Misuse of safety cases

Ello Weits and Stefano Stanghellini, 23 October 2019

Disclaimer

- “This is a work of fiction. Names, characters, places and incidents either are products of the author’s imagination or are used fictitiously. Any resemblance to actual events or locales or persons, living or dead, is entirely coincidental.”
- Moreover, the presentation of the story is rather black and white.

More introductory remarks and contents

- Topic of this presentation is misuse of safety cases
  - The subject is part of a broader issue: this presentation is ‘pars pro toto’. Focus on (existence and conclusions of) documents instead of processes can be counterproductive.
- For simplicity we will describe three ways of producing safety cases, A, B and C (and of course the correct one is no. C).
- What follows is a plea for moving from a focus on safety cases (A, B) to safety management (C).
- Largely a supplier perspective is adopted.

A. Collect
B. Pull
C. Push

A. External consultant collects what is there

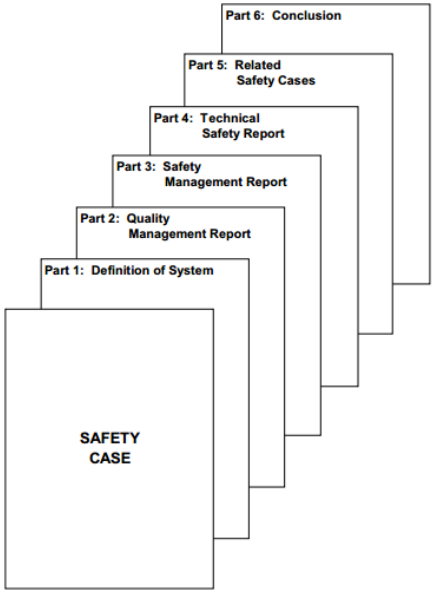


Figure 3 – Structure of Safety Case

- Safety case writing: special assignment for external consultant, flown in towards end of project
- At the Safety Case Symposium 2018 in Singapore Mike Bates writes about the still existing practice of safety cases as a ‘paper exercise’ performed just for regulatory reasons, with a lack of involvement from operators and maintainers. The writing is often outsourced to consultants who “do not know the company or the facility”.

Dialogue on where we are now (B. Pull)

- [VAL/SAF] The test report mentions many postponed tests. When will they be executed?
- [VER] This depends on the availability of the extended test environment. We do not know when that will be.

After a long time

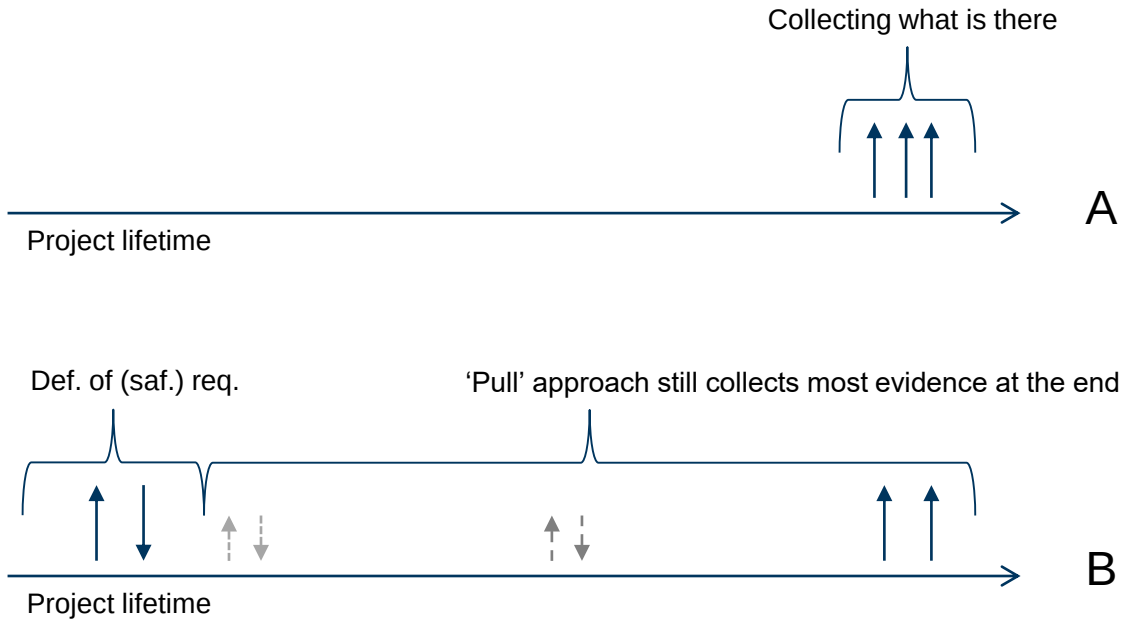
- [VAL/SAF] The safety case is due next month. How about executing the postponed tests?
- [PM] Indeed, we have to allocate extra resources to close this gap. Can you indicate which ones are minimally needed for the safety case?

