ISA Working Group 2020 Webinar Series

(Webinar will commence at 11:02 am)

Are you interested in joining the ISA Working Group? Let us know by e-mailing SEP@theiet.org

Assurance in a Connected World

Webinar 4: Sufficient Assurance?

<u>Panellists</u>

John Spriggs – Speaker

Stephen Hatton – ISA WG Chair

Pete Hutchison – ISA WG Deputy Chair

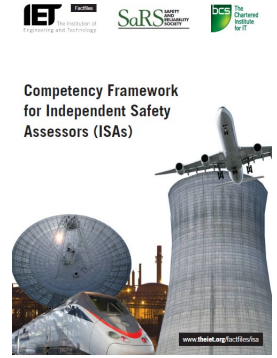
John Canning – ISA WG Secretary

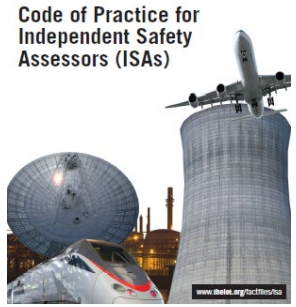
ISA WG Terms of Reference – Purpose

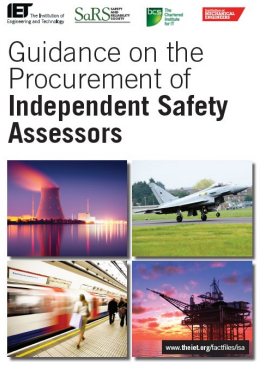
- Promote the ISA role as a means of providing independent safety assurance of products to the supplier, purchaser and user
- Promote the ISA role of a safety professional in standards
- Support professional development by defining minimum standards, identifying training that meets minimum standards and supporting resources
- Support professional ISAs by developing guidance and providing information that affects their role

Guidance – Published

- General
  - ISA Working Group Terms of Reference
  - What is Independent Safety Assessment (ISA)? in Review for update
- Professional
  - ISA Code of Practice for Independent Safety Assessors (ISAs)
  - Competency Framework for Independent Safety Assessors (ISAs)
- Substantive Guidance
  - Assessment of Safety Related Compliance Claims (SRCC)
  - Guidance on the Procurement of Independent Safety Assessors
- Guidance Notes / Position Papers
  - Guidance on the Use of Accident and Incident Data by ISAs
  - Documents useful to Independent Safety Assurance
  - Position Statement on Security, Safety and ISA

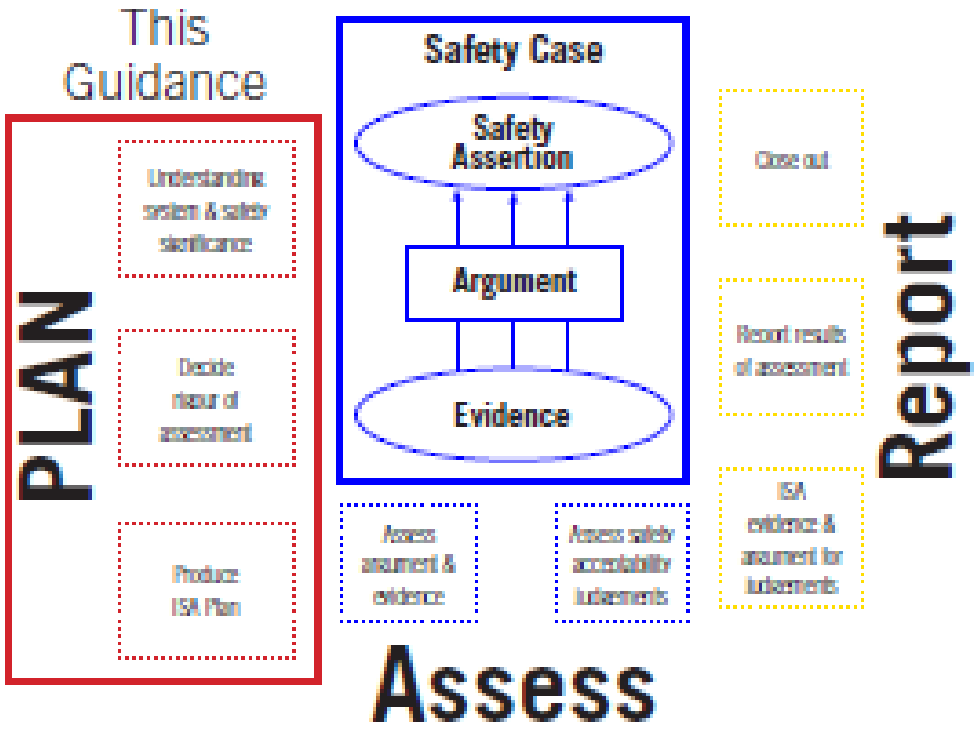






Assessing a Safety Case Series

- Assessing a Safety Case Series
  - Guidance for Producing an ISA Plan for Assessing a Safety Case — published
  - Guidance on Safety Assessment Reports — to be published
  - Guidance on Degree of Rigour — in progress



Documents in Development

- Standards Group
  - Requirements for independent review/assessment called up in Standards and Industry Guidance
  - Environment Assurance and Safety Assurance

- Professionalism Group
  - Using Key Performance Indicators with an ISA Contract ready for issue
  - Agile Development
  - Guidance on Degree of Rigour – IDEAS NEEDED (Please complete our questionnaire!)

