Mistakes & Misconceptions



John Spriggs discusses how mistakes and misconceptions can unwittingly creep into our world and, in particular, when presenting assurance cases. He explains the perils of failing to understand the context or grasp the bigger picture and asks if lessons are being learnt from past failures.

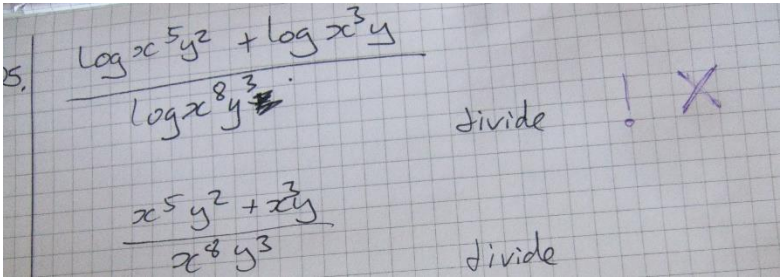
Talking with some school maths teachers recently, I found that one of their key skills is the ability to anticipate misconceptions in a topic, and plan to address them in the lessons before they arise. Similarly, over a period of teaching a topic, they identify common mistakes, and so can put more emphasis on those parts of the topic that cause problems. This is like identifying a vulnerability and implementing appropriate controls (or mitigations for hazards). What mistakes and misconceptions could make your assurance project go pear-shaped?

Mistakes

Some mistakes arise due to a change of context. For example, a student may be perceived as proficient with logarithms but, when a more complicated logarithm problem is posed, they make a basic error. For example, they are told to simplify an expression like (log a + log b)/log c where a, b, and c are scary-looking expressions, like x^5y^2. "This is obviously an algebraic manipulation problem", so the student unthinkingly divides through by log, as if it were a quantity. Such a switch in perceived context led to an assurance mistake I once saw, where a system supplier assured the regulator of their new customer that all was OK, because they complied with Standard X. The assurance was rejected; more work was required. The supplier was surprised, because they had sold an equivalent system into another

regulated industry recently, and compliance with Standard X was all that was required of them then.

What the supplier did not know was that the earlier regulator had their own explicit requirements, which they had placed on the customer, and within those was a note saying that demonstrating compliance with Standard X is an acceptable means of compliance to these requirements. The customer had taken the easy route and just specified compliance with that standard, rather than passing the detailed requirements on. The regulator in the new market had a different set of requirements, and did not identify use of Standard X as an acceptable means of compliance. In this scenario, it is up to the assurer to justify their claims that meeting Standard X also satisfies that regulator's requirements. The mistakes made by the maths student and the supplier are both understandable given the changed context.



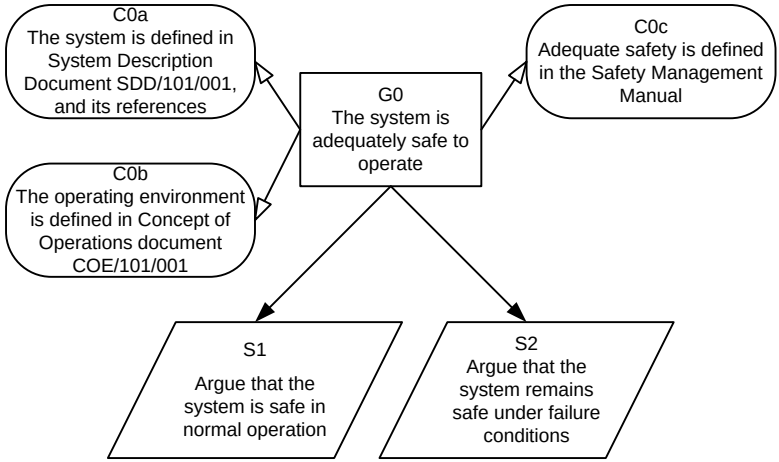
Misconceptions

What about misconceptions? This is where the mental model of a concept does not accord with the real 'mechanism'. This can often arise from a misunderstanding of what a teacher said or, in many cases, due to ambiguity in the way the concept was presented by the teacher. For example, a young student may have written 3.6 X 10 = 3.60 and challenged it being marked wrong, saying, "But you said to multiply a number by 10, just write 0 next to that number, like 5 times 10 equals 50"…

