Safety Regulation Group

Acceptable Means of Compliance to CAP 670 SW 01

Guidance for Producing SW 01 Safety Arguments for COTS Equipment

www.caa.co.uk

© 2010 Civil Aviation Authority.

All rights reserved. Copies of this publication may be reproduced for personal use, or for use within a company or organisation, but may not otherwise be reproduced for publication.

To use or reference CAA publications for any other purpose, for example within training material for students, please contact the CAA at the address below for formal agreement.

First issue 9 September 2008
Issue 2 September 2009
Issue 3 March 2010

Enquiries regarding the content of this publication should be addressed to:

Air Traffic Standards, Safety Regulation Group, Civil Aviation Authority, Aviation House, Gatwick Airport South, West Sussex, RH6 0YR.

The latest version of this document is available in electronic format at www.caa.co.uk, where you may also register for e-mail notification of amendments.

Contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide guidance to Air Navigation Service Providers (ANSPs) and their suppliers on addressing the objectives of CAP 670 SW 01 (Reference 1) when deploying COTS equipment.

This Guidance only addresses the safety assurance required by SW 01 for the software content of Commercial Off The Shelf (COTS) equipment. It therefore does not replace the need to demonstrate satisfaction of the System Safety Requirements in the manner required by the ANSP's Safety Management System (SMS) or as specified in the applicable contract for equipment supply.

1.2 Background

The CAA published SW 01 in CAP 670 in December 2002. The primary objective of SW 01 is to 'ensure that the risks associated with deploying any software used in a safety related ATS system have been reduced to a tolerable level'.

Though all parties agree that the principles behind SW 01 are sound (discussed in Reference 2), it has become apparent that ANSPs are unclear how to address the objectives of SW 01 in a satisfactory manner. Consequently, SRG plans to publish a working understanding of the arguments and types of evidence that can demonstrate satisfaction of the objectives of SW 01 for:

a) a bespoke software development project;

b) a significant modification to a legacy system;

c) assurance of COTS equipment (e.g. a modem); and

d) a bespoke equipment development project that uses procured COTS software (e.g. a tracking subsystem; a database or an Operating System).

This Guidance covers point c) in the list 'Assurance of COTS equipment'.

This Guidance provides support for ANSPs utilising COTS equipment in developing an SW 01 argument in two ways:

- Firstly, this Guidance outlines example safety arguments for addressing SW 01 for COTS equipment, illustrated using 'Claim – Argument – Evidence' (CAE) diagrams (see Annex A1).
- Secondly, this Guidance provides ANSPs with a way to determine what evidence is necessary to support the SW 01 argument and, from this, the activities necessary to develop the evidence.

This Guidance is based on understandings of industrial practice as it existed in 2005, and so will be updated and maintained to reflect developments in industrial practice and better understanding of arguing COTS compliance with SW 01 (see Annex L Roadmap).

ANSPs and assessors can use the checking aid in Annex M when preparing the submission and verifying whether the submission complies with this guidance. It is recommended that ANSPs exceed the guidance given in this document by actively seeking to develop a fuller understanding of the best arguments to make regarding SW 01 compliance, and by generating more objective and specific evidence of satisfaction of each of the five SW 01 sub-objectives.

1.3 Scope

The Guidance is concerned solely with the software assurance required by SW 01 and does not address how it is integrated with the system safety assurance.

This Guidance applies specifically to satisfying SW 01 objectives for COTS equipment; in so doing, it does not replace the need to fully meet the requirements of the ANSP’s own Safety Management System (SMS) with regard to software assurance.

The term ‘COTS equipment’ refers to equipment that is a standard product from a manufacturer. Some examples could be:

- a network hub/switch/router; and/or
- a modem.

Whilst the arguments in this Guidance preclude its use for more complex COTS equipment (such as Voice Switches and Radar Data Processing Systems) during stage 1 of the Roadmap (Annex L), its use for such equipment will be permitted.

However, it is (and will remain) valid to apply this Guidance to equipment that is an assembly or COTS modules, provided that:

1 The architecture of the equipment permits arguments to be made that the equipment safety requirements have been validly apportioned to safety requirements for the modules within the COTS equipment; and

2 Detailed design information and evidence are available to support the arguments made in the 10^{-4} Guidance at the module level.

This approach is consistent with that discussed in the Rationale (Annex K). In future stages of the Roadmap, this Guidance will define constraints for how modularisation in 1 above should be argued.

If there is no software in the equipment, or none of the safety functions of the equipment are provided or affected by the software, then there is no need to make claims against the objectives in SW 01. However, an argument substantiating the claim that SW 01 does not apply is required in the safety case. Guidance on some such cases is provided in Reference 4.

1.4 Limitations on Applicability

This Guidance is applicable to COTS equipment that meets a set of conditions defined in paragraph 2.3 below. Failure to meet these conditions will mean that this Guidance cannot be applied and an alternative method of satisfying the SW 01 objectives will need to be used.

This Guidance cannot be applied to software in isolation from the target platform on which it is to run, e.g. this Guidance cannot be used to provide assurance of an Operating System on its own.

This Guidance cannot be used to argue for multiple pieces of equipment unless they can be shown to be identical (hardware and software). If they cannot be shown to be identical they are assumed to be different, and separate evidence will need to be generated for them. It is not uncommon for COTS equipment with identical part numbers to have different software versions or hardware components. When an argument addresses the installation of multiple identical equipments, the supporting test evidence must be valid for each installation.

1.5 Initial Reading

Before using the guidance given here, the reader should be familiar with the software safety objectives and the behavioural attributes of a Software Safety Requirement defined in SW 01 of CAP 670.

2 Assurance Approach

2.1 Overview

This section provides a description of the steps that an ANSP needs to follow when applying this Guidance. The steps are listed below and each one is expanded upon in the following sections:

Step 1: Set valid Safety Requirements

Step 2: Present Arguments that the Conditions for the use of the Guidance are met

Step 3: Present Arguments that the SW 01 objectives are satisfied

Step 4: Present evidence underpinning the argument

Step 5: Claim compliance with this AMC

2.2 Step 1 - Set Valid Safety Requirements

The ANSP should follow its SMS to establish Safety Objectives, through a process of hazard analysis and risk assessment, and define System Safety Requirements to control hazard rates to be tolerable and to specify mitigations. The System Safety Requirements are refined according to the system architecture, down to the level of the COTS equipment. The System Safety Requirements will normally be documented in a 'Requirements Safety Case' (sometimes referred to as a Safety Case Part 1).

System Safety Requirements are defined to address hazards and provide mitigations. They express the tolerable rate of specific failure modes of a function. A complete set of System Safety Requirements for a safety-related function addresses each behavioural attribute[1], unless it has been justified as having no impact on safety. For example:

'The probability that position information is inaccurate (position incorrect by more than 2 NM but less than 10 NM) due to the Radar Data Processor (RDP) shall be no greater than 6.0 x 10^{-4} per hour.[2]'

The example probability would have been arrived at by:

- Using a Functional Hazard Assessment (FHA), HAZOPS or FMECA process to identify potential effects at the level at which their severities are classified by the ANSP.
- Using the ANSP's Risk Classification Scheme to identify the broadly acceptable rate of occurrence of these potential effects.
- Defining and documenting the available mitigations as new or enhanced Safety Requirements.

[1] See 'Glossary and Definitions'

[2] This figure is given for illustration only, and should not be assumed to apply to any particular RDP.

- Apportioning the acceptable rate of occurrence across all the sub-systems involved in the sequence of event leading to each effect, and by taking account of the mitigations. This defines the tolerable rate for the safety requirement with respect to each hazard. The hazards and their tolerable rates, together are known in Single European Sky legislation as Safety Objectives.

Determining and analysing the available mitigations is one of the most important parts of the above process, as it may reduce the integrity required from the equipment. The reduced integrity requirement increases the feasibility of selecting equipment for which it is possible to successfully generate the required safety assurance evidence, and prevents the need to select over-engineered equipment to meet an unnecessarily onerous target (see *CAP 760 Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases*, Appendix D, Using Event Diagrams for an example of analysing the effect of mitigation).

2.2.1 Form of Safety Requirements

This Guidance depends on Safety Requirements being stated in a manner such that they can be tested, as testing provides the primary evidence to support the requirements satisfaction argument. The Safety Requirement must therefore precisely identify what must be tested, and specify objective limits beyond which the Requirement is not met. Failure to properly specify Safety Requirements affects the practicality of providing assurance that they are met.

In the past it has been common practise to derive a single Safety Requirement to address one ‘corruption’ hazard for several disparate parameters/attributes, for example, “The probability of corruption of Radar Data due to the RDP shall be no greater than 6.0 x 10^{-4} per hour”. The problem with this form of Requirement is that the individual end effects and mitigations can be very different for each parameter/attribute, such that the tolerable rate of occurrence for each Safety Requirement could be very different. It is also extremely difficult to test for ‘corruption’ when it is not properly identified.

Additionally, the Requirement must properly define limits beyond which the parameters would be considered incorrect. A Requirement such as “The probability that position information is inaccurate due to the Radar Data Processor (RDP) shall be no greater than 6.0 x 10^{-4} per hour” fails to do this.

Therefore, the various aspects that are commonly referred to incorrectly as ‘corruption’ could be specified as follows:

> “The probability that position information is inaccurate (position incorrect by more than 2 NM but less than 10 NM) due to the Radar Data Processor (RDP) shall be no greater than 6.0 x 10^{-4} per hour.”
>
> “The probability that position updates are delayed (by more than 2 seconds) due to the Radar Data Processor (RDP) shall be no greater than 4.0 x 10^{-3} per hour.”
>
> And similarly for incorrect call-sign, altitude, etc.

It is sometimes necessary to specify several Safety Requirements in respect of one behavioural attribute, for example, for different levels of inaccuracy or different time periods. In the case of accuracy, small inaccuracies may be unlikely to lead to accidents, and large inaccuracies may be incredible, so that large and small inaccuracies may be permitted to occur at higher rates than the ‘grey area’ in between.

2.3 Step 2 – Present Arguments that the Conditions for the use of the Guidance are met

The argument and evidence Requirements of this guidance are only valid (provide adequate assurance) under certain circumstances, which are listed below. Failure to meet these means that this Guidance cannot be applied and an alternative method of satisfying the SW 01 objectives must be used.

Therefore, in order to use this SW 01 COTS Guidance it is necessary to claim that it is valid for the ANSP's application of COTS equipment by presenting arguments that demonstrate that the following are satisfied:

1 **The COTS item is an equipment.** This Guidance cannot be applied to software in isolation from the target platform on which it is to run, e.g. this Guidance cannot be used to provide assurance of an Operating System on its own. A simple statement suffices to satisfy this pre-requisite.

2 **The COTS equipment has an adequate equipment specification**. The COTS equipment specification must be sufficiently detailed to demonstrate implementation of the System Safety Requirements.

3 **The most onerous integrity Requirement on an individual COTS equipment is no worse than 1 x 10^{-5}** occurrences per hour. An acceptable argument is that none of the Equipment Safety Requirements have an integrity Requirement more onerous than 1 x 10^{-5} per hour. This pre-requisite is based upon the limits of credibility of the evidence stipulated in this Guidance.

4 **Equipment monitoring Requirements are specified in the associated System Safety Case.** An acceptable argument (from the time that the COTS equipment enters service) is that the in-service monitoring Requirements are documented in the associated System Safety Case (in accordance with the ANSP's SMS), and that these requirements monitor the behaviour specified in the COTS Equipment Safety Requirements.

For submissions addressing more than one equipment:

5 **The argument and evidence apply to all equipments.** If the submission covers more than one deployment of the equipment, then a short argument must be provided, addressing the multiple equipment issues in Section 1.4.

Warning: Whilst the following additional conditions must be met in order to use this Guidance they do not form part of the argument required above, as they are addressed in the argument templates:

1 **The Safety Objectives must have been set at a 'broadly acceptable' level (see RS 1.1.1)**. This establishes the acceptability of low confidence, as discussed in the rationale Annex K.

2 **The Safety Requirements are all expressed in terms of the COTS equipment outputs (see RS 1.1.2)**. The System Safety Requirements have to be derived in accordance with the ANSP's SMS, and allocated/apportioned among the system components to define safety requirements for the COTS equipment that are observable.

3 **All the equipment behaviour specified in the COTS Equipment Safety Requirements are testable (see RS 1.1.3)**. The behaviour specified by the COTS Equipment Safety Requirements can be stimulated using the equipment inputs and the available test facilities. The practicality of this limits the complexity of the equipment for which this Guidance can be used.

2.4 Step 3 – Present Arguments that the SW 01 Objectives are Satisfied

Using the templates provided in this guidance, the ANSP presents the argument that the objectives of SW 01 have been met. This Guidance provides arguments (the rationale for which can be found in Annex K of this document), illustrated by Claim, Argument and Evidence (CAE) diagrams as follows:

- Annex B covers the Arguments and CAEs for software in equipments with Safety Requirements no more onerous than 1×10^{-4}, for COTS equipment that meet the conditions of paragraph 2.3.
- Annexes C to G cover the Arguments and CAEs for software in equipments with Safety Requirements no more onerous than 1×10^{-5}, for COTS equipment that meet the conditions of paragraph 2.3.

The safety case documentation must contain the textual arguments from the Annexes, but the ANSP may choose whether or not to replicate the CAE diagrams.

ANSPs are free to use an alternative argument representation such as Goal Structuring Notation (GSN), provided the argument is completely equivalent.

The arguments and CAE diagrams shown in this Guidance need minor tailoring to cover variations in the evidence actually provided to support the arguments. For example, using the COTS Evidence Evaluation Tables (CEET) from Annexes I and J allow different combinations of evidence to support the arguments; the actual CAEs (or other argument form) used should indicate the actual evidence used and provide explicit references.

Text in ***italics*** in the template arguments provides explanations and information on the presentation of the argument, and should **not** be included in an actual software safety submission.

To assist ANSPs with the preparation of their CAEs, editable electronic copies are available from:

Air Traffic Standards
Safety Regulation Group
Civil Aviation Authority
Aviation House
Gatwick Airport South
West Sussex
RH6 0YR

e-mail: ats.enquiries@caa.co.uk

Annex A provides more information on CAE construction.

2.5 Step 4 - Present Evidence Underpinning the Argument

To satisfy the objectives of SW 01 it is not sufficient to merely present or refer to the CAE arguments; evidence specific to the use of the equipment is also required to support and justify the arguments.

The ANSP must generate and/or collect the required evidence and embed specific references to the evidence in the arguments. The evidence used in the argument must be examined when preparing the software safety submission to ensure that it is suitable (e.g. relevant, adequate and credible). The ANSP must have access to the evidence for its own evaluation, or for SRG audit purposes.

This Guidance includes COTS Evidence Evaluation Tables (CEETs) that define the only permitted options for the evidence that needs to be provided to support the given 'Requirements Satisfaction' argument. The CEETs cover 'Integrity Assurance' and 'Functional Assurance' of Safety Requirements separately by awarding assurance points for various types of evidence. The arguments for the other SW 01 objectives require the same evidence to be provided in all cases, as shown in the relevant CAE Annexes (see 2.7 below), so no CEETs are provided for these.

The CEETs include some criteria (Evidence Satisfaction Criteria) that the evidence must satisfy to be acceptable.

Often it is sufficient to just include a reference to the evidence. However, sometimes it is necessary to show explicitly how the available evidence supports the arguments, particularly in the Requirements Satisfaction argument. For example, in presenting Site Acceptance Testing (SAT) results, it would be necessary to show which Safety Requirements have been successfully and fully exercised by which SAT tests, e.g. through provision of a matrix linking Safety Requirements to the specific SAT tests.

2.6 Case 1 Equipment with Safety Requirements no more Onerous than 1 x 10^{-4}

The 1 x 10^{-4} CEETs in Annex I must be used to justify that sufficient evidence is presented to satisfy the 'Requirements Satisfaction' argument of Annex B. A score of 100 assurance points or more must be accumulated from the Integrity Assurance CEET and a further 100 assurance points must be accumulated from the Functional Assurance CEET.

2.7 Case 2 Equipment with Safety Requirements no more Onerous than 1 x 10^{-5}

The necessary evidence for equipment with Safety Requirements no more onerous than 1 x 10^{-5} breaks into three categories:

- A fixed set of evidence that must be developed in all cases to support the arguments provided (for all five of the SW 01 sub-objectives).
- Acceptable combinations of (types of) Requirement Satisfaction evidence defined by the CEET from which the ANSP can choose, according to the evidence available.
- Additional ANSP-defined evidence to support the Requirements Traceability and Non-Interference arguments.

2.7.1 Fixed Evidence

The following must be provided for COTS Equipment Safety Requirements no more onerous than 1 x 10^{-5}:

- the ‘Requirements Validity’ argument and evidence shown in Annex C;
- the ‘Configuration Consistency’ argument and evidence shown in Annex D;
- the ‘Requirements Traceability’ argument shown in Annex F (no fixed evidence is required over and above that required for ‘Requirements Validity’); and
- The ‘Non Interference’ argument shown in Annex G (no mandatory evidence is required over and above that required for ‘Requirements Satisfaction’).

2.7.2 Acceptable Combinations of Evidence Defined using the CEET

The 1 x 10^{-5} CEET in Annex J should be used to justify that sufficient evidence is available to support the ‘Requirements Satisfaction’ argument (Annex E). A score of 100 points or more should be accumulated from the Integrity Assurance CEET and 100 points should be accumulated from the Functional Assurance CEET.

2.7.3 Additional ANSP-defined Evidence

This is evidence that SRG cannot pre-define at this stage. The ANSP must identify suitable evidence to support certain arguments. Guidance on this is provided at applicable points in the template arguments provided in the annexes.

2.8 Step 5 – Claim Compliance with this AMC

The ANSP must claim that this guidance has been complied with. This claim should provide assurance that the AMC has only been modified in those areas permitted by the guidance. This claim should be supplemented with explanations of how the ANSP has chosen to present the arguments, e.g. with respect to the satisfaction of multiple groups of Safety Requirements.

ANSPs and assessors can use the checking aid in Annex M to verify compliance with this guidance. ANSPs may wish to complete this checking aid and include it in the submission to support their claim of compliance.

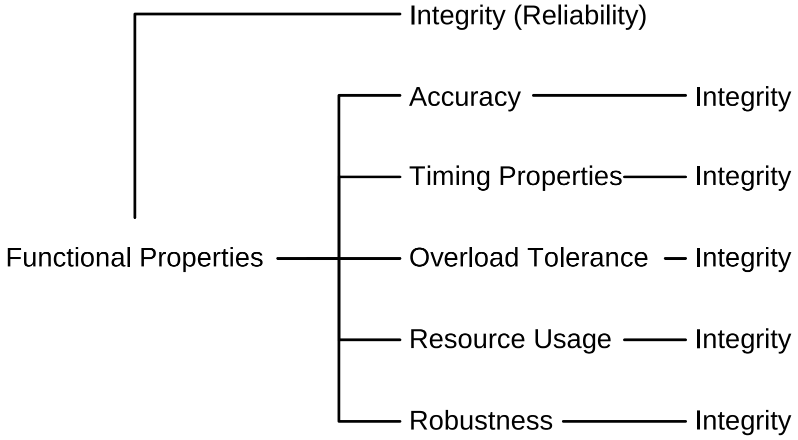
3 Glossary and Definitions

AMC — Acceptable Means of Compliance

ANSP — Air Navigation Service Provider

Architectural Unit (AU) — An AU is defined as, a set of elements protected against interference and may be hardware or software. A feature of an AU is that it can be assessed independently.

Behavioural attributes — “Functional properties, Timing properties, Robustness, Reliability, Accuracy, Resource usage, Overload tolerance” (as defined in SW 01). The relationship between the Behavioural attributes is illustrated below:



CAA — Civil Aviation Authority

CAP 670 — Civil Aviation Publication 670, *Air Traffic Services Safety Requirements* (Reference 1)

CAE — Claims- Arguments - Evidence (diagram)

CC — Configuration Consistency

SW 01 Sub-Objective E - To ensure that the arguments and evidence, for the safety of the software in the system context, are from a known executable version of the software and a known set of software products, data and descriptions that have been used in the production of that version.

CEET(s) — COTS Evidence Evaluation Tables

Composable relationship — Composable relationship relates to the demonstration that lower level requirements / specifications collectively are fully equivalent to a parent requirement / specification.

COTS — Commercial Off The Shelf [in this guidance it relates to equipment that is commercially available with little or no modification].

Equipment — Equipment within the scope of this guidance comprises Hardware and Software.

This Guidance applies to software in equipment and cannot be used for Hardware components or Software components in isolation.

Evidence Satisfaction Criteria

These are contained in appropriate rows of the CEET, and set minimum criteria for evidence to be valid so that the associated assurance ‘points’ can be claimed.

FAT

Factory Acceptance Testing can be used to show that the equipment meets the supplier product specification or the customer specification or a combination of both. Usually, simulated data is required to exercise the full range of the input domain. This testing is normally conducted at the manufacturer’s premises before the equipment is installed on site.

FHA

Functional Hazard Assessment

FMECA

Failure Mode Effects and Criticality Analysis

GSN

Goal Structuring Notation

HAZOPS

HAZard and **OP**erability **S**tudy

Mandatory

Compulsory if this guidance is used by an ANSP as its means of compliance with SW 01.

Integrity

The probability or rate of failure to meet a specification.

Note: This is not constrained to complete loss of function but addresses all of the attributes of a requirement and the addition of unintended behaviour.

NI

Non-Interference

SW 01 Sub-Objective D - To ensure that functions implemented as a result of Software Safety Requirements are not interfered with by other functions implemented in the software.

PSSA

Preliminary System Safety Assessment

RCS

Risk Classification Scheme

Requirements Safety Case

That part of a system safety case which provides arguments and evidence that the System Safety Requirements therein (or referenced) are valid (correct and complete). It may be presented as a separate document (sometimes known as a Safety Case Part 1) or a specific section of a wider safety case report.

Roadmap

An outline of the future enhancements required to this guidance and supporting material. See Annex L.

RS

Requirements Satisfaction

SW 01 Sub-Objective B - To ensure that arguments and evidence are available which show that the software satisfies its Safety Requirements.

RT

Requirements Traceability

SW 01 Sub-Objective C - To ensure that arguments and evidence are available which show that all Safety Requirements can be traced to the same level of design at which their satisfaction is demonstrated.

RV

Requirements Validity

SW 01 Sub-Objective A - To ensure that arguments and evidence are available which show that the Software Safety Requirements correctly state what is necessary and sufficient to achieve tolerable safety, in the system context.

Safety Requirement

In the context of this guidance, a Requirement that defines safety behaviour such that a Safety Objective will be satisfied. Each Safety Requirement is specified in terms of Behavioural Attributes.

Safety Objective

The definition of a hazard together with a qualitative or quantitative definition of the maximum frequency or probability at which the hazard can occur in order to meet safety targets.

SAT

Site Acceptance Testing is intended to show that the equipment will work in the operational environment and typically meets that sub-set of its specification that will be used operationally when supplied with data from real interfaces.

SES

Single European Sky – European legislation EC 549/2004, EC 550/2004, EC 2096/2005 and EC 482/2008.

SMS

Safety Management System. Under SES legislation ANSPs must have an SMS that is compliant with EC 2096/2005 in order to be Certificated.

State Space

The State Space is the set of logical states that a component or system, normally a software system, can assume.

SW 01

Regulatory Objectives for Software Safety Assurance in ATS Equipment (Reference 1)

The prime objective of SW 01 is “To ensure that the risks associated with deploying any software used in a safety related ATS system have been reduced to a tolerable level”. SW 01 does not apply to electronic items such as application specific integrated circuits, programmable gate arrays, solid-state logic controllers or software requirements that can be demonstrated not to affect safety (SW 01, Part 1, Paragraph 2.3).

4 References

1. CAA, CAP 670 *Air Traffic Services Safety Requirements*, Part B Section 3 ‘Systems Engineering’, section SW01, www.caa.co.uk/cap670.

2. *The Practicalities of Goal-Based Safety Regulation*, J Penny and A Eaton, CAA (SRG), PG Bishop, RE Bloomfield (Adelard), http://www.adelard.co.uk/resources/papers/pdf/scsc2001_sw01.pdf.

3. CAA, CAP 760 *Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases*, www.caa.co.uk/cap760.

4. CAA, AMC to CAP 670: Guidance on Reasoning that SW 01 does not apply to a Change, www.caa.co.uk/amctocap670.

ANNEX A ARGUMENT TEMPLATES FOR 1 X 10^{-4} AND 1 X 10^{-5} REQUIREMENTS

Paragraph 1 introduces the notation used to illustrate arguments and paragraph 2 explains the use of the template arguments in Annexes B to G.

A.1 Claims-Argument-Evidence (CAE) Diagrams

SW 01 requires that arguments and supporting evidence are available to show that the risks associated with deploying any software used in a safety related ATS system have been reduced to a tolerable level.

While this argument is documented as text, it is helpful to use diagrams to illustrate the structure and relationship of the various parts of the argument. There are two points in the process at which diagrams are most useful. The first, being the planning stage, where the actual evidence that needs to be produced is being defined. The second is when presenting the final safety argument that the COTS equipment will be tolerably safe to operate in its operational environment.

