Misuse of safety cases

Ello Weits, Movares
Stefano Stanghellini, Alstom

SUMMARY

In the everyday practice of railway signalling projects safety management seems to be the same as delivery of safety cases. There is a very strong focus on producing safety cases which, after positive ISA statements have been obtained, are submitted to a regulator (usually the NSA).

After ISA assessment and approval by the regulator any change to the baseline makes the safety case invalid, unless assessment and approval processes are restarted. Safety cases usually are Word documents, full of references to other documents regarding design, HW and SW versions, V&V documents and reports, safety analyses and studies, as-installed baseline etcetera. Updating safety cases and renewal of assessment and approval therefore are time-consuming tasks. In summary there is a severe penalty on changes to a baseline (implementing improvements and upgrades), once the safety case has been finalised and assessed. They tend to immobilise the status quo.

A second and more important and unfortunate side effect of the focus on safety cases is that the safety case and its approval tend to drive in various ways the safety management processes, instead of the other way around. The deadlines for completing the safety case are transferred to the safety management processes. These processes and their supporting quality management processes are likely to be delayed until the safety case has to be completed. Furthermore, the scope of the safety management processes tends to be reduced to what needs to be captured in the safety case. Instead of a push relation (safety management is summarised in the safety case) we often see a pull relation (the summarising safety case reduces the scope of the safety management processes). In summary, the set-up of the safety cases, for people not involved in safety, determines scope and timing of safety management work.

This too strong focus on the safety cases (at the cost of safety management) process is seen both at supplier's and at customer's side. Partly because of contractual reasons discussions between customer and supplier tend to concentrate on the delivery of safety cases that are positively assessed by an ISA. Then it is up to, firstly the safety manager and possibly to ISA to proactively request and inspect evidences that must be produced during the life cycle of the project.

*The paper describes the situation just sketched in more detail and outlines a solution. In essence the solution is to clearly separate safety management from the delivery of safety cases. As Wim Coenraad wrote in 2009 on behalf of the International Technical Committee of the IRSE (in "Towards the one page safety case: less paper and more assurance"): "any project, any supplier that applies the systems- and safety assurance processes that are now the norm in our industry […] should not need more than ten pages and two weeks [for a safety case] to explain all that and convince their Independent Safety Assessor (ISA)". In other words safety management is the central, continuous and controlled activity; safety cases are just a by-product, a "snap-shot" of that activity (as defined in the CENELEC standard EN 50126:2017: "*The safety case consists of the documented structured safety justification").

1 INTRODUCTION

Both authors have been involved in the safety management of several large signalling projects. The drive to write this paper is certainly fuelled by these projects. But we also draw from experiences of colleagues.

The examples in this paper are taken from experiences. But in the transfer to this paper they have been simplified and maybe even distorted, so that their illustrative character is emphasised. Not only the examples, but also the argument is characterised by simplification and thus exaggeration. In other words: this paper is to some extent is a work of fiction.

This paper has grown out of the observation that many people presume that much of our work consists in writing safety cases. And these safety cases, even if they are started at the first stage of the projects, can only be fed with most of the evidence at the very end of a project phase shortly before the start of a test campaign or the start of

commercial operation. In the last weeks before, such a deadline, the project as a whole, but safety management in particular gets absorbed in a frenzy of activities:

- Collecting information from all sides.
- Checking that all references in the safety cases are still up to date: have some supporting documents been updated in at late stage without notification?
- Waiting until the last minute for information like verification reports and test reports.
- Checking the quality of inputs (including verification reports) and validating them.
- Checking consistency of information.
- Checking lists: have issues been closed yes or no?
- Reading endless series of emails.
- Propagating last minute changes through supporting documents and the safety cases.

Such a period of intense activity seems often heroic, but is also wearing out the people involved. Moreover, other important work is postponed. The workload at the end of a project phase (in particular just before the start of Commercial Operation) is immense. This is in itself a reason to look for a change.

