ISA WG Webinar 1: Is independence an overrated virtue? (revisited)

The Independent Safety Assurance Working Group (ISA WG) held the first of its online seminar series on 21 October 2020, supported by the IET. The series has the overall theme "Assurance in a connected world" and is a replacement for the bi-annual seminar day, which provides input to the guidance being developed by the ISA WG.

During our Q&A session, there were a variety of questions that were asked by attendees. We unfortunately did not have the time to answer all questions but have responded to the questions below.

Please note that the answers to the questions are personal opinions based in the context of the webinar. It is not intended to be a guidance note with a specified set of recommendations or actions but rather seeks to add understanding and debate around the topic.

Responses to unanswered questions:

1. **What if any assurance process is applied to the follow-up on recommendations from public enquiries? i.e. If no one is tracking / assuring that recommendations completed (or amended with agreement) then why make them?**

   They are tracked. It will depend on the inquiry who by but usually by a Regulatory arm of government. In the case of the Ladbroke Grove inquires tracking and progressing the inquiries fell to the HMRI (then part of the HSE) and to the ORR. The separation between safety and commercial regulation in rail (unlike the CAA which was responsible for both for air) was criticised at the inquires and later the HMRI was moved to the ORR and later still the ORR changed from being the Office of Rail Regulation to being the Office of Road and Rail. Many of the inquiry recommendations were closed out in the recommended time, others proved unrealistic.

2. **Would you agree that the B737-Max series of accidents are therefore 'normal accidents' as envisaged by Charles Perrow?**

   Probably not, as subsequent analysis has shown that the accident was identifiable by safety analysis methods and thus not so 'complex' and 'tightly coupled' that the accident was inevitable. In particular the reliance on the pilots to change between the Angle of Attack (AoA) sensors with little or no transparency on the existence or functioning of MCAS and the AoA 'out of correspondence' alarm being an option (not fitted on either of the crash aircraft) should have been recognised as posing significant risks.

3. **Why is 'no objection' accepted in the rail industry? It isn't in defence wrt design certification. Is there truly a difference between 'accept' and 'don't object'?**

   Regulators often use 'letters of no objection' to signify that whilst they have examined a case for safety, and all the issues are closed to their satisfaction, responsibility remains with the duty

ISA WG Webinar 1: Is independence an overrated virtue? (revisited)

holder. In many ways that is reasonable, but it can lead to weak Regulation if the 'stakes are high' to get a system, platform or project into service.

4. **Is there a language bias or problem (perhaps a product of the implicit process or perspective/context)? e.g. In software engineering there are Use Cases (but not Misuse Cases) and notations are based on defining / describing function and hence non-functional aspects tend to get forgotten unless picked up by those with experience.**

   Terminology is the bane of our existence and can be used to mask areas of concern. One person's definition of risk is different to another's. Part of an ISA's responsibility is to look beyond the words to identify safety issues – this comes with experience and cross sector knowledge. This is one of the strongest arguments for an ISA team to contain competencies in all the technologies and techniques used.

5. **The whole culture of the company should be looked at following an incident. I have found this can have huge effects on the actions of employees.**

   Agreed but depends on the severity of the incident and the degree of organisational complexity. Buncefield and Nimrod and the Challenger disaster are three examples where this has occurred.

6. **Are these IEEE documents seen as cross-industry?**

   Yes. Whilst there is a degree of focus on software driven systems the standards are intended to cover all possible applications.

7. **How should a provider demonstrate competence to a customer or regulator?**

   Suppliers (Providers) would be expected to provide evidence that there is a process within their organisation (or within a particular programme or project) by which necessary competencies are identified / defined and against which members of the organisation (or programme / project) are measured in some way (through reference to training, experience or other evidence). Guidance on the implementation of such a process is provided in, for example, the IET's "Code of Practice – Competence for Safety-Related Systems Practitioners" (ISBN 978-1-78561-111-7 or ISBN 978-1-78561-184-1).

   If the question relates to the competence of Independent Safety Assessors (ISAs), then it is worth noting that ISAs are not regulated in the UK. Many skills are transferrable across the various domains, and the ISA WG was set up to address some of the issues. An Assessor as part of a medium/large company is almost certainly in a company competence scheme of some sort. Some industries have their own registration/competence schemes (eg Rail and air), but failing that, the route recommended by the ISA WG is through a mixture of CPD, record keeping, adherence and demonstration of adherence to ISA WG guidelines…

ISA WG Webinar 1: Is independence an overrated virtue? (revisited)

8. **Suitably qualified and experienced persons are assessed through examination and then develop experience through application of their knowledge. AI might be "examined" during initial verification and validation, but does this mean that we must let AI learn on the job?**

   This is one of the biggest questions that the standard on Fail-Safe machine learning systems (in particular) is attempting to address. The concepts being discussed include having immutable (unchangeable) and mutable (adapting or changing) functionality and the degree to which ML can be used to generate immutable functionality by 'learn then freeze'.

9. **It worries me on a system I have worked on for 20 years that the only really competent people are lost in the supply chain. How do we get their competence as independent but non-conflicted people?**

   This is very difficult to answer without knowing the specific circumstances. Supply chain contracts can include specific support provisions with the right protections for independence - but there are no 'free lunches'.

10. **Formal methods do not solve the problem with defects/errors in the requirements. Many software failures are attributed to defects/errors in the requirements. How do you propose to improve the situation?**

    You are correct. Requirements management is extremely important, and it is vital that people with the right domain knowledge (competency) are involved in validating not just the primary requirements but the derived software requirements too. Often these are left to the software specialists alone which leads to misinterpretations. If you have access to the IRSE News this issue will be covered in more detail in an article I have written for the January 2021 issue.