The Safety Critical Systems Club Transferable Safety – Fact or Fiction

Andrew Eaton

5th December 2013

A regulator's expectations for safety case re-use

A sceptics view on the re-use of
arguments and evidence in safety cases

Civil Aviation Authority

The Civil Aviation Authority

The CAA is the UK's specialist aviation regulator. Its regulatory activities range from making sure that the aviation industry meets the highest technical and operational safety standards to preventing holidaymakers from being stranded abroad or losing money because of tour operator insolvency.

Andrew Eaton

Safety critical systems engineer with the United Kingdom Civil Aviation Authority in the Aerodrome & Air Traffic Standards Division.

Focused on Regulatory Models, Models of Regulation, Regulatory Risk, Risk Assessment & Mitigation techniques, Safety Case Development and Safety Case Evaluation for CNS/ATM services and systems.

Aerodrome & Air Traffic Standards,
2W Aviation House,
Gatwick Airport South,
West Sussex,
RH6 0YR.
Andrew.eaton@caa.co.uk

Overview

- What a safety case is
- What are they for
- What Regulators do with them
- What Arguments does a Regulator look for
- The attributes of a safety case
- Re-use
- What makes re-use tricky
- Which attributes are more and less disposed to re-use

What is a safety case, what are they for and why do Regulators look at them

- A valid safety case is a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment.
- 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. regulator, judicial review or court.
- Regulators review safety cases 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.
- The Regulators is trying to determine whether the applicant has a effective understanding of what makes the system safe

Warning!

- The role of the regulator is to only approve a change if it has been adequately justified by the delivered safety case. It is not for the regulator to augment the safety case or to provide an alternative safety case in order to approve the change.
- Approval 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 Regulator's enquiries.
- The Regulator may reject the safety case because it is logically flawed or incomplete.
- He may also reject the safety case because he can rebut the argument based on his knowledge or his independently acquired information.
- The approval of a safety case does not transfer ownership of the risk to the regulator, it remains with the service provider

Fundamental arguments of a Safety Case

To argue that the changed* service or any transitional stages can and will be provided safely, the change safety case must provide structured, compelling, comprehensible and valid arguments that:

- the service to be changed and its constituent systems, subsystems, components, when operating within their context of use, are understood sufficiently to design a safe change,
- the safety risks associated with the change and any transitional changes have been determined ,
- the safety risks associated with the change and any transitional changes are acceptable,
- the change and any transitional changes are implementable,
- the changed service and any transitional services can/will be made safe should they be shown to be less safe than predicted.

*The Introduction of a new system is a change. Hence we are only interested in change safety cases.

The attributes of a Safety Case

- Specification of service and changes to be made
- Directly & Indirectly Impacted Components, their relationships & their specifications
- Safety analysis of the change (RAM)
  - Justification of operational arrangements
- Acceptability of risk:
  - The level of risk that will be acceptable
  - The level of risk posed by the service after the change:
    - Risk contribution from impacted parts of the system (Relative & Absolute)
    - Risk contribution from un-impacted parts of the system(Absolute)
- Installation, Commissioning, Transition and Recovery Plans
- Adequacy of arrangements to correctly implement planned change
- Arguments & Evidence that the changed system will achieve the level of safety that is a argued to be acceptable
- Validity of argumentation of above

Re-use

What could be re-used ?

- The whole argument structure of the safety case e.g. plot extractor using the same strategy as for a plot combiner
- Descriptions
- The argument strategy
- Elements of the safety case argument with evidence
- Fragment (pattern) of the safety case argument without evidence
- Evidence

Where might it be re-used ?

- Systems and their intents are very similar
- Differing systems

The problem is context!

- Context of use of the physical component
  - Input domain
  - Interfaces
  - Local environment
- Context of use of the safety case element/fragment
  - The architectural Impact of the element or fragment on the recipient safety case
    - Context of use
    - Required confidence
  - Consistency of arguments and evidence
  - Completeness of arguments and evidence

So can arguments & evidence be re-used in a safety case ?

YES but.....

- the recipient safety case must be valid
  - In order to make the re-use of elements of a safety case viable the context of the two uses must be identical. This is unlikely to be the case for any sizeable or significant element of a safety case without the additional effort needed to take account of the differences of context.
  - The re-used argument must remain salient in its new environment i.e. have the same relevance and provide appropriate confidence
- and the regulators belief that the applicant has an effective understanding of what makes the system safe should be undiminished.