But we can also observe that the quality of the safety documentation is just not as good as it could have been. This is perhaps the real negative effect of the current focus on safety cases.

The remainder of this paper is organised as follows.

- In section 2 we discuss the relationship between safety management work and safety cases in terms of push and pull.
- Sections 3 and 4 deal with the effects and causes of the pull relationship.
- In section 5 we sketch the outline of a push approach.
- Section 6 formulates conclusions.

2 PUSH AND PULL

What does a safety manager do? The simplified picture is that initially he defines safety requirements and at the end he writes safety cases. If the safety requirements are inherited from an earlier project, the whole emphasis lies on the safety case writing.

This picture, that can be found among people not involved in safety (like project managers, both on customer and supplier side), ignores the essential difference between safety management and safety case writing. In this section we will elaborate a bit on the difference.

The Common Safety Method for Risk evaluation and assessment (CSM RA) [1], which regulates risk assessment for mainline railways in Europe, emphasises the risk assessment process. The regulation is brief on the "Demonstration of Compliance with Safety Requirements" (chapter 3 of Annex I). The regulation also provides only a few requirements on the documentation that must be produced (chapter 5 of Annex I). In particular the CSM RA does not mention safety cases.

The CENELEC standard EN 50126:2017 [2] deals with safety management as part of RAMS management. The standard does mention safety cases as a specific product/deliverable. What the standard says about safety cases, can be summarised as follows.

- EN 50126:2017, Part 1, §8.1. "The safety case consists of the documented structured safety justification which provides the evidence of how the system under consideration complies with the specified safety requirements, within the defined scope of its proposed use." The safety case "allows those who are to use the system to have confidence that the system complies with the specified safety requirements."
- The safety case is a document that needs to be completed only at the end just before independent safety assessment and acceptance. Part 2 says (§6.2) that "Whenever independent safety assessment is

required for the system under consideration, this is performed before system acceptance, in order to provide additional assurance that the necessary level of safety has been achieved."

- EN 50126:2017, Part 1 has 1 chapter on safety cases (chapter 8, 2 pages) and also Part 2 has 1 chapter on safety cases (chapter 6, 6 pages). All other chapters are devoted to the RAMS management process (Part 1) and the Safety management process (Part 2).

We can conclude that the safety case is the safety justification, which summarises the results from the safety management process. This safety management process is part of the system life cycle, as shown in Figure 7 in part 1 of the EN 50126:2017 [2].This is a 'push' relationship: the safety management process produces results, driven by requirements imposed on that process (and of course the signalling project at hand).

In practice we often see a 'pull' relationship. The set-up and writing of safety cases determines scope, extent and timing of safety management work. This pull relationship has two aspects. First, the focus on safety cases as prime deliverable tends to reduce the scope and extent of safety management work to what is 'useful' for the safety case. Secondly, the timing of safety management work will be adjusted to the time the results are needed for the writing of the safety cases. We note that, even though EN 50126:2017, Part 1 repeatedly says that the safety case should/shall be prepared from phase 6 onwards, in practice the safety case sits waiting being rather incomplete until the very end.

In the next section we discuss in more detail why this shift of emphasis is unfortunate.

But first let us present a piece of good news! In the Safety Case Symposium 2018 [3], a few papers dealt with the fact that writing safety cases can be an activity that is only undertaken as an obligation. Mike Bates writes about safety cases as a 'paper exercise' performed just for regulatory reasons, with a lack of involvement from operators and maintainers. The writing has been outsourced, according to Mike Bates, to consultants who are not familiar with the company or the facility. Bronwyn Brookman Smith notes that a safety case is intended to be a 'live' document, but updating and maintaining the Safety Case to ensure it remains current continues to be problematic. The main cause is that the Safety Case development process is seen as a project, a one off task to achieve a specific goal.

In our experience, safety cases of railway signalling systems are written by persons well involved in the signalling projects and much effort is devoted to capture the essential information from the safety cases to feed the Safety Management Systems of the customer or to allow the customer to prepare its own Safety case, when applicable.

