IRSE INTERNATIONAL TECHNICAL COMMITTEE

TOWARDS THE ONE PAGE SAFETY CASE: LESS PAPER AND MORE ASSURANCE

Written and edited by Wim Coenraad, IRSE-ITC on behalf of the International Technical Committee of the IRSE

I. Introduction

It should be possible to produce a “one page safety case” (well perhaps 10 pages max.) and assess it in two weeks. All it takes is to be clever about it and manage the safety assurance processes well.

In essence, 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 to explain all that and convince their Independent Safety Assessor (ISA).

II. Manage scope, planning and budget

The perception appears to be that both Cenelec and the Independent Safety Assessment process require an extensive body of evidence and the easiest way of satisfying these requirements is thought to be producing an exhaustive safety case in the form of the proverbial “paper mountain”. And the ISAs we are used to work with like using this style of input. But, in EN50129 assessment is defined as*” the process of analysis to determine whether the design authority and the validator have achieved a product that meets the specified requirements and to form a judgement as to whether the product is fit for its intended purpose”.*

One important logical consequence is that the ISA is not the validator or the design authority and should not be allowed to assume these roles or responsibilities. But sometimes they try to, or act as if they are, and if we let them, this leads to requests to spend more hours to cover their responsibilities, and for more and more evidence. But we should never forget who is the validator and resist the tendency to repeat validation in an assessment.

Instead, the ISA should check whether or not there is a sound validation plan, which as a matter of fact should have been produced as part of the Safety Case Strategy and agreed with the ISA and Safety Authority at the start of the project. In fact the Safety Case Strategy should be included with our call for tender for the assessment services if we can. The ISA can then comment it and ask for modifications, but once agreed, we manage our strategy and so manage our ISA, because an unmanaged ISA is a recipe for scope creep.

Secondly, we should watch and manage the ISA cost carefully. The rule of thumb is that the cost of the ISA should not be more than 10% of the Verification & Validation (V&V) activities cost (and this is true for the budgeted costs as well, but be careful not to extrapolate past expensive practices when budgeting for V&V). If the ISA cost exceeds more than 30% of the V&V cost, one of two things may have happened:
Either the ISA is repeating the validation work (and this is more likely to be a risk with ISA's that operate their own test laboratories etc.), or we have a project with a lot of errors (findings), or a lot of variations and consequently repeat or follow-up assessments. In both cases we are probably not managing our project as we should.

The lesson to learn is that by formulating and agreeing a Safety Case Strategy and a Safety Case Acceptance Plan up front and sticking to it, we can control the assessment scope and budget without jeopardising the ISA's independence, and both the customer and the ISA should be professional about this.

III. Structure and Format

The second point we need to make relates to the structure of the safety case. EN50129 is wonderful in that it gives us a structure and guidelines for scope, content and format of the safety case. But it does not specify anywhere that it *has* to be a paper mountain! 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, reports mostly, of those quality and safety management activities that we have agreed upfront in our Safety Case Strategy and Safety Case Acceptance Plan and that is why these two are such important starting documents.

The safety case itself then is just a top-level document acting as a set of pointers to, and a summary of the results of these reports.

But we have to remember that these must be presented in a very clear, concise and assessor friendly manner. We do not want the assessor to have to search for documents that cannot be found, have illogical names and document titles etc. It costs the ISA a lot of time and hence the customer a lot of money and frustration.

Once again the Safety Case Strategy and Safety Case Acceptance Plan comes to the rescue. We have set out in them what evidences we were going to produce and how we would present those and we have agreed it with the ISA up front. So it can be used as the basis for the Safety Case and we can use simple methods like providing hyperlinks to the documents we are providing. And of course, it must be kept current if things do change in the project.

In summary, use the Cenelec 50129 structure, since it is an accepted one and we and the ISA are used to it. It avoids unnecessary discussions. But manage the scope ad the size of the evidences and present them in a clear, very structured, concise and assessor friendly way. This will certainly still require a lot of effort, but not more than the systems and safety assurance work that would have to be done if there was no Safety Case and ISA to begin with.

For follow-up on this discussion or to contribute, visit http://signalling.wordpress.com

Author
This article was produced for the International Technical Committee (ITC) of the Institution of Railway Signal Engineers (IRSE) by Wim Coenraad – Movares. More information on the IRSE-ITC and its reports an be found at http://www.irse-itc.org

Jargon helper

The concepts of verification and validation, assessments and the role of the independent safety assessor can be confusing, especially to a non-specialist reader. They are defined and explained in European Standards such as EN50126 and EN50129 and even these standards differ slightly in their definitions. As EN50129 is the standard that defines the scpe, structure and content of safety cases in great detail, the defintions included here were copy from that standard.

assessment
the process of analysis to determine whether the design authority and the validator have achieved a product that meets the specified requirements and to form a judgement as to whether the product is fit for its intended purpose

validation
the activity applied in order to demonstrate, by test and analysis, that the product meets in all respects its specified requirements

verification
the activity of determination, by analysis and test, at each phase of the life-cycle, that the requirements of the phase under consideration meet the output of the previous phase and that the output of the phase under consideration fulfils its requirements

design authority
the body responsible for the formulation of a design solution to fulfil the specified requirements and for overseeing the subsequent development and setting-to-work of a system in its intended environment