UK Civil Aviation Authority

Guidance: Assessment of Change Safety Cases

CAP 1801

Published by the Civil Aviation Authority, 2021

Civil Aviation Authority
Aviation House
Beehive Ring Road
Crawley
West Sussex
RH6 0YR

First published December 2019
Second edition June 2021

The latest version of this document is available in electronic format at: www.caa.co.uk/CAP1801

Civil Aviation Authority

Guidance

Assessment of Change Safety Cases

Executive summary

This document defines a systematic approach for Competent Authorities to use to assess a safety case for a change to a system providing an operational service.

The guidance is not specific to any one particular application domain. It therefore encompasses everything that might be necessary to check any change safety case, without regard to whether it is proportionate for the change in question. Consequently, it might at first sight appear inappropriately onerous for some situations.

The guidance is organised around the logically necessary documentary artefacts that are part of the safety argument in a completed change safety case, and provides a sufficient set of candidate assessment activities for each artefact, and for the argument itself. Consequently, the approach is applicable to any safety argument, regardless of its structure and presentation. Guidance is provided on selecting appropriate assessment activities and their execution. This document does not provide tutorial material: the guidance is written for use by trained staff, and the assessment method assumes adequate competence in the system and application domain addressed by the change safety case.

The guidance provides the means to vary the assessment of any change safety case according to the associated risk factors, by choosing activities that have appropriate rigour, varying the sample size, etc. Methods for doing this are outlined, but are not formally defined, as it is not yet sufficiently understood how this can be achieved.

The guidance is generic and applicable to all types of change in all types of context. It may be beneficial to instantiate the guidance for changes in a specific domain or context, or for specific types of change. Such instantiation could usefully include incorporating any specific regulatory provisions or risk criteria for the domain.

The following pages provide a summary of the assessment method.

Assessment process summary

This document presents guidance to Competent Authorities on a risk based approach for assessing a safety case for a change to a service. The assessment has the following Phases:

1. Confirm change safety case is suitable for assessment

   In the first Phase of the assessment, the assessor gains an understanding of the nature and scope of the change, and the structure and organisation of the change safety case. The assessor gains an understanding of the stages in which the change will be implemented, and what the change safety case claims is the scope of the change at each stage, and how this was determined. As part of this process, the assessor identifies and records where key topics are addressed to support later assessment activities. In doing so, the assessor confirms that the change safety case is likely to address a sufficiently wide part of the functional system and is suitable for assessment.

2. Determine risks that govern the assessment

   As it is impractical to undertake all the candidate assessment activities in this Guide for the complete scope of the change, it is necessary to determine the parts and amount of the change safety case that will be assessed, and which assessment activities will be undertaken. The assessor's legal obligations govern the strategy for modulating the assessment activities so that some overall objective is achieved, such as seeking the most serious errors in the safety case or gaining confidence in the safety performance predictions. To implement this strategy, the risks associated with the change need to be determined.

   Phase 2 establishes the risks used to plan the extent of assessment activities. This is determined from the characteristics of: the changed service, the project, operational/organisational aspects, the change, and the change safety case.

   For the lowest grades of risk, the assessment inherently undertaken during Phase 1 may be judged to be sufficient to assess the adequacy of the change safety case, so that no further assessment is required.

3. Plan and assess stage independent parts of the change safety case

   The planner prepares a plan of an appropriate set of assessment activities to assess the material in the change safety case that is not specific to one of the transitional stages. The risks identified in Phase 2, and the assessment modulation strategy identifies the parts and amount of the change safety case that will be assessed, and which assessment activities will be undertaken.

   The assessor then undertakes the assessment activities in the assessment plan, judging whether the change safety case addresses the topics defined in the assessment plan satisfactorily.

   If, during the assessment, the assessor determines that the initial planning was based on an incorrect understanding of the risks associated

with the change, then the risks are re-assessed (Phase 2) and the assessment plan is revised. The assessment then resumes according to the revised assessment plan.

4. Determine whether the planned change is credible

   This Phase determines whether the change(s) can and will be made as planned. This confirms that the functional system is likely, in actuality, to exist in the states supported by the change safety case.

   This Phase also provides an understanding of the transitional activities that should appear in the safety analyses of the services during each transitional stage, which are assessed in Phase 5.

5. Plan and assess stage dependent parts of the change safety case

   This assessment Phase assesses the change safety case material for the transitional stages. Each individual transitional stage is assessed using the following Steps:

   1) Confirm risk associated with the transitional stages and activities

   2) Plan and assess descriptions, declared SMS and claim of safety for the stage

   3) Plan and assess the scope of the change

   4) Plan and assess specification and safety analysis material (safety criteria, safety requirements and evaluation of acceptability of predicted safety performance)

   5) Plan and assess justification of specification elements (arguments of verification)

   6) Plan and assess safety of transitional activities

   7) Ensure assessment of the stage is adequately completed.

   Should any part of the assessment result in significant new information about the risks associated with the change, the assessment should revert to either Step 1 of this Phase, or even Phase 2 of the assessment process.

6. Findings and reporting

   The concerns recorded during the assessment are collated and categorised either as a comment or, if the assessor considers that the change safety case would be unacceptable if the concern remained, as a deficiency. An internal CA report and records of the assessment activities are then filed for use in subsequent processes, according to the regulatory context for review of changes.

The subsequent CA procedures regarding communication and resolution of the review findings are not addressed in this Guide.

Contents

Figures

Introduction

This document presents guidance to Competent Authorities (CA) on a systematic risk based approach for assessing a safety case for a change to a service.

The guidance may also be used by other organisations for internal or independent assessment, with any necessary adaptations if a partially developed change safety case is to be assessed.

The assessment takes place in the following Phases:

1. Confirm change safety case is suitable for assessment
2. Determine risks that govern the assessment
3. Plan and assess stage independent parts of the change safety case
4. Determine whether the planned change is credible
5. Plan and assess stage dependent parts of the change safety case
6. Findings and reporting

This document offers guidance to support the assessment. This guidance is not comprehensive, and is expected to evolve as experience is gained. It provides the topics that an assessment should investigate in a safety case. Whilst this guidance is written as if the assessment is to be conducted by a single assessor, it may be applied by a team if required. Assessors must be competent to interpret the generic guidance of this document in the context of a specific change.

Purpose of this document

This document is intended to provide guidance to a CA on how to assess a change safety case.

The assessment should also be conducted in accordance with applicable regulations and internal procedures. In particular, the CA will need procedures that address:

a. receipt of change notifications
b. deciding whether a change safety case should be reviewed
c. receipt of change safety case submissions/resubmissions
d. instigating an assessment of a change safety case using this guidance
e. the actions taken following the conclusion of the assessment.

This guidance does NOT provide tutorial material, but assumes that the assessor is competent for the task. This competence may be acquired through appropriate training and experience.

This guidance does NOT address the assessment of a change safety case to determine whether the Service Provider has followed its CA-approved safety management system (SMS) procedures, or any deviations approved by the CA.

These activities may be performed as part of regular Service Provider oversight activities conducted by the CA or as part of the CA review procedure.

This guidance does NOT address assessment of compliance with interoperability regulations.

This guidance does NOT address the safety of personnel undertaking installation activities, etc. If required, Phase 5 Step 6 could be enhanced to address this.

Purpose of assessing change safety cases

A CA assesses a change safety case to reduce the probability of an unsafe change entering service, by confirming that the change safety case is valid and accepting that the claimed level of safety is acceptable.

In some domains, not all change safety cases are assessed. Risk may be used to govern whether the CA assesses a change safety case. In this case, the risk is likely to be a combination of the safety risk associated with the change and the likelihood that the change safety case contains errors. Where this risk is low, the change safety case is unlikely to be selected for review by the CA. The change can then be implemented after the Service Provider has followed its approved change procedures, which must lead to the production of a valid change safety case prior to the change being implemented. However, when the risk associated with the change exceeds given risk criteria, the CA is required to review the safety case for the change and the Service Provider must not implement the change until it has been approved by the CA. The CA procedures for this selection process are outside the scope of this assessment Guide.

The change safety case assessment determines whether the change safety case has significant deficiencies, and hence whether it should be accepted or rejected. However, the CA procedures regarding the use of the assessment findings are outside the scope of this assessment Guide.

Assessment approach used by this guide

The overall approach implemented in this guide is that relevant aspects of the change, the change project, the change safety case, etc are considered and used to identify the 'risk factors' that govern the assessment.

Given that a complete assessment is impractical, the assessment is planned to reflect the risks associated with the identified risk factors. In principle (Phase 2 provides more detail), greater rigour is used when assessing:

a. change safety cases for which there is greater risk, as identified by the identified risk factors

b. the parts of a change safety case relating to the risk from the identified risk factors.

Hence appropriate assessment activities must be selected for each topic of the change safety case (e.g. the specifications), and for each selected activity the associated scope of assessment (e.g. some part of the functional system).

The assessment is planned by selecting from the candidate assessment activities defined in this Guide, at the same time defining the scope (e.g. of the system,

safety argument) for each activity, resulting in a review that is modulated in accordance with the risk factors. The candidate assessment activities are mainly 'syntactic' in nature, in that they determine the correctness of the various logically necessary parts of a change safety case, including their relationships to each other. Consequently, the assessment of the change safety case requires appropriately competent personnel to undertake the planning and assessment activities, in order to properly interpret the findings of the assessment activities.

Technical basis of guidance

Generically, a valid safety case is a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a functional system is safe for a given application in a given operating environment. As well as arguing that the service provided by the changed functional system will be provided safely, change safety cases also need to demonstrate that feasible transition plans are in place to implement the planned change. If services are provided while changes are being implemented, then the change safety case must argue that the services can and will continue to be provided safely during this change implementation.

The change safety case is mainly a prediction of the safety of the service that will be provided by the functional system during each transitional stage. Although many of the development and safety assurance processes for the change may go through many iterations, only the change and safety assurance established upon completion of all these iterations is relevant to the submitted change safety case.

This Guide considers that a change is implemented as one or more 'transitional stage'. When a change is implemented incrementally, each intermediate transitional stage must be justified by the change safety case as for a single change. The last transitional activities are completed in the final transitional stage, leaving the functional system and service in the final operational state. The final transitional activity could be just to implement new procedures such that the service is changed.

To argue that the changed service can and will be provided safely, for each transitional stage, the nature of a change safety case is that (in outline) it provides a structured, compelling, comprehensible and valid argument that a valid set of safety criteria has been set for a service and demonstrates that they have all been satisfied. However, this simple argument structure rapidly becomes more complex when taking into consideration different parts of the architecture of the system, the technologies deployed in each part and the contractual boundaries involved in the provision of the parts.

To be convinced that the changed service can and will be provided safely, the CA must be satisfied that:

a. the change safety case addresses the complete scope of the change (Phase 5 Step 3)

b. the service(s) to be changed and its constituent systems, subsystems, components, environment and context are specified sufficiently such that a safe change could be designed (Phase 5 Steps 3 & 4)

c. there is sufficient evidence to support the correctness of the specifications, for the operational configuration (Phase 5 Step 5)

d. safety criteria for acceptable safety performance of the changed functional system/service have been established, and appropriate safety requirements derived (Phase 5 Step 4)

e. the safety performance of the changed functional system/service has been predicted (Phase 5 Step 4)

f. the predicted safety performance of the changed functional system/ service is acceptable because it meets the safety criteria (Phase 5 Step 2)

g. uncertainties do not undermine the change safety case (approach examined in Phase 3, evaluated when encountered)

h. the proposed transitional activities are feasible (Phase 4)

i. the transition activities will be undertaken safely (Phase 5 Step 6)

j. there is sufficient evidence that the arrangements to implement the change will be provided (Phase 4)

k. when the functional system/service is changed, it will be made safe should the change not be successfully completed (Phase 5 Step 6)

l. there is sufficient evidence that the arrangements to support the operational system will be provided (Phase 5 Step 5)

m. justification that the change is a good change (Phase 3).

However, while a CA needs to be convinced on these points, it is very unlikely that they will be evident as specific claims in the safety case submission due to the complexities of the argument structure. Consequently, this Guidance defines a process to identify the elements of the safety arguments that address the above points, and organises the review process around these elements.

Principles and assertions

This document requires the reader to understand the following principles, assertions and definitions.

a. No part of a current functional system may be changed until a valid safety case exists that shows that the safety risk will be acceptable according to valid risk criteria for the change.

b. A safety case is: "a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a [functional] system is safe for a given application in a given operating environment".

c. The purpose of the safety case is to convince the Service Provider that the proposed change will be safe and to communicate the reasons for that belief to an interested stakeholder e.g. directors and senior management, regulator, judicial review or court.

d. A change safety case demonstrates that the proposed change (in all modes of operation, including fallback), and the transitional stage(s) to implement it, are implementable and will be acceptably safe.

e. A change safety case is notionally an amendment to the safety case that demonstrates all of the Service Provider's operations are acceptably safe.

f. The Service Provider only makes changes to the functional system providing its service(s). The Service Provider does not make changes to the environment into which the service is provided, though it has to prepare a change safety case if the environment is changed. Activities associated with publishing or notification of changes to other stakeholders are considered to be coordination.

g. The Service Provider has a responsibility to amend the current unit safety case (or create a change safety case) before modifying the existing functional system. This responsibility is not affected by whether the CA selects the change for review.

h. The change safety case contains safety monitoring criteria, which will be used during transitional stages and after the change has been completed to determine whether the safety performance of the changed functional system is as predicted by the change safety case. The safety criteria explicitly define measurable parameters with acceptable limits, which demonstrate acceptable safety during transitional stages and in the final operational state, and the continuing validity of the change safety case.

i. The CA assesses a change safety case to reduce the probability of an unsafe change entering service, by confirming that the change safety case is valid and demonstrates that the claimed level of safety is acceptable.

j. The CA assesses the submitted change safety case. It is not for the CA to augment the safety case or to provide an alternative safety case in order to decide that there is sufficient confidence in the claims made. Findings can only be based upon the contents of the delivered change safety case, together with any documented clarifications or further information supplied in response to the CA's enquiries. However, the CA may challenge or rebut the safety case on the basis of expert knowledge or independently acquired information.

k. The change safety case must declare the basis of any judgement or claim of sufficiency or adequacy, and justify the validity of that basis. The role of the CA is to determine whether it concurs with these declared arguments, not to determine sufficiency or adequacy itself.

l. The CA does not undertake any 'independent verification' activities as part of the assessment of the change safety case. If the change safety case cannot make a sufficiently strong argument without evidence from independent verification, then the Service Provider must procure such evidence, and integrate the results in the change safety case.

m. The change safety case must address all harm within the scope of the CA's responsibilities that the changed service can cause. 'Harm' includes both unintended harm and harm due to malevolent action.

n. A single change safety case may address forms of harm falling within the remit of more than one CA.

o. The change safety case is NOT responsible for justifying that the delivered service meets any stipulated physical security criteria.

p. The change safety case needs to reference a justification of the controls that ensure that only authorised changes are made to the functional system, so that the functional system remains in the state addressed by the change safety case.

q. The change safety case needs to reference a justification of the physical security arrangements protecting the functional system so that the residual risk of physical alteration by a malevolent actor of the functional system (from the state addressed by the change safety case) is known.

r. The change safety case must justify that the safety effects of malevolent actors modifying the functional system have been addressed.

Definitions and Terminology

Baseline system

The baseline system is that build of the functional system used as the baseline for impact analysis and comparative safety criteria.

It is possible that some brief transitional stages may be permitted when only weak assurance is available, for example to gather safety performance data, for the purpose of creating assurance. Such transitional stages are unsuitable as a baseline.

Functional system, operational system and support system

A functional system is operated by a Service Provider to deliver a desired service, and comprises a combination of equipment, procedures and human resources. This includes all those things considered as being assets (e.g. buildings, expertise, information in a database) or resources that are required for the operation of the functional system.

This Guide considers the functional system as comprising an operational system that delivers the desired service, and support systems that support running the operational system.

The operational system includes all systems that directly contribute to the provision of the service(s), including systems such as telecommunications, power, cooling, and underlying IT infrastructure.

Support systems include training, data preparation, and test and development systems (a longer list of examples is in candidate assessment activity 32.5 on page 156).

The distinction between operational system and support system is made for two reasons:

a. the need to assure changes and impacts on support systems is often not recognised

b. the degree of assurance required for support systems is typically lower than that for the operational system, and the Guide needs to identify suitable candidate assessment activities for both.

Impact & Impact Analysis

The purpose of the impact analysis is to identify all POSSs whose existing assurance (arguments and evidence that their specifications are trustworthy) will be invalidated by the change, and hence establish the Scope of the change (see below). The assurance for a POSS may be impacted by:

a. a direct change made to the POSS

b. a change to the environment of the POSS, such that it is outside the range for which its specification was valid, brought about by changes in communications or resources shared with other POSSs

c. a change to the safety requirements apportioned to the POSS in the changed functional system, either in terms of function, integrity or confidence.

The complex issues associated with impact are addressed by this Guide in the candidate assessment activities for the 'Lists of changed and impacted Parts of the Operational and Support Systems (POSSs)' (page 141), and the 'Justification of lists of changed and impacted POSSs' (page 142).

POSS - Part of the Operational and Support Systems

The complete set of POSSs makes up the functional system. See glossary entry for 'Functional system, operational system and support system'.

The scope of the safety case can be minimised by identifying only those POSSs that are changed or impacted, rather than assure the complete functional system. See glossary entry for 'Scope of the change'.

The term 'Part' is used to avoid the architecture level implications of terms like 'component', 'subsystem' and 'system'.

POSSs must be uniquely identifiable and under configuration management. They can be defined at any architectural level (for example an electronic component or a data processing system), and so a POSS is usually part of another POSS, its parent. Parent POSSs are only considered to be changed if at least one of their (immediate) child POSSs has changed behaviour (which includes new and removed child POSSs).

Risk factor

The term 'risk factor' refers to those considerations that govern the extent to which the change safety case is assessed. Risk factors influence the assessment (its rigour and which aspects will be the foci of the

assessment) either on the grounds of the level of safety risk or because there is a risk that they could lead to the change safety case being incorrect, i.e. the change made is not as defined in the change safety case, or the claims made are not demonstrated with sufficient confidence due to inadequacies in the inferences or evidence. Consequently, the risk factors are derived not only from safety risks, but also project or operational circumstances, and properties of the change or the change safety case.

The 'modulation' of the review ensures that the change safety case is reviewed in a manner that is proportionate to the associated risk or risks. The relevant risk factors (and the modulation applied) are dependent on the objective of the review, which may be defined by legislation or regulations.

Risk factors are analysed to support review modulation in Phase 2 of the review process.

Risk factors may relate to the complete change, or be specific to individual transitional stages. Additionally, deficiencies found previously, when assessing an earlier version of the change safety case, would also influence the modulation.

A single assessment modulation is not appropriate for the whole change safety case, so different assessment modulations need to be defined for the different parts of the change safety case according to the risk factors relevant to the part. To support the review process in this Guide, it is necessary to define the modulation for assessment of the parts of the change safety case relating to:

a. the safety of the service provided during each individual transitional stage (Phase 5 Steps 2 to 5)
b. the safety of the transitional activities during each individual transitional stage (Phase 5 Step 6)
c. the feasibility of the transitional activities during each individual transitional stage (Phase 4)
d. all other aspects, which are not specific to a specific transitional stage (Phase 3).

Some risk factors may influence the assessment of more than one of these, and/or for more than one transitional stage. For example, a certain contractor might be involved in transitional activities for several of the transitional stages, and be thought to be inexperienced (high risk), and so this would influence the modulation towards activities and functional system aspects that are related to the contractor.

The following is an indicative list of categorised risk factors:

Changed service

a. the nature of the changed services, including complexity and novelty

b. the safety risks associated with the changed services

Project

c. the project competence in technologies, activities, and safety assurance

d. implementation resources required

e. timescales

Operational / Organisational

f. organisational competence e.g. in operating the relevant technologies, processes, and safety management

Change

g. the nature and safety risks associated with the POSSs within the scope of the change

h. the extent of risk reduction intended to be provided by the change

i. the safety risks associated with undertaking the transitional activities to implement the planned changes

j. technical novelty and complexity

k. the modes of operation

Change safety case

l. presentation style and quality

m. structure of the safety argument.

Safety performance and safety criteria

The term 'safety performance' is used to denote the functional system or service properties that measure the safety of the service provided, both when setting the safety criteria which specify acceptable performance, and when predicting the performance of the changed functional system to determine whether it meets those safety criteria. The term is used so that either acceptable levels of risk or usually acceptable rates of occurrence (if they can be shown to be a valid proxy for risk) can be the defined measure, according to the nature of the change. In the main, it is expected that changes affecting the logic of the accident sequences (the path from hazard to the accidents) will be measured in terms of risk.

Scope of the change

The change safety case is concerned only with justifying the change, including its impact. Together, the POSSs that are changed or impacted define the 'Scope of the change'. The change safety case does not need to justify the safety of the functional system outside the scope of the change, although some specifications may be required outside the scope of the change to help apportion safety performance criteria correctly.

Specification

> A declaration of all the behaviour and properties of a POSS exhibited in the predicted operational environment. This includes all potential behaviour, including that induced by failures and that identified as potentially unsafe behaviour by safety analysis.
>
> Each element of behaviour and property in the specification must be supported by evidence, i.e. the specification declares actual behaviour revealed by test or analysis, not the behaviour that may have been originally intended or specified as a requirement.
>
> For each element, the specification states the associated integrity and confidence, derived from the supporting evidence and analysis by an appropriate argument (according to the quantity, pedigree, etc of the evidence and the nature of the POSS and of the behaviour or property).
>
> The way that this holistic view of a specification is currently implemented in practice is described in 'Appendix C – Description of change safety case topics', 'Specifications of parts of the operational system (Page 152)' on page 108.

Transition Plan

A single transition plan for a transitional stage (see below) can encompass installation, commissioning, (other) transition activities and recovery, or each of these aspects could have its own separate plan. Typical content of these plans (as relevant to assessment of a change safety case) is described in the introduction to the Phase 4 Topic Tables on page 131.

Terminology relating to changes and transitional stages

A change can be implemented as a single transitional stage, or as a sequence of transitional stages by operating the functional system/service in a sequence of states, where the last fully implements the intended change. A transitional stage starts with the transition of the functional system/service to a new state, this change being implemented by specified transitional activities. Most transitional activities, however, do not affect the functional system/service during a transitional stage. They concern adding or modifying assets that are currently non-operational, so that they ready to be used operationally, or clearing up – 'making good' and removing assets for disposal. The safety case will usually justify that such transitional activities will not affect the functional system. It may therefore be necessary to define an additional initial transitional stage, to consider the effects of the preparatory transitional activities on the extant functional system i.e. before the first transition.

The service provided during a transitional stage may either be the full service or a reduced/restricted service, or the service may be completely withdrawn.

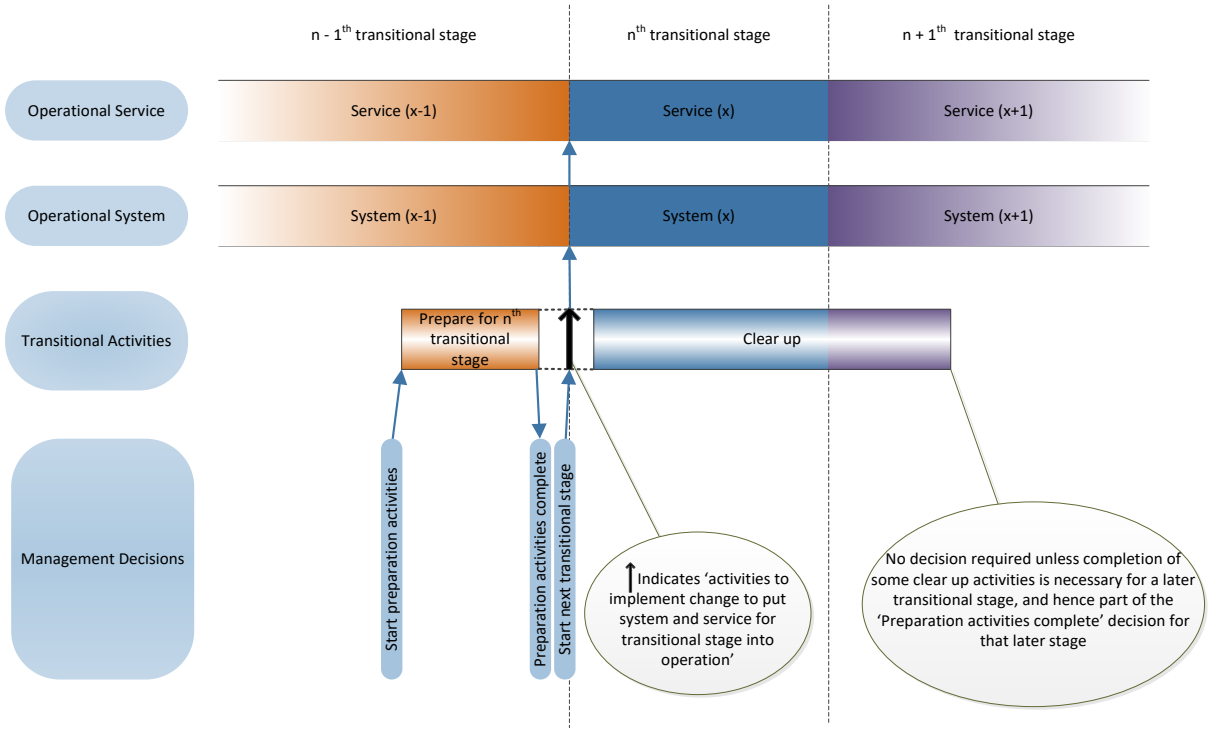

Figure 1: Representation of a transitional stage, including associated transitional activities and decisions

For each transitional stage, the following must be defined:

a. the criteria for deciding whether each transitional stage can be started, which must include the availability of the assets/resources required to make the transition and to operate once transition is completed

a. a specification of the assets/resources required in a)

b. the transitional activities to be undertaken during the transitional stage (typical transitional activities are listed in the introduction to the topic tables for Phase 4)

c. the criteria for deciding when the transitional activities have been successfully completed

d. the plan for recovery to a safe assured state, should the change be judged unsuccessful, e.g. the change is not successfully implemented as planned.

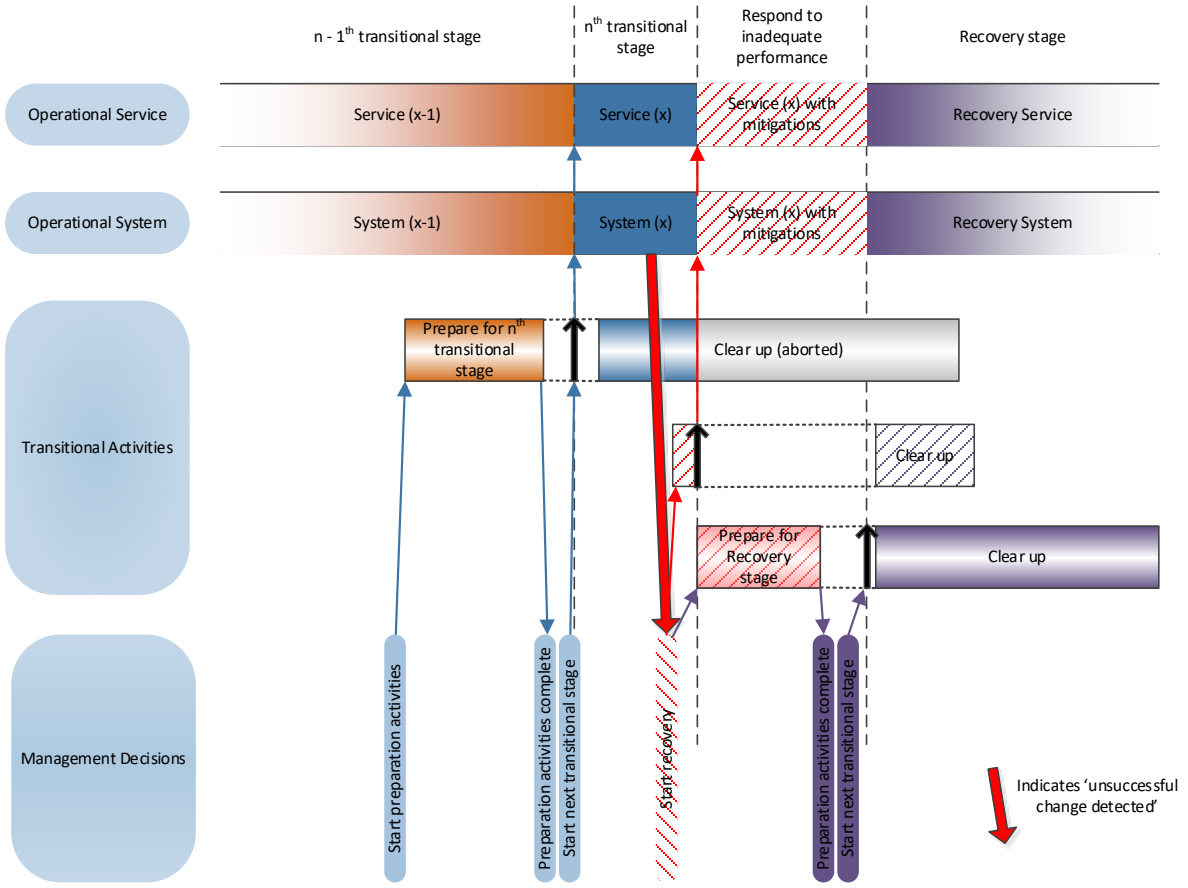

Figure 2: Recovery activities instigated because change is found to be unsuccessful

The first transitional stage may not be commenced until the CA's approval of the change safety case has been granted, although preparations that have no impact on the existing functional system and service may be undertaken, whether this is patently obvious (e.g. manufacture of equipment offsite) or demonstrated by impact analysis in accordance with the Service Provider's SMS.

The change safety case demonstrates:

a. the safety of the functional system/service as it exists during each transitional stage

b. the safety of the collection of transitional activities occurring during each transitional stage, which mainly comprises preparations for subsequent transitional stages or clearing up after preceding transitional stages[1].

The safety of the existing pre-change service does not need to be justified by the change safety case, as it has an existing approval.

The final transitional stage includes the transitional activities that implement the last of the planned changes to the functional system and service and remove surplus assets, which means that the change safety case for the final transitional

[1] Any activities required to gather evidence of behaviour to provide safety assurance for a later transitional stage are considered to be part of the safety monitoring activities included in the operational system.

stage justifies the safety of the functional system and service in the ongoing operating state i.e. complete implementation of the change.

The safety of the transitional activities undertaken during each transitional stage needs to be demonstrated by establishing the risk to the functional system and the service(s) being provided during the transitional stage. This needs to take account of all transitional activities occurring during that transitional stage. The transitional activities during a transitional stage are mostly associated with preparation for the subsequent transitional stages, and/or with clearing up from the previous transitional stages. The safety of all these transitional activities together needs to be demonstrated in the context of the functional system/ service prevailing when the transitional activities are undertaken.

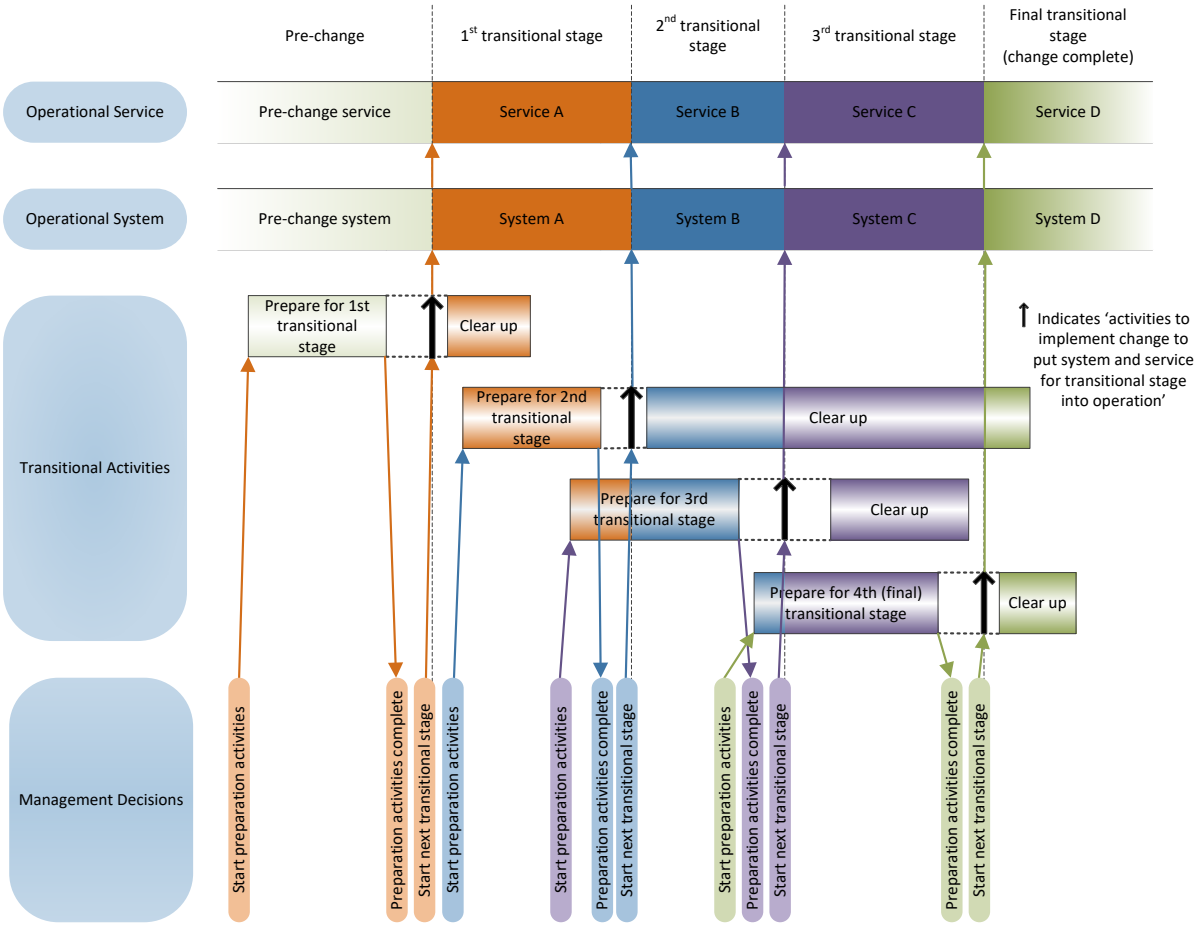

Figure 3: Transitional activities during each stage may be associated with more than one transitional stage for a change implemented using multiple transitional stages.

Assessment method

Overview

This section overviews the method used in this Guide for the assessment of a change safety case. This assessment is part of the overall procedure for CA review of change safety cases (see Appendix A). The process for selecting which change safety cases should be reviewed is outside the scope of this guidance, as is the CA's response to any deficiencies that are identified.

The approach described here is for the assessment of the change safety case submitted for approval, but the same general approach can also be used for assessing earlier drafts of the change safety case e.g. for large or protracted projects.

The input to the assessment process is a change safety case for a proposed change. The Service Provider will submit a safety case report (perhaps with key supporting documents) for the change, rather than a complete safety case. The safety case report for the change will identify the claims and arguments (although not necessarily all of them), but will probably not include the bulk of the supporting evidence due to the practicalities of providing access to it. The Service Provider is obliged to facilitate access to any of this additional information that the CA requires for the assessment. Therefore, for conciseness, this guidance only makes reference to the change safety case and not the safety case report from this point.

The guidance recognises the separate roles of the planner and the assessor, with the planner also usually providing overall management and coordination of the change safety case assessment. There is no reason why there should not be more than one planner or assessor if this fits the size or scope of the assessment, or both roles could be fulfilled by one person. However, dividing the assessment between multiple assessors reduces the ability of each to identify inconsistencies etc. Although the guidance includes various provisions for the assessor(s) to make records to aid communication, this only partially mitigates the problem.

The planner progressively plans the assessment at various points during the assessment process, so setting the best focus for successive assessment activities as the characteristics of the change and the change safety case are understood more fully[2]. The guidance provides an approach for assessing change safety cases in an efficient and logical process, which progressively builds the assessor's understanding, by viewing the material provided by the change safety case in the following layered manner:

a. material that initially familiarises the assessor, and allows confirmation that the change safety case is suitable to be assessed
b. introductory and other material that is independent of the transitional stages
c. material that is specific to each transitional stage

[2] This also avoids wasted effort in cases where significant deficiencies are identified early in the process

d. specification and safety analysis material, specific to each transitional stage

e. verification material, specific to each transitional stage

The assessment process is defined as a sequence of Phases, as illustrated in Figure 4. The term 'Phase' is used exclusively for the Phases of the assessment defined in this Guide. Where necessary, Phases are broken down into 'Steps'. This terminology is used so that the term 'stage' can be used exclusively to refer the stages of implementation of the change defined by the Service Provider.

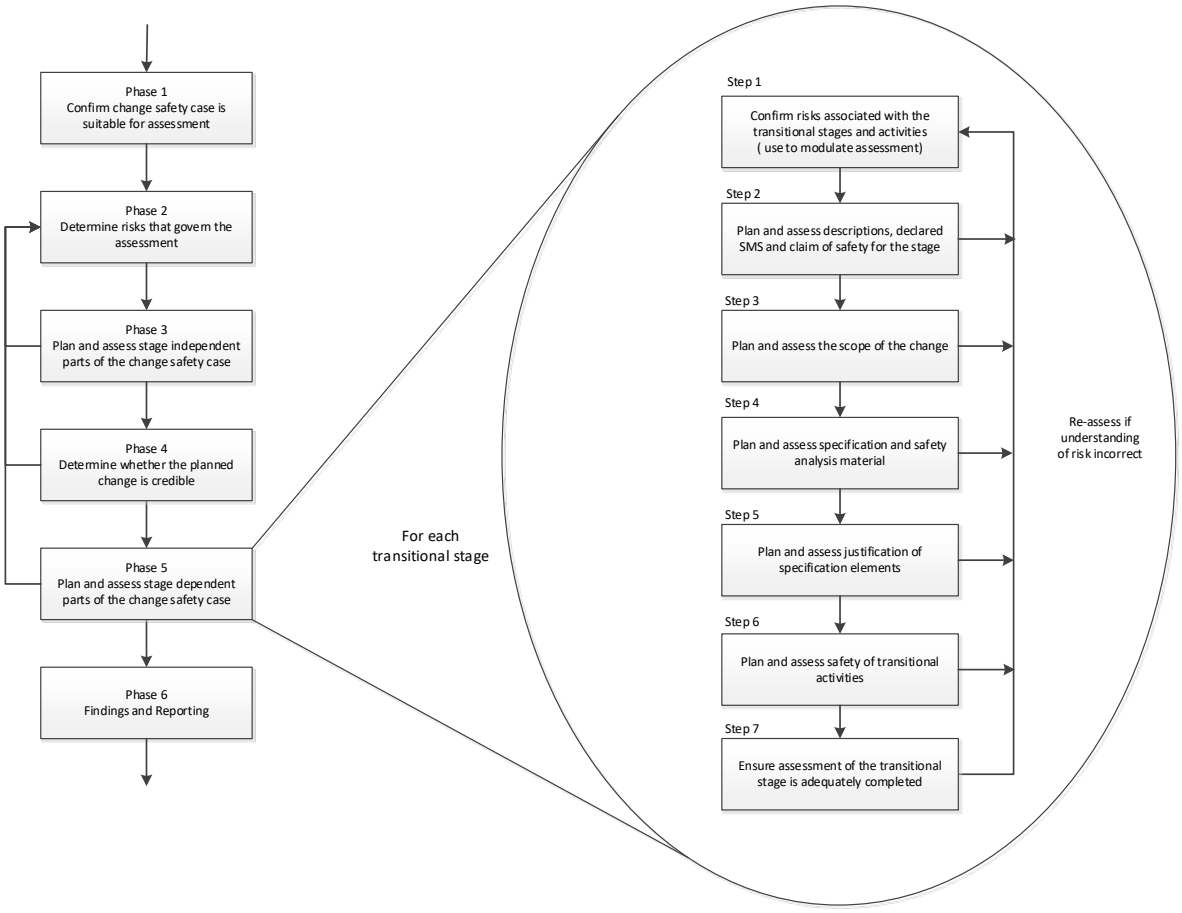

Figure 4: Change Safety Case Assessment Process Overview

In Phase 1 of the assessment, the assessor gains an understanding of the nature and scope of the change, and the structure and organisation of the change safety case. The assessor gains an understanding of the stages in which the change will be implemented, and what the change safety case claims is the scope of the change at each stage, and how this was determined. As part of this process, the assessor identifies and records where key topics are addressed to support later assessment activities. In doing so, the assessor confirms that the change safety case is likely to address a sufficiently wide part of the functional system and is suitable for assessment.

During Phase 1, the assessor also confirms that the safety analyses appear adequately trustworthy to use the information to plan the rest of the assessment. These safety analyses are those for the services provided during each transitional stage, and also the transitional activities that implement the changes to the functional system. The general feasibility of the proposed change is also initially confirmed.

As it is impractical to undertake all the candidate assessment activities in this Guide for the complete scope of the change, it is necessary to determine the parts and amount of the change safety case that will be assessed, and which assessment activities will be undertaken. The assessor's legal obligations inform the strategy for modulating the assessment activities so that some overall objective is achieved, such as seeking the most serious errors in the safety case or gaining confidence in the safety performance predictions. To implement this strategy, the risks associated with the change need to be determined.

Phase 2 establishes the risks used to plan the extent of assessment activities by considering the relevant 'risk factors'. In subsequent Phases appropriate assessment activities are selected to assess the change safety case, based on an understanding of these risks.

In Phase 3, the material in the change safety case that is not associated with a specific transitional stage is assessed. The planner prepares a plan of an appropriate set of assessment activities. The risks identified in Phase 2, and the assessment modulation strategy identify the parts and amount of this material that will be assessed, and which assessment activities will be undertaken.

The assessor then undertakes the assessment activities in the assessment plan, judging whether the change safety case satisfactorily addresses the topic(s) covered by the Phase or Step.

If, during the assessment, the assessor determines that the assessment planning was based on an incorrect understanding of the risks associated with the change, then the risks are re-assessed (Phase 2) and the assessment plan is revised. The assessment then resumes according to the revised assessment plan.

Phase 4 determines whether the change(s) can and will be made as planned. This confirms that the functional system is likely, in actuality, to exist in the states supported by the change safety case.

For each individual transitional stage, Phase 4 of the assessment assesses:

a. the feasibility (not safety) of the planned transitional activities that implement the change
b. whether the planned transitional activities are sufficient to implement the stated change
c. whether the prepared parts to be inserted into the functional system will be available
d. whether the necessary resources to undertake the change will be available
e. whether the criteria to support transition decisions are adequate.