The Pull approach is always late.

VAL = Validator, SAF = Safety (Manager), VER = Verifier (tester), PM = Project Manager

From Collect to Pull

- A: external consultant
- B: safety case writer internal
- As safety manager already pulling during development
- Still concentration of activities in the very last weeks or even days – checking consistency



"It is increasingly recognised by both safety case practitioners and many safety standards that safety case development, contrary to what may historically have been practised, cannot be left as an activity to be performed towards the end of the safety lifecycle."

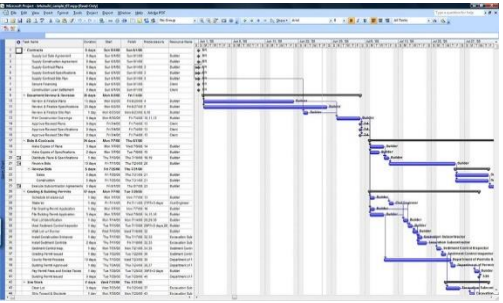
(Tim Kelly, in "A Systematic Approach to Safety Case Management", 2003 SAE International)

Why is late/delayed action harmful?

- Insufficient checks in external inputs
- Reductions in amount of evidence (or shortcuts taken when collecting evidence)
- Certain technical/functional issues are discovered late, when change of baseline is no longer possible > unnecessary restrictions and workarounds
- Omissions in project documentation
  - Documentary inconsistencies have been positively investigated in safety case (i.e. all required changes known and listed), but backlog can do harm afterwards,
  - Backlog includes cleaning up design documents, processing retrofits, updating test procedures and test tools, finalising manuals for installation and maintenance.

  Note that in the Pull approach safety documentation tends to maintain a shadow monitoring of the project status, via separate recording of e.g. Assumptions, Dependencies and Caveats (ADC, cf. Yellow Book, issue 4, chapter 12)

Causes and Why is it difficult to change?



- Human nature
- Strong focus by project management on simple milestones in a project schedule
  - Has safety case been completed?
  - Has it been assessed and accepted by the ISA?

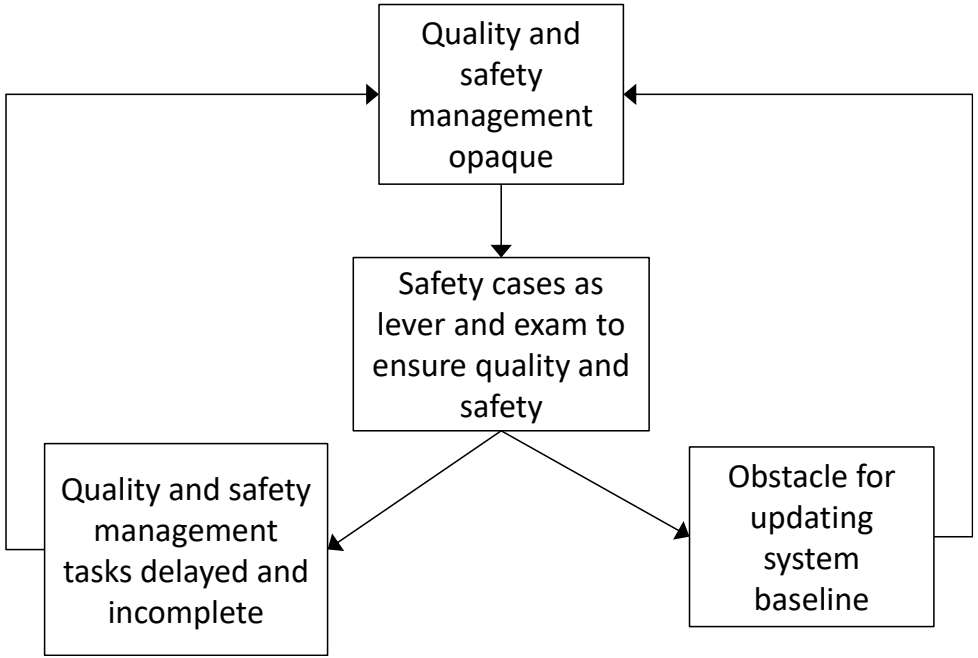
  Defining good indicators for progress of safety management and monitoring these indicators is difficult
  - Project management starts pushing for co-operation only when deadline for safety case delivery is approaching
- Customer does not want to interfere with safety management, partly because safety management by the supplier is rather opaque
  - Strong focus on the same simple indicators
  - Safety case delivery as lever for quality and safety

