Civil Aviation Authority

Guidance

Assessment of Change Safety Cases

Temporary CM info:
Saved by: stephen.barker on 17/12/2018 11:03:00

Executive summary

This document has been written to define a systematic approach for Competent Authorities 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 identifies the documentary artefacts that should exist in a completed change safety case, and for each one provides a sufficient set of candidate assessment activities. 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 competence in the system 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. The use of different assessment activities to vary the assessment 'rigour' or 'depth' is termed 'modulation'. This is achieved by choosing activities that have appropriate rigour, varying the sample size of the change safety case material examined, etc. Methods for systematically modulating the assessment, according to the risk factors, have not been 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. Where there are common types of change, it may be beneficial to instantiate the guidance to specifically address those types of change. This may also be beneficial for other reasons, for example for changes in a specific domain or context. Such instantiation could usefully include incorporating any specific regulatory provisions or risk criteria for the domain.

The guidance only considers whether the change safety case addresses the potential impact of cyber security threats on the safety of the services, but is not adequate to form the basis of a comprehensive security or cyber security assessment.

The next few pages provide a summary of the assessment method.

Assessment process summary

This document presents guidance to Competent Authorities on a risk based[1] approach for assessing a safety case for a change to a service. The assessment has the following Phases[2]:

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 Service Provider, its services, the change and the organisations involved.

   For the lowest grades of risk, the assessment inherently undertaken during Phase 1 may be judged to be sufficient to judge the safety of the proposed change, 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.

[1] Currently this document addresses the complete assessment of a change safety case and only provides an initial indication of how to vary the assessment according to risk.
[2] 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.

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.

   For each individual transitional stage, the assessment assesses:

   - the feasibility (not safety) of the planned transitional activities that implement the change during that stage
   - whether the planned transitional activities are sufficient to implement the stated change
   - whether the prepared parts to be inserted into the functional system will be available
   - whether the necessary resources to undertake the change will be available
   - 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
   - whether internal coordination arrangements, included to synchronise or sequence the transitional activities, appear credible and sufficient
   - whether the criteria to support transition decisions are adequate.

   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.

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 introductory material

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.

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 overall 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.

The appendices to this document provide additional material that is intended to provide further guidance and to explain the context within which parts of the assessment process take place.

Contents