The assessment activities are planned, according to the risks (determined in Phase 2) associated with the transitional activities for the relevant transitional stage.

Additionally, Phase 4 provides an understanding of the transitional activities that should appear in the safety analyses of the services during each transitional stage, which are assessed in Phase 5 Step 6.

Assessment Phase 5 assesses the change safety case material for the transitional stages. Each individual transitional stage is assessed using the following Steps:

1. Confirm risk associated with the transitional stages and activities
2. Plan and assess descriptions, declared SMS and claim of safety for the stage
3. Plan and assess the scope of the change
4. Plan and assess specification and safety analysis material (safety criteria, safety requirements and evaluation of acceptability of predicted safety performance)
5. Plan and assess justification of specification elements (arguments of verification)
6. Plan and assess safety of transitional activities
7. Ensure assessment of the stage is adequately completed.

The confirmed risk from Step 1 is used to modulate the planned assessment activities in the other Steps, for the relevant transitional stage.

Phase 5 Steps 2 to 5 address related parts of the change safety case (for a specific transitional stage), in a sequence where each provides information that is useful for planning the subsequent assessment steps e.g. what to focus on when selecting samples, in accordance with the risk modulation.

The assessment of each transitional stage is planned and assessed individually. Given sufficient competent resources to conduct the assessments, stages could be assessed concurrently, provided that there are no interdependencies.

Should any part of the assessment result in significant new information about the risks associated with the change, the assessment should revert to either Step 1 of Phase 5, or even Phase 2 of the overall assessment process.

Finally, in Phase 6, the concerns recorded during the assessment are collated and evaluated to determine their significance in the context of the overall safety case. The concerns are categorised as either a deficiency, if the assessor considers that the change safety case would be unacceptable if the concern remained, or else a comment. An internal CA report is prepared that documents the activities used to assess the change safety case in each Phase, and records the findings (deficiencies and comments). The report and assessment records are then held for use in subsequent processes, according to the regulatory context for the review (discussed in 'Appendix A – Context of change safety case assessment guide' on page 92).

Through-project oversight of change

Oversight of a change may commence prior to receipt of the change safety case. By witnessing project activities and discussion with the Service Provider, the

assessor can build an understanding of the change as the project progresses[3], and can identify and evaluate risk factors. The understanding gained may be used to challenge but not supplement the submitted change safety case, which must provide a sufficient justification by itself.

Recording additional material

Where the assessor requires further information or clarifications from the Service Provider, all queries sent and responses received should be kept as part of the assessment records. If the responses supplement the information in the change safety case, or provide substantial explanation, then the assessor should record a finding that the change safety case needs to be changed to incorporate the information provided in the response.

Generic guidance on assessment planning

Introduction

This section provides guidance on assessment planning that applies throughout the assessment. Specific guidance is provided, where applicable, in each assessment Phase.

Planning of the assessment is conducted by the assessment planner in accordance with the governing CA procedure. The relationship between this Guide and the governing procedure is illustrated in 'Appendix A – Context of change safety case assessment guide' on page 92.

The CA procedure may constrain the assessment, for example by stipulating certain aspects of the change safety case that should or should not be assessed, to reflect CA policy decisions regarding expectations of practice in the industry domain. The planner must ensure that the assessment plan reflects any such constraints.

Planning using the candidate assessment activities

The first version of the assessment plan is created in Phase 3, and addresses the parts of the change safety case that are independent of the change's transitional stages. The assessment plan is developed further during subsequent assessment Phases, at several points, as more information becomes available. The plan defines the assessment activities, including their scope and rigour and the appropriate elements of the change safety case to be assessed.

The objective of the review may need to be interpreted to define the practical strategies to be used when carrying out the assessment. The planner should adopt an appropriate balance between 'practical strategies' such as: identifying the greatest number of errors, finding the most serious errors in the safety case,

[3] There are other regulatory benefits from doing this that are out of scope for this guidance e.g. influencing the safety of the change, monitoring compliance with the SMS, and gathering information to influence regulatory strategy.

checking correctness of the inferences, or gaining confidence in the safety performance predictions.

The assessment phases address the various topics that form part of a change safety case. For each topic, the guidance section for each Phase references tables in the appendices to assist the planner. Each table addresses a candidate subject, related to the topic, that can be presented in a change safety case, and provides candidate assessment activities.

The candidate subjects are either:

a. key subjects of the change safety case

b. worksheets or analyses that record the derivation of the key subjects (for those key subjects where these records are usually likely to be examinable, and this is likely to be worthwhile)

c. a justification of the validity of the key subjects, or sometimes of their derivation or verification.

The plan must identify which assessment activities will be conducted. These may vary for different parts of the changed functional system or different transitional stages (for example). Specific guidance is provided in each assessment Phase to help the planner use the tables to identify the appropriate assessment activities.

When it is desired to ensure that candidate subjects are correctly integrated in the overall safety argument, the planner should select those candidate assessment activities that examine whether the candidate subjects are correctly related to others.

In some cases, candidate assessment activities are provided that have different levels of expectation regarding the rigour with which the change safety case addresses the topic, to permit the appropriate assessment of arguments providing greater or lesser confidence. Similarly, the Guide provides multiple candidate assessment activities to check the same or related aspects, varying in power or rigour, or addressing broader or more targeted scopes. The planner needs to select the activities that are most appropriate for the specific assessment.

Whilst the candidate assessment activities in this Guide are intended to be a reasonably complete set of the activities that could be undertaken for each candidate element generically, the planner may specify further activities. This may be necessary because the generically stated activities do not adequately examine the scope of specific concerns relating to the change or the change safety case.

The candidate assessment activities are ‘stand-alone’ activities, addressing essential attributes of the candidate subjects, and so, for example, the planner can stipulate that a justification is assessed in isolation, or that the invoked evidence is also examined at the same time. The essential attributes of a candidate subject which may be assessed include:

a. the formal aspects of the change safety case, e.g. process records, scope, responsibility, conformity to regulations

b. the formulation, readability, traceability, clarity, etc. of the documentation

c. the correctness of relationships with other candidate subjects (consistency)

d. the content of the candidate subject (and any referenced items)

e. the correctness of the argumentation e.g. its logic, associated evidence, induction, deduction, consistency, and whether the evidence supports the arguments.

The candidate assessment activities are defined only for key logically necessary candidate subjects. However, those candidate subjects that are justifications will also identify the complete set of evidence necessary to support the argument made.

Whilst related candidate assessment activities are presented using various levels of indenture, the planner is not constrained to select these grouped candidate assessment activities together, but should select appropriate activities according to the risk factors and content of the change safety case.

Modulating the rigour of the review in accordance with risk

The assessment of the change safety case must be conducted in a manner proportionate to the risks associated with the change, which are the result of risk factors. This section describes the generic mechanism of how the assessment is varied to respond to these risks. The guidance in Phase 2 gives more detail on how this is actually enacted.

The risk factors include 'safety risks', because it is clear that a change safety case associated with greater safety risk should be reviewed more rigorously than one associated with lower safety risk. However, this must be considered in conjunction with a view of the difficulty of achieving an acceptable level of safety, because a system that requires great complexity in architecture and mitigation to be acceptably safe would be of greater concern than one that achieved it in a straightforward manner.

According to the risks associated with the change safety case, not all parts of the safety case need to be assessed with the same rigour. These risks are established, by identifying and analysing the risk factors that give rise to them (Phase 2), in order to plan appropriate assessment activities for the parts of the change safety case relating to:

a. the safety of the service provided during each individual transitional stage (Phase 5 Steps 2 to 5)

b. the safety of the transitional activities during each individual transitional stage (Phase 5 Step 6)

c. the feasibility of the transitional activities during each individual transitional stage (Phase 4)

d. all other aspects, which are not specific to a specific transitional stage (Phase 3).

Whilst the appropriate assessment activities formulated in subsequent Phases are primarily based on the identified risks, the planner should also consider:

a. the dependencies between the safety case elements identified in this Guide

b. the structure of the service provider's argument, e.g. considering commonalities and other structural features of the argument

c. the system architecture, e.g. commonalities and other structural features created by the relationships of the POSSs.

The variation of rigour of assessment is enacted by strategies such as:

a. varying sampling levels

b. varying the degree of challenge[4]

c. varying the formality with which the assessor undertakes and records the assessment

d. selecting stronger or weaker assessment activities, according to the techniques specified in them.

If a revised change safety case is being assessed, any deficiencies identified when assessing the previous version will be identified along with the risk factors in Phase 2. Assessment activities should always be planned to determine whether the deficiencies have been rectified, as well as addressing the risk factors.

It is possible that the risks associated with the change safety case are such that it is not necessary to undertake any assessment activities for some parts of the change safety case. This is a valid result of using risk to govern the change safety case review. In some cases, this may be due to earlier assessment activities, having provided sufficient confidence. In others, it is that the risks meant that no assessment activities were necessary.

The rigour with which the change safety case is assessed should not be influenced by either the planner's or the assessor's familiarity with the type of change and functional system or service, as they may be unaware of some peculiarity associated with the change.

The assessment plan may stipulate first-hand inspection of some of the documents or POSSs referred to by the change safety case submission[5]. Such inspection should verify that the document or POSS is in fact as described in the change safety case arguments, and so establish confidence in the reliability of the information presented. The Service Provider and planner should be aware that accessing referenced documents may impact the assessment timescales. Where possible, the planner should anticipate the need to access such documents and 'pre-order' them in advance of the relevant assessment phase/ step.

[4] 'Challenge' is taken to be the attempt to identify rebutting arguments or counter evidence, e.g. from previous experience and incident reports.

[5] These documents may not form part of the safety case submission and so may need to be requested from the Service Provider.

Specifying assessment activities

The resulting assessment plan should specify activities to be conducted on parts of the change safety case in terms of:

a. purpose, if not obvious (e.g. the rationale or higher-level objective for the specified set of activities and objects of assessment)

b. which topics and candidate subjects in the change safety case will be assessed

c. for each candidate subject, the specific examples that are to be assessed. Those specified may represent, for example, those for:

   i. specific parts of the functional system

   and/or

   ii. specific threads of assessment (e.g. certain functions or safety requirements) that a set of activities follow, through different parts of the change safety case, as identified by the risks

d. which activities are to be conducted for each specified example of the candidate subject

e. instructions that govern the 'rigour' of the assessment activity e.g.:

   i. guidance on what is viewed as 'acceptable' under the activity

   ii. the techniques to be used (e.g. unguided review, check based on general appreciation of the candidate assessment activities, undocumented conduct of specified candidate assessment activities, explicit documented analysis according to specified candidate assessment activities)

   iii. the sample to be assessed, either by

      - specifying a sample identified by the planner, using an appropriate sampling strategy
      - specifying the sampling strategy to be implemented by the assessor, and criteria for the sample size e.g. a random sample of six items, or all items referring to a certain function

   iv. whether supporting evidence is assessed in conjunction with arguments, e.g. to determine whether the evidence is:

      - as indicated in the argument
      - adequate to support the conclusion drawn by the argument
      - sufficiently trustworthy

   v. the extent to which the claims, arguments and evidence are to be subject to assessment against the generic rules of argumentation

   vi. the extent to which the claims, arguments and evidence are to be subject to challenge[4]

vii. identification of individual assessors with the necessary competences to undertake the specified activities[6].

Generic guidance on conduct of planned assessment activities

This section provides generic guidance to the assessor(s) on how to conduct the planned assessment activities. Where applicable, more detailed guidance for assessors is provided in the guidance for each Phase.

In cases where an assessor did not participate in the earlier Phases of the change safety case assessment, the assessor may need to examine the familiarisation records and introductory material in the change safety case.

In order to achieve the objectives of efficient and risk-based assessment, the assessor should only undertake the activities stipulated by the planner. However, this should not prevent the assessor from recording any other issues identified whilst carrying out the planned activities.

When undertaking the defined assessment activities, the assessor:

a. uses the information collected in previous Phases and the assessment plan to identify the documentation related to the required assessment activity
b. refers to any specific guidance provided for the topic or activity
c. considers whether any of the material reviewed provides information that identifies or relates to a risk factor
d. completes each activity allocated to the assessor, recording the result of the assessment[7]

In some cases, the assessor will have to make judgements regarding adequacy based on experience and understanding of industry working practices and standards. These reflect a historic view of risk, so the assessor should be aware that such practises may need to be revised to address:

a. changes in demand or the environment into which the service is delivered
b. changes in societal expectations and the legislative environment
c. developments in good practice
d. innovative approaches, applications or technologies.

Some of the candidate assessment activities specifically use the phrase ‘appears to’ where it is recognised that the check given cannot be completely undertaken without actually verifying the point. As it is not the responsibility of the assessor to undertake verification, the assessor is only required form a judgement based on the appearance of the material presented.

At any time, the assessor can use the candidate assessment activities for Uncertainties in Phase 3 to determine whether the change safety case

[6] Some activities may require more than one assessor to cover the necessary competences, for example competence in a safety technique, and competence in the related industry operation.
[7] These records must be made to demonstrate that the change safety case has been properly assessed.

satisfactorily addresses any uncertainties that need to be addressed at the point they are encountered. The assessor should check that any significant uncertainty issues identified during the assessment are present in the Justification of the treatment of uncertainties (page 126), to determine whether the change safety case makes all stakeholders aware of them.

The assessor is cautioned against making assumptions about the content or nature of the change safety case on the basis of previous experience or familiarity with the subject matter, as the submitted change safety case may differ from what is assumed.

In addition to carrying out any assessment activities stipulated by the Planner, the assessor can enlist the aid of the generic checks for assessing argumentation (see Appendix E – Candidate assessment activities for elements of arguments, page 186), where this clarifies any issue with the target of assessment. Many of the candidate assessment activities address specific 'justifications' that should be present in the change safety case. The term 'justification' denotes that these are appropriately presented arguments that should comply with the generic rules for argumentation, with a rigour appropriate for the subject and nature of the argument. For example, it would be normal for justifications to present or reference supporting evidence.

Should a justification declare, or the assessor find, that an evidence item required to support a justification does not yet exist, then the assessor should record this as an assessment finding unless the evidence item is declared in the list of outstanding evidence items in the change safety case. This declaration may be made by referencing the justifications or documents that require evidence. If a particular outstanding evidence item is of concern, the assessor may check that the change safety case shows that:

a. the outstanding evidence item is sufficiently defined
b. the acceptability criteria (for the evidence item to support the justification using it) are defined
c. the method for generating the evidence is known
d. the conditions under which the evidence will be collected do not invalidate the evidence
e. the activity to generate the evidence has been planned and is consistent with the decision criteria in the transition plans
f. the evidence will be generated in a timely manner.

When all allocated assessment activities for a topic area have been completed, the assessor:

a. considers whether the arguments and evidence examined provide sufficient confidence in the supported claim
b. considers whether arguments in the change safety case have suitably taken into account known generic issues associated with similar changes
c. considers whether the claims made relating to the topic appear sufficient to address the full scope of the topic

d. considers whether or not the assessor has any knowledge that can demonstrate that any of the claims made are false

e. considers whether any concerns noted during previous assessment Phases have been resolved

f. records any concerns that may require follow up

g. records any concerns that appear to be findings of the assessment, and tentatively assigns each a finding category, using the scheme defined in Phase 6.

In some cases, the assessor may identify that there are significant issues with the change safety case, and may agree with the planner to terminate the assessment before completing all the assessment activities. This decision must only be made if there is clear reason to reject the change safety case.

Phase 1 Confirm change safety case is suitable for assessment

Introduction

The purpose of this Phase is to confirm that the change safety case is suitable for assessment, and to gain familiarity with it.

During this Phase the assessor gains an understanding of the nature and scope of the change, and the structure and organisation of the change safety case. The assessor gains an understanding of the stages in which the change will be implemented, and what the change safety case claims is the scope of the change at each stage, and how this was determined. As part of this process, the assessor identifies and records where key topics are addressed to support later assessment activities. In doing so, the assessor confirms that the change safety case is likely to address a sufficiently wide part of the functional system and is suitable for assessment.

This Phase comprises several Steps:

1. Check change safety case been adequately prepared
2. Understand the proposed change
3. Confirm the declared scope of the change is credible
4. Build familiarity with the parts of the change safety case
5. Identify applicable standards and regulations
6. Consider plans for Installation, Commissioning, Transition and Recovery
7. Check scope of safety analyses
8. Decide whether the change safety case is suitable for assessment

Phase 1 Step 1 Check change safety case has been adequately prepared

Introduction

The purpose of this step is to determine whether the change safety case has been adequately prepared and reviewed, in order to confirm that the assessment should proceed.

Conduct

The planner nominates a suitable assessor to undertake Phase 1 of the assessment, perhaps according to the nature of the change, and the Service Provider concerned.

The assessor establishes whether the change safety case:

a. provides evidence that it was authorised for release (publication) by the Service Provider

b. provides evidence that it has been subject to review and verification by the Service Provider to ensure its validity before presenting it for assessment by the CA

c. provides evidence that the Service Provider has verified that the change safety case complies with the Service Provider's SMS

d. provides evidence of the authorisation and release of the change safety case was conducted in accordance with the Service Provider's SMS

e. describes the verification of the change safety case[8], and gives references to the verification records

f. makes a clear overall claim of safety of the proposed change

g. addresses the safety of:

    i. transitional activities, including decommissioning and removal, if appropriate

    ii. the service(s) affected by the change during transitional stages

h. refers to plans for the activities and resources required for installation, commissioning, transition and recovery, and (if appropriate) decommissioning and removal

i. appears to be: finished, comprehensive, formal and free of grammatical and typographical errors

j. appears to comply with any regulations that stipulate the mandatory contents of a change safety case.

If the change safety case has not been adequately prepared and reviewed, the assessor should terminate the assessment at this point without any further assessment, proceeding directly to Phase 6.

[8] For example, verification of the correctness of calculations, safety models, and the syntactic correctness of the arguments presented.

Phase 1 Step 2 Understand the proposed change

Introduction

The purpose of this step is for the assessor to gain an understanding of the change by reading the parts of the change safety case that describe the change and associated systems and services, accepting what the change safety case states 'at face value'.

The assessor records the relevant information and its location for use by the planner and any other assessors.

Conduct

The assessor will gain an understanding of the change largely from descriptive material that describes the changes to be made to the functional system and services, the impact of those changes, and the resultant effect on their behaviour and properties.

The assessor identifies and records the location of where the descriptions of the change (and any further details identified) are given in the change safety case, for each transitional stage.

The assessor may need to create several separate records of location references, for example to address:

a. each transitional stage, when the change is to be implemented in several stages
b. each service, when more than one service is affected
c. different modes of operation, where the safety of each is justified separately.

When understanding the change, the assessor should be careful not to make assumptions because of familiarity with the type of change and application, as the assessor may be unaware of an unusual property of the services or environment.

The assessor should:

a. establish which functional system and service is being changed
b. establish the potential accidents associated with the service(s), and the accident sequences that could lead to those accidents
c. establish an appreciation of the relationship between the change and the safety of the service, including the impacted accident sequences
d. establish the cause(s) of the change to the service, whether:
    i. the change is in response to a change in the operational environment
    ii. the Service Provider wishes to change one or more of its services
    iii. the Service Provider wishes to change one or more part of the functional system used to provide the service(s)

e. establish an understanding of any change in the operational environment, e.g. changes to the behaviour or characteristics of the consumers of the service, or physical environment

f. establish an understanding of any change to the services to be provided

g. establish an understanding of the change described in the change safety case, in terms of the changed and impacted parts of the functional system, and how its behaviour will change

h. establish an understanding of the change to be made at each transitional stage, if the change is to be implemented in more than one transitional stage

i. decide whether it is acceptable to assess a change safety case for only part of the change, if the change safety case does not address all transitional stages required to complete the change

j. determine whether the change safety case identifies other concurrent changes that potentially have an impact, or require coordination. Such concurrent changes should be noted for use when planning assessment activities, to ensure that the change safety case accounts for any consequences of these concurrent changes

The assessor records any concerns noted during this Phase. Such concerns could relate to the scope and nature of the change, but also may include any perceived risk, query or open issue

Phase 1 Step 3 Confirm the declared scope of the change is credible

Introduction

The purpose of this step is for the assessor to develop an understanding of the declared scope of the change, and confirm that this appears to be correct. This understanding needs to be gained for the change in its totality and for each transitional stage.

The sources for this understanding are the descriptions of the change, the scope of the change declared and its justification (these are formally assessed in later phases). When the change is implemented using transitional stages, then the scope of the change must be understood for each transitional stage, and must be consistent with the scope of the complete change.

Conduct

Understand the described change

The assessor examines the descriptions of the changes made for each transitional stage, seeking to understand:

a. the situation before the change is implemented at the start of the transitional stage, in terms of
    i. the environment of operation
    ii. the services provided in this environment
    iii. any interactions between the services
    iv. the functional systems providing these services
    v. the interactions between functional systems
    vi. the POSSs that make up the functional systems
    vii. the interactions between the POSSs
    viii. the external interfaces, resources and services used
    ix. the organisational responsibilities
b. the change that is implemented at the start of the transitional stage, in terms of:
    i. a description of the change implemented for this transitional stage
    ii. the modifications to be made to the functional system and any change effected collaboratively in the service environment
    iii. the impacts of these changes

If the descriptions of the change are insufficient to understand the points above, the assessor should consult the formal change declarations provided in the change safety case (these are assessed in Phase 5 Step 3, page 73) to try to gain this understanding.

Having gained an understanding of the functional system, the assessor then considers whether the descriptions of the change suggest that the change safety

case has failed to address some changed or impacted parts of the functional system. This possibility should be considered for each transitional stage, and the overall change.

If there is a clear problem with the scope(s) of the change(s) addressed in the change safety case that cannot be resolved by discussion with the Service Provider, the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Augment Records

The assessor then augments the records made in Phase 1 Step 2, with more details of the locations of the following, for each transitional stage:

a. the situation before the change is implemented at the start of the transitional stage

b. the description of the change, and its impacts, implemented at the start of the transitional stage

c. the statement that lists the changed and impacted parts of the functional system, and the references to their specifications

d. the justification that the identified changed and impacted parts were correctly identified

e. the impact analyses that support the justification.

Check scope of change includes anticipated parts of the operational and support systems

The assessor then conducts a coarse-grained check to determine whether the defined scope of the change includes POSSs that will be changed and also those that will be changed or impacted as a consequence of the change. To do this, the assessor reviews the lists of changed and impacted POSSs that define the scope of the change for each transitional stage, to check that the lists contain the POSSs anticipated, based on the assessor's understanding of the change. This may also be checked by examining the changed items on the build state for the transitional stage.

The assessor then conducts a further coarse-grained check, that the overall change includes changes to the anticipated POSSs, at the same time considering general consistency with what has been learnt about the individual transitional changes. To do this, the assessor checks that the anticipated POSSs will be changed, by either:

a. aggregating the POSSs listed as changed during each transitional stage

b. comparing the items changed between the build state for before the change and the build state for the last transitional stage.

If necessary, the assessor could obtain further details of the change during each transitional stage from the Installation, Commissioning, Transition and Recovery plans.

Check that the impact analyses appear justified

The assessor checks the justification of the impact analysis for each transitional stage, to decide whether the impact analysis methods appear to have been adequate to identify the impact of the change, and provide sufficient confidence that the statement of the change and its impact is correct. A thorough check of the scope of the change may be carried out in Phase 5 Step 3, which may be consulted as further guidance for this initial familiarisation activity. The change safety case will usually argue the adequacy of the methods used when justifying that the identified changed and impacted POSSs were correctly identified. From this justification, or from examining the analyses if the justification is insufficient, the assessor forms an opinion as to the adequacy of the impact analyses. This is done by considering factors such as whether the impact analyses:

a. were conducted properly
b. addressed each transitional stage
c. used methods that were adequate to identify the impact on connected POSSs and on the Service Provider's services
d. used techniques that were appropriate for the nature and scale of the change (e.g. simulation, modelling, architecture diagrams, task analysis, varieties of failure mode analysis, expert review)
e. included suitable measures to identify impact through shared resources, including cumulative effects
f. were iterative in nature, correctly identifying when one impact led to a further impact
g. addressed all service configurations and modes of operation, including those associated with fallback modes
h. included suitable measures to identify whether changes to the environment of a service are required as a consequence of a change to the service (e.g. a building may need to be demolished to facilitate installation)
i. included suitable measures to identify whether changes to another service are required as a consequence of a change to the service
j. included suitable measures to identify whether there are impacts or consequential changes from the need to address new hazards and changes to existing hazards (e.g. as new mitigations or changes to existing mitigations)[9]

Decide whether the declared scope of change is credible

The assessor considers whether the declared scope of the change for each transitional stage is sufficiently credible to support:

a. the validity of the change safety case

[9] Evidence of the adequacy of these activities may be difficult for the assessor to identify because such impacts would have been identified through the safety analyses, and reflected back into the impact analyses. When the change safety case is submitted, all analyses would be complete and consistent with each other, obscuring the fact that these impacts were identified.

b. the identification of the correct risk(s) associated with the change, so the assessment is modulated correctly.

Completion of Phase 1 Step 3

The assessor checks the records of the locations where the impacts of the change are identified in the change safety case, and adds any clarifying notes or summary necessary to record the assessor's understanding.

The assessor should record any concerns noted during this step. Such concerns should not be limited to the scope of the change, but may also include any perceived risk, query or open issue. The assessor should consider whether any concerns noted during earlier assessment Steps have been resolved.

If the scope of the change (i.e. the change and its impact) is insufficiently credible to support continuing the assessment the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Phase 1 Step 4 Build familiarity with the parts of the change safety case

Introduction

In the previous parts the assessor has built up an understanding of the scope of the change and the effect on the services provided.

The purpose of this Step is for the assessor to build an all-round understanding of the submitted material, identifying any arguments made in the change safety case, and its coverage of the necessary topics. This includes the specific activities and arguments that applicable regulations require.

Assessment of the sufficiency of the arguments and evidence presented for these topics is not addressed in this Phase.

Conduct

The assessor should establish an understanding of the structure of the safety case submission, and of the safety argument. The assessor should record the locations of places where the change safety case describes these structures, for example where the transitional stages are described, or where the argument states that it addresses different parts of the functional system that are within the scope of the change. These descriptions should be augmented with the assessor's own observations from examining the change safety case, and the important structural features should be summarised to support planning of assessment activities.

The assessor should use the tables in 'Appendix B – Change safety case topics' to identify and record the location(s) where the change safety case addresses each of the specified topics, and any associated arguments. The assessor is seeking information about the topics for all of the POSSs and aspects of the service related to the scope of the change identified, but is not assessing adequacy in this Phase.

The assessor should identify significant structural features of the argument, for example where it:

a. partitions a claim according to the architecture of the functional system
b. addresses certain parts of the change collectively e.g. those associated with certain POSSs, a specific contractor, or a mode of operation
c. utilises diverse supportive threads
d. addresses contradicting evidence and rebuttals
e. relies on a single source of evidence to support multiple arguments.

Ideally, the change safety case would describe these major features in an overview or summary of the argument, but the assessor may have to examine the argument directly.

According to the structure of the change safety case submission or the safety arguments, the assessor may need to maintain separate records of location references to address (for example):

a. each transitional stage, when the change is to be implemented in several stages

b. each service, when more than one service is affected

c. different modes of operation, where the change safety case defines safety criteria (which define acceptable safety performance) for more than one mode of operation.

In addition to the generic topics, the assessor should record the location of specific information that may be useful. This may be predefined for certain types of changes.

Completion of Phase 1 Step 4

The assessor should record any concerns noted during this Phase. Such concerns could include any perceived risk, query or open issue.

If there is an apparent serious deficiency in the content of the change safety case that cannot be resolved by discussion with the Service Provider, the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Phase 1 Step 5 Identify applicable standards and regulations

Introduction

The purpose of this step is for the assessor to ensure that the assessment will address the change's implementation of all applicable standards and regulations.

Conduct

The assessor considers the total extent of the changes and their impact, and determines whether there are applicable regulations, acceptable means of compliance or standards with which the change process or the changed functional system must comply.

Change safety cases should identify mandatory standards and regulations, and any others that the service provider commits to comply with. These constrain the change that may be made and how it is made. The assessor should consider whether the list of mandatory standards and regulations seems complete.

The assessor should identify whether any assessment activities are required to determine compliance with these regulations and standards, and if so, the assessor should instigate the relevant regulatory processes to assess this compliance. Such activities are not considered within the scope of this guidance, although planning guidance in Phase 5 reminds the planner to include such activities if necessary.

The assessor should consider whether the parts of the change safety case so far assessed suggest that applicable regulations or standards have not been or will not be complied with, and discuss this with the Service Provider if necessary. Where standards are not complied with, this introduces a risk that rectifying the non-compliance will mean that the proposed change will not be made as specified in the change safety case.

The assessor also checks that the change safety case complies with any regulations that stipulate the mandatory contents of a change safety case. The indices prepared in Phase 1 Step 4 may assist with this check.

Phase 1 Step 6 Consider plans for Installation, Commissioning, Transitioning and Recovery

Introduction

The purpose of this Step is for the assessor to gain familiarity with the plans for implementing the changes, and determine whether they appear adequate and feasible.

Conduct

The assessor identifies from the change safety case material submitted, how the Service Provider plans to install and commission the change, including a description of each transition that will take place, and the arrangements for recovery if transition is unsuccessful. Complex changes may require separate plan documents for installation, commissioning, transitioning and recovery, but in simpler cases this may be a single transition plan or even just a short statement. Transition plans must address each activity to implement the changes, whether or not the changes will be implemented while providing an operational service. The assessor should make a record that summarises the structure of the plans, for future reference.

As the assessor carries out this Step, a record should be made of any transitional activity that appears to have a potentially significant safety impact on the provided service(s). This list can be used in Phase 1 Step 7 to check the adequacy of the associated safety analysis.

The assessor decides whether the plans seem adequate in that they:

a. are compatible with the assessor's understanding of the transitions
b. are consistent with the assessor's understanding of the scope of the change
c. are commensurate with the extent and complexity of the activities planned
d. are sufficiently detailed to understand and confirm their correctness in later assessment Phases
e. define a contiguous set of changes from the pre-change functional system/service to the final, completely changed functional system/ service
f. describe a set of activities that appear to change all necessary parts of the functional system to implement the complete change
g. include coordination activities to notify parties impacted by the change or who are required to make coordinated changes to properly implement the change.

The assessor also determines whether the transition plans appear feasible. If the plans are not feasible, any further assessment would probably be nugatory as the proposed change could not be made. The assessor achieves this by checking that, for each transitional stage, the transition plan:

a. addresses the identified scope of the change, appearing to implement all necessary changes
b. including all activities, timings and likely availability of resources
c. addresses relevant aspects from those described later in this guide, where the topic tables for Phase 4 are introduced.

Completion of Phase 1 Step 6

The assessor should consider whether the plans for implementing the changes appear adequate and feasible.

If there is an apparent serious deficiency in the content of the change safety case that cannot be resolved by discussion with the Service Provider, the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Phase 1 Step 7 Check scope of safety analyses

Introduction

The purpose of this Step is for the assessor to initially confirm that the safety analysis material in the change safety case appears to address an appropriate part of the functional system, related to the change.

Conduct

The assessor confirms that the information in the change safety case appears suitable for use when planning the rest of the assessment, by checking that the safety analyses appear to be appropriate and address the correct scope of the change.

These safety analyses are those for the services provided during each transitional stage, and also for the transitional activities that implement the changes to the functional system.

The safety analyses (which may use safety modelling techniques) to be examined during this step were identified during Step 4, and address:

a. Setting safety criteria to define acceptable safety performance, either in terms of risk or occurrence rates
b. Decomposing safety requirements from the safety criteria
c. Predicting the safety performance of the functional system during the transitional stage, by composing occurrence rates of lower-level events
d. The safety of the transitional activities

This step only addresses a) and d) of the list above, because they are sufficient to confirm that the safety analyses appear adequately trustworthy to use the information to plan the rest of the assessment.

The assessor must first establish against which baseline system the change safety case defines the scope of the change for each transitional stage, as they may each use different baselines. Service Providers may choose to argue the safety of the service provided by the functional system during each transitional stage in terms of the difference in safety performance compared with that during the previous transitional stage or that provided by the original pre-change functional system, or a combination of these approaches. (However, if it is necessary for there to be a temporary reduction in safety performance during a specific transitional stage, this needs a suitable justified, perhaps on the basis of as low risk and as short a duration as reasonably practicable.)

Having established the baseline system used for each transitional stage, the assessor then conducts a preliminary examination of the safety analyses to determine whether they are sufficiently correct to drive the risk-based activities in later Phases of the assessment. The assessor achieves this by checking that, for each transitional stage:

a. the safety analyses for the operational service during the transitional stage:
    i. address the correct scope of the change defined for the transitional stage
    ii. appear to have derived safety criteria for the parts of the functional system that are within the scope of the change
    iii. appear to have used appropriate techniques to determine the safety risk associated with the change
b. and the safety analyses for the transitional activities associated with the transitional stage:
    i. address all transitional activities
    ii. use valid risk evaluation criteria to determine the acceptability of the safety risks of the transitional activities
    iii. appear to have used appropriate techniques to identify the safety risks of the transitional activities.

If the safety analyses are found to be insufficient in coverage of the scope of the change, or in their approach, and this cannot be resolved by discussion with the Service Provider, the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Establish baseline system for each transitional stage

The assessor determines which functional system state the change safety case identifies as the change baseline for the impact analysis, for each individual transitional stage. If the change safety case does not declare this explicitly, the assessor can terminate the assessment, or else determine the baseline(s) by examining the impact analyses.

The assessor records where the baseline system is defined by the change safety case, for each transitional stage.

Determine whether safety analyses address the correct scope of the change defined for the transitional stage

The assessor then determines whether the safety criteria for the transitional stage appear to address the scope of the change identified by the impact assessment for that transitional stage, by checking that:

a. the impact analysis appears to identify:
    i. all parts of the functional system that are changed at the transitional stage, and
    ii. all parts of the functional system that are impacted by the changes
b. the change and impact was identified with respect to a clearly defined baseline system
c. the safety analyses appear to define safety criteria that address the safety related behaviour of all the parts of the functional system that

are within this scope of change, being the changed and impacted parts.

The assessor records whether the safety analyses define safety criteria that appear to address the scope of the change identified by the impact analysis, for each transitional stage, and records any potential concerns.

Determine whether safety analyses appear to have derived appropriate safety criteria

The assessor determines whether the safety criteria, which specify acceptable safety performance for the change for a specific transitional stage, are appropriately specified.

The assessor determines whether the safety criteria appear to address all safety-related behaviours (or properties) of the parts of the functional system that are within the scope of the change. The safety criteria must either specify:

a. acceptable risk for the functional system/service within scope of the change, or

b. acceptable rates for each potential trajectory, which progresses through the scope of the change, to an accident.

The assessor determines whether the safety criteria appear to have been derived in accordance with the Service Provider's SMS.

Where previous safety performance has not been used to define safety criteria (e.g. for a new functional system or a change to an existing functional system whose safety performance has not been adequately established):

a. the assessor determines whether the safety criteria for the change appear to have been established in accordance with the applicable risk criteria, in accordance with the Service Provider's SMS.

Where the safety criteria are derived from the safety performance of an earlier baseline system/service[10]:

a. the assessor determines whether the earlier baseline system used to establish safety performance is the same baseline system used for the impact analysis

b. the assessor determines whether the safety performance specified by the safety criteria results in the same or better risk than the baseline system/service. An acceptable justification (normally agreed with the CA before submitting the change safety case) must be present if the safety criteria specify reduced safety performance.

c. the assessor determines whether the baseline system was one with increased risk, by prior agreement with the CA. This is unlikely to be acceptable, but if so, the assessor must check that the safety performance of the functional system during this transitional stage is

[10] This is written as if the baseline functional system existed in the past, which it is from the point of view of the transitional stage 'using' it, but as the change safety case is submitted before the first transitional stage, the baseline functional system is probably not yet realised.

not used to define safety criteria in any subsequent stage without a justification (it seems unlikely that this will be done).

d. the assessor should consider whether the baseline system was unsuitable to provide a baseline definition of safety performance, for example:

    i. an incompletely assured change was included in the functional system (by agreement with the CA following acceptance of the justification of the necessity of this)

    ii. the baseline system/service was not operational for a sufficient period of time

    iii. the utilisation of the functional system/service during the baseline stage was insufficient

    iv. the operation did not demonstrate the efficacy of the safety functions of the functional system relevant to the scope of the change.

The assessor must establish that such baselines are suitable before proceeding with the assessment, or else terminate the assessment.

Determine whether safety analyses appear to have used appropriate techniques to determine the safety risk associated with the change

The assessor determines whether the safety analyses appear to have used techniques that were selected in accordance with the procedures in the Service Provider's SMS.

The assessor judges whether the safety analysis techniques used are as expected for the type of change, and have produced the types of records expected.

Initially assess whether safety analyses address all transitional activities

The assessor performs an initial assessment of whether all transitional activities have been subject to safety analysis by:

a. determining whether the transition plans for each transitional stage appear to specify all required transitional activities

b. determining whether the safety analyses of the transitional activities appear to address each transitional stage, and all specified transitional activities.

The assessor checks that the analyses appear to address the transitional activities on the list produced in Phase 1 Step 6, being those that appeared to have a potentially significant safety impact on the provided service(s).

The assessor checks that the transitional activities analysed include those associated with recovery actions, should the change be unsuccessfully completed. However, it would be normal for these recovery activities to be less rigorously treated than the analysis of the 'forward' activities of installation, commissioning and other transitional activities. However, in critical applications, the safety of intended recovery activities should be analysed in the same manner as 'forward' transitional activities.

Determine whether safety analyses use valid risk evaluation criteria to determine the acceptability of the safety risks of the transitional activities

The assessor must determine whether the acceptability of the risks from transitional activities appears to have been properly evaluated.

In some cases, additional safety analysis may address the safety of the personnel undertaking the transition activities, but this is outside the scope of this Guide.

The assessor first determines the approach used to determine the acceptability of the risks associated with the potential effects of the transitional activities, and potential deviations from them, on operational services. For each transitional stage, acceptability is determined either:

a. by considering the potential effects as (negative) contributors to the safety of the services provided during the transitional stage, integrating the contribution of transitional activities with other causes of service hazards in their safety analyses.

b. by showing that the potential effects have been evaluated and, if necessary, mitigated so that the risk from them is acceptable (perhaps negligible or ALARP)

In the former case, the assessor checks that the potential contribution of transitional activities appears to have been identified and integrated into the prediction of safety performance for the functional system/service during the transitional stage.

In the latter case, the assessor checks what the change safety case states about the way that risk acceptability was determined. The change safety case may use criteria provided by the Service Provider's SMS or applicable regulations, or else state the criteria or method used, providing the rationale.

The assessor determines whether the acceptability of the risks associated with transitional activities appear to have been evaluated in accordance with the Service Provider's SMS, if applicable.

The assessor must form an opinion on the apparent validity of the criteria or method used to determine the acceptability of the risk. The assessor may consider:

a. the level of threat to the service being changed, and the potential consequences of effects on that service

b. the level of threat to other services, and the potential consequences of effects on those services

c. the 'one time' nature of the risk from transitional activities, as opposed to the continuous risk from hazards throughout the operational period

d. the inclusion of appropriate mitigations to prevent errors being made in, and deviations from, the transitional activities and to ensure successful completion of the intended change.

e. the absence of unnecessary risk

f. the absence of better alternatives or further mitigations (ALARP)

g. whether there is an overall risk budget for all transitional activities.

The assessor should also take into account the reliance on expert judgement, and the competence of the people that performed the analyses.

The assessor should examine a small sample of the analyses to determine whether the risk acceptability criteria appear to have been appropriately used, and appear to have resulted in the right judgements.

The assessor makes records of the approach used in the change safety case for each transitional stage, to inform assessment planning during Phase 5 Step 6.

Determine whether safety analyses appear to have used appropriate techniques to identify the safety risks of the transitional activities

The assessor determines whether the safety analyses of the transitional activities appear to have been carried out appropriately, to:

a. identify the potential impact of credible deviations from the planned transitional activities and from the expected outcome of the transitional activities (usually additional effects)

b. determine that sufficient mitigations are available or else have been added to the arrangements for the planned activities.

To do this, the assessor checks whether it appears that the safety analyses of the transitional activities:

a. have been conducted systematically, referencing transition plans, schematics, etc

b. considered an appropriately wide set of potential deviations from the planned transitional activities

c. considered deviations from the planned coordination and communication arrangements

d. considered an appropriately wide set of potential deviations from the expected outcome of the transitional activities (usually additional effects)

e. considered the influence of the environment of the transitional activity when identifying potential deviations

f. considered whether the deviations threaten both the service being changed, and any other services (e.g. those collocated or sharing resources)

g. considered potential impacts on both the service being changed and the other services

h. considered potential impacts on the various possible modes of operation of the service being changed and the other services

i. considered potential impacts transferring through the environment where the transitional activity will be conducted (including heat, smoke, etc)

j. considered potential impacts arising from the use of shared resources

k. took account of the possibility that the service being changed may not have the normal full range of operational or fallback modes of operation available during the transitional stage

l. identified the types of impacts that might be expected from the activities planned

m. identified credible mitigations

n. included the types of mitigations that might be expected for the activities planned

o. have been undertaken by competent people

p. were completed fully.

Completion of Phase 1 Step 7

The assessor decides whether the safety analyses examined in this step appear adequately trustworthy to use the information they provide, during later assessment Phases, to govern the rigour and emphasis of the assessment activities.

The assessor records any useful information for the later Phases that examine these safety analyses in more detail. This includes a summary of the structure of the safety analyses and documents.

If there is an apparent serious deficiency in the content of the change safety case that cannot be resolved by discussion with the Service Provider, the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Phase 1 Step 8 Decide whether the change safety case is suitable for assessment

Introduction

The purpose of this Step is to decide whether the assessment should continue, or otherwise sentence the safety case as unsuitable for assessment.

Conduct

The assessor should review the records and findings recorded, to determine whether the change safety case is suitable for assessment, or else terminate the assessment by proceeding directly to Phase 6.

The assessment should be terminated if:

a. it is apparent that the change safety case was not properly prepared

b. there are significant errors or omissions

c. the scope of the change (i.e. the change and its impact) is not properly identified or incorrectly established

d. mandatory topics have not been addressed

e. plans for installation, commissioning, transition and recovery do not provide sufficient detail, or appear infeasible

f. the safety analyses appear inadequate in coverage of the scope of the change or approach.

The assessor should review the records of this Phase and ensure that they are complete before continuing to the next Phase, or terminating the assessment.

