs	39
4.18	G18: Evidence meets assurance requirement	40
A	Informative Annexes	42
	Document Control and References	43
	Changes history	43
	Changes forecast	44



This report has been funded by the Future Business Group, DPA, MoD

This document has been prepared for MoD and may be referenced if the source is acknowledged.

This document is not a final, endorsed MoD document and your comments and feedback on the SafSec Methodology and its principles are very welcome.

Input from the SafSec Stakeholders is duly acknowledged and their time and involvement has been greatly appreciated.

IPR

Intellectual Property Rights for SafSec, which includes the Standard 50.2 and the Guidance Document 50.3, reside jointly with Praxis High Integrity Systems and MoD.

Caveat on Use

Caveat on Use: Adherence to a process does not ensure certification and therefore use of the SafSec Methodology does not guarantee certification for your module or system. Praxis High Integrity Systems and MoD accept no liability for any loss or damage incurred or suffered as a result of the application of the SafSec methodology.

Distribution

Approval for wider use or distribution must be sought from:

SafSec Project Manager,

Praxis High Integrity Systems, 20 Manvers St, Bath, BA1 1PX

www.praxis-his.com/safsec



1 Background

1.1 Foreword

- 1 This Standard was developed by Praxis High Integrity Systems under the **SafSec** study placed by the MoD to consider how best to combine safety and security certification in a complicated system environment such as Advanced Avionics Architectures (AAvA) or Integrated Modular Avionics (IMA).
- 2 This Standard does not replace the current safety and security standards, nor does it abrogate nor deprecate any of their specific requirements. Rather, it provides a framework in which such standards may be met more cost effectively and with reduced risk, based on the following properties:
 - a) A clear set of safety and security goals are required from system conception.
 - b) A goal-based approach rather than a process-based approach to evidence generation can be adopted, allowing the issues affecting safety and security to influence the system design more easily.
 - c) A modular approach to certification can be undertaken, allowing system complexity to be handled, easing the re-certification due to changes in system requirements, design, or use, and aiding the potential reuse of modules.
 - d) An incremental approach to establishing the certifiability of components of the system is supported.
 - e) A common approach to the generation of evidence can be adopted to maximise re-use for both safety certification and security accreditation.
 - f) Evidence to support the safety and security goals can be built up systematically during application of the process, rather than be generated retrospectively, which eases the certification authorities' and assessors' tasks, and reduces the risk of costly re-work of the design.
- 3 The background to the study is provided by the following standards governing the safety and security aspects of military avionics development:
 - a) for safety aspects:
 - Defence Standard 00-56, Safety Management Requirements for Defence Systems [3, 4]
 - b) for security aspects:
 - Common Criteria for Information Technology Security Evaluation [2]
 - Manual of Protective Security [5].
- 4 These standards were selected as being the most appropriate for the domain that **SafSec** has been designed to address. Nevertheless, the principles that are embodied within this Standard are consistent with general good practice in safety and security engineering, and thus can be applied to systems that are being developed to other similar standards.



1.2 Introduction

- 1 This document defines the *Standard* for the SafSec methodology. It describes the objectives of the methodology for development of certified systems, specifically aimed at IMA for AAva, but likely to be applicable to other systems also.
- 2 The document describes goals to be achieved and criteria for assessing satisfaction of those goals. The structure of the method is such that if these goals are satisfactorily achieved, the resulting evidence will support both safety and security certification, but this document does not attempt to reiterate the detailed requirements of all applicable standards. It should thus be read in conjunction with the relevant security and safety standards.
- 3 A more detailed description of the structure of this document is given in Section 2.3 below.
- 4 There is an accompanying document [B] that provides *Guidance* in meeting this Standard.



2 Scope and References

2.1 Scope

- 1 This *Standard* defines the objectives that must be met by a systems development in order to be certified by both safety and security certifiers within a **SafSec** framework. The Standard is non-prescriptive, defining only the aims to be met, not the means by which they will be met.
- 2 The *Guidance* [B] expands on the objectives set out in this Standard with indications of how the objectives may be met while conforming to existing safety and security standards.
- 3 Following this Standard will not necessarily be enough to obtain certification for security or safety. Actual certification will normally require conformance with specific safety or security standards (such as DS 00-56[3, 4] or the CC[2]). This **SafSec** Standard does not supersede these standards, but it does help to achieve the certifications with the minimum of duplicated work and the maximum of re-use of evidence between the different certifiers.

2.2 Limitations

- 1 This Standard and Guidance is focused on combined *safety* and *security* certification. It is couched in the wider context of *dependability*, which incorporates reliability, availability, performance, and other properties of systems that affect the ability of a system to carry out its functions. Although it is believed that the **SafSec** approach is applicable to most of the dependability properties, all of the development effort has focused on safety and security. It should be used for other dependability properties with care.

2.3 Reading this Standard

- 1 The body of this document consists of two parts:
 - a) An Explanatory Model (Section 3) that introduces the concepts and terminology of the Standard and presents the overall structure of the Standard (Section 3.3).
 - b) Requirements (Section 4) structured according to a breakdown of the top-level *goal* (G1: System is demonstrably dependable). The requirements are structured according to the conventions of the Goal Structuring Notation (GSN) [C] in a form that is outlined in Section 3.3. Each part of Section 4 defines the criteria to be used in assessing if the goal has been met. These criteria are divided between the applicable **SafSec** frameworks.
- 2 In order to be compliant with this Standard, the top-level goal given in Section 4.1: “G1: System is demonstrably dependable” shall be achieved.



2.4 Normative References

- 1 ISO/IEC Directives, Part 2, Rules for the structure and drafting of International Standards, fourth edition, 2001.
- 2 Common Criteria for Information Technology Security Evaluation, version 2.1 August 1999.
- 3 Defence Standard 00-56, Safety Management Requirements for Defence Systems, Issue 2, UK Ministry of Defence, 13 December 1996.
- 4 Defence Standard 00-56, Safety Management Requirements for Defence Systems, Provisional Issue 3, UK Ministry of Defence, 17 December 2004.
- 5 Manual of Protective Security, (incorporating ISO/IEC 17799/BS7799 and HMG InfoSec Standard No. 1), June 2003.
- 6 Not used.
- 7 Defence Manual of Security, JSP 440.
- 8 DO-178B/ED-12B, Software Considerations in Airborne Systems and Equipment Certification, December 1992.
- 9 British Standard EN 61508 Functional Safety of electrical/electronic/programmable electronic (E/E/PE) safety-related systems Parts 1-7 , 2002.
- 10 Common Methodology for Information Technology Security Evaluation (CEM) Version 2.2, Revision 256, January 2004.
- 11 HMG Infosec Standard 1 Residual Risk Assessment Method, June 2003.
- 12 HMG Infosec Standard 2 Risk Management and Accreditation Document Set, July 2005.
- 13 HMG Infosec Standard 3 Connecting Business Domains, October 2001.
- 14 HMG Infosec Standard 4 Communications Security and Cryptography, July 2005.
- 15 HMG Infosec Standard 5 Secure Erasure of Protectively Marked Information, May 2003.
- 16 EUROCAE IMA document: Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations WG-60/SC-200 Working Paper, April 2005.

Informative references, cited as [A], [B], etc. are listed in annex A.1, Informative References.



2.5 Terms and Definitions

- 1 Terms in *italics* are further expanded in section 3.1.
- 2 The definition of some terms is dependent on context of use (e.g. sufficient, or sound). These terms are not defined below, but are defined in the Context bubbles of the GSN (see section 3.3.1 and figure 2) and their associated textual expansions.

