Safety Regulation Group

AMC to CAP 670

Guidance on Reasoning that SW 01 does not apply to a Change

First issue 6 February 2009

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

Air Traffic Standards Division, 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

1.1.1 The purpose of this document is to provide guidance specifically aimed at identifying and justifying cases where a change to a piece of equipment (normally expected to be to a legacy system for the purposes of this document) is outside the scope of CAP 670 SW 01.

1.1.2 This Guidance does not replace the need to fully meet the ANSP's SMS requirements for equipment safety assurance.

1.2 Background

1.2.1 The CAA mandated 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".

1.2.2 This document provides guidance to those seeking to identify and justify that there is no need to develop an SW 01 argument when changing operational equipment.

- Firstly, this Guidance presents Cases that justify that SW 01 compliance does not need to be demonstrated. The Cases give structured arguments, each part showing how some evidence and/or sub-claims together mean that a valid top level claim can be made.
- Secondly, for these Cases, it provides a way to determine what evidence is necessary.

1.2.3 It should be noted that various arguments rely on the competence of people. To justify that the person is competent at the task in hand it will be necessary to not only relate the formal qualification/experience to the task but also to show that the qualification/ experience is sufficient for the task.

1.3 Scope

1.3.1 This document only applies to operational equipment (or equipment that interfaces to operational equipment), i.e. all equipment that has safety requirements[1]. If the equipment has been assessed as having no safety requirements, no SW 01 arguments of any form are needed.

1.3.2 The arguments developed within this Guidance cover cases where hardware and/or software are changed. Changes to software safety requirements are **not** covered within this Guidance and would need to be addressed by an argument against the SW 01 sub-objectives. Hence an argument against the five sub-objectives of SW 01 would be required for cases such as:

- The action of implementing a change results in new functions/failures which may themselves introduce the need for new software safety requirements; and/or
- The behaviour of the modified equipment in its operational environment necessitates changes in software safety requirements (e.g. derived software safety requirements).

[1] Non-operational equipment is obviously out of scope as it cannot have any safety requirements derived from system safety analysis. It is therefore out of the scope of SW 01 and consequently no "SW 01 arguments" are needed.

1.4 Roadmap

1.4.1 In the process of generating this document, issues have been identified that will need further work to add more objectivity to the arguments. Such issues have been identified in the appropriate places within this document.

1.5 Document Content

1.5.1 This document is structured as follows:

- Section 2 identifies the Definitions of key terms and terminology used by the arguments within this Guidance document. *These definitions encapsulate some important concepts essential for the arguments to be valid. It is important that these are correctly understood*.

- Section 3 explains how to use this document.

- Sections 4 to 8 document the arguments for various cases where equipment changes do not require an argument against the SW 01 objectives.

2 Definitions

2.1 The following terms used within this document have a specific meaning within it.

Term	Definition
Assured Envelope	A Safety Case should define the conditions for which the Safety Case is valid. This would typically be for a range of circumstances and could include, for example, aspects such as adaptation data item values, operating environment or hardware configurations. This range is that for which the arguments in the Safety Case are valid, and for which valid evidence has been created, and is referred to as the 'Assured Envelope'. As an example: a Safety Case states that it is valid for a range of values for a particular adaptation data item. Changes subsequently made within the valid range can be claimed to be within the Assured Envelope, whilst changes outside the range would need a new safety argument (see Case B).
Software	The Glossary in SW 01 states: 'Software comprises the programs that execute in stored program digital computers (including Programmable Logic Controllers). Software also includes any data contained within the programs or held in external storage media, which is necessary for the safe operation of the system. Software may: • be developed for a particular application; • be re-used from previous applications, with or without modification; • have been obtained from third party software suppliers (commonly called Commercial Off The Shelf (COTS) software), e.g. database systems and operating systems; • or be any combination of these three types of software.' SW 01 Part 1 paragraph 2.3 states: 'SW 01 does not apply to Application Specific Integrated Circuits (ASICs), Programmable Gate Array (PGAs), and Solid State Logic Controllers.'
Changed Components	Those components of hardware and/or software that have been modified as a consequence of the change.
Impacted Components	Those components of hardware and/or software that have NOT been changed, but whose behaviour may be indirectly affected as a consequence of the change (e.g. change of CPU may impact the execution time of unchanged software).
Project	The term 'project' is used to define any framework within which a change is managed.