Phase 2 Determine risks that govern the assessment

Introduction

There is not currently a method for identifying how to modulate the assessment according to the relevant risks. Therefore Phase 2 utilises the risk factors that cause these risks to provide an interim approach to modulation. These risk factors include the safety risk(s) associated with the change.

Some of the information required to identify the risk factors may not be available or fully understood the first time that this Phase is executed, so the overall assessment process allows for the modulation to be revised as further information is discovered during the assessment activities of subsequent phases.

There are several aspects of the modulation process (which involves identifying risk factors, deriving risks, and then using these to identify which assessment activities will be undertaken) that are not properly understood. These include:

a. how to identify a risk (an adverse outcome graded by its severity and probability) from each risk factor or from the aggregation of the risk factors

b. how to define which risks and risk factors are relevant to the objectives of the review

c. how to simultaneously use each of the risks, which may have different natures, in the modulation process

d. how to define a review modulation index from a risk

e. how to use a modulation index to fully define the necessary assessment activities (see Specifying assessment activities on page 29)

Consequently, at this version of the Guide, the activities of this Phase are restricted to evaluating the risk factors that are relevant for the various stages of the assessment process. This means that in later Phases, when the planner defines the assessment activities, instead of being informed by a modulation index, the planner uses expert judgement to define assessment activities according to the information in the risk factors.

Conduct

Establish objective of review

The assessor should consider the objective of the review (e.g. to validate the safety argument), so that only the relevant risk factors are subsequently

considered. This may be defined in applicable legislation or regulations, or else be defined in the governing review procedure.

Identify risk factors

The assessor identifies the relevant risk factors, considering the objective of the review, for the overall change and for each transitional stage.

The assessor reviews the information and notes collected in Phase 1 to identify risk factors that could be the source of risks for the proposed change. The definition of risk factors (in Definitions and Terminology on page 13) can be used to help in this process. To complement this 'bottom up' approach, a 'top down' approach can be used, by considering whether there are risk factors that could threaten the creation of the fundamental safety arguments in 'Technical basis of guidance' on page 10.

The assessor ensures that Phase 1 records show the location of the safety criteria and the safety analyses of the transitional activities for each transitional stage, to support analysis of the risk factors associated with safety risks. If these cannot be located, the assessor must consider whether an appropriate assessment rigour can be determined in the absence of this information.

If an earlier version of the change safety case was previously assessed, the assessor should augment the list of risk factors with the deficiencies found in the previous assessment.

Analyse risk factors defining rigour of assessment

The assessor needs to consider a combination of information to define the required rigour for the assessment, for four different parts of the assessment:

a. The rigour of assessment of the safety of the service provided during each individual transitional stage (Phase 5 Steps 2 to 5) is defined using:
    i. the material in the change safety case that defines the safety criteria (the main driver for the required rigour, but modified by the following considerations)
    ii. the information about the change that caused the change to be selected for review
    iii. the descriptions provided in the change safety case
    iv. the material in the change safety case that defines the scope of the change
    v. the assessor's understanding of the credible system-level outcomes (accidents) of unsafe behaviour within the scope of the change
    vi. the assessor's belief in the correctness of the derivation of the safety criteria
    vii. the assessor's belief in the correctness of the safety criteria, considering the provided service(s) and the relationship of the scope of the change to the other parts of functional system
    viii. the safety models in the change safety case.

ix. the assessor's belief in the ease of achievement of the safety criteria, considering the technologies and novelty of the changed POSSs (if complex architecture and mitigations are required to satisfy the safety criteria then this would require more rigorous assessment)

x. the assessor's belief in the ease (and availability) of assurance of the achievement of the safety criteria considering the technologies and novelty of the changed POSSs, and whether assurance is available from suppliers

b. The rigour of assessment of the safety of the transitional activities during each individual transitional stage (Phase 5 Step 6) is defined using:

i. the descriptions provided in the change safety case

ii. the service(s) that may be affected by the transitional activities

iii. the defined transitional activities

iv. the information (arguments, analyses) provided to demonstrate the safety of the transitional activities

c. The rigour of assessment of the feasibility of the transitional activities during each individual transitional stage (Phase 4) is defined using:

i. the descriptions provided in the change safety case

ii. the provided service(s) during the transitional stage, which may affect access to undertake the transitional activities

iii. the defined transitional activities

iv. the information (arguments, analyses) provided to demonstrate that resources, tools etc will be available

d. The rigour of assessment of all other aspects, which are not specific to a specific transitional stage (Phase 3) is defined by considering the highest rigour defined for a transitional stage for item a, above.

The assessor needs to define the rigour required regarding items a, b and c above for each transitional stage.

The assessor identifies the required rigour that is used when subsequently undertaking planning activities, using relevant information from the risk factors identified above. This could be in the form of:

a. summary statements of the relevant information

b. a review level scheme

c. one or more numeric modulation indices.

At this point, this guidance has reached the limit of what is understood about modulating the assessment. To use approaches b and c (above), a scheme would need to be defined by the CA that the planners and assessors can work with.

Given that it is not currently known how to properly define levels of rigour of assessment, approach a (above) could be used initially, in conjunction with a

modified form of approach b (above), where levels of assessment rigour might be defined using a scheme such as:

a. level 0 could denote that the assessment inherent in the conduct of Phase 1 is judged to be sufficient

b. level 1 could denote that (in addition to level 0) the assessment should be conducted according to pre-existing practice, even if this means that only selected parts of the change safety case are given a general review (without reference to the candidate assessment activities). This omits Phases 3 to 5 of the assessment processes in this Guide.

c. level 2 could reflect level 1, but involves assessing all parts of the change safety case, as identified in this Guide, with the rigour applied in pre-existing practice (without reference to the candidate assessment activities).

d. level 3 could denote that the planner should attempt to properly plan the assessment using the candidate assessment activities in this Guide, and defining the rigour of the assessment in accordance with the risk factor information.

It should be recognised that this would be an interim scheme that does not properly define assessment rigour levels, but permits experience in the assessment process to be built up to subsequently define a better scheme.

Analyse risk factors defining foci of assessment

The assessor identifies risk factors that potentially threaten the production of an acceptable change safety case, in order to identify the foci of the assessment. This is in addition to the modulation of the rigour of the assessment, which is based on those risk factors relating to safety risk. The foci are defined when the assessment identifies risk factors that introduce a risk that:

a. the change made may not be as defined in the change safety case, or

b. the claims made may not be demonstrated with sufficient confidence due to inadequacies in the inferences or evidence

For example, although the risk factors in the previous step (assessment rigour) lead to a requirement that six specifications should be examined, the risk factors in this step may indicate that certain parts of the system are more likely to be poorly assured, and so the sample of specifications examined should be biased towards these. The foci are not necessarily specific parts of the functional system, but are identified according to the impact of the causal risk factor.

The assessor uses generally the same information as before to determine risk factor information, for the same four parts of the assessment defined in the previous step:

a. the safety of the service provided during each individual transitional stage (Phase 5 Steps 2 to 5)

b. the safety of the transitional activities during each individual transitional stage (Phase 5 Step 6)

c. the feasibility of the transitional activities during each individual transitional stage (Phase 4)

d. all other aspects, which are not specific to a specific transitional stage (Phase 3).

Again, the assessor needs to define the foci required regarding items a, b and c above for each transitional stage.

Some risk factors may influence the assessment of more than one of these four parts, and/or for more than one transitional stage. For example, a certain contractor might be involved in transitional activities for several of the transitional stages, and be thought to be inexperienced (high risk), and so this would bias the assessment activities towards activities and functional system aspects that are related to the contractor.

Whilst this Phase could just pass on the four sets of relevant risk factors to support the planning activities, it would be preferable to consider the nature and level of risk that each risk factor represents. Ideally, this would be undertaken in a tabular format that provides a record of the analysis. The analysis should be based on expert judgement, perhaps incorporating subjective quantification, and identify, for each risk factor:

a. to which of the four modulation categories above the risk factor is related (this can be more than one)

b. the potential impact on one or more of: the elements of the change safety case, the four modulation categories above, and the fundamental safety arguments in 'Technical basis of guidance' on page 10

c. the way it might materialise in the change safety case (how would the impact be recognised)

d. the potential severity of the impact on the change safety case arguments, perhaps as an integer or as High/Medium/Low.

The structure of the overall safety argument, as identified in Phase 1 Step 4, should be considered to understand whether it affects the relevance of the risk factors e.g. the structure may modify the consequences of errors in the arguments or weaknesses in the evidence.

At the end of this Step, the assessor should ensure that the identified risk factor information has been collated for each of the four parts of the assessment, and according to each transitional stage.

Completion of Phase 2

The assessor records the sets of analysed risk factors, for use in subsequent phases. These include the deficiencies found in any previous assessment of the change safety case. All supporting notes and analyses should be retained, as they may be revisited in later phases as further information is revealed by the assessment.

The risk factor information is not strictly 'the risks' that should be used by the planner in subsequent phases and steps to define the planned activities.

Consequently, the planner has to formulate a view of the relevant risks from the identified risk factor information, and use this understanding to drive the planning. This is the best approach currently identified in the light of the difficulties identified at the start of this section (Phase 2).

The risks determined in this Phase may indicate that the assessment inherently conducted during Phases 1 is sufficient as an assessment of the change safety case. If so, the reasons for this judgement are recorded, and the assessment process continues at Phase 6. Otherwise the assessment continues at Phase 3, or at the point from which Phase 2 was revisited.

Subsequent iterations of Phase 2

Phase 2 is revisited when further information has been identified by undertaking assessment activities in subsequent phases. This information may revise and refine understanding of the risk factors and their impact on the change safety case.

If the identified risk factors are found to be significantly different to those previously understood, parts of the assessment already undertaken may need to be repeated with greater rigour or using assessment activities that focus on different risks.

Phase 3 Plan and assess stage independent parts of the change safety case

Introduction

The purpose of this Phase of the assessment is to assess the parts of the change safety case that are not specific to the transitional stages that will be used to implement the change.

The feasibility of the change is not considered here, as it is addressed in Phase 4.

Planning

The assessment planner creates the first version of the assessment plan, which addresses the parts of the change safety case that are independent of the change's transitional stages. The risks identified in Phase 2, and the assessment modulation strategy identifies the parts and amount of the change safety case that will be assessed, and which assessment activities will be undertaken.

The plan is expanded to define further activities in subsequent Phases.

The plan must address the following change safety case topics, which are introductory and independent of the transitional stages:

a. Relationship to SMS
b. Overall claim of acceptability of predicted safety performance
c. Justification of treatment of uncertainties
d. Descriptions of functional system, changes and service during the transitional stages
e. Justification that the proposed change is a good change

The assessment needs to be planned to reflect the risks associated with the project's characteristics, the characteristics of the change and the change safety case. The project characteristics include the technical capability and safety culture of the Service Provider, and any contracting organisations assisting the Service Provider to assure and implement the change.

When preparing the plan, the planner should consider whether the familiarisation Phase and any completed assessment activities have already provided sufficient assessment to meet the objectives of the current Phase of the assessment. Effectively, consideration of the applicable risk factors shows that no additional assessment activities are necessary.

The candidate assessment activities for this Step are in Phase 3 Topic Tables on page 121 (in Appendix D – Candidate assessment activities).

Conduct

The assessor determines whether the change safety case material assessed as part of this Phase is satisfactory when judged using the assessment activities stipulated in the assessment plan, and records any concerns.

Completion of Phase 3

Before moving on to the next Phase, the assessor checks that all the assessment tasks specified in the assessment plan for Phase 3 have been completed, and that adequate records exist to demonstrate this.

The assessor should agree with the planner whether any concerns require further investigation as part of this Phase, or in subsequent Phases. They also consider whether the assessment activities have revealed new information that means that the risks determined in Phase 2 need to be reconsidered, so that additional assessment activities are then planned and conducted.

If there is an apparent serious deficiency in the content of the change safety case that cannot be resolved by discussion with the Service Provider, the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Phase 4 Determine whether the planned change is credible

Introduction

The purpose of this Phase is to determine whether the change(s) can and will be made as planned. If the functional system is unlikely, in actuality, to exist in the states supported by the change safety case, the assessment should be terminated.

This Phase assesses the credibility of the transitional activities, whereas their safety is assessed during Phase 5. This Phase is considered to be optional, as the credibility of the change may be obvious, or already adequately confirmed during earlier assessment Phases.

For each individual transitional stage, the assessment assesses:

a. the feasibility (not safety) of the planned transitional activities that implement the change

b. whether the planned transitional activities are sufficient to implement the stated change

c. whether the prepared parts to be inserted into the functional system will be available

d. whether the necessary resources and tools to undertake the change will be available

e. whether external coordination arrangements, included notifying parties impacted by the change or who are required to make coordinated changes to properly implement the change, appear credible and sufficient

f. whether internal coordination arrangements, included to synchronise or sequence the transitional activities, appear credible and sufficient

g. whether the criteria to support transition decisions are adequate

h. whether the material (evidence and justifications) in the change safety case that shows that the resources and tools required to make the change meet their specifications.

The assessment activities are planned, according to the risks (determined in Phase 2) associated with the transitional activities for the relevant transitional stage.

Additionally, this Phase provides an understanding of the transitional activities that should appear in the safety analyses of the services during each transitional stage, which are assessed in Phase 5.

In some cases, additional safety analysis may be necessary regarding the safety of the personnel undertaking the transition activities, but this is outside the scope of this Guide.

Confirm risks associated with the feasibility of the transitional stages

The assessor reviews the records of assessment Phase 2, where the risks were determined for the feasibility of the activities in the installation, commissioning, transition and recovery plans. The assessor considers whether any other relevant information has been gained during assessment activities conducted since Phase 2, which requires the risk to be revised. The same method as in Phase 2 should be used when revising the risk estimate.

The confirmed or revised risk is used to modulate the planned assessment activities for the feasibility of the installation, commissioning, transition and recovery plans.

Planning

The planner must decide whether to implement this optional assessment phase, which establishes the credibility of the planned transitional activities to implement the change. The planner should consider whether the familiarisation Phase and any completed assessment activities have already provided sufficient assessment to meet the objectives of the current Phase of the assessment. Effectively, consideration of the applicable risk factors shows that no additional assessment activities are necessary.

If the planned activities are judged not to be credible, the assessment can be terminated, thus avoiding nugatory assessment activity to assess the safety of a change that cannot be made as described in the change safety case.

Alternatively, the planner can decide that checks of credibility can be undertaken during Phase 5 Step 6, alongside the assessment of the safety of the transitional activities. This may be more efficient when the credibility of the transitional activities does not seem in doubt.

The planner should take account of the 'Risks associated with credibility of transitional activities' identified in Phase 2.

As part of demonstrating that the change will be made as planned, the change safety case may need to justify that the resources and tools used during transitional activities meet their specifications. This is only necessary when the defined performance is not within normal expectations. A candidate assessment activity is provided below to instruct the assessor to assess this, or else if particularly critical, the planner can stipulate further activities to assess the justification of:

a. the specification (see candidate assessment activities in Justification of the specifications for the POSSs within the scope of the change associated with the transitional stage on page 157), and/or

b. the elements of the specification defining the performance (see candidate assessment activities in Justification of a directly substantiated behavioural element of a specification on page 174)

The assessment planner updates the assessment plan, adding the activities to be undertaken during this Step, including the scope and required rigour of the assessment activities, and addressing the:

a. Installation, Commissioning, Transition and Recovery Plans
b. Evidence and justification that the resources and tools for transitional activities will be as specified.

The candidate assessment activities for this Step are in Phase 4 Topic Tables on page 131 (in Appendix D – Candidate assessment activities).

Conduct

Once the plan is prepared, and competent assessors identified, the assessor(s) conduct the planned activities.

When the planned assessment activities include the assessment of justifications that support the specifications of the resources and tools for transitional activities, the assessor may find that the applicable properties are not well specified (compared with those for the operational system). Also, there may be little justification that the properties of the resources and tools meet their specifications. For many resources and tools for transitional activities or where common practice applies, it may be acceptable for the Service Provider not to provide any evidence or justification at all. When the change safety case does justify the performance of the resources and tools for transitional activities, a lower level of confidence may be necessary than for the operational system, and the assessor's expectations for the evidence and justification may need to be adjusted accordingly.

If the assessor finds that a detailed justification of the performance of resources or tools has been provided and needs to be assessed, the planner should be consulted to define suitable assessment activities to assess the justification of:

a. the specification (see candidate assessment activities in Justification of the specifications for the POSSs within the scope of the change associated with the transitional stage on page 157), and/or
b. the elements of the specification defining the performance (see candidate assessment activities in Justification of a directly substantiated behavioural element of a specification on page 174)

The assessor determines whether the change safety case material assessed as part of this Phase is satisfactory when judged using the assessment activities stipulated in the assessment plan, and records any concerns.

In addition to the normal recording of issues that may require investigation, the assessor should record any notable aspect of the installation, commissioning, transition and acceptance plans that should considered when assessing the safety of the transitional activities in Phase 5. This also applies to aspects that may cause revision of the associated risks for the transitional stages, which is re-assessed in Phase 5 Step 1.

Completion of Phase 4

The knowledge acquired during this Phase will be used to refine the planning of assessment activities in the next Phase. For example:

a. notable aspects of the transitional activities may be considered when assessing the safety of the transitional activities in Phase 5 Step 6

b. the installation, commissioning, transition and recovery plans define any resources and tools required to undertake the planned activities, and the safety of these transitional activities may be assessed in Phase 5, where the specifications and supporting verification for some resources and tools may also be assessed from a safety point of view.

Before the assessor moves on to the next Phase, the assessor should check that all the assessment tasks specified in the assessment plan have been completed, and that adequate records exist to demonstrate this.

The assessor should record any concerns noted during this Phase. The assessor should consider whether any concerns noted during earlier assessment Phases have been resolved.

The assessor should agree with the planner whether any concerns require further investigation as part of this Phase, or in subsequent Phases. They also consider whether the assessment activities have revealed new information that means that the risks determined in Phase 2 need to be reconsidered, so that additional assessment activities are then planned and conducted.

If the proposed change seems incredible, and this cannot be resolved by discussion with the Service Provider, the assessor and planner can agree to terminate the assessment by proceeding directly to Phase 6.

Phase 5 Plan and assess stage dependent parts of the change safety case

Introduction

The purpose of this assessment Phase is to assess the change safety case material for the transitional stages. Each transitional stage is assessed individually, in seven Steps.

For each individual transitional stage:

1. Confirm risks associated with the stage
2. Plan and assess descriptions, declared SMS and claim of safety for the stage
3. Plan and assess the scope of the change
4. Plan and assess specification and safety analysis material (safety criteria, safety requirements and evaluation of acceptability of predicted safety performance)
5. Plan and assess verification material
6. Plan and assess safety of transitional activities
7. Ensure assessment of the stage is adequately completed.

Steps 2 to 5 address related parts of the change safety case (for a specific transitional stage), in a sequence where each provides the subsequent assessment Step with the appropriate emphasis e.g. the best focus when selecting samples.

The assessment of each transitional stage is planned and assessed individually. Given sufficient resources to conduct the assessments, stages could be assessed concurrently, provided that there are no interdependencies.

Notes:

Multiple services. Where multiple services may be affected by the change, the planner must decide whether the assessor will assess each service separately for the stage, or assess more than one service at the same time. The planner must also consider the best order of assessment for the stages and services. These decisions will be driven by factors such as:

- the extent to which the safety argument treats them separately or together, as reflected by the change safety case structure
- whether the risks identified for the services during this stage are the same
- the coupling of the services
- the coupling of the systems
- the commonality of the systems
- similarity of the change safety case material (which could mean either it is a good idea or a bad idea to assess the material together)

- availability of multiple assessors.

Multiple modes of operation. Where the change safety case defines safety criteria (which define acceptable safety performance) for more than one mode of operation, then the planner must decide how these different modes of operation will be assessed, in a similar way as for multiple services. The planner must also consider the best order of assessment for the stages and modes. These decisions will be driven by factors such as:

- whether the risks identified for the modes of operation during this stage are the same
- similarity of the change safety case material (which could mean either it is a good idea or a bad idea to assess the material together)
- availability of multiple assessors.

Should any part of the assessment result in significant new information about the risks associated with the change[11], the assessment should revert to either Step 1 of this Phase, or even Phase 2 of the overall assessment process.

When planning the assessment of the parts of the change safety case for a specific transitional stage, the planner should consider whether an assessment of another transitional stage[12] has already sufficiently (commensurately with risk) covered that part of the change safety case. This may be, for example, because some parts of the case safety case may address more than one of the transitional stages.

[11] e.g. dependencies on previous transitional stages for risk baseline information

[12] The assessment may address the stages in a different order to that used to implement the change.

Phase 5 Step 1 Confirm risks associated with the transitional stages and activities

Introduction

The purpose of this Step is to confirm that the risks to be used to modulate the assessment remain valid for the transitional stages. These risks were first determined in Phase 2, but need to be confirmed in the light of increased understanding of the transitional stages and specifically the transitional stage being assessed and its role in the overall change.

Different risks govern modulation for the assessment of the safety of:

a. the services provided during each transitional stage

b. the transitional activities undertaken during each transitional stage.

Confirm risks associated with the transitional stages

The assessor reviews the records of assessment Phase 2, where the risks were determined for the transitional stage being assessed. The assessor considers whether any other relevant information has been gained during assessment activities conducted since Phase 2 (including any previous iterations of Phase 5), which requires the risks to be revised. Phase 4 in particular may have revealed aspects of the transitional activities that may influence the risk estimates.

The same method as in Phase 2 should be used when revising the risk estimates. Consequently, the planner might identify that the completed assessment activities are sufficient either for a particular transitional stage (or stages), or possibly for all transitional stages in which case the assessment is then terminated by proceeding to Phase 6.

The confirmed or revised risks are used to modulate the planned assessment activities for the transitional stage being assessed.

The first time this Step is conducted, the assessment plan will not have addressed the order in which the transitional stages will be assessed. It would be natural for the stages to be assessed in order, but this is not necessarily so: for example, it may be judged best to first address the final transitional stage, or a transitional stage where a large change is introduced. It would be normal to assess all stages, but the modulation introduced by the risks associated with a particular stage may minimise the assessment activities.

On subsequent iterations of this Step, further information will have been revealed about the change and the change safety case, and it is this information that may cause these associated risks to be revised, and possibly change the order in which the stages are assessed.

Completion of Phase 5 Step 1

If the risks determined for the transitional stages are revised, the assessor updates the records. Otherwise, the assessor records that the risks have been confirmed.

The assessment continues at Step 2 for a single transitional stage, until all stages have been assessed. The stages can be assessed concurrently if multiple assessors are available.

Phase 5 Step 2 Plan and assess descriptions, declared SMS and claim of safety for the stage

Introduction

The purpose of this Step is to address material that should be present in the change safety case for each transitional stage, assessing:

a. Service, operational system and change descriptions (and their justification)

b. Support system descriptions (and their justification)

c. The correct relationship of the change safety case to Service Provider's SMS

d. Claim of acceptability of predicted safety performance for the stage.

Planning

The planner uses the risk(s) (from Phase 5 Step 1) associated with the stage being assessed, and develops a plan for assessing the change safety case elements for which candidate assessment activities are given in this Step.

The assessment needs to be planned to reflect the risks associated with the project's characteristics, the characteristics of the change and the change safety case. The project characteristics include the technical capability and safety culture of the Service Provider, and any contracting organisations assisting the Service Provider to assure and implement the change.

When preparing the plan, the planner should consider whether the familiarisation Phase and any completed assessment activities have already provided sufficient assessment to meet the objectives of the current part of the assessment. Effectively, consideration of the applicable risk factors shows that no additional assessment activities are necessary.

The assessment planner updates the assessment plan, adding the activities to be undertaken during this Step, including the scope and required rigour of the assessment activities, and addressing the:

a. Service, operational system and change descriptions (and their justification)

b. Support system descriptions (and their justification)

c. Correct relationship of the change safety case to Service Provider's SMS

d. Claim of acceptability of predicted safety performance for the stage.

The planner should consider whether, at Phase 1 Step 5 Identify applicable standards and regulations, it was determined that certain aspects of compliance with regulations should be examined during assessment of the material associated with the stage being assessed. If so, the planner adds relevant activities into the assessment plan.

The candidate assessment activities for this Step are in Phase 5 Step 2 Topic Tables on page 136 (in Appendix D – Candidate assessment activities).

Additionally, where the planner considers it necessary to assess the justifications for the descriptions, candidate assessment activities can be used from the Justification of descriptions table (table 4 on page 124 in Appendix D – Candidate assessment activities).

Conduct

Once the plan is prepared, and competent assessors identified, the assessor(s) conduct the planned activities.

The assessor should review the description of the basis on which the safety criteria were set for this transitional stage. This allows the assessor to understand and take an initial view on the validity of this approach, and to establish whether it depends on establishing the safety performance in a previous transitional stage. This also sets the context for understanding the role of the Service Provider's SMS risk tolerability and classification scheme in this approach.

When reviewing the descriptions of the functional system and service, the assessor should consider whether there are any limitations on their use during any transitional stage that may affect the transitional stage's suitability for use as a baseline for setting safety criteria for later transitional stages. For example, the descriptions should highlight if the transitional stage:

a. will include an incompletely assured change
b. will be operated only for a short period of time
c. the utilisation of the baseline system/service will be low
d. the operation will not, for some reason, demonstrate the efficacy of the safety functions.

If it is planned that the functional system during a transitional stage will be a pre-existing fallback mode of operation (of the pre-change functional system), and no further assurance is presented, the assessor should consider whether the assurance previously established, which was suitable for short-term use as a fall-back under (hopefully rare) failure conditions is sufficient for use for the duration of the transitional stage.

If the descriptions state (or the assessor otherwise finds this is the case) that it is planned to introduce greater safety risk for some reason at this transitional stage, by prior agreement with the CA, the assessor checks that:

a. there is an adequate justification of why this is necessary
b. there is an adequate justification that this condition is rectified as soon as possible (i.e. the change is reversed)
c. the plans for subsequent transitional stages (and possibly also the configuration states) include the measures to restore operation of the functional system to the prior level of risk as soon as possible
d. the safety performance of the functional system during this transitional stage is not used to define safety criteria in any subsequent stage without a justification (it seems unlikely that this will be done).

If the descriptions state (or the assessor otherwise finds this is the case) that it is planned to introduce an incompletely assured change at this transitional stage, the assessor checks that:

a. there is an adequate justification of why this is necessary
b. there is an adequate justification that this condition is rectified as soon as possible (i.e. the change is reversed)
c. the plans for subsequent transitional stages (and possibly also the configuration states) include the removal of the incompletely assured change as soon as possible
d. the safety performance of the functional system during this transitional stage is not used to define safety criteria in any subsequent stage without a justification (it seems unlikely that this will be done).

The assessor determines whether the change safety case material assessed as part of this Step is satisfactory when judged using the assessment activities stipulated in the assessment plan, and records any concerns.

Completion of Phase 5 Step 2

Having conducted the assessment activities, the assessor considers whether it has become apparent that other regulations are applicable. The assessor discusses this with the assessment planner and they decide whether it is necessary for the assessor to determine compliance. Cases where it is not necessary to check compliance may be:

a. when checks of compliance have already been undertaken in Phase 3, or for other transitional stages
b. compliance with those regulations is outside the scope of regulatory responsibility
c. compliance with those regulations is outside the scope of the change safety case
d. compliance with those regulations is outside the scope of the change safety case assessment task.

Before moving on to the next Step, the assessor checks that all the assessment tasks specified in the assessment plan for the Step have been completed, and that adequate records exist to demonstrate this. The assessor should agree with the planner whether any concerns require further investigation as part of this Step, or in subsequent Steps.

If there is an apparent serious deficiency in the content of the change safety case that cannot be resolved by discussion with the Service Provider, the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Phase 5 Step 3 Plan and assess the scope of the change

Introduction

The purpose of this Step is to assess the material presented in the change safety case that identifies the change and its scope.

This part of the assessment checks that the change safety case defines the scope of the change, in terms of the POSSs[13] that are changed or impacted, from a declared baseline.

Planning

The assessment needs to be planned to reflect the risks associated with the project's characteristics, the characteristics of the change and the change safety case. The project characteristics include the technical capability and safety culture of the Service Provider, and any contracting organisations assisting the Service Provider to assure and implement the change.

The planner uses the risk(s) (from Phase 5 Step 1) associated with the transitional stage being assessed, and knowledge gained when conducting the Step 2 assessment activities, and develops a plan for assessing the change safety case elements for which candidate assessment activities are given in this Step.

This part of the assessment must check that the change safety case defines the scope of the change for which specifications needed to be subjected to safety analysis and verified. This scope of the change is defined by the POSSs that are changed and impacted, both in terms of the bottom-most POSSs and the parent POSSs whose specifications are changed or impacted. Later assessment steps examine the adequacy of the specifications of these POSSs (Phase 5 Step 4) and the arguments and evidence that the specifications are satisfied (Phase 5 Step 5).

Identifying the limits of the scope of the change depends on correct determination that changed interfaces and resources have no further impact, which in turn depends on correct understanding of the connected parts of the baseline system, and their behaviour (specifications). This understanding should primarily be in the specifications of the baseline system, but can in some cases be enhanced by the knowledge of its developers/maintainers. The planner should define assessment activities for the 'Lists of changed and impacted Parts of the Operational and Support Systems (POSSs)' (page 141), and the 'Justification of lists of changed and impacted POSSs' (page 142).

The planner would not normally stipulate any assessment activities to examine the impact analysis records, leaving it to the assessor to do this if greater confidence is required (see 'Conduct' below).

When preparing the plan, the planner should consider whether the familiarisation Phase and any completed assessment activities have already provided sufficient

[13] Recall that the definition of a POSS in Definitions and Terminology (page 15) states that parent POSSs are only considered to be changed if at least one of their (immediate) child POSSs has changed behaviour (which includes new and removed child POSSs).

assessment to meet the objectives of the current part of the assessment. Effectively, consideration of the applicable risk factors shows that no additional assessment activities are necessary.

The planner updates the assessment plan, adding the activities to be undertaken during this Step, including the scope and required rigour of the assessment activities, and addressing the:

a. Declaration of the scope of the change.

The candidate assessment activities for this Step are in Phase 5 Step 3 Topic Tables on page 141 (in Appendix D – Candidate assessment activities).

Conduct

Once the plan is prepared, and competent assessors identified, the assessor(s) conduct the planned activities.

The assessor then assesses the scope of the change established in the change safety case, in accordance with the assessment plan, keeping in mind the baseline.

When checking the correctness of the change and impact identified in the change safety case, the assessor should determine that these are defined from the correct baseline.

The assessor should determine whether the material examined gives sufficient confidence in the declared scope of the change. If necessary, the assessor can seek further assurance regarding:

a. the impact analyses, using the candidate assessment activities in 'Impact analysis records' (page 143) below to assess the records of the analyses.
b. the specifications of the baseline POSSs, using relevant assessment activities:
    i. suggested by the candidate assessment activities in 'Impact analysis records' (page 143), to determine whether the specifications of the baseline POSSs contain sufficient information to support the impact analyses
    ii. from 'Specifications of architectures' (page 151) and/or 'Specifications of parts of the operational system' (page 152) to assess whether the specifications of the baseline POSSs are adequate as specifications
    iii. from, if such justifications are made, 'Justification of the specifications for the POSSs within the scope of the change associated with the transitional stage' (page 157) to determine whether the specifications of the baseline POSSs appear sufficiently trustworthy.

The assessor determines whether the change safety case material assessed as part of this Step is satisfactory when judged using the assessment activities stipulated in the assessment plan, and records any concerns.

Completion of Phase 5 Step 3

Having conducted the assessment activities, the assessor considers whether it has become apparent that other regulations are applicable. The assessor discusses this with the assessment planner and they decide whether it is necessary for the assessor to determine compliance. Cases where it is not necessary to check compliance may be:

a. when checks of compliance have already been undertaken in Phase 3, or for other transitional stages

b. compliance with those regulations is outside the scope of regulatory responsibility

c. compliance with those regulations is outside the scope of the change safety case

d. compliance with those regulations is outside the scope of the change safety case assessment task.

The assessor should consider whether the examined material violates any of the provisions in Table 56, 'Argument' on page 189.

Before moving on to the next Step, the assessor checks that all the assessment tasks specified in the assessment plan for the Step have been completed, and that adequate records exist to demonstrate this.

The assessor should agree with the planner whether any concerns require further investigation as part of this Step, or in subsequent Steps.

If there is an apparent serious deficiency in the content of the change safety case that cannot be resolved by discussion with the Service Provider, the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Phase 5 Step 4 Plan and assess specification and safety analysis material

Introduction

The purpose of this Step is to assess the:

a. Specifications of the changed functional system/service
b. Safety criteria for acceptable safety performance
c. Evaluation of acceptability of predicted performance
d. Safety requirements.

It is not necessary to examine the adequacy of the specifications of the baseline POSSs in this Step because they represent the historic system, and the specification checks made in this Step are quite general. However, the planner may elect to assess the justifications of specific elements of the baseline specifications in the next Step, where judged necessary in the context of the safety argument.

Planning

The planner uses the risks (from Phase 5 Step 1) associated with the transitional stage being assessed, and knowledge gained when conducting previous assessment activities, and develops a plan for assessing the change safety case elements for which candidate assessment activities are given in this Step.

When preparing the plan, the planner should consider whether the familiarisation Phase and any completed assessment activities have already provided sufficient assessment to meet the objectives of the current part of the assessment. Effectively, consideration of the applicable risk factors shows that no additional assessment activities are necessary.

The planner must plan assessment activities to assess:

a. the specification of the transitional stage
b. the specification sets
c. the service and operational environment
d. the specifications for the parts of the functional system that are within the scope of the change
e. justification of specifications for the POSSs within the scope of the change
f. justification of additional specifications to support safety analysis
g. the safety criteria for acceptable safety performance
h. the evaluation of acceptability of predicted performance
i. the safety requirements.

The planner should only stipulate assessment activities for specifications that the change safety case needs to assure the scope of the change for the transitional

stage. Smaller change scopes may not include top-level specifications (the environment of the service, the service, the functional system environment and the operational system), and perhaps external services, supply of resources and support systems.

Safety analyses will have been used to derive safety criteria, derive safety requirements and predict the safety performance of the change. These safety analyses should have used appropriate techniques, including the creation and use of safety models. It is not possible to generalise which elements of causal and consequence modelling were required, but some indication of what has been used in this change safety case will be available from Phase 1 and any previously conducted iterations of Phase 5. The planner should therefore stipulate whatever assessment activities seem appropriate for assessment of the safety model elements (using the candidate assessment activities in Appendix F – Candidate assessment activities for safety analysis models, page 191), but expect that the assessor may revert to the planner to agree this in more detail as the assessment progresses.

The most natural sampling strategy for identifying which specifications etc are to be examined is to focus the review on the accident chains that are of most interest (e.g. due to perceived risk or uncertainty, or previous experience). However, this approach could be supplemented or replaced by other sampling strategies, including:

a. random sampling
b. based on specific attributes
c. determining the sample by some relationship to
    i. the risk factors
    ii. specific constituent parts according to risk or supplier
    iii. involvement in some other threads
    iv. expert judgement based on understanding of the issues raised in previous phases of the assessment.

Where the change must implement behaviour that is specified by mandatory standards or regulations, or where the change safety case otherwise claims compliance with such a standard or regulation, the planner may elect to plan some assessment activities to address that behaviour in the POSS specifications or the justification of the specifications.

The change safety case should declare the set of specifications for the scope of the change (this is one of the candidate subjects for assessment), so the specifications to be assessed need to be selected from this set.

When defining the sample to be assessed (or sampling strategy) during each assessment activity, the planner needs to take account of hierarchical relationships for the specifications (for the parts of the functional system that are within the scope of the change) and safety requirements, i.e.:

a. The specifications that identify the scope of the change (see Phase 5 Step 3), include bottom-most and parent specifications (usually). Different specification sampling strategies may be appropriate for these two distinct types of POSS.

b. The safety requirements are also in a hierarchical structure. The planner may define different sampling strategies for assessment of bottom-most and higher safety requirements.

The assessment planner updates the assessment plan, adding the activities to be undertaken during this Step, including the scope and required rigour of the assessment activities.

The candidate assessment activities for this Step are in Phase 5 Step 4 Topic Tables on page 146 (in Appendix D – Candidate assessment activities).

Conduct

Once the plan is prepared, and competent assessors identified, the assessor(s) conduct the planned activities.

When assessing the derivation of the safety criteria, safety requirements and the predicted safety performance, the reliance of each safety analysis upon safety modelling will become apparent. Although the planner should have stipulated whatever assessment activities seemed appropriate for assessment of the safety model elements (using Appendix F – Candidate assessment activities for safety analysis models, page 191), the assessor may need to revert to the planner to agree this in more detail as the assessment progresses.

The assessor determines whether the change safety case material assessed as part of this Step is satisfactory when judged using the assessment activities stipulated in the assessment plan, and records any concerns.

Completion of Phase 5 Step 4

Having conducted the assessment activities, the assessor considers whether it has become apparent that other regulations are applicable. The assessor discusses this with the assessment planner and they decide whether it is necessary for the assessor to determine compliance. Cases where it is not necessary to check compliance may be:

a. when checks of compliance have already been undertaken in Phase 3, or for other stages

b. compliance with those regulations is outside the scope of regulatory responsibility

c. compliance with those regulations is outside the scope of the change safety case

d. compliance with those regulations is outside the scope of the change safety case assessment task.

The knowledge acquired during this Step will be used to refine the planning of assessment activities in the next Step. For example:

a. assessing specifications and safety requirements may identify those whose supporting evidence should be assessed

b. assessing safety criteria may identify those functions that should be assessed, via the associated specifications.

The assessor should consider whether the examined material violates any of the provisions in Table 56, 'Argument' on page 189.

The assessor should agree with the planner whether any concerns require further investigation as part of this Step, or in subsequent Steps. In particular, this could arise if the assessor has failed to gain confidence that the change safety case has demonstrated a clear understanding of the safety issues associated with the change.

Before moving on to the next Step, the assessor checks that all the assessment tasks specified in the assessment plan for the Step have been completed, and that adequate records exist to demonstrate this.

If there is an apparent serious deficiency in the content of the change safety case that cannot be resolved by discussion with the Service Provider, the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Phase 5 Step 5 Plan and assess justification of specification elements

Introduction

The purpose of this Step is to assess the change safety case's justifications that demonstrate that each individual element of the specifications is substantiated by verification or other evidence, or the composition of lower-level specifications, i.e. that the behaviour will be (post-change) as specified.

The primary focus of the assessment in this step is to examine justifications, provided in the change safety case, that argue that the elements of a specification have been demonstrated directly, or demonstrated by composition of the properties or behaviour in 'child' specifications. Whilst it is expected that the assessment will identify individual elements of the specification for which the supporting justifications will be assessed, the change safety case may present justifications that address either all elements or sets of elements together. In this case the assessor will have to identify the relevant justifications.

Whilst an in-depth assessment might sample the referenced verification evidence, the assessor is not able to assess this evidence without understanding its role in the argument. Consequently the candidate assessment activities do not allow for verification documentation to be examined in the absence of the context of the argument that uses it, as its adequacy cannot be judged outside this context.

The subject of verification has been extensively covered by other documents and standards, and in most industries norms have been established for what is adequate. Consequently this section does not attempt to define adequacy or sufficiency, leaving it to the domain expertise of the planner and assessor to identify and apply such norms.

Planning

The assessment planner uses the risks (from Phase 5 Step 1) associated with the transitional stage being assessed, and knowledge gained when conducting previous assessment activities, and develops a plan for assessing the change safety case elements for which candidate assessment activities are given in this Step. The planner should consider whether the familiarisation Phase and any completed assessment activities have already provided sufficient assessment to meet the objectives of the current part of the assessment. Effectively, consideration of the applicable risk factors shows that no additional assessment activities are necessary.

In many domains, the activities of this Step may be rarely undertaken, or conducted on a very small sample of specification elements, relying mainly on the confidence gained in the previous Step.

In this step the planner plans the assessment of the change safety case justifications that demonstrate that each individual element of the specifications is substantiated by the verification or other evidence, or the composition of lower-level specifications. The assessment could address the justifications of elements in:

a. the specifications for the POSSs within the scope of the change
b. the 'additional specifications for safety analyses'[14], but only if the change safety case justifies them
c. the specifications of the baseline POSSs, but only if the change safety case justifies them.

This assessment step is primarily concerned with assessing the justifications for the elements in the specifications for POSSs within the scope of the change. These justifications are always necessary to support the change safety case. However, if it has been established that the change safety case also includes justifications of elements in the 'additional specifications for safety analyses'[14] or in specifications for the POSSs in the baseline functional system, then the planner should consider whether it is necessary to assess those justifications also, according to the role of these specifications in the safety argument.

The planner stipulates which justifications will be assessed by one or more of the following ways:

a. defining specific elements in specific specifications
b. defining specific specifications from which the assessor must identify elements using a specified sampling strategy or objectives
c. specifying a sampling strategy or objectives that the assessor must use to identify specifications and then elements.

The planner does not stipulate the assessment activities to be used to assess the justifications because this cannot be predetermined without understanding the nature of the justification, though guidance can be given.

Possible sampling strategies could include one or more of:

a. random sampling
b. based on specific behavioural attributes (e.g. timing)
c. based on the various technologies used in the functional system (e.g. mechanical, software)
d. determining the sample by some relationship to the risk factors
e. selecting POSSs according to risk or supplier
f. involvement in some other threads e.g. an accident chain
g. expert judgement based on understanding of the issues raised in previous phases of the assessment.

The planner should consider whether the sampling strategies should stipulate how to select which specifications to select from and/or which types of element to consider. If so, the planner could direct the assessor to select elements from:

a. one or more of the various specification types for a Transitional Stage

[14] This is the 'Set of additional specifications required to support safety analysis and/or safety modelling' addressed on page 159.

i. Service specification
ii. Environment specification
iii. Specification of build state

b. one or more of the various specification types for the Functional system
    i. specifications for POSSs (including assets, resources, supplied services)
    ii. architecture specifications
c. one or more of the different bases by which an element is justified
    i. elements in bottom-most specifications, whose justification is based on direct verification evidence (e.g. test, analysis, inspection)
    ii. elements in parent specifications, whose justification is mainly based on composing the behaviour/properties in child POSS specifications, according to architecture specifications.
d. one or more of the various types of element
    i. a behavioural element
    ii. a property element
    iii. an architectural element.

The planner identifies any applicable standards or norms defining verification adequacy or sufficiency that the change safety case should demonstrate compliance with.