Assessors	Independently responsible to the Evaluation Authority for ensuring that the dependability requirements and the requirements of this Standard have been met. <small>c.f. Assessors, in CC</small>
Asset	Defining dependability requires that there is an understanding of the entities of value in the domain in which the system operates. These valued entities are assets. The entities may be people, equipment, data or services. <small>c.f. Asset, in CC, MPS</small>
<i>Assurance Requirement (AR)</i>	The level of confidence in the evidence needed for certifying that the system meets its dependability target.
Causal and Impact Analysis	An analysis of losses that ties together causes (eg system failures, security attacks) and the impact that follows from these causes. <small>c.f. Accident sequence, Fault Tree Analysis, Hazard Analysis, in 00-56 Threat Analysis, Assumptions-Objectives-Requirements, in CC</small>
Component	A logical or physical element of the system architecture
Composition	A system may be <i>composed</i> with another system that it interfaces to, with respect to dependability, if the system dependability cases are consistent with each other. A module hierarchy is said to be <i>composed</i> , with respect to dependability, if the module boundary contracts for all of its constituent modules are consistent with each other.
Context clause	Part of a Module Boundary Contract that defines the assumptions relating to the operational context of the implementation of the system components that contribute to the guarantee and rely clauses



Counter-evidence clause	Part of a Module Boundary Contract that defines the limitations that exist in the contract. This clause may reference known defects in the implementation, as well as the residual risk that has been classified as acceptable. c.f. Counter-evidence in 00-56
Customer	Ultimate owner of the system, responsible for operational requirements. c.f. Sponsor, in CC Duty Holder's organisation, in 00-56
<i>Dependability</i>	The ability to deliver service that can justifiably be trusted.
Dependability Objectives	A set of objectives that define an acceptable scope for the dependability of a system, and hence the meaning of "dependable" for the system, as agreed by the stakeholders.
<i>Dependability Specification (DS)</i>	A specification of the system or one of its components that defines its dependability properties.
Dependability Target	Quantitative or qualitative measures for determining the acceptability of a risk, and hence assessment of dependability. A system's dependability target is set by its stakeholders in the context of the environment in which the system will be used. c.f. Tolerability Criteria, in 00-56
Evaluation/Certification Authority	Responsible for approving one or more dependability aspects of the system prior to its acceptance into service. c.f. Evaluation Authority, in CC Accreditor
Evidence	In order to be able to demonstrate that a system or module meets its dependability target, <i>evidence</i> for the dependability argument is prepared and presented. Evidence shall be permanent, traceable and managed in such a way as to provide later readers confidence in its source, contents and validity.
Exposure	A significant class of losses arise when a specified event occurs only in some particular state of the system or its environment. In these cases, it can be useful to separate out the likelihood of the triggering event from the probability that such an event will occur in the sensitive state. This latter probability (typically expressed as a proportion of the life of the system) is the <i>exposure</i> to the (potential) loss. When separating the attributes of a loss in this way, both the likelihood of the triggering event and the exposure are elements of the risk associated with the loss.



External stakeholders	Those in the wider community who have a stake in agreeing the dependability targets, and agreeing acceptable levels of risk.
Guarantee clause	Part of a Module Boundary Contract specifying the conditions this module guarantees to be true.
<i>Identified losses</i>	The set of losses, identified by the project stakeholders, whose occurrence is relevant to the dependability of the system, usually due to each having an associated inherent risk that is unacceptable.
Integrity (as part of security)	The prevention of the unauthorised modification of information.
Likelihood	Losses have a probability or frequency with which they are likely to occur (in a particular environment). This probability or frequency is the <i>likelihood</i> of the loss. Likelihoods may be expressed qualitatively (on a scale from Frequent to Incredible, for example) or quantitatively (as a probability of occurrence within a specified interval, as a mean time between occurrences, or as a number of occurrences expected in a specified interval). Likelihoods may also be characterised by constraints which govern the occurrence of events – the likelihood of a challenge to system security for example, may be measured by the means and opportunity required to make the challenge (measured as a cost of mounting an attack, for example). c.f. Attack potential, in CC
Loss	A state of the system that has the potential to lead to an undesired external effect. c.f. Hazard, in 00-56 Vulnerability, in IS1
Mitigation argument	An argument that a set of dependability specifications are appropriate to mitigate the risk associated with a loss to an acceptable level. This means a justification, with appropriate evidence, that the stated DSs are sufficient to achieve a residual risk that meets the dependability target.



<p><i>Module</i></p>	<p>A logical grouping of dependability specifications for the purposes of abstraction and encapsulation. A module may be the subject of a <i>module dependability case</i> in its own right. Modules may be implemented by physical components, software packages, or combinations of hardware and software. Modules may include social elements (eg operating rules and procedures) as well as technical components.</p> <p style="text-align: right;">c.f. TOE in CC Module, in 00-56, IMA Component, in 00-56 Domain, in IS3</p>
<p><i>Module Boundary Contract (MBC)</i></p>	<p>The externally-viewable (black-box) definition of all dependability-related characteristics of a module in the context of its intended operation. This includes the dependability properties that the module provides, those that it relies upon, its assumptions relating to operational context, its assurance level, and any counter-evidence, such as residual risk.</p>
<p>Previously-Developed Component</p>	<p>A component that is pre-existing, including COTS, other re-usable components, and enhanced legacy components. Previously-developed components are often developed to operate in a variety of environments.</p>
<p>Rely clause</p>	<p>Part of a Module Boundary Contract specifying the conditions this modules relies upon from other modules in order to achieve its guarantee clause, and the level of assurance in those conditions.</p>
<p>Residual Risk</p>	<p>The risk that is associated with a loss which remains once the system is accepted, with all mitigations in place.</p> <p style="text-align: right;">c.f. Residual risk, in MPS</p>
<p><i>Risk</i></p>	<p>The combination of severity of a loss, and its likelihood.</p> <p style="text-align: right;">c.f. Risk, in 00-56, MPS</p>
<p>Safety</p>	<p>The property of a system, in a given application and in a given operational context, that relates to the extent to which risk that may affect human life or environmental health has been demonstrated to have been reduced to an acceptable level.</p> <p style="text-align: right;">c.f. Safe, in 00-56</p>
<p>Security</p>	<p>The combination of confidentiality, integrity and availability.</p> <p style="text-align: right;">c.f. Security, in CC</p>



Severity	The <i>severity</i> of a loss is a measure of the amount of harm caused by the loss. The measure may be qualitative or quantitative, and a variety of measures may be used: financial loss, number of people affected, or political impact, for example.
Significant event	An event that contributes to the assessment of risk for an identified loss
Sub-contractors	Any organisation contracted to carry out some task by another.
Suppliers	Producer of the system, responsible for delivering the system and all necessary evidence to support acceptance.
System	The artefact being produced. May include hardware, software, personnel, manual procedures, documentation, etc. This Standard is focussed on IMA systems, but is also applicable to other types of systems. c.f. System, in 00-56, CC
System / Module Dependability Case	A structured argument, supported by a body of evidence, that provides a compelling, comprehensive and valid case that a system or module is dependable. In the case of a system dependability case, dependability is for a given application, in a given operating environment. c.f. Safety Case, in 00-56, JSP 553 Risk Management and Accreditation Document Set, Accreditation Document Set in IS2
TEMPEST	The protection of electronic equipment against the influence or leakage of electromagnetic radiation.
Threat	An action or event that has the potential to prejudice or compromise the security property of an asset. Emphasis is given to malicious intent by a threat agent, that may be dynamically mutable in execution. c.f. Threat, in ITSEC
Threat Agent	The person or organisation associated with, and carrying out, a specific attack.



2.6 Symbols and Abbreviated Terms

00-56	Defence Standard 00-56 [3]
AAvA	Advanced Avionics Architectures
ALARP	As Low As Reasonably Practicable
AR	Assurance Requirement
CC	Common Criteria [2]
CG _n	Number of Context associated with a Goal (e.g. CG3 is Context associated with Goal G3, and CG1.2 is the second Context associated with Goal G1.)
CS _n	Number of Context associated with a Strategy (g. CS2 is Context associated with Strategy S2.)
DS	Dependability Specification
EMC	Electromagnetic Compatibility
G _n	Number of Goals (e.g. G1, G2, G3, etc.)
GSN	Goal Structuring Notation [C]
IMA	Integrated Modular Avionics
MBC	Module Boundary Contract
MoD DPA	Ministry of Defence, Defence Procurement Agency
MPS	Manual of Protective Security [5]
S _n	Number of Strategy (e.g. S1, S2, S3)



3 Explanatory model

- 1 The requirements of this Standard, as presented in Section 4, rely upon a well-defined set of terms, used within a model of dependability analysis. This section defines these terms and presents the model.

3.1 Concepts and Terminology

3.1.1 System

- 1 A *System* is the term used to describe the totality of the operational artefact whose dependability must be demonstrated. A system may include hardware, software, personnel, manual procedures, documentation, etc. The complexity of a system ranges from large distributed “system of systems”, to a single federated node that performs a simple function.
- 2 The internal structure of the system is defined by its *components* and by the *system architecture*.