Legacy System	A pre-existing system.
Equipment	Hardware and Software.

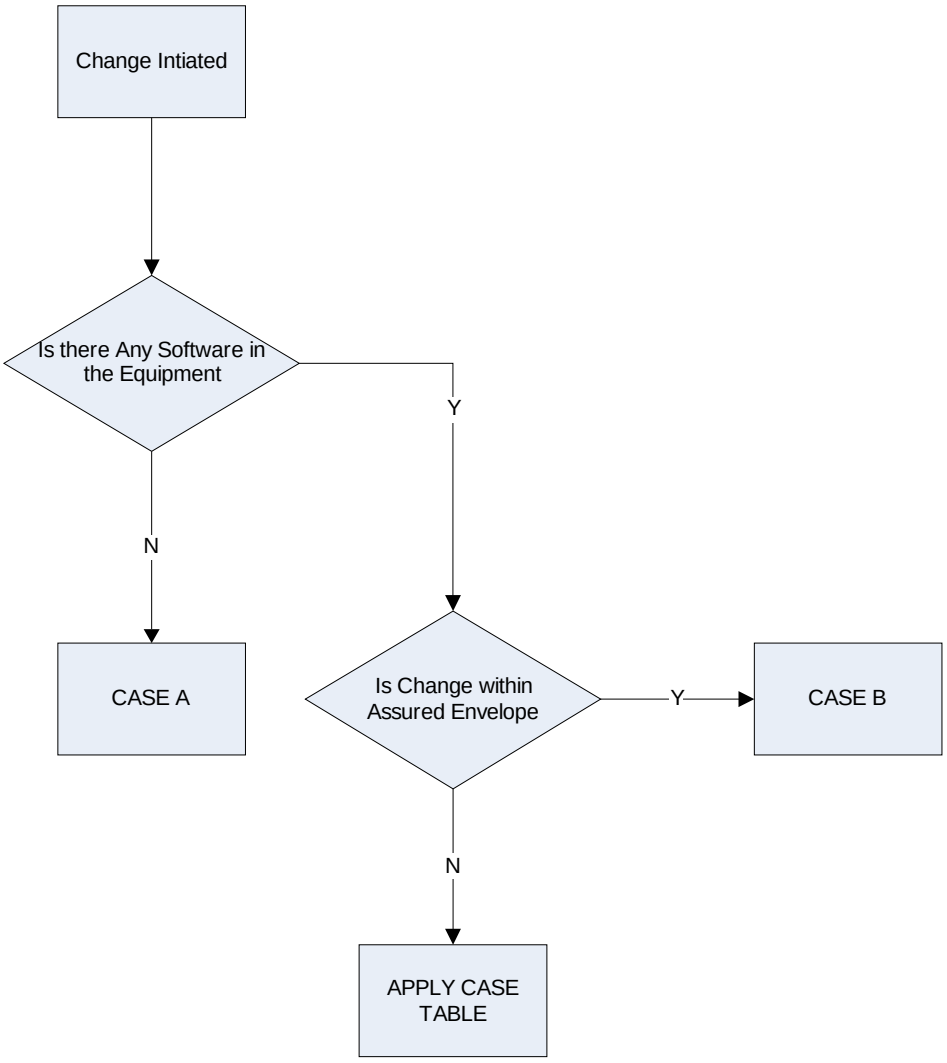
2.2 The following acronyms and abbreviations are used within this document:

ANSP	Air Navigation Service Provider
ATS	Air Traffic Services
CAA	Civil Aviation Authority
COTS	Commercial Off The Shelf
CPU	Central Processor Unit
HW	Hardware
SMS	Safety Management System (documentation)
SRG	Safety Regulatory Group
SW	Software

3 How to use this Document

3.1 Steps to follow:

Step 1 **Decide which Case to use.** Use the following flow chart and Case Table. Once the project has selected a case (or combination of cases), it must check that the case is valid for the project circumstances, and that the evidence listed is available or can be generated.