In the assurance world, we have the Goal Structuring Notation as one way to present an argument. It transpires that some people see this name and have the misconception that the notation is all about setting goals and achieving them. From this viewpoint, presenting assurance that "the top goal is met", means that all the sub-goals are "met", and consequently all the required evidence is available to support the lowest level goals. Presenting assurance under this misconception is therefore just accounting of evidence items as if they were all equally important. This view may have been valid for the origins of the notation, which was developed in support of engineering requirements decomposition (and verification composition). In an extreme example (where the argument was prepared by someone else, maybe as a template), as the goals are all "met", it is assumed that we do not need to see them clearly, and so the whole argument structure is presented in a single unreadable diagram, or not presented at all.

The Goal symbol in the Goal Structuring Notation … is just a proposition; a statement that may be either True or False. Truth is in the eye of the beholder.

The Goal symbol in the Goal Structuring Notation, when used to present an assurance argument, is just a proposition; a statement that may be either True or False. Truth is in the eye of the beholder in this context. Those who are to be assured need to see the argument to assess its validity, and how it appeals to the evidence. They can then judge whether the evidence presented is necessary and sufficient for their needs. Just claiming that, "The top goal is met, because the evidence is available for audit" should be insufficient to assure anyone.



Seeing the whole picture

The student's misconception arose from being exposed to only part of the picture. To multiply by ten, you must bounce the decimal point one place to the right, and you append zero if there is then an unprotected decimal point on the end; if there is no decimal point just append zero. We can be exposed to only part of the picture in engineering too. I was once told by a supplier that I would receive the "complete assurance package" the following week, which was a surprise because I was producing the assurance for that project. Another surprise was that it actually arrived midweek; "next week" usually means after five o'clock on the Friday. When it arrived, it was a set of test reports and explanations of how those tests demonstrated satisfaction of the requirements. This was actually what I was expecting from the supplier, as set out in the Contract Schedule. They had been contracted to supply various items, and the main body of the contract, to which I did not have access, specified them under sub-headings, like Training Materials, Maintenance Manuals, and Assurance Documentation.

Surely, there is no problem with a completely understandable mis-naming like that. But, what if that supplier bids for your next project, and the non-specialist negotiators accept their offer of a "complete assurance package", because it is cheaper than your proposed work package? Not a likely scenario, but I did experience something similar many years ago, where a bidder was accepted because they promised full compliance with a standard that had a number similar to the one actually specified…

There is a school of thought that specifying safe behaviour in a set of requirements, and then demonstrating that those requirements are "met", is sufficient assurance for the equipment part of a system. This too is a misconception. I also need to be persuaded, inter alia, that the set of requirements is correct and complete, and also that there are no unwanted interactions. Each requirement has been demonstrated separately, but what if the behaviour arising from one requirement adversely impacts on correct operation of a safety function (mitigation) specified by another? Similarly, satisfactions of the people and procedure requirements may not be sufficient assurance either. Such requirements often include ones of the form, "There shall be a procedure for performing periodic maintenance", for example; satisfaction is then demonstrated by pointing to the procedure in the management system. Assurance will also be required that the right people have been trained to use this procedure, and that records exist of its use with the system.

There is a school of thought that specifying safe behaviour in a set of requirements, and then demonstrating that those requirements are "met", is sufficient assurance for the equipment part of a system. This too is a misconception.

Lessons Learnt?

Can we improve our assurance processes by anticipating misconceptions and preventing common mistakes? Many companies have procedures for lesson learning; most concentrate on impacts to time and cost, but the principles can be extended to extracting lessons learned from assurance failures too. Make sure that the lessons are actually learned, so that the same problems can be avoided in future. It is easy to record the lesson and then forget it. Someone once told me that his employer has a formal meeting at the end of each project intended for lesson learning, but the minutes of the meeting are just archived with the project. There is no requirement to raise actions for process change. I think that is a mistake.

John Spriggs, Independent Author and Presenter

John Spriggs was a designer of avionics systems in the 1970s and '80s. In the 1990s, he became an assurer of equipment for Air Traffic Management and Airports. From 2000, he was the Safety Assurance Consultant for an innovations factory, and later provided assurance for air navigation services providers. John is now an independent author and presenter; he is author of the Goal Structuring Notation textbook.

The author retains copyright of this article, the diagram, and the photographs.