For the author of an argument, such diagrams define distinct parts of the argument, helping to keep each part directly relevant to a specific issue. It follows that such diagrams may be used to prepare an argument without necessarily forming part of the final presentation of the argument. However, for the reader, the diagrammatic representation of the argument is very helpful, being the equivalent to the contents list of a book, as it shows the elements of the argument, where to find them, and the way that they relate to support the top most claim.

Two diagram types are commonly used: Goal Structuring Notation (GSN) and Claims – Argument - Evidence (CAE). CAE diagrams are used in this document, but readers familiar with GSN can easily construct an equivalent GSN structure. Examples of GSN are given in CAP 760 (Reference 3).

The use of 'Claims – Argument - Evidence' diagrams in this Guidance document is explained here.

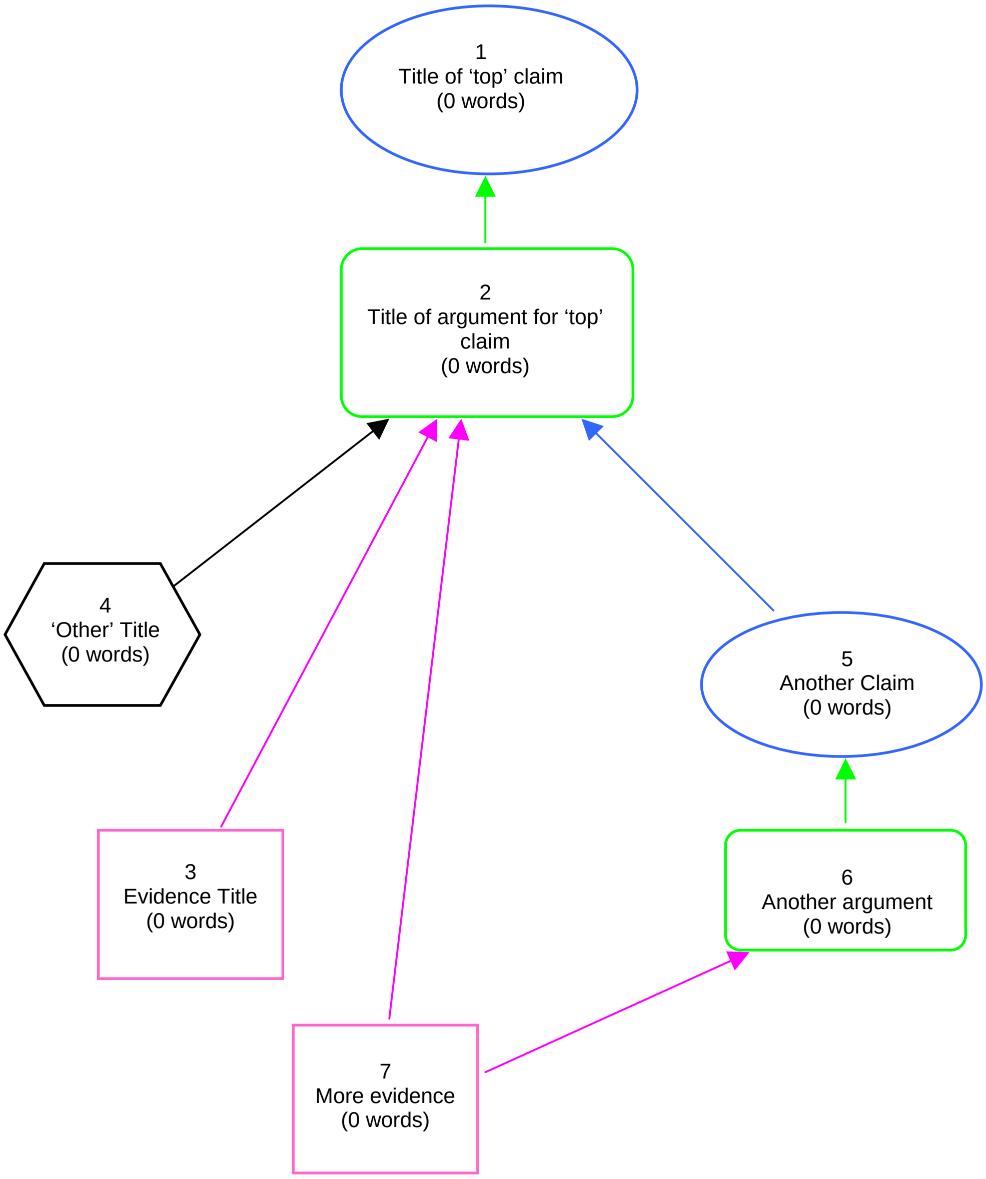
The meaning of the following words in this context is:

- Claim - an assertion, the truth of which is subsequently reasoned;
- Argument - A course of reasoning aimed at demonstrating truth or falsehood;
- Evidence - objects (e.g. maps, records, diagrams, documents or models) that, if believed, immediately establish the factual matter to be proved, without the need for inferences[2].

A CAE diagram therefore shows an assertion that something is true: the Claim. The claim is substantiated by reasoning that it is true: the Argument. The argument is supported by Evidence. An illustrative fictional CAE diagram is shown below, followed by an explanation of each element.

[2] If inferences are required the item is not evidence but in fact a claim that has to be substantiated with further argumentation.

Example CAE Diagram



CAE diagrams use four types of node, linked by lines that show their supporting relationships. Items 1 and 5 represent claims (circles or ellipses). Items 2 and 6 represent arguments (round-cornered squares or rectangles). Items 3 and 7 represent items of evidence (squares or rectangles). Item 4 is an 'other' node, which does not strictly form part of the argument, but is used for whatever purpose is useful – context, annotations, etc. The size and aspect ratio of a node is not significant.

Each node represents a fragment of a complete argument. The important features of each node are:

- The node’s type – claim, argument, evidence or ‘other’.
- The node’s relationship to other nodes – see below.
- The node’s title, as shown on the diagram – note that this is just a title which is usually just a summary of the information it represents.
- The relationship between the node symbol and the fragment of the argument.

The overall argument starts with the desired top safety claim. Each claim must be supported by one or more arguments (usually only one). Argument nodes must be supported by at least one (sub-) claim or evidence node[3]. Evidence nodes are not supported, as they represent items that exist, and cannot directly support a claim without an intervening argument. The bottom-most nodes are therefore always evidence nodes. A (sub-) claim may support more than one argument and, similarly, an item of evidence may be used by more than one argument to show the same or different things.

There is no definitive convention for titling argument nodes, some approaches being:

- Repeat the claim verbatim;
- Use no words, just a reference to the full argument (because a summary may be misleading);
- Attempt to summarise the argument, in a bottom-up manner;
- Attempt to provide a continuing narrative from the claim, providing the reason that the claim is true, for example starting “As …”.

It is recommended that a single approach is adopted consistently throughout an overall argument. In this document, the last of these is used.

For ANSPs that do not have a proprietary safety argument tool, the CAE diagrams in this Guidance have been re-created using standard office software. Nodes usually have a numeric reference (1 to 7 are used above), which can be used as the section number of the document containing the relevant fragment of the argument, or a document reference for an evidence item.

The nodes may be coloured to reinforce the difference in shape: in this document, claim nodes are blue, argument nodes are green, evidence nodes are magenta, and ‘other’ nodes are grey.

[3] In theory, an argument could comprise self-evident assertion, assumptions etc., which could be represented as unsupported sub-claims, but in practice these are subsumed directly into the text in the argument node. Therefore, the theoretical case where there is an unsupported argument node does not occur in practice.

Where a proprietary tool is used that stores the diagram and all the text of the claims, arguments and evidence, there is a tendency to think of the diagram as the safety argument. The diagram on its own is not sufficient; all the fragments of the argument are required. Moreover, all evidence items referenced in the argument form an integral part of the safety argument.

A.2 Argument Templates Annexes B to G

A.2.1 Templates

Annex B provides a template of an acceptable argument that addresses the objectives of SW 01 for equipment with Safety Requirements no more onerous than $1x10^{-4}$.

Annexes C to G are a template of an acceptable argument that addresses the objectives of SW 01 for equipment with Safety Requirements no more onerous than 1 x 10^{-5}.

The diagrams in each Annex represent a single argument structure, divided into manageable portions for presentation purposes. As this division is for convenience, any other partitioning of the overall structure that an ANSP might choose to adopt would be equally valid. Where a claim is developed further in a child diagram, the reference number of the child diagram is given in the claim node. Each CAE diagram illustrates a fragment of the argument and is followed by the full argument text.

A.2.2 Using the Templates

The ANSP must take responsibility for its own safety case, whether the material originates from this Guidance or otherwise. It is important that the ANSP ensures that it only uses arguments from this Guidance that are valid for the COTS equipment. The ANSP may find that it is necessary to add further arguments and evidence to create a complete and correct argument.

Normal text in Annexes B to G is intended to be invariant, and so is written for direct inclusion in the ANSP's software safety arguments. Footnotes and text in *italics* provides information on the presentation of the argument, and should not be included in an actual software safety submission.

As a template, the diagrams and arguments include the complete range of assurance evidence options permitted by the CEET. These diagrams may therefore require modification according to the actual evidence called upon, which will vary depending on the ANSP circumstances.

Where the word [REF] is found in the supporting argument text, users are required to replace it with a discrete and precise reference to the documentary evidence being called for to support the argument. This evidence may need to be examined during an audit.

A.2.3 Referencing System

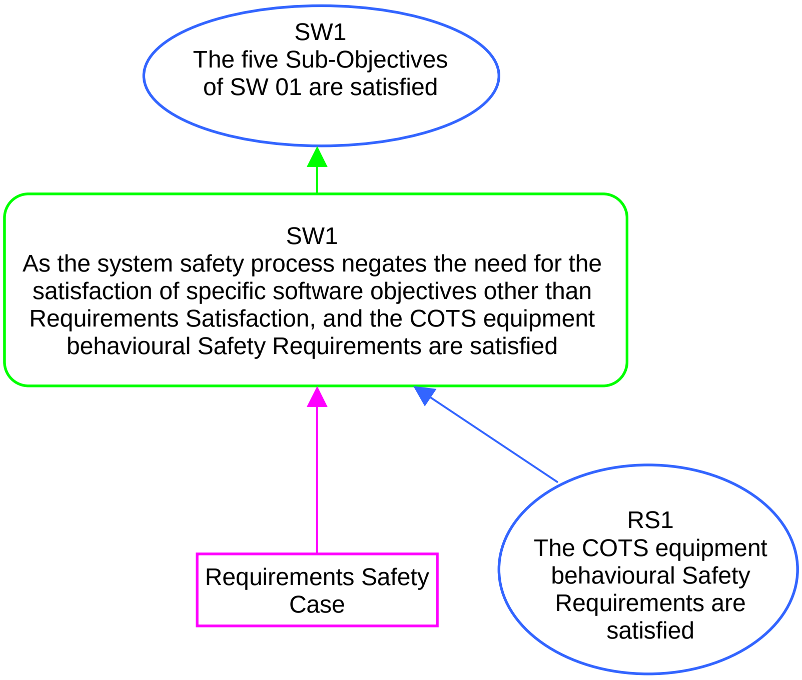
In the Claims – Argument – Evidence (CAE) diagram diagrams in this guidance, the claim and argument nodes include a reference (e.g. 'RS1.2'). This identifies the paragraph where the full argument is provided (the diagram is merely a summary).

A.2.4 Comparison of 10^{-4} Argument with 10^{-5} Argument

The 10^{-4} argument is a shortened version of the 10^{-5} argument. This is because the 10^{-4} argument addresses the assurance of the COTS equipment safety at the equipment boundary and the 10^{-5} argument may require knowledge of the software architecture of the COTS equipment. Consequently, only the 'sufficient assurance can be gained' part of the argument (RS1.1) and the 'Safety Requirements are met' part (RS1.2) from the 10^{-5} argument are required in the 10^{-4} argument. These are the same in both arguments, at the current Roadmap stage, as the two CEETs (Annexes I and J) invoke the same evidence. However, the assurance points available are different.

ANNEX B ARGUMENT DIAGRAM TEMPLATE FOR 1 X 10^{-4} REQUIREMENTS

SW1 The Safety Objective of SW 01 is satisfied


SW1
The five Sub-Objectives of SW 01 are satisfied
SW1
As the system safety process negates the need for the satisfaction of specific software objectives other than Requirements Satisfaction, and the COTS equipment behavioural Safety Requirements are satisfied
Requirements Safety Case
RS1
The COTS equipment behavioural Safety Requirements are satisfied

Safety Requirements have been derived using a risk identification and mitigation process under the ANSP's Safety Management System. For the purposes of SW 01 compliance, the validity of these Safety Requirements does not require justification at this Roadmap position.

The System Safety Assessment has identified valid behavioural Safety Requirements [REF to Requirements Safety Case] at the equipment level[4, 5], hence the Requirements Validity sub-objective need not be argued here because we are treating the equipment as a black box. Similarly, the Safety Requirements do not need to be traced into the software, so the SW 01 sub-objective for Requirements Traceability does not need to be argued.

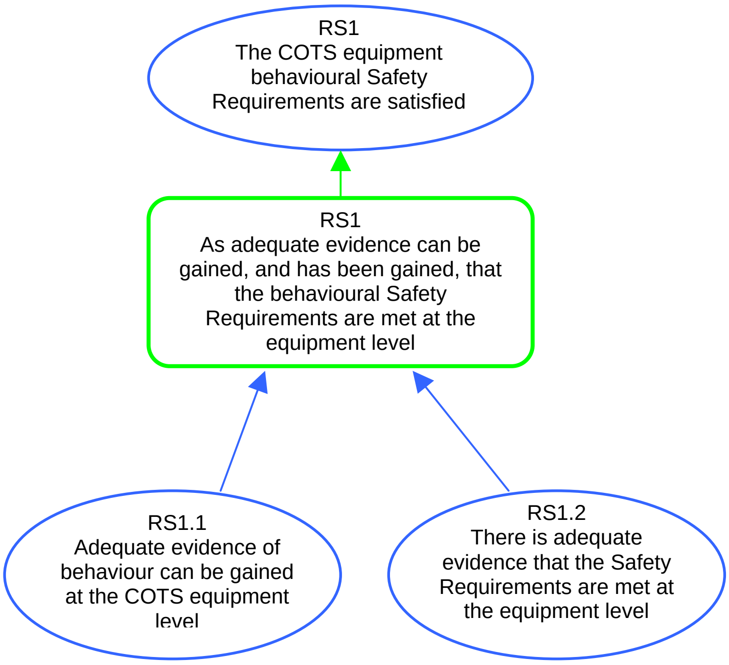
[4] Valid Safety Requirements are as defined in the 'Glossary and Definitions', and satisfy the apportionment Requirement of the Rationale in Annex K.3 of this document. See Section 2.3.

[5] This assumes that the System Safety Assessment has addressed all of the behaviour exhibited by the COTS Equipment including un-specified behaviour.

As the evidence came from an unchanged off the shelf purchased equipment all of the evidence generated relates to the version of software to be put into operation and hence no Configuration Consistency argument is required[6].

Satisfaction of the requirements shows that the software within the equipment has not interfered with its safety functions over the full range of operations and for sufficient time. Consequently, the Non-Interference sub-objective is not argued separately because the argument that the software Safety Requirements are satisfied includes an argument that sufficient state space has been exercised. Therefore, the only sub-objective that requires arguing is Requirements Satisfaction (Claim RS1).

RS1 The COTS equipment behavioural Safety Requirements are satisfied

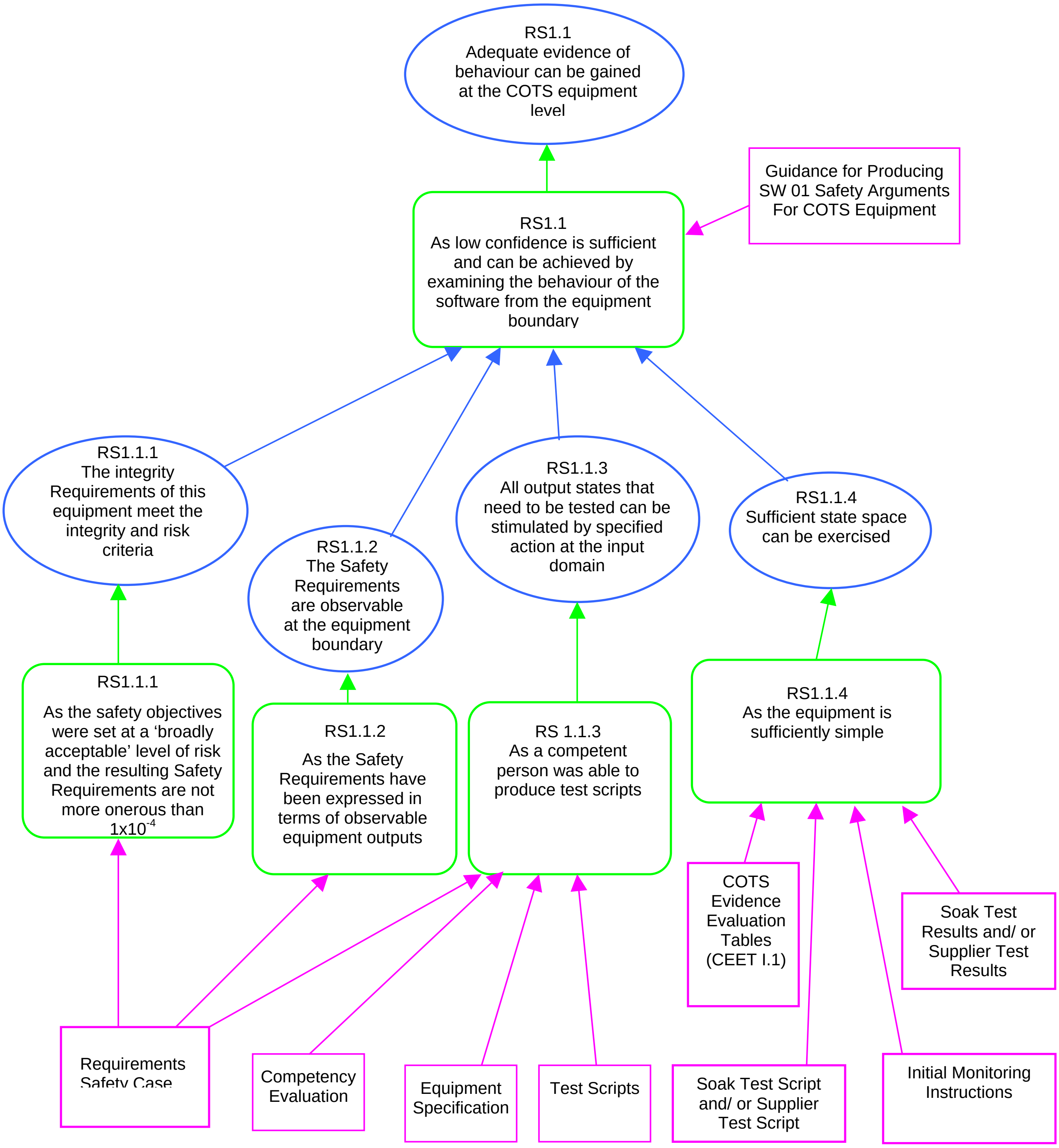

RS1
The COTS equipment behavioural Safety Requirements are satisfied
RS1
As adequate evidence can be gained, and has been gained, that the behavioural Safety Requirements are met at the equipment level
RS1.1
Adequate evidence of behaviour can be gained at the COTS equipment level
RS1.2
There is adequate evidence that the Safety Requirements are met at the equipment level

Adequate evidence of behaviour can be gained at the COTS equipment level (Claim RS1.1), and there is adequate evidence that the Safety Requirements are met at the COTS equipment level (Claim RS1.2). *Optional text:* , supplemented by some knowledge of internal design features.

Therefore, there is adequate evidence that the COTS equipment behavioural Safety Requirements are satisfied.

[6] Unless two equipments can be shown to be identical (hardware and software) then they are assumed to be different and separate evidence will need to be generated for both. It is not uncommon for COTS equipment with identical part numbers to have different software versions or hardware components.

RS1.1 Adequate evidence of behaviour can be gained at the COTS equipment level


RS1.1 Adequate evidence of behaviour can be gained at the COTS equipment level
Guidance for Producing SW 01 Safety Arguments For COTS Equipment
RS1.1 As low confidence is sufficient and can be achieved by examining the behaviour of the software from the equipment boundary
RS1.1.1 The integrity Requirements of this equipment meet the integrity and risk criteria
RS1.1.2 The Safety Requirements are observable at the equipment boundary
RS1.1.3 All output states that need to be tested can be stimulated by specified action at the input domain
RS1.1.4 Sufficient state space can be exercised
RS1.1.1 As the safety objectives were set at a 'broadly acceptable' level of risk and the resulting Safety Requirements are not more onerous than 1x10-4
RS1.1.2 As the Safety Requirements have been expressed in terms of observable equipment outputs
RS 1.1.3 As a competent person was able to produce test scripts
RS1.1.4 As the equipment is sufficiently simple
COTS Evidence Evaluation Tables (CEET I.1)
Soak Test Results and/ or Supplier Test Results
Requirements Safety Case
Competency Evaluation
Equipment Specification
Test Scripts
Soak Test Script and/ or Supplier Test Script
Initial Monitoring Instructions

It is possible to stimulate the equipment's inputs and observe the required safety behaviour at its outputs (Claim RS1.1.2 and Claim RS1.1.3). When the software state space is sufficiently small (Claim RS1.1.4), the CAA 'Guidance for Producing SW 01 Safety Arguments for COTS Equipment' authorises the assumption that testing at equipment level can cover sufficient of this state space to demonstrate Requirement Satisfaction, with a low level of confidence, for integrity Requirements no worse than 1 x 10^{-4}, without further supporting evidence.

A low level of confidence of Requirement Satisfaction is acceptable when system Safety Requirements are set to achieve 'broadly acceptable' levels of risk. The integrity Requirements of this equipment meet the integrity and risk criteria (Claim RS1.1.1).

Under these circumstances, equipment test results adequately demonstrate equipment behaviour.

RS1.1.1 The integrity Requirements of this equipment meet the integrity and risk criteria

The Safety Requirements are not more onerous than 1 x 10^{-4} [REF to Requirements Safety Case], and are valid because they are derived from Safety Objectives that were set at a 'broadly acceptable' level of risk [REF to Requirements Safety Case], such that low confidence is required thus meeting the integrity and risk criteria set in this guidance (see the Rationale in Annex K of the CAA 'Guidance for Producing SW 01 Safety Arguments for COTS Equipment').

RS1.1.2 The Safety Requirements are observable at the equipment boundary

The required safety behaviour (COTS Equipment Safety Requirements) is observable at the equipment boundary because they are expressed in terms of effects at the output of the equipment. This can be seen by inspection of the COTS Equipment Safety Requirements in the Requirements Safety Case [REF to Requirements Safety Case].

RS1.1.3 All output states that need to be tested can be stimulated by specified action at the input domain

All output states that need to be tested can be stimulated by specified action at the input domain. This was demonstrated by the successful creation of the test scripts by a person familiar with the application, using the equipment specification to create tests that, for each Safety Requirement, adequately cover the output range, without identifying any aspects of the Requirements as being un-testable. The Test Scripts [REF to Test Scripts] show a comprehensive set of tests for each Safety Requirement [REF to Requirements Safety Case], and were prepared by [NAME of competent person], who is considered competent [REF to Competency Evaluation] to prepare test scripts and to have adequate knowledge of the equipment [REF to Equipment Specification] and application.