Case Table

Not Safety Related		Safety Related		Case
HW change?	SW Change/ Impact?	HW change?	SW Change/ Impact?	
No	No	No	Yes	SW 01 argument[2]
No	No	Yes	No	C
No	No	Yes	Yes	SW 01 argument
No	Yes	No	No	E
No	Yes	No	Yes	SW 01 argument
No	Yes	Yes	No	D + E[3]
No	Yes	Yes	Yes	SW 01 argument
Yes	No	No	No	C
Yes	No	No	Yes	SW 01 argument
Yes	No	Yes	No	C
Yes	No	Yes	Yes	SW 01 argument
Yes	Yes	No	No	D + E
Yes	Yes	No	Yes	SW 01 argument
Yes	Yes	Yes	No	D + E
Yes	Yes	Yes	Yes	SW 01 argument

Step 2 **Present the argument that the change does not need to address SW 01.** The basic argument text should be copied, and adapted to incorporate project-specific circumstances (e.g. merging of arguments from more than one case) and evidence (see 3 below).

The ANSP should clearly state the source of the argument (i.e. that it is derived in accordance with Case X of this guidance), claim that the selected case is applicable to the change, and describe any adaptations made to the template arguments provided in this guidance including any Cases used to support Sub-claims.

Note: In some cases two or more alternative arguments have been presented. The fact that there is an option is clearly indicated and the reader needs to choose which is most appropriate to the circumstances of the change.

[2] 'SW 01 argument' in this context means an argument that addresses the 5 sub-objectives of SW 01 for the change (only), and is not addressed by this guidance.

[3] Case D is to be used for the hardware aspects of the change, case E is to be used for the software aspects of the change.

Step 3 **Present the evidence supporting the argument** as required by the relevant argument. This evidence may need to be generated. Without the described evidence, the claim is invalid, and an alternative argument must be made. The evidence may be included into the document containing the argument, or referenced from it. References must be correct and specific (e.g. to the relevant paragraph, not the whole document).

Step 4 **Confirm Validity of argument and evidence.** In view of what has been learnt in the course of the previous three steps, confirm that the circumstances match those for the case being used. The evidence must be credible and support the conclusions drawn by the arguments.

4 Case A: There is no Software in the Changed Equipment

4.1 Introduction

4.1.1 This claim can be used where there is no Software in the equipment.

4.1.2 Three alternative arguments are presented below. The first and second arguments are where an inspection/review is undertaken by a competent person. The third argument is where a formal statement from a supplier is available and the ANSP and its supplier are unable to complete the previous two arguments.

Note: It is preferable to comply with paragraph 4.2.1 or 4.2.2 by requiring the Supplier to provide the necessary documentation.

4.2 Arguments

4.2.1 Equipment has been Physically Inspected

Claim0 The change does not necessitate an argument that the SW 01 objectives have been met because there is no Software in the changed equipment.

Argument

IF A Competent Person [EVIDENCE2] has inspected the equipment and confirmed that the components cannot contain software [EVIDENCE1].

THEN An argument against SW 01 is not required.

Evidence1 Record of examination, by Competent Person, of physical equipment referencing items examined, including:

a) Model, version number and serial number of the equipment examined.

b) Statement signed by the Competent Person that the inspection was completed (components were identified down to a level where it is apparent that they cannot contain software).

c) Brief description of the examination and an overview of the components found.

Evidence2 Statement arguing that the person has relevant competence for the task. The argument should define relevant competence criteria (e.g. training, experience), including at least one from the following list, according to the task being undertaken by the Competent Person[4]:

a) Has a formal qualification in the discipline in which they are being asked to review, e.g. electrical engineering; or

b) Has experience in lieu of formal qualifications.

[4] The relevance and sufficiency of competence needs to be established.

4.2.2 **Equipment Design has been Assessed**

Claim0 The change does not necessitate an argument that the SW 01 objectives have been met because there is no Software in the changed equipment.

Argument

IF A Competent Person [EVIDENCE2] has reviewed the design and confirmed that the components cannot contain software [EVIDENCE1].

AND All evidence presented in support of this argument either relates directly to the version of the equipment for which assurance is sought [EVIDENCE3] **OR** arguments are presented to justify why evidence from previous version(s) of the equipment remain valid [EVIDENCE4].