3 CONSEQUENCES OF PULL

3.1 Immobilisation of baselines

After ISA assessment (and, if appropriate, approval by the regulator) any change makes the safety case invalid, unless assessment and approval processes are restarted or unless the modification can be shown as insignificant. In practice it is difficult to make a distinction between insignificant changes and significant changes. So, the 'safe' reaction is not to touch a baseline once it has been 'stamped' by the ISA.

Upgrading the safety cases and redoing the assessment and approval processes is complicated by the fact that safety cases are usually Word documents, full of references to other documents regarding design, HW and SW versions, as-installed baseline etcetera. Updating safety cases and renewal of assessment and approval therefore are time-consuming tasks. A related problem is that several labels (in particular baseline numbers) reach, after assessment, a kind of 'proven' status, also outside of the core documentation. Changing the baseline after assessment thus creates confusion, partly because the old baseline numbers live on for a while, even if the core documentation has been consistently updated.

In summary there is a severe penalty to changes to a baseline (implementing improvements and upgrades), once the safety case has been finalised and assessed. This penalty tends to immobilise the status quo.

> Example. Due to a minor error in the calculation of approach distances, a restriction on manual route cancellation had to be formulated: "Manual Route Release shall only be used, when the Signalling Operator knows that no train is approaching or any train approaching the route concerned is at standstill." This restriction was in place for a long time, because it was decided not to update the GA.

This situation is one of the obstacles for timely improvements. In this context we refer to the paper 'Command and Control 4.0', by Josef Doppelbauer [4]. On page 8 the author mentions as one of his goals "'migrateability', followed by continuous updateability".

A timely response is not only needed for a timely response to bugs or to include enhancements (for example improved equipment), but it is also (increasingly) needed to respond to cyber security threats. Norbert Howe wrote (in the paper "Cybersecurity in railway signalling systems" [5]) that "Security adds to safety but should not be mixed with it – it is like two sides of the same coin, but they have to be looked at and covered separately. Why?

- Update cycles for the signalling system are much longer than those needed for the security coverage.
- Even though design and constructive precautionary measures will be taken, security updates may be needed frequently, comparable to common IT."

In this paper we argue that the "update cycles for the signalling system" are affecting, via the safety cases and underling documents, the update cycles of the security updates. Indeed, it can happen that because of a customer request, security patches appear in the same list as interlocking issues.

A suggestion to avoid this issue is to maintain segregated the two aspects of the railway safety and security, even if at the end they can have the same final catastrophic effect. In this way maintaining the system updated in terms of security is much easier and can be done quicker.

3.2 Postponement of quality and safety management tasks

Because of the focus on safety cases the contractor is tempted to finalise all kinds of tasks only at the time the safety case needs to be completed. If this happens we end up in a situation in which both customer and contractor misuse the (need to finalise the) safety case as a lever to clean up the administration, to bring configuration management to a (temporary) conclusion (enforcing completeness and consistency of the final baseline), to complete the hazard log, in summary to finalise all pending tasks concerning quality management and safety management.

Here are some symptoms of delayed quality management and safety management.

- (Information about) the baseline consists of many files: specification documents (Word documents, Excel documents), drawings, V&V documents (Word documents, Excel documents), SW files etc. In the end it is up to the safety case writer to demonstrate completeness and consistency of the final baseline (that is used for testing and/or for operation). If documenting completeness and consistency is left to the safety case writer, some details (like change requests in status 'recorded' or not closed after realisation) may be overlooked.
- Documents such as drawings may formally be in draft state (but nevertheless in use for detailed design, manufacturing and installation). In particular test procedures and manuals may be lagging behind. The need to complete the safety case(s) is a lever for the completion of these documents.
- Also design changes and retrofits may be informally recorded, until the need to complete the safety case(s) is a lever for completion of the design description (as designed baseline), product baseline (of HW and SW items) and the as built baseline.