Specifications associated with the support systems may be identified among the POSSs impacted by the change. They usually have a less direct relationship to the safety analysis of the operational service, and so may not need to be specified in such great detail, or be so well supported by evidence of their behaviour/properties. The planner should therefore take account of this when providing guidance on assessment activities for justifications of elements in such support system specifications.

The planner may also stipulate that the assessor should assess a sample of verification documentation and compositional analysis records referenced from examined justifications, to ensure that the documents exist and are as inferred by the justification using them.

The planner should consider the impact of any access considerations regarding the justifications and supporting evidence. These are likely to have to be specifically obtained for examination, as they are unlikely to be part of the basic change safety case material submitted due to the quantity of information.

The planner updates the assessment plan, adding the stipulations and strategies to guide the assessment during this Step to assess the justifications of selected elements in selected specifications.

The candidate assessment activities for this Step are in Phase 5 Step 5 Topic Tables on page 173 (in Appendix D – Candidate assessment activities).

Conduct

Once the plan is prepared, and competent assessors identified, the assessor(s) implement the plan for this step.

The assessor undertakes the assessment according to the stipulations and guidance in the plan, including implementing any sampling strategies indicated by the planner.

The assessor should ensure that the necessary justifications and supporting evidence have been requested and received if, as is likely, they are not part of the change safety case material initially submitted (due to the quantity of information).

The assessor may need to take account of any 'collective justifications' used in the change safety case, addressing the justifications for groups of elements for a specification, groups of specifications, etc. Compositional justifications in particular are likely to have a single compositional analysis to address most, if not all, elements in a single specification.

The assessor records the specifications and elements selected for assessment, and the locations of the justifications and collective justifications assessed.

Before commencing assessment of the justifications for the elements, the assessor should ensure that they apply to the correct version of the specification, the one that is applicable to the transitional stage being assessed.

On examining each selected justification, the assessor has to decide which of the relevant candidate assessment activities to use, according to:

a. the nature of the selected specification element:
    i. a behavioural element
    ii. a property element
    iii. an architectural element.
b. the type of justification:
    i. justifications based on direct verification evidence (e.g. test, analysis, inspection) for 'bottom level' specifications
    ii. justifications based on composing the behaviour/properties in child POSS specifications, according to architecture specifications, for parent specifications.

The assessor records the assessment activities used for each element justification.

When considering which assessment activities should be undertaken, the assessor can take account of what has been learnt in Phase 5 Step 4 regarding the decomposition of safety requirements ('Safety Requirements'), to inform assessment of the composition of behaviour in specifications. For example, if a thorough examination of the decomposition of safety criteria into safety requirements was performed in Phase 5 Step 4, then it may be appropriate to reduce effort in examining composition justifications in this step.

The planner may have specified assessment of justifications of elements in support system specifications. Support systems usually have a less direct relationship to the safety analysis of the operational service, and so may not need to be specified in such great detail, or be so well supported by evidence of their behaviour/properties. The assessor should take account of the safety influence of the support system to set expectations for this, when assessing justifications of elements in support system specifications.

The assessor only assesses a sample of verification documentation (e.g. test documents) and compositional analysis records, to ensure that the documents exist and are as inferred by the justification using them:

a. if the plan stipulates or provides guidance that it should be done
b. if the assessor has any concerns, and feels that supporting verification documents should be examined (after gaining the agreement of the planner).

The assessor determines whether the change safety case material assessed as part of this Step is satisfactory when judged using the assessment activities stipulated in the assessment plan, and records any concerns.

Completion of Phase 5 Step 5

Having conducted the assessment activities, the assessor considers whether it has become apparent that other regulations are applicable. The assessor discusses this with the assessment planner and they decide whether it is necessary for the assessor to determine compliance. Cases where it is not necessary to check compliance may be:

a. when checks of compliance have already been undertaken in Phase 3, or for other stages
b. compliance with those regulations is outside the scope of regulatory responsibility
c. compliance with those regulations is outside the scope of the change safety case
d. compliance with those regulations is outside the scope of the change safety case assessment task.

The assessor should consider whether the examined material violates any of the provisions in Table 56, 'Argument' on page 189.

Before moving on to the next Step, the assessor checks that all the assessment tasks specified in the assessment plan for the Step have been completed, and that adequate records exist to demonstrate this. The assessor should agree with the planner whether any concerns require further investigation as part of this Step, or in subsequent Steps.

If the justification of specification elements is apparently inadequate, and this cannot be resolved by discussion with the Service Provider, the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Phase 5 Step 6 Plan and assess safety of transitional activities

Introduction

The purpose of this Step is to assess the change safety case's justification of the safety of the transitional activities that will be undertaken, during each transitional stage.

In some cases, the Service Provider may have to conduct additional safety analyses regarding the safety of the personnel undertaking the transition activities, but this is outside the scope of this Guide.

Any performance monitoring activities, necessary to collect assurance evidence, are not considered to be transitional activities, and so their safety should be addressed by the safety analysis for the functional system.

Any performance monitoring activities, necessary to collect assurance evidence, are considered part of the behaviour in the functional system, and not considered to be transitional activities. Consequently, the safety of their effect on system behaviour should be addressed as part of the safety analysis for the functional system.

Planning

The planner uses the risk (from Phase 5 Step 1) associated with the safety of the transitional activities that will be undertaken during the stage being assessed, and develops a plan for assessing the change safety case elements for which candidate assessment activities are given in this Step. If the previous Steps have revealed significant new information, it may be necessary to reconfirm this risk, as in Phase 5 Step 1. Phase 4 in particular may have revealed aspects of the transitional activities that may influence the risk, or identify specific aspects for which the planner should plan assessment activities.

This Step (Phase 5 Step 6) is usually conducted after:

a. Phase 3, when the descriptions of the transition activities for the whole change may have been assessed

b. Phase 4, when the feasibility of the transitional activities may have been assessed

c. Phase 5 Step 2, when the descriptive material regarding the transitional stage being assessed may have been assessed.

As a result, it may not be necessary to check the plans and descriptions of the transitional activities during this Step. However, according to what has in fact been done before, the Planner may decide that the descriptive material and the plans require further assessment, and so defines assessment activities for this Step from the candidate assessment activities in Phase 3, 4 and Phase 5 Step 2 as above.

The assessment needs to be planned to reflect the risks associated with the project's characteristics, the characteristics of the transitional activities and the change safety case. The project characteristics include the technical capability

and safety culture of the Service Provider, and any contracting organisations assisting the Service Provider to assure and implement the change.

When preparing the plan, the planner should consider whether the familiarisation Phase and any completed assessment activities have already provided sufficient assessment to meet the objectives of the current part of the assessment. Effectively, consideration of the applicable risk factors shows that no additional assessment activities are necessary.

The planner should ensure that the planned assessment activities reflect the approach used by the Service Provider to assure the safety of the transitional activities. The change safety case should evaluate the intended and unintended impact of the transitional activities, and also the impact of potential deviations from the intended transitional activities, and either:

a. argue that the effects have been identified and mitigated so that the risk from them is acceptable according to criteria (perhaps negligible risk or ALARP) set in the Service Provider's SMS

b. treat the effects as (negative) contributors to the safety of the services provided during the transitional stage, integrating the contribution of transitional activities with other causes of service hazards in their safety analyses.

In addition to the candidate assessment activities in the Stage 5 Step 6 tables, the planner can select further candidate assessment activities from those in Stage 4 'Determine whether the planned change is credible', to build confidence in the general suitability of the plans as a suitable basis for safety analysis or as detailed guidance to the assessor on specific aspects to assess.

As part of demonstrating that the change will be made safely, the change safety case may need to justify that the resources and tools used during transitional activities meet their specifications. A candidate assessment activity is provided (in Justification of acceptability of the safety of the transitional activities on page 183) to instruct the assessor to assess this, or else if particularly critical, the planner can stipulate further activities to assess the justification of:

a. the specification (see candidate assessment activities in Justification of the specifications for the POSSs within the scope of the change associated with the transitional stage on page 157), and/or

b. the elements of the specification defining the performance (see candidate assessment activities in Justification of a directly substantiated behavioural element of a specification on page 174).

The assessment planner updates the assessment plan, adding the activities to be undertaken during this Step, including the scope and required rigour of the assessment activities, and addressing the:

a. planned transitional activities

b. safety of the planned transitional activities

c. evidence and justification that resources and tools for transitional activities are as specified.

The planner should consider whether, at Phase 1 Step 5 Identify applicable standards and regulations, it was planned that certain aspects of compliance with regulations would be examined during assessment of the material associated with the transitional activities during the stage being assessed. If so, the planner adds relevant activities into the assessment plan.

The candidate assessment activities for this Step are in Phase 5 Step 6 Topic Tables on page 179 (in Appendix D – Candidate assessment activities).

Conduct

Once the assessment plan is prepared, and competent assessors identified, the assessor(s) conduct the planned activities.

The assessor should identify where the change safety case identifies the transitional activities that will be undertaken during the stage being assessed. They may be specified collectively, given separately for each transitional stage or for individual subsystems, or split some other way.

The assessor should consider whether the change safety case needs to address the safety of preparatory transitional activities that take place before the first transition (intended change to the functional system). In some cases, a simple direct justification of no impact on the extant functional system may be adequate, according to the nature of these activities and their relationship to the functional system. The change safety case may have defined a separate transitional stage for this purpose. Alternatively, it may directly reference a separate risk assessment or safety case that, in some domains, may be considered as justifying a different change, and therefore be out of scope of the current assessment.

When the assessment plan stipulates the assessment of justifications that support the specifications of the resources and tools for transitional activities, the assessor may find that the applicable properties are not well specified, in the manner expected for the operational system, and there may be little justification that the properties of the resources and tools meet their specifications. For many resources and tools for transitional activities or where common practice applies, it may be acceptable for the Service Provider not to provide any evidence or justification at all. When the change safety case justifies the performance of the resources and tools for transitional activities, a lower level of confidence may be necessary than for the operational system, and the assessor's expectations for the evidence and justification may need to be adjusted accordingly.

If the assessor finds that a detailed justification of the performance of resources or tools has been provided and needs to be assessed, the planner should be consulted to define suitable assessment activities to assess the justification of:

a. the specification (see candidate assessment activities in Justification of the specifications for the POSSs within the scope of the change associated with the transitional stage on page 157), and/or

b. the elements of the specification defining the performance (see candidate assessment activities in Justification of a directly substantiated behavioural element of a specification on page 174).

The assessor determines whether the change safety case material assessed as part of this Step is satisfactory when judged using the assessment activities stipulated in the assessment plan, and records any concerns.

Completion of Phase 5 Step 6

Having conducted the assessment activities, the assessor considers whether it has become apparent that other regulations are applicable. The assessor discusses this with the assessment planner and they decide whether it is necessary for the assessor to determine compliance. Cases where it is not necessary to check compliance may be:

a. when checks of compliance have already been undertaken in Phase 3, or for other transitional stages

b. compliance with those regulations is outside the scope of regulatory responsibility

c. compliance with those regulations is outside the scope of the change safety case

d. compliance with those regulations is outside the scope of the change safety case assessment task.

The assessor should consider whether the examined material violates any of the provisions in Table 56, 'Argument' on page 189.

Before moving on to the next Step, the assessor checks that all the assessment tasks specified in the assessment plan for the Step have been completed, and that adequate records exist to demonstrate this. The assessor should agree with the planner whether any concerns require further investigation.

If the justification of the safety of the transitional activities is apparently inadequate, and this cannot be resolved by discussion with the Service Provider, the assessor and planner agree whether to terminate the assessment by proceeding directly to Phase 6.

Phase 5 Step 7 Ensure assessment of the transitional stage is adequately completed

Introduction

The purpose of this Step is for the planner and assessor to determine whether any further assessment activities are required to assess the parts of the change safety case addressing the transitional stage being assessed.

Conduct

The assessor considers whether, in the light of what has been learnt, it is necessary to reconsider the suitability of the descriptions, to determine whether they are correct and adequately communicate to uninformed readers. The assessor can select appropriate activities from the tables regarding 'descriptions' in Phase 3 and Phase 5 Step 2.

The assessor checks that all the assessment tasks specified in the assessment plans for Phase 5 (Steps 1 to 6) for the transitional stage have been completed, and that adequate records exist to demonstrate this.

The assessor should also agree with the planner whether any concerns require further investigation as part of this Phase, either for the transitional stage being assessed or other transitional stages affected by the concerns identified. They also consider whether the assessment activities have revealed new information that means that the risks determined in Phase 2 need to be considered, or if the risks associated with just the transitional stage being assessed need to be reconsidered, so that additional assessment activities are then planned and conducted.

Continuing the assessment

If significant issues, errors or omissions have been identified, the planner and assessor should discuss whether to terminating the assessment by proceeding directly to Phase 6.

When the assessment of the transitional stage is considered complete, the same process (Phase 5) is used for the next transitional stage[15], until all transitional stages have been addressed.

[15] The change stages are not necessarily assessed in implementation order.

Phase 6 Findings and reporting

Introduction

The purpose of this Phase is to collate and evaluate the concerns recorded during the assessment, to determine their significance in the context of the overall safety case, and document the findings.

This Phase is undertaken by an 'arbiter', perhaps with the support of other members of the assessment team. In most cases the planner or one of the assessors will be the best arbiter, due to having the best overall perspective.

Conduct

The arbiter collates all concerns recorded during the assessment. Concerns must not be discarded due to some sort of prioritisation or time limit for the assessment or follow-up activities.

The arbiter may believe that some individual concerns can be closed or made properly specific by requesting information or clarification from the Service Provider. This action and the assessment of the result are usually undertaken by the assessor who raised the concern.

The arbiter should consider whether there is benefit in discussing the outstanding concerns with the Service Provider. For example, it would provide an opportunity for the Service Provider to confirm their factual accuracy.

The arbiter retains all queries sent and responses received, and files them as part of the assessment records. If the responses supplement the information in the change safety case, or provide substantial explanation, then the arbiter should record a finding that the change safety case needs to be changed to incorporate the information provided in the response.

The outstanding concerns are considered to be formal assessment findings. The assessor who raised each concern should review its initial finding categorisation, definitively categorising it as either a deficiency, or as a comment. The concern should be considered a deficiency if the assessor would consider the change safety case unacceptable if the concern remained. A more detailed categorisation scheme, like the one in Table 1: Finding Categories below can be used to provide an indication of the nature of the deficiency or comment.

In deciding whether a concern should be categorised as a deficiency or a comment, the assessor takes account of the following:

a. the safety risk associated with the functions whose assurances are affected by the error
b. the extent to which the validity of the assurances are undermined by the error. This is determined by the role of the part of the change safety case (e.g. the specific argument, evidence item, safety analysis element) in which the error is present
c. the objectives of the CA's review
d. any applicable mandatory requirements of standards and regulations

e. other regulatory motivations such as the promotion of good practices or enforcement of minimum standards, where this is appropriate and effective in the context of the change safety case review.

The CA may adopt a standard classification scheme for deficiencies, for example in terms of which of the fundamental safety arguments in 'Technical basis of guidance' (page 10) is being undermined.

The findings can be summarised according to any specific objectives or priorities set for the review or used to influence the modulation process.

The arbiter also reviews the concerns to identify whether there are related concerns that together suggest a new concern (which is then classified as a deficiency or comment). The risk factors that governed the assessment may suggest how concerns may be related. More generally, related concerns may be identified by correlating them by identifying common factors like:

a. POSS
b. change safety case topic
c. safety function
d. organisation
e. technology
f. change safety cases attributes including confidence, uncertainty, informality.

Deficiencies	D1	Potential safety issue with the proposed change (deficiency)
	D2	Deficiency in the change safety case (deficiency)
	D3	Non-compliance with an applicable mandatory requirement of a standard or regulation (deficiency)
	D4	Query or recommendation (deficiency as there is an issue to resolve)
Comments	C1	Suggestion or other comment, for example an improvement, but not an issue upon which acceptability of the change safety case depends (comment, but the Service Provider may need to consider action)
	C2	Typographic or grammatical error or improvement, or other trivial comment (comment, but the solution is considered obvious)

Table 1: Finding Categories

The arbiter should prepare an internal CA report that documents the Phases used to assess the change safety case and records the findings (deficiencies and comments). The report and assessment records should be held on file, for use in subsequent processes, according to the governing CA procedure for the review (illustrated in 'Appendix A – Context of change safety case assessment guide' on page 92).

Appendix A – Context of change safety case assessment guide

This diagram shows the context within which this Guide is used. The change safety case assessment, which is addressed by this Guide, is presented by the just the central box ('Assess CSC'). All other aspects of the diagram fall within the scope of the CA's or SP's procedures. In particular, the CA will need procedures for:

- receipt of change notifications
- deciding whether a change should be reviewed
- receipt of change safety case submissions/ resubmissions
- the actions taken following the conclusion of the assessment.

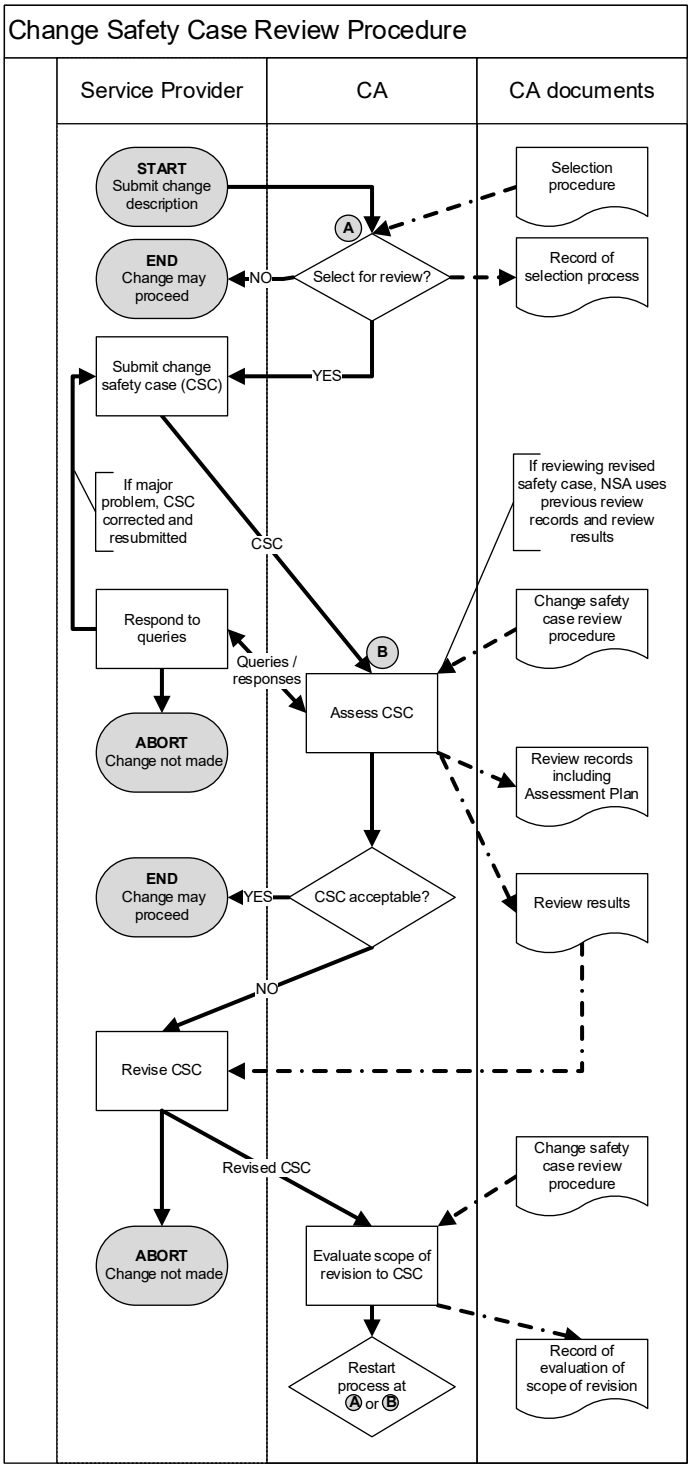

Figure 5: Overview of Change Safety Case Review Procedure

Appendix B – Change safety case topics

This appendix provides a list of all the assessment topics and subjects for assessment in this Guide, organised according to the phases and steps where they may be examined.

As well as providing an index to the Guide, it should be used during in Phase 1 of the assessment to record the location of the related material in the change safety case submission, and any notes. This information is useful to both the planner and the assessor(s), and can be augmented during any assessment activity.

The tables below are split according to the assessment phase, with separate tables for the safety model and argumentation topics. This eases the production of multiple copies of the tables, especially for Phase 5, where it is envisaged that the assessment will use one copy per transitional stage.

Completed tables should be filed as part of the assessment records.

Phase 3 Plan and assess stage independent parts of the change safety case (page 60)

Topic/Subject for assessment	Document, Location & Notes
Description of functional system and service, and changes to be made (page 121)	
1 Descriptions of the existing functional system and service, before the proposed change (Page 122)	
2 Descriptions of the change (Page 122)	
3 Descriptions of transitional stages (Page 124)	
4 Justification of descriptions (Page 124)	
5 Installation, Commissioning, Transition and Recovery Plans (contiguity check) (Page 124)	
Claim of acceptability of predicted safety performance for all changes proposed in the change safety case (Page 125)	
6 Top-most claim of the change safety case (Page 125)	
Uncertainties in the change safety case (Page 125)	
7 Justification of the treatment of uncertainties (Page 126)	
Justification that the change is a good change (Page 127)	
8 The change management procedures used, as claimed by change safety case (Page 127)	
9 Justification that the proposed change is a good change (Page 128)	

Phase 4 Determine whether the planned change is credible (Page 62)

Topic/Subject for assessment	Document, Location & Notes
Installation, Commissioning, Transition and Recovery Plans (Page 131)	
10 Installation, Commissioning, Transition and Recovery Plans (Page 132)	
11 Justification of Installation, Commissioning, Transition and Recovery Plans (Page 135)	

Phase 5 Plan and assess stage dependent parts of the change safety case (Page 66)

Topic/Subject for assessment	Document, Location & Notes
Phase 5 Step 1 Confirm risks associated with the transitional stages and activities (Page 68)	
Phase 5 Step 2 Plan and assess descriptions, declared SMS and claim of safety for the stage (Page 70)	
Service, functional system and change descriptions (Page 136)	
12 Descriptions of service, functional system and change before the transition, and change to be made (Page 136)	
Support system descriptions (Page 137)	
13 Descriptions of changed support systems (Page 138)	
Relationship of the change safety case to Service Provider's SMS (Page 139)	
14 Risk tolerability and classification scheme used in change safety case (Page 139)	
Claim of acceptability of predicted safety performance for the stage (Page 140)	
15 Top-most safety claim for the stage (Page 140)	
Phase 5 Step 3 Plan and assess the scope of the change (Page 73)	
Declaration of the scope of the change (Page 141)	
16 Lists of changed and impacted Parts of the Operational and Support Systems (POSSs) (Page 141)	
17 Justification of lists of changed and impacted POSSs (Page 142)	
Impact analysis records (Page 143)	
18 Records of analysis that identified those POSSs that have changed, but their behaviour has NOT been changed (i.e. their new specifications show the same behaviour as before the change) (Page 144)	
19 Records of analysis that identified those POSSs that have changed, and their behaviour has been changed (i.e. their new specifications show different behaviour to before the change). This includes all new and removed POSSs. (Page 144)	

20 Records of analysis that identified those POSSs that have NOT changed, but whose specification has been changed due to a change in the interactions across one or more of its interfaces and/ or in the resources it shares with other POSSs (Page 144)	
21 Records of analysis that identified those POSSs that have NOT changed, but whose specification has been changed due to a change in their safety requirements (Page 145)	
Phase 5 Step 4 Plan and assess specification and safety analysis material (Page 76)	
Specification of transitional stage (Page 146)	
22 Transitional stage specification (Page 146)	
23 Specification of build state (Page 147)	
Specification sets (Page 147)	
24 Set of specifications for the scope of change (Page 147)	
25 Set of additional specifications required to support safety analysis and/or safety modelling(Page 148)	
Specification of service and operational environment (Page 148)	
26 Specification of the service(s) (Page 148)	
27 Specification of the environment(s) of the service(s) (Page 149)	
Specification of the parts of the functional system that are within the scope of the change (Page 150)	
28 Specification of functional system environment (Page 150)	
29 Specifications of architectures (Page 151)	
30 Specifications of parts of the operational system (Page 152)	
31 Specification of external services, including supply of resources (Page 154)	
32 Specifications of the parts associated with arrangements for support of the operational system (Page 155)	

Justification of Specifications within the scope of the change (Page 156)	
33 Justification of the specifications for the POSSs within the scope of the change associated with the transitional stage (Page 157)	
Justification of additional specifications to support safety analyses (Page 159)	
34 Justification of additional specifications to support safety analyses for the transitional stage (Page 159)	
Safety criteria (Page 160)	
35 Set of safety criteria that define acceptable safety performance for the specific transitional stage being assessed (Page 160)	
36 Records of analyses to derive set of safety criteria (Page 162)	
37 Justification of safety criteria (Page 163)	
Evaluation of acceptability of predicted safety performance (Page 165)	
38 Evaluation of acceptability of the predicted safety performance associated with the changed service, during the transitional stage being assessed (Page 166)	
39 Source of each predicted safety performance (Page 167)	
40 Justification of evaluation of acceptability of the predicted safety performance associated with the changed service, during the stage being assessed (Page 167)	
Safety Requirements (Page 168)	
41 Set of safety requirements (Page 169)	
42 Records of analyses to derive set of safety requirements (Page 169)	
43 Justification of set of safety requirements (Page 170)	
Phase 5 Step 5 Plan and assess justification of specification elements (Page 80)	
Justifications of elements of specifications (Page 173)	
44 Justification of an element of a specification by composition (Page 173)	
45 Justification of a directly substantiated behavioural element of a specification (Page 174)	
46 Justification of a (non-behavioural) directly substantiated property element of a specification (Page 175)	

47 Justification of a directly substantiated element of an architectural specification (Page 177)	
Phase 5 Step 6 Plan and assess safety of transitional activities (Page 85)	
Safety of the planned transitional activities (Page 179)	
48 The set of transitional activities that will be undertaken during the transitional stage (Page 180)	
49 Analysis of the impact of the transitional activities, and of potential deviations (Page 181)	
50 Recovery plan (possibly contained within transition plan) (Page 183)	
51 Justification of safety of potential services/functional system states during recovery and after recovery complete. (Page 183)	
52 Justification of acceptability of the safety of the transitional activities (Page 183)	

Elements of Arguments (Page 186)

Topic/Subject for assessment	Document, Location & Notes
53 Claims other than the top-most claim (Page 186)	
54 Inferences (Page 186)	
55 Evidence (Page 189)	
56 Argument (Page 189)	

Safety Models (page 191)

Topic/Subject for assessment	Document, Location & Notes
Identified Hazards (Page 191)	
57 Set of identified hazards (Page 191)	
58 Justification of the identified hazards (Page 192)	
Correctness of consequence model (Page 193)	
59 Set of accident trajectories (Page 193)	
60 Justification of the set of accident trajectories (Page 195)	
61 Mitigation analysis (Page 195)	
62 Justification of mitigation analysis (Page 196)	
63 Set of identified accidents (Page 197)	
64 Justification of set of identified accidents (Page 197)	
65 Set of accident risks (Page 198)	
66 Justification of the set of accident risks (Page 199)	
Correctness of causal model (Page 200)	
67 Set of top events (Page 200)	
68 Justification of set of top events (Page 200)	
69 Identification of hazard causes (Page 200)	
70 Justification of identification of hazard causes (Page 202)	
71 Set of predicted occurrence rates of hazard causes (e.g. basic events in a fault tree) (Page 203)	

72 Justification of set of predicted occurrence rates of hazard causes (e.g. basic events in a fault tree) (Page 204)	
73 Set of predicted hazard occurrence rates (Page 205)	
74 Justification of set of predicted hazard occurrence rates (Page 205)	
Overall properties of cause-consequence models (Page 206)	
75 Cause-consequence models e.g. a set of bow tie models, one for each hazard (Page 206)	
76 Justification of overall properties of cause-consequence models (Page 208)	

Appendix C – Description of change safety case topics

Introduction

This appendix describes the change safety case topics assessed when following this change safety case assessment guide. It explains each topic and its relationship to the other topics.

The description highlights cases where this guide has taken a forward-looking view, in the sense that what is required in a complete safety argument may exceed common practice for some change safety case topics. However, if the topic does not fulfil these expectations, related change project artefacts (e.g. process records) should provide the necessary information: if not the safety argument is incomplete. By taking this approach, in the cases where it was believed warranted, the guide highlights where perhaps common practices need to move forward. In some cases, such progress is dependent on academic developments that lead to more objective arguments being made as part of industrial practise e.g. regarding the assured integrity and confidence associated with behaviour in specifications.

1 Descriptions of the existing functional system and service, before the proposed change (Page 122)

Descriptions of the functional system and service to be changed, provided to introduce the context and baseline for the change.

The descriptions should be well written, correct and cover the important features of the functional system and service, but are not the definitive specification of the functional system and service. Descriptive material is vital to understanding the safety case, and assists assessment planning.

2 Descriptions of the change (Page 122)

Descriptions of what changes are going to be made to the functional system and service, providing a clear statement of the nature and extent of the change.

The descriptions should be well written, correct and cover the important features of the change, but are not the definitive specification of the change. Descriptive material is vital to understanding the safety case, and assists assessment planning.

3 Descriptions of transitional stages (Page 124)

Descriptions of how the changes are going to be made to the functional system and service.

The descriptions should describe the transitional stages that will be used to implement the overall change and, for each transitional stage (including the final transitional stage where the complete change has been implemented), describe:

a. the changes that will be made at the start of the transitional stage to the functional system

b. the changes that will be made at the start of the transitional stage to the service provided

c. the transitional activities that are carried out during the transitional stage (clear-up after previous transitional stages and preparation for later transitional stages).

The descriptions should be well written, correct and cover the important features of the change, but are not the definitive specification of the change. Descriptive material is vital to understanding the safety case, and assists assessment planning.

4 Justification of descriptions (Page 124)

An argument that the descriptions (see previous entries) have been adequately verified, and are therefore trustworthy representations of their subject matter.

5 Installation, Commissioning, Transition and Recovery Plans (contiguity check) (Page 124)

These plans are defined in item 10 below. Only the highest level of information is of interest when checking the contiguity of the plans in Phase 3.

6 Top-most claim of the change safety case (Page 125)

A claim that the change is acceptably safe because the predicted safety performance associated with the changed service, and all transitional stages, is acceptable, and the changes will be made safely.

This claim is based upon an equivalent claim for each transitional stage.

7 Justification of the treatment of uncertainties (Page 126)

A discussion leading to a claim that there are no outstanding uncertainties that invalidate the change safety case. This is a summary of the overall situation, discussing any major uncertainties and how they have been addressed, and referencing out to any detailed discussion of specific issues covered by the change safety case.

8 The change management procedures used, as claimed by change safety case (Page 127)

A reference to the specific change management procedures used to develop the change and the change safety case. Inherent in this is a claim that the change management procedures were suitable for the change, from the Service Provider's SMS and, if required, approved by the CA.

9 Justification that the proposed change is a good change (Page 128)

A justification that the Service Provider has addressed issues that are not directly indicative of the acceptability of the safety of the change, but are associated with the wider responsibilities of the Service Provider. This is associated with technical and societal practices during the change and the future operation, including:

a. compliance with standards, regulations, best practice and risk principles

b. minimisation of impact on other entities

c. optimisation of operational robustness and availability .

10 Installation, Commissioning, Transition and Recovery Plans (Page 132)

Plans that define, for each transitional stage, the transitional activities to manage and implement the change, and any resources required. There may be a single 'transition plan', or a set of plans covering each transitional stage separately, or to cover the separate aspects of installation, commissioning and recovery.

The transitional activities that the plans need to address include:

a. Confirmation that the initial state of the functional system is compatible with the plan

b. Initiating the services to be provided during the transitional stage, and are provided while the other transitional activities are undertaken

c. Coordination with the operational services being offered at the time of the activity

d. Installation or modification of non-operational assets to ready them for use

e. Commissioning to ensure that the installed or modified assets are in the expected state

f. Removal of redundant assets, and similar clearing up tasks

g. Collection and analysis of assurance evidence (conducted as part of in-service performance monitoring)

h. Activities to recover the functional system to a known state that has acceptable risk (usually by regressing to the previous state), if a transitional stage cannot be successfully completed.

11 Justification of Installation, Commissioning, Transition and Recovery Plans (Page 135)

An argument that the installation, commissioning, transition and recovery plans (see previous entry) are credible.

12 Descriptions of service, functional system and change before the transition, and change to be made (Page 136)

Descriptions of the service, functional system and what changes are going to be made during the individual transitional stage being assessed.

The descriptions should be well written, correct and cover the important features of the service, functional system and change, but do not provide the definitive specification of these. Descriptive material is vital to understanding the safety case, and assists assessment planning.

13 Descriptions of changed support systems (Page 138)

Descriptions of what changes are going to be made to the support systems during the individual transitional stage being assessed.

The descriptions should be well written, correct and cover the important features of the changes, but do not provide the definitive specification of these. Descriptive material is vital to understanding the safety case, and assists assessment planning.

14 Risk tolerability and classification scheme used in change safety case (Page 139)

A scheme that defines the classification and tolerability of the risks associated with the accidents that can occur as a result of the service provided.

The change safety case uses a risk tolerability and classification scheme to define the safety criteria, if the predicted safety performance of the changed service is evaluated at the level of service risk. This Guide expects an applicable scheme to be defined by the Service Provider's SMS. The scheme is not required when change safety cases set safety criteria based on maintaining or improving safety-related behaviour (hazard rates or proxies).

The scheme defines how the risk presented by all potential accidents can be consolidated, and the acceptability of the resultant total risk can be determined. It may separately address the acceptability of the risk to different parties e.g. the general public, employees.

The scheme does not include the implementation of additional risk management principles (e.g. ALARP, GAMAB) which must also be considered when setting the safety criteria.

15 Top-most safety claim for the stage (Page 140)

A claim that the change is acceptably safe because the predicted safety performance associated with the changed service during the transitional stage is acceptable, and the transitional activities during the transitional stage will be conducted safely.

This, along with equivalent claims for each transitional stage supports the top-most claim of the change safety case.

This claim is made as a consequence of comparing the predicted safety performance and the safety criteria for the transitional stage, and justifying the safety of the transitional activities (either as part of the prediction of safety performance or in a separate safety analysis).

16 Lists of changed and impacted Parts of the Operational and Support Systems (POSSs) (Page 141)

A set of lists of the changed and impacted parts of the operational and support systems, which together define the scope of the change for the transitional stage. POSSs are architecturally identifiable, and hence are a sub-set of those POSSs in the build state for the transitional stage.

The change safety case can define the scope of the change from the initial (pre-change) state or from that during a preceding transitional stage. The safety analyses (setting safety criteria and predicting safety performance) have to be consistent with this scope, and need to address all safety-related behaviour within it. Therefore, a specification is required for each POSS in the lists.

The changed and impacted POSSs comprise those POSSs that have:

a. changed, but their behaviour has NOT been changed (i.e. their new specifications show the same behaviour as before the change)

b. changed, and their behaviour has been changed (i.e. their new specifications show different behaviour to before the change). This includes all new or deleted POSSs.

c. NOT changed, but whose specification has changed due to a change in the interactions across one or more of its interfaces

d. NOT changed, but whose specification has changed due to a change in the resources it shares with other POSSs

e. NOT changed, but whose specification has changed due to a change in their safety requirements[16].

17 Justification of lists of changed and impacted POSSs (Page 142)

A justification that the changed and impacted POSSs (see previous entry) have been correctly identified for the transitional stage by the impact analysis.

The justification of the correctness of the impact analysis may include arguments that:

a. there are (credible) specifications for the POSSs the analysis analysed

b. the analysis was correctly done from a stated baseline

c. regression testing supports the correctness of the analysis including the artefacts the analysis relied on

[16] If a POSS has a changed safety requirement that only increases the required integrity or confidence, there is no further impact from this change, because the behaviour has not changed. If, however, new behaviour is identified as a result of the increased verification (undertaken to increase the assured integrity or confidence in the required behaviour), the POSS's specification has changed and so the POSS is treated as changed.

d. all new behaviour detected (e.g. during formal verification and other test or monitoring activities) resulted in changes to the behaviour recorded in the specification for the relevant POSSs, and therefore revisions to the impact analysis.

18 Records of analysis that identified those POSSs that have changed, but their behaviour has NOT been changed (i.e. their new specifications show the same behaviour as before the change) (Page 144)

The records of the analysis are the worksheets or equivalent working documents or files used in the systematic analysis that identified the relevant POSSs. The analysis records provide evidence of the conduct of the analysis, enabling the assessor to assess the credibility of the justification of the analysis output, and hence the output itself.

19 Records of analysis that identified those POSSs that have changed, and their behaviour has been changed (i.e. their new specifications show different behaviour to before the change). This includes all new and removed POSSs. (Page 144)

The records of the analysis are the worksheets or equivalent working documents or files used in the systematic analysis that identified the relevant POSSs. The analysis records provide evidence of the conduct of the analysis, enabling the assessor to assess the credibility of the justification of the analysis output, and hence the output itself.

20 Records of analysis that identified those POSSs that have NOT changed, but whose specification has been changed due to a change in the interactions across one or more of its interfaces and/or in the resources it shares with other POSSs (Page 144)

The records of the analysis are the worksheets or equivalent working documents or files used in the systematic analysis that identified the relevant POSSs. The analysis records provide evidence of the conduct of the analysis, enabling the assessor to assess the credibility of the justification of the analysis output, and hence the output itself.

21 Records of analysis that identified those POSSs that have NOT changed, but whose specification has been changed due to a change in their safety requirements (Page 145)

The records of the analysis are the worksheets or equivalent working documents or files used in the systematic analysis that identified the relevant POSSs. The analysis records provide evidence of the conduct of the analysis, enabling the assessor to assess the credibility of the justification of the analysis output, and hence the output itself.

22 Transitional stage specification (Page 146)

A specification that defines the functional system, service and operational environment that will exist during a transitional stage. This is usually provided by reference to separate specifications for the operational environment, service and the build state of the functional system.

23 Specification of build state (Page 147)

A specification that defines the functional system that will exist during a transitional stage. It identifies the POSSs that it comprises, including their versions.

Build state specifications are commonly hierarchical, inherently invoking the build state specification of those POSSs that have their own.

24 Set of specifications for the scope of change (Page 147)

The set of specifications that defines the parts of functional system that are within the scope of the change. It comprises the specifications for all the POSSs (at each architectural level) in the scope of the change and their specified architectures. Depending on the scope, this will include items 29 and 30 below, and may include specifications of the types in items 26, 27, 28, 31, and 32 below.

The POSSs in the scope of the change are those that will have been changed or impacted by the change.

The specifications in the set provide the behaviour/property information that is used to predict the safety performance of the changed functional system.

25 Set of additional specifications required to support safety analysis and/or safety modelling (Page 148)

The set of specifications that are not part of the set in item 24, but are necessary to support safety analysis and/or safety modelling.

These specifications are those used when either decomposing historical safety targets to set safety criteria at the level of the scope of the change, or (equivalently) composing safety performance from the level of the scope of the change to safety criteria set at a higher level. Hence they comprise specifications relating to design levels above the scope of the change, and to sibling-level POSSs required to contribute to the decomposition/composition.

26 Specification of the service(s) (Page 148)

The specification that defines the service(s) provided by the functional system in its specified environment (item 27). A service specification is only required for services that are impacted by the change.

27 Specification of the environment(s) of the service(s) (Page 149)

The specification that defines the environment(s) into which the service(s) provided by the functional system are delivered. The environment only needs to be specified for those services that are impacted by the change.

The environment specification includes not only the properties and entities associated with the physical environment, but also wider aspects: other related services and Service Providers, the regulatory environment, and security environment, etc.

28 Specification of functional system environment (Page 150)

The specification that defines the environment of a POSS. The environment only needs to be specified for those POSSs that are in the scope of the change.

The environment specification includes not only the properties and entities associated with the physical environment, but also wider aspects: co-existing systems and participating organisations, the regulatory environment, etc.

29 Specifications of architectures (Page 151)

The specifications that define the architectures that link the specified POSSs, either functionally, by sharing of resources or by sharing of their environment.

These are used when:

a. identifying POSSs impacted by the change, and hence the scope of the change
b. decomposing historical safety targets to set safety criteria at the level of the scope of the change, or (equivalently) composing safety performance from the level of the scope of the change to safety criteria set at a higher level
c. decomposing safety criteria and safety requirements to set safety requirements on lower-level POSSs
d. composing behaviour in child POSS specifications to create parent POSS specifications.

30 Specifications of parts of the operational system (Page 152)

The specifications that define the behaviour/properties of the parts of the operational system, for all operational modes including failure and fall-back modes, for the predicted operational environment. These parts may be human, procedures, equipment, assets, resources, external services or a combination of these.

The specifications contain individual specification elements that each define an individual behaviour/property of the part, which was determined from test evidence or analysis. The elements together address all behaviour/properties of the part, including those which match the safety requirements for the part. All

elements that match the safety requirements (and possibly other elements) include a statement of their verified integrity and associated confidence.

[The following applies to specifications for both operational and support systems (see item 32 on page 110).] Common practice may not create a single comprehensive specification for a POSS in the predicted operational environment. In particular:

a. the non-normal behaviours/properties may be identified as the result of specific analyses or tests (e.g. FMEA, safety requirement identification/apportionment), and not subsequently consolidated into a single specification for the POSS

b. the specification may not be instantiated for the predicted operational environment, but stated for a generic environment, leaving safety analysts to instantiate the behaviour/properties

c. the behavioural or property elements may not have (individually or even collectively) associated statements of the integrity (probability that the behaviour is delivered), leave this aspect to be addressed in some other way. This is a complex subject where practice and theory are slowly advancing.

d. similarly, the confidence to which the statement of integrity is known is commonly not addressed. This is an even more complex subject that is poorly developed, along with the related problem of defining how much confidence is required. This guidance has candidate assessment activities for how uncertainties are addressed in the change safety case.

e. the behaviours/properties in specifications are rarely completely composed all the way up to create the service level specifications, commonly terminating at an intermediate level, so leaving upper-level behaviour to be represented in safety models.

31 Specification of external services, including supply of resources (Page 154)

The specification that defines the behaviour/properties of an external service, in all operational modes including failure and fall-back modes, for the predicted operational environment. Such external services support the functional system, and could include the supply of physical resources and consumables, maintenance services, electrical power, operational data etc.

The specification contains individual specification elements that each define an individual behaviour/property of the external service, as guaranteed by the supplier of the service. The elements together address all behaviour/properties of the external service, including those which match the safety requirements for the external service. All elements that match the safety requirements (and possibly other elements) include a statement of their assured integrity and associated confidence.