3.1.2 Dependability

- 1 Before a system may be certified, sufficient confidence in a variety of properties must be established. These properties span both functional and non-functional objectives. The two properties that are addressed by this Standard are *safety* and *security*.
- 2 This Standard addresses the establishment of sufficiency of confidence in the safety and security properties of the system using a common framework. The Standard treats both safety and security as aspects of a more general property – *dependability*:
 - a) *Dependability of a computing system is the ability to deliver service that can justifiably be trusted. [D]*
- 3 The set of objectives that define an acceptable scope for the dependability of a system, and hence the meaning of “dependable” for that system, is termed the *dependability objectives*.
- 4 The quantitative or qualitative measures for determining the acceptability of a risk, and hence the assessment of whether the dependability objectives have been met in the context of the environment in which the system will be used, is termed the *dependability target*.

3.1.3 Loss

- 1 A *loss* is a state of the system that has the potential to lead to an undesired effect in the application domain. Such effects include loss of life and compromise of confidential information.
- 2 The set of losses that must be addressed in order to establish the required safe and secure deployment of the system governs the setting of the dependability objectives for the system.



- 3 The strategy for identification of the losses to be addressed by this Standard is based on an informed selection by the stakeholders of the set of losses that have an associated inherent risk that is unacceptable. Such a loss is termed an *identified loss*.
- 4 Each identified loss is associated with an *asset*.
- 5 Each identified loss is assessed to determine its level of *risk*.

3.1.4 Risk

- 1 Losses can be characterised by the seriousness of the event (severity) and the frequency or probability with which the event can be expected to occur (likelihood). This combination of severity and likelihood is the *risk* associated with a particular loss.
- 2 Risks may be assessed quantitatively (when sufficient information is available to characterise its parameters numerically) or qualitatively using a relative risk classification. The likelihood part of risk may be a single likelihood value, or it may be expressed as the combination of the likelihood of some undesirable event together with a measure of the exposure of the system to circumstances where the event may cause a loss (the exposure).
- 3 The level of risk that remains for each identified loss after all risk mitigation measures have been adopted is termed the *residual risk*.
- 4 All residual risk must be *acceptable* before the dependability of the system can be achieved. The criteria for determining the acceptability of residual risk in the context of the environment in which the system is to be used, governs the setting of the dependability target for the system.

3.1.5 Assurance Requirement (AR)

- 1 *Assurance requirements* specify the level of confidence or assurance in the evidence needed for certifying that the system meets its dependability target.

3.1.6 Dependability Specification (DS)

- 1 The argument and supporting evidence to establish the required level of confidence as defined by the assurance requirements are underpinned by a set of *Dependability Specifications*. A dependability specification reflects what the system (or component) can achieve of its own accord, in that it refers to phenomena that are under its control, and hence are either statements about the system (or component) behaviour or design constraints. The dependability specification may use knowledge of how the system is intended to operate (“white-box”).
- 2 Dependability specifications are analogous to safety and security requirements, including interface requirements, on the disparate components of the system that contribute to the meeting of the dependability target.



3 Each dependability specification defines the assurance requirement that its supporting evidence must be able to demonstrate.

4 Note: Previously-Developed Components

5 A set of dependability specifications is not explicitly required to be generated retrospectively for the inclusion of a previously-developed component in the system, where the safety and security requirements and interfaces for the component are specified in a controlled requirements specification. If no such specification exists for the component, it is highly recommended that the claimed dependability properties of the component, and the claimed level of confidence in their realisation, be recorded in a set of retrospectively-generated DSs for the purpose of simplifying the processes that are defined in this Standard.

3.1.7 Mitigation Argument

1 A *mitigation argument* justifies that a set of dependability specifications are appropriate to mitigate the risk associated with a loss to an acceptable level. This means a justification, with appropriate evidence, that the stated DSs are sufficient to achieve a residual risk that meets the dependability target.

3.1.8 Satisfaction Argument

1 A *satisfaction argument* provides a justification, with appropriate evidence, that a set of assertions is consistent with a conclusion.

3.1.9 Module

1 A *module* is a logical grouping of dependability specifications for the purposes of achieving abstraction and encapsulation.

2 A module provides a “black-box” summary of all dependability-related characteristics of the grouping, such that its dependability can be independently assessed. A module may thus be the subject of a dependability case in its own right.

3 A module defines the assurance requirement that specifies the claimed level of confidence in the evidence of meeting its dependability properties (via implementation of the related dependability specifications).

4 A module may be decomposed into *sub-modules*. The structure and dependency relationships of the module and its sub-modules is termed the *module architecture*.

3.1.10 Module Boundary Contract (MBC)

1 The definition of a module is termed a *Module Boundary Contract (MBC)* in this Standard. The MBC defines the externally-viewable (“black-box”) definition of all dependability-related characteristics of the module in the context of its intended operation.



- 2 A module boundary contract includes at least the following parts:
 - a) the *guarantee clause*, which defines the dependability characteristics that this module *guarantees* to hold true;
 - b) the *rely clause*, which defines the dependability characteristics that this module *relies* upon in order to achieve its guarantees, including the assurance requirement for each characteristic;
 - c) the *context clause*, which defines the assumptions relating to the operational context of the implementation of the system components that contribute to the guarantee and rely clauses;
 - d) the *assurance requirement clause*, which defines the level of confidence or assurance that is claimed for the contract. The assurance requirements may be split into sub-clauses to reflect the safety level of confidence and the security assurance level that is claimed for the module as a whole;
 - e) the *counter-evidence clause*, which defines the limitations that exist in the contract. This clause may reference known defects in the implementation, as well as the residual risk that has been classified as acceptable.
- 3 A satisfaction argument for the validity of the mapping between the module boundary contract and its related set of dependability specifications must be established.
- 4 Note: Previously-Developed Components
- 5 A module boundary contract is not explicitly required to be generated retrospectively for the inclusion of a previously-developed component in the system, where the internal information about the component design and implementation is available “white-box”, such as the re-use or upgrade of a legacy sub-system. In this case, it is sufficient to treat the dependability aspects of this component in the same way as for other newly developed components of the system.
- 6 Otherwise, when the component is to be treated as a “black box”, for example a COTS product, it is highly recommended a module boundary contract be defined retrospectively to encapsulate formally the dependability characteristics of the component. This approach increases confidence in the use of such components for dependable systems, since any associated risk is more likely to be revealed through the process of validation of module composition.

3.1.11 Dependability Case

- 1 A *system dependability case* is a structured argument, supported by a body of evidence, that provides a compelling, comprehensive and valid case that a system is dependable, for a given application, in a given operating environment.
- 2 A *module dependability case* is a structured argument, supported by a body of evidence, that provides a compelling, comprehensive and valid case that a module has dependability properties, to a specified level of confidence.



- 3 The dependability case encapsulates all artefacts relating to the system or module that are required to show compliance with this Standard.

3.1.12 Composition

- 1 A system may be *composed* with another system that it interfaces to, with respect to dependability, if the system dependability cases are consistent with each other. Consistency of two system dependability cases is established by:
- a) ensuring that the external dependencies of one system on the other system do not conflict;
 - b) ensuring that the external dependencies of each system on all other systems do not conflict;
 - c) ensuring that the operational context assumptions and limitations of one system do not conflict with those of the other system.
- 2 A module hierarchy is said to be *composed*, with respect to dependability, if the module boundary contracts for all of its constituent modules are consistent with each other. The following properties shall hold for a module hierarchy to be composed:
- a) If a guarantee clause entry is apportioned to a (set of) sub-module(s), there shall be a satisfaction argument to show how the guarantees in the sub-module(s) satisfy the guarantee in the super-module.
 - b) If a rely clause entry is propagated from a sub-module to its super-module, there shall be a satisfaction argument to show how the rely in the super-module covers the rely in the sub-module, including sufficiency of assurance requirement.
 - c) If a rely clause entry is satisfied by a guarantee clause entry in the same module hierarchy, the definitions of the two entries shall match, and the assurance requirement for the guarantee entry shall be sufficient to meet the assurance requirement of the rely entry.
 - d) All rely clause entries in the module hierarchy shall be satisfied, either via guarantee clause entries within the same module hierarchy, or via propagation to a super-module, or via an assumption on the external environment that is recorded in the context clause or counter-evidence clause of the top-level module.
 - e) All context clause entries in the entire module hierarchy shall be non-conflicting, and there shall be a satisfaction argument to show that the context clause of the top-level module covers all other context clauses in the same module hierarchy.
 - f) The assurance requirement clause for the top-level module shall be consistent with all other assurance requirement clauses in the same module hierarchy.
 - g) There shall be a satisfaction argument to show that the counter-evidence clause for the top-level module covers all other counter-evidence clauses in the same module hierarchy.