RS1.1.4 Sufficient state space can be exercised

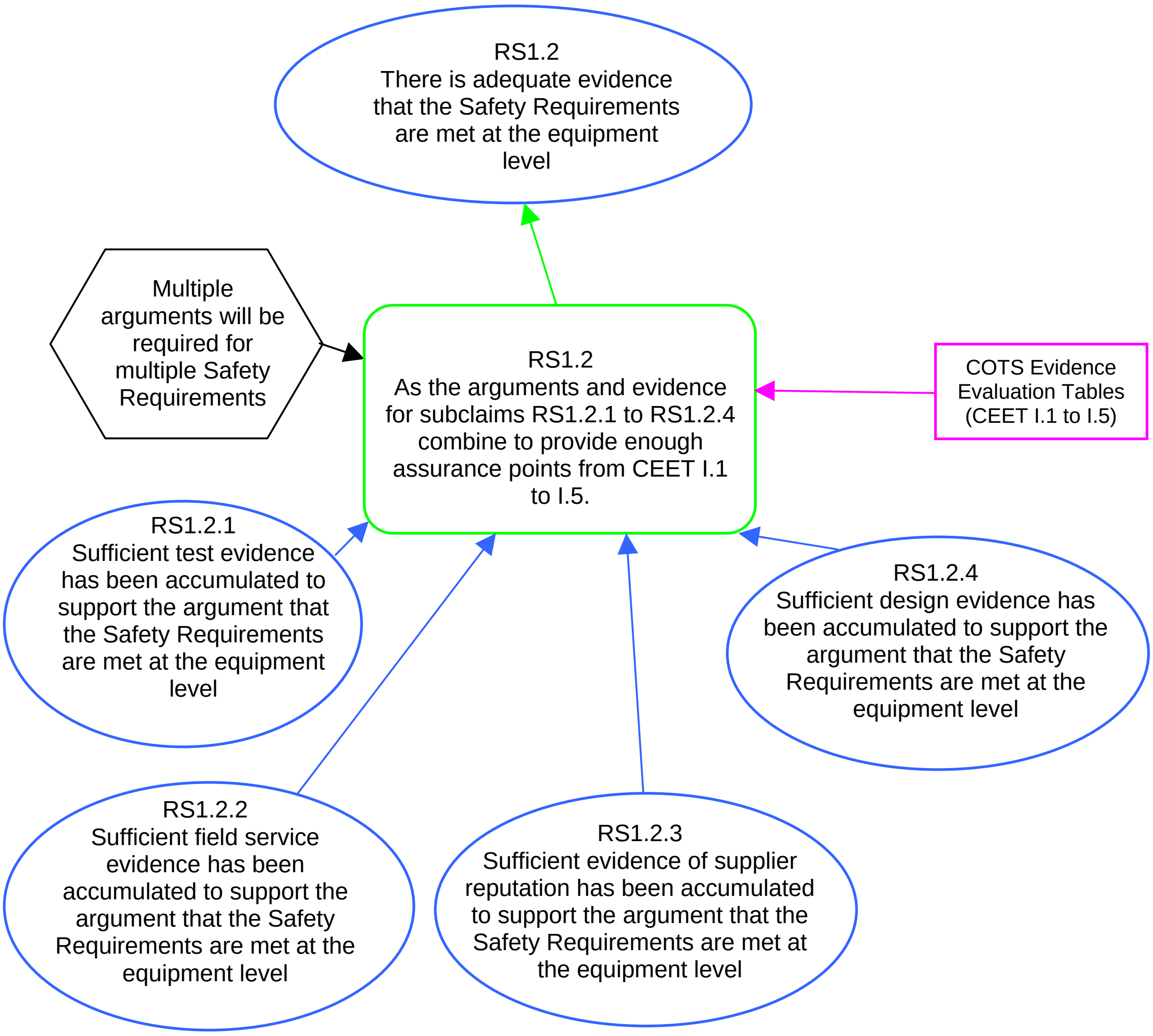
Although the input and output domains of the equipment are known sufficiently to test the full range of outputs, the internal variable domain of the software is not known. Without knowledge of the complexity of the implementation, this Safety Argument cannot provide assurance that sufficient state space can be exercised. However, due to the mitigations provided by setting Requirements at a broadly acceptable level of risk (such that low confidence of Requirement Satisfaction is required), and the extra initial vigilance on entry to service [REF to Initial Monitoring Instructions], SRG authorises the assumption that meeting the soak testing Requirements in the CEET (Annex I of ‘Guidance for Producing SW 01 Safety Arguments for COTS Equipment’) provides adequate coverage of the state space for simple equipment[7].

The equipment is sufficiently simple and *(either or both of the following)* soak testing *and/ or* supplier test evidence meets the evidence criteria in the CEET [REF to Soak Test Script and Soak Test Results *and/ or* Supplier Test Scripts and Supplier Test Results].

The ‘Initial Monitoring Instructions’ should attempt to detect and record any behaviour that is not specified in the COTS Equipment Specification.

[7] The claim that “Sufficient state space can be exercised” is far more credible for a ‘smaller’, single purpose equipment with bespoke platform like a radio than for a ‘larger’ sub-system based on a more general purpose computing platform. It would not be a credible claim for a cluster of PCs or similar.

RS1.2 There is adequate evidence that the Safety Requirements are met at the equipment level


RS1.2
There is adequate evidence that the Safety Requirements are met at the equipment level
Multiple arguments will be required for multiple Safety Requirements
RS1.2
As the arguments and evidence for subclaims RS1.2.1 to RS1.2.4 combine to provide enough assurance points from CEET I.1 to I.5.
COTS Evidence Evaluation Tables (CEET I.1 to I.5)
RS1.2.1
Sufficient test evidence has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.4
Sufficient design evidence has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.2
Sufficient field service evidence has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.3
Sufficient evidence of supplier reputation has been accumulated to support the argument that the Safety Requirements are met at the equipment level

In the 'Guidance for Producing SW 01 Safety Arguments for COTS Equipment', SRG has provided a scheme for determining the level of assurance provided by Requirement Satisfaction evidence. The COTS Evidence Evaluation Table defines criteria for the evidence and assurance points that can be claimed for that evidence. The Guidance requires that the total of the assurance points must exceed a defined minimum level.

[ANSP] agrees that the assurance provided by evaluation of the COTS equipment, using this scheme, is sufficient[8].

[8] This is effectively a formal statement by the ANSP that the argument is not invalidated by contrary evidence or other circumstances.

Sufficient functional and integrity evidence has been accumulated that shows that the Safety Requirements are met at the equipment level. This evidence comprises: Test; Field Service; Supplier reputation and Design evidence *[delete as applicable]*.

For each type of evidence, the claim for the number of 'functional points' and 'integrity points' is justified in the arguments that follow, in accordance with the CEET. The points claimed are:

- 100 functional points[9] from test evidence;
- I_t integrity points from test evidence (see RS1.2.1);
- I_f integrity points from field service evidence (see RS1.2.2);
- I_s integrity points from supplier reputation evidence (see RS1.2.3);
- I_d integrity points from design evidence (see RS1.2.4).

The evidence is judged to be sufficient because the CEET was used to determine that the minimum of 100 functional and 100 ($I_t + I_f + I_s + I_d$) integrity points has been achieved.

Notes regarding multiple arguments for multiple Safety Requirements

It is important that the evidence is credible for each Safety Requirement. The arguments should show this as clearly as possible to ease review and audit. For example, if a single Safety Requirement were selected, then the relevant tests and test records for that Requirement must be identifiable, and it is best to include such traceability in the Safety Argument. The CEET includes some Evidence Satisfaction Criteria that are intended to address this.

It may not be possible (valid) to claim the same level of assurance for all Safety Requirements from a particular source of evidence. For example, even though the CEET requires a similar environment, the available field-service evidence may not have exercised certain features of a product relevant to some Safety Requirements. For those Safety Requirements, alternative evidence must be used and therefore other variants of the arguments used.

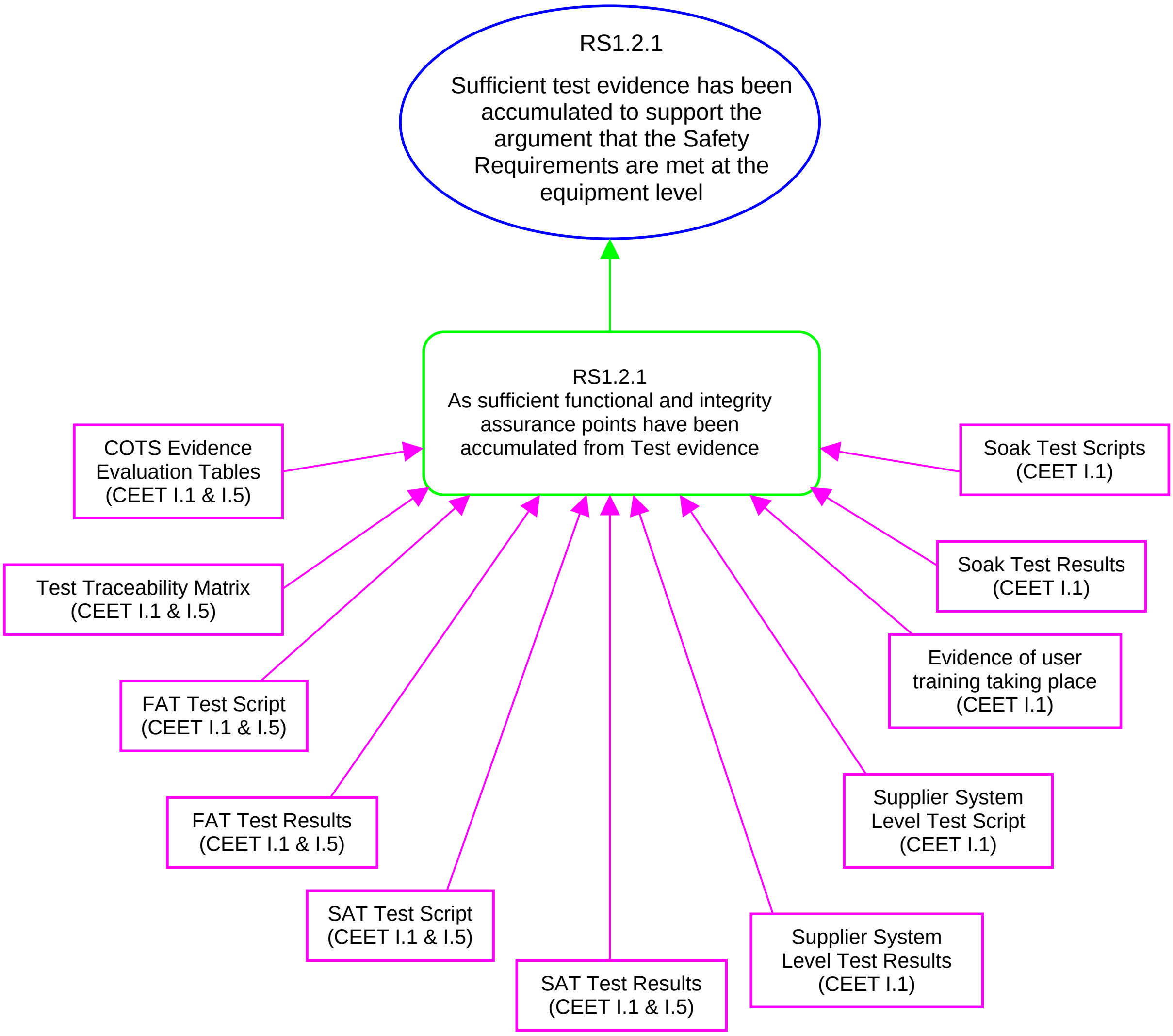
Different arguments may be presented for groups of Safety Requirements, according to the available evidence from test, field service, supplier reputation and design. These arguments could have common elements, for example the claim and argument for FAT and SAT, but might refer to different evidence from field service experience, supplier testing and design evidence.

Diagrammatically, there would be one sub-CAE diagram from this point downwards for each group of Safety Requirements.

In practice, at this stage of the Roadmap, the CEET points scheme means that there will be few cases where there are such variations in the points claimed from each evidence type.

[9] No other result is possible in a complete argument.

RS1.2.1 Test Evidence


RS1.2.1
Sufficient test evidence has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.1
As sufficient functional and integrity assurance points have been accumulated from Test evidence
COTS Evidence Evaluation Tables (CEET I.1 & I.5)
Test Traceability Matrix (CEET I.1 & I.5)
FAT Test Script (CEET I.1 & I.5)
FAT Test Results (CEET I.1 & I.5)
SAT Test Script (CEET I.1 & I.5)
SAT Test Results (CEET I.1 & I.5)
Supplier System Level Test Results (CEET I.1)
Supplier System Level Test Script (CEET I.1)
Evidence of user training taking place (CEET I.1)
Soak Test Results (CEET I.1)
Soak Test Scripts (CEET I.1)

Comparison of the available evidence with the CEET I.1 and I.5 shows that a total of I_t integrity points and 100 functional points can be claimed. This is made up as follows:

All Safety Requirements are shown to have been addressed by tests either in FAT or in SAT [REF to Test Traceability Matrix], meeting the evidence criteria in the CEET I.5. Therefore, 100 functional points are claimed.

FAT has been conducted, and met the evidence criteria in the CEET I.1 [REF to FAT Test Script and FAT Test Results]. No violations of the Safety Requirements were observed during the tests [REF to FAT Test Results]. Therefore x integrity points[10] are claimed.

SAT has been conducted, and met the evidence criteria in the CEET I.1 [REF to SAT Test Script and SAT Test Results]. No violations of the Safety Requirements were observed during the tests [REF to SAT Test Results]. Therefore x integrity points are claimed.

ANSP Soak Testing (y weeks[11]) has been conducted, and met the evidence criteria in the CEET I.1 [REF to Soak Test Scripts and Soak Test Results]. No violations of the Safety Requirements were observed during the tests [REF to Soak Test Results]. Therefore x integrity points are claimed.

User Training (y weeks) has been conducted, and met the evidence criteria in the CEET I.1 [REF to Evidence of user training taking place]. No violations of the Safety Requirements were observed during the training (no counter-evidence available). Therefore x integrity points are claimed.

y system-months of Supplier testing (System Level) have been conducted, and met the evidence criteria in the CEET I.1 [REF to Supplier System Level Test Script and Supplier System Level Test Results]. No violations of the Safety Requirements were observed during the tests [REF to Supplier System Level Test Results]. Therefore x integrity points are claimed.

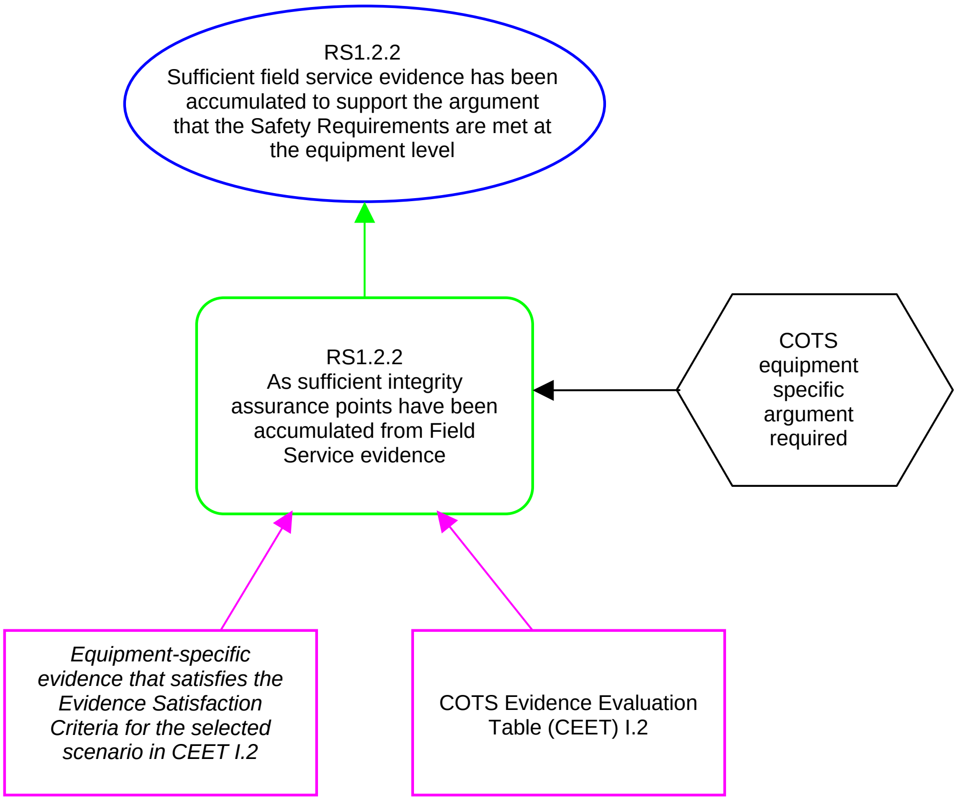
[If applicable] The integrity points total exceeds the maximum claimable (CEET I.1) for testing of 1 x 10^{-4} requirements, and so this is capped at 90.

In each case, this argument has assumed that the 'Evidence Satisfaction Criteria' in the CEET have been met for each evidence item. In a real argument this should be briefly argued, otherwise each reviewer will need to access the evidence to determine whether the criteria are met. Note that SRG may require the supply of any evidence item used.

[10] Here, x is used throughout to denote a number of points derived from the CEET, according to the evidence provided.

[11] Here, y is used throughout to denote a period of time specific to the COTS in question.

RS1.2.2 Field Service Evidence


RS1.2.2
Sufficient field service evidence has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.2
As sufficient integrity assurance points have been accumulated from Field Service evidence
COTS equipment specific argument required
Equipment-specific evidence that satisfies the Evidence Satisfaction Criteria for the selected scenario in CEET I.2
COTS Evidence Evaluation Table (CEET) I.2

Comparison of the available evidence with CEET I.2 shows that I_f integrity points can be claimed.

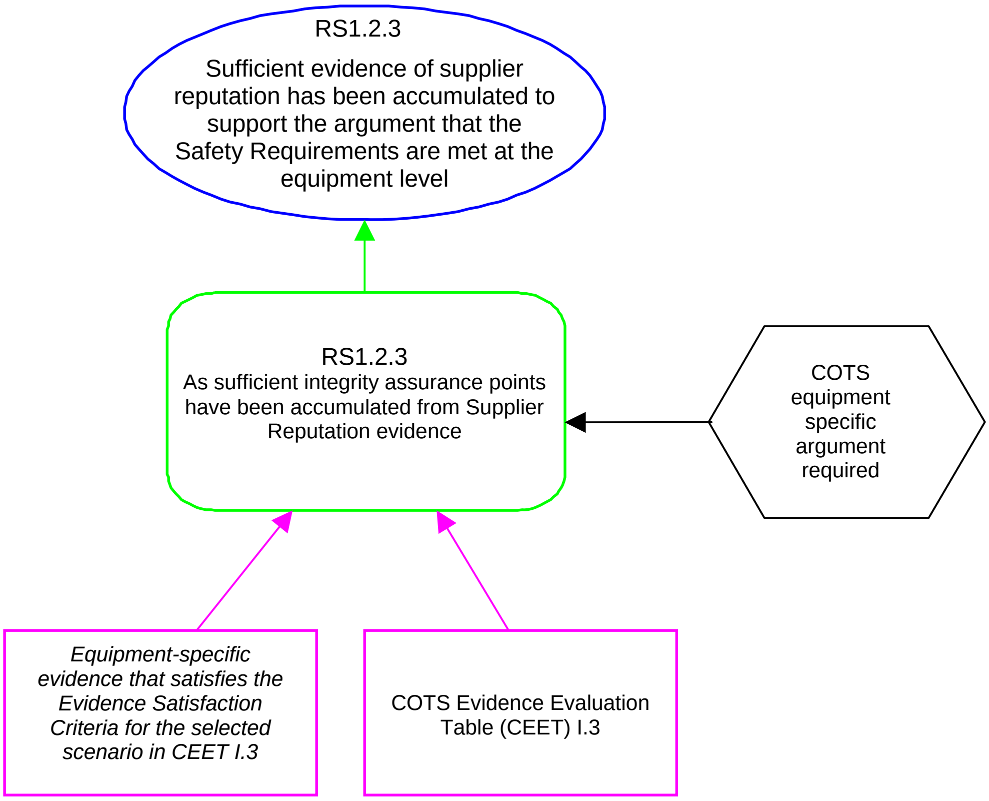
The argument that the field service experience meets the evidence criteria in CEET I.2 is as follows.

*The **COTS equipment specific argument** that needs to be inserted here to claim field service experience will depend on the data held. Having selected a matching Field Service experience scenario from CEET I.2 (e.g. 'Same system on a similar platform'), the argument must show that the available field service experience matches that scenario, and justify that the evidence available meets the Evidence Satisfaction Criteria given in that row of CEET I.2.*

As an example, the argument that the field service for which evidence is held meets the evidence criteria in the CEET for field service experience 'of the same system on the same platform' could be similar to the following:

Field service experience is being claimed from an equipment that has been operating for 1.5 years at <location>. The equipment is identical to that being justified in this example [REFs to equipment build statement in Doc Y and build statement for operational equipment], and therefore qualifies as 'the same system on the same platform' in the CEET. It also meets the criterion for a similar environment. Analysing the occurrences reported by users [REF to written statement of observed failures in Doc Y], it was found that none contravene the current Safety Requirements, indicating that the future rates are expected to be less than those stipulated for each Safety Requirement.

RS1.2.3 Supplier Reputation Evidence


RS1.2.3
Sufficient evidence of supplier reputation has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.3
As sufficient integrity assurance points have been accumulated from Supplier Reputation evidence
COTS equipment specific argument required
Equipment-specific evidence that satisfies the Evidence Satisfaction Criteria for the selected scenario in CEET I.3
COTS Evidence Evaluation Table (CEET) I.3

Comparison of the available evidence with CEET I.3 shows that I_S integrity points can be claimed.

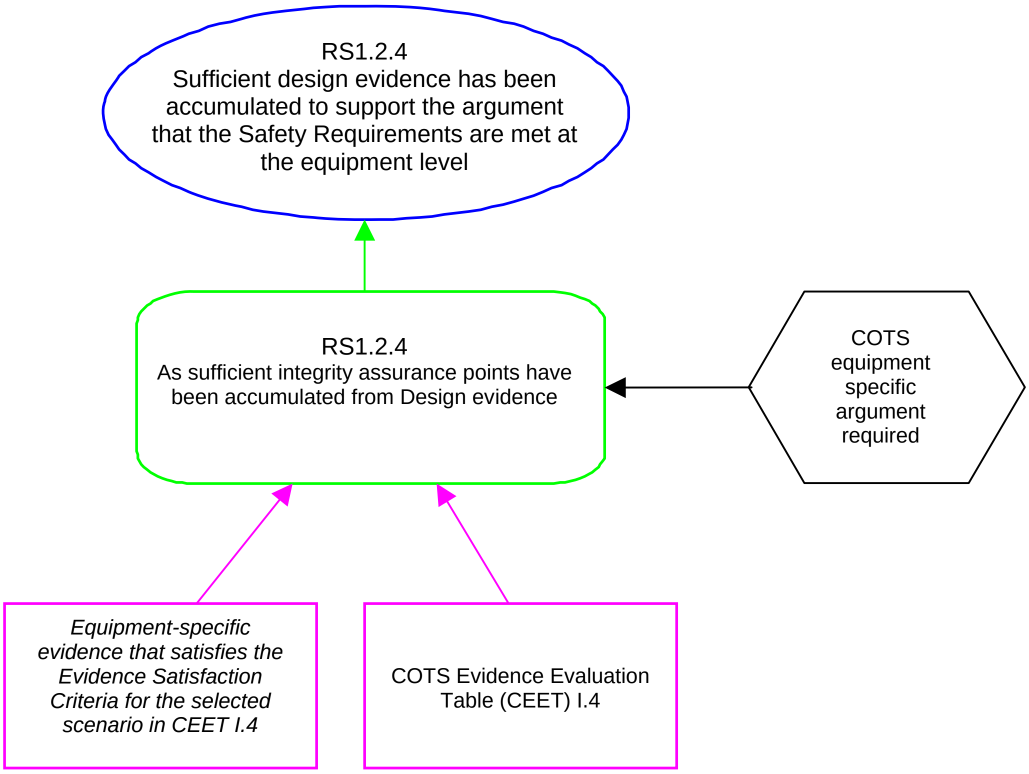
The argument that the supplier experience and expertise evidence meets the evidence criteria in CEET I.3 is as follows.

*The **COTS equipment specific argument** that needs to be inserted here to claim supplier reputation will depend on the data available. Having selected a matching supplier reputation scenario from CEET I.3 (e.g. 'Supplier has experience of deploying systems of the same type into the ATC market'), the argument must show that the available evidence matches that scenario, and justify that it meets the Evidence Satisfaction Criteria given in that row of CEET I.3.*

As an example, the argument that the supplier experience and expertise evidence meets the evidence criteria in CEET I.3 for ‘Supplier has experience of deploying systems of the same type into the ATC market’ could be similar to the following:

The supplier has been producing similar types of system for greater than 15 years, is experienced in the ATC domain and has delivered systems successfully to other ANSPs and can provide evidence to support the success at these other units. The service history records [REF to service history records] show service records for all equipment of this type. Analysing these records, it was found that no faults occurred that contravene the current Safety Requirements, indicating that the future rates are expected to be less than those stipulated for each Safety Requirement. Additionally, the supplier has provided a statement regarding its experience in the market [REF to supplier experience statement], which shows successful installations at 30 locations over the last 17 years, with no instances of significant faults being reported.