The specification may be at least partly derived from a Service Level Agreement, possibly augmented by additional assurance generated either by the supplier or the Service Provider. It may also be necessary to adjust the service specification to the predicted operational environment.

32 Specifications of the parts associated with arrangements for support of the operational system (Page 155)

The specifications that define the behaviour/properties of the parts of the support systems, for all their operational modes including failure and fall-back modes, for the predicted operational environment. These parts may be human, procedures, equipment, assets, resources, external services or a combination of these.

The specifications contain individual specification elements that each define an individual behaviour/property of the part, which was determined from test evidence or analysis. The elements together address all behaviour/properties of the part, including those which match the safety requirements for the part. All elements that match the safety requirements or are known to be related to safety (and possibly other elements) include a statement of their verified integrity and associated confidence.

See notes on common practice under item 30 on page 108.

33 Justification of the specifications for the POSSs within the scope of the change associated with the transitional stage (Page 157)

A justification that the specifications for the POSSs within the scope of the change are trustworthy. The justification should demonstrate that the specifications are correct, consistent, sufficiently detailed, and verified statements of the behaviour/properties of the POSSs in their defined environments.

The more-detailed justifications that the specifications correctly reflect direct verification evidence, or the composition of lower-level specifications, are addressed separately in items 44 to 47.

34 Justification of additional specifications to support safety analyses for the transitional stage (Page 159)

A justification that the additional specifications to support the safety analyses are trustworthy. The justification records why the Service Provider is prepared to use these specifications, even if they have not been fully verified as part of preparing the current change.

As these specifications are not within the scope of the change, but are necessary to support the safety analyses, the change project needs to justify why it accepts that they are sufficiently trustworthy for this purpose. If use of the existing specifications could not be justified, then the change project will have had to undertake additional verification to provide the justification.

35 Set of safety criteria that define acceptable safety performance for the specific transitional stage being assessed (Page 160)

The criteria that define acceptable safety performance for all safety-related behaviour within the scope of the change for the transitional stage.

The safety criteria are set according to the safety goals or principles established by the Service Provider's SMS and/or applicable legislation and regulations. They define acceptable safety performance in terms of risk, rates of occurrence, or proxies, and so are the basis for the decision as to whether the predicted safety performance of the changed functional system is acceptable.

36 Records of analyses to derive set of safety criteria (Page 162)

The records of the analysis show the basis and calculations that were used to derive the set of safety criteria. The analysis records provide evidence of the conduct of the analysis, enabling the assessor to assess the credibility of the justification of the analysis output, and hence the output itself.

The records will show that the analysis involved:

a. the Service Provider's SMS, which set requirements on how acceptable safety performance is established when a change is made

b. a model of safety, derived either from first principles or by updating an existing safety model, which identifies the safety-related behaviour of the whole functional system/service, and how it relates to the POSSs

c. the relevant safety-related behaviour for which criteria were established is that with a contribution from behaviour of POSSs within the scope of the change, as revealed by their specifications. This will also be consistent with the safety requirements.

37 Justification of safety criteria (Page 163)

A justification that the safety criteria for the transitional stage are valid.

38 Evaluation of acceptability of the predicted safety performance associated with the changed service, during the transitional stage being assessed (Page 166)

A demonstration that the predicted safety performance of the changed functional system meets the safety criteria that define acceptable safety performance for the transitional stage. The safety performance for the transitional stage can only be claimed to be acceptable on the basis that all the individual safety criteria for that transitional stage have been shown to be satisfied.

39 Source of each predicted safety performance (Page 167)

The source of each predicted safety performance used in item 38. In each case this is either a POSS specification or a safety analysis that derived the predicted

safety performance by composing the behaviour/properties in POSS specifications. The composition may have been based on a safety model.

If not separately argued to be negligible, the contributions of transitional activities, maintenance, environmental events etc. would be expected to be included in the predicted safety performance by safety modelling, rather than being incorporated in the POSS specifications.

40 Justification of evaluation of acceptability of the predicted safety performance associated with the changed service, during the stage being assessed (Page 167)

A justification that the predicted safety performance associated with the changed service was correctly identified, and that the evaluation of its acceptability was correctly undertaken, for each safety criterion.

41 Set of safety requirements (Page 169)

The safety requirements derived from the safety criteria that collectively specify all safety-related behaviour within the scope of the change. Each safety requirement defines a necessary behaviour or property of a defined part of the functional system, and is refined to successively lower-level safety requirements until they are defined for the bottom-most specified POSS.

Different safety requirements for the same behaviour or property may be established for different operational modes.

The role of safety requirements in the change safety case is to:

a. establish that, at each level of specification, the assured behaviour matches that required to satisfy the safety criteria
b. support identification of the scope of the change
c. support safety performance monitoring.

42 Records of analyses to derive set of safety requirements (Page 169)

The records of the analysis show the method used to derive the set of safety requirements from the safety criteria. The analysis records provide evidence of the conduct of the analysis, enabling the assessor to assess the credibility of the justification of the analysis output, and hence the output itself.

The records will show that the analysis involved:

a. the derivation of the safety requirements from the safety criteria
b. architecture specifications
c. POSS specifications
d. environment specifications applicable to each level of architecture
e. deriving the confidence to which each safety requirement must be demonstrated.

43 Justification of set of safety requirements (Page 170)

A justification that the set of safety requirements was correctly identified and shown to be satisfied, including demonstration that:

a. the safety requirements were derived from the safety criteria
b. the set of safety requirements completely addresses all safety criteria
c. each safety requirement is correct
d. each safety requirement is specified in a verifiable manner
e. there has been adequate verification of the safety requirements and their derivation to ensure that they are complete and correct
f. each safety requirement is completely satisfied (in the relevant POSS specification or by a compositional safety analysis).

44 Justification of an element of a specification by composition (Page 173)

A justification that an element of a parent specification was correctly derived by composing the behaviour/properties of its child specifications.

45 Justification of a directly substantiated behavioural element of a specification (Page 174)

A justification that an element of a specification is a correct statement of the verified behaviour of the POSS.

46 Justification of a (non-behavioural) directly substantiated property element of a specification (Page 175)

A justification that an element of a specification is a correct statement of the verified property of the POSS.

47 Justification of a directly substantiated element of an architectural specification (Page 177)

A justification that an element of an architectural specification is a correct statement of the verified property of the architecture.

48 The set of transitional activities that will be undertaken during the transitional stage (Page 180)

The set of transitional activities that will be undertaken during the transitional stage. These usually are defined in a transition plan, being the activities necessary to physically implement the change to the functional system, and comprise:

a. positioning new assets (non-operational) or modifying assets that are currently non-operational, so that they ready to be transitioned into operational use during a subsequent transitional stage
b. coordination activities internally and with external parties

c. activities that place prepared parts into the functional system, and/or remove parts from it, so changing (or 'transitioning') the functional system/service[17] , and so start a new transitional stage

d. clearing up – 'making good' and removing assets for disposal.

The set of transitional activities that the change safety case must justify is therefore a summation of these activities, considering that some activities temporally occur during the transitional stage, but are associated with clear-up and preparation for other transitional stages. Only the transitional activities in bullet c. above should impact the operational system/service.

If not shown to be adequately safe in isolation, the contribution of transitional activities to hazardous behaviour may have to be included in the safety analyses that predict safety performance during the relevant transitional stage.

49 Analysis of the impact of the transitional activities, and of potential deviations (Page 181)

An analysis to determine the effect of the transitional activities on the operational services. This includes the intended and unintended impact of the transitional activities, and also the impact of potential deviations from the intended transitional activities.

The identified impacts must either be argued to be mitigated so that the risk from them is acceptable, or else treated as (negative) contributors to the safety of the services provided during the transitional stage.

50 Recovery plan (possibly contained within transition plan) (Page 183)

A plan that defines, for a given transitional stage, the activities to undertake if a transitional activity results in an unintended outcome. There may be a single 'recovery plan', or a set of plans addressing recovery from each unexpected outcome that could occur during the transitional stage. The plans need to address at a minimum:

a. the response to all credible potential unintended outcomes from undertaking the transitional activities

b. the resultant services/functional system states following execution of each recovery plan scenario.

51 Justification of safety of potential services/functional system states during recovery and after recovery complete. (Page 183)

A justification that for every recovery scenario, the state that the services/ functional system enter when recovery is complete, and any transient states that occur during the recovery period, have been subject to appropriate safety analysis.

[17] These activities define the start of a transitional stage, as they put in place the operational system/service for that transitional stage.

52 Justification of acceptability of the safety of the transitional activities (Page 183)

A justification that the transitional activities are acceptably safe, which must address the impacts of:

a. the intended effects of the transitional activities that will transition the functional system/service at the start of the transitional stage

b. the unintended effects (side effects) of all transitional activities

c. the potential effects of unintended deviations from all transitional activities.

53 Claims other than the top-most claim (Page 186)

A claim is an assertion that something is true or not true. The claim can include any applicable limitations on its scope, for example the uncertainty in any stated value or property, or the duration for which the claim is valid.

For each claim, there is an associated confidence to which it has been demonstrated by its supporting arguments and evidence. This confidence may be explicitly stated, but currently it usually remains unstated, which is an inherent statement that the claim is sufficiently demonstrated by the supporting arguments and evidence. Part of the supporting argument (or perhaps a sub-claim) may explicitly demonstrate this sufficiency.

54 Inferences (Page 186)

The reasoning (rationale, argument, justification) that the presented evidence substantiates the truth of a claim.

55 Evidence (Page 189)

A managed artefact (e.g. a physical document, computer file, or material object), used by one or more inferences, having a known relationship to the subject(s) of the claim(s) being substantiated.

56 Argument (Page 189)

The complete set of claims, inferences and evidence in the change safety case.

57 Set of identified hazards (Page 191)

Hazards are functional system/service events or states, preferably defined at the point of service delivery, which can potentially result in an accident.

The set of identified hazards is the set of hazards identified in the course of the risk and safety analysis activities during the project that is implementing the change.

The set of identified hazards applicable to the change only includes those associated with the behaviour within the scope of the change. Any other identified hazards associated with the service(s) being changed do not form part of the set necessary for the change safety case.

58 Justification of the identified hazards (Page 192)

A justification that the set of identified hazards is complete and correct.

59 Set of accident trajectories (Page 193)

The accident trajectories identified in the course of the risk and safety analysis activities during the project that is implementing the change.

Accident trajectories link each hazard to each accident that could potentially result from that hazard, identifying the sequence of events occurring between the hazard and the accident. These events are the 'mitigations': circumstances or actions that intervene to prevent escalation to an accident, or to change the resultant accident to another one (intended to be less severe).

If mitigation means that the escalation is terminated without harm occurring, this is referred to as an incident.

60 Justification of the set of accident trajectories (Page 195)

A justification that the set of accident trajectories is complete and correct.

61 Mitigation analysis (Page 195)

The analyses undertaken to determine the effectiveness of the mitigatory features occurring on the accident trajectories, and their relationships to other mitigations and hazards.

Note: the scope of the mitigation analysis referred to here is restricted to mitigations associated with accident trajectories.

62 Justification of mitigation analysis (Page 196)

A justification that the mitigation analysis correctly identifies the effectiveness of the mitigations, and their relationships to other mitigations and hazards.

63 Set of identified accidents (Page 197)

The potential accidents identified in the course of the risk and safety analysis activities during the project that is implementing the change.

Accidents are events where harm is caused i.e. people are killed or injured. The set of accidents includes all events affected by the change that cause harm to any person.

The set of identified accidents applicable to the change only includes those that can result from the hazards associated with the behaviour within the scope of the change. Any other identified accidents associated with the service(s) being changed do not form part of the set necessary for the change safety case.

Events where harm is avoided are classified as incidents, and are not accidents.

Note: There may be other types of accident that cause alternative forms of harm (financial consequences, reputational consequences, environmental consequences) that are outside the scope of this safety case assessment guide.

64 Justification of set of identified accidents (Page 197)

A justification that the set of accidents is complete and correct.

65 Set of accident risks (Page 198)

The set of risks associated with the set of potential accidents identified in the course of the risk and safety analysis activities during the project that is implementing the change.

The risk of each potential accident is the combination of its predicted likelihood and the severity of the harm caused to a person or people (i.e. it is a safety risk).

Note: There may be other risks associated with an accident (financial business risk, reputational business risk, environmental risk) that are outside the scope of this safety case assessment guide.

66 Justification of the set of accident risks (Page 199)

A justification that the set of accident risks is complete and correct.

67 Set of top events (Page 200)

The top events of the causal analyses, which should match the identified hazards. The concept of top events is used to represent cases where there is a relationship more complex than one causal analysis to one hazard.

68 Justification of set of top events (Page 200)

A justification that the set of top events correctly relates to the set of hazards.

69 Identification of hazard causes (Page 200)

Hazard causes are the events and conditions that can combine to make the hazard occur, including any necessary combinations of events that must occur for the hazard to result.

The fundamental events and conditions should be identifiable behaviour or properties in the POSS specifications.

According to the nature of the functional system and the hazard, a causal model (e.g. fault tree analysis or failure mode and effect analysis) may be required to identify the causes of a hazard. Such analyses are based on the POSS specifications, which define the functional system and its architecture. The analyses may identify mitigations in the functional system architecture that may prevent an event causing a hazard, and the need for a combination of events to cause the hazard must be represented in the causal model.

70 Justification of identification of hazard causes (Page 202)

A justification that the identified causes of hazards are complete and correct.

71 Set of predicted occurrence rates of hazard causes (e.g. basic events in a fault tree) (Page 203)

For each fundamental event and condition in the causal model, the predicted occurrence rate must be identified to permit prediction of the hazard rate.

72 Justification of set of predicted occurrence rates of hazard causes (e.g. basic events in a fault tree) (Page 204)

A justification that the predicted occurrence rates of the fundamental events and conditions are correct and trustworthy.

73 Set of predicted hazard occurrence rates (Page 205)

The predicted rates of occurrence of the hazards, determined from an understanding of how hazard causes can combine to make the hazard occur, and the predicted rates of occurrence of these causes.

74 Justification of set of predicted hazard occurrence rates (Page 205)

A justification that predicted rates of occurrence of the hazards are correct.

75 Cause-consequence models e.g. a set of bow tie models, one for each hazard (Page 206)

The cause-consequence model of a hazard is the totality of the safety model associated with the hazard, including:

a. The causal model, from fundamental events and conditions via the top event to the hazard
b. The hazard
c. The consequence model, including the accident trajectories, mitigations and accidents
d. The associated calculations to predict occurrence rates.

76 Justification of overall properties of cause-consequence models (Page 208)

A justification that the cause-consequence models are complete and correct.

Appendix D – Candidate assessment activities

This appendix defines the candidate assessment activities for specific individual Phases/Steps. Further candidate assessment activities that may be used in more than one Phase/Step are given in:

a. Appendix E – Candidate assessment activities for elements of arguments

b. Appendix F – Candidate assessment activities for safety analysis models.

Phase 3 Topic Tables

Description of functional system and service, and changes to be made

The change safety case should provide adequate and correct descriptions of:

a. the functional system and service to be changed
b. the transitional stages[18] including
    i. the service(s) offered during that stage, if any
    ii. the modifications to be made to the functional system and any change effected collaboratively in the service environment during that stage.

Descriptions are summary in nature, and so the assessor must not view them as the definitive specification of the service, the parts of the functional system or the change. Whilst the assessor will have read these descriptions during the familiarisation Phase, it is only now, during this assessment Phase, that their adequacy can be judged.

The assessor should determine whether the provided descriptions are appropriate to communicate the change safety case to a variety of stakeholders, who have different competences and foreknowledge of the change. For example, they must be correct without being too long, and so they must selectively summarise the important aspects of their subject.

The assessor should determine whether the descriptions cover the important features of the change. These will address the service, operational environment, functional system, subsystems, architectures, and the changed and impacted POSSs for the transitional stages used to implement the change, and their relationship to the safety of the service.

When undertaking the planned assessment activities, the assessor should check that the descriptions appear to be correct. The assessor should note any items of interest or concern and subsequently check the relevant specifications.

Descriptions that are poorly written, incorrect or have significant omissions will mislead stakeholders reading the document, and may be a negative indicator of the Service Provider's understanding of the change. Such defects are therefore significant.

The contiguity check of the Installation, Commissioning, Transition and Recovery Plans in Phase 4 is a deeper check than the contiguity check of their descriptions.

[18] The final operational state is inherently described by the last transitional stage, which implements the final operational state.

1	**Descriptions of the existing functional system and service, before the proposed change**
1.1	General adequacy. Check the general adequacy of descriptions as an introduction to the existing functional system and service, for example: a) clarity, correctness, consistency, readability, sufficiency b) coverage of services, their characteristics and operational environment c) coverage of functional system architecture e.g. connectivity and physical location d) coverage of functional system behaviour and performance e) coverage of changed and impacted POSSs f) absence of assumption of prior knowledge
1.2	Scope. Check that the descriptions address the following, as appropriate: a) the existing service(s) changed or impacted by the change b) the constituent systems, interfaces and environment c) interactions with other services via interfaces or the environment d) the potential accidents associated with the service(s), and the accident sequences that could lead to those accidents e) the architectural safety features of existing functional system/service, including inherently safe or fail-safe features, redundancy and diversity, recovery mechanisms, etc f) the safety concerns (causes, mitigations, accident sequences, etc) or issues that are most important, or require most careful management g) the operations, phases, modes, uses, scenarios, etc which must be safe/affect safety h) the notable threats and challenges to the provision of the service, including issues such as: resource availability, complexity of human tasks i) the existing safety requirements j) support systems including training, data preparation, and test and development systems.
1.3	Correctness. Check that: a) the descriptions given reflect the Service Provider's specific service(s), i.e. the specific Service Provider's specific usage, not a generic usage b) the descriptions reflect the service as it exists just before the change is implemented c) the descriptions appear to be consistent with the specifications.

2	**Descriptions of the change**
2.1	General adequacy. Check the general adequacy of descriptions as an introduction to the change, for example: a) clarity, correctness, consistency, readability, sufficiency b) coverage of services, their characteristics and operational environment c) coverage of interaction with other services via interfaces or the environment d) coverage of functional system architecture e.g. connectively and physical location e) coverage of functional system behaviour and performance f) coverage of changed and impacted POSSs

	g) absence of assumption of prior knowledge
2.2	Impact. Check that the change descriptions address parts of the functional system/service that will be impacted by the changes, not just the modifications that implement the change.
2.3	Scope. Check that the descriptions of the change address the following, as appropriate: a) the changes to all services changed b) the changes to the parts of the functional system, interfaces and environment c) the changes in interactions with other services via interfaces or the environment d) the consequential effects on other unmodified services, systems and parts of the functional system e) the changes to the functional system behaviour f) the changes to the potential accidents associated with the service(s), and the accident sequences that could lead to those accidents g) the changes to architectural safety features of the functional system/service, including inherently safe or fail-safe features, redundancy and diversity, recovery mechanisms, etc h) the effect of the change on the pre-existing safety concerns (causes, mitigations, accident sequences, etc) or issues that are most important, or require most careful management i) the safety concerns (causes, mitigations, accident sequences, etc) or issues that are most important, or require most careful management during and following the change j) the changes to the operations, phases, modes, uses, scenarios, etc which must be safe/affect safety k) the changes to the notable threats and challenges to the provision of the service, including issues such as: resource availability, complexity of human tasks l) new safety requirements m) the changes to existing safety requirements n) transitional stages
2.4	Changes to behaviour/properties. Check that there is a description of the how the functional system will change, considering the effects of applicable operational mechanisms, such as: a) intended behaviour b) failure modes and failure rates c) failure detection and correction d) failure propagation or tolerance e) scheduled and corrective maintenance activities f) intended interface conditions, ranges and protocols g) proximity of POSSs or environmental elements (e.g. visual reference points) h) critical thresholds (e.g. of resource usage) i) stress, capacity or loading j) positive or negative feedback effects.
2.5	Correctness. Check that: a) the change is described specifically for the Service Provider's service(s), i.e. the specific Service Provider's specific usage, not a generic usage b) the descriptions appear consistent with the specifications

	c) the descriptions appear consistent with the Installation, Commissioning, Transition and Recovery Plans.

3	**Descriptions of transitional stages**
3.1	Check that the approach for implementing the change is described, e.g. transitional stages.
3.2	Check that the descriptions are sufficient to understand the functional system and service during each transitional stage, as in 'Descriptions of the existing service, before the proposed change' and 'Descriptions of the change' above.
3.3	Check that there is a clear description of the service(s) to be provided (if any) during each transitional stage.
3.4	Check that there is a clear description of the transitional activities to be undertaken to implement changes during each transitional stage.
3.5	Check that the changes described form a contiguous set of changes from the pre-change functional system/service to the completely changed functional system/service.
3.6	Check that the transitional activities described together appear to implement the complete change.

4	**Justification of descriptions**
4.1	Check that there is a satisfactory argument that justifies the adequacy of the descriptions i.e. check that the argument is coherent, suitably convincing, etc.
4.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
4.3	Verification activities. Check that there is a justification that verification activities were adequate to verify: a) the correctness of the descriptions of the existing service before the proposed change, the change and the transitional stages b) that the descriptions are consistent with the specifications c) that the descriptions are consistent with the Installation, Commissioning, Transition and Recovery Plans. d) that the descriptions are comprehensible by someone not involved in developing or assuring the change e) that the descriptions have sufficient scope and detail to communicate the necessary material f) that the descriptions address the needs of all the safety case stakeholders g) that the descriptions were verified in accordance with the Service Provider's SMS

5	**Installation, Commissioning, Transition and Recovery Plans (contiguity check)**
5.1	Check that the changes addressed in the Installation, Commissioning, Transition and Recovery Plans form a contiguous set of changes from the pre-change functional system/ service to the completely changed functional system/service.

5.2	Check that the complete set of activities described in the set of plans appears to change all necessary parts of the functional system to implement the complete change.
5.3	Check that the plans appear consistent with the descriptions of the transitional stages.

Claim of acceptability of predicted safety performance for all changes proposed in the change safety case

The change safety case must make a claim that the predicted safety performance associated with each transitional stage is acceptable.

At this top level, the supporting arguments are not checked. It is just necessary to check that this claim is made, and that this claim is supported by individual equivalent claims for each transitional stage.

The assessor determines the planned transitional stages from the descriptions in the change safety case and transition plans (part of the Installation, Commissioning, Transition and Recovery Plans).

6	**Top-most claim of the change safety case**
6.1	Check that the top-most safety claim of the change safety case is essentially that 'the predicted safety performance associated with the changed service, and all transitional stages, is acceptable, and the changes will be made safely'.
6.2	Check that the top-most claim is clear and well-formed.
6.3	Check that the top-most claim is NOT ambiguous or vague, and does not use undefined terminology.
6.4	Check that the top-most claim is evidently made on the basis of equivalent claims for each transitional stage.
6.5	Check that the set of top-most claims for the safety of the transitional stages appears to form a continuous set.

Uncertainties in the change safety case

The change safety case must argue that there are no outstanding uncertainties that invalidate the change safety case. This should include a summary of the overall situation, discussing any major uncertainties and how they have been addressed, and referencing out to any detailed discussion of specific issues.

During this top level assessment Phase, the assessor checks the issues highlighted seem to have been reasonably addressed, and include any significant uncertainties of which the assessor is already aware. The intent is to check the most important issues, which should be highlighted by the change safety case summary. Detailed individual arguments regarding uncertainty are checked at the point they are encountered during other assessment activities.

The necessity of addressing uncertainty varies, according to the importance of the uncertainty in terms of supporting the overall safety claim. Higher

uncertainty may be tolerable when the associated safety risks are lower (e.g. if there is short exposure time, and a reduced service). For some changes no such discussion will be required. The discussion may address some uncertainties for a specific transitional stage, and others across all stages.

7	Justification of the treatment of uncertainties in the change safety case
7.1	Check that there is a satisfactory argument that justifies the adequacy of the treatment of uncertainties in the change safety case i.e. check that the argument is coherent, suitably convincing, etc.
7.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
7.3	General adequacy. Check the general adequacy of the justification, for example: a) clarity, correctness, consistency, readability, sufficiency b) coverage of the scope of the uncertainty c) absence of assumption of prior knowledge
7.4	Check that the justification explains how the change safety case addresses the possibility of unanticipated circumstances, if necessary, and shows that the risk from this is acceptable due to the low probability of these circumstances existing or happening, and the ability of the functional system to response. For example: a) the functional system being in an unanticipated state b) unanticipated interactions with another system
7.5	Check that the justification identifies and discusses all types of uncertainties that the change safety case needs to consider, and explains where and how the change safety case considers them. These uncertainties may relate to: a) quantitative aspects, for example in required, measured or predicted safety performance, or specifications b) correctness, e.g. regarding models and methods used c) the validity of assumptions d) potential changes in the environment e.g. weather, traffic levels and patterns e) knowledge and understanding f) the design of a POSS (e.g. material properties, defects, dynamic behaviour) g) knowledge of the environment h) data i) margins of safety j) activities of external agencies, e.g. construction projects k) the potential for technical failure to successfully introduce the change, under which circumstance the recovery plans would have to be instigated l) the potential for not implementing all planned transitional stages, perhaps for financial/ business reasons, or failure of the improved service to stimulate the expected response from other parties in the business environment.
7.6	Check that the justification explains how the change safety case addresses identified uncertainties, e.g. by: a) generating additional evidence b) other mitigating measures

	c) conservatism when drawing conclusions from the associated analyses or arguments).
7.7	In the case of novel systems, large systems, changes to unsupported legacy systems, or where novel arguments, check that the justification explains how the change safety case addresses 'unknown unknowns'.
7.8	Check that the justification explains how the change safety case evaluates the consequences and significance of any remaining uncertainty.
7.9	Verification activities. Check that there is a justification that verification activities were adequate to verify that uncertainty has been adequately addressed in the change safety case.

Justification that the change is a good change

This topic addresses issues that are not directly indicative of the acceptability of the safety of the change, but are associated with the wider responsibilities of the CA to challenge and possibly reject inappropriate changes, even if safe. These issues, necessary for the change safety case to be acceptable, may be stipulated by applicable regulations, standards, etc., or suggested by the role of the CA.

Additionally, the first set of candidate assessment activities defined here include checking that the Service Provider has complied with regulations concerning using approved change management procedures.

The planner considers more widely whether any specific standards and regulations are applicable to the change or changed service, and whether the CA must confirm compliance as part of the assessment of the change safety case. If so, the planner allocates these checks to either this Phase, or to Phase 5, when individual transitional stages are assessed.

Safety performance monitoring is not necessary to predict the safety of the change, but it is required to feed operational safety performance information to the Service Provider's SMS. The monitoring of the operational system and the support systems (e.g. the maintenance functions) against the performance specified in their POSS specifications may be addressed either as monitoring of safety requirements (9.13 on page 129) or as monitoring of assumptions or constraints (9.14 on page 129).

In some domains the CA may be required to approve the Service Provider's SMS procedures, including change management procedures, before the Service Provider uses them for a change, and so the change management procedures may be assumed to be valid.

8	**The change management procedures used, as claimed by change safety case**
8.1	Check that the change safety case identifies which change management procedures have been followed during the development of the change and the change safety case.
8.2	Check that the change management procedures that were followed were approved for use by the CA (or other authority if permitted by the applicable regulations).

8.3	Check that the change management procedures followed are from the SMS applicable to the Service Provider's services being changed, not another Service Provider, a different service, or some generic source.
8.4	Check that there is nothing about the change that makes the change management procedures from the Service Provider's SMS, inappropriate for the change (e.g. technologies are used that are not addressed by the Service Provider's SMS).

9	**Justification that the proposed change is a good change**
9.1	Check that there is a satisfactory argument that justifies that the proposed change is a good change i.e. check that the argument is coherent, suitably convincing, etc.
9.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
9.3	Standards and regulatory compliance. Check that: a) the change safety case shows that it complies with regulatory requirements b) the change safety case shows that the changed functional system and service complies with all the CA's regulatory requirements c) the change safety case shows that all necessary approvals have been gained (e.g. planning permission, radio licenses) d) the change safety case shows that the changed functional system and service complies with other regulators' and legal requirements, for example: Interoperability, Technical Files, Health and Safety, Wiring regulations, Wireless & Telegraphy. e) the change safety case shows that the changed functional system complies with other applicable technical standards (those not mandated by regulations)
9.4	Use of good or best practice. Check that: a) the change safety case shows that good or best practice has been followed in development and implementation b) the change safety case shows that good or best practice has been followed in risk assessment and mitigation, safety assurance, etc c) the change safety case shows that the planned change is such that good or best practice will be followed in operation d) where applicable the change is similar to previous successful changes (made by the Service Provider or anyone else) e) where the change is similar to unsuccessful changes (made by the Service Provider or anyone else), the change safety case justifies why the change will be successful this time f) where applicable 'lessons learned', both good and bad, from similar changes (made by the Service Provider or anyone else) have been taken into consideration.
9.5	Implementation of risk principles (e.g. SFAIRP, GAMAB). Check that: a) the change safety case justifies that appropriate risk principles have been applied appropriately b) the change safety case justifies the omission of possible options, alternative safety arrangements, etc.
9.6	Check that the change safety case addresses how the changed functional system and service will be robust with respect to anticipated changes (e.g. by accommodating changes to interfacing systems and services).

9.7	Check that the change safety case addresses whether the change correctly accommodates predicted changes to the operating environment, and those anticipated in strategic industry forecasts. If not, determine whether this is a shortcoming.
9.8	Check that the change safety case addresses whether the change correctly accommodates anticipated changes to the (local) environment of the POSSs. If not, determine whether this is a shortcoming.
9.9	Check that the change safety case justifies that the transitional activities have been designed to minimise the associated risks
9.10	Check that the change safety case justifies that the maintenance and support activities have been designed to minimise the associated risks.
9.11	Acceptability of planned service. Check that the change safety case justifies that: a) contingency arrangements, service robustness, and service continuity are sufficient to continue providing an adequate (and safe) service in case of: i) failures ii) emergency or threat iii) external event (e.g. weather, road accident). b) the changed service does not adversely affect any anticipated changes to the operating environment and/or interfacing systems c) the changed service does not adversely affect any other service, or any anticipated changes to such services d) if the change has an impact on other services, that: i) the impact is necessary or desirable ii) the change has been coordinated with the responsible Service Provider(s).
9.12	Check that the change safety case identifies any necessary impact on the Service Provider's SMS, arising from the change. [It is not within the scope of this assessment to check the implementation of these impacts].
9.13	Check that the justification shows that the in-service safety performance monitoring system (required to support the overall SMS) will correctly monitor the changed service, including: a) Monitoring of predicted emergent properties, as specified in the safety requirements b) Monitoring of mitigation performance e.g. rate and scope of effectiveness c) Monitoring for occurrence of unanticipated circumstances (e.g. violation of assumptions) or emergent properties d) Arrangements for how the monitoring results in a) to c) above will be used e) Criteria for judging the acceptability of the monitoring results e.g. predetermined thresholds derived from the change safety case f) Reporting acceptability of monitoring results g) Resulting action if monitoring results not acceptable
9.14	Check that the justification shows that necessary monitoring systems are defined to detect if the service violates the conditions and constraints defined in the change safety case, for example: a) Monitoring human compliance with procedures, etc. b) Monitoring the operational environment. c) Monitoring the correctness of assumptions made in the change safety case. d) Monitoring that operation/service remains within the scope or constraints that the change safety case assured.

e) Periodicity or events that initiate reviews of the results of monitoring.

f) Analysing and reporting the results of these monitoring activities.

Phase 4 Topic Tables

Installation, Commissioning, Transition and Recovery Plans

The change safety case must include adequate plans for the transition to operational use of the changed functional system, including the plans to recover to a safe state, should the change not be successfully implemented as intended.

The assessor must identify whether the transitional activities are addressed in a single 'transition plan', or whether aspects such as integration, commissioning and recovery have separate plans. In such cases, there is usually still a transition plan that addresses all other necessary transitional activities, for example:

a. Decision points
b. Coordination internally and with external parties
c. Collection and analysis of assurance evidence (conducted as part of in-service performance monitoring)
d. Training for operators and engineers, and preparation of the facilities required for this
e. Issuing of procedures
f. Individuals' and organisations' responsibilities for undertaking the activities
g. Record keeping
h. Acquisition of required resources and tools
i. When the defined activities are to be undertaken (addressing concurrent activities, time of day, the services being offered at the time of the activity).

The Service Provider may decide to implement the change in several transitional stages, with installation and commissioning of parts of the overall change taking place during these stages. The Service Provider may also need to define transitional stages to permit collection of evidence of safety. The Service Provider must also define a way to recover the functional system into a known state that has acceptable risk (usually by regressing to the previous state), if a transitional activity or transition to the next transitional stage cannot be successfully completed.

For each of these transitional stages, as well as addressing all required transitional activities (as above), these plans need to identify the functional system and service in operation during the stage (which cannot be affected by the transitional activities taking place during the stage).

The assessment activities should also determine whether the change safety case demonstrates that there are adequate arrangements to ensure that the change to the functional system is made correctly. The planner must take account of the extent to which this is necessary, which varies according to factors such as:

a. the extent of the installation or removal activity - there may only be minor adjustments, or complete new systems or structures may be installed

b. the complexity or novelty of the installation or removal activities

c. the required performance of the installation or removal activities, e.g. high precision or short timescale

d. the likelihood of error in the installation or removal activities.

10 Installation, Commissioning, Transition and Recovery Plans	
10.1	General adequacy. Check the general adequacy of the plans, for example: a) clarity, correctness, consistency, readability, sufficiency b) coverage of the scope of the change c) absence of assumption of prior knowledge
10.2	Check that the Installation, Commissioning, Transition and Recovery activities appear practical.
10.3	Check that the plans reflect good practice.
10.4	Check that the plans identify, and are consistent with, any constraints on Installation, Commissioning, Transition and Recovery for this change.
10.5	Current functional system/service. Check that the plans reflect the actual state of the functional system/service (insofar as required to plan the change, as opposed to analyse the safety of the changed service), in that: a) The plan defines or references an adequate definition of the current operational environment, service, functional system and its POSSs. b) The plan takes account of the physical condition of the POSSs. c) The plan takes account of the presence or absence of optional fittings, connections, etc. d) The plan takes account of any potential discrepancies between the actual functional system POSSs present and the declared build state/build records.
10.6	Check that the plans identify the functional system and service before and during the transitional stage (e.g. by specifying the applicable build state or specifications), including any special provisions or mitigations (e.g. reduced traffic flow).
10.7	Check that the transitional activities for each transitional stage are consistent with implementing the required change for the transitional stage[19].
10.8	Check that the set of Installation, Commissioning, Transition and Recovery Plans together define transitional activities that appear to implement the complete change.
10.9	Activities. Check that the plans define all the transitional activities taking place during the transitional stage, including: a) Training for operators and engineers, and the facilities required for this b) Issuing of procedures c) installation, commissioning and connection of new equipment and interfaces. d) changes to, and commissioning of, existing equipment. e) Removal of replaced or obsolete equipment.

[19] The transitional activities should be consistent with the specifications for the functional system before and after each transitional stage, which are assessed in Phase 5 Step 4.

	f) Initiating the services to be provided during the transitional stage, and are provided while the other transitional activities are undertaken. g) Communication with other stakeholders concerning transitional activities, at the start of and during the transitional stage h) Internal coordination to synchronise and sequence the transitional activities i) Co-ordination with other changes j) Verification and assurance activities, including checking that the systems have been changed as planned
10.10	Check that the organisations carrying out Installation, Commissioning, Transition and Recovery activities have sufficient: a) verification procedures to confirm that the changes have been made as planned b) technical capabilities to carry out the planned activities properly c) financial resources to carry out the planned activities properly d) capabilities to carry out the planned activities properly in the time stated e) management commitment to carry out the planned activities properly f) instructions to carry out the planned activities properly g) procedures and controls for the parts used to carry out the planned activities, to ensure that the correct parts are used, and are in the correct condition (stores management).
10.11	Where the required quantities of the resources or tools makes their timely acquisition questionable, check that there is sufficient description or evidence that they will be acquired successfully. Successful acquisition may be questionable due to quantity, timing, scarcity, novelty, the item being bespoke or having a long lead-time, or there is a likelihood of significant error in the supply of the resource/tool.
10.12	Where the required performance of the resources or tools makes their acquisition questionable, check that there is sufficient description or evidence that the acquired resources or tools will have the required performance e.g. accuracy.
10.13	Check that, where the properties of the required resources or tools are particularly important (e.g. when the resources or tools are used for verification that the change has been installed correctly), the plan (or change safety case) provides sufficient evidence of verification of these properties (or describes how this evidence will be produced).
10.14	Check that the physical logistics associated with the Installation, Commissioning, Transition and Recovery activities are possible.
10.15	Check that the plans define the criteria for: a) deciding to start transitional activities b) deciding that transitional activities are completed c) deciding to start the next transitional stage
10.16	Check that decision criteria include, if appropriate: a) confirmation that enabling changes/projects have completed b) the publication or communication of information about the change c) the existence of signed contracts, e.g. for supplied services d) acknowledgement of notifications e) decisions associated with collection of safety performance evidence.
10.17	Check that the plans define recovery or contingency arrangements if the intended changed state is not achieved.

10.18	Check that the plans define clear criteria for recognising when the planned recovery arrangements should be invoked.
10.19	If the changed service introduces a new concept of operation (different from the existing one), check that the change is accommodated by all actors interacting with the service.
10.20	Collection of safety performance evidence. Where evidence of safety performance is to be collected (as part of safety performance monitoring) during a transitional stage: a) Check that the plans (or modified safety performance monitoring procedures) define any evidence-collecting and analysis activities at any stage, and that they are consistent with any outstanding evidence of behaviour of a POSS or other system[20]. b) Check that the evidence that is to be generated is stated clearly c) Check that the acceptance criteria for the results are defined unambiguously. d) Check that the conditions under which the evidence is collected do not invalidate the evidence e) Check that decision criteria for completion or starting a transitional stage include those associated with successful evidence collection.
10.21	Completion of transitional activities. Check that: a) The plans define arrangements and criteria for deciding the transitional activities are complete. b) the plans define acceptance and handover activities and responsibilities.
10.22	For each defined activity, check that: a) Individuals and organisations undertaking the activity are defined. b) Responsibilities for undertaking the activity are defined. c) adequate procedures and methods are defined where appropriate d) the necessary records are defined for the activity e) any resources required are: i) defined ii) specified adequately e.g. a full specification may be required if they are novel, or need to have specific or unusual properties iii) available, in consideration of other potential demands for the resource. f) the plans define when the defined activities are to be undertaken g) concurrent activities are considered h) time of day is considered i) the services being offered at the time of the activity are considered j) other changes being made at the same time are stated and accounted for by the plans k) any uncertainties or assumptions are identified and are managed.
10.23	Documentation. Check that the plans: a) define which documents will be produced as a result of the transitional activities b) define any updates to the change safety case to be made at each stage
10.24	Check that the plans contain sufficient provisions to address any uncertainties identified by the Assessor.

[20] See candidate assessment activity 33.13 on page 163, in 'Justification of the specifications for the POSSs within the scope of the change associated with the transitional stage'.

10.25	Check that the set of Installation, Commissioning, Transition and Recovery Plans appear to be complete and consistent, and together the plans define transitional activities that appear to implement the complete change.

11 Justification of Installation, Commissioning, Transition and Recovery Plans	
11.1	Check that there is a satisfactory argument that justifies the adequacy of the Installation, Commissioning, Transition and Recovery Plans i.e. check that the argument is coherent, suitably convincing, etc.
11.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
11.3	Check that the justifications, so far as appropriate, show the completeness and suitability of the plans, in respect of the issues above, regarding Installation, Commissioning, Transition and Recovery Plans.
11.4	Check that the justifications, so far as appropriate, show the completeness and suitability of the planned activities to ensure that the correct change is made.
11.5	Check that the justifications show that appropriate support systems have been made available for stages where an operational service is offered (any change to these should be identified as part of the scope of the change).
11.6	Check that the justifications, so far as appropriate, show that the plans define adequate activities to collect evidence necessary to support the change safety case for later implementation stages and/or to demonstration that transition criteria are met.
11.7	Check that the justifications show that the plan is valid in this particular instance, when a generic plan is to be used.
11.8	Check that the justifications show that the effects that Human Factors can have during implementation of a change (e.g. error-prone activities) are accounted for.
11.9	Check that the justifications, so far as appropriate, show that appropriate controls are in place to ensure that the activities are conducted in accordance with the plan
11.10	Check that the justifications address the suitability of external coordination arrangements.
11.11	Check that the justifications address the suitability of arrangements to publicise the change.
11.12	Check that the justifications address the suitability of internal coordination arrangements to synchronise and sequence transitional activities.
11.13	Check that the justifications, so far as appropriate, show that necessary resources will be available.
11.14	Check that the justifications show that the plan accounts for the implications of the timing of change implementation with respect to other changes and with regular or exceptional operational issues.
11.15	Check that the justifications, so far as appropriate, show that the plans are credible.
11.16	Check that the justifications, so far as appropriate show that the plans take account of potential deviations from the planned transitional activities[21].

[21] Safety justifications for the transitional activities are addressed in Phase 5 Step 7.

Phase 5 Step 2 Topic Tables

Service, functional system and change descriptions

As this Step is usually conducted before the assessor has examined specifications and plans for the stage, it may not be possible to properly conduct all these checks. However, it makes sense for the assessor to examine the descriptions from the perspective of someone unfamiliar with the material to check for clarity. Correctness aspects may be better checked at Step 6 of Phase 5, where the assessor is instructed to revisit these checks if necessary.

The change safety case should clearly describe the pre-change functional system and service, and the functional system and service provided at each transitional stage. It should also describe the basis upon which the safety criteria were derived for each transitional stage.

A change is often implemented with a single transition, but can be implemented as a sequence of transitional stages, where the last fully implements the intended change. The change safety case should describe the changes made by transitional activities at each stage. The change safety case may describe the whole change in one place, or else describe the change at different levels (e.g. for each individual system, or for each stage).

The descriptions must be consistent, and prove to be correct with respect to the detail of the change safety case.

The same criteria used for descriptions of the overall service and change are applicable to individual stages, and so candidate activities 12.2 and 12.3 reference the tables in Phase 3, rather than repeating them here.

12 Descriptions of service, functional system and change before the transition, and change to be made	
12.1	Check that the approach for implementing and transitioning the change is described.
12.2	Check that the descriptions are sufficient to understand the functional system and service before the transition, as in 'Descriptions of the existing functional system and service, before the proposed change' on page 122.
12.3	Check that the change to be implemented in the transition is described in the same way as 'Descriptions of the change' on page 122.
12.4	Check that the descriptions appear to be consistent with the Installation, Commissioning, Transition and Recovery Plans.
12.5	Check that the descriptions are consistent with those of the overall change.
12.6	Check that the described basis on which the safety criteria were set for this transitional stage appears to be valid.
12.7	Check that the descriptions reference or outline the physical security measures that restrict access to prevent malevolent modification of the functional system.
12.8	Check that the descriptions have been verified adequately (see Justification of descriptions, page 124).