3.2 Establishing Sufficient Dependability

3.2.1 Principles

- 1 This Standard's approach to establishing sufficient dependability of a system or component is based on three principles:
 - a) identifying and managing the risk of loss;
 - b) directing design to mitigate the risk of loss;
 - c) encapsulating the dependability arguments of logically-separate modules.
- 2 The risk management process takes account of safety hazards and security threats, together with the operational requirements of the target system, to produce a risk model alongside the architectural and functional models of the system.
- 3 The risk directed design process uses the risk model, together with the architectural model of the system, to define the dependability specifications of all the system components in parallel with their functional properties, and to produce the arguments supporting traceability of this process.
- 4 Modular certification groups related dependability specifications into a module that defines dependability properties, and uses supporting arguments and evidence to justify certification of the module to a stated level of confidence. As modules can be composed from collections of other modules, multiple application of this process can result in system certification. The result of the process is a set of safety and security certificates, and information which can support operational acceptance.
- 5 Figure 1 below shows the relationships between the key concepts and terms.

3.2.2 Risk Assessment

- 1 The strategy to assess the level of risk associated with each identified loss is based on analysis of cause and effect. This is termed *risk assessment*.
- 2 The causes of each identified loss, and their likelihood or probability, are determined by *causal analysis*. Identification and analysis of all possible causes of losses involves investigating the possible events or states that the system or application domain can pass through, concentrating on the behaviours that can contribute to loss. The exact technique and level of detail may vary.
- 3 The effect of each identified loss, and the consequential severity of sustaining the loss, is determined by *impact analysis*. An impact analysis determines all possible consequences of the occurrence of the loss within the domain in which the system is deployed, to determine the severity of the worst-case outcome. The exact technique and level of detail may vary.

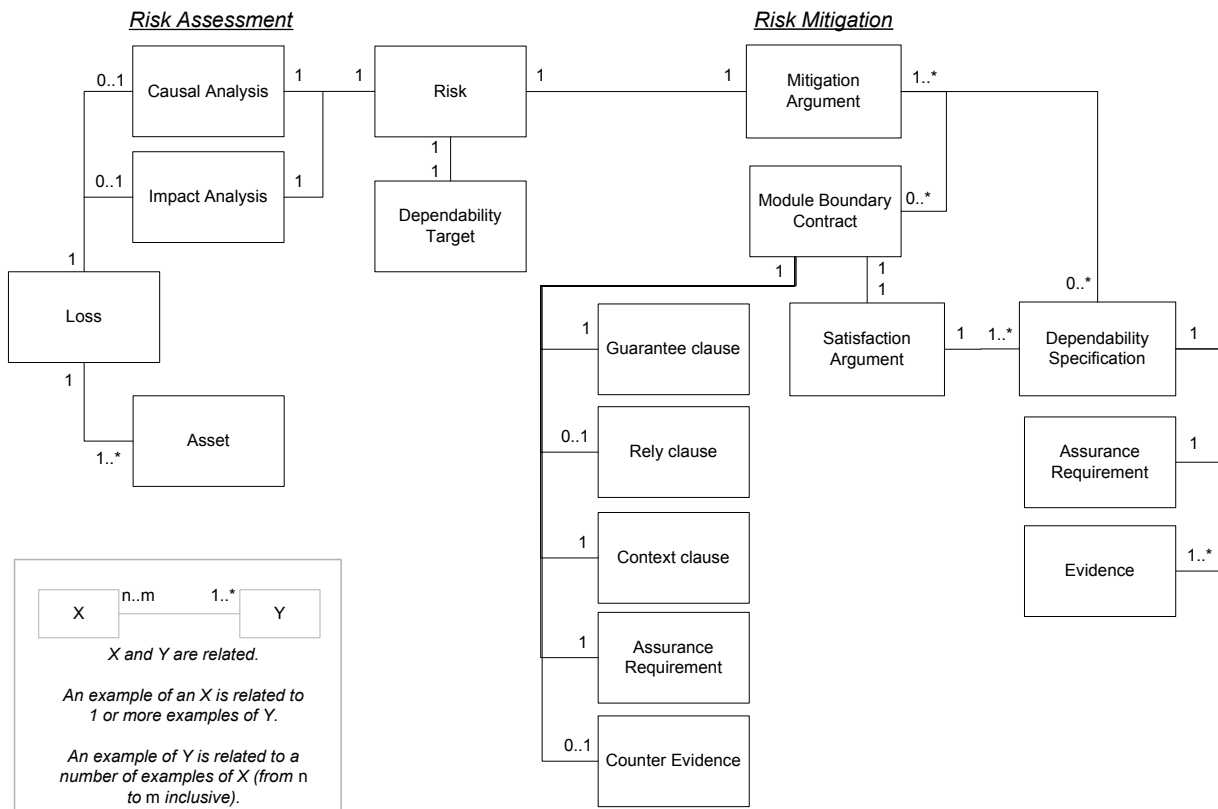


Figure 1: Relationship between key concepts and terms

- 4 The following properties hold for the results of the causal and impact analyses that are defined by this Standard:
- the system is involved in the analysis at some point, otherwise the loss is irrelevant to the development of this system;
 - the eventual result is a set of relevant losses that the system may sustain, each with their associated risk (which may be null);
 - the cause and effect relationships are argued by relying on properties of the domain, or specified properties of the system, or by laws of physics. There is a stated argument justifying why the effects follow from the causes.



3.2.3 Risk Mitigation

- 1 The strategy to reduce the level of risk associated with each identified loss to an acceptable level is termed *risk mitigation*.
- 2 A mitigation argument is generated to justify the acceptability of the residual risk associated with each loss. The justification makes use of dependability specifications (that may be abstracted into module boundary contracts) together with the evidence that demonstrates that the corresponding assurance requirements have been satisfied.
- 3 The following property holds for the results of risk mitigation:
 - a) all risks must be reduced to a level that is acceptable, based on the applicable dependability target.

3.3 GSN Structure

3.3.1 Explanation of the Goal Structure

- 1 Figure 2 summarises the goals and subgoals that must be achieved in order to comply with the SafSec Standard.
- 2 Each goal has an associated subsection in section 4 that gives the details of the arguments that must be presented in order to achieve that goal. In general, goals may be achieved either *directly* or by *goal breakdown*. To achieve a goal directly, a number of things must be argued – the details of these are explained in the relevant subsection. These things are organised into seven frameworks, and the diagram labels each goal with the frameworks that are applicable to that goal.
- 3 In order to achieve a goal by goal breakdown, each of its subgoals must be achieved. In general, all of the things needing to be achieved by a goal are carried down and allocated to one or more of its subgoals, and hence once the decision has been made to use goal breakdown, the higher level goal does not need to be referred to again. For this reason, many of the requirements stated in one goal are also required in its subgoals, sometimes verbatim, sometimes slightly enhanced.
- 4 Due to the broad reach of two of the frameworks (Organisational and Procedural) they have not been carried down and allocated to subgoals. Therefore, even if goals are achieved by goal breakdown, there is still a requirement to *achieve the Organisational and Procedural aspects of goal G2*.
- 5 An approximate mapping between the goals presented and the MoD standard view of system development (CADMID) is given for each goal in Figure 2. CADMID breaks a system's life into six phases: Concept, Assessment, Demonstration, Manufacture, In-service, and Decommission/Disposal. Each of the goal's likely contribution during these phases is defined in terms of four activities: no contribution, planning, achievement, and maintenance.