THEN An argument against SW 01 is not required.

Evidence1 Record of examination, by Competent person, of design information referencing items examined, including:

a) Model and version number of equipment to be assured.

b) Statement signed by the Competent Person that the review was completed (components were identified down to a level where it is apparent that they cannot contain software).

c) Reasons why the examiner knew that the set of design documents was complete, or at least sufficient to allow the examination.

d) Brief description of the examination and an overview of the components found.

e) List of design documents examined.

Evidence2 Statement arguing that the person has relevant competence for the task. The argument should define relevant competence criteria (e.g. training, experience), including at least one from the following list, according to the task being undertaken by the Competent Person:

a) Has a formal qualification in the discipline in which they are being asked to review, e.g. electrical engineering; or

b) Has experience in lieu of formal qualifications.

Evidence3 Traceability from all evidence cited in this argument to the version of the equipment that is being assessed.

Evidence4 If applicable, argument(s) justifying why any evidence from previous version(s) of the equipment remains valid for the version of the equipment being assured.

4.2.3 **Supplier Provides Formal Statement**

Claim0 The change does not necessitate an argument that the SW 01 objectives have been met because there is no Software in the changed equipment.

Argument

IF The supplier provides a formal statement that there is no Software within the supplied system [EVIDENCE1].

AND The supplier statement is credible because the supplier is reputable [EVIDENCE2].

THEN An argument against SW 01 is not required.

Evidence1 Statement from the supplier confirming that there is no *Software* within the changed equipment (i.e. this statement has to address the version of the system being assured).

Note: It is preferable to comply with paragraph 4.2.1 or 4.2.2 by requiring the Supplier to provide the necessary documentation.

Evidence2 Evidence of the supplier having a successful track record in a relevant market sector (this might include evidence of a number of successful and similar installations). Where available, this should include the ANSP's first hand experience of the supplier.

5 Case B: Change is within the Assured Envelope

5.1 Introduction

5.1.1 This claim can be used when the Safety Case identifies an Assured Envelope[5] and when the change has been implemented, the equipment remains within its Assured Envelope. This may include adaptation changes.

5.2 Argument

Claim0 The change does not necessitate an argument that the SW 01 objectives have been met because the change is within the Assured Envelope.

Argument

IF The equipment has an Assured Envelope identified [EVIDENCE1] and it has been adequately assured [EVIDENCE2].

AND The equipment remains within the Assured Envelope following the change [EVIDENCE3].

AND The equipment has been configured as intended [EVIDENCE 4].

AND The general behaviour of the equipment has not unexpectedly changed [EVIDENCE5].

AND All evidence presented in support of this argument either relates directly to the version of the equipment for which assurance is sought [EVIDENCE6] **OR** arguments are presented to justify why evidence from previous version(s) of the equipment remain valid [EVIDENCE7].

THEN An argument against SW 01 is not required.

Evidence1 A document which identifies the Assured Envelope parameters and their ranges. This may be the system safety case, other system documentation or, if such documentation does not currently exist, an agreed, documented, system expert's opinion. The source of the information should be stated.

If a system expert's opinion is used, this must be supported by an argument that the person has relevant competence for the task.

Evidence2 Evidence of assurance of the Assured Envelope. Currently this may include Test Plans, Test Scripts and Test Results from **previous** version(s) of the equipment, identifying the testing that has been completed along with its success/failure. [Refer to all appropriate plans, scripts and results, for example regression, site and installation] [6].

[5] Or the necessary documentation is available to support the Assured Envelope concept, even if not referenced in the system safety case.

[6] In future is it likely that a more robust argument justifying the existence of the Assured Envelope will be required. This is recognised as a roadmap issue.

Evidence3 Test Plans, Test Scripts and Test Results from the **current** version of the equipment, identifying the testing that has been completed along with its success/failure. [Refer to all appropriate plans, scripts and results, for example regression, site and installation].

Evidence4 Evidence of Inspection, tests or other evaluation that confirmed that the equipment has been configured as intended.

Evidence5 The selected sample of Test Scripts and Test results that have been run against the unchanged parts of version of the equipment to be assured, showing that the behaviour of the equipment has not unexpectedly changed. [Refer to all appropriate scripts/reports].

