

Assessment of Change Safety Cases



Stephen Barker discusses a recent publication from the Civil Aviation Authority (CAA) that provides guidance on the assessment of change safety cases. The guidance is Civil Aviation Publication 1801 (CAP 1801) and is freely downloadable from the CAA website.

CAP 1801, a guide on reviewing safety cases, recently received a minor update. As its original publication wasn't publicised, this opportunity has been taken to make its existence more widely known to the safety community.

The Guidance

The guidance in CAP 1801 is not specific to aviation, to ensure comprehensive coverage, and so is applicable in other industries. It makes no assumptions about the rigour or structure of the safety case being reviewed, and so includes a range of review checks that reflect the likely content of a range of safety cases, from basic arguments and evidence to the more onerous backing arguments that may only be present in safety cases addressing higher levels of risk. Part of the assessment evaluates how the risk acceptability criteria are justified, so supporting whatever approach is appropriate in the application domain.

"CAP 1801 is not specific to aviation, to ensure comprehensive coverage, and so is applicable in other industries"

Whilst CAP 1801 is focussed on review at the point of approval, by inherently defining the required content of a change safety case the material is informative for planning and development stages, and so can support review at these earlier project lifecycle stages.

CAP 1801 coherently addresses multiple concerns in an integrated method. Its assessment method allows for coordination of multiple assessors, accommodating proportionality issues by providing for reviews of varying rigour to reflect the varying content of safety cases addressing different levels of risk. The assessment process is structured to build understanding of the change and the change safety case in a logical sequence, and permits the assessment to be terminated early if it becomes apparent that the change safety case is inadequate.

The method recognises that it is almost always impractical to submit a complete safety case, including all supporting evidence. A safety case report is usually submitted, comprising descriptive material and only an extract of the safety case. Some key evidence items may be included as part of the submission.

Whilst CAP 1801 presents a systematic method, it provides no tutorial material, and assumes the competence of the assessors in all matters, including the application and regulatory domains.

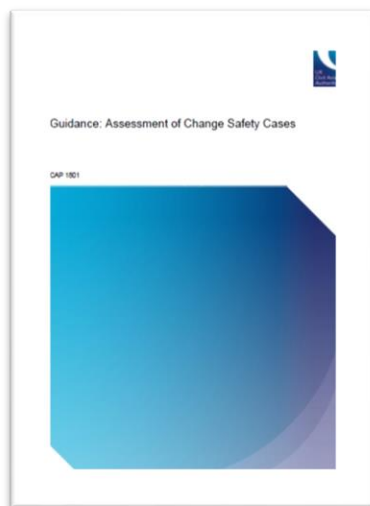
The rest of this article mainly comprises material extracted from CAP 1801, showing the approach behind the design of the guidance, and providing an overview of the assessment method.

Approach and background

A Competent Authority (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 that the claimed level of safety is acceptable. The change safety case assessment determines whether the change safety case has significant deficiencies, and hence whether it should be accepted or rejected.

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.

CAP 1801 considers that a change is implemented as one or more 'transitional stage'. Each transitional stage must be justified by the change safety case. 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.

The change safety case is mainly an argument about the predicted safety of the service that will be provided by the functional system. 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.

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:

- the change safety case addresses the complete scope of the change
- 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
- there is sufficient evidence to support the correctness of the specifications, for the operational configuration
- safety criteria for acceptable safety performance of the changed functional system/service have been established, and appropriate safety requirements derived
- the safety performance of the changed functional system/service has been predicted
- the predicted safety performance of the changed functional system/service is acceptable because it meets the safety criteria
- uncertainties do not undermine the change safety case
- the proposed transitional activities are feasible
- the transition activities will be undertaken safely
- there is sufficient evidence that the arrangements to implement the change will be provided
- when the functional system/service is changed, it will be made safe should the change not be successfully completed
- there is sufficient evidence that the arrangements to support the operational system will be provided
- justification that the change is a good change.

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, CAP 1801 defines a process to identify the elements of the safety arguments that address the above points, and organises the review process around these elements.

CAP 1801 offers guidance on planning and conduct of the assessment. 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 is structured in a way that can be applied concurrently in a coordinated manner by a team. Assessors must be competent to interpret the generic guidance of CAP 1801 in the context of a specific change.

CAP1801 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 addresses this by including planning activities during which appropriate assessment activities are defined, according to the circumstances prevailing. The approach used by the guidance to 'modulate' the assessment according to the risk is overviewed at the end of this article.

The generic method in CAP 1801 could be instantiated 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 assessment should also be conducted in accordance with applicable regulations and internal procedures. In particular, the CA will need procedures that address:

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

Summary of assessment method

The assessment method in CAP 1801 comprises six Phases:

1. Confirm change safety case is suitable for assessment

1) 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) As it is impractical to undertake all the candidate assessment activities in CAP 1801 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 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.

2. Determine risks that govern the assessment

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.

It is possible that, for the lowest grades of risk, the assessment inherently undertaken during Phase 1 could 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 transitional stage independent parts of the change safety case

3) 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) 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.

4. Determine whether the planned change is credible

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 transitional stage dependent parts of the change safety case

5) 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 Safety Management System 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 transitional stage is adequately completed.

Should any part of the assessment in this Phase 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) 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 for communication and resolution of the review findings, according to the regulatory context for review of changes.

6. Findings and reporting

Modulation of assessment according to risk

CAP 1801 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 overall approach implemented in CAP 1801 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, 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.

The assessment is planned by selecting from the candidate assessment activities defined in CAP 1801 for each topic of the change safety case (e.g. the specifications), 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. Planning is conducted incrementally as the assessment progresses, so that the assessment activities are planned on the basis of the latest, most complete understanding of the change and the change safety case.

“CAP 1801 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.”

Conclusion

The guidance consolidates many different facets of the assessment problem into an integrated and flexible approach. It is based on real-life experience, coupled with a desire to identify how safety cases can be improved by identifying what an assessor needs to determine whether it is acceptable. It is hoped that this guidance for assessing safety cases will assist other organisations wishing to establish a systematic approach to conducting risk-based assessments, as well as informing those preparing safety cases for assessment.

CAP 1801 was written by Stephen Barker and Andrew Eaton, and is freely downloadable from the CAA website [1].

References

[1] "CAP1801 Guidance: Assessment of Change Safety Cases": <https://www.caa.co.uk/CAP1801>, CAA, June 2021, Issue 1.1

Stephen Barker and Andrew Eaton

Following 20 years' experience in electronics and software development, safety and reliability consultancy and third-party inspection for various industries, Stephen Barker has for more than 20 years been a Safety Assessment Engineer for the Safety and Airspace Regulation Group of the United Kingdom Civil Aviation Authority. Whilst specialising in assessing software-based systems, he has conducted various oversight activities relating to the safety of air traffic control in the UK, with an emphasis on En-Route air traffic services. Stephen recently retired from the CAA.

For the past twenty-eight years Andrew Eaton was a National Requirements & Strategy Specialist for the Safety and Airspace Regulation Group of the United Kingdom Civil Aviation Authority. His field of responsibility was safety assurance of safety related Air Traffic Control and Management services. In this role he was responsible for advancing the UK's capabilities in these areas and sat on several international standards and regulatory committees. Andrew has an MSc in safety critical systems engineering from the University of York and is now an independent consultant.

The authors retain copyright of this article, which includes material extracted from CAP 1801.