Support system descriptions

The change safety case must justify that necessary support systems, or changes to existing support systems, associated with the change have been correctly identified and their provision planned. The changed support systems must support ongoing operation of the changed and impacted parts of the operational system.

It is possible that no changes are required to existing support systems, to provide continued support to the changed operational system.

The assessment activities should be designed to determine whether the change safety case adequately addresses changes to support systems with respect to the proposed change to the operational system. The planner must take account of the extent to which the change safety case needs to address the adequacy of changed support systems, which varies according to factors such as:

a. the scope of the change - there may only be minor adjustments to existing support systems, or a complete new support service may be needed

b. the complexity or novelty of the changed support systems

c. the required performance of the changed support systems, e.g. high availability

d. the likelihood of significant error in the support systems.

For changes where the change safety case needs to rigorously address support systems, the planner can choose to:

a. include assessment activities for the assessor to determine whether the descriptions adequately justify the sufficiency of the support systems

and/or

b. repurpose the candidate assessment activities for the safety of transitional activities (Phase 5 Step 6) to assess the adequacy of maintenance and other support activities, to supplement the candidate assessment activities below.

The planner should also take account of the phasing of the introduction of changes to the support systems with respect to the transitional stages. It may be that some transitional stages have no changes to the support systems. It is quite common for change projects to introduce all such changes at once, perhaps during the first or final transitional stage.

The descriptions of the changes to the support systems may address all the changes associated with the change, or there may be separate plans or descriptions for each transitional stage. The planner should ensure that activities check that changes to support systems will be introduced before they are required to support the operational system.

The specifications (rather than descriptions) for changed and impacted support systems (including new support systems) are assessed in Phase 5 Step 4.

13 Descriptions of changed support systems	
13.1	General adequacy. Check the general adequacy of the descriptions, for example: a) clarity, correctness, consistency, readability, sufficiency b) coverage of the scope of the change (i.e. the changed and impacted parts of the support system) c) absence of assumption of prior knowledge.
13.2	Check that the descriptions reference the specifications of the support systems (which are assessed under 'Specifications of the parts associated with arrangements for support of the operational system' on page 155), if required.
13.3	Check that the descriptions reflect good practice for support systems.
13.4	Check that the descriptions identify, and are consistent with, operational constraints.
13.5	Check that changes to support systems will be introduced before they are required to support the operational system.
13.6	Activities. Check that the descriptions address support systems for all the necessary activities to support ongoing operation of the changed and impacted parts of the operational system, including: a) training for operators and engineers, and the facilities required for this b) issuing of procedures c) maintenance and inspection activities d) regular database or adaptation updates, including how safety assurance will be undertaken e) updates occurring according to an externally-imposed schedule.
13.7	For each defined support system activity, check that the descriptions address: a) the individuals and organisations undertaking the activity b) responsibilities for undertaking the activity c) procedures and methods d) the necessary records for the activity e) any resources required f) when the defined activities are to be undertaken g) issues arising from concurrency of activities h) issues arising from time of day i) issues arising from the services being offered at the time of the activity
13.8	Training. Check that the descriptions address all necessary support systems to provide training of operators and engineers, including: a) refresher training regarding normal operations b) training for emergencies and unusual circumstances, including Fallback operation, and contingency.
13.9	Check that the change safety case defines how it will be maintained (update, access, archival and linkage to safety performance data), and defines associated responsibilities.

13.10	Check that management system arrangements (including responsibilities and authorities) to support the changed service are specified. If not, determine whether this is a significant issue.
13.11	Check that the descriptions address changes to the support systems (see examples in candidate assessment activity 32.5 on page 156).
13.12	Check that the descriptions have been verified adequately (see Justification of descriptions, page 124).

Relationship of the change safety case to Service Provider's SMS

The change safety case may address this topic collectively, possibly for all the stages together. The planner should consider whether the assessment of another stage has already sufficiently covered this part of the change safety case.

As it is not within the scope of the assessment to determine compliance with the SMS procedures, it is only necessary to determine whether the safety criteria, used to judge the acceptability of the change, were defined in accordance with the requirements of the SMS.

The change safety case may establish safety criteria (assessed in Phase 5 Step 4) for the changed service based on either risk or rates of occurrence of hazardous events. The candidate assessment activities in this table are only applicable if risk is used as the basis of the safety criteria. If any other approach to define the safety criteria is used, then the assessor should check that the approach is compliant with any provisions made in the Service Provider's SMS, if any.

14 Risk tolerability and classification scheme used in change safety case	
14.1	Check that the change safety case appears to correctly identify the parties that may be harmed (including those associated with the service and non-participants in the environment), from the declared scope of the change.
14.2	Check that the change safety case appears to correctly identify the parties that may be harmed (including those associated with the service and non-participants in the environment), during implementation of the change.
14.3	Check that the change safety case identifies risk classification and tolerability criteria for the potentially harmed parties.
14.4	Check that the risk classes are defined in terms of severity and likelihood of potential accidents, or surrogates for accidents.
14.5	Where risk classes are defined in terms of surrogates for accidents, check that surrogates are defined for all types of potential accident associated with the change.
14.6	Check that the risk severity and likelihood schemes are clearly applicable and valid for the potential accidents associated with the change, e.g. measurement units and ranges are compatible with the service.
14.7	Check that the relationship between the risk classification and the tolerability criteria is clear and correct.
14.8	Check that the risk tolerability criteria are stated in terms that support the type of argument made in the change safety case for evaluating the acceptability of the predicted risk associated with the changed service. They must support the 'Evaluation of acceptability

	of the predicted safety performance associated with the changed service, during the transitional stage being assessed' on page 166 (topic 38).
14.9	Check that the risk classification and tolerability criteria are derived from (or using a method stipulated in) the Service Provider's SMS.
14.10	Check that the risk classification and tolerability criteria used are those for the Service Provider's services being changed, not another Service Provider, a different service, or some generic source.
14.11	Check that there is nothing about the change that makes the risk classification and tolerability criteria from the Service Provider's SMS, inappropriate for the change (e.g. a change that takes the provided services beyond those envisaged when the Service Provider's SMS was created).

Claim of acceptability of predicted safety performance for the stage

The change safety case must make a claim that the predicted safety performance associated with the stage is acceptable.

The supporting arguments are not checked during this Step. It is just necessary to check that this claim is made.

15 Top-most safety claim for the stage	
15.1	Check that there is a top-most safety claim for the stage.
15.2	Check that the top-most safety claim for the stage is essentially that 'the predicted safety performance associated with the service is acceptable, and the transitional activities during the transitional stage will be conducted safely'.
15.3	Check that the top-most claim for the stage is clear and well-formed.
15.4	Check that the top-most claim for the stage is NOT ambiguous or vague, and does not use undefined terminology.
15.5	Check that the top-most claim is evidently made on the basis of supporting arguments.

Phase 5 Step 3 Topic Tables

Declaration of the scope of the change

The change safety case must specify the scope of the change (the changed and impacted POSSs) for the transitional stage. The change safety case can define this scope from the initial (pre-change) state or from any other preceding transitional stage. The safety analyses (setting safety criteria and predicting safety performance) have to be consistent with this scope - a cross-check may already have been made by the assessor in Phase 4 that the sum of the transitional stages' scopes encompasses the whole scope of the overall change.

Additionally, the change safety case must justify that it has correctly identified all the changed and impacted POSSs.

16 Lists of changed and impacted Parts of the Operational and Support Systems (POSSs)	
16.1	Check it is clear against which functional system/service baseline build state the changed and impacted POSSs have been identified.
16.2	Check that there is a list[22] of: a) POSSs that have changed[23], but their behaviour (in their specification) did NOT change b) POSSs that have changed, and their specification has been changed (which includes new and removed POSSs) c) POSSs that have NOT changed, but whose specification has been changed due to a change in the POSS's context, which is either a change in the attributes of what traverses the POSS's interfaces and/or in the access to resources shared with other POSSs d) POSSs that have NOT changed, but whose specification has been changed due to a change in their safety requirements.
16.3	Check that the listed POSSs appear to be uniquely identifiable parts of the operational and support systems.
16.4	Check that the lists of POSSs appear to be complete, considering: a) the reason for the change b) the implications of the interactions of the POSSs, the service(s) and the environment, i.e.: i) to change a service, POSSs must be modified ii) when POSSs are modified, other POSSs may be impacted iii) when POSSs are modified or impacted, one or more services may be changed iv) when the environment is changed, the behaviour of one or more POSSs may be impacted v) when a service changes, it usually impacts the environment.
16.5	Check that, collectively, the lists of POSSs appear to be complete.

[22] There must be at least one changed POSS, but it is acceptable for lists to be null if this is shown to be correct in the impact analyses and their justification (see later tables in this topic).
[23] Parent POSSs are only considered to be changed if at least one of their (immediate) child POSSs has changed behaviour (which includes new and removed child POSSs).

16.6	Check that the lists of changed and impacted POSSs have been established by comparison with the same baseline build as used in the safety criteria used for the transitional stage.
16.7	Check that each POSS whose specification has been up-issued is present in one of the four lists required above in 16.2.

17 Justification of lists of changed and impacted POSSs	
17.1	Check that there is a satisfactory argument that justifies the adequacy of the lists of changed and impacted POSSs, i.e. check that the argument is coherent, suitably convincing, etc.
17.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
17.3	Check that the justification states the baseline system used to identify the changed and impacted POSSs.
17.4	Check that the justification shows that all impact analyses used the identified baseline system.
17.5	Justification of the identified sets of changed and impacted POSSs. Check that there is a valid justification that: a) the list of changed POSSs includes those that have changed, but their behaviour (in their specification) did NOT change b) the list of changed POSSs includes those that have changed, and their specification changed (which includes new and removed POSSs). c) the list of impacted POSSs includes those that have NOT changed, but whose specification changed due to a change in the POSSs' context, which is either a change in the interactions across one or more of their interfaces and/or in the resources they share with other POSSs d) the list of impacted POSSs includes those that have NOT changed, but whose specification changed due to a change in their safety requirements e) all POSSs whose specification has changed are included in the lists of changed or impacted POSS.
17.6	Justification of limit of impact. Check that there is a valid justification that, in cases where connected POSSs were determined to not be impacted, this was correctly ascertained, by a suitable combination of: a) Analysis of adequately complete specifications for the POSSs and their architecture b) Testing to confirm that there is no impact from the change.
17.7	Justification of impact analysis. Check that there is a valid justification that: a) the impact analysis procedures used to identify changed and impacted POSSs specified appropriate analysis techniques, including: i) ensuring that any further impacts from impacted POSSs were identified ii) correctly identifying when connected POSSs are not impacted. b) the people that performed the impact analyses were competent, according to the nature of the change in behaviour, the technology providing the behaviour, and the impact analysis techniques used c) the impact analysis procedures were executed completely, for the whole change d) the impact analyses considered all modes, all uses, all scenarios, etc in accordance with specified environments and operational system configurations

	e) the impact analyses considered all support systems, e.g. training, data preparation, and test and development systems. f) the specifications analysed were adequate to support impact analysis, and are applicable to the specific proposed change g) all assumptions made during impact analysis have been validated h) the impact analyses were revised to identify any new impact, if specifications are revised or the final change to be implemented differs from that originally analysed
17.8	Completeness of behaviour/properties considered. Check that there is a valid justification that the impact analyses considered the effects of all mechanisms when deciding whether changed behaviour has an impact. This justification could address, for example: a) intended behaviour b) failure modes and failure rates c) failure detection and correction d) failure propagation or tolerance e) scheduled and corrective maintenance activities f) intended interface conditions, ranges and protocols g) proximity of POSSs or environmental elements (e.g. visual reference points) h) critical thresholds (e.g. of resource usage) i) stress, capacity or loading j) positive or negative feedback effects
17.9	Check that the justification appeals to appropriate measures to provide confidence that the set of changed and impacted POSSs is correct, for example: a) comparison with impacts of previous similar changes b) consideration of impact mechanisms previously experienced c) regression testing, beyond the POSSs identified as impacted, showing no further impact.
17.10	Check that, if the impact analysis showed an effect on the interface with another service that is not addressed by the change safety case, then it states that the owners of that service have been notified of the effects of the planned change.

Impact analysis records

The following tables provide candidate assessment activities for use in cases where it is necessary to establish increased confidence in the impact analysis by examining the records of the analysis.

If required, the assessor could also check that the worksheets support the justifications addressed by the candidate assessment activities in Justification of lists of changed and impacted POSSs on page 142 (whether or not the change safety case includes that justification).

18	**Records of analysis that identified those POSSs that have changed, but their behaviour has NOT been changed (i.e. their new specifications show the same behaviour as before the change)**
18.1	Check that records show that a systematic analysis identified the POSSs that are different to those in the baseline system, and whose behaviour (in their specification) has NOT changed.
18.2	Check that records show that the POSSs identified by this analysis included: a) all bottom-most POSSs that were changed, but whose specification did not change b) all parent POSSs whose specification did not change, but that have at least one immediate child POSS that has changed behaviour (which includes new and removed child POSSs).
18.3	Check that the POSSs analysed and listed appear to be uniquely identifiable parts of the operational and support systems.

19	**Records of analysis that identified those POSSs that have changed, and their behaviour has been changed (i.e. their new specifications show different behaviour to before the change). This includes all new and removed POSSs.**
19.1	Check that records show that a systematic analysis identified the POSSs that are different to those in the baseline system, and whose behaviour (in their specification) has changed.
19.2	Check that records show that the POSSs identified by this analysis included: a) all bottom-most POSSs whose specification and behaviour changed b) all parent POSSs whose specification and behaviour changed.
19.3	Check that this analysis appears to have been adequate to identify any new or removed POSSs.
19.4	Check that the POSSs analysed and listed appear to be uniquely identifiable parts of the operational and support systems.

20	**Records of analysis that identified those POSSs that have NOT changed, but whose specification has been changed due to a change in the interactions across one or more of its interfaces and/or in the resources it shares with other POSSs**
20.1	Check that it is clear against which baseline system the changed specifications have been identified.
20.2	Check that records show that a systematic analysis appears to have identified the POSSs that have NOT changed, but whose specification has been changed due to a change in the interactions across one or more of its interfaces, and/or the resources it shares with other POSSs, by at least: a) identifying all POSSs whose specifications have changed b) identifying POSSs subject to a change in the attributes of what traverses its interfaces: i) identifying the interfaces of the POSSs in a) ii) analysing the specification changes of the POSSs in a) to identify any changes to the attributes of what traverses each of the POSS's interfaces

	iii) identifying the POSSs connected to each of these interfaces with changed attributes[24], and determining the combined effect of all the changes in interface attributes, for each of these interfacing POSSs c) identifying POSSs subject to changed access to shared resources: i) identifying all the resources used or produced by the POSSs in a) ii) analysing the specification changes to identify any effects on each of the resources used or produced by the POSSs in a) iii) identifying coupled POSSs that use or supply each of these changed resources, and determining the combined effect of all the changes in access to the resources, for each of these coupled POSSs iv) identifying, from these identified POSSs, those whose behaviour was NOT already specified for the changed interface attributes and/or changed access to shared resources (the majority of cases)
20.3	Check that, where POSSs that had changed interactions across one or more of its interfaces, and/or the resources it shares with other POSSs, was judged not to have a changed specification as a result, that: a) this judgement appears sound b) there was adequate knowledge/specification of the POSS.
20.4	Check that, when identifying connected POSSs, it appears that the analysts had adequate knowledge/specification of the various interfaces between POSSs and coupling via shared resources.
20.5	Check that analysis appears to have been adequate to identify any POSSs impacted by the effects of the changes propagating through the service environment back to the operational system's inputs.
20.6	Check that the POSSs analysed and listed appear to be uniquely identifiable parts of the operational and support systems.

21	**Records of analysis that identified those POSSs that have NOT changed, but whose specification has been changed due to a change in their safety requirements**
21.1	Check that it is clear against which baseline system the changed specifications have been identified.
21.2	Check that records show that a systematic analysis appears to have identified all POSSs that have NOT changed, but whose specification has been changed due to a change in its safety requirements, by at least: a) identifying all POSSs whose safety requirements have changed b) identifying, from these POSSs, those whose specified behaviour did NOT already satisfy the changed safety requirements e.g. the behaviour was not previously supported to the required integrity or confidence
21.3	Check that the POSSs analysed and listed appear to be uniquely identifiable parts of the operational and support systems.

[24] Where changes exit the functional system, connections could be created by the effects of the changes propagating through the service environment back to the functional system's inputs.

Phase 5 Step 4 Topic Tables

The change safety case must provide adequate specifications of the functional system and services, operating during the transitional stage. These specifications must incorporate any changes made to the functional system and services by transitional activities in previous transitional stages.

The change safety case must specify the safety criteria that specify acceptable safety performance, and show that the predicted safety performance has been evaluated against them.

The change safety case must specify the safety requirements developed from the safety criteria. These are necessary to support impact assessment to set the scope of the change, and support verification so that the specifications are valid.

Specification of transitional stage

The assessment activities should be designed to determine whether the change safety case correctly identifies the operational environment, the service and the build state of the functional system that will exist during the transitional stage.

22 Transitional stage specification	
22.1	Check that the change safety case identifies, for the transitional stage being assessed: a) the specification of the operational environment b) the specification of the service c) the build state of the functional system.
22.2	Check that the change safety case either: a) declares that all evidence to support the change safety case for the transitional stage being assessed already exists, or b) declares a list of outstanding evidence items (perhaps by referencing the justifications or documents that require evidence), for the transitional stage being assessed.
22.3	If a list of outstanding evidence items is declared for the transitional stage being assessed, check that there is a justification that there has been adequate verification that, for each outstanding evidence item: a) the evidence item is defined b) the acceptability criteria (for the evidence item to support the justification using it) are defined c) the method for generating the evidence is known d) the conditions under which the evidence is collected do not invalidate the evidence e) the activity to generate the evidence has been planned and is consistent with the decision criteria in the transition plans f) the evidence will be generated before the transitional stage being assessed commences.

23 Specification of build state	
23.1	Generic properties. Check that: a) it is clear that the specification of build state applies to the transitional stage being assessed b) the specification of build state is for the Service Provider's specific operation and POSS versions c) the scope of the specification of build state appears to be sufficient d) the specification of build state appears to be: i) correct ii) complete iii) sufficiently detailed iv) accurate v) unambiguous vi) consistent
23.2	Check that the specification of build state appears to be consistent with the Installation, Commissioning, Transition and Recovery Plans associated with the transitional stage.
23.3	Check that the specification of build state identifies the functional system that will exist during the transitional stage, identifying the POSSs that it comprises, including their versions.

Specification sets

For the functional system that will be extant during the transitional stage, the assessment activities should be designed to determine whether the change safety case correctly identifies the sets of specifications that specify the POSSs within the scope of the change, and those additional specifications (if any) that are necessary to support safety analysis and/or safety modelling.

24 Set of specifications for the scope of the change	
24.1	Check that it is clear that the set of specifications for the scope of the change applies to the transitional stage being assessed
24.2	Check that the set of specifications for the scope of the change is for the Service Provider's specific operation and POSS versions.
24.3	Check that the scope of the set of specifications for the scope of the change appears to be sufficient, e.g. that it covers all POSSs changed or impacted by the change.
24.4	Check that the set of specifications for the scope of the change appears to: a) be correct b) be complete c) identify each specification's version unambiguously.
24.5	Check that the set of specifications for the scope of the change appears to identify specifications to a level of design indenture that is consistent with:

a) the POSSs analysed in the impact analysis

b) the bottom-most POSSs that are shown to be directly verified.

25	Set of additional specifications required to support safety analysis and/or safety modelling
25.1	Check that it is clear that the set of additional specifications applies to the transitional stage being assessed.
25.2	Check that the set of additional specifications is for the Service Provider's specific operation and POSS versions.
25.3	Sufficiency of the set of additional specifications. Check that: a) the set defines the functional system at design levels that enables: i) decomposition of historical safety targets to set safety criteria at the level of the scope of the change ii) composition of safety performance from the level of the scope of the change to safety criteria at a higher level. b) the set defines any sibling-level POSSs required to contribute to the decomposition/ composition in a).
25.4	Check that the set of additional specifications appears to: a) be correct b) be complete c) identify each specification's version unambiguously.

Specification of service and operational environment

The assessment activities should be designed to determine whether the change safety case adequately specifies the service(s) and environment with sufficient detail and correctness to support the safety analysis, for the transitional stage being assessed.

26	Specification of the service(s)
26.1	Generic properties. Check that: a) it is clear that the specifications apply to the transitional stage being assessed b) the specifications are for the Service Provider's specific service and environment c) if the specifications mention POSSs used to provide the service: i) they are those used by the Service Provider ii) they do not contradict the build state referenced in the change safety case d) the scope of the specifications appears to be sufficient, e.g. that they cover all services changed or impacted by the change. e) the specifications appear to be: i) correct ii) complete iii) sufficiently detailed

iv) accurate
v) unambiguous
vi) consistent

f) the set of specifications appears to be:
i) complete
ii) consistent

26.2 Content. Check that the specification:

a) defines the behaviour and performance of the service and its interfaces, including failure behaviour[25]

b) defines its operational environment, or references where it is specified

c) defines the capacity of the service

d) defines any constraints on usage of the services

e) defines the environmental conditions under which the service can be provided, e.g. time of day, weather

f) addresses day-to-day variations in modes of service, e.g. night-time closures, fall-back operations, opening and close down arrangements.

27 Specification of the environment(s) of the service(s)

27.1 Generic properties. Check that:

a) it is clear that the specifications apply to the transitional stage being assessed

a) the specifications are for the Service Provider's specific service

b) the scope of the specifications appears to be sufficient, e.g. that they cover, as a minimum, everything relevant to the services changed or impacted by the change

c) the specifications appear to be:
i) correct
ii) complete
iii) sufficiently detailed
iv) accurate
v) unambiguous
vi) consistent

d) the set of specifications appears to be:
i) complete
ii) consistent

27.2 Check that the specification defines the environment into which the changed service will be delivered, i.e. this is not necessarily the same as the pre-change environment.

27.3 Check that the specification appears to include all entities in the environment and their behaviour/properties.

27.4 Check that the specification appears to address all organisations that participate in the environment of the provided service:

[25] The failure behaviour may have originally been identified by FMEA or possibly HAZOPS, and should subsequently been incorporated into the specification.

	a) Identity and description b) Contribution to operations in the environment c) Scope of participation d) Constraints e) Operational and service level agreements f) Contact details of responsible person
27.5	Check that the specification appears to include all regulatory aspects that apply to the service: a) applicable regulators and regulations b) other applicable law.
27.6	Check that the specification includes other services with which the changed service interacts, through the environment.
27.7	Check that the specification identifies potential security threats from malevolent actors in the operational environment.

Specification of the parts of the functional system that are within the scope of the change

The assessment activities should be designed to determine whether the change safety case adequately specifies the parts of the functional system identified as within the scope of the change, including their local environments, the system and subsystem architectures, and the changed and impacted POSSs, with sufficient detail and correctness to support safety analysis.

In consideration of the indirect relationship of the support systems to the safety of the service(s) provided by the operational system, the roles of the support systems should govern:

a. the planned assessment activities and samples

b. the assessor's view of what is acceptable.

Note: the assessor may also use the activities below to assess the specifications of the surrounding POSSs when assessing the credibility of the declared scope of the change in Phase 5 Step 3

28 Specification of functional system environment	
28.1	Generic properties. Check that: a) the specification is for the Service Provider's specific functional system b) the scope of the specification appears to be sufficient, e.g. that it covers, as a minimum, the environments of all POSSs changed or impacted by the change c) the specification appears to be: i) correct ii) complete iii) sufficiently detailed iv) accurate v) unambiguous

	vi) consistent
28.2	Check that the specification defines the environment in which the changed functional system will reside, i.e. this is not necessarily the same as the pre-change environment.
28.3	Check that the specification appears to include all entities in the environment in which the functional system resides, and their behaviour/properties including: a) location b) supply and support of power, assets and resources c) physical environment d) electro-magnetic environment e) demand characteristics f) interfaces g) externally-supplied resources and services h) maintenance arrangements.
28.4	Check that the specification appears to address all organisations that participate in the environment of the changed POSSs, e.g. different operating and maintenance organisations: a) Identity and description b) Contribution to operations in the environment c) Scope of participation d) Constraints e) Operational and service level agreements f) Contact details of responsible person
28.5	Check that the specification appears to include all regulatory aspects that apply to the changed functional system: a) applicable regulators and regulations b) other applicable law
28.6	Check that the specification identifies potential security threats from malevolent actors in the functional system environment.

29 Specifications of architectures	
29.1	Generic properties. Check that: a) the specifications are for the Service Provider's specific functional system b) the scope of the specifications appears to be sufficient, e.g. that they cover all parts of the functional system changed or impacted by the change. c) the specifications appear to be: i) correct ii) complete iii) sufficiently detailed iv) accurate v) unambiguous vi) consistent

	d) the set of specifications appears to be: i) complete ii) consistent
29.2	Check that the architectures that link the changed, impacted and adjacent POSSs are specified.
29.3	Check that architecture specifications, when identifying the POSSs that are linked by the architecture: a) clearly identify these POSSs b) appear to identify every POSS that is linked by the architecture.
29.4	Check that architecture specifications identify how the POSSs are linked by the architecture, including the nature of the interaction.
29.5	Check that the architectures are specified down to the level of design of the lowest level POSSs specified.
29.6	Check that the architectures define: a) all functional connections and interfaces b) linkages created by sharing of resources (e.g. electrical power, maintenance staff or operators) c) linkages created by sharing of the physical or electromagnetic environment (e.g. ambient temperature, physical support).
29.7	Check that architectures include feedback mechanisms via the functional system environment and via the operational environment into which the service is delivered, including interactions with other services.
29.8	Check that the interfaces defined by the architectures are adequately specified so that the impact of the change can be understood, for example: a) protocols b) demand rates c) dependencies d) service level agreements
29.9	Check that the architectures are specified for all functional system configurations and reconfigurations e.g. fall back operation, maintenance configurations, facility interrupts, and periods of unavailability.

30 Specifications of parts of the operational system	
30.1	Generic properties. Check that: a) the specifications are for the Service Provider's specific POSS versions b) the scope of the specifications appears to be sufficient, e.g. that they cover all POSSs changed or impacted by the change c) the specifications appear to be: i) correct ii) complete iii) sufficiently detailed iv) accurate

	v) unambiguous vi) consistent d) the set of specifications appears to be: i) complete ii) consistent e) the individual elements of the specifications appear to be presented with sufficient granularity, in an unambiguously traceable manner, such that verification can properly demonstrate their satisfaction.
30.2	Check that the properties and behaviour of the POSSs, including failure behaviour[26], are specified in a manner that can be verified[27].
30.3	Check that the specification appears to address the behaviour/properties in all modes of operation, e.g. fall-back operations, start up and shut down arrangements.
30.4	Check that the specifications of the POSSs define their operational environments, or references where they are specified.
30.5	Specifications of People. Check that specifications for people appear to be adequate in respect of: a) complete expected behaviour b) performance in terms of tasks, accuracy, response times, capacity/work load, and reliability c) skills, qualifications, training, experience, knowledge (e.g. technical and language) d) physical attributes e) necessary personal attributes/characteristics (e.g. dependable, performs well under pressure).
30.6	Specifications of Procedures. Check that the specification for each procedure appears to be adequate in respect of: a) what is achieved b) exceptional actions/behaviour c) the circumstances for its enactment d) responsibilities e) the inputs and resources needed f) supporting documentation including forms g) cross-checks h) the timing and accuracy of the actions i) capacity and other constraints for procedure to be valid.
30.7	Specifications of Equipment. Check that specifications for equipment appear to be adequate in respect of: a) characteristics b) functions c) capacity and other constraints for specification to be valid d) operating and maintenance manuals

[26] The failure behaviour may have originally been identified by FMEA or possibly HAZOPS, and should subsequently been incorporated into the specification.
[27] The specifications must be shown to be correct by verification, as checked under 'Justification of Specifications'

e) implementation technology

f) resources consumed during operation

g) training required for operators and maintainers

h) aging effects and maintenance, fault tolerance and fall-back behaviour

i) fault detection and repair

j) updating during operation

k) configuration for operation (jumper settings, configuration data, etc.), covering the range or set of configurations for which the specification is valid.

30.8 Specification of assets. Check that specifications for assets appear to be adequate in respect of:

a) characteristics

b) supply capacity and any other constraints on usage

c) support and/or maintenance manuals

d) form of implementation

e) resources

f) training required for users and maintainers of asset

g) aging effects

h) fault detection and repair arrangements

i) updating

j) configuration.

30.9 Check that the specifications, if appropriate, address different configurations, specific behaviour and procedures for resilience, for example:

a) use and accessibility in case of emergency or threat, or external event (e.g. weather, road accident), maintenance etc

b) start-up/restart/re-initialisation

c) fall back operation

d) maintenance configurations

e) facility interrupts and periods of unavailability

f) response/resilience to internal and external errors

g) tolerance of faults (and consequent possibility of latent faults)

h) self–checking, built in test, etc

i) mechanisms for correction of invalid internal data.

31 Specification of external services, including supply of resources

[If these specifications need to be specified in greater detail, they can additionally be assessed using candidate assessment activities 30.5 onwards (see **Specifications of parts of the operational system** on page 152).]

31.1 Generic properties. Check that:

a) the specifications are for the specific external service supplied to the Service Provider

b) if the specification mentions the systems used to provide the service:

i) they are those used by the supplier

ii) they do not appear to contradict any descriptions in the change safety case

c) the specifications appear to cover all external services used by the changed or impacted parts of the Service Provider's functional system

d) the specifications appear to be:

i) correct

ii) complete

iii) sufficiently detailed

iv) accurate

v) unambiguous

vi) consistent

e) the set of specifications appears to be:

i) complete

ii) consistent

31.2 Content. Check that the specification:

a) defines the behaviour and performance of the external service and its interfaces to the Service Provider, including failure behaviour

b) defines the capacity of the external service

c) defines any constraints on usage of the services

d) defines the environmental conditions under which the external service can be provided, e.g. time of day, weather

e) addresses all day-to-day variations in modes of service, e.g. fall-back operations, opening and close down arrangements

31.3 Check that the specification appears to be compatible with the Service Level Agreement.

32 Specifications of the parts associated with arrangements for support of the operational system[28]

[If these specifications need to be specified in greater detail, they can additionally be assessed using candidate assessment activities 30.5 onwards (see **Specifications of parts of the operational system** on page 152).]

32.1 Generic properties. Check that:

a) the specifications are for the Service Provider's specific POSS versions

b) the scope of the specifications appears to be sufficient, e.g. that they cover all parts of the support systems changed or impacted by the change

c) the specifications appear to be:

i) correct

ii) complete

iii) sufficiently detailed

iv) accurate

v) unambiguous

vi) consistent

d) the set of specifications appears to be:

[28] Support systems are part of the functional system. They are addressed separately here because they have a less direct relationship to the safety analysis of the operational service, and so may not need to be specified in such great detail.

	i) complete ii) consistent e) the individual elements of the specifications appear to be presented with sufficient granularity, in an unambiguously traceable manner, such that verification can properly demonstrate their satisfaction.
32.2	Check that the properties and behaviour of the parts of the support systems, including failure behaviour[29], are specified in a manner that can be verified[30].
32.3	Check that the specification appears to address the behaviour/properties in all modes of operation, e.g. fall-back operations, start up and shut down arrangements.
32.4	Check that the specification addresses the capacity of the support systems and any other constraints.
32.5	Check that the necessary support systems are specified, for example: a) Simulator requirements to support initial and ongoing training b) Test & development facility to 'prove' updates c) Ongoing training system for operators and maintainers d) Change management arrangements e) Control of configuration and adaptation of the operational system f) Analysis of automatic and manual event and fault logging, reporting and corrective action (DRACAS/FRACAS) g) Systems to supply and maintain resources and assets, including minimum staffing levels, competences, etc h) The capability to maintain and repair the operational and support systems i) Through-life provision of authentic (from intended manufacturer) spare parts that are as intended (as specified, the correct version, configured correctly, etc) j) Secure disposal of redundant parts k) Appropriate organisation and management arrangements, including defined responsibilities & accountabilities l) Management of maintenance, facility interrupts, periods of unavailability, 'quick fixes' m) Management of external interfaces n) Communication and coordination with stakeholders o) Periodic changes, e.g. environmental data updates. p) Detection of corrupt data, and correction. q) Optimisation, 'housekeeping', etc r) Safety performance monitoring system

Justification of Specifications within the scope of the change

The assessment activities should be designed to determine whether the change safety case adequately justifies that the specifications for the scope of the change are correct, consistent, sufficiently detailed, and verified.

[29] The failure behaviour may have originally been identified by FMEA or possibly HAZOPS, and should subsequently been incorporated into the specification.
[30] The specifications must be shown to be correct by verification, as checked under 'Justification of the specifications for the POSSs within the scope of the change associated with the transitional stage' on page 169.

Whilst showing that the specifications correctly reflect the test evidence, or the composition of the behaviour in lower-level specifications, is logically part of the justification of the specifications, this is not assessed in this Step, but is covered in Phase 5 Step 5 Plan and assess justification of specification elements (page 80). This separation has been made because assessment planning must select from the large number of arguments required to justify the evidential support for each specification element. Moreover, the assessment of the other, less technical, justifications may identify the most appropriate selection criteria.

33	**Justification of the specifications for the POSSs within the scope of the change associated with the transitional stage**
33.1	Check that there is a satisfactory argument that justifies the adequacy of the specifications for the POSSs within the scope of the change i.e. check that the argument is coherent, suitably convincing, etc.
33.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
33.3	Check that the justification shows that each specification is for the Service Provider's specific operation and POSS versions.
33.4	Check that the justification shows that each specification is for the transitional stage being assessed.
33.5	Check that the justification shows that the specifications cover all changed or impacted services and parts of the functional system.
33.6	Check that the justification shows that each specification has been checked/verified and approved in accordance with the Service Provider's QMS and SMS.
33.7	Check that the justification shows that there has been adequate verification that the set of specifications is: a) complete b) consistent.
33.8	Check that the justification shows that there has been adequate verification that all the specifications in the set are: a) correct b) complete c) sufficiently detailed d) accurate e) unambiguous f) consistent.
33.9	Check that the justification shows that the specifications state all behaviour/properties of each POSS in the defined environment, in that each specification reflects: a) all the direct verification evidence resulting from verification activities that were sufficient[31] to demonstrate all behaviour/properties of the POSS

[31] Assessing the Service Provider's argument of sufficiency is a major area where the assessor's judgement is necessarily based on experience and understanding. Industry norms or standards may apply. Relevant issues for the adequacy of testing to reveal all behaviour/properties include: the independence or inter-dependence of individual elements of the specification; observation of behaviour on all outputs during tests; claims to have

	b) a complete and correct composition of all behaviour/properties in the child specifications.
33.10	Check that the justification shows that there has been adequate verification that each individual element of the specifications is proved from either: a) direct verification, or b) composition from the behaviour in child specifications
33.11	Check that the justification shows that there has been adequate verification that all the evidence used to justify behaviour of each POSS exists or that the evidence item has been defined, and has been planned to be generated during a transitional stage prior to use of the POSS.
33.12	Check that the justification shows that evidence of each POSS's behaviour addresses aging effects, if appropriate.
33.13	Check that the justification shows that when confirming the behaviour in the specifications, this was done in conditions that provided an adequate check for unexpected behaviour.
33.14	Check that the justification shows that any unspecified behaviour discovered (e.g. during testing) has been included in the specifications, or equivalently accommodated.
33.15	If there is a human in any POSS, check that there is a justification that the POSS's specification includes all effects of an appropriate human's behaviour and interaction (e.g. human response times, mis-interpretation of procedures), including the human contribution to failure behaviour rates.
33.16	Check that the justification shows that each POSS whose behaviour was verified is an example/instance of the POSS whose identity is given (e.g. part number and version) in the specification.
33.17	Check that the justification shows that the provenance of evidence of behaviour is recorded.
33.18	Check that the justification shows that there has been adequate verification that, for each POSS specification, their defined operational environment is valid for the conditions that will be present during the transitional stage.
33.19	Check that the justification shows that there has been adequate verification that, for each POSS specification, their defined operational environment is consistent with: a) the test conditions used when demonstrating the behaviour in the specification b) the environmental conditions predicted by composition of lower-level specifications c) the environmental conditions predicted by decomposition of higher-level specifications d) the true operational environmental conditions, as verified by test/monitoring in an appropriate system/subsystem assembly (e.g. an assembly undergoing integration test).
33.20	Check that the justification shows that, for each specification, there has been adequate verification of the justifications that there is adequate evidence to demonstrate[32]: a) the veracity of the specified behaviour and properties, including their associated integrity and confidence b) that the specified behaviour and properties will be exhibited for the specified environment.

covered the complete state space of the POSS (perhaps appealing to the use of coverage criteria and random or statistical testing) across the whole of the POSS's predicted operational environment.

[32] The justification should encompass all aspects addressed by Candidate assessment activities in Phase 5 Step 5 Plan and assess justification of specification elements (page 79).

33.21	Check that the justification shows that there has been adequate regression test[33] to: a) confirm that there has been no change in the top level specifications for the scope of the change, and specifically in behaviour related to the change b) search for unexpected impact on functional system behaviour outside the scope of the change, including that covered by specifications required for safety analysis that are not in the scope of the change c) search for unexpected impact on functional system behaviour within the scope of the change.
33.22	Check that there is a justification that the POSS specifications include all behaviour that is specified by mandatory standards or regulations, and by any other standards or regulations for which compliance is claimed.

Justification of additional specifications to support safety analyses

The assessment activities should be designed to determine whether the change safety case adequately justifies that the additional specifications required for the safety analyses are adequate for this purpose. These specifications are for parts of the functional system outside the scope of the change (parent levels or siblings), but which are required for safety analyses, e.g. for the setting of the safety criteria, or demonstration that they will be satisfied. The justification records why the Service Provider is prepared to use these specifications, even if they have not been fully verified as part of preparing the current change.

The planner can also, if appropriate, select from the candidate assessment activities for 33 Justification of the specifications for the POSSs within the scope of the change associated with the transitional stage (page 157).

If the justification argues that the specifications are based on test evidence, or the composition of the behaviour in lower-level specifications, and it is appropriate to conduct a detailed assessment, the candidate assessment activities in Phase 5 Step 5 Plan and assess verification material (page 80) can also be used.

34	**Justification of additional specifications to support safety analyses for the transitional stage**
34.1	Check that there is a satisfactory argument that justifies the adequacy of the additional specifications to support safety analyses i.e. check that the argument is coherent, suitably convincing, etc.
34.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
34.3	Check that the justification records why the Service Provider deems that all the additional specifications are suitably trustworthy to support the safety analyses.
34.4	Check that the justification evaluates the existence of contra-evidence to the trustworthiness of the additional specifications.

[33] 'Regression test' refers to random and/or informed testing to check for unexpected impact on behaviour. It is not intended to provide formal verification of specified behaviour.

34.5	Check that the justification is not refuted by known in-service behaviour and performance of the functional system.

Safety criteria

The change safety case must set valid safety criteria that define acceptable safety performance for the transitional stage being assessed. A valid safety criterion is specified:

a. either in terms of the acceptable risk of accidents, in terms of the acceptable rates of occurrence of hazardous events, or using a proxy[34] AND

b. either by identifying acceptable safety performance absolutely, or relative to previous safety performance.

The safety criteria collectively encompass all safety-related behaviour within the scope of the change, and so each safety criterion has its own defined scope. Additionally, different safety criteria may be established for different operational modes.

This section addresses the assessment of these safety criteria and their provenance for the specific transitional stage being assessed.

As a minimum, for any stage, the existence of safety criteria is established. It would be unusual not to assess the safety criteria for the final transitional stage, but the most detailed assessment of the safety criteria would usually be conducted for those transitional stages having the greatest scope of change.

The planner selects assessment activities from the appropriate tables below, according to the nature of the safety performance acceptability argument, specifying that they are to be applied to the relevant parts of the argument.

35	**Set of safety criteria that define acceptable safety performance for the specific transitional stage being assessed**
35.1	Check that the change safety case states or references safety criteria for the transitional stage being assessed.
35.2	Check that the change safety case provides or references the analysis by which the safety criteria were derived.
35.3	Check that the safety criteria appear credible, and there are no obvious omissions.
35.4	Check that the safety criteria appear to address the safety-related behaviour of all parts of the operational and support systems within the scope of the change.
35.5	Check that the safety criteria appear consistent with those for comparable functional systems or changes.
35.6	Check that, if necessary, the safety criteria address different operational modes and scenarios.

[34] If the applicable legislation or regulations permit proxies to be used as safety criteria. A proxy is some (quantitatively or qualitatively) measurable property that can be used to represent the value of something else related to risk, e.g. visibility or crowd density.

35.7	Check that, for each safety criterion, the following are defined: a) the safety behaviour, property or event to which the criterion applies b) the safety-related attributes of the behaviour, property or event (e.g. timing performance) c) the acceptable safety performance d) the units in which its acceptable safety performance is specified e) the confidence to which satisfaction of a) and b), must be known f) the associated system scope i.e. which part of the functional system or service must satisfy this acceptable safety performance g) the environment of the associated system scope, including its local environment, constraints, and its view of the operational environment, as applicable.
35.8	Check that, if the change was instigated by the SMS to achieve a certain risk reduction, the change safety case clearly identifies whether the safety criteria: a) specify the intended risk reduction for the change b) specify risk reduction less than that intended when the change was instigated[35], with a justification, in the context of the overall safety management of the service, why the Service Provider intends to proceed with the change.
35.9	Check that the safety criteria appear to address the safety-related behaviours (or properties) of the parts of the functional system that are within the scope of the change i.e. there is at least one safety criterion for each trajectory from an accident cause to the accident, where the trajectory progresses through the scope of the change.
35.10	Check that each safety criterion is either: a) expressed in terms of the acceptable risk of a specified accident or set of accidents b) expressed in terms of acceptable rates of occurrence for a specified safety-related behaviour
35.11	Check that the safety criteria are sufficient to define acceptable safety performance because either: a) the performance they specify results in the same or better risk (compared to existing safety requirements) than the original unchanged service, or b) the performance they specify results in the same or better risk (compared to the existing safety performance, where this is known to better the safety requirements) than the original unchanged service, or c) agreement has been reached with the CA that a service may be offered (temporarily for non-final transitional stages) with increased risk, or d) when considering a new service, the performance they specify results in acceptable risk.
35.12	Check that the safety criteria are expressed in terms that permit objective comparisons to be made with predicted safety performance.
35.13	Check that the change safety case contains an evaluation that compares each safety criterion with the predicted safety performance of the changed functional system (see section 38).
35.14	Check that, where safety criteria are defined for multiple modes of operation of a service, that:

[35] If the change fails to deliver the intended risk reduction, it may still be acceptable that the change is implemented (provided that the change does not increase risk), but the Service Provider must identify that a further change is required to deliver the desired risk reduction.

	a) the set of modes appears to be complete. b) the change safety case shows that the total safety performance implied by the safety criteria for the modes satisfies any overall safety performance criteria.
35.15	Check that there appear to be adequate safety criteria for the support system(s) to evaluate their contribution to safe operation.