Evidence6 Traceability from all evidence cited in this argument to the version of the equipment that is being assessed.

Evidence7 Argument(s) justifying why any evidence from previous version(s) of the equipment remains valid for the version of the equipment being assured.

5.3 Alternative Argument (for Routine Changes)

5.3.1 In cases where changes within the Assured Envelope are a routine occurrence (e.g. adaptation data), the relevant system authority must decide whether to implement (and document) an adaptation delivery process such as that identified in EUROCAE document ED109 Section 4.2[7] or whether to make the argument defined above for each individual adaptation change. It is not necessary to do both. If the 'adaptation delivery process' approach is used, the process must include measures that ensure that all permitted changes remain within the Assured Envelope. The validity of the process need only be argued once (not for each change). This argument must justify that the process will inherently ensure that the argument at paragraph 5.2 would hold for all adaptation delivery under the procedure, and that all required evidence would be generated. The truth of this should be apparent if subject to audit at any adaptation delivery. Hence an argument is not required at each adaptation delivery.

5.3.2 ANSPs should note that this guidance does not provide this argument, and that SRG will not accept such arguments lightly.

[7] That is, mechanisms for generating and modifying adaptation data are defined, together with the associated verification, quality, configuration management (including record management, archive and retrieval), approval and installation processes.

6 Case C: The Hardware has Changed without Impacting any of the Software

6.1 Introduction

6.1.1 This claim can be used where there are ONLY hardware changes and the software within the equipment is not impacted by the change. The hardware changes may be to Safety Related components.

6.2 Argument

Claim0	The change does not necessitate an argument that the SW 01 objectives have been met because the hardware has changed without impacting any of the software.
Argument	
IF	The Changed Components and the Impacted Components have been identified [EVIDENCE1].
AND	The Changed Components and Impacted Components do not contain Software [SUB-CLAIM1].
AND	All evidence presented in support of this argument either relates directly to the version of the equipment for which assurance is sought [EVIDENCE2] **OR** arguments are presented to justify why evidence from previous version(s) of the equipment remain valid [EVIDENCE3].
AND	Testing has provided no counter evidence of impacts being to any components other than those identified as Impacted Components [EVIDENCE4].
THEN	An argument against SW 01 is not required.
Evidence1	Documentation detailing the Changed Components required to implement the change and any Impacted Components, and a brief description of how these were identified (to provide confidence that all impacted components were identified). Note that this must also ensure that other (possibly unchanged) equipments are not impacted.
Evidence2	Traceability from all evidence cited in this argument to the version of the equipment that is being assessed.
Evidence3	Argument(s) justifying why any evidence from previous version(s) of the equipment remains valid for the version of the equipment being assured.
Evidence4	Documentation identifying the required testing has successfully completed to confirm the change has been implemented correctly and that there is no discernable impact to the operation of the unchanged parts of the system [Refer to related documentation e.g. test plans, scripts and results].

Sub-claim 1 The Changed Components and Impacted Components do not contain software.

This claim can be addressed by following the guidance for “Case A: There is no Software in the changed equipment” and replacing ‘changed equipment’ by ‘Changed components and Impacted Components*’.*

7 Case D: The Hardware has Changed without Impacting any of the Safety Related Software

7.1 Introduction

7.1.1 This claim can be used where there are ONLY hardware changes and these changes do not impact the Safety Related Software components (this may impact non-Safety Related software). The hardware changes may be to Safety Related components.

NOTE: A re-platforming that requires device driver changes would be considered a change to hardware and software and therefore does *not* fall within the scope of this case.