Housekeeping

- Q&A (Zoom Webinar)
  - Use Q&A button to type your question (don’t use chat button; don’t raise hand)
  - Use ‘thumbs up’ to vote up or vote down a question (once only)
  - Panellists will select and pose questions on your behalf
  - Questions not discussed today will be recorded and commentary provided afterwards
- Feedback
  - Short re-cap article after the event
  - Please read and complete our questionnaire (to be e-mailed to you)
    - What gives you confidence in safety assurance provided for acceptance?
    - No need to answer all questions
  - Let us know if you’re interested in joining the ISA Working Group

Sufficient Assurance?

John Spriggs

John has worked in the aerospace industries for over forty-five years, starting as an avionics designer for Plessey. He moved on to be safety assurance manager in both Siemens and Thomson CSF, working on systems for Airports, Air Traffic Management, Communications, Navigation and Surveillance. John then offered his services to the innovations factory at Roke Manor, as safety assurance consultant, working on the same topics plus spacecraft and other autonomous vehicles. John's last employer was an Air Navigation Services Provider that had previously been a Customer; the poacher turned gamekeeper?.

Sufficient Assurance?

IET ISA Webinar:

"Assurance in a Connected World", 2nd December 2020

John Spriggs

http://www.linkedin.com/in/johnspriggs

Previously presented at the Safety Critical Systems Club:

Safety-Critical Systems Symposium, 5th February 2019

Abstract

Many previous Safety Critical Systems Club events have featured presentations on how to present assurance, and how not to, but never how to receive assurance; how to be assured. If you were the owner and operator of a new system or service, how would you assess the assurance you have been given? Whether you are the Customer, the Customer's Regulator, or the Customer's Friend ("independent eyes"), you need to know what to look for in an assurance argument; this paper provides a guide to judging what is enough, or where more work needs to be done. Identifying what a reader needs to look for in assurance documentation will also inform authors what to include - and what to miss out.

What is Assurance?

A dictionary definition

A positive declaration intended to give confidence

dictionary.com

For Example…

- “I assure you that this system is safe!”
- Not very convincing, is it? Insufficient Assurance!
- The positive declaration by itself is not enough; in order to give the reader confidence, it needs to be justified.
  - **Not: “**This is ready to go into service”
  - **Instead: “**This is ready to go into service, because…”

Claims and Arguments

- “This is ready to go into service, because…”
- The “because” is to be followed by the justification; that is, an argument persuading you that the declaration is indeed true.
- The declaration is a Claim made by the author.
- The justification, often called the Assurance Argument, is how the author persuades the readers that their claim is true.