36 Records of analyses to derive set of safety criteria

[If the source of the safety criteria is an analysis that used modelling, the appropriate safety model elements can be assessed using the candidate assessment activities in **Appendix F – Candidate assessment activities for safety analysis models**, page 191, as described in the guidance for this assessment step]

36.1	Check that the records of the specific derivation of each safety criterion can be identified.
36.2	Check that the method for deriving the safety criteria appears appropriate for the change.
36.3	Check that, if the change was instigated by the SMS to achieve a certain risk reduction, the records show that the safety criteria were derived to achieve the intended risk reduction for the change[35].
36.4	Check that the records show that either: a) the safety criteria were set on the basis of the safety requirements or safety performance of a baseline functional system/service, using the same baseline functional system/service used in the impact analysis b) the safety criteria were derived from service risk, analysing the service provided during the transitional stage.
36.5	Check that the source of data used to derive the safety criteria is clear and appears to be valid.
36.6	Check that the records show that the environment associated with each safety criterion has been derived from the environmental specification applicable to the transitional stage, considering the local environment, and applicable aspects of functional system constraints, and the operational environment.
36.7	Check that safety criteria were derived to address the risks to all vulnerable assets (including those associated with the service and non-participants in the environment) affected by the change.
36.8	Check that the safety criteria were derived to address the scope of the change for the transitional stage being assessed.
36.9	Check that safety criteria were derived to address the risks of all services that use the changed or impacted POSSs, as identified by the impact analysis.
36.10	Check that safety criteria were derived to address the safety-related behaviours (or properties) of the parts of the functional system that are within the scope of the change.
36.11	Check that the derivation referenced specifications of the functional system and service, and these specifications are for the correct transitional stage.
36.12	Check that the functional system and service specifications used in the derivation of the safety criteria are consistent with the functional system extant at the transitional stage being assessed.

36.13	Check that, where safety criteria are defined for multiple modes of operation of a service, that there was a valid apportionment of any overall safety performance criteria to the safety criteria for the modes.
36.14	Check that it appears that the confidence to which each safety criterion must be demonstrated was correctly determined.

37 Justification of safety criteria	
37.1	Check that there is a satisfactory argument that justifies that the safety criteria are correct i.e. check that the argument is coherent, suitably convincing, etc.
37.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
37.3	Check that the justification clearly identifies the method used for deriving the safety criteria.
37.4	Check that the justification shows that the safety criteria were derived in accordance with Service Provider's SMS[36].
37.5	Derivation process. Check that there is a justification that: a) the safety criteria derivation techniques used were appropriate b) the people that performed the safety criteria derivation were competent, according to the nature of the POSSs and the derivation techniques used c) the safety criteria derivation procedures were executed completely and correctly d) the safety criteria derivation considered all modes, all uses, all scenarios, etc e) the safety criteria derivation process covered all potential accidents associated with the scope of the change.
37.6	Check that the justification shows that the method for deriving the safety criteria ensured that they address the safety of all services that use the changed or impacted POSSs.
37.7	Check that there is a justification that there are safety criteria that address the safety of all services that use the changed or impacted POSSs.
37.8	Check that there is a justification that it has been ensured that any assumptions made have been validated and are consistent with each other, and with the operational circumstances and environment in the accident sequence.
37.9	Check that the justifications show that the safety criteria are for the Service Provider's specific services and for the correct transitional stage.
37.10	Check that there is a justification that the specifications used to derive the safety criteria were for the transitional stage being assessed.
37.11	Check that there is a justification that it has been verified that the specifications, used in the derivation of the safety criteria, describe all parameters that are pertinent, including consideration of whether new parameters may have become pertinent due to the nature of the change being implemented.
37.12	Traceability. Check that there is a justification that each safety criterion can be traced: a) to the (specific part of the) analysis that identified the safety criterion

[36] It is assumed that the SMS ensures that the acceptability criteria are defined to address all applicable regulations and risk principles (e.g. GAMAB, ALARP).

	b) 'upwards' to the data from which it was derived c) 'downwards' to its child safety requirements d) to the specification of the part of the functional system that must satisfy the safety criterion (if the safety criterion is set at a point beyond the scope of the change, then its scope must be defined).
37.13	Check that there is a justification that the set of safety criterion was revised, if necessary, when additional accident trajectories are implicated, due to: a) increases in the scope of the change, e.g. when impacted parts of the operational and support systems were identified b) additional behaviour identified by verification and included in the specifications.
37.14	Check that the justification shows that: a) the safety criteria are: i) correct ii) completely specified, according to the criteria in section 35.7 iii) accurate iv) unambiguous v) consistent b) the set of safety criteria is: i) complete ii) consistent iii) non-contradictory c) the safety criteria are specified in a manner such that they are verifiable.
37.15	Check that there is a justification that, where necessary according to their scope, the derivation of safety criteria correctly accounted for multiple functional system states or operating modes, e.g. maintenance, facility interrupts, periods of unavailability.
37.16	Check that there is a justification that verification activities were conducted in accordance with the applicable SMS procedures.
37.17	Verification activities. Check that there is a justification that verification activities were adequate to verify: a) the absence of contradictory or inconsistent safety criteria b) that the set of safety criteria completely addresses all accident trajectories associated with the scope of the change c) that the safety criteria were correctly derived d) that the confidence to which each safety criterion must be demonstrated was correctly derived e) that safety criteria derivation method was carried out correctly f) the absence of orphan safety criteria (having no associated accident trajectory).
37.18	Check that there is a justification that the data used to derive the safety criteria was appropriate (e.g. trustworthy, applicable).
37.19	Check that, if the change was instigated by the SMS to achieve a certain risk reduction, the justification shows that either: a) the safety criteria were derived to achieve the intended risk reduction for the change b) the set of safety criteria used in the change safety case do not achieve that intended risk reduction, and the reasons why the change should proceed[35].

37.20	Check that the justification shows that either: a) the safety criteria were set on the basis of the safety requirements or safety performance of a baseline functional system/service, and this used the same baseline functional system/service used in the impact analysis b) the safety criteria were derived from service risk, and that the service analysed is that provided during the transitional stage.
37.21	Check that there is a justification that the safety criteria are sufficient to define acceptable safety performance because either: a) the performance they specify results in the same or better risk than the baseline service b) or, when considering a new service, the performance they specify results in acceptable risk.
37.22	Check that, if the justification shows that the safety criteria for the transitional stage are based on the previous safety performance of the functional system in a state where it operated at increased safety risk, by prior agreement with the CA, the justification demonstrates that it is acceptable to use the safety performance of this increased-risk functional system to define safety criteria (it seems unlikely that this can be done).
37.23	Check that, if the justification shows that the safety criteria for the transitional stage are based on the previous safety performance of the functional system, the justification demonstrates that the baseline functional system/service was suitable to provide a baseline definition of safety performance, for example: a) an incompletely assured change was not included in the functional system b) the baseline functional system/service was operational for a sufficient period of time c) the utilisation of the functional system/service during the baseline transitional stage was sufficient d) the operation demonstrated the efficacy of the safety functions of the functional system relevant to the scope of the change.
37.24	Check that there is a justification that safety criteria were derived to address the risks to all vulnerable assets affected by the change.
37.25	Check that there is a justification that the confidence to which each safety criterion must be demonstrated was correctly derived.

Evaluation of acceptability of predicted safety performance

The change safety case must include an appropriate demonstration that the predicted safety performance meets the safety criteria that define acceptable safety performance for each transitional stage. This section addresses the comparison of the predicted safety performance with the safety criteria that define acceptable safety performance, for a specific transitional stage. The safety performance for the transitional stage should only be claimed to be acceptable on the basis that all the individual safety criteria for that transitional stage are shown to be satisfied.

As a minimum, for any transitional stage, the presence of a safety performance comparison is established. It would be unusual not to assess the comparison for the final transitional stage, but the most detailed assessment would usually be conducted for those transitional stages having the greatest scope of change.

The prediction of safety performance at any transitional stage (apart from the first one) may be contingent on evidence of behaviour that has to be collected in a previous transitional stage.

38	**Evaluation of acceptability of the predicted safety performance associated with the changed service, during the transitional stage being assessed**
38.1	Check that the safety performance evaluation complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
38.2	Claim regarding acceptability of safety performance of the change during the transactional stage being assessed. Check that: a) There is a claim that the predicted safety performance associated with the changed service during the transitional stage is acceptable. b) The claim regarding the acceptability of predicted safety performance is that 'the predicted safety performance is acceptable' only if all the individual safety criteria for the transitional stage are satisfied. c) No other claim for acceptability is made, i.e. other than on the basis of comparing predicted safety performance with valid safety criteria.
38.3	Claims regarding satisfaction of safety criteria for the transitional stage. Check that: a) For each safety criterion, there is a claim that the acceptable safety performance is acceptable. b) For each safety criterion, the claim that 'the predicted safety performance is acceptable' is made only if the safety criterion is satisfied by the predicted safety performance. c) For each safety criterion, no other claim for acceptability is made, i.e. other than on the basis of comparing predicted safety performance with valid safety criteria.
38.4	Comparison of predicted safety performance with the safety criteria for the transitional stage. Check that: a) There are individual comparisons of predicted safety performance with each safety criterion for the transitional stage, which defines acceptable safety performance. b) The comparisons address safety performance during the correct transitional stage. c) Each comparison is arithmetically valid, e.g. the things that it compares are expressed in the same units. d) In each comparison, the predicted safety performance has the same scope as that in the safety criterion. e) No other judgement of acceptability is made, i.e. other than by using the defined safety criteria.
38.5	Predicted safety performance. Check that: a) There is a predicted safety performance, in clearly stated units, for each of the safety criteria. b) In each case, the safety performance prediction has the same scope as in the safety criterion. c) The safety performance prediction relates to the functional system/service for the transitional stage being considered. d) The predicted safety performance is expressed in terms that permit objective comparison with the safety criteria.
38.6	Check that the source is stated for each predicted safety performance, either:

a) which specification and which item in that specification, or

b) which safety analysis, and which parameter in that analysis.

39 Source of each predicted safety performance

[If the source is a safety analysis that used safety modelling, the appropriate safety model elements can be assessed using the candidate assessment activities in **Appendix F – Candidate assessment activities for safety analysis models**, page 191, as described in the guidance for this assessment step]

39.1 Check that the source specification or safety analysis is:

a) a formally controlled document

b) for the functional system/service in operation during the transitional stage being assessed

c) for the functional system architecture, service environment and local environment in operation during the transitional stage being assessed (e.g. does not just use the performance from a generic specification without considering the effect of the environment in the changed functional system).

39.2 Where source of the predicted safety performance is stated to be an item in a specification, check that the item referenced in the specification:

a) describes exactly the same behaviour as in the safety criterion

b) states the safety performance (e.g. failure rate) for that behaviour.

39.3 Where source of the predicted safety performance is stated to be a parameter in a safety analysis, check that the parameter referenced in the safety analysis:

a) describes exactly the same behaviour as in the safety criterion

b) states the safety performance (e.g. failure rate) for that behaviour

c) is derived using an appropriate safety analysis and/or safety model.

40 Justification of evaluation of acceptability of the predicted safety performance associated with the changed service, during the stage being assessed

40.1 Check that there is a satisfactory argument that justifies the adequacy of the evaluation of acceptability of the predicted safety performance associated with the changed service i.e. check that the argument is coherent, suitably convincing, etc.

40.2 Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).

40.3 Justification of comparison of predicted safety performance with the safety criteria for the transitional stage. Check that there is a justification that:

a) individual comparisons of predicted safety performance have been made with each and every safety criterion for the transitional stage.

b) the comparison of predicted safety performance with the safety criteria was valid[37], e.g. justifying that:

i) the comparison is arithmetically valid

[37] It would be unusual for a justification of this necessary condition to need to be made to provide sufficient confidence.

	ii) the predicted safety performance used in the comparison have the same scope as those in the safety criteria.
40.4	Justification of analysis to predict safety performance. Check that there is a justification that: a) there is an analysis to predict the safety performance that corresponds to each safety criterion for the transitional stage b) the method for predicting the safety performance was correctly implemented, e.g. the calculations are correct. c) the predicted safety performance matches the system scope of the safety criterion, where necessary including the contributions from relevant unchanged parts of the functional system. d) the POSS and service specifications used for the prediction of safety performance were: i) verified (see Justification of Specifications) ii) adequate to support the prediction iii) applicable to the stage. e) there is sufficient confidence in the safety performance predictions used to judge acceptability. f) the confidence in the safety performance predictions meets confidence criteria stipulated in the safety criteria, if any.

Safety Requirements

The change safety case must include safety requirements derived from the safety criteria (for the transitional stage being assessed). The safety requirements must collectively specify all safety-related behaviour within the scope of the change, each safety requirement being applicable to a defined part of the functional system. Satisfaction of these safety requirements must be demonstrated.

When considering the resources required for the planned assessment activities, the planner may consider that the decomposition of the safety requirements is the converse of the composition of behaviour in specifications ('Justifications of elements of specifications'), and so there may be a trade-off to consider when planning the assessment of these areas. In practice, both composition and decomposition are difficult to perform correctly, so a balanced assessment approach should be considered.

The planner and assessor should keep in mind that the safety requirements for support systems usually require less rigorous justification than those for the operational system.

As a minimum, for any stage, the existence (41.1) and justification of satisfaction (43.17) of safety requirements is established. It would be unusual not to assess the safety requirements for the final transitional stage, but the most detailed assessment of the safety requirements would usually be conducted for those transitional stages having the greatest scope of change.

41 Set of safety requirements	
41.1	Check that the change safety case states or references the safety requirements for the transitional stage being assessed.
41.2	Check that the change safety case provides or references the analysis by which the safety requirements were derived.
41.3	Check that the safety requirements appear credible, and there are no obvious omissions.
41.4	Check that the safety requirements appear consistent with comparable functional systems or changes.
41.5	Check that, if necessary, the safety requirements address different operational modes and scenarios.
41.6	Check that the safety requirements for the POSS are well-formed and objective, clearly and unambiguously defining: a) the required safety behaviour, property or event b) the safety-related attributes of the behaviour, property or event (e.g. timing performance) and the units in which they are specified c) the required maximum rate of occurrence or probability d) the confidence to which the behaviour, as required in a) to c), must be demonstrated e) the part of the functional system or service must satisfy this safety requirement f) the environment of the associated part of the functional system or service, including its local environment, constraints, and its view of the operational environment, as applicable.

42 Records of analyses to derive set of safety requirements [If the source of the safety requirements is an analysis that used modelling, the appropriate safety model elements can be assessed using the candidate assessment activities in **Appendix F – Candidate assessment activities for safety analysis models**, page 191, as described in the guidance for this assessment step]	
42.1	Check that the records of the specific derivation of each safety requirement can be identified.
42.2	Check that the records show that the safety requirements were ONLY derived from the safety criteria for the transitional stage being assessed.
42.3	Check that the records show that each safety requirement was derived from (one or more) safety criterion or higher-level safety requirement.
42.4	Check that the records show, for each safety requirement, from which (one or more) safety criterion or higher-level safety requirement it was derived.
42.5	Check that the records show that safety requirements were derived to address each safety criterion for the transitional stage being assessed.
42.6	Check that there is traceability to the parent safety requirement (or safety criterion) from which each safety requirement was derived.
42.7	Check that there is traceability from the parent safety requirement to child safety requirements, where lower-level safety requirements have been derived.

42.8	Check that it appears that child safety requirements were correctly decomposed from parent safety requirements (or from safety criteria at the top level).
42.9	Check that it appears that there are no orphaned safety requirements, i.e. without a parent safety requirement or safety criterion.
42.10	Check that the records state which architecture and POSS specifications were used to decompose the safety requirements.
42.11	Check that it appears that the correct (including being valid for the transitional stage being assessed) architectural specifications were used when decomposing parent safety requirements (or safety criteria at the top level).
42.12	Check that the records state which environmental specification was used at each point that parent safety requirements (or safety criteria at the top level) were decomposed.
42.13	Check that it appears that the local environmental conditions were correctly identified when decomposing parent safety requirements (or safety criteria at the top level), and were valid for the transitional stage being assessed.
42.14	Check that it appears that the confidence to which each safety requirement must be demonstrated was correctly determined when decomposing parent safety requirements (or safety criteria at the top level).

43 Justification of set of safety requirements	
43.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of set of safety requirements i.e. check that the argument is coherent, suitably convincing, etc.
43.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
43.3	Check that there is a justification that the safety requirements were derived in accordance with the procedures in the SMS.
43.4	Derivation process. Check that there is a justification that: a) the safety requirement derivation techniques used were appropriate b) the people that performed the safety requirement derivation were competent, according to the nature of the POSSs and the derivation techniques used c) the safety requirement derivation procedures were executed completely and correctly d) the safety requirement derivation considered all modes, all uses, all scenarios, etc e) the safety requirement derivation process covered all the safety criteria
43.5	Check that there is a justification that the safety requirements completely address all the safety criteria for the transitional stage being assessed, i.e. that the safety requirements collectively satisfy all the safety criteria.
43.6	Check that there is a justification that any assumptions made have been validated and are consistent with each other, and with the operational circumstances and environment in the accident sequence.
43.7	Check that there is a justification that the architectural specifications and environmental specifications used to derive the safety requirements were for the transitional stage being assessed.
43.8	Check that there is a justification that it has been verified that the architectural specifications and environmental specifications, used in the derivation of the safety

	requirements, describe all parameters that are pertinent, including consideration of whether new parameters may have become pertinent due to the nature of the change being implemented.
43.9	Traceability. Check that there is a justification that each safety requirement can be traced: a) to the (specific part of the) analysis that identified the safety requirement b) 'upwards' to its parent safety requirement (or safety criterion) c) 'downwards' to its child safety requirements, if applicable d) to the specification of the part of the functional system that must satisfy the safety requirement.
43.10	Check that there is a justification that the set of safety requirements was revised, if necessary, when new behaviour was identified by verification and included in the specifications.
43.11	Check that the justification shows that: a) the safety requirements are: i) correct ii) completely specified, according to the criteria in section 41.6 iii) accurate iv) unambiguous v) consistent b) the set of safety requirements is: i) complete ii) consistent iii) non-contradictory c) the safety requirements are specified in a manner such that they are verifiable.
43.12	Check that there is a justification that safety requirement apportionment calculations correctly address the combination of rates or probabilities for multiple functional system states or operating modes, e.g. maintenance, facility interrupts, periods of unavailability.
43.13	Check that there is a justification that verification activities were conducted in accordance with the applicable SMS procedures.
43.14	Verification activities. Check that there is a justification that verification activities were adequate to verify: a) the absence of contradictory safety requirements b) that the set of safety requirements completely addresses all the safety criteria c) that the safety requirements were correctly derived d) that the confidence to which each safety requirement must be demonstrated was correctly derived e) that safety requirement derivation method was carried out correctly f) the absence of orphan safety requirements (having no parent).
43.15	Level of decomposition. Check that there is a justification that the safety requirements were decomposed down to the level of specification: a) at which the part of the safety requirement is directly verified, i.e. verification is not dependent on analytical composition of lower-level specifications b) which supports the impact assessment that established the scope of the change

	c) which supports safety performance monitoring arrangements.
43.16	Check that there is a justification that the confidence to which each safety requirement must be demonstrated was correctly derived.
43.17	Safety Requirements Satisfaction. Check that there is a justification that each safety requirement is completely satisfied either: a) in the specification for the part of the functional system that fully implements it b) in a safety analysis of higher-level behaviour that composes behaviour from the specifications towards the safety criteria.

Phase 5 Step 5 Topic Tables

The change safety case must justify that the elements of the specifications are trustworthy by demonstrating that they reflect referenced evidence, which is primarily that generated by verification activities.

Justifications of elements of specifications

The assessment activities should be designed to determine whether the change safety case adequately justifies that the elements of the specifications are substantiated by verification or other evidence, or by composition of the behaviour/properties in other specifications.

The candidate assessment activities for the three tables representing directly substantiated behaviours or properties are very similar, but have been kept separate in case significantly different activities are identified in future.

44 Justification of an element of a specification by composition	
44.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of an element of a specification by composition i.e. check that the argument is coherent, suitably convincing, etc.
44.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
44.3	Check that the justification references the child specifications (and elements) being composed and the architecture specification that combines them.
44.4	Check that the referenced child and architecture specifications are for the transitional stage being assessed.
44.5	Check that the justification presents the composition calculation.
44.6	Check that the justification records the result of the composition calculation.
44.7	Check that the justification addresses the correctness of the composition, if appropriate according to its complexity and the required confidence[38].
44.8	Check that the result of the composition calculation is the same as the element that the justification is substantiating.
44.9	Check that the justification demonstrates that the composition takes account of all behaviour in the child specifications i.e. that no other behaviour interferes with the behaviour of the element being substantiated.
44.10	Check that, if appropriate, the justification demonstrates that the composition addresses the integrity and confidence associated with the behaviour or property.
44.11	Check that, if composed behaviour has been predicted by exercising a model, the model has been appropriately validated so that there is sufficient confidence in its results.

[38] The justification may appeal to the decompositional analysis and/or the results of integration tests (which demonstrate the composed behaviour).

45	Justification of a directly substantiated behavioural element of a specification
45.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of a directly substantiated behavioural element of a specification i.e. check that the argument is coherent, suitably convincing, etc.
45.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
45.3	Check that the justification references the verification or other evidence being used to substantiate the element.
45.4	Check that the referenced verification or other evidence is for the transitional stage being assessed.
45.5	Check that the justification presents the analysis that demonstrates that the referenced verification or other evidence substantiates the element.
45.6	Check that the justification addresses the correctness of the analysis of verification or other evidence, if appropriate according to its complexity and the required confidence[39].
45.7	Check that the justification demonstrates that the analysis of verification or other evidence takes account of all the available relevant evidence i.e. that the behaviour specified in the element is complete and independent of other behaviour.
45.8	Check that, if appropriate, the justification demonstrates that the analysis of verification or other evidence addresses the integrity and confidence associated with the behaviour.
45.9	Check that the justification addresses the trustworthiness of the verification used to substantiate the element, including justifying that: [text specialised for analysis in square brackets] a) the measurement/observation of the behaviour [result of analysis] was correct and correctly recorded b) the evaluation arrangements under which the POSS was measured/observed [the setup and environment of the model] were appropriate to reveal the behaviour (e.g. accuracy and calibration of test equipment) c) the identity (including version) of the measured/observed POSS [model] was recorded, and matches the identity of [is derived from] the POSS for which the specification (where the element being substantiated resides) is valid d) there is sufficient evidence that the behaviour was observed during all operations of the POSS (for which the element is specified) [the results showed the behaviour during all analyses] e) there is sufficient evidence that the behaviour was observed [analysed] under all appropriate environmental conditions f) there is sufficient evidence that the behaviour was observed [analysed] under all appropriate input conditions g) there was an adequate search for counter-evidence of the behaviour stated in the element being substantiated h) the provenance of measurements/observations was recorded (e.g. the identity and version of the POSS [model] measured/observed and all relevant items associated with its test [analysis] environment/conditions)

[39] The justification may also increase confidence in the results of the analysis by appealing to the predicted results from design analyses.

	i) the recorded measurements/observations [results] have not been corrupted since recording.
45.10	Check that the justification demonstrates that any model used for analysis was suitable, i.e.: a) the specific model and the specific POSS are equivalent b) the model represents the relevant aspects of the POSS c) the model uses notations that are capable of representing everything necessary to determine the behaviour d) the model only relies on parameters that are: i) derived from the POSS design (the equivalence of the POSS design and the implemented POSS must also be argued) and ii) known (have been tested/measured).
45.11	Check that the justification demonstrates that any analysis techniques used were appropriate for: a) the behavioural attributes of the model and of the specification element b) the notation used in the model c) the implementation technology/nature of the POSS.
45.12	Check that the justification addresses the trustworthiness of any other evidence used to substantiate the element. (This refers to non-verification evidence).

46	**Justification of a (non-behavioural) directly substantiated property element of a specification**
46.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of a (non-behavioural) directly substantiated property element of a specification i.e. check that the argument is coherent, suitably convincing, etc.
46.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
46.3	Check that the justification references the verification or other evidence being used to substantiate the element.
46.4	Check that the referenced verification or other evidence is for the transitional stage being assessed.
46.5	Check that the justification presents the analysis that demonstrates that the referenced verification or other evidence substantiates the element.
46.6	Check that the justification addresses the correctness of the analysis of verification or other evidence, if appropriate according to its complexity and the required confidence[40].
46.7	Check that the justification demonstrates that the analysis of verification or other evidence takes account of all the available relevant evidence i.e. that the property specified in the element is complete and independent of other behaviour/properties.
46.8	Check that, if appropriate, the justification demonstrates that the analysis of verification or other evidence addresses the integrity and confidence associated with the property.

[40] The justification may also increase confidence in the results of the analysis by appealing to the predicted results from design analyses.

46.9 Check that the justification addresses the trustworthiness of the verification used to substantiate the element, including justifying that: [text specialised for analysis in square brackets]

a) the measurement/observation of the property [result of analysis] was correct and correctly recorded

b) the evaluation arrangements under which the POSS was measured/observed [the setup and environment of the model] were appropriate to reveal the property (e.g. accuracy and calibration of test equipment)

c) the identity (including version) of the measured/observed POSS [model] was recorded, and matches the identity of [is derived from] the POSS for which the specification (where the element being substantiated resides) is valid

d) there is sufficient evidence that the property was observed during all operations of the POSS (for which the element is specified) [the results showed the property during all analyses]

e) there is sufficient evidence that the property was observed [analysed] under all appropriate environmental conditions

f) there is sufficient evidence that the property was observed [analysed] under all appropriate input conditions

g) there was an adequate search for counter-evidence of the property stated in the element being substantiated

h) the provenance of measurements/observations was recorded (e.g. the identity and version of the POSS [model] measured/observed and all relevant items associated with its test [analysis] environment/conditions)

i) the recorded measurements/observations [results] have not been corrupted since recording.

46.10 Check that the justification demonstrates that any model used for analysis was suitable, i.e.:

a) the specific model and the specific POSS are equivalent

b) the model represents the relevant aspects of the POSS

c) the model uses notations that are capable of representing everything necessary to determine the property

d) the model only relies on parameters that are:

i) derived from the POSS design (the equivalence of the POSS design and the implemented POSS must also be argued) and

ii) known (have been tested/measured).

46.11 Check that the justification demonstrates that any analysis techniques used were appropriate for:

a) the properties of the model and of the specification element

b) the notation used in the model

c) the implementation technology/nature of the POSS.

46.12 Check that the justification addresses the trustworthiness of any other evidence used to substantiate the element. (This refers to non-verification evidence).

47	Justification of a directly substantiated element of an architectural specification
47.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of a directly substantiated element of an architectural specification i.e. check that the argument is coherent, suitably convincing, etc.
47.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
47.3	Check that the justification references the verification or other evidence being used to substantiate the element.
47.4	Check that the referenced verification or other evidence is for the transitional stage being assessed.
47.5	Check that the justification presents the analysis that demonstrates that the referenced verification or other evidence substantiates the element.
47.6	Check that the justification addresses the correctness of the analysis of verification or other evidence, if appropriate according to its complexity and the required confidence[41].
47.7	Check that the justification demonstrates that the analysis of verification or other evidence takes account of all the available relevant evidence i.e. that the architecture specified in the element is complete.
47.8	Check that, if appropriate, the justification demonstrates that the analysis of verification or other evidence addresses the integrity and confidence associated with the architecture.
47.9	Check that the justification addresses the trustworthiness of the verification used to substantiate the element, including justifying that: [text specialised for analysis in square brackets] a) the observation of the property [result of analysis] was correct and correctly recorded b) the evaluation arrangements under which the architecture was observed [the setup and environment of the model] were appropriate to reveal the property c) the identity (including version) of the measured/observed architecture [model] was recorded, and matches the identity of [is derived from] the architecture for which the specification (where the element being substantiated resides) is valid d) there is sufficient evidence that the property was observed during all configurations/ modes of the architecture (for which the element is specified) [the results showed the property during all analyses] e) there is sufficient evidence that the property was observed [analysed] under all appropriate environmental conditions f) there is sufficient evidence that the property was observed [analysed] under all appropriate input conditions[42] g) there was an adequate search for counter-evidence of the property stated in the element being substantiated h) the provenance of observations was recorded (e.g. the identity and version of the architecture [model] observed and all relevant items associated with its test [analysis] environment/conditions) i) the recorded observations [results] have not been corrupted since recording.

[41] The justification may also increase confidence in the results of the analysis by appealing to the predicted results from design analyses.
[42] No example of architecture being sensitive to input has been identified.

47.10	Check that the justification demonstrates that any model used for analysis[43] was suitable, i.e.: a) the specific model and the specific architecture are equivalent b) the model represents the relevant aspects of the architecture c) the model uses notations that are capable of representing everything necessary to determine the property d) the model only relies on parameters that are: i) derived from the architecture design (the equivalence of the architecture design and the implemented architecture must also be argued) and ii) known (have been tested/measured).
47.11	Check that the justification demonstrates that any analysis techniques used were appropriate for: a) the properties of the model and of the specification element b) the notation used in the model c) the implementation technology/nature of the architecture.
47.12	Check that the justification addresses the trustworthiness of any other evidence used to substantiate the element. (This refers to non-verification evidence).

[43] No example of verifying an element of an architecture specification using modelling has been identified.

Phase 5 Step 6 Topic Tables

Safety of the planned transitional activities

The change safety case must justify that the transitional activities that will be undertaken during the transitional stage, or any potential deviation from them, will not compromise the safety of any services being provided during those activities.

Such a justification may include:

a. Identification of the full set of transitional activities that will be undertaken during the transitional stage, as a summation of:
    i. preparation activities for later transitional stages
    ii. clear-up activities from earlier transitional activities
    iii. co-ordination activities with internal and external parties
    iv. activities that place prepared parts into the functional system, and/or remove parts from it, so changing (or 'transitioning') the functional system/service.
b. Identification of the impact of the transitional activities, and of the identified potential deviations on the functional service being changed, or any other.
c. Whether the recovery plan addresses all credible outcomes from the transition activities and their potential deviations.
d. Whether all services/functional system states, which could result from credible potential deviations and their associated recovery actions, have been assured by the change safety case.
e. Justification of acceptability of the safety of the transitional activities.

The safety of any performance monitoring activities, necessary to collect assurance evidence, should be addressed within the scope of safety analysis for the functional system.

The appropriate rigour with which the change safety case needs to address these topics can vary tremendously, according to the associated risks. The candidate assessment activities below address the lower end of this spectrum, in terms of rigour of the change safety case arguments (regarding the safety of the transitional activities) and of rigour of assessment. For higher-level risk scenarios, complete impact analysis and complete Hazard Identification, causal analyses and/or consequence analyses may be warranted, the Planner can identify assessment activities from 'Scope of the Change' (Phase 5 Step 3) and the 'Appendix F – Candidate assessment activities for safety analysis models' section (page 191).

It would be normal to expect less rigorous treatment of the analysis and justification of recovery activities than the 'forward' activities of installation, commissioning and other transitional activities. It therefore would be usual for the planner to select less rigorous assessment activities to assess recovery activities - some candidate assessment activities below are specific to recovery activities. However, in critical scenarios, the planner should consider whether the

safety of intended recovery activities should be assessed in the same manner as transitional activities.

Further candidate assessment activities can be selected from those in Stage 4 'Determine whether the planned change is credible', to build confidence in the general suitability of the plans as a suitable basis for safety analysis or as detailed guidance to the assessor on specific aspects to assess.

48 The set of transitional activities that will be undertaken during the transitional stage	
48.1	Check that the set of transitional activities that will be undertaken during the transitional stage are clearly identified.
48.2	Check that the order and timing of the transitional activities that will be undertaken during the transitional stage are clearly identified for each activity (as far as is necessary for analysis of their potential impact).
48.3	Check that the identified the set of transitional activities appears to be complete.
48.4	Check that the set of transitional activities to be undertaken during the transitional stage include: a) the activities that actually implement the change to the functional system and service at the start of the transitional stage b) those preparation activities for later transitional stages that are to be implemented during the transitional stage c) those clear-up activities for earlier transitional stages that are to be implemented during the transitional stage d) external coordination arrangements, including notifying parties impacted by the change or who are required to make coordinated changes to properly implement the change e) internal coordination arrangements, including those to synchronise or sequence the transitional activities.
48.5	Check that the set of transitional activities for the transitional stage includes: a) Training for operators and engineers, and the facilities required for this b) Issuing of procedures c) installation, commissioning and connection of new equipment and interfaces. d) changes to, and commissioning of, existing equipment. e) Removal of replaced or obsolete equipment. f) Initiating the services to be provided during the transitional stage, and are provided while the other transitional activities are undertaken. g) Communication with other stakeholders concerning transitional activities, at the start of and during the transitional stage h) Internal coordination to synchronise and sequence the transitional activities i) Co-ordination with other changes j) Verification and assurance activities, including checking that the POSSs have been changed as planned k) Any specific activities required to ensure and maintain the security of the current and changed functional system.

48.6	Check that the transitional activities are defined sufficiently, such that they can be analysed for potential safety impact on the operational service being provided when they are carried out, including whether: a) Individuals and organisations undertaking the activity are defined. b) Responsibilities for undertaking the activity are defined. c) adequate procedures and methods are defined d) any resources required are: i) defined ii) specified adequately e.g. a full specification may be required if they are novel, or need to have specific or unusual properties iii) available, in consideration of other potential demands for the resource. e) the plans define when the defined activities are to be undertaken f) concurrent activities are considered g) time of day is considered h) other changes being made at the same time are stated and accounted for by the plans i) any uncertainties or assumptions are identified and are managed.

49 Analysis of the impact of the transitional activities, and of potential deviations	
49.1	Check that there is an analysis of the impact of the planned transitional activities, determining whether they have an impact on any operational services or systems providing an operational service. Note that transitional activities could impact a further service or system that is not otherwise changed or impacted by the proposed change.
49.2	Check that the analysis considers the potential effects on the operational service(s) that the change safety case has declared as being provided during the transitional stage.
49.3	Check that there is an analysis that identified the potential impact of: a) unintended effects (side effects) of the planned transitional activities b) credible deviations from the planned transitional activities c) credible deviations from the expected outcome of the transitional activities (usually additional effects).
49.4	Check that the impact analyses considered: a) the aggregated effect of all the transitional activities that will be undertaken during the transitional stage b) whether there are consequences of the sequencing and timing relationships (e.g. concurrency) of the transitional activities that will be undertaken during the transitional stage.
49.5	Check that it is determined that sufficient mitigations are available or else have been added to the arrangements for the planned activities.
49.6	Check that the methods used showed that the risk of the potential impact on the operational services is acceptable, by arguing that either: a) The potential effects have been identified and mitigated so that the risk from them is acceptable (perhaps negligible or ALARP) b) The potential effects have been included as contributors to the occurrence of service hazards in their safety analyses.

49.7	Check that a systematic method was used in these analyses.
49.8	Check that the analyses were based on sufficiently detailed plans for the transitional activities.
49.9	Check that the analyses were based on specifications, schematics, layouts, etc, that appear to be sufficiently detailed.
49.10	Check that the methods used to identify and classify the safety consequences are appropriate: a) in accordance with the Service Provider's SMS or regulations, if applicable b) with regard to the level of threat to the service provided during the transitional activities, and the potential consequences of effects on that service c) with regard to the 'one time' nature of the transitional activities, as opposed to continuous hazards throughout the operational period.
49.11	Check that the analyses identified impacts that might be expected from the types of activities planned.
49.12	Check that the people that performed the analyses were competent, according to: a) the nature of the transitional activities b) the location of the activities c) the things being changed and potentially impacted d) the impact and safety analysis techniques used.
49.13	Check that the analyses were executed completely, and appear to have analysed all planned activities.
49.14	Check that the analyses appear to have considered: a) all credible potential deviations b) all credible side effects c) sufficiently wide scope to identify any potential impact on the functional system or its environment d) all necessary functional system and environmental scenarios, operational modes etc e) deviations in intended coordination and communication f) deviations due to coordinating actors being unable or unwilling to co-operate in the expected time manner g) all vulnerable assets that could be affected by the change h) the influence of the environment of the transitional activity when identifying potential deviations i) potential impacts through the environment where the transitional activity will be conducted j) potential impacts arising from the use of shared resources k) impacts on all potentially affected services, not just those being changed.
49.15	Check that the assumptions made during the analyses have been validated.
49.16	Check that there is a justification that the analysis is complete and correct.
[The planner is reminded that the above candidate assessment activities may be augmented by using those from Phase 5 Step 3 'Scope of the Change' for greater rigour]	

50 Recovery plan (possibly contained within transition plan)	
50.1	Check that the recovery plan appears to address recovery from all credible potential unintended outcomes from undertaking the transitional activities, should the intended state not be reached.
50.2	Check that the recovery plan clearly identifies the resultant services/functional system states following execution of each recovery plan scenario.
50.3	Check that the activities defined in the recovery plan are, if appropriate, subject to safety analysis in the same manner as transitional activities.
50.4	Check that there is a justification that the recovery plan addresses recovery from all credible potential unintended outcomes, and in each case the planned set of recovery activities is complete and correct.
[The planner is reminded that the above candidate assessment activities may be augmented by using those from Phase 4 for greater rigour. Recognising that the transitional activities (already) include safeguarding mitigations to prevent the need to recover, in high risk situations it may still be appropriate to assess the recovery actions in the same way as a set of transition activities.]	

51 Justification of safety of potential services/functional system states during recovery and after recovery complete.	
51.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of safety of potential services/functional system states during recovery and after recovery complete i.e. check that the argument is coherent, suitably convincing, etc.
51.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
51.3	Check that there is a justification that, for every recovery scenario: a) the state of the functional services/systems when recovery is complete has been subject to appropriate safety analysis, considering the likelihood of recovery being required, the persistence of this recovery state, its normality and subsequent recommencement of transitional activities. b) any transient states of the operational services/functional systems occurring during the recovery period have been subject to appropriate safety analysis, considering the likelihood of recovery being required, the period of exposure of the transitory state, and the risk to the services.
[In high risk situations, it may be appropriate for the safety of the transient states during recovery to be justified as for a transitional stage.]	

52 Justification of acceptability of the safety of the transitional activities	
52.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of acceptability of the safety of the transitional activities i.e. check that the argument is coherent, suitably convincing, etc.
52.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
52.3	Check that the justification of the transitional activities shows how it was determined that the risk of the potential impact on the operational services is acceptable, by arguing that either:

	a) The potential effects have been identified and mitigated so that the risk from them is acceptable (perhaps negligible or ALARP) b) The potential effects have been included as contributors to the occurrence of service hazards in their safety analyses.
52.4	Check that the justification of the transitional activities shows that the impact analyses considered: a) the aggregated effect of all the transitional activities that will be undertaken during the transitional stage b) whether there are consequences of the sequencing and timing relationships (e.g. concurrency) of the transitional activities that will be undertaken during the transitional stage.
52.5	Check that there is a justification that the defined set of transitional activities for the transitional stage is complete and correct.
52.6	Check that there is a justification that the defined set of transitional activities to transition the functional system/service at the start of the transitional stage implements the planned change.
52.7	Check that the justification of the recovery activities shows the recovery plan addresses recovery from all credible potential outcomes from undertaking the transitional activities, should the intended state not be reached.
52.8	Check that, where appropriate, the justification of the transitional activities shows that: a) The impact on the functional system/all services that are impacted or potentially impacted by transitional activities, side effects, or credible deviations of the transitional activities, has been shown to be acceptable. b) The planned transitional activities have no impact on the service being offered whilst the transitional activities are conducted (apart from those that are intended to transition the service at the start of the transitional stage). c) The services/functional system states extant during the transitional activities have been shown to be safe by appropriate safety analyses, or are covered by existing procedures or safety case(s). d) Appropriate mitigations have been included to prevent errors being made in, and deviations from, the transitional activities and to ensure successful completion of the intended change. e) The transitional activities can reasonably be completed as planned, e.g. they avoid timing, coordination and resource issues[44]. f) The resources and tools will be as specified[45]. g) The transitional activities do not unnecessarily introduce or elevate risk to any operational service (ALARP). h) The transitional activities do not unnecessarily extend any period of increased risk to any operational service. i) (if applicable) it is acceptable to reduce or stop a service in the manner planned during the transitional activities. j) Appropriate operational fallback arrangements are in place should (normal) functional system failures occur whilst the transitional activities are being conducted, which recognise the modified functional system state due to the transitional activities. k) The transitional activities include adequate and robust coordination arrangements with all affected parties

[44] See 'Phase 4 Determine whether the planned change is credible' on page 62.
[45] Such a justification may require verification evidence - see 'Evidence and justification that resources for transitional activities are as specified'

	l) Adequate verification activities are included to decide whether the transitional activities are completed as planned, and the change has been made as planned (see decision criteria in 10.16).
52.9	Check that, where appropriate, the justification of the transitional activities shows that they appropriately address security issues, including: a) The provision of physical security measures that restrict access to prevent malevolent modification of the functional system, prepared parts, resources or tools. b) The prepared parts, resources and tools will not be compromised (e.g. supply chain issues). c) No security-related information is released. d) The personnel undertaking the transitional activities do not represent a security threat. e) Disposal of removed parts does not jeopardise the security of the service, e.g. by revealing security-related information, or by providing equipment useful in an attack. f) Appropriate measures have been included to prevent errors being made in, and deviations from, the transitional activities to ensure that security is not compromised.

Appendix E – Candidate assessment activities for elements of arguments

The arguments presented in a change safety case must make valid claims, using valid inferences (reasoning/justifications) and evidence. Due to the ubiquitous nature of argumentation, the checks provided below can be used with any planned assessment activity. The checks address:

a. claims (other than the top-most claim of the change safety case)

b. inferences

c. evidence

d. argument.