7.2 Argument

Claim0	The change does not necessitate an argument that the SW 01 objectives have been met because the Hardware has changed without impacting any of the Safety Related Software.
Argument	
IF	The Safety Related software and/or hardware components in the changed equipment have been identified [SUB-CLAIM1].
AND	The Changed Components and the Impacted Components are identified [EVIDENCE1].
AND	The Changed Components do not contain any Software [SUB-CLAIM2].
AND	The Impacted Components do not contain Safety Related Software [SUB-CLAIM3].
AND	All evidence presented in support of this argument either relates directly to the version of the equipment for which assurance is sought [EVIDENCE2] **OR** arguments are presented to justify why evidence from previous version(s) of the equipment remain valid [EVIDENCE3].
AND	Testing has provided no counter evidence of impacts being to any components other than those identified Impacted Components [EVIDENCE4].
THEN	An argument against SW 01 is not required.
Evidence1	Documentation detailing the Changed Components required to implement the change and any Impacted Components and a brief description of how these were identified (to provide confidence that all impacted components were identified). Note that this must also ensure that other (possibly unchanged) equipments are not impacted.
Evidence2	Traceability from all evidence cited in this argument to the version of the equipment that is being assessed.

Evidence3	Argument(s) justifying why any evidence from previous version(s) of the equipment remains valid for the version of the equipment being assured.
Evidence4	Documentation identifying the testing designed and conducted to confirm the change has been implemented correctly and that there is no discernable impact to the operation of the unchanged parts of the system [refer to related documentation e.g. test plans, scripts and results].
Sub-claim1	The Safety Related software and/or hardware components in the changed equipment have been identified.
Argument	
IF	The equipment safety requirements have been identified and are correct and complete (valid) [EVIDENCE5].
AND	The traceability or apportionment that identifies the components that implement the equipment Safety Requirements exists and is valid [EVIDENCE6].
THEN	The Safety Related software and/or hardware components in the changed equipment have been identified.
Evidence5	Document that identifies the equipment safety requirements.
Evidence6	Traceability/apportionment information and record of verification (for completeness and correctness) of this information. *It is recognised in the short term this may not exist and instead a project may rely on System Safety Requirements and expert knowledge of the architecture. In such cases an argument would also be required as to why the expert's judgement is credible (i.e. [EVIDENCE7]). This is recognised as a roadmap issue.*
Evidence7	Statement arguing that the person has relevant competence for the task. The argument should define relevant competence criteria (e.g. training or experience) according to the task being undertaken by the Competent Person.
Sub-claim2	The Changed Components do not contain any Software. This claim can be addressed by following the guidance for "Case A: There is no Software in the Changed Equipment" and replacing 'changed equipment' by 'Changed Components'.

Sub-claim3 The Impacted Components do not contain Safety Related Software.

Note: The argument provided is one of inspection, however there is the potential to present an argument based on traceability.

IF A Competent Person [EVIDENCE8] has reviewed the design and confirmed [EVIDENCE9] that the Impacted Components do not contain Safety Related Software.

THEN The Impacted Components do not contain Safety Related Software.

Evidence8 Statement arguing that the person has relevant competence for the task. The argument should define relevant competence criteria (e.g. training, experience), according to the task being undertaken by the Competent Person.

Evidence9 Record of examination, by Competent person, of design information referencing items examined, including:

a) List of Impacted Components that were examined;

b) Statement signed by the Competent Person that the review was completed;

c) Reasons why the examiner knew that the set of design documents for the Impacted Components was complete, or at least sufficient to allow the examination;

d) Brief description of the examination and its results; and

e) List of design documents examined.

8 Case E: Software Change does not Impact Safety Related Software

8.1 Introduction

8.1.1 This claim can be used where there are Software changes, but they do not impact the Safety Related Software components.

8.1.2 This claim relies on being able to identify some form of barrier (e.g. hardware and/or software partitioning) between the Safety Related software and the non-Safety Related software that is being changed. Guidance on identifying possible applicable barriers will be available in the future; in the meantime any barrier will need to be self-evident. An example might be where software in a logging device is being modified and it can be demonstrated that all communication is into the logging device (i.e. a one way communication channel). It is unlikely that this case applies unless design provisions within the equipment or software architecture are already known.

8.2 Argument

Claim0	The change does not necessitate an argument that the SW 01 objectives have been met because the Software change does not impact Safety Related Software.
Argument	
IF	The Changed Components and the Impacted Components are identified [EVIDENCE1].
AND	The Changed Components and the Impacted Components do not contain Safety Related software [SUB-CLAIM1].
AND	All evidence presented in support of this argument either relates directly to the version of the equipment for which assurance is sought [EVIDENCE2] or arguments are presented to justify why evidence from previous version(s) of the equipment remain valid [EVIDENCE3].
AND	Analysis has confirmed that the failure of the Changed Components or the Impacted Components will have no impact on Safety [SUB-CLAIM 2].
AND	No unexpected impacts have been detected by the tests designed to confirm correct implementation of the change [EVIDENCE4].
THEN	An argument against SW 01 is not required.