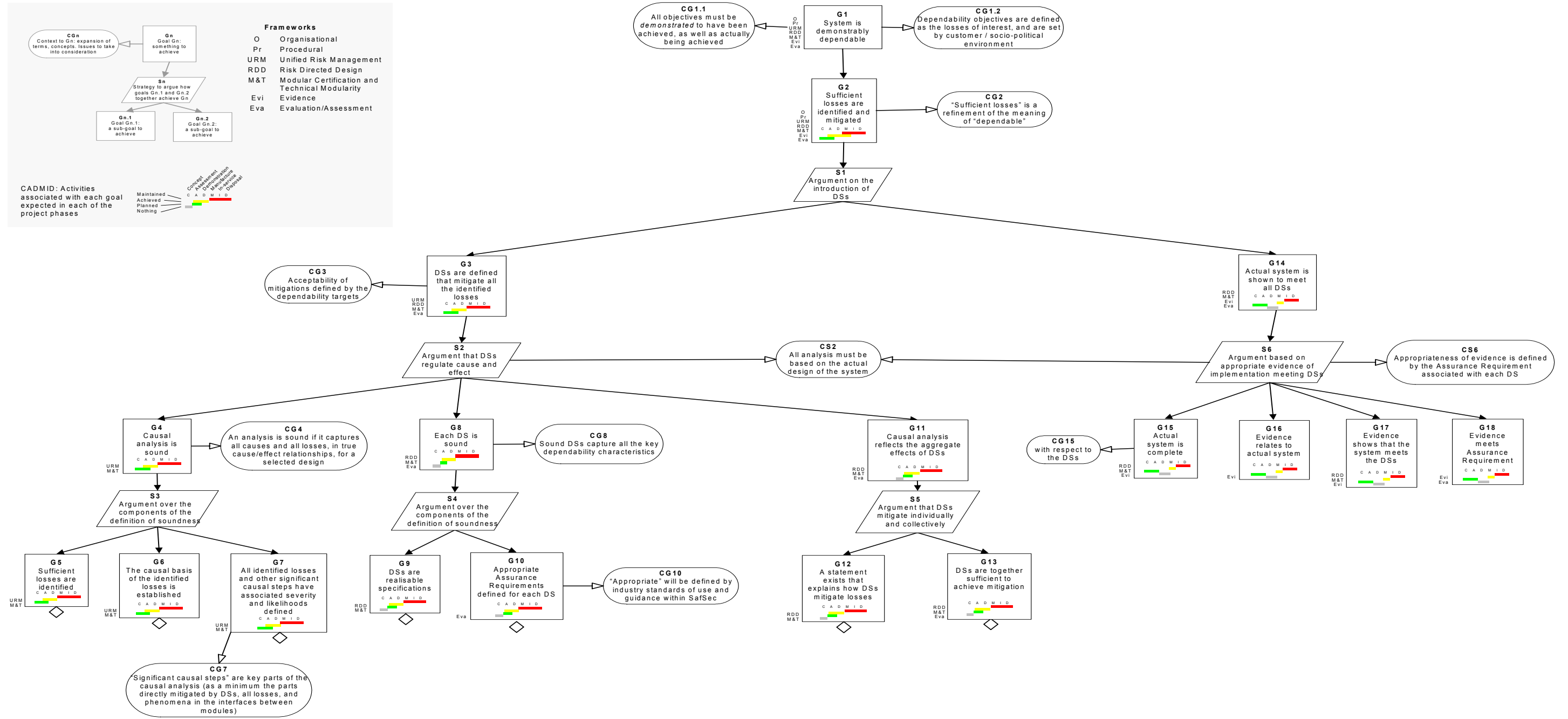


Figure 2: Goal structure for the achievement of a dependable system



4 Requirements

- 1 In order to be compliant with this Standard, the top-level goal: “G1: System is demonstrably dependable” shall be achieved.
- 2 Note: The term “system” as used within this chapter shall be understood to include “component” whenever the component may sensibly be the subject of its own dependability case.

4.1 G1: System is demonstrably dependable

- 1 The top level objective is the delivery of a dependable system, supported by evidence demonstrating its dependability.

4.1.1 Context CG1.1 and Context CG1.2

- 1 This whole goal breakdown is directed toward the *demonstration* of dependability as well as the *achievement* of dependability. For this reason, many of the goals ask for documentation to support the claim that certain actions were carried out or that certain decisions were justified, rather than just asking for the actions to be done.
- 2 The meaning of “dependable” is defined by the dependability objectives for the system (see section 3.1.2).

4.1.2 By goal breakdown

- 1 This goal shall be achieved by documenting in the system dependability case:
 - a) a definition of the system sufficient to ensure that there is no doubt about the scope covered by the term “system” as used throughout the dependability case;
 - b) a definition of the dependability properties of other systems that this system relies upon to achieve its dependability, including the required dependability target;
 - c) a definition of the operational context or environment that is assumed by the system.
- 2 **and** by meeting the acceptance criteria for:
 - a) G2: Sufficient losses are identified and mitigated

4.1.3 Directly

- 1 This goal shall be achieved only by following the goal breakdown given above.



4.2 G2: Sufficient losses are identified and mitigated

4.2.1 Context CG2

- 1 The meaning of “sufficient losses are identified” is defined to be the set of identified losses (see section 3.1.3),
- 2 An identified loss is said to be mitigated if its residual risk is acceptable, as defined by the dependability target (see section 3.1.2).

4.2.2 By goal breakdown

- 1 This goal shall be achieved by meeting the acceptance criteria for:
 - a) G3: DSs are defined that mitigate all the identified losses; **and**
 - b) G14: Actual system is shown to meet all DSs; **and**
 - c) The specific acceptance criteria for the organisational and procedural frameworks as defined in sections 4.2.3.1 and 4.2.3.2.

4.2.3 Directly

- 1 This goal shall be achieved by meeting the following acceptance criteria:

4.2.3.1 Organisational Framework

- 1 The project shall identify the organisations fulfilling the following roles, and facilitate the tasks they carry out:
 - a) Customer – ultimate owner of the system, responsible for operational requirements.
 - b) Suppliers – producer of the system, responsible for delivering the system and all necessary evidence to support acceptance.
 - c) Sub-contractors – any organisation tasked to carry out some activity by another.
 - d) Evaluation/Certification Authority – responsible for approving one or more dependability aspects of the system prior to its acceptance into service.
 - e) Assessors – independently responsible to the Evaluation Authority for ensuring that the dependability requirements and the requirements of this Standard have been met.
 - f) External stakeholders – those in the wider community who have a stake in agreeing the dependability objectives and targets, and agreeing acceptable levels of risk.



- 2 The relationship between key organisations above is shown in Figure 3.

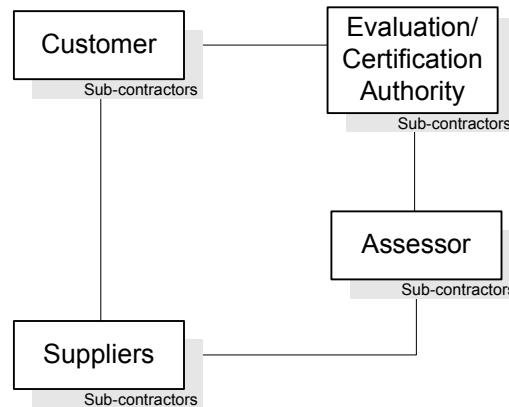


Figure 3: Relationship between key organisations

- 3 The project shall document the form of the interfaces between the organisations adopting these roles, and the approach the project will take in managing these interfaces to ensure that dependability is maintained across them, especially across all sub-contractor boundaries.
- 4 As well as the above organisational roles, the following individual roles shall be identified:
- Project Manager: responsible for the project overall.
 - Dependability Manager: responsible for all aspects of achieving dependability.
- 5 The project shall ensure that the staff carrying out any dependability-related activities are competent, and shall document the evidence of this competency. The environment of the Supplier and their sub-contractors shall be demonstrated to be appropriate to ensure that dependability is maintained (e.g. is secure).

4.2.3.2 Procedural Framework

- 1 In order to be confident that the system is dependable, and to achieve certification, the certification authorities must be sure that certain actions have been carried out. To support this, the project shall:
- document *plans* before any activities are carried out;
 - document the expected *outputs* (documentation) that will be used for certification;
 - put in place a Dependability Management system, which shall incorporate quality management, change control, and document control.
- 2 The project shall identify all other standards, legislation, policies and such that must be adhered to, and shall document how these will be met.



4.2.3.3 Unified Risk Management Framework

- 1 The project shall document the following in the system dependability case:
 - a) a systematic, repeatable *process* that identifies all the relevant losses associated with this system;
 - b) evidence that this process has been followed;
 - c) all the identified losses with which this system is associated;
 - d) a justification that all the relevant losses have been identified;
 - e) the result of consolidating all identified losses to eliminate replication, conflicts, inconsistencies and ambiguities;
 - f) the process to ensure identified losses stay current and sufficiently complete in the face of any change, such as a change to the design or use, a change in the environment in which it is used, or modifications made (such as in-service fault fixing);
 - g) a systematic, repeatable process to assess the residual risk of each identified loss;
 - h) a justification that the process adopted to assess the risk of each identified loss is appropriate;
 - i) the agreed top level dependability objectives that define the context of the meaning of “dependable” (see section 3.1.2);
 - j) the agreed top level dependability target that defines the “acceptable” level of risk for each identified loss (see section 3.1.2);
 - k) the residual risk associated with each loss, ie the risk associated with each loss once the system is fully implemented and operational;
 - l) a justification for the acceptability of each residual risk against the agreed and documented top level dependability target.