RS1.2.4 Evidence of Design


RS1.2.4
Sufficient design evidence has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.4
As sufficient integrity assurance points have been accumulated from Design evidence
COTS equipment specific argument required
Equipment-specific evidence that satisfies the Evidence Satisfaction Criteria for the selected scenario in CEET I.4
COTS Evidence Evaluation Table (CEET) I.4

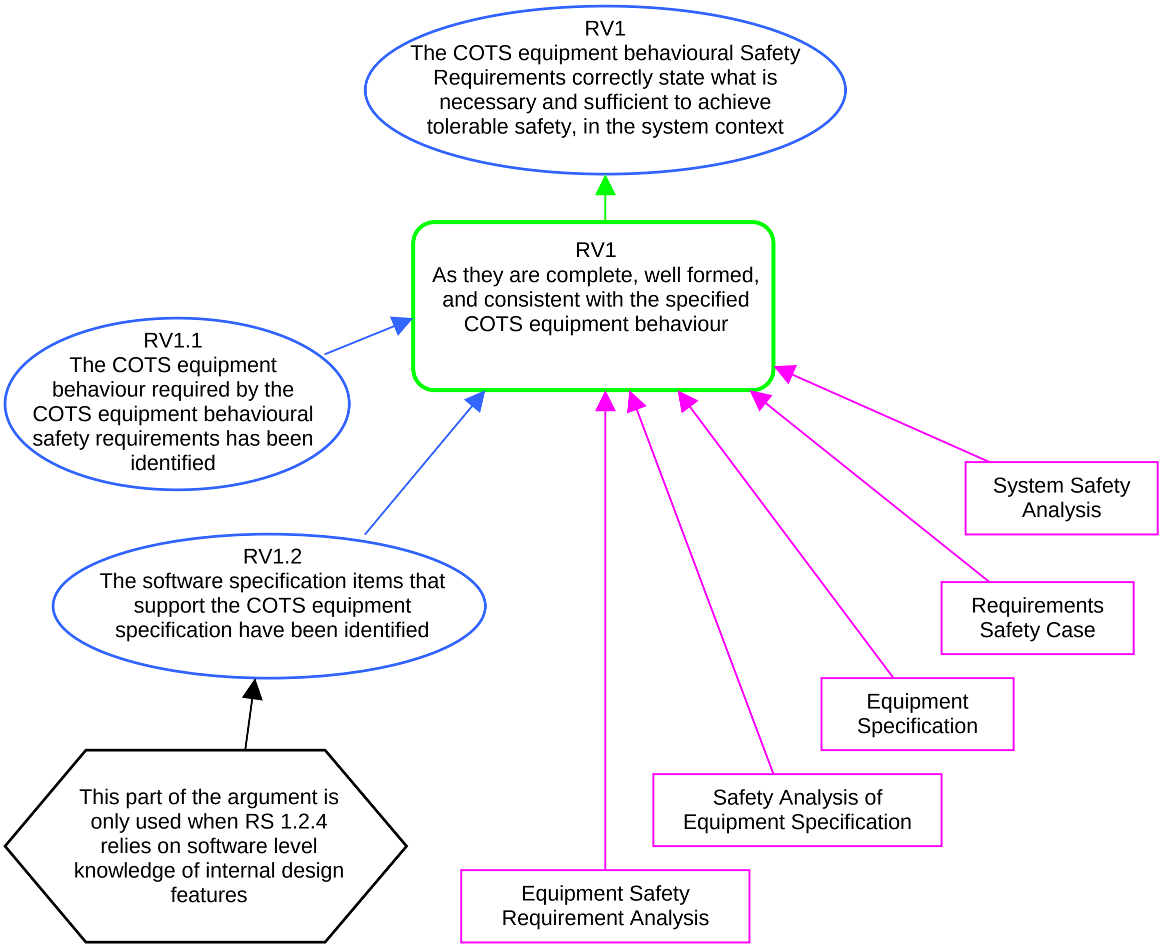
Comparison of the available design evidence with CEET I.4 shows that I_d integrity points can be claimed.

The argument that the Design evidence meets the evidence criteria in CEET I.4 is as follows.

*The **COTS equipment specific argument** that needs to be inserted here to claim design evidence will depend on the data available. Having selected a matching design evidence scenario from CEET I.4 (e.g. 'Knowledge of internal design features which have been put in place to limit the possibility of unwanted system action"), the argument must show that the available evidence matches that scenario, and justify that it meets the Evidence Satisfaction Criteria given in that row of CEET I.4.*

ANNEX C REQUIREMENTS VALIDITY ARGUMENT DIAGRAM TEMPLATE FOR 1 X 10^{-5} REQUIREMENTS

RV1 The COTS equipment behavioural Safety Requirements correctly state what is necessary and sufficient to achieve tolerable safety, in the system context


RV1
The COTS equipment behavioural Safety Requirements correctly state what is necessary and sufficient to achieve tolerable safety, in the system context
RV1
As they are complete, well formed, and consistent with the specified COTS equipment behaviour
RV1.1
The COTS equipment behaviour required by the COTS equipment behavioural safety requirements has been identified
RV1.2
The software specification items that support the COTS equipment specification have been identified
This part of the argument is only used when RS 1.2.4 relies on software level knowledge of internal design features
System Safety Analysis
Requirements Safety Case
Equipment Specification
Safety Analysis of Equipment Specification
Equipment Safety Requirement Analysis

Safety Requirements have been derived using a risk identification and mitigation process under the ANSP's Safety Management System. For the purposes of SW 01 compliance, the validity of these Safety Requirements does not require justification at this Roadmap position.

The system safety analysis identified Safety Requirements [REF to Requirements Safety Case] at the equipment level[12].

[12] Valid safety requirements are as defined in the 'Glossary and Definitions', and satisfy the apportionment requirement of the Rationale in Annex K.3 of this document.

Analysis of the equipment level safety requirements [REF to Equipment Safety Requirement Analysis] identified the COTS equipment behavioural Safety Requirements, and confirmed that they are correctly formed[13].

All specified behaviour of the COTS equipment [REF to Equipment Specification] was analysed[14] [REF to Safety Analysis of Equipment Specification[15]] to identify behaviour required by the COTS equipment behavioural Safety Requirements (Claim RV1.1), and to determine whether further safety requirements (known as derived safety requirements) were necessary to address unrequired behaviour [REF to all identified derived Safety Requirements, usually contained in Equipment Safety Requirement Analysis]. These derived Safety Requirements were apportioned, in the System Safety Analyses [REF to System Safety Analysis], to appropriate system components[16].

Therefore, the COTS equipment behavioural Safety Requirements correctly state what is necessary and sufficient to achieve tolerable safety, in the system context.

> *For 10^{-5} it may not be possible to sufficiently demonstrate satisfaction of the apportioned safety requirements at equipment level. This means that evidence about the software within the COTS equipment must be used to provide sufficient assurance of requirement satisfaction, so the software safety requirements must be identified (by apportionment from the equipment safety requirements). Under these circumstances, it is also necessary to analyse all behaviour of the software (at the same level as the safety requirements), to identify any further 'derived' safety requirements from unrequired software behaviour.*
>
> *The previous paragraph considers the issues in principle. However, at the present Roadmap position, the constraints of this Guidance are not so onerous. The only case when it is necessary to argue Requirement Validity at software level is when the Requirement Satisfaction argument claims integrity points for "knowledge of internal design features". Moreover, this Guidance only stipulates identification (not apportionment of safety requirements) of the software functionality that relates to the equipment safety requirements, so that the relevance of designed-in safety features can be demonstrated.*

Text for the option when the Requirement Satisfaction argument claims integrity points for "knowledge of internal design features": The software specification items that support the COTS equipment behavioural Safety Requirements have been identified (Claim RV1.2).

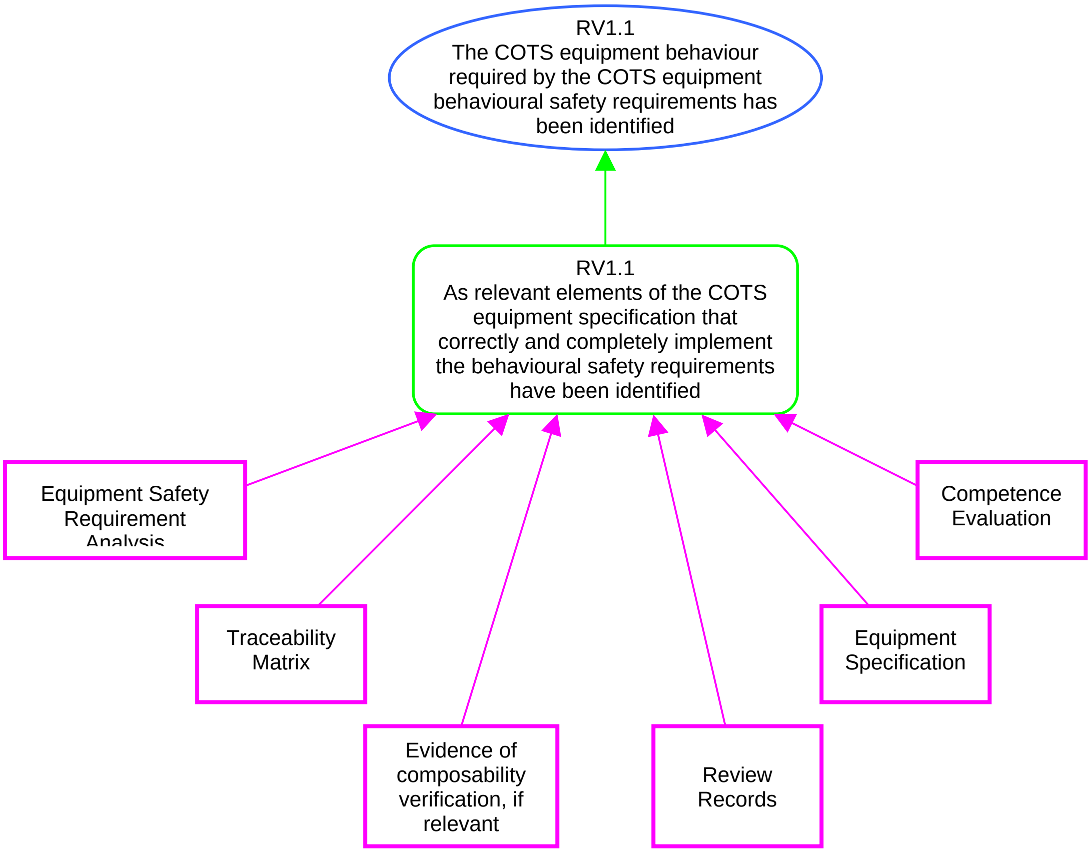
[13] See Section 2.2 and 'Glossary and Definitions' for behavioural attributes.

[14] This guidance does not require the quality of the product specification to be argued at this stage of the roadmap, as the analysis could not be completed if the product specification does not provide sufficient detail. This guidance cannot be used if the analysis is incomplete.

[15] This document may be integrated with the Equipment Safety Requirement Analysis.

[16] These derived safety requirements may be allocated to parts of the system other than the COTS equipment, and have to be addressed as part of further safety arguments supporting putting the COTS equipment into service.

RV1.1 The COTS equipment behaviour required by the COTS equipment behavioural safety requirements has been identified


RV1.1
The COTS equipment behaviour required by the COTS equipment behavioural safety requirements has been identified
RV1.1
As relevant elements of the COTS equipment specification that correctly and completely implement the behavioural safety requirements have been identified
Equipment Safety Requirement Analysis
Traceability Matrix
Evidence of composability verification, if relevant
Review Records
Equipment Specification
Competence Evaluation

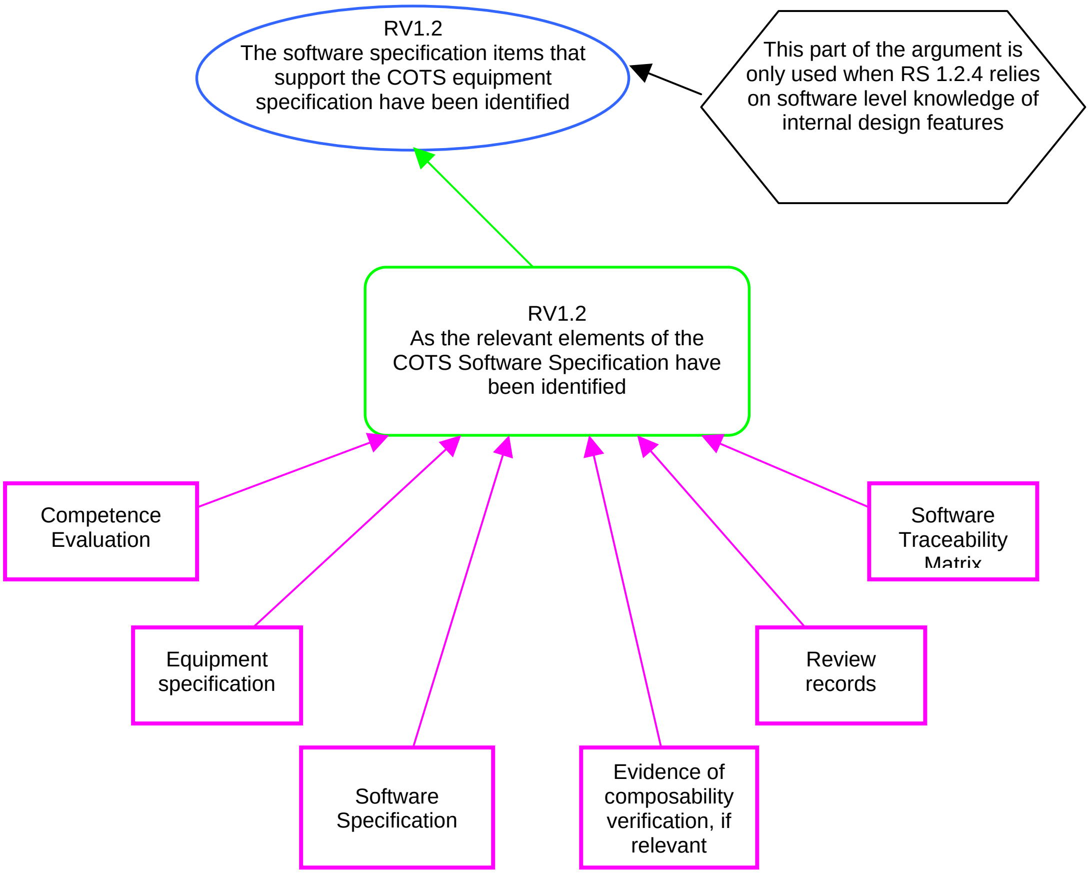
For each COTS equipment behavioural safety requirement (as identified by the analysis of the equipment level safety requirements [REF to Equipment Safety Requirement Analysis][17], the relevant elements of the COTS equipment specification [REF to Equipment Specification] that correctly and completely implement the requirement have been identified [REF to Traceability Matrix].

For example, specification items x to z may fulfil a particular COTS equipment behavioural Safety Requirement. In some cases, the traceability matrix may have to be supplemented by analyses to show that two or more product specification elements compose to satisfy an equipment Safety Requirement [REF to Evidence of composability verification, if relevant].

This was identified by a review [REF to Review Records] conducted by competent [REF to Competence Evaluation] staff from both the ANSP and the supplier. *The criteria for competence need to be specified here.*

[17] See RV1.

RV1.2 The software specification items that support the COTS equipment specification have been identified


RV1.2
The software specification items that support the COTS equipment specification have been identified
This part of the argument is only used when RS 1.2.4 relies on software level knowledge of internal design features
RV1.2
As the relevant elements of the COTS Software Specification have been identified
Competence Evaluation
Software Traceability Matrix
Equipment specification
Review records
Software Specification
Evidence of composability verification, if relevant

This part of the requirements validity argument justifies requirement validity at software level, and so is intended for cases where assurance (e.g. requirement satisfaction assurance) is gained from software-level evidence (e.g. software design features).

At the current Roadmap position, the CEET usually permits sufficient assurance to be gained from equipment-level evidence only (for Safety Requirements up to 1 x 10^{-5}). This part of the argument is only required, for requirement validity at software level, when integrity points are claimed for "knowledge of internal design features".

To argue about the safety requirements at software level, the COTS equipment behavioural safety requirements have to be apportioned to the relevant software functionality. However, to support the limited usage of software-level evidence at this roadmap stage, and to address issues associated with unrequired software functionality, complete tracing (not apportionment) is required, as follows.

For each element of the COTS equipment specification [REF to Equipment Specification], the relevant elements of the COTS Software Specification [REF to Software Specification] have been identified [REF to software traceability matrix].

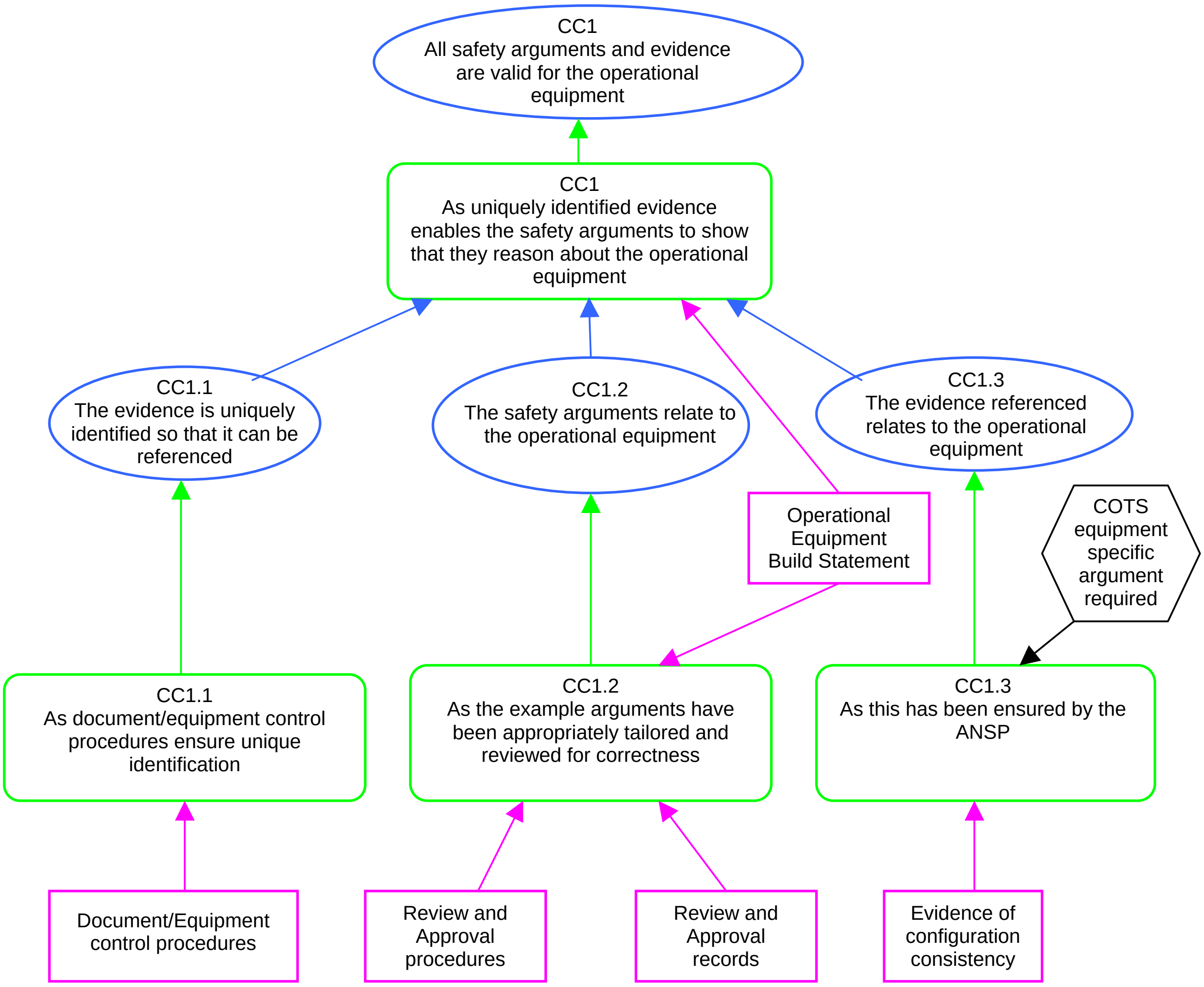
For example, COTS Software Specification items Sx to Sz fulfil the COTS equipment specification items x to z. In some cases, the software traceability matrix may have to be supplemented by analyses to show that two or more software specification elements compose to satisfy a COTS equipment specification element [REF to Evidence of composability verification, if relevant].

Therefore, the software specification items that support the COTS equipment specification have been identified.

This was identified by a review [REF to Review Records] conducted by competent [REF to Competence Evaluation] staff from the supplier.

ANNEX D CONFIGURATION CONSISTENCY ARGUMENT DIAGRAM TEMPLATE FOR 1 X 10^{-5} REQUIREMENTS

CC1 All safety arguments and evidence are valid for the operational equipment


CC1
All safety arguments and evidence are valid for the operational equipment
CC1
As uniquely identified evidence enables the safety arguments to show that they reason about the operational equipment
CC1.1
The evidence is uniquely identified so that it can be referenced
CC1.2
The safety arguments relate to the operational equipment
CC1.3
The evidence referenced relates to the operational equipment
Operational Equipment Build Statement
COTS equipment specific argument required
CC1.1
As document/equipment control procedures ensure unique identification
CC1.2
As the example arguments have been appropriately tailored and reviewed for correctness
CC1.3
As this has been ensured by the ANSP
Document/Equipment control procedures
Review and Approval procedures
Review and Approval records
Evidence of configuration consistency

The evidence is uniquely identified so that it can be referenced (Claim CC1.1), and the build state of the operational equipment is known [REF to Operational Equipment Build Statement]. These claims allow the argument to be made that the safety arguments (Claim CC1.2) and the evidence referenced (Claim CC1.3) relate to the operational equipment.

Therefore, the arguments and evidence, for the safety of the software in the system context, are from: a known executable version of the software and a known set of software products, data and descriptions that have been used in the production of that version (i.e. all safety arguments and evidence are valid for the operational equipment).

CC1.1 The evidence is uniquely identified so that it can be referenced

All evidence is uniquely identified because normal management procedures [REF to Document/Equipment control procedures] stipulate that unique reference identifiers are given to items such as equipment and documents used as evidence, etc. This allows different versions of the same item to be differentiated from each other.

Therefore, evidence is uniquely identified so that it can be referenced.

It may be possible to draw on audit reports to show evidence that the procedure is followed.

It may be possible to give the list of evidence items referenced in the safety argument, to demonstrate that they have unique identifiers.

CC1.2 The safety arguments relate to the operational equipment

The safety arguments presented here are valid for the operational version of the equipment because they have been derived from the template arguments in the SRG ‘Guidance for Producing SW 01 Safety Arguments for COTS Equipment’ with appropriate tailoring to suit the circumstances of the COTS equipment [REF to Operational Equipment Build Statement] and the available evidence[18].

The review and approval [REF to Review and Approval procedures, and REF to Review and Approval records] of these arguments confirm their validity for the operational version.

Therefore, the safety arguments relate to the operational equipment.

CC1.3 The evidence referenced relates to the operational equipment

The ANSP must provide an argument here, addressing the following issues.

For a COTS purchase, evidence derived from the equipment by the ANSP will be valid for the operational version of the equipment. However, where the evidence refers to a different version, a rationale must be given to justify why the evidence remains valid for the argument for the operational version. Such arguments may be inserted at the point of use elsewhere in the safety arguments (it would add to the credibility of this argument if these points are listed/referenced here), or this may be addressed by making all such arguments in one place i.e. as part of this argument.

Appropriate practices are (naturally) selected by the ANSP manager to ensure that this claim is true. This could be by knowledge that only a single valid version exists of each evidence item, or could require a more formal examination of the versions of evidence, and configuration management data, and documenting the results. Evidence of this may already exist as the result of a Quality Assurance activity. Any such results are ‘Evidence of Configuration Consistency’ and should be referenced.

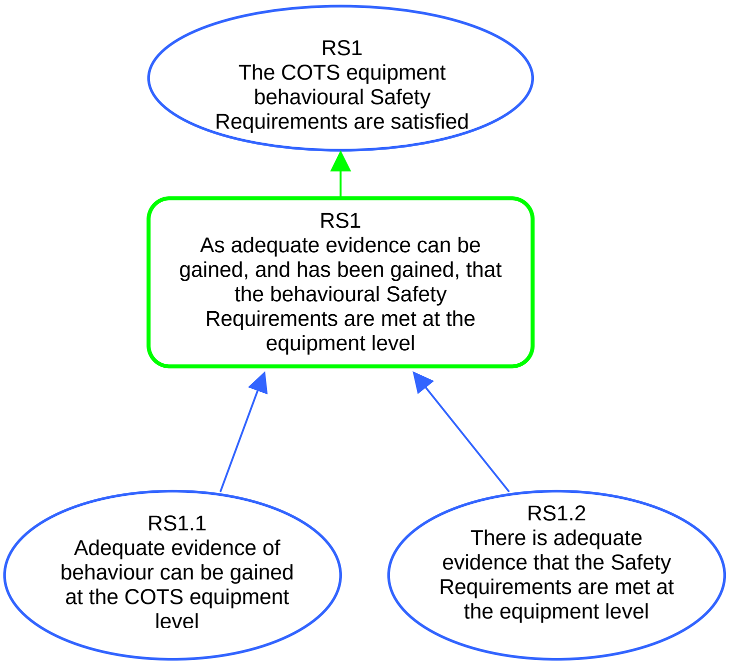
[18] This is effectively a formal statement by the ANSP that the arguments presented are suitable for the particular equipment, such that the ANSP takes ownership of the safety argument.

If evidence has been altered, it must be argued that the alterations are justified.

Some evidence accepted by the 'COTS Evidence Evaluation Tables' (CEET) is not version specific (e.g. supplier experience), and some evidence inherently relates to previous versions (e.g. field service experience). The CEET discounts the assurance benefit to account for the differences. These cases are inherently justified by showing that the evidence meets the evidence criteria in the CEET.