The pull approach leads to omissions. What isn't requested, is not (always) done. If in a late stage the customer or the ISA start making demands on the evidences supplied in the safety case, it is tempting to provide only the minimum evidence asked for. And this evidence is supplied at the time it is asked for. This can be much too late for changes/improvements.

> Example. Reuse of data prep tools developed long before the EN 50128:2011 came into force. Formally validation of these tools in accordance with the EN 50128:2011 can be postponed. The existence of grandfather rights make this possible. When the tools have to be upgraded for use in a slightly different context, ad hoc actions are needed to produce the necessary evidences. The drawback is that the ad hoc actions may be directed at the application at hand, so that the next time the work needs to be repeated.

Once we are in this situation, the doubts about pending tasks lead to requests to frequently update the safety case and have each update of the safety case fully assessed by ISA. The consequence is that this workload becomes

even more reason to keep baselines frozen as long as possible. Changing/updating a safety case is seen as a major obstacle.

- Safety case undergoes major revision. All references have to be checked.
- Re-assessment by ISA.
- Approvals (by e.g. NSA) become invalid and/or need to be updated.

Postponement of quality and safety management tasks may also lead to a situation in which external inputs are accepted in a preliminary state (without timely verification). In particular assumptions concerning external inputs handed over by the customer present a risk. In the period before safety cases are finalised supplier and customer can have diverging opinions about the checks of customer. The customer assumes that supplier will take care of integration of these inputs, while at the same time the supplier does not venture to doubt the quality of the customer inputs. Thus for a long time, consistency and completeness of inputs are not (sufficiently) checked. Only in a late stage a check of (consistency and completeness of) inputs is performed (when the time to compile safety cases has come).

> Example. In case of a brown field project the one to one replacement of the trackside elements can be requested and applied. When applying this principle to e.g. the fouling points and the distance between the signals and track section borders it shall be considered that new regulations (standardisation) may be not in line with old national regulations. The verification of the difference between the regulation applied to the legacy system and the new European ones shall be planned on time.

In the next section some causes of this state of affairs will be discussed.

4 CAUSES

Every problem has multiple causes, as is the case for hazards. We focus here on two interrelated major causes, but we realise that more causes can be added.

The first cause is quite simply optimism. In the beginning of a (larger) project, project members (on customer and supplier side) are happy to work with assumptions, draft input documents and the like. Detailed checks will follow later. In other words strict quality and safety management is a nuisance in the early phases of a project.

Secondly, quality and safety management by the contractor is rather opaque for the customer. Partly this is the case because the plans describe the outlines and ideal processes, but do not fully reflect in detail the actual processes. Partly, the plans are technical and/or rely heavily on established company procedures. In this setting, it is an easy option for the customer to rely on the certainty that at the time the safety cases are produced, quality and safety management will be demonstrated.

Both causes lead to situation in which the safety cases and their ISA assessment function like a kind of final exam. Before the examination takes place, it is not quite sure how well one has to prepare; one may be tempted to pass the exam with a rather light preparation. The result is a ‘misuse of safety cases’ as external lever to ensure sufficient quality and safety management. But it must be noted that, since the safety cases are usually coming late, it is a Pandora’s box, with surprises that can only be changed at the cost of delays and cost overruns. Thus, we add another set of risks to the list compiled in article “Why do signalling projects fail?” in IRSE News 244 [6].

We note that the effects listed in the previous section tend to aggravate the causes of this too strong emphasis on safety cases. Delayed quality and safety management tasks obscure the status of quality and safety management for in particular external parties. The immobilisation of baselines has as side effect that various improvements and bug fixes are executed, but collected in an issue log or in a CR database. The bugs will be found several times and often recorded multiple times, thereby creating an unfortunate and rather confusing picture of the current system baseline. This vicious circle is illustrated by the figure below.