4.2.3.4 Risk-Directed Design Framework

- 1 The project shall:
 - a) document a justification for achievement, by the design of the system, of acceptable residual risk, to a level of confidence appropriate for that risk.
 - b) document a justification that the design of risk reduction measures is appropriate for the level and importance of the risk reduction.



4.2.3.5 Modular Certification and Technical Modularity Framework

- 1 Where there is an organisational interface in which two different organisations have dependability responsibilities for different parts of the system that will work together, then modularity shall be used, and the module boundaries shall match the organisational boundaries.
- 2 Where the system interfaces to other systems, including systems that have not be assessed according to this Standard, these other systems shall be treated as modules (and their dependability properties shall be defined by a module boundary contract). Any properties of the other systems that this system relies upon to achieve its dependability shall be documented in the rely clause of the module boundary contract corresponding to this system.
- 3 Any assumptions about the operational environment in which the system will be deployed shall be documented in the context clause of the module boundary contract corresponding to this system, including the assurance requirement.
- 4 If the system is itself modular, and this modularity is used in achieving the dependability properties, then the requirements of the rest of this section shall be met.
- 5 A top-level module shall be defined whose contract is consistent with the dependability properties claimed in the system dependability case.
- 6 The top-level module shall be decomposed into a module hierarchy based on a logical grouping of responsibility for delivery of contributions to the system dependability properties.
- 7 The structure of the module hierarchy shall be documented.
- 8 Each module in the module hierarchy shall be defined using a module boundary contract, as specified in section 3.1.10.
- 9 The modules in the module hierarchy shall be composable, as defined in section 3.1.12.
- 10 All conflicts arising from module composition and their resolutions, shall be managed and documented.
- 11 For each module in the modular hierarchy of the system, evidence shall be recorded to show how its verification justifies the validity of the claims of its module boundary contract. In particular, there shall be evidence to show:
 - a) how the guarantee clauses of each module provide the dependability properties that have been apportioned to it in the design of the system;
 - b) how all conflicts in the composition of the modules of the module hierarchy have been resolved;
 - c) that all dependencies required by each module in its rely clause have been acceptably satisfied;
 - d) that all assumptions made by each module in its context clause are consistent with the operational context of the system;
 - e) how all counter-evidence contributed by each module in its counter-evidence clause has not caused the residual risk for any identified loss in the system to become unacceptable.



4.2.3.6 Evidence Framework

- 1 The project shall maintain evidence of:
 - a) plans & procedures used to meet the requirements of this Standard;
 - b) inputs and dependencies employed;
 - c) output of activities undertaken (e.g. documents, deliverables, etc.);
 - d) assurance that the requirements of this Standard have been met.
- 2 The evidence shall be:
 - a) permanently recorded, with adequate provision for back-up and disaster recovery;
 - b) protected against unauthorised interference or modification;
 - c) protected against unauthorised disclosure or loss to an extent suitable for the information contained.
- 3 The evidence shall be sufficiently comprehensive to allow:
 - a) any activities to be revisited or reviewed at any time in the life of the system;
 - b) responsibility for any activity or decision to be determined;
 - c) the impact of any change or error to be determined.

4.2.3.7 Evaluation / Assessment Framework

- 1 The project shall:
 - a) document a justification for demonstrating, by the implementation of the system, acceptable residual risk for each identified loss, to a level of confidence appropriate for that risk;
 - b) in agreement between the Customer, Supplier and Evaluator, document how the evaluator will verify the acceptability of each residual risk;
 - c) document a justification that the level of confidence, and the means of demonstrating acceptability, is appropriate for the risk.
- 2 The project shall:
 - a) document and implement a process for maintaining the validity of all approvals and certifications;
 - b) document and implement a process for identifying changes in the system, its environment or its mode of use that might affect the validity of its dependability argument, and implement any necessary changes to the system or its dependability case;
 - c) document and implement a process for tracking the operation of the system after deployment, confirming that its operation meets its dependability targets, and implementing any necessary corrective action.



4.3 G3: DSs are defined that mitigate all the identified losses

4.3.1 Context CG3

1 The residual risk associated with each identified loss is acceptable if it meets its dependability target.

4.3.2 Context CS2

- 1 Each risk mitigation argument provides a justification for the acceptability of the residual risk associated with each identified loss in the context of the operation of the system. The justification is based on the dependability specifications of the system (some of which may be abstracted and encapsulated into module boundary contracts where appropriate).
- 2 Any aspect of the justification of risk mitigation that is not covered by a system-level dependability specification or module boundary contract shall be recorded as an assumption in the system dependability case.

4.3.3 By goal breakdown

- 1 This goal shall be achieved by meeting the acceptance criteria for:
- a) G4: Causal analysis is sound; **and**
 - b) G8: Each DS is sound; **and**
 - c) G11: Causal analysis reflects the aggregate effects of DSs.

4.3.4 Directly

1 This goal shall be achieved by meeting the following acceptance criteria:

4.3.4.1 Unified Risk Management Framework

1 Section 4.2.3.3 shall apply.

4.3.4.2 Risk-directed Design Framework

- 1 The project shall document:
- a) all the Dependability Specifications for the system;
 - b) a justification that acceptable residual risk, to a level of confidence appropriate for that risk, is achievable for all of the identified losses, based on the collection of DSs;
 - c) and manage the conflicts that arise in the design of the components that are to implement the DSs, and their resolutions;
 - d) a justification that each DS is appropriate for the level and importance of the risk reduction.



4.3.4.3 Modular Certification and Technical Modularity Framework

- 1 Section 4.2.3.5 shall apply.
- 2 In addition:
 - a) the association between each module and its corresponding DSs shall be documented;
 - b) module boundary contracts of the modules in the hierarchy shall be used in lieu of their corresponding DSs, in the justification that acceptable residual risk is achievable for all of the identified losses.

4.3.4.4 Evaluation / Assessment Framework

- 1 The project shall document a justification for demonstrating, by the implementation of the dependability specifications, acceptable residual risk for each identified loss, to a level of confidence appropriate for that risk.
- 2 In addition, section 4.2.3.7 paragraphs 1b, 1c and 2 shall apply.

4.4 G4: Causal analysis is sound

4.4.1 Context CG4

- 1 A causal analysis is *sound* if it captures all causes for all identified losses in true cause/effect relationships, in the context of the system design and operation. This results in a correct assessment of the risk associated with each identified loss of the system.

4.4.2 By goal breakdown

- 1 This goal shall be achieved by meeting the acceptance criteria for:
 - a) G5: Sufficient losses are identified; **and**
 - b) G6: The causal basis of the identified losses is established; **and**
 - c) G7: All identified losses and other significant causal steps have associated severity and likelihoods defined.

4.4.3 Directly

- 1 This goal shall be achieved only by following the goal breakdown given above.



4.5 G5: Sufficient losses are identified

4.5.1 Acceptance Criteria

1 This goal shall be achieved by meeting the following acceptance criteria:

4.5.1.1 Unified Risk Management Framework

1 Section 4.2.3.3 paragraphs 1a through 1f shall apply.

4.5.1.2 Modular Certification and Technical Modularity Framework

1 The requirements for identification of loss at system level shall meet section 4.5.1.1 irrespective of the modular structure of the system.

2 Losses that may arise due to the behaviour of other systems that this system interfaces with shall be considered outside the scope of this system's dependability.

3 If the system is modular then section 4.2.3.5 paragraphs 1 through 8 shall apply.

4 In addition, the identification of relevant losses for the system shall also include assessments of the effect on the assets of the system, and within the system operational context, of:

- a) each module boundary contract (in particular the counter-evidence clause) in the module hierarchy of the system;
- b) any conflicts in the composability of the modules in the module hierarchy of the system (see section 3.1.12 paragraph 2);
- c) any conflicts in the composability of the system, with all other systems that the system interfaces to (see section 3.1.12 paragraph 1).