ANNEX E REQUIREMENTS SATISFACTION ARGUMENT DIAGRAM TEMPLATE FOR 1 X 10^{-5} REQUIREMENTS

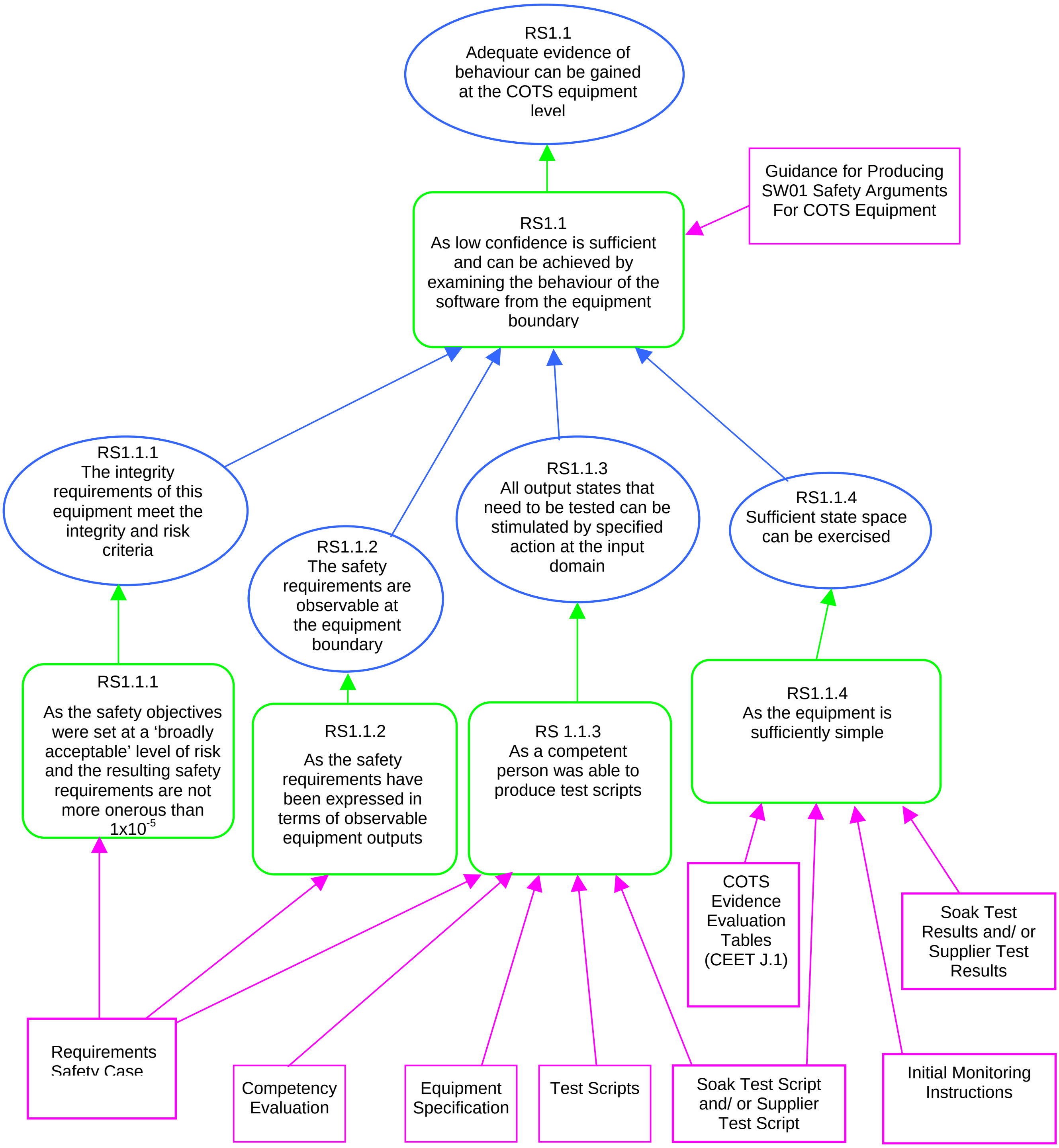
RS1 The COTS equipment behavioural Safety Requirements are satisfied


RS1
The COTS equipment behavioural Safety Requirements are satisfied
RS1
As adequate evidence can be gained, and has been gained, that the behavioural Safety Requirements are met at the equipment level
RS1.1
Adequate evidence of behaviour can be gained at the COTS equipment level
RS1.2
There is adequate evidence that the Safety Requirements are met at the equipment level

Adequate evidence of behaviour can be gained at the COTS equipment level (Claim RS1.1), and there is adequate evidence that the Safety Requirements are met at the COTS equipment level (Claim RS1.2). *Optional text:* , supplemented by some knowledge of internal design features.

Therefore, there is adequate evidence that the COTS equipment behavioural Safety Requirements are satisfied.

RS1.1 Adequate evidence of behaviour can be gained at the COTS equipment level


RS1.1
Adequate evidence of behaviour can be gained at the COTS equipment level
RS1.1
As low confidence is sufficient and can be achieved by examining the behaviour of the software from the equipment boundary
Guidance for Producing SW01 Safety Arguments For COTS Equipment
RS1.1.1
The integrity requirements of this equipment meet the integrity and risk criteria
RS1.1.2
The safety requirements are observable at the equipment boundary
RS1.1.3
All output states that need to be tested can be stimulated by specified action at the input domain
RS1.1.4
Sufficient state space can be exercised
RS1.1.1
As the safety objectives were set at a 'broadly acceptable' level of risk and the resulting safety requirements are not more onerous than $1x10^{-5}$
RS1.1.2
As the safety requirements have been expressed in terms of observable equipment outputs
RS 1.1.3
As a competent person was able to produce test scripts
RS1.1.4
As the equipment is sufficiently simple
COTS Evidence Evaluation Tables (CEET J.1)
Soak Test Results and/ or Supplier Test Results
Requirements Safety Case
Competency Evaluation
Equipment Specification
Test Scripts
Soak Test Script and/ or Supplier Test Script
Initial Monitoring Instructions

It is possible to stimulate the equipment's inputs and observe the required safety behaviour at its outputs (Claim RS1.1.2 and Claim RS1.1.3). When the software state space is sufficiently small (Claim RS1.1.4), the CAA 'Guidance for Producing SW 01 Safety Arguments for COTS Equipment' authorises the assumption that testing at equipment level can cover sufficient of this state space to demonstrate Requirement Satisfaction, with a low level of confidence, for integrity requirements no worse than 1 x 10^{-5}, without further supporting evidence.

A low level of confidence of requirement satisfaction is acceptable when system Safety Requirements are set to achieve 'broadly acceptable' levels of risk. The integrity requirements of this equipment meet the integrity and risk criteria (Claim RS1.1.1).

Under these circumstances, adequate evidence of behaviour can be gained at the COTS equipment level.

RS1.1.1 The integrity requirements of this equipment meet the integrity and risk criteria

The Safety Requirements are not more onerous than 1 x 10^{-5} [REF to Requirements Safety Case], and are valid because they are derived from Safety Objectives that were set at a broadly acceptable level of risk [REF to Requirements Safety Case], such that low confidence is required thus meeting the integrity and risk criteria set in this guidance (see the Rationale in Annex K of the CAA 'Guidance for producing SW 01 Safety Arguments for COTS Equipment').

RS1.1.2 The safety requirements are observable at the equipment boundary

The required safety behaviour (COTS Equipment Safety Requirements) is observable at the equipment boundary because they are expressed in terms of effects at the output of the equipment. This can be seen by inspection of the COTS Equipment Safety Requirements in the Requirements Safety Case [REF to Requirements Safety Case].

RS1.1.3 All output states that need to be tested can be stimulated by specified action at the input domain

All output states that need to be tested can be stimulated by specified action at the input domain. This was demonstrated by the successful creation of the test scripts by a person familiar with the application, using the equipment specification to create tests that, for each safety requirement, adequately cover the output range, without identifying any aspects of the requirements as being un-testable. The Test Scripts [REF to Test Scripts] show a comprehensive set of tests for each safety requirement [REF to Requirements Safety Case], and were prepared by [NAME of competent person], who is considered competent [REF to Competency Evaluation] to prepare test scripts and to have had adequate knowledge of the equipment [REF to Equipment Specification] and application.

RS1.1.4 Sufficient state space can be exercised

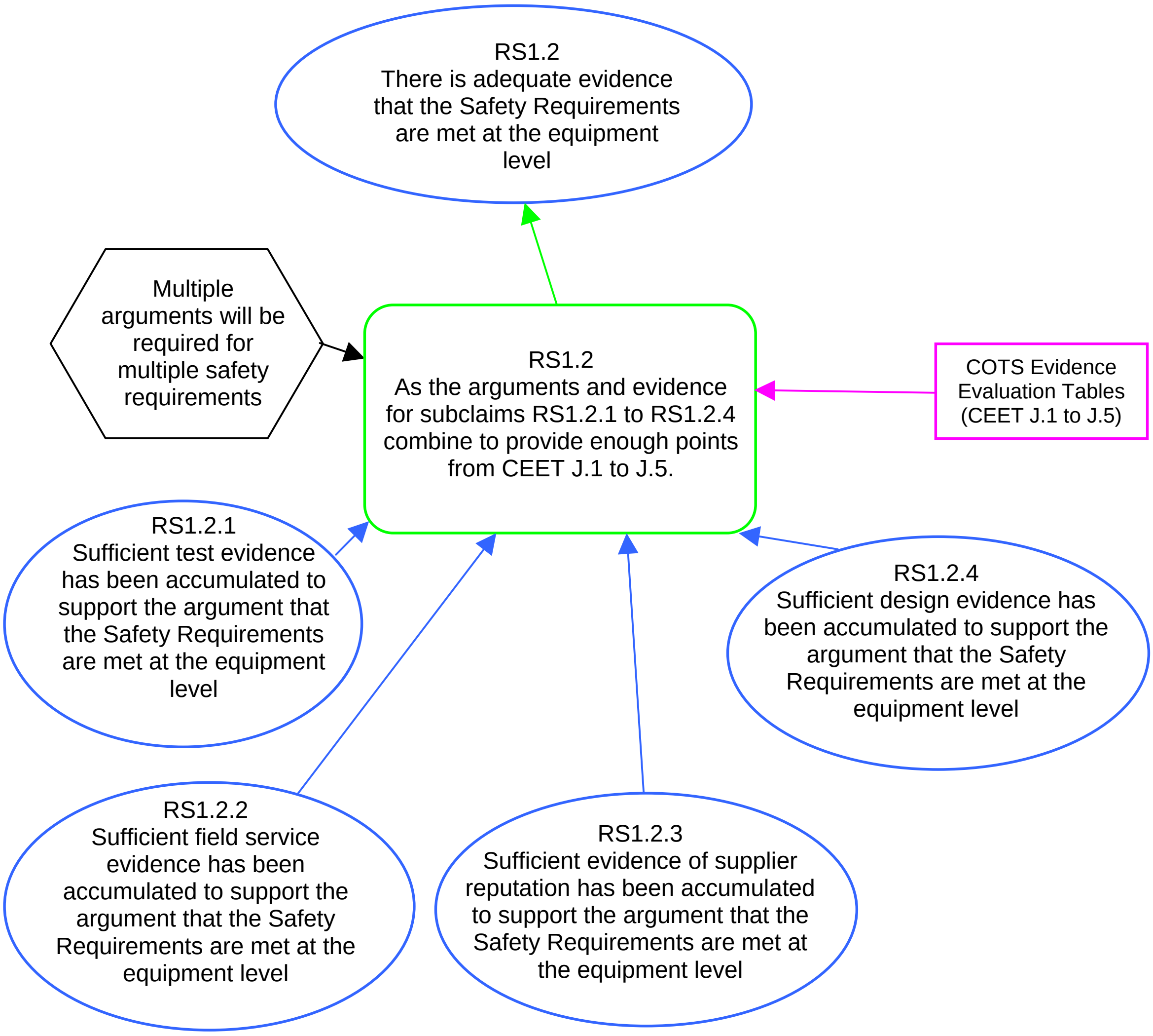
Although the input and output domains of the equipment are known sufficiently to test the full range of outputs, the internal variable domain of the software is not known. Without knowledge of the complexity of the implementation, this safety argument cannot provide assurance that sufficient state space can be exercised. However, due to the mitigations provided by setting requirements at a broadly acceptable level of risk (such that low confidence of requirement satisfaction is required), and the extra initial vigilance on entry to service [REF to Initial Monitoring Instructions], SRG authorises the assumption that meeting the soak or supplier testing requirements in the CEET (Annex J of 'Guidance for Producing SW01 Safety Arguments for COTS Equipment') provides adequate coverage of the state space for simple equipment[19].

The equipment is sufficiently simple and *(either or both of the following)* soak testing *and/ or* supplier test evidence meets the evidence criteria in the CEET [REF to Soak Test Script and Soak Test Results *and/ or* Supplier Test Scripts and Supplier Test Results].

The 'Initial Monitoring Instructions' should attempt to detect and record any behaviour that is not specified in the COTS Equipment Specification.

[19] The claim that "Sufficient state space can be exercised" is far more credible for a 'smaller', single purpose equipment with bespoke platform like a radio than for a 'larger' sub-system based on a more general purpose computing platform. It would not be a credible claim for a cluster of PCs or similar.

RS1.2 There is adequate evidence that the Safety Requirements are met at the equipment level


RS1.2
There is adequate evidence that the Safety Requirements are met at the equipment level
Multiple arguments will be required for multiple safety requirements
RS1.2
As the arguments and evidence for subclaims RS1.2.1 to RS1.2.4 combine to provide enough points from CEET J.1 to J.5.
COTS Evidence Evaluation Tables (CEET J.1 to J.5)
RS1.2.1
Sufficient test evidence has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.4
Sufficient design evidence has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.2
Sufficient field service evidence has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.3
Sufficient evidence of supplier reputation has been accumulated to support the argument that the Safety Requirements are met at the equipment level

In the ‘Guidance for Producing SW01 Safety Arguments for COTS Equipment’, SRG has provided a scheme for determining the level of assurance provided by Requirement Satisfaction evidence. The COTS Evidence Evaluation Table defines criteria for the evidence, and assurance points that can be claimed for that evidence. The Guidance requires that the total of the assurance points must exceed a defined minimum level.

[ANSP] agrees that the assurance provided by evaluation of the COTS equipment, using this scheme, is sufficient[20].

[20] This is effectively a formal statement by the ANSP that the argument is not invalidated by contrary evidence or other circumstances.

Sufficient functional and integrity evidence has been accumulated that shows that the safety requirements are met at the equipment level. This evidence comprises: Test, Field Service, Supplier reputation and Design evidence *[delete as applicable]*.

For each type of evidence, the claim for the number of 'functional points' and 'integrity points' is justified in the arguments that follow, in accordance with the CEET. The points claimed are:

- 100 functional points[21] from test evidence
- I_t integrity points I_t from test evidence (see RS1.2.1)
- I_f integrity points from field service evidence (see RS1.2.2)
- I_s integrity points from supplier reputation evidence (see RS 1.2.3)
- I_d integrity points from design evidence (see RS 1.2.4)

The evidence is judged to be sufficient because the CEET was used to determine that the minimum of 100 functional and 100 (I_t + I_f + I_s + I_d) integrity points has been achieved.

Notes regarding presentation of multiple arguments for multiple groups of Safety Requirements:

It is important that the evidence is credible for each Safety Requirement. The arguments should show this as clearly as possible to ease review and audit. For example, if a single Safety Requirement were selected, then the relevant tests and test records for that requirement must be identifiable, and it is best to include such traceability in the safety argument. The CEET includes some Evidence Satisfaction Criteria that are intended to address this.

***I**t may not be possible (valid) to claim the same level of assurance for all Safety Requirements from a particular source of evidence. For example, even though the CEET requires a similar environment, the available field-service evidence may not have exercised certain features of a product relevant to some Safety Requirements. For those Safety Requirements, alternative evidence must be used and therefore other variants of the arguments used.*

Different arguments may be presented for groups of Safety Requirements, according to the available evidence from test, field service, supplier reputation and design. These arguments could have common elements, for example the claim and argument for FAT and SAT, but might refer to different evidence from field service experience, supplier testing and design evidence.

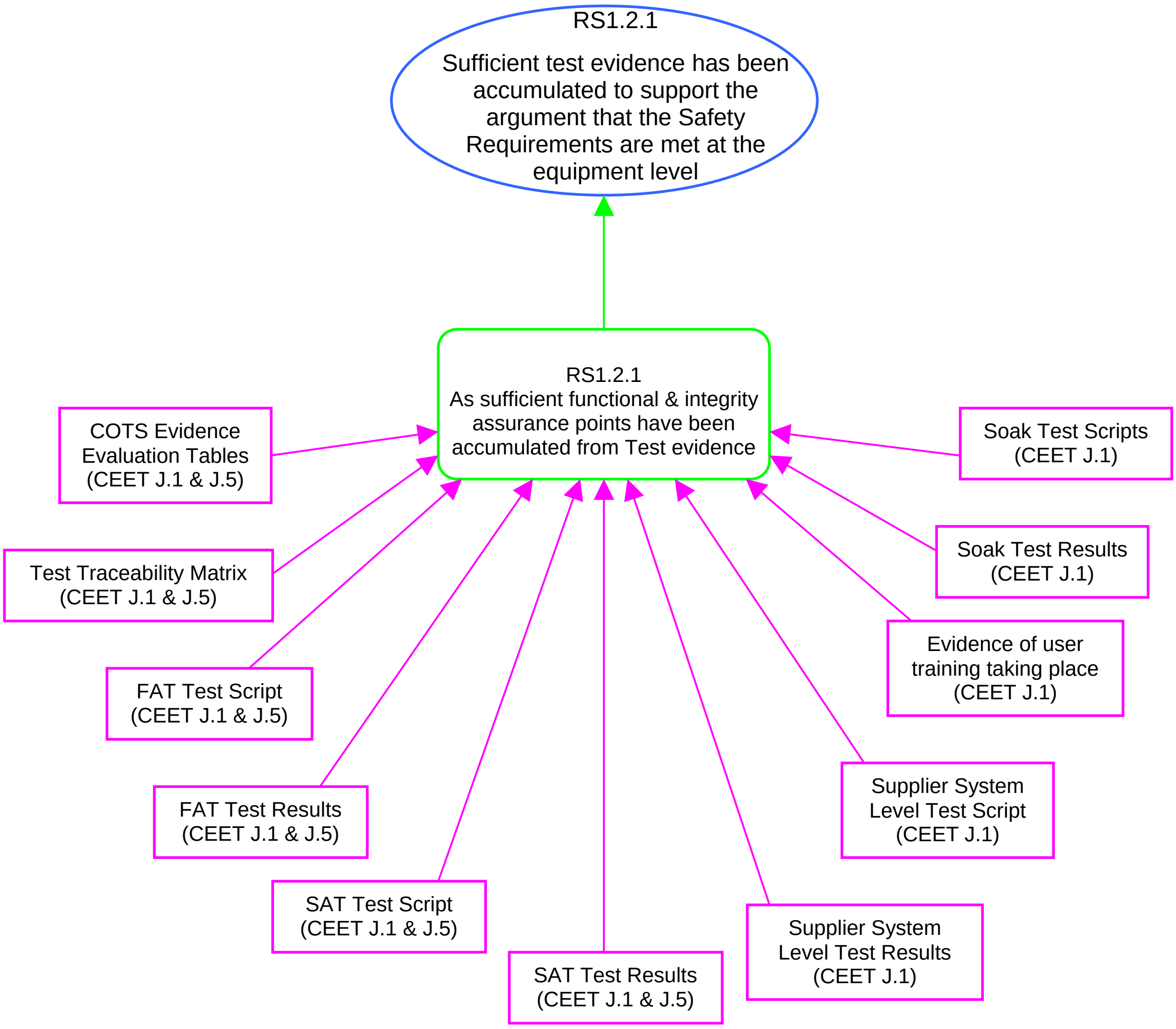
[21] No other result is possible in a complete argument.

The RS1.2 boilerplate text above presents an argument where all Safety Requirements are shown to be satisfied using the same types of evidence. ANSPs may group safety requirements together, according to the requirement satisfaction evidence available, and present separate requirement satisfaction arguments (for the CAE sub-diagram RS1.2 and below) for each group, or even for single safety requirements. Each requirement satisfaction argument sub-diagram must show that 100 functional points and 100 integrity points have been accumulated for each safety requirement in the group.

When there is more than one Safety Requirement group, it must be shown that each Safety Requirement has been allocated to one of the groups.

In practice, at this stage of the Roadmap, the CEET points scheme means that there will be few cases where there are such variations in the points claimed from each evidence type.

RS1.2.1 Test Evidence


RS1.2.1
Sufficient test evidence has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.1
As sufficient functional & integrity assurance points have been accumulated from Test evidence
COTS Evidence Evaluation Tables (CEET J.1 & J.5)
Test Traceability Matrix (CEET J.1 & J.5)
FAT Test Script (CEET J.1 & J.5)
FAT Test Results (CEET J.1 & J.5)
SAT Test Script (CEET J.1 & J.5)
SAT Test Results (CEET J.1 & J.5)
Supplier System Level Test Results (CEET J.1)
Supplier System Level Test Script (CEET J.1)
Evidence of user training taking place (CEET J.1)
Soak Test Results (CEET J.1)
Soak Test Scripts (CEET J.1)

Comparison of the available evidence with the CEET J.1 and J.5 shows that a total of I_t integrity points and 100 functional points can be claimed. This is made up as follows:

All Safety Requirements are shown to have been addressed by tests either in FAT or in SAT [REF to Test Traceability Matrix], meeting the evidence criteria in the CEET J.5. Therefore, 100 functional points are claimed.

FAT has been conducted, and met the evidence criteria in the CEET J.1 [REF to FAT Test Script and FAT Test Results]. No violations of the Safety Requirements were observed during the tests [REF to FAT Test Results]. Therefore x integrity points[22] are claimed.

[22] Here, x is used throughout to denote a number of points derived from the CEET, according to the evidence provided.

SAT has been conducted, and met the evidence criteria in the CEET J.1 [REF to SAT Test Script and SAT Test Results]. No violations of the Safety Requirements were observed during the tests [REF to SAT Test Results]. Therefore x integrity points are claimed.

ANSP Soak Testing (y weeks[23]) has been conducted, and met the evidence criteria in the CEET J.1 [REF to Soak Test Scripts and Soak Test Results]. No violations of the Safety Requirements were observed during the tests [REF to Soak Test Results]. Therefore x integrity points are claimed.

User Training (y weeks) has been conducted, and met the evidence criteria in CEET J.1 [REF to Evidence of user training taking place]. No violations of the Safety Requirements were observed during the training (no counter-evidence available). Therefore x integrity points are claimed.

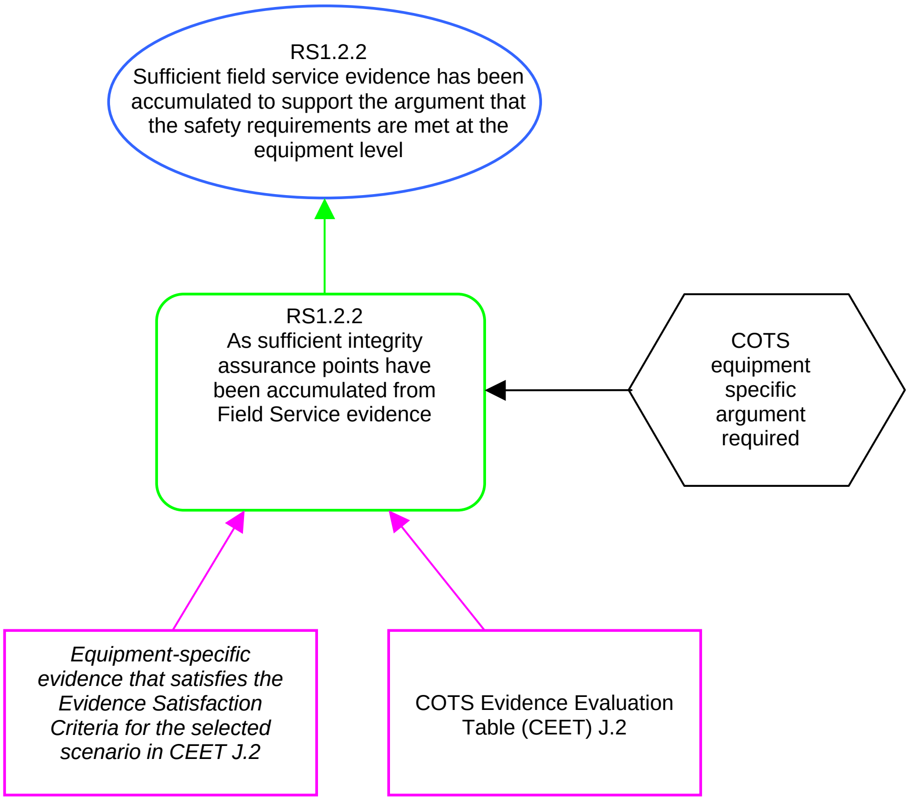
y system-months of Supplier testing (System Level) have been conducted, and met the evidence criteria in the CEET J.1 [REF to Supplier System Level Test Script and Supplier System Level Test Results]. No violations of the Safety Requirements were observed during the tests [REF to Supplier System Level Test Results]. Therefore x integrity points are claimed.