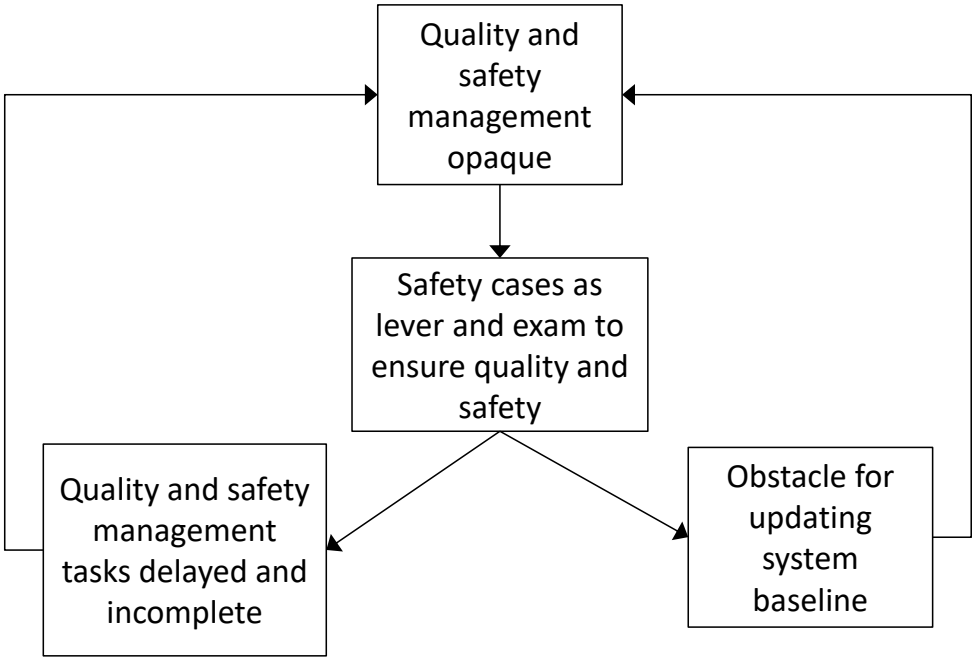

Figure 1: Circle of cause and effect

In the next section we will discuss what we can do to break this vicious circle.

5 OUTLINE OF A PUSH APPROACH

Wim Coenraad wrote in 2009 (in "Towards the one page safety case: less paper and more assurance" [7]): "any project, any supplier that applies the systems and safety assurance processes that are now the norm in our industry and adequately documents the efforts they are making anyway, should not need more than ten pages and two weeks [for a safety case] to explain all that and convince their Independent Safety Assessor (ISA)".

And later on the article says "If we have a professional Quality and Safety Management system in our company and we have a proper Quality Management and V&V plan for the project, the safety case does not need to be more than the collected evidences […], of those quality and safety management activities […]."

The essence of the above statements is that we must (more fully) adopt a push approach. Safety management processes are central, including hazard management and supported by strong systems engineering and configuration management, including change management and continuous 'configuration status accounting'.

Thus the safety manager shall ensure that the safety management process is properly deployed, in time and aligned with the other processes of the project such as: development process, quality process and V&V process. In case of a deviation, an escalation shall be initiated, if necessary, for a timely reaction. Appropriate KPIs can be set to monitor the trend of the processes and to prevent unmanageable drifts from the correct processes.

The safety management processes (incl. configuration management and hazard management) shall always be up to date. Check points or stage reviews shall be regularly performed to confirm that this is the case. Safety cases are simply side products or a spin-off of the safety management processes. They are a picture, a snap shot, at any chosen moment. The results of the safety management processes are stored in a continuously up-to-date repository and the safety case is at any moment an extraction from that repository.

Also in 2009 Eddie Goddard added, in IRSE News 150 [8], an element to this approach: self documentation. "Systems should be self checking, verification and validation built into the production process, and the safety case built around the production process". Building safety management processes into the production process ensures their timeliness.