5 The results of these assessments shall be documented.

4.6 G6: The causal basis of the identified losses is established

4.6.1 Acceptance Criteria

1 This goal shall be achieved by meeting the following acceptance criteria:



4.6.1.1 Unified Risk Management Framework

- 1 A causal analysis of the identified losses shall be carried out and documented. The following properties of this analysis shall hold:
 - a) The behaviour of the system and the environment in which the system is used shall be specified accurately enough to ensure that the correct causal relationships are used;
 - b) The aspects of the system behaviour or design that are needed to perform the causal analysis shall be documented;
 - c) All causes of the identified losses shall be documented.
 - d) The justification of sufficient completeness of the causes of the identified losses shall be documented.
 - e) The process to ensure the causal analysis stays current and sufficiently complete in the face of any change, such as a change to the design or use, a change in the environment in which it is used, or modifications made (such as in-service fault fixing) shall be documented.

4.6.1.2 Modular Certification and Technical Modularity Framework

- 1 The causal analysis for the system shall meet the requirements of section 4.6.1.1 irrespective of the modular structure of the system.
- 2 In addition, in the cases where the assessments defined in section 4.5.1.2 paragraph 4 result in any update to the set of identified losses (due to modularity issues), the causal analysis shall include an analysis of how the modules that are identified in this update can contribute to the causes of these losses.

4.7 G7: All identified losses and other significant causal steps have associated severity and likelihoods defined

4.7.1 Context CG7

- 1 Within the causal analysis, every event that contributes directly or indirectly to the cause of an identified loss shall constitute a significant event.
- 2 Within the causal analysis, every use of a Dependability Specification or module boundary contract as a mitigation for a cause of an identified loss shall constitute a significant event.



4.7.2 Acceptance Criteria

1 This goal shall be achieved by meeting the following acceptance criteria:

4.7.2.1 Unified Risk Management Framework

1 For each identified loss, an impact analysis shall be carried out to determine the severity of each of the possible adverse consequences when the system sustains the loss.

2 The project shall document the set of significant events that contribute to the risk assessment process.

3 For each significant event in the causal analysis, the following characteristics shall be determined and documented:

- a) likelihood of event occurring (qualitative or quantitative);
- b) worst-case severity of the identified loss that the significant event can contribute to.

4 In addition, section 4.2.3.3 paragraphs 1i through 1l shall apply.

4.7.2.2 Modular Certification and Technical Modularity Frameworks

1 The impact analysis for each identified loss shall meet the requirements of section 4.7.2.1 irrespective of the modular structure of the system.

2 Where the analysis is modular, each contribution of an element in a clause of a module boundary contract to a cause or mitigation of an identified loss shall constitute a significant event.

3 When determining the residual risks of the identified losses in a modular system, the level of confidence in each entry in the guarantee clause of a module boundary contract shall depend on:

- a) the assurance requirement clause for the module;
- b) the impact on the guarantee clause of the entries in the counter-evidence clause for the module.

4.8 G8: Each DS is sound

4.8.1 Context CG8

1 A Dependability Specification is sound if it captures the necessary dependability characteristics and properties in a consistent, unambiguous, and complete specification, and has an associated assurance requirement that defines its acceptance criteria.



4.8.2 By goal breakdown

- 1 This goal shall be achieved by meeting the acceptance criteria for:
 - a) G9: DSs are realisable specifications; **and**
 - b) G10: Appropriate Assurance Requirements defined for each DS

4.8.3 Directly

- 1 This goal shall be achieved only by following the goal breakdown given above.

4.9 G9: DSs are realisable specifications

4.9.1 Acceptance Criteria

- 1 This goal shall be achieved by meeting the following acceptance criteria:

4.9.1.1 Risk-directed Design Framework

- 1 Section 4.3.4.2 paragraphs 1a and 1d shall apply.
- 2 Each Dependability Specification shall define properties that can be achieved directly by the system, so that it is possible for the system developer to ensure the system meets the DS completely, without relying on external behaviour of the domain.
- 3 Note: Although the implementation of a DS does not rely on external behaviour of the domain to implement its dependability properties, it may include interface control specifications that define interactions internal to the system, and also external interfaces. It may also include procedures that have to be carried out in the domain in order to achieve its specification.

4.9.1.2 Modular Certification and Technical Modularity Framework

- 1 If the system is itself modular, and this modularity is used in achieving the dependability properties, then the requirements of the rest of this section shall be met.
- 2 Section 4.2.3.5 paragraphs 5 through 10 shall apply.
- 3 A satisfaction argument for the validity of the mapping from each module boundary contract in the module hierarchy of the system, to its related set of dependability specifications, shall be documented.
- 4 Note: In contrast to a DS, a module boundary contract includes assumptions about its operational environment (in the context clause) and explicit statements of external dependencies (in the rely clause). Hence, whilst the DS specifies a claimed dependability property, the MBC specifies how a set of dependability properties will be realised in the context of the operation of the system.



4.10 G10: Appropriate Assurance Requirements defined for each DS

4.10.1 Context CG10

- 1 An assurance requirement for a Dependability Specification is *appropriate* if it is at a sufficiently high level of confidence for the DS to fulfil its risk mitigation role in the causal analysis.

4.10.2 Acceptance Criteria

- 1 This goal shall be achieved by meeting the following acceptance criteria:

4.10.2.1 Evaluation / Assessment Framework

- 1 Every Dependability Specification shall have a documented Assurance Requirement, as defined in section 3.1.5.
- 2 Together with the Assurance Requirement there shall be two further aspects documented, in agreement between the Customer, Supplier and Evaluators:
 - a) how the assurance requirement will be verified by the evaluator;
 - b) why the assurance requirement is deemed appropriate for the stated DS, including the rationale for any conflict resolution between the needs of different evaluators.

4.11 G11: Causal analysis reflects the aggregate effects of DSs

4.11.1 By goal breakdown

- 1 This goal shall be achieved by meeting the acceptance criteria for:
 - a) G12: A statement exists that explains how DSs mitigate losses; **and**
 - b) G13: DSs are together sufficient to achieve mitigation.

4.11.2 Directly

- 1 This goal shall be achieved only by following the goal breakdown given above.



4.12 G12: A statement exists that explains how DSs mitigate losses

4.12.1 Acceptance Criteria

1 This goal shall be achieved by meeting the following acceptance criteria:

4.12.1.1 Risk-directed Design Framework

1 For every Dependability Specification that contributes to risk mitigation, there shall be a justification of why the DS satisfies its contribution to that mitigation.

4.12.1.2 Modular Certification and Technical Modularity Framework

1 If the system is itself modular, and this modularity is used in achieving the dependability properties, then the requirements of the rest of this section shall be met.

2 For every module that contributes to risk mitigation, there shall be a justification of why the module boundary contract satisfies its contribution to that mitigation.

3 In addition, section 4.9.1.2 paragraph 3 applies.

4.13 G13: DSs are together sufficient to achieve mitigation

4.13.1 Acceptance Criteria

1 This goal shall be achieved by meeting the following acceptance criteria:

4.13.1.1 Risk-directed Design Framework

1 Section 4.3.4.2 paragraphs 1b and 1c shall apply.

4.13.1.2 Modular Certification and Technical Modularity Framework

1 Section 4.3.4.3 shall apply.

2 In addition, where multiple module boundary contracts contribute to the mitigation of a single risk, there shall be a justification that the MBCs mutually support each other, and work together consistently to achieve the mitigation.

4.13.1.3 Evaluation / Assessment Framework

1 Section 4.3.4.4 paragraph 1 shall apply.



4.14 G14: Actual system is shown to meet all DSs

4.14.1 Context CS2

1 Section 4.3.2 shall apply.

4.14.2 Context CS6

1 The evidence in support of the correct implementation of a DS is said to be *appropriate* if it meets the assurance requirement that is associated with the DS.

4.14.3 By goal breakdown

- 1 This goal shall be achieved by meeting the acceptance criteria for:
- a) G15: Actual system is complete; **and**
 - b) G16: Evidence relates to actual system; **and**
 - c) G17: Evidence shows that the system meets the DSs; **and**
 - d) G18: Evidence meets assurance requirement.

4.14.4 Directly

1 This goal shall be achieved only by following the goal breakdown given above.

4.15 G15: Actual system is complete

4.15.1 Context C15

- 1 The set of DSs that apply to the system shall be identified.
- 2 If the system is modular, the set of modules that are included in the system shall be identified.
- 3 The set of DSs applicable to a system, and the set of modules that are included in the system, provide the baseline against which completeness is judged. A system is said to be *complete* when all identified DSs and modules have been implemented.
- 4 The identification the correct set of DSs that apply to the system, and the correct set of modules that are included in the system, shall be maintained through all changes that may be made to the system in the course of its life.