[If applicable] The integrity points total exceeds the maximum claimable for (CEET J.1) for testing of 1 x 10^{-5} requirements, and so this is capped at 75.

In each case, this argument has assumed that the 'Evidence Satisfaction Criteria' in the CEET have been met for each evidence item. In a real argument this should be briefly argued, otherwise each reviewer will need to access the evidence to determine whether the criteria are met.

[23] Here, y is used throughout to denote a period of time specific to the COTS in question.

RS1.2.2 Field Service Evidence


RS1.2.2
Sufficient field service evidence has been accumulated to support the argument that the safety requirements are met at the equipment level
RS1.2.2
As sufficient integrity assurance points have been accumulated from Field Service evidence
COTS equipment specific argument required
Equipment-specific evidence that satisfies the Evidence Satisfaction Criteria for the selected scenario in CEET J.2
COTS Evidence Evaluation Table (CEET) J.2

Comparison of the available evidence with CEET J.2 shows that I_f integrity points can be claimed.

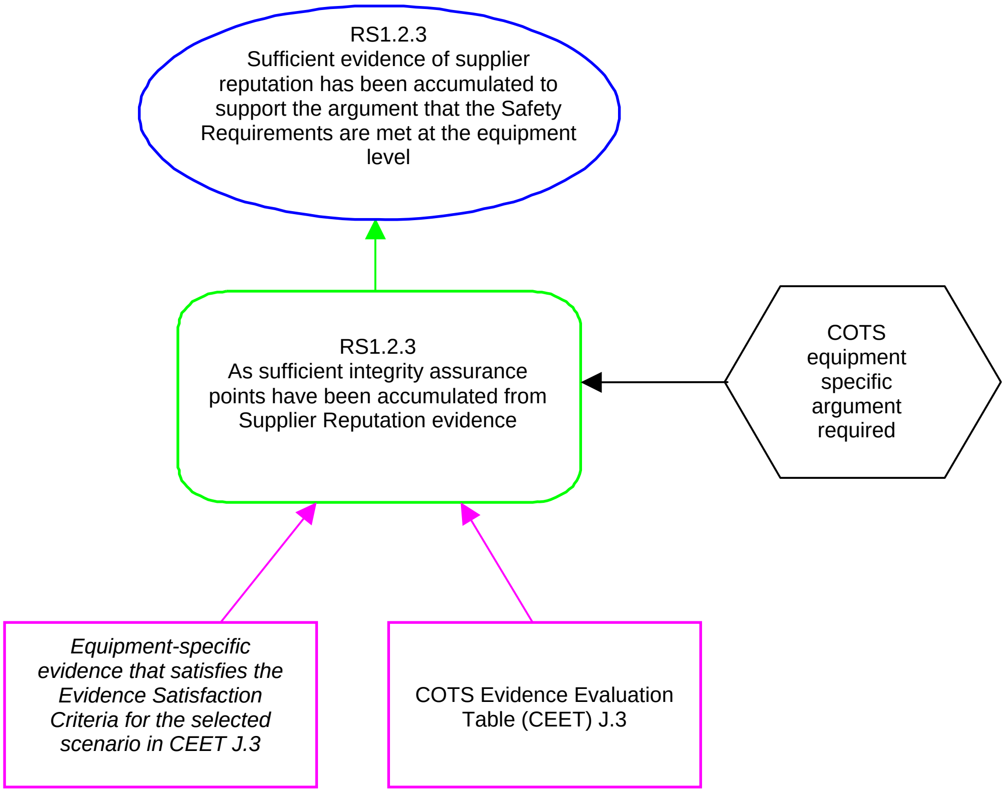
The argument that the field service experience meets the evidence criteria in CEET J.2 is as follows.

*The **COTS equipment specific argument** that needs to be inserted here to claim field service experience will depend on the data held. Having selected a matching Field Service experience scenario from CEET J.2 (e.g. 'Same system on a similar platform'), the argument must show that the available field service experience matches that scenario, and justify that the evidence available meets the Evidence Satisfaction Criteria given in that row of CEET J.2.*

As an example, the argument that the field service for which evidence is held meets the evidence criteria in the CEET for field service experience 'Of the same system on the same platform' could be similar to the following:

Field service experience is being claimed from an equipment that has been operating for 1.5 years at <location>. The equipment is identical to that being justified in this example [REFs to equipment build statement in Doc Y and build statement for operational equipment], and therefore qualifies as 'the same system on the same platform' in the CEET. It also meets the criterion for a similar environment. Analysing the occurrences reported by users [REF to written statement of observed failures in Doc Y], it was found that none contravene the current Safety Requirements, indicating that the future rates are expected to be less than those stipulated for each Safety Requirement.

RS1.2.3 Supplier Reputation Evidence


RS1.2.3
Sufficient evidence of supplier reputation has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.3
As sufficient integrity assurance points have been accumulated from Supplier Reputation evidence
COTS equipment specific argument required
Equipment-specific evidence that satisfies the Evidence Satisfaction Criteria for the selected scenario in CEET J.3
COTS Evidence Evaluation Table (CEET) J.3

Comparison of the available evidence with CEET J.3 shows that I_s integrity points can be claimed.

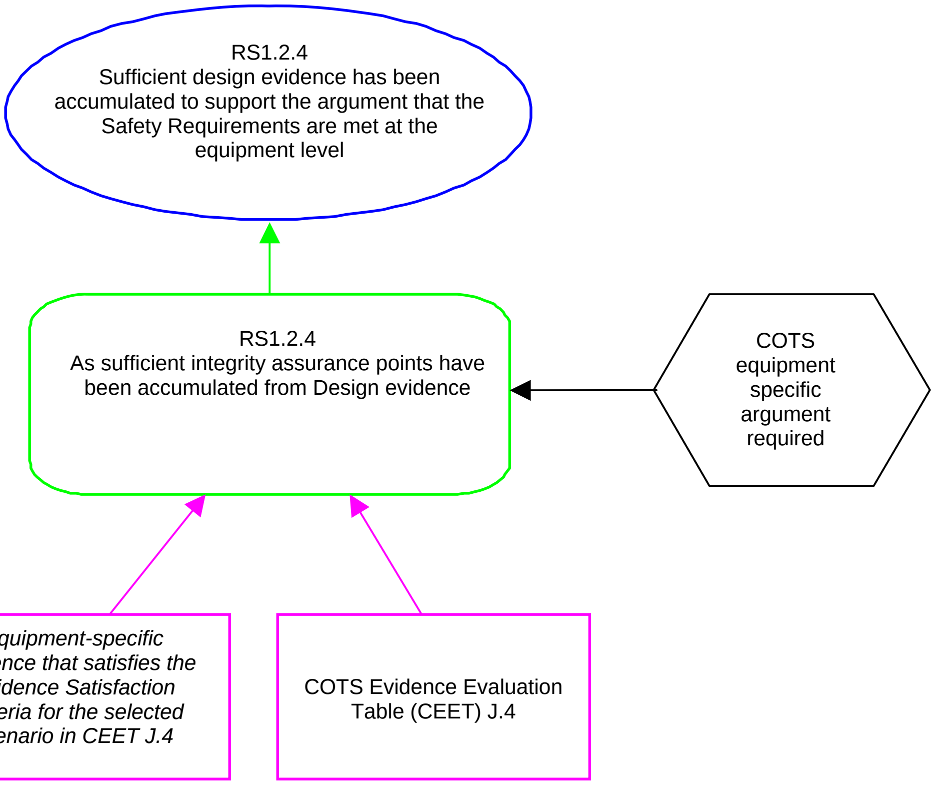
The argument that the supplier experience and expertise evidence meets the evidence criteria in CEET J.3 is as follows.

*The **COTS equipment specific argument** that needs to be inserted here to claim supplier reputation will depend on the data available. Having selected a matching supplier reputation scenario from CEET J.3 (e.g. 'Supplier has experience of deploying systems of the same type into the ATC market'), the argument must show that the available evidence matches that scenario, and justify that it meets the Evidence Satisfaction Criteria given in that row of CEET J.3.*

As an example, the argument that the supplier experience and expertise evidence meets the evidence criteria in CEET J.3 for 'Supplier has experience of deploying systems of the same type into the ATC market' could be similar to the following.

The supplier has been producing similar types of system for greater than 15 years, is experienced in the ATC domain and has delivered systems successfully to other ANSPs and can provide evidence to support the success at these other units. The service history records [REF to service history records] show service records for all equipment of this type. Analysing these records, it was found that no faults occurred that contravene the current Safety Requirements, indicating that the future rates are expected to be less than those stipulated for each Safety Requirement. Additionally, the supplier has provided a statement regarding its experience in the market [REF to supplier experience statement], which shows successful installations at 30 locations over the last 17 years, with no instances of significant faults being reported.

RS1.2.4 Evidence of Design


RS1.2.4
Sufficient design evidence has been accumulated to support the argument that the Safety Requirements are met at the equipment level
RS1.2.4
As sufficient integrity assurance points have been accumulated from Design evidence
COTS equipment specific argument required
Equipment-specific evidence that satisfies the Evidence Satisfaction Criteria for the selected scenario in CEET J.4
COTS Evidence Evaluation Table (CEET) J.4

Comparison of the available design evidence with CEET J.4 shows that I_d integrity points can be claimed.

The argument that the Design evidence meets the evidence criteria in CEET J.4 is as follows.

*The **COTS equipment specific argument** that needs to be inserted here to claim design evidence will depend on the data available. Having selected a matching design evidence scenario from CEET J.4 (e.g. 'Knowledge of internal design features which have been put in place to limit the possibility of unwanted system action"), the argument must show that the available evidence matches that scenario, and justify that it meets the Evidence Satisfaction Criteria given in that row of CEET J.4.*

The intent of this argument is to permit appropriate assurance points to be claimed for using professionally engineered equipment, which has been developed with product assurance in mind and incorporates suitable design features.

If the manufacturer provides sufficient evidence of having followed recognised assurance processes during the development of the COTS equipment, then it is permissible to claim assurance points for these at this stage of the Roadmap. In future stages of the Roadmap the efficacy of these processes will have to be demonstrated.

Professionally engineered equipment usually utilises features that are absent from budget consumer-level equipment, and are designed to address failures, whether caused internally or externally. Examples of these features include checksums, range checking, and anti-jabber circuits.

If the manufacturer provides sufficient details of mitigatory features, in a controlled specification document applicable to the specific version of COTS equipment used, then the relevance of these features to the safety requirements can be considered. If a specified feature provides relevant mitigation for failure to meet a safety requirement, then it is permissible to claim assurance points for it.

Naturally, assurance points for a mitigatory feature only apply to the safety requirement(s) mitigated. When requirement satisfaction is argued for a group of safety requirements (see notes under RS1.2), assurance points from mitigations can only be claimed if there is a relevant mitigation for each safety requirement in the group. Safety requirements not so mitigated would need to be addressed in another group, and arguments presented accordingly.

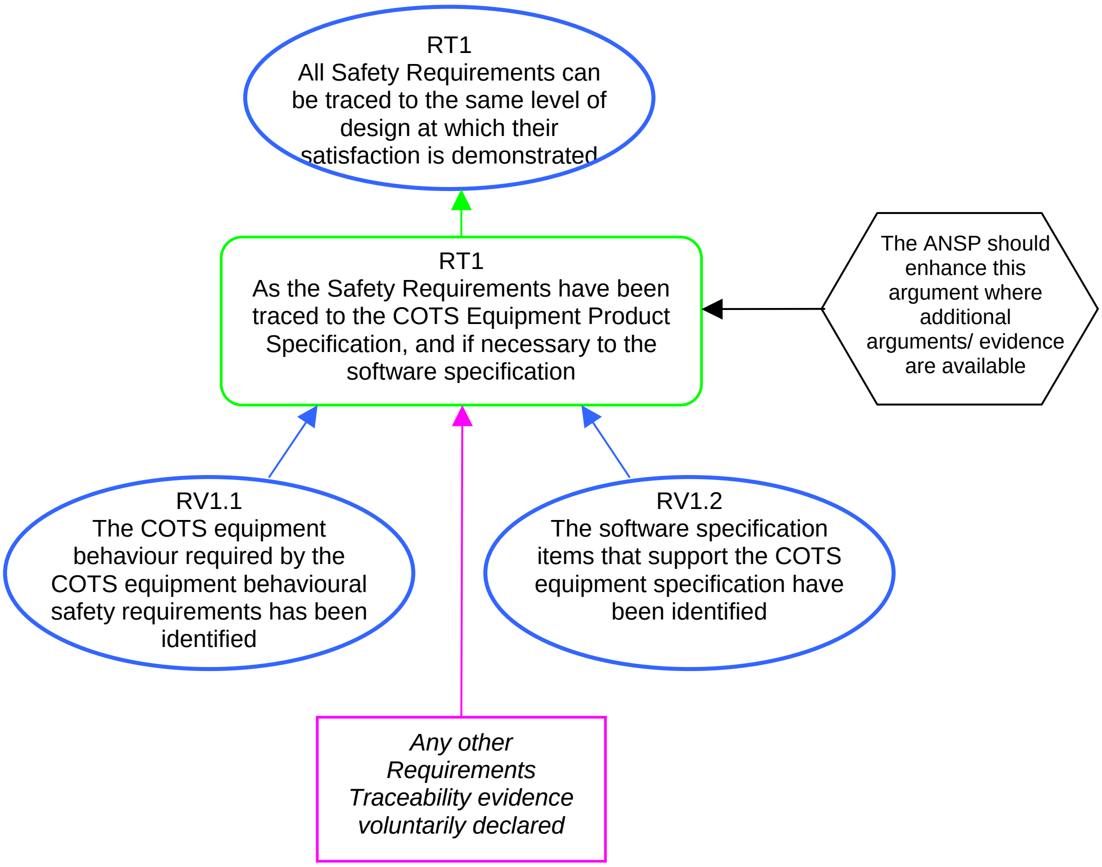
At this stage of the Roadmap mitigatory features are permitted to be implemented in the same software as the function being mitigated (i.e. they are not strictly independent). This admits the mitigation provided when the output of a function is range checked. However, a limiting proviso on this is that there is no obvious common cause for their failure, for example a failure that causes loss of one software function is likely to cause loss (failure) of the mitigatory feature.

It is accepted that some mitigatory features may be impossible to test due to inability to stimulate the error that causes it to operate, but where practical the efficacy of the feature should be tested.

Arguments about design features can be made at the equipment level if they are revealed in the product specification. Alternatively, if they are revealed in the software specification the argument can be made at that level, provided that argument RV1.2 is also addressed in the submitted safety argument.

ANNEX F REQUIREMENTS TRACEABILITY ARGUMENT DIAGRAM TEMPLATE FOR 1 X 10^{-5} REQUIREMENTS

RT1 All Safety Requirements can be traced to the same level of design at which their satisfaction is demonstrated


RT1
All Safety Requirements can be traced to the same level of design at which their satisfaction is demonstrated
RT1
As the Safety Requirements have been traced to the COTS Equipment Product Specification, and if necessary to the software specification
The ANSP should enhance this argument where additional arguments/ evidence are available
RV1.1
The COTS equipment behaviour required by the COTS equipment behavioural safety requirements has been identified
RV1.2
The software specification items that support the COTS equipment specification have been identified
Any other Requirements Traceability evidence voluntarily declared

References to Requirements Validity in this argument are deliberate as at this stage of the Roadmap sufficient assurance of Requirements Traceability may be gained by completing the Requirements Validity argument.

Traceability of the system Safety Requirements to the COTS equipment specification was demonstrated as part of demonstrating that system Safety Requirements have been correctly apportioned to the COTS equipment specification in Requirements Validity (Claim RV1.1).

Either: Therefore, as Requirement Satisfaction is demonstrated at the COTS equipment level, the system Safety Requirements are traceable to the level at which Requirement Satisfaction is demonstrated.

Or: *Text for when 'knowledge of internal design features' is used in the Requirement Satisfaction argument:* Traceability of the COTS equipment specification to the COTS Software Specification (Claim RV1.2) was established as part of the successful demonstration of Requirements Validity.

Therefore, as Requirement Satisfaction is demonstrated at the COTS equipment level, supplemented by 'knowledge of internal design features,' the system Safety Requirements are traceable to the level at which Requirement Satisfaction is demonstrated.

In theory Requirements Traceability needs to support the Non-Interference argument in addition to the Requirement Satisfaction argument. Currently, this Guidance permits sufficient assurance of non-interference to be claimed from the same evidence used in the Requirement Satisfaction argument, and therefore no additional Requirements Traceability is required to support the Non-Interference argument. (The Non-Interference argument would normally be required to support the Requirement Satisfaction argument, because the COTS equipment specification is unlikely to completely specify the behaviour of the COTS equipment).

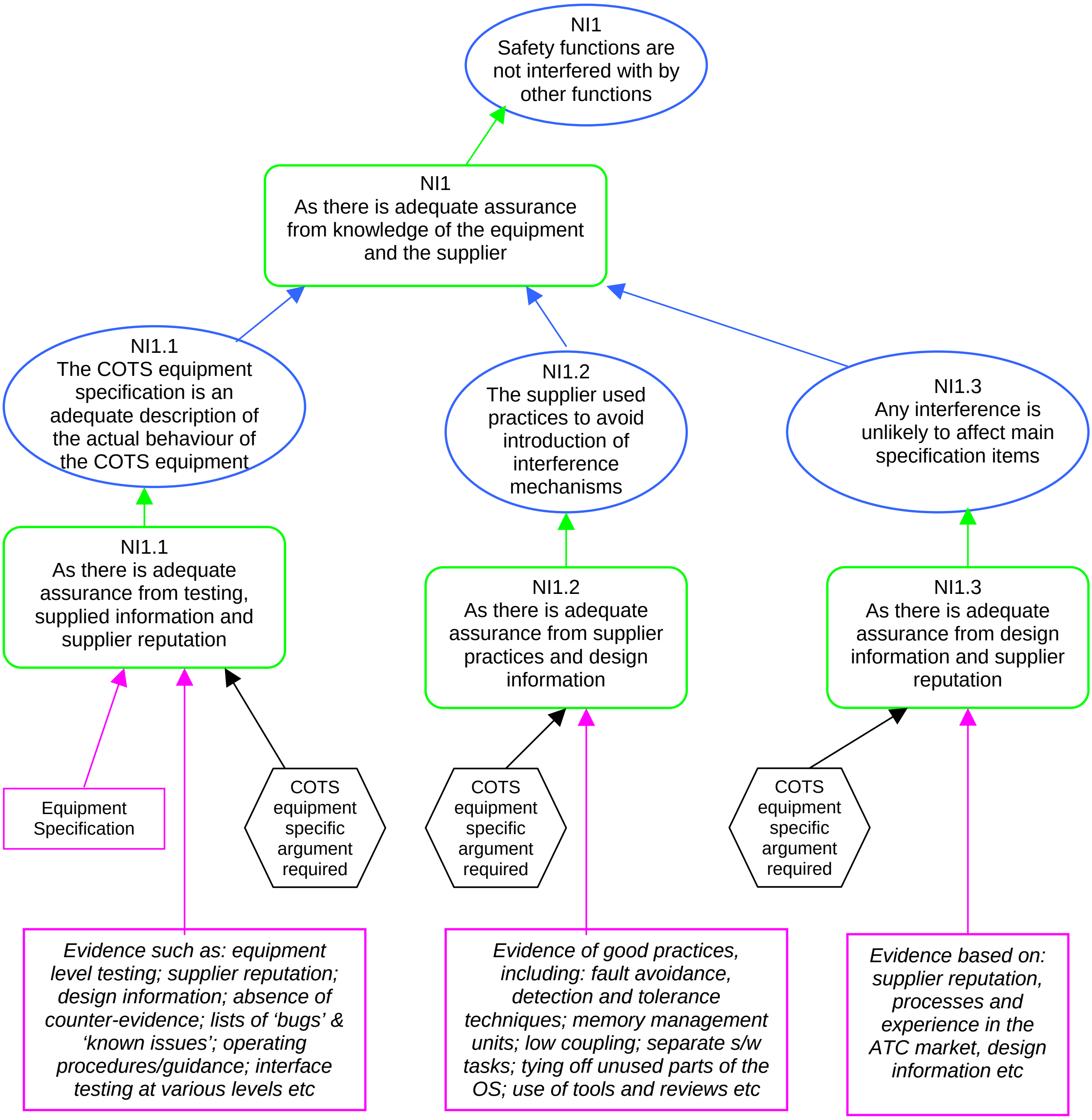
ANSPs should reference any directly relevant Requirements Traceability evidence items, and consider what the evidence shows about requirements traceability. It is not currently mandatory to seek additional evidence for Requirements Traceability.

The Requirements Validity argument uses traceability matrices and the Requirement Satisfaction argument requires a traceability matrix from requirements to tests and results (see the CEET J.1 and J.5).

Some forms of evidence (e.g. supplier reputation) can apply to set of requirements 'en masse' and so cannot be traced to a specific requirement.

ANNEX G NON-INTERFERENCE ARGUMENT DIAGRAM TEMPLATE FOR 1 X 10^{-5} REQUIREMENTS

NI1 Safety functions are not interfered with by other functions


NI1
Safety functions are not interfered with by other functions
NI1
As there is adequate assurance from knowledge of the equipment and the supplier
NI1.1
The COTS equipment specification is an adequate description of the actual behaviour of the COTS equipment
NI1.2
The supplier used practices to avoid introduction of interference mechanisms
NI1.3
Any interference is unlikely to affect main specification items
NI1.1
As there is adequate assurance from testing, supplied information and supplier reputation
NI1.2
As there is adequate assurance from supplier practices and design information
NI1.3
As there is adequate assurance from design information and supplier reputation
Equipment Specification
COTS equipment specific argument required
COTS equipment specific argument required
COTS equipment specific argument required
Evidence such as: equipment level testing; supplier reputation; design information; absence of counter-evidence; lists of 'bugs' & 'known issues'; operating procedures/guidance; interface testing at various levels etc
Evidence of good practices, including: fault avoidance, detection and tolerance techniques; memory management units; low coupling; separate s/w tasks; tying off unused parts of the OS; use of tools and reviews etc
Evidence based on: supplier reputation, processes and experience in the ATC market, design information etc

References to Requirements Satisfaction in this argument are deliberate as at this stage of the Roadmap sufficient assurance of Non-Interference may be gained by completing the Requirements Satisfaction argument.

The non-interference argument is mainly COTS equipment specific. This example provides several conjectured arguments for non-interference to indicate the relevant types of argument and evidence.

Currently, sufficient assurance of non-interference may be claimed from the same evidence used in the Requirement Satisfaction argument, although ANSPs may choose to provide additional evidence. ANSPs must submit COTS equipment specific arguments, perhaps based on the conjectured arguments, and reference the available relevant evidence items.

The COTS equipment specification is an adequate description of the actual behaviour of the COTS equipment (Claim NI1.1). Requirement Satisfaction confirms that this is true for the specification elements that relate to COTS equipment behavioural Safety Requirements. Therefore, other behaviour within the equipment does not interfere with the safety functions.

Additionally, the supplier used practices to avoid introduction of interference mechanisms (Claim NI1.2), and even if these failed to prevent interference, any such interference (unknown behaviour) is unlikely to affect main specification items of the COTS equipment in its declared specification (Claim NI1.3).

Therefore, safety functions are not interfered with by other functions.

NI1.1 The COTS equipment specification is an adequate description of the actual behaviour of the COTS equipment

The completeness of the supplier's specification cannot be fully known, but assurance can be gained to an extent commensurate with safety risk.

If the COTS equipment specification [REF Equipment Specification] specified all the behaviour of the COTS equipment, then there would be no additional behaviour to interfere with that behaviour. In these circumstances, if all elements of the COTS equipment specification relating to the COTS equipment behavioural Safety Requirements had been identified (i.e. Requirements Validity) and then verified (i.e. Requirements Satisfaction), then any other behaviour could not interfere with the safety functions, and the non-interference objective would be met.

The COTS equipment specification is considered adequately complete because:

*A **COTS equipment specific argument** should be made showing how this assurance is gained from available evidence, for example:*

- *Equipment-level testing (which is commensurate with perceived risk) is conducted over the range of expected operational scenarios, which should inherently reveal relevant undefined behaviour*
- *Supplier reputation*
- *Provided design information*
- *Absence of counter-evidence, e.g. tests may identify undocumented behaviour*
- *The level of detail regarding behaviour provided in the specification*
- *The provision of lists of ‘bugs’, ‘known issues’, etc*
- *The provision of operating procedures, or guidance.*

This could be augmented by drawing on interface testing at various levels of design, if the supplier were to provide such evidence.

NI1.2 The supplier used practices to avoid introduction of interference mechanisms

Suppliers adopt common good practices that are intended to result in a product that works to its requirements, and therefore they naturally avoid creating mechanisms that can lead to interference.

