

Experiences of Using ASCE in Assuring Complex Systems

I have been to a lot of lectures and presentations on System Safety Assurance¹ in which the analysis begins with asserting, on a clean page, that “It is Safe” and then goes on to define “It” and “Safe” in the context of the system to be assured. It is relatively straightforward to construct an argument starting from here

If the first draft argument is in the initial Safety Assurance Plan, you can use the argument to influence the architecture design so that it has the required properties². Also you can influence the choice of processes such that the evidence you need in support of your argument will arise as a matter of course and not be considered as something extra.

More practical books and lectures will point out that you must also argue that “It” will continue to be “Safe”, i.e. it is not sufficient to know it was safe when it was ready to go into service; can it continue to be used?

There is a third aspect in most of the systems with which I am involved. We do not have the luxury of starting with a clean sheet of paper. The system is there, already in service, assured by my predecessors. We want to add a function or replace an obsolete subsystem with a new one.

- The existing bit has been shown to be safe;
- The new bit is safe; and, making them into one system,
- It will continue to be safe

...but, what about the transition step of making them into one system?

We need to continue to provide a safe service whilst adding the new functions and replacing the obsolete sub-systems. Our Transition Managers are nocturnal beings – we do most transitions at night when there is less demand on the service and when there will be a free period in which to switch off the old and switch on the new.

That is a bit simplistic; it is, of course, necessary to install and commission the new before it can be used and, usually, there is something to decommission and remove. It is not unusual for the old to remain in place for a time to ‘fall back’ to, should the need arise. We need to provide arguments that we will not interfere with the service when installing, commissioning, decommissioning and disposing. Installation may be putting a new rack in an existing operational equipment room, or it could be a major construction project.

I am not intending to talk about how we argue all these things, but rather about how we manage this complexity and how using the ASCE tool can help. As I am sure you can imagine, the ASCE networks can become very large. There is an additional complication in my industry that may not arise in yours; our Regulator requires specific objectives to be argued for items that contain software.

For an argument to be complete, we need to validate the assumptions made therein and verify that the necessary evidence exists (and adequately supports the argument). Of course, as already mentioned, the argument develops as the system is being developed; some evidence does not exist at the time the argument is put together, but it must before reaching the project milestone that the argument is to support.

¹ ... and actually given a few

² I recommend that you read Nancy Leveson’s book draft to get an idea of the sort of properties you may need in your systems. <http://sunnyday.mit.edu/book2.pdf>

The "Confidence" fields can be used in ASCE to colour the evidence symbols, for example something we have to hand could be "high" confidence (green on the network), a draft could be "medium" (amber) and something yet to be done could be "low" (red). Progress can be seen at a glance.

Some of my colleagues like to extend the colour up the tree so that it is clear which branches of the argument are unsupported by complete evidence sets, but this is quite time consuming to do. It would be nice if ASCE had the option to roll-up the Confidence automatically, e.g. if one of the items of evidence supporting a goal is red and the rest green, then that goal would become red to indicate that something is missing.

We can also use the ASCE tabular view to help manage the task, e.g. by using the "Completed" status field to indicate what is available. We can also assign an owner to each item of evidence, using the "Resourced" status field; it is their responsibility to provide it, or acquire it, on time. This table view can be extracted from ASCE as an HTML document that can be provided to management as an illustration of progress.

There are actually insufficient columns in the table, i.e. we need more attributes. A column for the milestone date by when the owner needs to complete would be handy; it can be put as text in the "Resourced" field with the name, but it is fiddlier to maintain. An actual completion date would be good too, but not essential. I am sure that you can think of a number of other items that you may wish to track, dependencies for example.

What we do at present is to export the table as "comma separated" text and use Excel to add and maintain the additional columns. This is a practical solution for a static argument, but can be a large overhead if the argument is evolving. It would be a distinct advantage if the additional attributes were supported by the ASCE tool.

It is clearly impractical to create special schemas for every job – it would be much easier to provide a number of extra "user fields" for additional text and, possibly, enumerated and Boolean attributes. If the names of these user fields were to be embedded in the XML, they would be carried over to the reviewers' copies of ASCE, making it unnecessary to send a tailored schema too.

It is not just the evidence and assumptions that need to be tracked. Often document references will be given in GSN Contexts and/or Justifications. Are these available, or are you arguing for a future baseline? In the latter case you need to track their development and ensure they fulfil the rôles you expect them to when they eventually become available.

The argument does not need to be complete, in the sense that all evidence is to hand, for it to be ready for review. It is better to get the basic structure agreed as early as possible. It is best, although not always practical, to develop it incrementally; getting agreement as you proceed.

It would be very useful to have a facility for comparing two ASCE files and highlighting the differences of text and interconnection. The different relative positions of the entities do not matter, as long as we know how the argument has changed. Reviewers need only look at the new or modified bits in detail.

So, how do you get agreement on your argument structure when not all the stakeholders have the wherewithal to read ASCE files (and not all would know what they were looking at if they did)?

Probably the best way is to get the reviewers together and give them a presentation of the argument, using ASCE, highlighting those parts on which different reviewers may wish to concentrate, before sending them off with a printed version with which to review the detail. It has actually proved impossible on some projects to get everybody together at the same time for an explanatory session; the document therefore needs to stand alone, i.e. it should contain sufficient explanation for the reader to follow the argument.

To get an enormous network into a document it needs to be broken up. This is where the plug-in action "Arrangement: select sub-tree" comes in handy – it does just that, so one can use the "copy selection as an enhanced metafile" option from the Edit Menu to capture the sub-tree, which can then be pasted into your document.

GSN has a distinct advantage over CAE here; if you capture a CAE sub-tree, the text embedded in the nodes is lost and has to be separately captured. For a simple network fragment the diagram can actually become superfluous; the text is sufficient.

Those of my colleagues that do use CAE would like the embedded text be a bit more controllable, e.g. having selectable font types and sizes with more flexible paragraph and bulleted list styles. On the ASCE view screen, it would be useful to be able to see the embedded text when hovering the mouse pointer over a node. An extension of the existing label view is clearly impractical, but could the text view be implemented as a separate window in the same manner as the Bird's Eye View?

Often, when extracting sub-trees from ASCE, you can end up with diagrams that are tall and spindly, or level and wide, neither of which makes for a particularly readable document. It can take a long time to get things right, so remember to budget for this in your schedule.

We need ways of partitioning an argument so as to give reviewers an overview and enabling them to concentrate on those parts for which they have responsibility. One way of doing this is by using Views to suppress the detail of an argument and just present the key claims or goals, possibly annotated with where to find the detail of each elsewhere in the document.

Another representation is to use the modular GSN argument method developed by Tim Kelly and his co-workers at York. This works best for arguments comprising loosely coupled cohesive blocks. Each block can be elaborated in its own ASCE file. Different blocks requiring the same evidence can be managed using the table view to record the dependencies. Note that this method is less satisfactory when there is a lot of lower level cross-coupling.

A completely different approach is to print out large views on a plotter, put them up on the wall and invite your reviewers to mark them up. It has proved difficult plotting directly from the tool, but capturing a metafile, copying it (and scaling it) into an A0 template in, say, Visio and printing that has proved successful.

In summary, ASCE has been found to be suitable for preparing and presenting safety arguments for complex systems, but we have had problems in making the results available conveniently to the reviewers. The ASCE tool provides additional features for illustrating progress in collecting evidence, validating assumptions, etc. We have requested some extensions to these to simplify this management task.

John Spriggs

30/04/08

These opinions are my own, or those of my colleagues, and not necessarily those of my employer