The planner provides guidance to the assessor on the application of these checks, in order to determine whether the change safety case makes valid arguments. This guidance could be established:

a. once for the whole assessment

b. for each assessment phase

c. for each topic area, applying to all justifications examined in that topic area.

In each case, the guidance could also be varied for each transitional stage.

The assessor has discretion over the application of further checks.

In highly critical applications, it may be necessary to argue that one or more arguments are correct and/or valid. Separate candidate assessment activities are not defined for this because those below could be applied to such arguments.

53 Claims other than the top-most claim	
53.1	Check that the claim is clear and well-formed.
53.2	Check that the claim is NOT ambiguous or vague, and does not use undefined terminology.
53.3	Check that the scope of the claim is clear.
53.4	Check that the scope of the claim is NOT ambiguous or vague, and does not use undefined terminology.
53.5	Check that the claim is supported by an inference, unless the claim is axiomatic.

54 Inferences	
54.1	Existence. Check that inferences: a) are provided in support of each claim, unless the claim is axiomatic

54.2 Proper argumentation. Check that inferences:

a) are clearly and appropriately presented and communicated

b) satisfy rules of logic and argument

c) are complete

d) cover the necessary scope

e) are relevant to the change specified in the change safety case

f) are adequately precise and accurate

g) are definitive, not equivocal ("should show that") or predictive ("will show that")

h) address any uncertainty in the supporting evidence, if necessary

i) address any uncertainty that the inference supports the claim, if necessary

j) do NOT make unreasonable unsupported claims or assertions

k) do NOT make unreasonable unstated assumptions

l) do NOT make circular arguments

m) do NOT use circular definitions (can make claims trivially true)

n) do NOT assume that all actors are benevolent, accounting for malevolent actors (security threats)

o) do NOT assume common, best or latest practice is adequate

p) do NOT assume the validity of experts or standards

q) do NOT assume that application of resources (e.g. cost, effort) means that the objective was accomplished

r) do NOT assume that properties of one thing are inherently properties of another due to an association (which may be weak or irrelevant)

s) do NOT assume that past (historical) properties are still valid

t) do NOT derive absolute conclusions for probabilistic situations

u) do NOT assume that the probability of a random event has been altered by its historical occurrence or non-occurrence

v) do NOT use statistically insignificant sample sizes

w) do NOT make quantitative claims from qualitative data or quantitative data whose precision is less than that of the claim

x) do NOT use biased data (e.g. non-random samples)

y) do NOT cite a lack of evidence that the claim is false, in support of a claim

z) do NOT consider whether important differences exist between similar physical or evidence items (e.g. different versions of something)

aa) do NOT make claims that two things are different from each other, without substantive evidence of the difference between them

bb) do NOT cite evidence that suggests, but does not properly support the truth of the claim

cc) do NOT claim that two events are causally related because they are correlated, failing to consider the possibility that correlation is due to chance or a common cause

dd) do NOT claim that one alternative is superior (or adequate) because the others are unattractive, failing to establish the relative superiority (or adequacy) of the alternative it advocates

ee) do NOT assume that a norm applies, failing to consider whether the scenario is exceptional (outside the norm)

ff) do NOT claim that a scenario is exceptional (outside the norm) without justification

	gg) do NOT use reasoning, or come to a conclusion, that is contrary to accepted experience, norms or common sense without justification hh) do NOT use novel reasoning without justification for why it has been used and its validity ii) do NOT limit the alternatives for a decision, assuming that one of them must be correct, and failing to establish that the alternatives encompasses all the possibilities jj) do NOT incorrectly use an accepted pattern of reasoning, failing to instantiate all of the required elements of the pattern kk) do NOT claim that a property holds for something because it holds for each of its components, failing to consider interactions between the components ll) do NOT claim that a property of something automatically holds for each of its components mm) do NOT fail to address counter-evidence nn) do NOT use a model that oversimplifies relevant aspects of the subject oo) do NOT include subtleties in the meaning of words or the structure of the sentence that lead to multiple interpretations of the same prose pp) do NOT use different meanings for a term within or between inferences or claims qq) do NOT use wording that hides quantities to promote a misleading favourable interpretation rr) do NOT comprise explanations that lack substance or meaning ss) do NOT use poorly-defined terms
54.3	Relationship to evidence. Check that inferences: a) are based on objective evidence and claims b) clearly identify the evidence and claims they invoke c) clearly claim what the invoked evidence shows d) invoke sufficient evidence to address the scope of the claim e) do NOT invoke evidence that is not yet available
54.4	Strength of argument. Check that inferences: a) account for known counter-evidence and rebuttals b) are sufficiently insensitive to (i.e. valid in the presence of) any uncertainty in supporting evidence or data c) are proportionate (e.g. in their detail) to their contribution to the overall argument d) provide an appropriate level of persuasiveness and formality of argument, to provide sufficient confidence
54.5	Justification of evidence. Check that inferences, when invoking supporting evidence and where appropriate[46], justify that: a) the evidence is of suitable quality b) the evidence is trustworthy c) the evidence is correct d) the evidence is configuration consistent with the functional system extant during the transitional stage

[46] This is an issue of arguments being sufficiently rigorous to provide the necessary confidence. If low confidence is sufficient, then a simplistic argument might be made on the basis of one item of evidence. If higher confidence is required, then a more complete argument would be made invoking additional evidence, e.g. about the pedigree of that item of evidence.

e) the evidence was collected in an environment that yielded evidence valid for the operational environment

f) the evidence is valid in all cases when it is used for multiple instances of any POSS, e.g. multiple instances of a system, multiple installations of equipment, multiple people elements or multiple uses of a particular procedure

g) the effects that Human Factors can have on the evidence during its generation and interpretation (e.g. error-prone evidence generation, observation or analysis) are accounted for.

55 Evidence

55.1 Existence. Check that the evidence[47]:

a) exists as stated in related inferences i.e. work-off items all completed

55.2 Proper evidence. Check that the evidence:

a) is uniquely identified

b) is unaltered

c) is of known provenance:

i) creator

ii) source material

iii) what it relates to

iv) methods used

v) conditions under which generated

55.3 Validity. Check that the evidence:

a) is valid for the specific service

b) applies to the change specified in the change safety case

c) was collected in conditions that match operational use, where appropriate (mainly applies to test and field service evidence)

d) is as claimed in the inferences

55.4 Adequacy. Check that the evidence:

a) is in a form that can be read, used, archived and retrieved

b) has an appropriate level of persuasiveness and its formality provides sufficient confidence

c) appears credible based on experience (e.g. provenance appears appropriate)

d) appears credible considering its provenance

56 Argument

[Note: These candidate assessment activities are intended to assess aspects of the overall argument that cannot be assessed by examining individual inferences, claims or evidence]

56.1 Validity. Check that:

[47] These activities are only applicable to evidence that is invoked by an inference; otherwise it is irrelevant (Service Providers have been known to supply large amounts of evidence, perhaps to impress the assessor).

a) counter-evidence and rebuttals[48] do not invalidate the change safety case

b) no common element undermines diversity of evidence, where this is depended upon to provide sufficient confidence

c) no common element undermines diversity of inferences, where this is depended upon to provide sufficient confidence

d) the validity of the argument as a whole is not undermined by any of the issues raised by the criteria regarding inferences (above)

e) known fallacious lines of argument are not used

f) there is no over-dependence on an evidence item due to use by multiple inferences

g) there are no arguments presented that appear to support the safety argument, but are not integrated into the overall safety argument (and so mislead or distract the reader)

h) the argument is valid for each instance, where there are multiple systems, multiple installations of equipment, multiple people elements or multiple uses of a particular procedure.

56.2 Completeness. Check that:

a) all necessary lines of argument are present

b) obvious lines of argument are not omitted

c) each argument has been developed until it is based only upon evidence or reasonable assumptions (that are validated elsewhere)

d) the argument identifies all necessary supporting claims and evidence to address the full scope of the claim it supports.

56.3 Consistency. Check that:

a) the overall argument does not exhibit any anomalies or discontinuities associated with contractual boundaries

b) terminology is used in a consistent manner

c) terminology is sufficiently defined to prevent ambiguity or inconsistency

d) the uses of context in the argument are consistent

e) assumptions made are not inconsistent.

[48] As well as arising from the assessor's wider experience, the counter-evidence and rebuttal may be collected and formed by the assessor during earlier Phases of the assessment, and during general interaction with the project.

Appendix F – Candidate assessment activities for safety analysis models

The safety analysis models presented in a change safety case must be valid.

The generic candidate assessment activities provided below can be used where the change safety case has used safety analysis models to:

a. set safety criteria (from higher-level known rate or from risk)
b. decompose safety requirements (from safety criteria)
c. predict safety performance (by composing lower-level rates)
d. compose behaviour of lower-level POSSs to justify elements of the specification of a higher-level POSS
e. analyse the safety of the transitional activities.

The planner provides guidance to the assessor on the assessment activities to be conducted, in order to determine whether the safety analysis models used in the change safety case are valid. This guidance should be provided at each point a safety analysis model is used, and address the elements used in the specific safety analysis model. The elements addressed by the candidate assessment activities are:

a. Hazards
b. Consequence models
c. Causal models
d. Overall properties of cause-consequence models.

The assessor should interpret the candidate assessment activities in the context of the purpose of the safety analysis model being assessed.

Whilst the assessor should comply with the planner's guidance, this should not prevent the assessor from recording any other issues identified with the safety analysis model whilst carrying out the planned activities.

Identified Hazards

57 Set of identified hazards	
57.1	Check that all hazards are uniquely identified.
57.2	Check that all hazards are stated clearly, are consistent and readable, and if necessary are supported by a full definition or description.
57.3	Check that the set of hazards, and the individual hazards, appears to be complete e.g. all reasonable hazardous states or events are represented.
57.4	Check that the hazards are specific instances of the types of hazard defined in the SMS procedures for change management for this type of change (see item 8).
57.5	Check that the hazards are either identified at the service level, or else there is a defined relationship up to the service level.
57.6	Check that each hazard is defined in terms of:

	a) the functional system/service state or event that is hazardous b) the functional system/service scenarios under which the defined hazard occurs e.g. the specific operational procedures[49] being exercised.
57.7	Check that all functional system/service scenarios are included within an identified hazard, or else included within another equivalent hazard.
57.8	Check that there is traceability from each hazard to a causal analysis of exactly one top event identical to the hazard.
57.9	Check that there is traceability from each hazard to a consequence analysis.
57.10	Check that there is traceability from each hazard to the predicted rate of occurrence and, if used by the change safety case, the tolerable rate of occurrence.

58 Justification of the identified hazards	
58.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of the identified hazards i.e. check that the argument is coherent, suitably convincing, etc.
58.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
58.3	Check that there is a valid justification that: a) the set of identified hazards is complete and correct b) the hazard identification[50] techniques used were appropriate c) the people that performed the hazard identification were competent, according to the nature of the change and the hazard identification techniques used d) the hazard identification procedures were executed completely e) the hazard identification considered all threats, all phases, all modes, all uses, all scenarios, etc f) the hazard identification process covered the correct system scope, which includes the scope of the change, as identified by the impact analysis (as assessed in item 17). g) the POSS specifications analysed were adequate to support hazard identification, and are applicable to the specific proposed change h) the hazard identification process considered all necessary functional system/service scenarios i) all assumptions made during hazard identification have been validated j) the hazard identification analysis considered all vulnerable assets (including those associated with the service and non-participants in the environment) that could be affected by the change k) the hazard identification analysis was revised[51] to maintain consistency with the impact analysis, identifying any new hazards, so that the hazard identification analysis is valid for the final scope of the change

[49] These are those approved procedures that govern the operation of the service provided.
[50] In this table, 'hazard identification' includes the identification of hazards that are associated with the scope of the change, as well as others that the safety analysis finds necessary to support the risk tolerability judgement of the overall service.
[51] Hazard identification must address all specified behaviour, and so needs to be revised whenever behaviour changes and specifications are updated.

	l) the hazard identification analysis was revised to identify any new hazards, if verification or other activities showed that any POSSs did not meet their specifications, e.g. additional behaviour and any identified limitations or shortcomings m) the justifications made regarding a) to l) are valid for the potential effects of malevolent actors.
58.4	Check that there is a valid justification for any potential hazards that were identified but subsequently discounted as being actual hazards.

Correctness of consequence model

59 Set of accident trajectories	
59.1	Check that the starting hazard and end accident for each accident trajectory is identified.
59.2	Check that each accident trajectory is uniquely identifiable e.g. by being given a unique identity, or by uniquely identifying the hazard and accident it connects.
59.3	Check that the notation used to record accident trajectories is able to represent the accident sequence accurately.
59.4	Check that the functional system/service scenarios, during which the hazard in the accident trajectory occurs, are identifiable e.g. the specific operational procedures[52] being exercised.
59.5	Check that the participating entities are identifiable for each accident trajectory.
59.6	Check that, where necessary, supporting material sufficiently explains the consequence models to demonstrate their correctness.
59.7	Check that the sequence of events occurring between the hazard and the accident is understandable from the accident trajectory and any material provided to describe the accident scenario.
59.8	Check that the granularity of the accident trajectories is appropriate (i.e. the trajectory represents individual decision points where each mitigation takes effect, and where alternative outcomes may result)?
59.9	Accident trajectory completeness. Check that: a) there is at least one accident trajectory for each identified hazard[53]. b) all possible accident trajectories that could result from each hazard have been identified.
59.10	Accident trajectory correctness – fidelity. Check that: a) the accident trajectories are plausible considering the physical layout of the Service Provider's specific scenario and the service and environment b) the accident trajectories do not contradict experience c) the accident trajectories reflect reported incidents d) if a template has been used to create accident trajectories, that these have been properly instantiated[54]
59.11	Accident trajectory correctness – level of detail. Check that:

[52] These are those approved procedures that govern the operation of the service provided.
[53] Multiple instances of a hazard may be provided to model different circumstances that result in materially different accident trajectories.
[54] e.g. no 'cut and paste' errors.

	a) the level of detail is commensurate with similar analyses from the Service Provider and for similar changes. b) individual mitigations are shown, where possible, rather than being treated collectively c) aggregated mitigations, if used, are plausible
59.12	Accident trajectory correctness - mitigation completeness. Check that: a) all designed[55] mitigations affecting the accident trajectory have been included b) where providence is a factor, it has been appropriately included
59.13	Accident trajectory correctness - mitigation correctness. Check that: a) The entities participating in providing the mitigation are identifiable. b) The action performed by the mitigation is adequately described. c) The locations at which the mitigations take effect are identifiable. d) The mitigations are specified as either: Service Provider procedures, service consumer procedures, or technical equipment functions[56]. e) The accident trajectory correctly models the effect of the mitigation in terms of the outcomes i.e. the 'mitigation successful path' results in either i) A different accident arising from the same hazard (perhaps shown in a different accident trajectory) ii) A safe state i.e. an incident occurs, not an accident. iii) A functional system/service hazard that is different from the initiating one f) The outcome is in fact in a valid safe state, when the result of a mitigation is claimed to be an incident (not an accident). g) The mitigations account[57] for variations in outcome or outcome rates, across the range of the service level conditions defined by the hazard and the path to the mitigation. h) The mitigations account[57] for variations in outcome or outcome rates, caused by variations in the state, operating mode or condition[58] of the functional system.
59.14	Accident trajectory correctness – mitigation effectiveness. Check that: a) The effectiveness (success rate) of each mitigation is stated, and seems appropriate. b) the analysis that supports the claimed effectiveness of each mitigation is identifiable. c) The supporting analysis is valid for the scenario given by the hazard and the path to the mitigation.
59.15	Accident trajectory correctness – accident correctness. Check that: a) The location of the accident is identifiable b) The entities involved in the accident are identifiable c) The terminating accident of the (accident) trajectory correctly relates to the circumstances defined by (the hazard and) the accident trajectory.

[55] This includes mitigations primarily designed to mitigate other accident trajectories, but excludes providential intervention.
[56] Improvised actions are not designed mitigations, and therefore should not be included.
[57] These variations can be accounted for either by representing them in the logic of the trajectory(ies) or by weighting the numerical value for success of the mitigation.
[58] Different system configurations, operation modes, fall-back operation, maintenance outage etc.

60 Justification of the set of accident trajectories	
60.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of the set of accident trajectories i.e. check that the argument is coherent, suitably convincing, etc.
60.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
60.3	Check that there is a valid justification that: a) the set of identified accident trajectories is complete and correct b) the accident trajectory identification techniques used were appropriate c) the people that performed the accident trajectory identification were competent, according to the nature of the change and the accident trajectory identification techniques used d) the accident trajectory identification procedures were executed completely e) the accident trajectory identification considered all threats, all phases, all modes, all uses, all scenarios, etc f) the accident trajectory identification process covered the correct scope, which includes the scope of the change, as identified by the impact analysis (as assessed in item 17). g) the specifications analysed were adequate to support accident trajectory identification, and are applicable to the specific proposed change h) the accident trajectory identification process considered all necessary functional system/service scenarios i) all assumptions made during accident trajectory identification have been validated j) the accident trajectory identification analysis was revised to identify any new accident trajectories, if the identified hazards or mitigation changed as a result of revisions to the change or of its impact k) the accident trajectory identification analysis was revised to identify any new accident trajectories, if verification or other activities showed that any POSSs or other systems did not meet their specifications, e.g. additional behaviour and any identified limitations or shortcomings. l) the accident trajectories correctly reflect dependencies arising from for common mode failures, co-location issues, accessibility, etc. These dependencies can be between either: i) the cause of a hazard and a mitigation in a consequent accident sequence ii) one mitigation in an accident sequence and another mitigation m) the accident trajectories correctly reflect the possibility of malicious interventions.

61 Mitigation analysis	
61.1	Check that each mitigation analysis identifies the accident trajectory and mitigation under analysis.
61.2	Check that, for each mitigation in each accident trajectory, there is a correct analysis of the effectiveness of each mitigation that addresses: a) the success rate of the mitigation in the context of the scenario given by the hazard and the path to the mitigation

	b) the availability of the mitigation[59] such that the mitigation is present and working.
61.3	Check that, for each mitigation in each accident trajectory, there is sufficient confidence in the analysis of the effectiveness of each mitigation, (e.g. adequate supporting evidence and rigour, and specific to the context of the scenario given by the hazard and the path to the mitigation).
61.4	Common cause analysis of mitigations. Check that: a) the analysis of availability of the mitigation identifies the POSSs and/or other systems that provide the mitigation. b) the linkages with other mitigations have been identified. c) the linkages with causes of hazards have been identified.

62 Justification of mitigation analysis	
62.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of mitigation analysis i.e. check that the argument is coherent, suitably convincing, etc.
62.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
62.3	Check that there is a valid justification that: a) the effectiveness of each mitigation on an accident trajectory has been analysed, including the success rate of the mitigation and its availability b) the mitigation effectiveness was determined in the context of the scenario given by the hazard and the path to the mitigation c) the mitigation analysis techniques used were appropriate d) the people that performed the mitigation analysis were competent, according to the nature of the accident scenario and the mitigation technology e) the mitigation analysis procedures were executed completely f) the specifications analysed were adequate to support mitigation analysis, and are applicable to the specific proposed change g) the analysis to determine availability of the mitigation appropriately considered failure of other systems on which the mitigation depends h) all assumptions made during mitigation analysis have been validated i) the mitigation analysis was revised, if verification or other activities showed that any POSSs or other systems supporting the mitigation did not meet their specifications. j) the mitigation analysis correctly reflect dependencies arising from for common mode failures, co-location issues, accessibility, etc. These dependencies can be between either: i) the cause of a hazard and a mitigation in a consequent accident sequence ii) one mitigation in an accident sequence and another mitigation.

[59] The candidate tasks for correctness of the causal analysis (69 Identification of hazard causes, page 169, and 70 Justification of identification of hazard causes, page 171) can also be undertaken here.

63 Set of identified accidents	
63.1	Check that each accident is uniquely identifiable[60].
63.2	Check that, for each accident, it is possible to identify its: a) Location b) Participating entities c) Condition of entities and harmful event e.g. fatal collision due to brake failure. d) Consequences of accident in terms used by Service Provider's accident severity scheme e.g. amount of harm to each of the vulnerable asset types involved e) accident type e.g. using an industry-standard classification scheme
63.3	Check that the accident trajectories that can lead to each accident are identifiable.
63.4	Check accidents are described consistently, and if necessary are supported by a full definition or description.
63.5	Check that the accidents are comparable with those for other changes made by the Service Provider.
63.6	Check that the accidents are comparable with similar changes made by other Service Providers.
63.7	Check that the set of accidents, and the individual accidents, appear to be complete e.g. all reasonable types and locations of accident are represented.
63.8	Check that the accidents are specified in the manner required by the procedures in the Service Provider's SMS.
63.9	Check that the accidents are either specified in terms required by legislation (e.g. usually an accident must involve harm to people), or else there is a defined relationship from the terms used to those used in legislation.
63.10	Check the reasonableness of the absence of variants of each identified accident, with alternative: a) Locations b) Participating entities (including all types of vulnerable assets) c) Conditions of entities and harmful event e.g. fatal collision due to inattention (instead of brake failure). d) Consequences of accident e.g. amount of harm to vulnerable assets
63.11	Check that there is traceability from each accident to its associated accident trajectory(ies).
63.12	Check that there is traceability from each accident to the predicted rate of occurrence of that accident, and if used by the change safety case, the tolerable rate of occurrence.

64 Justification of set of identified accidents	
64.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of set of identified accidents i.e. check that the argument is coherent, suitably convincing, etc.

[60] It is possible for an accident to be given more than one identity or reference, e.g. on different accident trajectories.

64.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
64.3	Check that there is a valid justification that: a) the set of identified accidents is complete and correct b) the accident identification techniques used were appropriate c) the people that performed the accident identification were competent, according to the nature of the service and the accident identification techniques used d) the accident identification procedures were executed completely e) the accident identification process considered all possible: i) Locations ii) Participating entities iii) Condition of entities and harmful event e.g. fatal collision due to brake failure. iv) Consequences of accident in terms used by Service Provider's accident severity scheme e.g. amount of harm to each of the vulnerable asset types involved v) accident types e.g. those in standard industry accident classification schemes f) the accident identification process covered the correct service scope, i.e. that part affected by the change. g) the specifications analysed were adequate to support accident identification, and define the changed service h) all assumptions made during accident identification have been validated i) the accident identification analysis considered all vulnerable assets (including those associated with the service and non-participants in the environment) that could be affected by the change j) the accident identification analysis was revised to identify any new accidents, if the identified hazards or mitigation changed as a result of revisions to the change or of its impact k) the accident identification analysis was revised to identify any new accidents, if verification or other activities showed that any POSSs or other systems did not meet their specifications, e.g. additional behaviour and any identified limitations or shortcomings.
64.4	Check that there is a valid justification for any potential accidents that were identified but subsequently discounted as being actual accidents.

65 Set of accident risks	
65.1	Check that the risk of each identified accident has been predicted: a) Check that each identified accident has been correctly classified according to its severity. b) Check that the probability of occurrence of each identified accident has been predicted correctly, according to the identified accident trajectories
65.2	Check that the probabilities of the accidents are consistent with each other and common sense.
65.3	Check that the calculations of accident probabilities are complete and consistent
65.4	Check that the analysis is comparable with those for other changes made by the Service Provider.

65.5	Check that the analysis is comparable with similar changes made by other Service Providers.
65.6	Check that aggregate accident probabilities have been identified from all precursor hazards to each accident.
65.7	Check that the aggregated probabilities for each accident have correctly accounted for different phases, operational modes etc, and according to the predicted period at risk appropriate for each.
65.8	Check whether the analysis results are highly dependent on (sensitive to) any factors whose probability or effectiveness is particularly uncertain.
65.9	Check that calculations take account of any cases where evidence shows that POSSs or other systems providing mitigations do not meet their specification, and any other identified limitations and shortcomings.
65.10	Check that the accident risk calculations cover all accidents relating to the scope of the change.
65.11	Check that, if the exposure period for vulnerable assets[61] is accounted for, then this is correctly analysed, either: a) in the accident trajectories b) during aggregation of the risks of different accident trajectories c) when determining accident severities.
65.12	Check that the effect of common mode failures[62], co-location issues, accessibility, etc on the accident risks calculations has been accounted for correctly.

66 Justification of the set of accident risks	
66.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of the set of accident risks i.e. check that the argument is coherent, suitably convincing, etc.
66.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
66.3	Check that there is a valid justification that: a) the set of accident risks is complete and correct b) the accident risk analysis techniques used were appropriate c) the people that performed the accident risk analysis were competent d) the accident risk analysis procedures were executed completely, including identifying the effects of common mode failures, co-location issues, accessibility, etc e) all assumptions made during accident risk analysis have been validated f) the accident risk analysis was revised, to reflect revisions to the change or of its impact g) the accident risk analysis was revised, if verification or other activities showed that any POSSs or other systems did not meet their specifications, e.g. additional behaviour and any identified limitations or shortcomings. h) the accident risk analysis included all accidents related to the scope of the change.

[61] The probability of assets being present at an accident location may vary according to the asset type.
[62] Such as those identified during mitigation analysis – see item 61.

Correctness of causal model

67 Set of top events	
67.1	Check that the top events are clearly identifiable and clearly stated.
67.2	Check that there is traceability from each top event to the associated hazard[63].
67.3	Check that there is one and only one top event associated with each hazard.
67.4	Check that the operational scenario(s) associated with a top event is identifiable.
67.5	Check that the deviation from intent associated with a top event is identifiable.
67.6	Check that the description of the top event matches its associated hazard: a) The deviation from intent b) The operational scenario(s) c) Any further conditions necessary for the hazard to be able to result in an accident.
67.7	Check that each top event has a causal analysis to predict its rate of occurrence[64].
67.8	Check that there is traceability from each top event to its predicted rate of occurrence, and if used by the change safety case, the tolerable rate of occurrence.

68 Justification of set of top events	
68.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of set of top events i.e. check that the argument is coherent, suitably convincing, etc.
68.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
68.3	Check that there is a valid justification if there is NOT one and only one top event associated with each hazard.

69 Identification of hazard causes	
69.1	Check that causes have been identified for each top event.
69.2	Check that each cause is uniquely identifiable.
69.3	Check that causal relationships are represented in a manner that is unambiguous and correctly model the relationships.
69.4	Check that sufficient information is present to understand that events are truly related as shown by the causal relationships (e.g. not a conceptual leap from a low-level failure to top event).

[63] It would normally be expected that the top events would be service level hazards. However, for small changes, it may be possible to justify that the safety risk has not been increased by showing that a changed POSS meets the existing specification and that its failure rates have not increased. These failures would be the top events in the causal analysis.

[64] This could involve identifying lower-level events (e.g. a fault tree analysis), or could be a direct prediction of the top event rate, i.e. the top event is treated as a base event.

69.5	Check that, where necessary, supporting material sufficiently explains the causal models to demonstrate their correctness.
69.6	Check that causes are clearly described, e.g. in terms of participating entities and event description (failure mode).
69.7	Check that the causes of top events appear to be correct, and none appear to be omitted.
69.8	Check that all entities that could contribute to the top event are represented among the causal events.
69.9	Check that reported incidents, and experienced or known potential causes are present among the causal states.
69.10	Check that causes associated with different operational modes are included, if applicable.
69.11	Check that known mechanisms whereby natural hazards and interference can cause the top events are present among the causal states.
69.12	Check that the causes of top events identified are comparable with those for similar changes made by: a) the Service Provider b) other Service Providers.
69.13	Check that the causes of top events have been developed to a sufficiently low level, such that individual causes are each attributed to a POSS for which it is plausible that sufficient evidence can be provided to show that: a) the POSS meets its specifications of behaviour (including failure modes) and performance b) the POSS exhibits the claimed failure rates for the failure modes in the causal states.
69.14	Check that the specifications analysed were adequate to support the causal analysis techniques used, e.g. to support identification of all dependencies and failure modes.
69.15	Check that the specifications analysed are applicable to the specific proposed change (and not an earlier proposal for the change).
69.16	Check that the results of the causal analyses show that the analyses have been carried out in a logical and systematic manner, according to the techniques used.
69.17	Check that the causes identified are consistent with the top event, including the scenario under which the top event (hazard) occurs.
69.18	Check that, where appropriate, combinations of events that can cause the top event have been analysed and correctly identified (e.g. 'AND' gates).
69.19	Check that, where appropriate, mitigations that prevent events from resulting in the top event have been analysed and correctly identified.
69.20	Check that all designed mitigations have been included.
69.21	Check that mitigations are precisely identified (not vague) to support analysis, including the participating entities.
69.22	Check that the mitigations are specified as either: Service Provider procedures, service consumer procedures, or technical equipment functions[65].
69.23	If a mitigation is not always effective, check that:

[65] Improvised actions are not designed mitigations, and therefore should not be included.

	a) The effectiveness (success rate) of the mitigation is stated, and seems appropriate. b) the analysis that supports the claimed effectiveness of the mitigation is identifiable. c) The supporting analysis is valid for the scenario given by the hazard.
69.24	If a mitigation is not always effective, check that the mitigation accounts[66] for variations in success rates, e.g. different operational modes, and across the range of the service level conditions defined by the hazard.
69.25	Check that, where appropriate, mitigations that prevent events from resulting in the top event are independent of the primary event.
69.26	Check that common causes of causal events, which bypass redundancy and diversity, are identified.
69.27	Check that causes due to transitional activities and maintenance activities are appropriately included, if the acceptability of their risk is not separately demonstrated[67].

70 Justification of identification of hazard causes	
70.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of identification of hazard causes i.e. check that the argument is coherent, suitably convincing, etc.
70.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
70.3	Check that there is a valid justification that: a) the causal analysis has identified hazard causes completely and correctly b) the hazard cause identification techniques used were appropriate c) the people that performed the hazard cause identification were competent, according to the nature of the change and the hazard cause identification techniques used d) the hazard cause identification procedures were executed completely e) the hazard cause identification considered all threats, all phases, all modes, all uses, all scenarios, etc f) the hazard cause identification process covered the correct scope, which includes at least the scope of the change, as identified by impact analysis (as assessed in item 17). g) the specifications analysed were adequate to support hazard cause identification, and are applicable to the specific proposed change h) each top event has valid hazard causes identified for the functional system/service scenarios for which it can occur i) all assumptions made during hazard cause identification have been validated j) the hazard cause identification analysis was revised[68] as necessary, so that the analysis is valid for the final version of the scope of the change k) the hazard cause identification analysis was revised to identify any new hazard causes, if verification or other activities showed that any POSSs or external services did not

[66] These variations can be accounted for either by representing them in the logic of the trajectory(ies) or by weighting the numerical value for success of the mitigation.
[67] See 'Plan and assess acceptability of transitional activities'.
[68] Hazard cause identification must address all specified behaviour, and so needs to be revised whenever behaviour changes and specifications are updated.

meet their specifications, e.g. additional behaviour and any identified limitations or shortcomings.

l) the hazard cause analyses correctly reflect dependencies arising from for common mode failures, co-location issues, accessibility, etc. These dependencies can be between either:

i) the cause of a hazard and a mitigation in a consequent accident sequence

ii) one mitigation in a hazard cause chain and another hazard cause chain.

m) the hazard cause analysis correctly accounts for fall back operation and different functional system/service operating modes

n) the hazard cause analysis correctly accounts for maintenance, facility interrupts, and periods of unavailability

o) the hazard cause analysis correctly accounts for failure of external interfaces, actions of external stakeholders

p) the justifications made regarding a) to o) are valid to show that the hazard cause analysis correctly included the potential effects of malevolent actors.

70.4	Check that there is a justification that the potential effects of transitional activities and maintenance activities have been appropriately included in the causal analyses, if the acceptability of their risk is not separately demonstrated[69].

71 Set of predicted occurrence rates of hazard causes (e.g. basic events in a fault tree)	
[Note: These checks are intended for the bottom-most behaviour that has been identified as a contributor to the occurrence of a hazard.]	
71.1	Check that the rate of each identified hazard cause has been predicted.
71.2	Check that the rate of each identified hazard cause is credible.
71.3	Check that the derivation of the predicted rate of each identified hazard cause is credible.
71.4	Check that the rates of the hazard causes are consistent with each other and common sense.
71.5	Check that the calculations of hazard cause rates are complete.
71.6	Check that the predictions are comparable with those for other changes made by the Service Provider.
71.7	Check that the predictions are comparable with similar changes made by other Service Providers.
71.8	Check that the predicted rates for each hazard cause have correctly accounted for different phases, operational modes etc, and according to the predicted period at risk appropriate for each.
71.9	Check whether the predicted rates are highly dependent on (sensitive to) any factors whose probability or effectiveness is particularly uncertain.
71.10	Check that predictions take account of any cases where evidence shows that POSSs do not meet their specification, and any other identified limitations and shortcomings.
71.11	Check that the effect of common mode failures[70], co-location issues, accessibility, etc on the predicted rates has been accounted for correctly.

[69] See 'Plan and assess acceptability of transitional activities'.
[70] Such as those identified during mitigation analysis – see item 61.

71.12	Check that the effect of transitional activities and maintenance activities are appropriately included into the predicted rates, if the acceptability of their risk is not separately demonstrated[71].
71.13	Check that the analysis technique used is appropriate e.g. Mil-Hbk-217 for electronic hardware.
71.14	Check that the analyses are consistent with the hazard scenario(s) i.e. they are valid for the context created by the environment and operating conditions.

72 Justification of set of predicted occurrence rates of hazard causes (e.g. basic events in a fault tree)

[Note: These checks refer to the justification of the rates of occurrence of the bottom-most behaviour that has been identified as contributors to the occurrence of a hazard.]

72.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of set of predicted occurrence rates of hazard causes i.e. check that the argument is coherent, suitably convincing, etc.
72.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
72.3	Check that there is a valid justification that: a) the set of occurrence rates is correct b) the occurrence rate prediction techniques used were appropriate c) the people that performed the occurrence rate prediction were competent d) the occurrence rate prediction procedures were executed completely, including identifying the effects of common mode failures, co-location issues, accessibility, etc e) the occurrence rate prediction is valid for the hazard scenario(s) e.g. the environment and operating conditions. f) all assumptions made during occurrence rate prediction have been validated g) the predicted rates for each hazard cause are correct for the applicable phase, operational modes etc, and according to the predicted period at risk appropriate for each. h) if any of the predicted rates are highly dependent on (sensitive to) any factors whose probability or effectiveness is particularly uncertain, then this was identified, and appropriate action was taken to minimise this dependency. i) the occurrence rate predictions were revised, if the hazard causes change i.e. there are new or deleted hazard causes, or the specification of the causes change j) the occurrence rate predictions were revised, if verification or other activities showed that any POSSs or external services did not meet their specifications, e.g. additional behaviour and any identified limitations or shortcomings
72.4	Check that there is a justification that the potential effects of transitional activities and maintenance activities have been appropriately included in the occurrence rate predictions, if the acceptability of their risk is not separately demonstrated[72].

[71] See 'Plan and assess acceptability of transitional activities'.
[72] See 'Plan and assess acceptability of transitional activities'.

73 Set of predicted hazard occurrence rates	
73.1	Check that there is traceability from each predicted rate of occurrence to the associated hazard.
73.2	Check that the occurrence rate of each identified hazard has been predicted correctly, according to the associated causal analysis.
73.3	Check that the predicted hazard occurrence rates are consistent with each other and common sense.
73.4	Check that the calculations of predicted hazard occurrence rates are complete and consistent
73.5	Check that the calculations of predicted hazard occurrence rates are comparable with those for other changes made by the Service Provider.
73.6	Check that the predicted hazard occurrence rates are comparable with similar changes made by other Service Providers.
73.7	Check that the hazard occurrence rate predictions have included the contributions from all the hazard causes.
73.8	Check that the hazard occurrence rate predictions have correctly accounted for different phases, operational modes etc, and according to the predicted period at risk appropriate for each.
73.9	Check that the hazard occurrence rate predictions have correctly accounted for fallback operational modes etc, and account for fault detection time and mean time to repair.
73.10	Check that the hazard occurrence rate predictions have correctly accounted for fault tolerance mechanisms, and the possibility of latent faults.
73.11	Check that the hazards occurrence rate predictions included the potential effects of transitional activities and maintenance activities, if the acceptability of their risk is not separately demonstrated[73].
73.12	Check whether the hazard occurrence rate predictions are highly dependent on (sensitive to) any factors whose probability or effectiveness is particularly uncertain.
73.13	Check that the hazard occurrence rate predictions cover all hazards related to the scope of the change.
73.14	Check that aggregation of the contributions to the hazard rate is correctly calculated according to the causal analysis, e.g. correctly accounting for exposure periods, the effects of common mode failures, co-location issues, accessibility.
73.15	Check that calculations are correct when combining rates and probabilities.

74 Justification of set of predicted hazard occurrence rates	
74.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of set of predicted hazard occurrence rates i.e. check that the argument is coherent, suitably convincing, etc.
74.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).

[73] See 'Plan and assess acceptability of transitional activities'.

74.3 Check that there is a valid justification that:

a) the set of predicted hazard occurrence rates is complete and correct

b) the hazard occurrence rates prediction techniques used were appropriate

c) the people that performed the hazard occurrence rates prediction were competent

d) the hazard occurrence rates prediction procedures were executed completely

e) all assumptions made during hazard occurrence rates prediction have been validated

f) the hazard occurrence rates predictions were revised, if the identified hazard causes or the way they combine change

g) the hazard occurrence rates predictions were revised, if verification or other activities showed that any POSSs or external services did not meet their specifications, e.g. additional behaviour and any identified limitations or shortcomings.

h) the hazard occurrence rates prediction included all hazards related to the scope of the change.

Overall properties of cause-consequence models

This section defines candidate assessment activities to assess the properties of the cause-consequence models considered as a whole, as opposed to their individual components (the causal analysis, consequence analysis, mitigation analysis and the associated rate and risk calculations). It is not a higher-level check of the complete set of components. However, this section does address whether the components of the set of cause-consequence models for the change are all present and correct, and correctly related.

This section does not include high-level assessment activities for individual components of the cause-consequence models. If this is required, then the assessment plan should also select appropriate activities for the desired components.

This section does not address the calculation of accident risk, as that is addressed in an earlier topic area, as is predicting the hazard rate.

75 Cause-consequence models e.g. a set of bow tie models, one for each hazard

75.1 Generic properties. Check that:

a) the cause-consequence models are for the Service Provider's specific POSS versions

b) the scope of the cause-consequence models is sufficient, for example, coverage of:

i) all related hazards

ii) all causes of the hazards

iii) all potential accidents for the hazards

iv) all operating modes.

c) the cause-consequence models for each hazard are:

i) correct

ii) complete

iii) accurate

iv) unambiguous

v) consistent

	d) the set of cause-consequence models is: i) complete ii) consistent
75.2	Check that the components of the cause-consequence models are summarised, presented and/or referenced in a manner that is coherent, clear and understandable, such that there is confidence in the results derived from the cause-consequence models.
75.3	Check that the set of components summarised, presented and/or referenced includes all expected components.
75.4	Check that all components summarised, presented and/or referenced are included in a cause-consequence model.
75.5	Check that each cause-consequence model includes all necessary components.
75.6	Component linkages. Check that: a) a referencing/traceability mechanism exists to link components into a cause-consequence model b) the connections made are correct c) additional spurious connections are not made between components.
75.7	Check that risk calculations correctly account for any mechanism that affects both the causal and consequence analyses for a hazard e.g. common mode failure and barriers that both reduce the probability of a hazard occurring and mitigate its effect.
75.8	Check that risk calculations do not included errors[74]: a) of omission e.g. omits to include the contribution of a causal model component b) of commission e.g. includes a contribution of a causal model component twice c) of double discounting by any factor e.g. a rate or probability being discounted according to asset exposure period more than once d) of indirect double discounting through different views of same factor e.g. both by hours worked and by daylight hours e) when aggregating rates or probabilities for multiple functional system/service states or operating modes, e.g. maintenance, facility interrupts, periods of unavailability.
75.9	Check that any assumptions made have been validated and are consistent with each other, and the circumstances and environment in the accident sequence.
75.10	Check that the cause-consequence models are complete and correct by examining sample threads: a) check an expected/known sequence from cause to accident b) check a sequence from a cause to an accident c) check a sequence from accident to a cause d) check from a hazard to a cause and to an accident e) check all accident trajectories, and hazard causes, that lead to a specific accident f) check that environmental conditions and operational circumstances associated with an accident are correctly reflected throughout the related accident trajectories and causal analyses.

[74] The way that calculations are made and managed may make some types of error more likely e.g. calculating by hand or spreadsheets versus an integrated modelling tool.

76 Justification of overall properties of cause-consequence models	
76.1	Check that there is a satisfactory argument that justifies the adequacy of the Justification of overall properties of cause-consequence models i.e. check that the argument is coherent, suitably convincing, etc.
76.2	Check that the justification complies with the generic rules for claims, inferences and evidence (see items 53, 54 and 55).
76.3	Check that there is a valid justification that: a) the set of cause-consequence models is complete, correct and consistent b) the cause-consequence models were revised as necessary, so that the models are valid for the final version of the scope of the change c) the cause-consequence models were revised, if verification or other activities showed that POSSs or other systems did not meet their specifications, e.g. additional behaviour and any identified limitations or shortcomings.
76.4	Check that there is a justification that the components of the cause-consequence models are managed (including configuration management) such that the correct versions of the components have been used in the risk calculation.
76.5	Check that there is a justification that the risk calculations linked the correct cause-consequence model components correctly.
76.6	Check that there is a justification that risk calculations do not: a) double discount by any factor e.g. a rate or probability being discounted according to asset exposure period more than once b) indirectly double discount through different views of same factor e.g. both by hours worked and by daylight hours
76.7	Check that there is a justification that appropriate precautions have been taken to ensure that risk calculations are correctly carried out, according to the method of calculation, e.g. calculations may be hand-calculated, use spreadsheets or use an integrated modelling tool.
76.8	Check that there is a justification that risk calculations correctly aggregate rates or probabilities for multiple functional system/service states or operating modes, e.g. maintenance, facility interrupts, periods of unavailability.
76.9	Check that there is a justification that it has been ensured that any assumptions made have been validated and are consistent with each other, and the operational circumstances and environment in the accident sequence.
76.10	Check that there is a justification that it has been ensured that environmental conditions and operational circumstances associated with an accident are correctly reflected throughout the related accident trajectories and causal analyses.
76.11	Check that there is a valid justification that: a) any mechanism that affects both the causal and consequence analyses for a hazard (e.g. common mode failure and barriers that both reduce the probability of a hazard occurring and mitigate its effect) would have been identified b) any causal events that can contribute to the cause/consequence model of more than one hazard has been identified c) the cause-consequence models correctly model any occurrence of a mechanism as described in a) or b) d) the risk calculations correctly account for any occurrence of a mechanism as described in a) or b).