*A **COTS equipment specific argument** should be made showing how this assurance is gained from available evidence, for example, relevant practices can include:*

- *Fault avoidance techniques in general*
- *Fault detection and fault tolerant techniques may be used*
- *Use of memory management units*
- *Use of low coupling in the software design*
- *Creation of separate software tasks*
- *'Tying off' unnecessary functionality and services in Operating Systems*
- *Use of tools and reviews are used to encourage/enforce these practices.*

The exact arguments that can be made here depend on what evidence the supplier can provide.

NI1.3 Any interference is unlikely to affect main specification items of the COTS equipment in its declared specification

This is primarily drawn from belief in the quality of the processes used by the supplier, and the experience of the supplier in the Air Traffic Control and similar markets.

It is not in the interests of any reputable supplier to market goods that do not meet their specification, and so the supplier's activities/procedures are designed to prevent the incorporation of behaviour that adversely affects specified behaviour of the equipment.

Given the absence of malevolent intent, the effect of any unintended interference should be insignificant.

*A **COTS equipment specific argument** should be made showing how this assurance is gained from available evidence, for example:*

- *Supplier reputation*
- *Previous ANSP experience of the supplier*
- *Provided design information*
- *Supplier process evidence*
- *The level of detail regarding behaviour provided in the specification.*

ANNEX H (ANNEX DELETED)

ANNEX I CEET REQUIREMENTS NO MORE ONEROUS THAN 1 X 10^{-4}

The COTS Evidence Evaluation Table (CEET) for Requirements no more onerous than 1 x 10^{-4} is split into a number of tables that address the functional and integrity assurance aspects of the Safety Requirements. The tables presented are:

a) Integrity assurance:

- Testing: Table I.1
- Field service: Table I.2
- Supplier experience and reputation: Table I.3
- Supplier Software design and development: Table I.4

b) Functional assurance: Table I.5

At this stage of the Roadmap, the two CEETs (Annexes I and J) invoke the same evidence, although the assurance points awarded are different. At future Roadmap stages, the two CEETs may diverge. Currently, the only deliberate difference in the specified evidence is in the last row of table I.4/J.4 and is due to the differences in the arguments.

<table>
<tr><td colspan="4"><b>Table I.1: INTEGRITY Assurance Points</b></td><td><b>1 x 10^{-4}</b></td></tr>
<tr><td><b>Testing</b></td><td colspan="4"><b>A maximum of 90 points can be claimed for testing. Partial claims are not acceptable. Either the satisfaction criteria are met and the full points claimed or no points are claimed.</b>
<b>IT IS MANDATORY TO HAVE EITHER FAT OR SAT</b>
<b>IT IS MANDATORY TO HAVE EITHER ANSP SOAK TESTING OR SUPPLIER TESTING</b></td></tr>
<tr><td><b>Specific Testing (Site Acceptance)</b></td><td>Full test</td><td></td><td></td><td><b>Evidence Satisfaction Criteria</b></td></tr>
<tr><td>This testing is essentially designed to prove that the delivered system, after installation and commissioning, provides all of the required functionality. There is limited assurance as to whether the system will continue to operate in the same way with time in this testing.</td><td>20</td><td></td><td></td><td rowspan="3">1. Test Script.
2. Test Results.
3. Test Traceability matrix.
Each functional Safety Requirement must be tested either during site or factory testing.
Testing must include the extremes of conditions under which the system is expected to operate.
Objective evidence of testing (and passing) of all functional Safety Requirements by providing traceability of Safety Requirement to test script to successful result.</td></tr>
<tr><td><b>Specific Testing (Factory Acceptance)</b></td><td>Full test</td><td></td><td></td></tr>
<tr><td>This testing is essentially designed to prove that the system, prior to leaving the factory, provides all of the required functionality. There is limited assurance as to whether the system will continue to operate in the same way with time in this testing.</td><td>20</td><td></td><td></td></tr>
<tr><td><b>ANSP Soak Testing (including post Soak Testing observation)</b></td><td>1 week</td><td>2 weeks</td><td>1 month</td><td><b>Evidence Satisfaction Criteria</b></td></tr>
<tr><td>Running the system for a period of time (without reset) while it is exposed to a range of inputs which simulate the normal expected range of inputs - followed by a functional test (also without resetting the system) will give confidence that the system can continue to perform its function with time. The duration of time for which the system has been tested in this way together with any procedures that limit its expected operational time between resets will affect the level of confidence gained.</td><td>50</td><td>60</td><td>70</td><td>1. Test Script.
2. Test Results.
Objective evidence of testing (and passing).</td></tr>
</table>

Table I.1: INTEGRITY Assurance Points				**1 x 10^{-4}**
Testing	**A maximum of 90 points can be claimed for testing. Partial claims are not acceptable. Either the satisfaction criteria are met and the full points claimed or no points are claimed.** **IT IS MANDATORY TO HAVE EITHER FAT OR SAT** **IT IS MANDATORY TO HAVE EITHER ANSP SOAK TESTING OR SUPPLIER TESTING**			
Use of system for training	1 week	2 weeks	1 month	**Evidence Satisfaction Criteria**
The use of a system for user training will expose it to an independent set of user inputs that has the potential to expose previously un-noticed bugs in the system. This use of the system, assuming it is fault free, will also add to the overall confidence of operating the system.	20	30	40	Evidence that system has been used for training over the claimed period with no reported faults. (Note that where a fault is exposed and adequately mitigated the points can still be claimed). This evidence could be, for example, Training Plan and Records or Training Error Log
Supplier testing (System Level)	1 system-month	2 system-months	6 system-months	**Evidence Satisfaction Criteria**
As with ANSP Soak Testing, running the system for a period of time (without reset) while it is exposed to a range of inputs which simulate the normal expected range of inputs followed by a functional test (also without resetting the system) will give confidence that the system can continue to perform its function with time. The duration of time for which the system has been tested in this way together with any procedures that limit its expected operational time between resets will affect the level of confidence gained.	50	55	60	1. Test Script. 2. Test Results. Objective evidence of testing (and passing).

Table I.1: Integrity assurance from Testing

Table I.2: INTEGRITY Assurance Points				**1 x 10^{-4}**
Field service experience	**Only one item from Field service experience can be claimed**			
Of the same system on the same platform	1 system-year	5 system-years	10 system-years	**Evidence Satisfaction Criteria**
ATC systems operate in a very similar environment in terms of their inputs and outputs wherever they are deployed. Evidence of in service experience of the same system, together with information on the faults experienced in that time has the potential to provide the greatest confidence in the integrity of the system.	10	40	80	o **Equipment Build statement.** o **Statement of observed failures.** (Any failures that do not meet the Safety Requirement would result in not claiming points). o **Location meets criterion for similar environment.** Consideration of the operational environment where in service data is being claimed is adequately representative of the final operational environment.
Of an earlier version of the same system on the same platform	1 system-year	5 system-years	10 system-years	**Evidence Satisfaction Criteria**
An earlier version of the same system that reuses a very large percentage (95%) of the same code and is likely to exercise all of the hardware in the same way. Evidence of in service experience of such a system, together with information on the faults experienced in that time has the potential to provide a high degree of confidence in the integrity of the system.	10	30	65	o **Equipment Build statement.** Evidence from the supplier that 95% of the code is unchanged. o **Statement of observed failures.** (Any failures that do not meet the Safety Requirement would result in not claiming points). o **Location meets criterion for similar environment.** Consideration of the operational environment where in service data is being claimed is adequately representative of the final operational environment.

Table I.2: INTEGRITY Assurance Points				**1×10^{-4}**
Field service experience	**Only one item from Field service experience can be claimed**			
Of the same system on a similar platform (Operating System and or hardware)	1 system-year	5 system-years	10 system-years	**Evidence Satisfaction** **Criteria**
Systems that have been ported onto a new platform, which have minor hardware changes and uses the same application code. Considerable confidence can be achieved from evidence of the fault free performance of such systems. (This is to cater for situations such as same PC can no longer be purchased and the change is not significant for this application e.g. only change is CPU speed). To claim these points a reasoned argument with evidence would need to be presented, which included analysis of the platform changes (demonstrating that the changes have no impact on the application). An example of such evidence would be Microsoft Certification.	4	16	32	o **Equipment Build statement.** Evidence from the supplier that 100% of the application code is unchanged (NB application code excludes Operating System and Drivers). o **Statement of observed failures.** (Any failures that do not meet the Safety Requirement would result in not claiming points**).** o **Location meets criterion for similar environment.** Consideration of the operational environment where in service data is being claimed is adequately representative of the final operational environment.

Table I.2: INTEGRITY Assurance Points				**1 x 10^{-4}**
Field service experience	**Only one item from Field service experience can be claimed**			
Of the same system on a previous platform (Operating System and or hardware)	1 system-year	5 system-years	10 system-years	**Evidence Satisfaction** **Criteria**
Systems that have been ported onto a new platform (usually either for performance or obsolescence reasons) will re-use much if not all of the same application code. Considerable confidence can be achieved from evidence of the fault free performance of such systems.	2	8	16	o **Equipment Build statement.** Evidence from the supplier that 95% of the application code is unchanged. o **Statement of observed failures.** (Any failures that do not meet the Safety Requirement would result in not claiming points**).** o **Location meets criterion for similar environment.** Consideration of the operational environment where in service data is being claimed is adequately representative of the final operational environment.
Of a similar system by the same supplier	1 system-year	5 system-years	10 system-years	**Evidence Satisfaction** **Criteria**
Evidence that demonstrates that the supplier has deployed a similar system (similar use and some code re-use) may provide some confidence.	0	0	5	Evidence of an adequately low failure rate of re-used code. Minimum of 5% of re-used code.

Table I.2: Integrity assurance from field service data

Table I.3: INTEGRITY Assurance Points				**1 x 10^{-4}**
Supplier experience and expertise	**A maximum of 20 can be claimed from supplier experience and expertise**			
Supplier has experience of deploying systems of the same type into the ATC market	5 years experience	10 years experience	>15 years experience	**Evidence Satisfaction Criteria**
The ATC environment is very complex and suppliers having fielded systems of the same type into the market gives confidence in their understanding of the requirements and the issues surrounding the use of their systems.	5	10	15	Evidence of the supplier having a successful track record for the specified number of years in a relevant market sector.
Supplier personnel involved with the COTS equipment have demonstrated expert knowledge in the field in which they are working	Low confidence	Medium confidence	High Confidence	**Evidence Satisfaction Criteria**
The ATC environment is very complex and engineers having experience of fielded systems of the same type into the market gives confidence in their understanding of the requirements and the issues surrounding the use of their systems.	10	15	20	Evaluation of CVs of key personnel involved in the development and support of the COTS equipment.

Table I.3: Integrity assurance from supplier experience and expertise

Table I.4: INTEGRITY Assurance Points				**1 x 10^{-4}**
Supplier Software design / development	**A maximum of 30 can be claimed from supplier software design / development**			
Supplier can demonstrate successfully following an appropriate development process in the development of the system	To level below recommendation	To level meeting recommendation	To level above recommendation	**Evidence Satisfaction Criteria**
Processes such as IEC 61508 or ED 109 or other standards/processes that give confidence of the integrity of the software i.e. It has been designed in a consistent and documented manner and infers some level of review. This gives confidence that the coding will be robust. These processes apply recommended levels of rigour that vary with the integrity requirement on the software being produced.	10	25	30	1. Certificate of Conformance for the Product in question; **OR** 2. Independent Audit of conformance; **OR** 3. Independent Audit of Justified Supplier Procedures. Note: Independent is independent of the product development / support team.
Knowledge of internal design features which have been put in place to limit the possibility of unwanted system action	Some features	Comprehensive features	▨	**Evidence Satisfaction Criteria**
Features in a system such as limiting the range on inputs to those expected or remove unwanted elements of an Operating System to ensure non-interference, greatly increase confidence that the system will not act abnormally.	5	10	▨	Design Documentation supporting claimed features AND evidence of their efficacy. Note: If design features at software level are argued, then arguments would need to be presented showing Traceability from the requirements to the features.

Table I.4: Integrity assurance from supplier design and development methods

Table I.5: <u>FUNCTIONAL</u> Assurance Points				**1 x 10^{-4}**
Testing	**Functional assurance requirements can be fully satisfied through testing alone** **IT IS MANDATORY TO ACHIEVE COVERAGE OF ALL FUNCTIONAL SAFETY REQUIREMENTS THROUGH FAT OR SAT**			
Specific Testing (Site Acceptance)	Full test	▨	▨	**Evidence Satisfaction Criteria**
This testing is essentially designed to prove that the delivered system, after installation and commissioning, provides all of the required functionality.	100	▨	▨	1. Test Script. 2. Test Results. 3. Test Traceability matrix. Each functional Safety Requirement must be tested either during site or factory testing. Testing must include the extremes of conditions under which the system is expected to operate. Objective evidence of testing (and passing) of all functional Safety Requirements by providing traceability of Safety Requirement to test script to successful result. Note: These are the same criteria as those required to claim Integrity points from SAT and FAT.
Specific Testing (Factory Acceptance)		▨	▨	
This testing is essentially designed to prove that the system, prior to leaving the factory, provides all of the required functionality. Often this can include tests that cannot be repeated on site, particularly where a test harness is required and measurements related to timing and processor loading are being made.		▨	▨	

Table I.5 Functional assurance from 100% test coverage of functional Safety Requirements

ANNEX J CEET REQUIREMENTS NO MORE ONEROUS THAN 1 X 10^{-5}

The COTS Evidence Evaluation Table (CEET) for requirements no more onerous than 1 x 10^{-5} is split into a number of tables that address the functional and integrity assurance aspects of the Safety Requirements. The tables presented are:

- Integrity assurance:
    - Testing: Table J.1
    - Field service: Table J.2
    - Supplier experience and reputation: Table J.3
    - Supplier Software design and development: Table J.4
- Functional assurance: Table J.5

At this stage of the Roadmap, the two CEETs (Annexes I & J) invoke the same evidence, although the assurance points awarded are different. At future Roadmap stages, the two CEETs may diverge. Currently, the only deliberate difference in the specified evidence is in the last row of table I.4/J.4 and is due to the differences in the arguments.

Table J.1: INTEGRITY Assurance Points — 1×10^{-5}

Testing

A maximum of 75 points can be claimed for testing. Partial claims are not acceptable. Either the satisfaction criteria are met and the full points claimed or no points are claimed

IT IS MANDATORY TO HAVE EITHER FAT OR SAT

IT IS MANDATORY TO HAVE EITHER ANSP SOAK TESTING OR SUPPLIER TESTING

Specific Testing (Site Acceptance)	Full test	▨	▨	**Evidence Satisfaction Criteria**
This testing is essentially designed to prove that the delivered system, after installation and commissioning, provides all of the required functionality. There is limited assurance as to whether the system will continue to operate in the same way with time in this testing.	10	▨	▨	1. Test Script. 2. Test Results. 3. Traceability matrix. Each functional Safety Requirement must be tested either during site or factory testing. Testing must include the extremes of conditions under which the system is expected to operate. Objective evidence of testing (and passing) of all functional Safety Requirements by providing traceability of Safety Requirement to test script to successful result.
Specific Testing (Factory Acceptance)	Full test	▨	▨	
This testing is essentially designed to prove that the system, prior to leaving the factory, provides all of the required functionality. There is limited assurance as to whether the system will continue to operate in the same way with time in this testing.	10	▨	▨	
ANSP Soak Testing (including post Soak Testing observation)	1 week	2 weeks	1 month	**Evidence Satisfaction Criteria**
Running the system for a period of time (without reset) while it is exposed to a range of inputs which simulate the normal expected range of inputs - followed by a functional test (also without resetting the system) will give confidence that the system can continue to perform its function with time. The duration of time for which the system has been tested in this way together with any procedures that limit its expected operational time between resets will affect the level of confidence gained.	30	35	40	1. Test Script. 2. Test Results. Objective evidence of testing (and passing).
Use of system for training	1 week	2 weeks	1 month	**Evidence Satisfaction Criteria**
The use of a system for user training will expose it to an independent set of user inputs that has the potential to expose previously un-noticed bugs in the system. This use of the system, assuming it is fault free, will also add to	10	15	20	Evidence that system has been used for training over the claimed period with no reported faults. (Note that where a fault is exposed and adequately mitigated

Table J.1: INTEGRITY Assurance Points	**1 x 10^{-5}**
Testing	**A maximum of 75 points can be claimed for testing. Partial claims are not acceptable. Either the satisfaction criteria are met and the full points claimed or no points are claimed** **IT IS MANDATORY TO HAVE EITHER FAT OR SAT** **IT IS MANDATORY TO HAVE EITHER ANSP SOAK TESTING OR SUPPLIER TESTING**

the overall confidence of operating the system.				the points can still be claimed). This evidence could be, for example, Training Plan and Records or Training Error Log.
Supplier testing (System Level)	1 system-month	2 system-months	6 system-months	**Evidence Satisfaction Criteria**
As with ANSP Soak Testing, running the system for a period of time (without reset) while it is exposed to a range of inputs which simulate the normal expected range of inputs followed by a functional test (also without resetting the system) will give confidence that the system can continue to perform its function with time. The duration of time for which the system has been tested in this way together with any procedures that limit its expected operational time between resets will affect the level of confidence gained.	30	35	40	1. Test Script. 2. Test Results. Objective evidence of testing (and passing).

Table J.1: Integrity assurance from Testing

Table J.2: INTEGRITY Assurance Points				**1 x 10^{-5}**
Field service experience	**Only one item from Field service experience can be claimed**			
Of the same system on the same platform	1 system -year	5 system -years	10 system -years	**Evidence Satisfaction Criteria**
ATC systems operate in a very similar environment in terms of their inputs and outputs wherever they are deployed. Evidence of in service experience of the same system, together with information on the faults experienced in that time has the potential to provide the greatest confidence in the integrity of the system.	10	40	80	o **Equipment Build statement.** o **Statement of observed failures.** (Any failures that do not meet the Safety Requirement would result in not claiming points). o **Location meets criterion for similar environment.** Consideration of the operational environment where in service data is being claimed is adequately representative of the final operational environment.
Of an earlier version of the same system on the same platform	1 system-year	5 system-years	10 system-years	**Evidence Satisfaction Criteria**
An earlier version of the same system that reuses a very large percentage (95%) of the same code and is likely to exercise all of the hardware in the same way. Evidence of in service experience of such a system, together with information on the faults experienced in that time has the potential to provide a high degree of confidence in the integrity of the system.	10	30	65	o **Equipment Build statement.** Evidence from the supplier that 95% of the code is unchanged. o **Statement of observed failures.** (Any failures that do not meet the Safety Requirement would result in not claiming points). o **Location meets criterion for similar environment.** Consideration of the operational environment where in service data is being claimed is adequately representative of the final operational environment.
Of the same system on a similar platform (Operating System and or hardware)	1 system-year	5 system-years	10 system-years	**Evidence Satisfaction Criteria**
Systems that have been ported onto a new platform, which have minor hardware changes and uses the same application code. Considerable confidence can be achieved from evidence of the fault free performance of such systems.	4	16	32	o **Equipment Build statement.** Evidence from the supplier that 100% of the application code is unchanged (NB application code excludes Operating System and Drivers). o **Statement of observed**

Table J.2: INTEGRITY Assurance Points				**1×10^{-5}**
Field service experience	**Only one item from Field service experience can be claimed**			
(This is to cater for situations such as same PC can no longer be purchased and the change is not significant for this application e.g. only change is CPU speed). To claim these points a reasoned argument with evidence would need to be presented, which included analysis of the platform changes (demonstrating that the changes have no impact on the application). An example of such evidence would be Microsoft Certification.				**failures.** (any failures which do not meet the Safety Requirement would result in not claiming points) o **Location meets criterion for similar environment.** Consideration of the operational environment where in service data is being claimed is adequately representative of the final operational environment.
Of the same system on a previous platform (Operating System and or hardware)	1 system-year	5 system-years	10 system-years	**Evidence Satisfaction Criteria**
Systems that have been ported onto a new platform (usually either for performance or obsolescence reasons) will re-use much if not all of the same application code. Considerable confidence can be achieved from evidence of the fault free performance of such systems.	2	8	16	o **Equipment Build statement.** Evidence from the supplier that 95% of the application code is unchanged. o **Statement of observed failures.** (Any failures that do not meet the Safety Requirement would result in not claiming points). o **Location meets criterion for similar environment.** Consideration of the operational environment where in service data is being claimed is adequately representative of the final operational environment.
Of a similar system by the same supplier	1 system-year	5 system-years	10 system-years	**Evidence Satisfaction Criteria**
Evidence that demonstrates that the supplier has deployed a similar system (similar use and some code re-use) may provide some confidence.	0	0	5	Evidence of an adequately low failure rate of re-used code. Minimum of 5% of re-used code.

Table J.2: Integrity assurance from field service data

Table J.3: INTEGRITY Assurance Points				**1 x 10^{-5}**
Supplier experience and expertise	**A maximum of 20 can be claimed from supplier experience and expertise**			
Supplier has experience of deploying systems of the same type into the ATC market	5 years experience	10 years experience	>15 years experience	**Evidence Satisfaction Criteria**
The ATC environment is very complex and suppliers having fielded systems of the same type into the market gives confidence in their understanding of the requirements and the issues surrounding the use of their systems.	5	10	15	Evidence of the supplier having a successful track record for the specified number of years in a relevant market sector.
Supplier personnel involved with the COTS equipment have demonstrated expert knowledge in the field in which they are working	Low confidence	Medium confidence	High Confidence	**Evidence Satisfaction Criteria**
The ATC environment is very complex and engineers having experience of fielded systems of the same type into the market gives confidence in their understanding of the requirements and the issues surrounding the use of their systems.	10	15	20	Evaluation of CVs of key personnel involved in the development and support of the COTS equipment.

Table J.3: Integrity assurance from supplier experience and expertise

Table J.4: INTEGRITY Assurance Points				**1 x 10^{-5}**
Supplier software design / development	**A maximum of 30 can be claimed from supplier software design / development**			
Supplier can demonstrate successfully following an appropriate development process in the development of the system	To level below recommendation	To level meeting recommendation	To level above recommendation	**Evidence Satisfaction Criteria**
Processes such as IEC 61508 or ED 109 or other standards/processes that give confidence of the integrity of the software i.e. It has been designed in a consistent and documented manner and infers some level of review. This gives confidence that the coding will be robust. These processes apply recommended levels of rigour that vary with the integrity requirement on the software being produced.	10	25	30	1. Certificate of Conformance for the Product in question; **OR** 2. Independent Audit of conformance; **OR** 3. Independent Audit of Justified Supplier Procedures. Note – Independent is independent of the product development / support team.
Knowledge of internal design features which have been put in place to limit the possibility of unwanted system action	Some features	Comprehensive features	▨	**Evidence Satisfaction Criteria**
Features in a system such as limiting the range on inputs to those expected or remove unwanted elements of an Operating System to ensure non-interference, greatly increase confidence that the system will not act abnormally.	5	10	▨	Design Documentation supporting claimed features AND evidence of their efficacy. Note: If design features at software level are argued, then the RV Argument needs to include optional argument RV1.2 to demonstrate Traceability from the safety requirements to the features.

Table J.4: Integrity assurance from design and development methods

Table J.5: <u>FUNCTIONAL</u> Assurance Points				**1 x 10^{-5}**
Testing	**Functional assurance requirements can be fully satisfied through testing alone** **IT IS MANDATORY TO ACHIEVE COVERAGE OF ALL FUNCTIONAL SAFETY REQUIREMENTS THROUGH FAT OR SAT**			
Specific Testing (Site Acceptance)	Full Test	▨	▨	**Evidence Satisfaction Criteria**
This testing is essentially designed to prove that the delivered system, after installation and commissioning, provides all of the required functionality.	100	▨	▨	1. Test Script. 2. Test Results. 3. Traceability matrix. Each functional Safety Requirement must be tested either during site or factory testing. Testing must include the extremes of conditions under which the system is expected to operate. Objective evidence of testing (and passing) of all functional Safety Requirements by providing traceability of Safety Requirement to test script to successful result. Note: These are the same criteria as those required to claim Integrity points from SAT and FAT.
Specific Testing (Factory Acceptance)		▨	▨	
This testing is essentially designed to prove that the system, prior to leaving the factory, provides all of the required functionality. Often this can include tests that cannot be repeated on site, particularly where a test harness is required and measurements related to timing and processor loading are being made.		▨	▨	

Table J.5 Functional assurance from 100% test coverage of functional Safety Requirements

ANNEX K RATIONALE

K.1 Introduction

SRG believes that full satisfaction of the objectives of SW 01 (Reference 1) cannot be achieved using evidence generated by most ANSPs' current practices, but is achievable via several stages of increasing objectivity. These stages are identified in a Roadmap presented as Appendix L. The first stage is based on current practice and provides this Acceptable Means of Compliance (AMC). The AMC is largely based on a subjective argument gleaned from the current practices of ANSPs. The Roadmap defines the goals for the AMC, with the aim to make it more objective over time and thus aligned with the objective approach of SW 01. The first Roadmap stage for the safety assurance of software in COTS equipment is defined in this guidance document.

This Annex records the rationale for the first Roadmap stage.