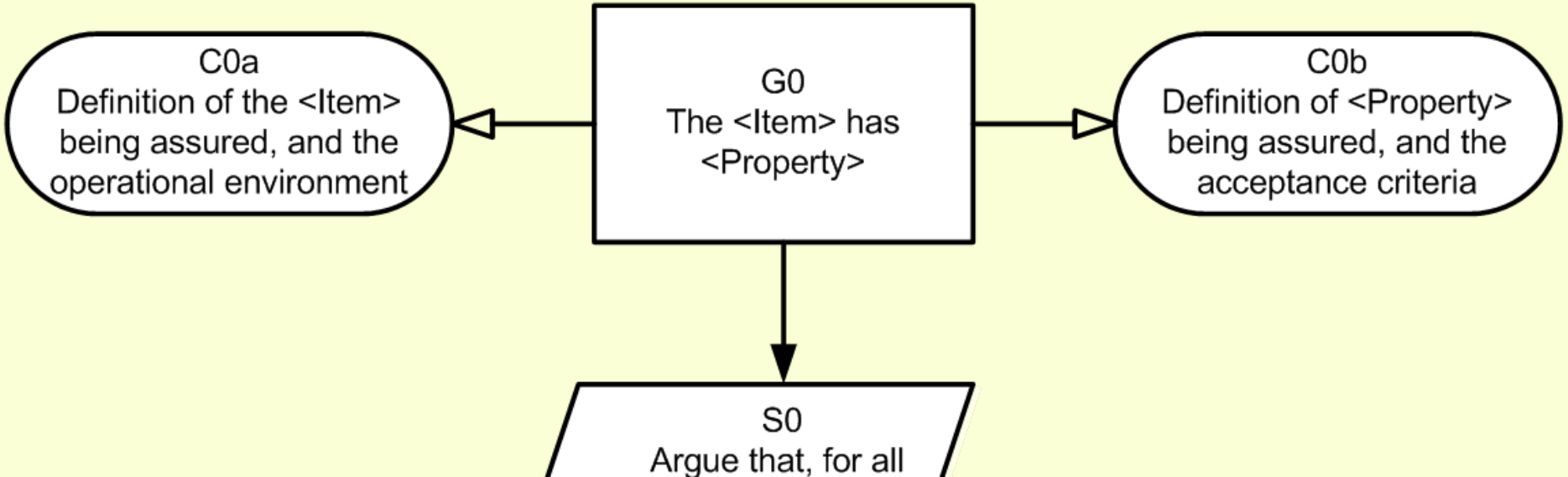
Key Principle

Assurance is …
intended to give confidence

Assurance documents must each make, and justify, at least one pertinent claim.

Assurance Arguments

- The argument could be presented using text, preferably structured, but it may be rambling, or it could use a notation.
- Often the claim is that the subject of the argument possesses some property



Properties

- Traditionally, in this forum, we have spoken of assuring system safety; more recently we have added (cyber)security, data safety and service assurance, and you may also have:
  - Environmental Impact,
  - Service or Business Continuity,
  - Regulatory Compliance,
  - Legislative Compliance, and/or
  - Lots of other things too, such as the “Laws of Robotics”

Properties

- Whatever property is being assured, the assurer needs to provide a clear definition of what is meant in the context of the thing being assured.
- Assurance, whatever properties may be considered, really comes down to documenting risk and what is being done about it.
- Receivers of assurance want to know if their particular risks have been identified, and are being properly managed.

Are You Assured Yet?

- When you receive an assurance document for review, do a quick check:
  - Does it make an unambiguous claim, or claims?
  - Are the claims justified; is evidence brought to support them?
- If the only claim is, in effect, “This is an Assurance Document”, I suggest that you reject the document, and ask for more work to be done to formulate clear claims and to justify them.

Are You Assured Yet?

- Also, when you receive an assurance document for review, check:
  - If a special notation is used, do you know how to read it?
  - Has any notation been explained for those unfamiliar with it?
- It is important that you understand the argument, so I suggest that, if you do not know the notation used, you ask the author to provide a tutorial. It is in their interest to make things easy for you to accept their claim(s); to persuade you that they are true.

Persuasion

The art of giving confidence

Aristotle wrote of three ‘modes of persuasion’ for use in the Symposium, or in other public speaking venues.

The Symposium

- The Symposium in Aristotle's day was part of a banquet, with music, dance, drink, and discourse.
- We do not have the music and dance nowadays…
- Well, not until later in the evening - allegedly

Giovanni Dall'Orto took the photograph of the bust of Aristotle, from which this image is derived, in March 2005.
The bust is housed in the Palazzo Altemps of the National Roman Museum in Rome, Italy.
The original was uploaded to Wikimedia Commons 26th February 2006.

The Three Modes

- Aristotle's three modes are:
  - Logos
  - Pathos
  - Ethos
- And there's also:
  - Kairos
- *(extra points if you thought "D'Artagnan" then)*

In English?

- **Kairos** is an auspicious point in space-time; the here and now as the appropriate moment to drive home the argument
- **Ethos** is an appeal to the authority of the presenter and how well qualified they are to speak on the subject
- **Pathos** is an appeal to the emotions of the audience, intended to reinforce feelings they may already have about the subject
- **Logos** is the logic behind an argument; the reasoning

Kairos

- An auspicious point in space-time; the here and now as the appropriate moment to drive home the argument
- This may be easy in public speaking and debate; doing it in a document is a bit more difficult – so we will take Kairos to be the delivery of the assurance document at the right time.
- When commissioning assurance, make it clear when you will want to be assured, about what, and to what level of detail.

Recommendation

Do not allow Kairos in the form of delivery “just in time”

Ask to see the argument as it develops; you can then ensure that it covers everything you need, and in enough detail.

Incremental reviews take more time early on, in order to save time later.

Ethos

- An appeal to the authority of the presenter and how well qualified they are to speak on the subject.
- Aristotle suggested a speaker should:
  - Have useful skills and wisdom,
  - Possess virtue and goodwill, and
  - Exhibit goodwill towards the audience.

Ethos

- A speaker can find it difficult to project their ethos qualities to an audience, so it must be really difficult to do in writing.
- How can the author of assurance documents exhibit goodwill towards their audience?
- I suggest that they can do this by clearly presenting their assurance; making sure that it is well laid out, clearly written and supported by compelling evidence.