4.15.2 Acceptance Criteria

- 1 This goal shall be achieved by meeting the following acceptance criteria:

4.15.2.1 Risk-Directed Design Framework

- 1 There shall be traceability between each Dependability Specification that applies to the system, and the set of uniquely identified components that are necessary to implement it.
- 2 All components that are required for the implementation of each Dependability Specification shall be implemented.
- 3 Procedures shall be documented to ensure that completeness of the system is maintained through all changes that may be made to the system in the course of its life.

4.15.2.2 Modular Certification and Technical Modularity Framework

- 1 The determination of completeness of the system shall meet the requirements of section 4.15.2.1 irrespective of the modular structure of the system.
- 2 If the system is modular, then all modules that are identified in the system architecture shall be implemented.

4.15.2.3 Evidence Framework

- 1 Section 4.2.3.6 shall apply to all evidence relating to this goal.
- 2 Each distinct instance of the system (including different versions and deployments) shall be uniquely identifiable and documented.
- 3 Where a system includes modules subject to a separate assessment, each module in the system architecture shall be uniquely identified, and its relationship with the unique identification of the system shall be recorded.
- 4 Each component that is included in the build of the system, and that is a separate configuration item, shall be uniquely identified, and its relationship with the unique identification of the system shall be recorded.
- 5 Evidence shall be provided to verify that the build of the system is complete, and consists of the correct versions of all modules and other configuration items.



4.16 G16: Evidence relates to actual system

4.16.1 Acceptance Criteria

1 This goal shall be achieved by meeting the following acceptance criteria:

4.16.1.1 Evidence Framework

- 1 Section 4.2.3.6 shall apply to all evidence relating to this goal.
- 2 There shall be traceability between each uniquely identified version of a system, and the evidence relating to the set of uniquely identified components that are included within it.
- 3 There shall be traceability between each Dependability Specification that applies to the system and the evidence relating to the set of uniquely identified components that are necessary to meet it.
- 4 There shall be traceability between each module included in the system architecture, and the evidence relating to the versions of the module components from which it is constructed.
- 5 Procedures shall be documented to ensure that the evidence traceability requirements of this Standard are maintained through all changes that may be made to the system in the course of its life.

4.17 G17: Evidence shows that the system meets the DSs

4.17.1 Acceptance Criteria

1 This goal shall be achieved by meeting the following acceptance criteria:

4.17.1.1 Risk-Directed Design Framework

- 1 The implementation of each component that is necessary to meet each Dependability Specification shall be verified, and evidence of the verification maintained.
- 2 Procedures shall be documented to ensure that evidence of re-verification of all components that are necessary to meet each Dependability Specification is maintained through all changes that may be made to the system in the course of its life.

4.17.1.2 Modular Certification and Technical Modularity Framework

- 1 The evidence of verification of all components that are necessary to implement the dependability properties of the system shall meet the requirements of section 4.17.1.1 irrespective of the modular structure of the system.
- 2 The implementation of each module shall be verified, and evidence of the verification maintained.



4.17.1.3 Evidence Framework

- 1 Section 4.2.3.6 shall apply to all evidence relating to this goal.
- 2 A plan shall be produced showing the means by which the satisfaction of each Dependability Specification and each module boundary contract (if the system is modular) is established.
- 3 Evidence shall be recorded to justify how each Dependability Specification is met by the verification of the set of components in the actual system that are necessary to meet it.
- 4 If any evidence of meeting a Dependability Specification is related to the components of the actual system through any sort of transformation or production process, additional evidence shall be recorded showing that the process correctly preserves the implementation of the DS.
- 5 If the system is modular, then section 4.2.3.5 paragraph 11 shall apply.
- 6 Procedures shall be documented to ensure that satisfaction of all Dependability Specifications that apply to the system, and justification of the validity of the claims in each module boundary contract, is re-established in accordance with the practices of this Standard, through all changes that may be made to the system in the course of its life.

4.18 G18: Evidence meets assurance requirement

4.18.1 Acceptance Criteria

- 1 This goal shall be achieved by meeting the following acceptance criteria:

4.18.1.1 Evidence Framework

- 1 Section 4.2.3.6 shall apply to all evidence relating to this goal.
- 2 The type of evidence shall be appropriate for each Dependability Specification and module boundary contract that is being shown to be met, and shall be appropriate to meet the requirements imposed by the associated assurance requirement . Justification of appropriateness shall be documented where necessary.
- 3 Evidence shall be managed by means sufficient to preserve and demonstrate its validity over time and any changes.
- 4 All validation and verification processes, including analyses, reviews, inspections, and testing-related activities, shall be carried out to agreed plans or descriptions that are compliant with the assurance requirements.



- 5 All results from validation and verification processes shall be documented, and sufficient information on these processes and their environment shall be recorded to allow the processes to be repeated at any time during the life of the product.
- 6 Any infrastructure or tools used in the validation and verification processes, and in other evidence generation, shall be sufficiently robust to the level in which trust is put in it, as required by the assurance requirements.

4.18.1.2 Evaluation / Assessment Framework

- 1 For each DS and module, the process to generate and record the evidence shall support the level of confidence in the evidence required by the AR.
- 2 There shall be a justification of why the level of confidence in the evidence required by the AR is not reduced to an unacceptable level, in the context of the system, for a DS by:
 - a) any conflicts that arise in the design of the components that are to implement the DS;
- 3 and for a module by:
 - a) any conflicts in the composability of the module with other modules in the module hierarchy of the system;
 - b) any counter-evidence applicable to the module that is recorded in its module boundary contract.
- 4 Section 4.2.3.7 paragraph 2 shall apply with respect to maintaining the necessary confidence that the evidence continues to satisfy the AR over any changes to the system or environment.



A Informative Annexes

A.1 Informative References

- A. Managing Successful Projects with PRINCE2, Office of Government Commerce, 2002.
- B. **SafSec** Methodology: Guidance Material, Praxis High Integrity Systems document S.P.1199.50.3 (Issue 3.0), 5th August 2005.
- C. T. P. Kelly: Arguing Safety – A Systematic Approach to Managing Safety Cases, University of York, YCST 99/05.
- D. Avizienis A., Laprie J.C., Randell B.: Fundamental Concepts of Dependability. Technical Report 739, pp. 1-21, Department of Computing Science, University of Newcastle upon Tyne, 2001.
- E. C.B. Jones, Specification and design of (parallel) programs. In *Proceedings of IFIP '83*, pages 321-332. North-Holland, 1983.

Normative references, cited as [1], [2], etc. are listed in section 2.



Document Control and References

Praxis High Integrity Systems Limited, 20 Manvers Street, Bath BA1 1PX, UK.
Copyright © Praxis High Integrity Systems Limited 2005. All rights reserved.

Changes history

Issue 0.1 (17/7/2003): Created from S.P1199.50.4 (Structure of Standards and Guidance)

Issue 0.2 (23/7/2003): Updated after internal SafSec review.

Issue 0.3 (28/7/2003): Updated after review by Tim Kelly, University of York.

Issue 1.0 (28th July 2003): First issue to the client.

Issue 1.1 (6th August 2003): Draft of new treatment of modularity added after meeting on 5th August.

Issue 1.2 (15th September 2003): Draft baselined before possible change to GSN.

Issue 1.3 (24th September 2003): Draft for review before final workshops

Issue 2.0 (25th September 2003): Provisional issue for discussion in workshop 1 October.

Issue 2.1 (10th October 2003): Draft with tracked changes for internal review, incorporating all the comments from the workshop of 1st of October and the security discussion of 7th of October.

Issue 2.2 (13th October 2003): Draft for review by Tim Kelly.

Issue 2.3 (20 November 2003): Draft incorporating comments from Tim Kelly and John Clark, ready for final review by sponsor.

Issue 2.4 (28 November 2003): Internal review comments incorporated.

Issue 2.5 (25th March 2004): External review comments incorporated.

Issue 2.6 (13th May 2004): Website distribution additions

Issue 2.7 (5th August 2005): Updates resulting from the Case Studies.

Issue 3.0 (12th August 2005): Definitive version incorporating internal review comments

Issue 3.1 (2nd November 2006): Change URL reference for SafSec website.



Changes forecast

None.