K.2 Interpretation of Risk Classification Schemes

Risk classification schemes typically define “bands” or classes of risk tolerability (normally three or four classes) with the highest band representing unacceptable risk, the lowest band representing broadly acceptable risk and the intermediate band(s) representing risks that may be tolerable under certain conditions.

The failure frequency of a Requirement is derived from a hazard/risk analysis and is set to be the acceptable rate of occurrence for a given hazard. If the rate of occurrence is such that the risk of the consequent accident is in the highest (unacceptable) risk class then a failure to meet the Requirement leads directly to failing to meet the target level of safety.

In order to accommodate uncertainties both in the analysis of the hazards and in the development of the system, ANSPs should design systems to operate at a lower risk class, which normally means that the failure frequency of the Requirement will be lower than for the highest risk class, and is thus considered to be equivalently less risky (this assumes a linear relationship between risk and frequency). Consequently, some safety margin of risk is gained and this can be traded for the level of confidence needed that the Requirement is achieved (satisfied). Therefore, the necessary confidence level for demonstrating that the Requirement is achieved may be varied according to the risk class used when setting the Requirement. These confidence levels may be categorised as “Low” for the lowest risk class, “Medium” to “High” for intermediate risk classes and “Absolute” (which is impossible to achieve) for the highest risk class. In other words, the level of confidence that can be achieved when satisfying the reliability attributes of a Requirement primarily dictates the risk class.

The following table illustrates this concept. In the example a function has to have a tolerable failure rate of 10^{-8} at risk class A (where A is the highest risk class and D the lowest). Mitigations within the system reduce the necessary COTS failure rate to 10^{-2}. The table can then be used to decide which risk class is to be set based on the confidence that can be achieved i.e. if perfect confidence can be achieved then the target frequency is 10^{-2} but if only low confidence can be achieved the target frequency is 10^{-5}.

Target Level of Safety / Risk Class	**A**	**B**	**C**	**D**
Accident rate	1×10^{-8}			
mitigation @ *1000:1*				
Gives a hazard rate of	1×10^{-5}	1×10^{-6}	1×10^{-7}	1×10^{-8}
Further mitigation @ *1000:1*				
Gives a COTS requirement rate of	1×10^{-2}	1×10^{-3}	1×10^{-4}	1×10^{-5}
Confidence Category Required	Absolute (impossible)	High	Med	Low

Note: In the above table, the figures are illustrative only and all rates are per hour.

It is not generally possible to set objective levels of confidence for these subjective confidence categories, because the assumed relationship between risk, failure frequency and confidence cannot be objectively confirmed. However, DEF STAN 00-56 gives similar guidance with respect to high, medium and low levels of confidence in evidence. An extract from DEF STAN 00-56 Part 2 Annex C is reproduced below.

> **C.1 General**
>
> **C.1.2** In setting safety integrity requirements and in assessing whether these are met, it is also necessary to consider that there is generally no absolute guarantee that a system meets such safety integrity requirements, only greater or lesser confidence that this is the case. In setting safety integrity requirements, it is therefore important to consider how much confidence is needed. The integrity requirement reflects the level of confidence there should be in the evidence. The higher the integrity requirement, the more confidence is needed in the evidence.
>
> **C.1.3** Safety integrity requirements may include quantitative values for reliability, availability, robustness etc, together with the statistical (numerical) confidence with which these should be demonstrated to adequately support the safety argument. The required confidence can be achieved by a combination of statistical confidence and other forms of evidence (including qualitative evidence such as conformance to standards) that, combined with the quantified evidence allows a judgement of acceptability to be made.
>
> **C.1.4** A qualitative categorisation scheme may be used for safety integrity requirements (for example see clause C.2), in which case high, medium or low safety integrity requirements (or some similar classification) are allocated to the system and its elements on the basis of the risk posed by the system and the contribution of the elements to the overall risk.
>
> …
>
> **C.1.8**. Even for the highest integrity systems, confidence is not the same as absolute proof. The reliability can be stated to be better than a certain value, to a stated statistical confidence and analyses and demonstration can show, to a level that might be judged convincing by expert practitioners, however, no argument can prove conclusively that failures can never occur. The level of confidence required in this Standard is that arguments and evidence should be compelling. When the confidence achieved is consistent with the safety integrity requirements, the evidence should be sufficient for the Safety Case and further

justification should not be needed. Table 3 provides guidance on the confidence that may be achieved with different forms of evidence.

Extract from DEF STAN 00-56 Pt 2 Annex C Table 3

Level of Confidence

High	**Medium**	**Low**
The highest level of confidence possible given the state of the art. The range of uncertainty (confidence) in the quantitative evidence claims should err on the side of pessimism.	The effort expended on providing confidence should be proportionate to the risk. The range of uncertainty (confidence) in the quantitative evidence claims may err on the side of optimism (e.g. by up to 1 order of magnitude).	The range of uncertainty (confidence) in the quantitative evidence claims may err on the side of optimism (e.g. by up to 2 orders of magnitude).

K.3 Requirement Refinement and Apportionment

The proper form of Safety Requirements is discussed in paragraph 2.2 of this guidance.

However, Safety Requirements are often set at a level that cannot be observed directly at the equipment's interface with the rest of the system. For example, a common Safety Requirement is: "there shall be no credible corruption…". In order for this Requirement to be satisfied the likely sources of credible corruption of the equipment concerned have to be identified e.g. accuracy, timeliness, completeness, freedom from additional artefacts. This process is a refinement of the functional part of the Requirement.

However, it is not correct to just apportion the integrity part of a corruption Requirement to the refined Safety Requirements. This is because the original analysis of the corruption Requirement was crude and will have used average or worst case considerations of mitigations and outcome (event) probabilities. Instead, each refined Safety Requirement identifies a specific type of failure (e.g. inaccuracy) against which some mitigations may be powerless, or extremely effective, and so each must be individually analysed to determine the acceptable rate of failure.

Consequently, when properly formed Requirements are refined, not only does the functional part of the Requirement need to be refined, but the integrity part does as well, which will normally require the original integrity part to be apportioned to the refined Requirements. For example, to say that a piece of COTS equipment shall not corrupt a display is to say (in one case) that it will only deliver data that is to a certain accuracy. However, there can be no guarantee that it will never deliver inaccurate data and so a rate is used to define the integrity of the accuracy Requirement i.e. it shall only be inaccurate (beyond ±x%) once every 10,000 hours – colloquially this is referred to as "accurate to 10^{-4}". This level of visibility should always be provided and so full functional and integrity Requirements should be placed on the COTS equipment. A fuller explanation of refinement and apportionment can be found in paragraph 2.2 Step 1: Set valid Safety Requirements.

Apportioning the Safety Requirement may have an impact on the testing approaches used by ANSPs. In general the apportioning of integrity is not currently performed. Instead, the most onerous Safety Requirement is used to establish the test activities conducted e.g. the parameters of the integrity testing (usually a soak test). The test is then designed to demonstrate that the most onerous Requirement is met. It is assumed that since all other Requirements are less onerous, their success or failure will be demonstrated within the parameters established by the most onerous Requirement. This approach relies on the following argument:

IF

- the equipment is tested over a period that would demonstrate that the most onerous Safety Requirement is met, and
- all input data values are presented with a probability distribution appropriate both for:
  - the operational domain, and
  - the creation of output data with a probability distribution also appropriate for the operational domain,

THEN

all less onerous Safety Requirements would have already been shown either to have been met or to have failed to be met.

However, in practice the criteria given in the argument above are currently not met. For example:

- The most onerous integrity Requirement is not being identified, as apportionment of a Safety Requirement is not usually done correctly. Correct apportionment would usually yield refined equipment integrity Requirements that are more onerous than the most onerous Safety Requirement.
- In designing the test parameters to satisfy the most onerous Safety Requirement it is very unlikely that the full extent of the operational data domain will be examined and even less certain that the operational probability distribution will be replicated.
- Not all of the attributes of a functional Requirements are tested sufficiently, e.g. whilst sufficient tests for accuracy are executed, insufficient testing is carried out to demonstrate the timing attribute of the Requirements.

This guidance sets limits of acceptability for the above approach. SRG considers this is acceptable for the first stage of the roadmap, but that a more objective approach to integrity testing will be needed in the future.

K.4 The Division between 10^{-4} and 10^{-5}

SRG generally accepts that at some level of Requirement integrity, satisfaction can be shown solely from evidence of testing i.e. by treating the equipment as a “black box”. Beyond that, other forms of direct evidence are needed to augment the test evidence. These additional forms of direct evidence could come from knowledge of the design of the equipment or knowledge of previous use of the equipment (or both). Indirect forms of evidence such as knowledge of the processes used and the reputation of the supplier can also increase confidence in making a claim that a Requirement had been satisfied.

There is a significant body of academic work that suggests that the limit of testability is 1×10^{-4} per hour. This is re-inforced by DEF STAN 00-56 interim version 3, which states in Part 2 Annex C:

> **C1.6.** Where quantified requirements are stringent (e.g. better than 10-4 failures per hour), it may be impracticable to demonstrate that these requirements are met by either examination, analysis, testing or operational experience alone to any meaningful statistical confidence.

For this reason, the category of COTS equipment whose Requirements Satisfaction can be demonstrated solely by equipment-level evidence is colloquially called “10^{-4} COTS equipment”.

Therefore, for COTS equipment where the design is based on a low level of risk, which means that it is allowable to demonstrate satisfaction of an apportioned Safety Requirement with “low” confidence, the COTS equipment may be treated as a “black box” provided the Safety Requirement (at the equipment level) is no more onerous than 1×10^{-4}/h and the COTS equipment meets the testability criteria below (K.5). In such a case, it is not necessary to make an assurance argument specifically for the software within the COTS equipment because adequate confidence is demonstrated from equipment-level evidence.

If it is not possible to demonstrate, with the required level of confidence, that a Safety Requirement has been satisfied at the black box level, then it is necessary to “open the box” (Of course it may be appropriate to open the box at any time if it is felt that this would help with the overall assurance argument). This is true of COTS equipment where a Safety Requirement has an integrity target of less than 10^{-4}/hr or one that cannot meet the testability Requirements (see K.5 below). In general, for COTS equipment used in the airport environment, Requirements that cannot be demonstrated solely by testing are still no more onerous than 1×10^{-5}/h. For this reason equipment falling into this category is colloquially called “10^{-5} COTS equipment”.

In order to “open the box” it is necessary to have an appropriate relationship with the COTS equipment supplier to have access to design documentation.

The design information will allow further apportionment of the Safety Requirements to be performed allocating the COTS Equipment Safety Requirements to the relevant architectural components, i.e. the hardware and software. This will need to be performed in conjunction with the COTS equipment supplier.

If, as will almost always be the case, this further apportionment results in some element of the equipment Safety Requirement being allocated to the software within the COTS equipment, then it will be necessary to produce a software assurance argument. This software assurance argument is required to bolster the level of confidence that has been achieved through black box testing, to a point where it can be argued with the appropriate level of confidence that the Safety Requirement has been satisfied.

K.5 Testability

The testability of a 'black box' does not depend only on the value of the failure rate of the requirement being demonstrated, it depends also on:

- the attribute of the Requirement being observable at the equipment boundary (e.g. via displays, alarms, external test equipment);
- all output states, that need to be tested, being stimulated only by action at the inputs of the equipment; and
- sufficient of the state space being exercised.

NOTE: The state space of an equipment is the set of internal logical states that it can assume; the concept of state space is particularly relevant to software.

This may be established from knowledge of the extent of:

- the input domain;
- the output domain; and
- the internal variables.

It is important to understand the extent of the internal variables, since if the equipment has persistent memory, as is usually the case with software based equipment, then its contribution to the state space will be very large (if not near-infinite).

The claim for testability is built into the CAE diagram for Requirements Satisfaction (see AMC, paragraph K.6, below) and this claim must be satisfied as well as the claim that testing has shown that the Requirement has been met, before the Requirements Satisfaction claim can be properly substantiated.

The testability of equipment also encompasses the notion that all the equipment's Requirements can be tested. The arguments provided in the guidance are for the satisfaction of a single Requirement. Usually, an equipment has to satisfy many (multiple) Requirements (only some being Safety Requirements) and the implementation tries to ensure they all are satisfied collectively i.e. without interfering with one another.

It is straightforward to argue that demonstrating satisfaction of multiple Requirements can be achieved by repeating the argument (provided in the guidance material) for a single Requirement, a number of times. This is not so for arguing about the collective satisfaction of the Requirements. Primarily this is because the collective argument depends upon the state space of the implementation (the equipment). A large number of Requirements usually mean an extensive input domain, an extensive output domain and an extensive domain for the internal variables. Thus in this instance the state space will be extremely large. Even if there are few input and output variables, the complexity indicated by the large number of Requirements (or a small number of complex Requirements) would indicate a large state space due to internal variables. Note the assumption that complexity can be related to state space. In general this may be valid but there are many exceptions, for example a recursive solution to a problem is structurally simple but creates an enormous state space.

Without knowledge of the size of the state space or a surrogate such as the complexity of the implementation there can be no assurance that testing has shown Requirements Satisfaction. There is no direct measure of state space and the complexity surrogate poses something of a paradox when trying to deal with a black box, where, supposedly, nothing is known about the box's internal features. In order to move forward SRG has taken the view that this issue would be resolved at some later stage of the roadmap subject to increased vigilance on the introduction of new equipment that satisfy the conditions for use of the AMC.

K.6 The AMC

Evidence that is generally available today, together with other evidence that should be readily available, form the baseline defined as Stage 1 of the roadmap and the basis of the AMC for all SW 01 sub-objectives. Generic arguments have been derived for both "10^{-4}" and "10^{-5}" COTS equipment and are reproduced in this guidance document.

However, for Requirements Satisfaction, the sufficiency of the varying types of evidence is unclear and so the AMC defines acceptable direct and indirect sources of Requirements Satisfaction evidence in two ways:

- as the lowest level leaves of the Claims – Arguments - Evidence (CAE) diagrams; and
- as a table (the "COTS Evidence Evaluation Table" (CEET) in Annexes I and J) that relates sources of evidence to a notional value of their contribution to the Requirements Satisfaction goal.

The significant aspect of the Requirements Satisfaction argument is that a method is provided for combining evidence of different types (Test, Field Service, Design, Process, Supplier credibility) to provide a claim that the Requirements have been satisfied.

In the CEET the various Requirements Satisfaction evidence items have been assigned a weighting based upon experience such that acceptable combinations of evidence result in a total of 100 points. The CEET only needs to address Requirements Satisfaction evidence, as the evidence required for the other SW 01 objectives does not need to be combined in varying ways. Dependent upon the evidence available and the integrity assurance points associated with the evidence, individual arguments may differ for specific Safety Requirements. However, there is the potential to group together Safety Requirements of a similar type and safety significance.

Two aspects of the AMC will need future improvement:

- The weightings in the current scheme for combining the sources of evidence are subjective. The scheme needs to be made fully objective but may need several steps to become so.
- The assessment of the evidence itself (the points allocated for a particular piece of evidence) is subjective and based upon good practice as of 2005. It too needs to be made fully objective over a number of steps.

The opportunities for improvement in the future have been identified and assigned as stages in the implementation of the roadmap (a defined way forward from the current baseline to a future level of assurance) – see Annex L. The improvements will provide more detail of the evidence, allow more kinds of evidence and allow the arguments to become more objective. Consequently, while the top-level structure of the guidance's CAE diagrams is viewed by SRG as being stable, as work progresses (during the various stages of the roadmap) it is expected that lower levels may be added and the arguments changed. It will have an impact on the CEET, as there is a direct relationship between the example arguments and the integrity assurance points available. However, it is likely that:

- the headings will remain but the contents of the CEET will change to reflect the added detail of the CAE diagrams;
- the assurance points will change to reflect more objective ways of combining the evidence (the arguments) and to associate assurance points with more detailed evidence; and
- the total number of assurance points required for the acceptance of a safety case may alter to reflect more objective views of the assurance required.

The CEET considers satisfaction of a single Safety Requirement. It is current practice to assume that although there may be several Safety Requirements for a piece of COTS equipment, they do not interfere with one another. The arguments in the AMC provide a framework for the satisfaction of multiple Safety Requirements. Consequently, at stage 1 of the roadmap, evidence that satisfies the CEET for each Safety Requirement is all that is required i.e. the CEET can be applied to each Requirement individually, or to each convenient group of Requirements.

In order to address the interference effects (collective satisfaction of Safety Requirements) of implementing several Requirements in a single architectural unit, the notion of the state space of the implementation needs to be used. While objectives for the input and output domains of the state space have been identified, albeit subjectively, the expansion of this notion into the internal variable domain has been deferred for this stage of the roadmap.

It is expected that over time, the AMC will be validated through use and refined in the light of experience.

ANNEX L ROADMAP

This Annex contains the outline Roadmap for the further development of this Guidance. It should be noted that this Roadmap might be influenced by subsequent findings by SRG when addressing non-COTS systems.

	Stage 1	Stage 2	…	Stage n
Summary	Introduction of Goal Based Regulation and creation of 'level playing field' across industry	Safety arguments made more robust by placing less reliance on subjective evidence, still based solely on adherence to the scheme	…	Full compliance with SES legislation i.e. ESARR 6 transposed in the Common Requirements
Schedule	2008 to 2010	2010	…	TBD
Transition Required	From an argument of 'following a process should make a safe product' to one of 'argument incorporating evidence in accordance with Guidance'	From 'argument incorporating evidence in accordance with Guidance' to one of 'diverse evidence shows the product is acceptably safe'	…	To full compliance with Single European Sky (SES) legislation - the software is tolerably safe
Safety Rationale	Introduction of structured arguments supported by evidence in a consistent repeatable manner-Encourages requirements with a complete set of safety attributes	As for Stage 1 except argument provided by the CAE diagrams is more objective - Requires requirements with a complete set of safety attributes	…	Full compliance e.g. arguments include the use of quantitative evidence for integrity claims
Supporting Evidence	Minimum acceptable standard of evidence defined	Evidence becomes more objective and quantitative (to support modifications in evaluation scheme)	…	Evidence dominated by quantitative rather than qualitative evidence
Evaluation scheme	Implementation of 1×10^{-4} and 1×10^{-5} evaluation schemes (CEET including evidence criteria)	Evaluation scheme modified in line with more objective assessment of the combination of evidence	…	Scheme fully objective

Regulatory Safety Assessment Regime	Assessment (validate the evidence and argument) of compliance with scheme	Assessment of argument and evidence	…	Objective assessment

ANNEX M CHECKING AID

This checking aid is provided to assist ANSPs and assessors when preparing the submission and verifying whether the submission complies with this guidance. ANSPs may wish to complete this checking aid and include it in the submission to support their claim of compliance.

Section/ Page	Item	Compliance
2.2 p8	The Safety requirements were set according to the ANSP's Safety Management System (not that of another ANSP or of a contractor).	
2.2 p8	The Safety requirements have been apportioned according to system architecture and available mitigations, down to COTS equipment level.	
2.2.1 p9	The COTS equipment safety requirements are properly formed.	
2.3 p10	The COTS item is an equipment. The guidance is not valid, and may not be used, for COTS software.	
2.3 p10	The COTS equipment specification is sufficiently detailed to demonstrate implementation of the system safety requirements.	
2.3 p10	The most onerous integrity requirement on an individual COTS equipment is no worse than 1 x 10^{-5}.	
2.3 p10	Equipment monitoring requirements are specified in the associated System Safety Case (from the time that the COTS equipment enters service).	
2.3, RS1 p10 p24	If the submission covers multiple equipments, they must be shown to be identical (hardware and software). [10^{-4} only] (Note that for 10^{-5}, the ANSP could choose to address this issue as part of the Configuration Consistency argument, or in introductory material.)	
2.3, RS1.1.1 p10, p26, 46	The Safety Objectives must have been set at a 'broadly acceptable' level.	

Section/ Page	Item	Compliance
2.3, RS1.1.2 p11, p26, 46	The Safety Requirements are all expressed in terms of the COTS equipment outputs.	
2.3, RS1.1.3 p11, p26, 46	The behaviour specified by the COTS Equipment Safety Requirements can be stimulated using the equipment inputs and the available test facilities.	
2.4 p11	The ANSP has presented the textual argument (not just the evidence) that the objectives of SW 01 have been met. Graphical representation of the argument is optional.	
2.4 p11	The arguments and optional diagrams have been tailored to cover variations in the evidence actually provided to support the arguments.	
2.4 p11	Text in italics in the template arguments has not been included in the software safety submission.	
2.5 p12	Specific references have been embedded in the arguments for all evidence required to support and justify the arguments.	
2.5 p12	The evidence used has been examined when preparing the submission to ensure it is suitable.	
2.5 p12	The ANSP has access to the evidence.	
2.5, RS1.2 p12 p29, 49	Where evidence items are those defined in the CEET, they satisfy relevant Evidence Satisfaction Criteria in the CEET.	
2.5 p12	Each evidence item has been checked to identify whether it is immediately obvious that the evidence supports the arguments. If necessary, explanations or arguments to show this have been added.	
2.6 & 2.7.2 p12, 13	A score of 100 assurance points or more has been accumulated from the Integrity Assurance CEET and a further 100 assurance points has been accumulated from the Functional Assurance CEET.	

Section/ Page	Item	Compliance
2.8 p13	It has been claimed that the guidance has been complied with. Assurance is given that the AMC has only been modified in those areas permitted by the guidance.	
2.8, RS1.2 p13 p29, 49	Explanations are given of how the ANSP has chosen to present the arguments, e.g. with respect to the satisfaction of multiple groups of safety requirements.	
Footnote 5 p23	The System Safety Assessment has addressed all of the behaviour exhibited by the COTS Equipment including un-specified behaviour. [10^{-4} only, as 10^{-5} has more detailed argument]	
RS1.1.4 p27, 47	'Initial Monitoring Instructions' attempt to detect and record any behaviour that is not specified in the COTS Equipment Specification.	
RS1.2 p28, 48	The ANSP agrees that the assurance provided by evaluation of the COTS equipment, using this scheme, is sufficient. The argument is not invalidated by contrary evidence or other circumstances.	
RS1.2 p29, 49	The evidence provided for the arguments RS1.2 and below is credible for each Safety Requirement. (An example of incredible evidence might be field-service evidence where certain features of a product relevant to some Safety Requirements have not been exercised)	
RS1.2 p29, 49	The arguments (RS1.2 and below) show the evidence relevant to each Safety Requirement in a manner that facilitates review and audit. For example, traceability mechanisms show the relevant tests and test records for each Safety Requirement.	
RS1.2.2, RS1.2.3, RS1.2.4 p32, 53, p33, 54, p35, 56	COTS equipment specific arguments have been completed where necessary. (The template has not fully detailed these arguments)	
RV1 p37	Safety requirements derived from un-required behaviour of the COTS equipment were apportioned, in the system safety analyses to appropriate system components.	

Section/ Page	Item	Compliance
RV1 p37 (see footnote 16)	If derived safety requirements were allocated to parts of the system other than the COTS equipment, further safety arguments are provided to address these safety requirements to support putting the COTS equipment into service.	
RV1 p37	The product specification is of adequate quality such that an analysis of all specified behaviour of the COTS equipment was satisfactorily completed.	
CC1.3 p42, 43	COTS equipment specific arguments have been completed where necessary. (The template has not fully detailed these arguments)	
NI p61, 62	COTS equipment specific arguments have been completed where necessary. (The template has not fully detailed these arguments)	
CEET p65, 74	FAT or SAT evidence has been used.	
CEET p65, 74	ANSP Soak Testing or Supplier Testing evidence has been used.	
CEET p65, 74	A maximum of 90/75 ($10^{-4}/10^{-5}$) integrity assurance points have been claimed for testing.	
CEET p65, 74	Assurance points have not been claimed when satisfaction criteria are not completely met.	
CEET p67, 76	A maximum of one item from Field service experience is claimed.	
CEET p70, 78	A maximum of 20 integrity assurance points have been claimed for supplier experience and expertise.	
CEET p71, 79	A maximum of 30 integrity assurance points have been claimed for supplier software design/development. (See RV1.2 on p39).	
CEET p71, 79	If design features at software level are argued, then arguments are presented showing Traceability from the requirements to the features.	
CEET p72, 80	All functional safety requirements are covered by FAT or SAT.	

General Checks

Section/ Page	Item	Compliance
	The submission is of a suitable general quality. For example: document identification and version control, authorisation, absence of spelling and typographic errors, absence of TBAs, work is complete, tailoring to specific application, general presentation.	
	Arguments are based on the templates in the Guidance, and reflect the explanations given of how the ANSP has chosen to present the arguments. See 2.8 (p13), RS1.2 (p29, 49). Compliance with the Guidance cannot be claimed if the template arguments are altered other than as permitted in the Guidance.	
	Evidence (or references to evidence) has been provided in every case that the argument invokes evidence, and that evidence exists.	
	The evidence is relevant to the application.	
	The actual evidence correctly exhibits the necessary characteristics to support each argument that invokes it. For example, test results shows that the right things were tested and passed the test.	
	Evidence is of a suitable general quality to support a safety submission.	

INTENTIONALLY BLANK