Ethos

- The author can also demonstrate their knowledge in such a way as to increase your confidence in their assurance.
- A good assurance document will provide you with an overview description of the subject of the assurance.
- This demonstrates the assurer’s understanding of the thing being assured. If it is incorrect, or vague, your confidence will be impacted before you have reached any arguments in the document.

Recommendation

Do not depend just on the virtue aspect of your assurer's Ethos

Your assurer may always be good and truthful, but the assurance would be more compelling to a wider audience if they were to bring clear, compelling evidence in support of their claims.

Pathos

- An appeal to the emotions of the audience, intended to reinforce feelings they may already have about the subject
- If the assurer has not done enough to win your confidence, don’t accept the assurance anyway just because you feel sorry for them ☺
- Beware; the assurer may have built your confidence in their claims so much that you not notice that they have omitted something.
- Perception of risk can be an emotional response; your frame of mind when reviewing assurance affects the likelihood of you accepting it

Logos

- The logic behind an argument; the reasoning
- To develop their argument, the author should consider the claim they have made and re-express it as a small number of sub-claims, which together would compose to be equivalent to the claim.
- For example, ‘The item is safe’ could be expressed as, ‘A complete set of valid safety requirements has been specified’ and, ‘The item satisfies each of the safety requirements’.

Logos

- These sub-claims can themselves be logically decomposed, and so on until the resulting statements can be directly demonstrated by bringing evidence.
- Some authors develop their arguments graphically, and then present them to their audience in text, which saves the reader from having to know the notation used.
- If an author states that they are going to use a standard notation, but does not use it properly, the readers' confidence in the integrity of that argument is likely to be reduced (Ethos!).

Logos

- Is the argument made to a consistent level of detail, or does the claim tree look as if it has Witch's Broom Disease?
- This may mean that something is being 'glossed over', or it may show that they ran out of time and had to hurry some of it….

Logos

- Both for clarity and for ease of maintenance, each argument needs to be presented only once. Discourage text description of graphical representations; it is a waste of effort that could be better directed at improving the argument.
- When reviewing an argument, look to see if anything significant may be missing from the claim decomposition, or if that decomposition is illogical.
- Check the evidence; does it fully support the claim that was made?

OK, I'm Persuaded

Assurance should be pitched to more than one person or rôle; has everybody been included?

Whom Shall The Assurance Assure?

- Assurance is presented to Customers & their Regulators, but who is that?
- There is a long list of potential Assurees in the associated paper (in the SSS'19 book). The, possibly, unexpected one is the Assurer themselves…
- Assurers need assurance that they have done enough, that they have checked enough, and that what they present is accurate.
- Once a draft is ready, they should get it thoroughly reviewed, ideally by another skilled assurer and by subject matter experts, as well as by the intended audience.

How Can We Assure the Assurer?

- The best way to assure the assurer is to provide challenge, to question the structure and logic of the arguments, to examine the provenance and completeness of the evidence, and to seek counter-evidence.
- Counter-evidence is something that does not support the argument; rather it serves to refute it. Usually, it is not catastrophic, only a sub-claim is refuted and the argument can be modified successfully.
- A shortfall in evidence may be a greater cause for concern than counter-evidence, because it shows that the argument is not properly supported and may need a major change to fulfil its purpose.

The Main Points Again

Please see the Symposium proceedings book for more detail

Summary I

- When you receive an assurance document for review, check; it should have:
  - A clear and correct description of the thing being assured, and of its intended operating environment - this gives you assurance that the author understands the problem;
  - Unambiguous claims about the properties being assured – *your* assurance needs should be properly addressed with *your* particular risks identified and managed;

Summary II

- Clear definitions of the properties being assured, i.e. what ‘safe’, ‘secure’, etc., mean in this context;
- A valid argument in support of each claim made, clearly declaring any assumptions made therein;
- A compelling set of evidence supporting each argument presented; and, if necessary,
- Clear description of any limitations of use of the system, service, etc., and/or any unresolved issues or known deficiencies of the assurance presented.

… And, In Conclusion

- Many authorities require a conclusion at the end; more powerful is a declaration of assurance right at the beginning, stating the claims made and supported in the document.
- What we do not want is a long-winded presentation of evidence followed by a section stating what conclusions may be drawn from that evidence.
- Worse would be a long-winded presentation of evidence **not** followed by a section stating what conclusions may be drawn…

Final Conclusion

Do you have any questions?

http://www.linkedin.com/in/johnspriggs

An assurance document must state claim(s) and present clear argument(s), supported by pertinent evidence.

If it does not, reject it.

Next Event in the Series

Webinar 5: Functional Safety and AI

(Thursday 17 December at 11:00)

(Register at IET Events)

Are you interested in joining the ISA Working Group?

Let us know by e-mailing SEP@theiet.org