Evidence1	Documentation detailing the Changed Components required to implement the change and any Impacted Components and a brief description of how these were identified (to provide confidence that all impacted components were identified). Note that this must also ensure that other (possibly unchanged) equipments are not impacted. This must be supported by arguments, based on design evidence, that explain the self-evident barriers that limit the impact of the change to the components detailed.
Evidence2	Traceability from all evidence cited in this argument to the version of the equipment that is being assessed.
Evidence3	Argument(s) justifying why any evidence from previous version(s) of the equipment remains valid for the version of the equipment being assured.
Evidence4	Documentation identifying the required testing to confirm the change has been implemented correctly and that there is no discernable impact to the operation of the unchanged parts of the system. This must show the relationship of the test cases to the Changed Components and Impacted Components.

Sub-claim1	The Changed Components and the Impacted Components do not contain Safety Related software.

Argument

IF	The equipment safety requirements have been identified and are correct and complete (valid) [EVIDENCE5].
AND	The traceability or apportionment that identifies the components that implement the equipment Safety Requirements exists and is valid [EVIDENCE6].
AND	A Competent Person [EVIDENCE7] has reviewed the design and confirmed [EVIDENCE8] that the Safety Requirements that trace to the Changed Component or the Impacted Component are NOT implemented in Software (i.e. the Changed Component or the Impacted Component does not contain Safety Related Software).
THEN	The Changed Component or the Impacted Component does not contain Safety Related Software.

Evidence5	Document that identifies the equipment safety requirements.
Evidence6	Traceability/apportionment information and record of verification (for completeness and correctness) of this information. *It is recognised in the short term this may not exist and instead a project may rely on System Safety Requirements and expert knowledge of the architecture. In such cases, an argument would also be required as to why the expert's judgement is credible (i.e. [EVIDENCE7]). This is recognised as a roadmap issue.*

Evidence7 Statement arguing that the person has relevant competence for the task. The argument should define relevant competence criteria (e.g. training, experience), according to the task being undertaken by the Competent Person.

Evidence8 Record of examination, by Competent person, of design information referencing items examined, including:

a) List of Changed and/or Impacted Components that were examined;

b) Statement signed by the Competent Person that the review was completed;

c) Reasons why the examiner knew that the set of design documents for the Changed and/or Impacted Components was complete, or at least sufficient to allow the examination;

d) Brief description of the examination and its results; and

e) List of design documents examined.

Sub-claim2 Analysis has confirmed that the failure of the Changed Components and the Impacted Components will have no impact on Safety.

Argument

IF A Competent Person [EVIDENCE10] has analysed the Changed Components and the Impacted Components for potential failures [EVIDENCE9].

AND The identified potential failures of Changed Components and/or Impacted Components do not affect or create new Safety Requirements [EVIDENCE9].

Note: If the safety requirements have been modified as a result of this analysis then a full argument against the 5 sub-objectives of SW 01 will be required.

THEN Analysis has confirmed that the failure of the Changed Components and the Impacted Components will have no impact on Safety.

Evidence9 Record of analysis, by Competent person, of design information referencing items examined, including:

a) List of Changed and Impacted Components that were analysed for potential failures and their impact on the safety requirements

b) Statement signed by the Competent Person that the analysis was completed .

c) Reasons why the analyst knew that the set of design documents for the Changed and Impacted Components was complete, or at least sufficient to allow the analysis.

d) Brief description of the analysis, including the method used and its results.

e) List of design documents analysed

Evidence10 Statement arguing that the person has relevant competence for the task. The argument should define relevant competence criteria (e.g. training, experience), according to the task being undertaken by the Competent Person.

8.3 Alternative Argument for Sub-claim 1

Where detailed traceability of Safety Requirements exists then an alternative argument can be presented based on Safety Requirements tracing only to Changed and Impacted Components that are fully implemented in hardware.