The benefits of this approach are in particular: no backlog in configuration management, no backlog in hazard management, small changes of a baseline can be easily processed, without the need to 're-open the safety cases' which is seen as a major obstacle. Instead at any time the status can be extracted and evaluated. In case of an 'insignificant' change, not reassessment of reconsideration of approvals is necessary. From the start 'insignificant changes' to a baseline as defined by CSM RA can be quickly introduced, provided safety and configuration management processes are up and running.

How can the above push approach prevail? A condition is that the safety management and quality management processes are transparent. For the ISA they are, to a certain extent, transparent. EN 50126:2017 writes (part1, §6.8.2) that "[e]ach independent safety assessment shall: […] evaluate the conformity of the process and the developed outcomes according to the requirements and activities defined in this European Standard [and] carry out inspections on the overall system development process as appropriate at various phases of development". However, as in the case of TSI certification the ISA can focus on type examination and product verification or on assessment of the quality management system. EN 50126:2017 writes (part1, §6.8.1) that "Independent safety assessment includes an evaluation and judgement that specified aspects of the safety management process have been adequately undertaken and/or specific requirements with regard to the system or part of the system are fulfilled." Clearly, we advocate an emphasis by the ISA on the safety management process.

But the safety management and quality management processes should also be transparent for the customer. The best way to achieve this is to align the safety management and quality management process of the supplier with the safety management system of the customer from the start. This is certainly not easy. Three main obstacles are the following

- Full disclosure of all processes on supplier side may conflict with requirements of confidentiality.
- Sometimes on customer side a project organisation is defined that does not follow the customer's safety management system.
- Alignment between the supplier's safety management process and the customer's safety management system may be difficult due to various divergences. Here also different cultural backgrounds play an important role, especially in large projects with multicultural teams in several countries.

Despite all problems we still support such an alignment as a key success factor. In fact it is better to have problems of understanding and alignment in the beginning of a project than at the end (when safety cases are due to be accepted).

> Example. At the start of the project customer and supplier need to agree on the format of drawings, in particular the signalling layout. A signalling layout is often supplemented by several data that are not visible on the drawing, but are part of associated documents or an underlying database. It is essential that customer and supplier also agree the full content of the signalling layout. A thorough common understanding of what it means to approve the signalling layout, will be a major step in aligning the safety management on both sides. Any delay or misunderstanding will have its percussions later on.

6 CONCLUSION

We started with referring to the enormous workload experienced by the 'safety team'. Of course, this is not only typical for the safety team, but it is typical for projects and all project teams. In fact safety case writing in the heat of preparations for an approval of tests or commercial operation can be rather thrilling.

But in the paper we have argued that, beyond personal considerations of well-being, the strong focus on safety cases has negative consequences for the quality of safety management. As far as this strong focus is a lever to get projects tasks, including safety management tasks, completed, this is a misuse of safety cases. Instead collaboration and transparency in a much earlier stage is the right approach.

ACKNOWLEDGEMENT

The authors thank several colleagues from Alstom and Movares for reading the manuscript and providing valuable comments.

REFERENCES

1. European Commission, *Regulation 402/2013 on the common safety method for risk evaluation and assessment,* 30 April 2013 (+ amendment 2015/1136 of 13 July 2015)
2. CENELEC. *Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*, Part 1 and Part 2, EN 50126:2017
3. TÜV Rheinland. *Safety Case Symposium 2018*, Singapore, 2018
4. Doppelbauer, J. *Command and Control 4.0, IRSE News*, no 246, pp 2-9, July August 2018).
5. Howe N, on behalf of the IRSE International Technical Committee. *Cybersecurity in railway signalling systems*, *IRSE News*, no 236, pp 26-29, September 2017
6. Rumsey, A. *Why do signalling projects fail?, IRSE News*, no 244, pp 24-27, May 2018
7. Coenraad. WJ, on behalf of the IRSE International Technical Committee. *Towards the one page safety case: less paper and more assurance*, 2009
8. Goddard, E. *Signalling: Have we lost the plot?, IRSE News*, no 150, pp 2-7, November 2009