We end up in a vicious circle

2nd effect of strong focus on safety case as project milestone:

Tendency to freeze system baseline captured in safety case (also when changes are not safety related)

> more unnecessary workarounds > more uncertainty about safety management



C. Push instead of pull

- Do what is in the standards
- Quote from Cenelec
  - EN 50126:2017, Part 1, §8.1. “The safety case consists of the documented structured safety justification which […]”
  - Only few pages are devoted to the safety case. Almost all of the text relates to RAMS and safety management activities.
  - Safety activities are defined throughout the lifecycle.
  - Thus the safety case is the safety justification, which summarises the results from the safety management process. This is a ‘push’ relationship: the safety management process produces results, driven by requirements imposed on that process.

Success factors of Push

- Execute safety management process from the start
  - aligned with (integrated with) the other processes of the project such as: development process, quality process and V&V process
  - appropriate KPIs are set so that project management can monitor the progress of the safety management processes (and other processes) > transparency for project management
- Alignment with customer > transparency for the customer

Why is it difficult to change, revisited?

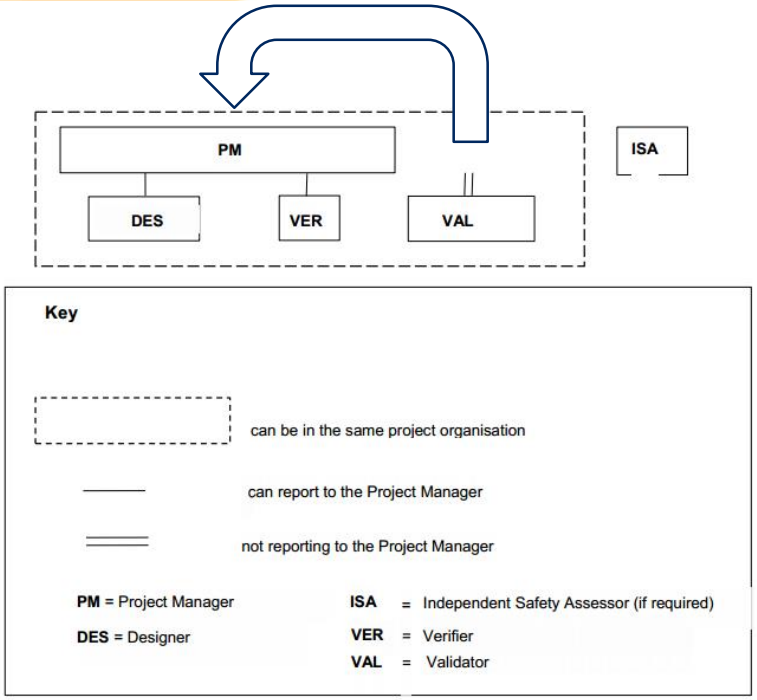


Figure 5 — Independence of Roles in the early phases (phases 1 to 4) of the lifecycle

- (Human nature never changes)
- *Push* implies that safety managers stop staying at a distance, for reasons of independence, but more directly ensure delivery of evidence (and do not hesitate to block next steps in a project when needed)
- How to avoid, in the case of *strong* safety management, that ‘safety’ takes control over the project?

Side-remark

- This presentation was about worries, instead of successes.
- Sometimes it is a relief to express worries and failures. Everybody likes to talk about worries, and to complain about what others fail to do (correctly). But usually in private circles.
  (Talking about failures is even less popular - though the podcast “How to Fail with Elizabeth Day” is very popular in the UK.)
- So, the stage is usually reserved for success stories.
- But we hope this discussion of worries helps us, personally and as a profession, to improve further.

Conclusion

- Compromise with human nature
- Follow the standards
- Explain (to all involved) why the safety management process is more important than the by-product safety case
- Make the safety management process more transparent
  - For project management
  - For customer

  (Then they will cling less to safety cases.)