|  |  |
| --- | --- |
| Meeting: | Security Informed Safety Working Group - Meeting 22/2 |
| Meeting Date: | 8th June 2022 |
| Attendees[[1]](#footnote-1): | Stephen Bull (Ebeni, Rail), Kate McDougall (Jacobs, Cross-sector), Nikita Johnson (Rolls Royce, Cross-sector), Wendy Owen (UoW, Cross-sector), Mark Bowell (ONR, Nuclear), Yevhen Zolotavkin (Berghausen Institute, Cross-sector\*), Ian Wolforth (BMT Defence and Security, Maritime), Dave Banham (Blackberry QNX, Cross-sector), Anees Abdul Vaheed (BAe, Defence), Paul Hampton (CGI, Cross-Sector), Giles Howard (Thales, Defence\*), Stephen Gill (Ebeni, Cross-sector\*), Jane Fenn (BAe Systems, Defence) |
| Apologies: | Emma Taylor (Razor Secure, Cross-sector\*) |
| Author: | Stephen Bull |
| cc: | Members of SISWG |
| Issue Date: | 17/06/2022 |
| Reference: | SISWG 22-2 (Issue 1)  |

# Background

SISWG has established three task groups:

1. Co-ordination of Safety and Security within the system lifecycle ([remit](https://scsc.uk/file/gi/SISWG_TG1_Guidance_Plan_%28v1%29-1218.docx))
2. Security-Informed Safety Risk Evaluation and Assessment (SiS-REA) ([remit](https://scsc.uk/file/gi/SiSWG_TG2_Remit_Draft_v2_-_clean-1213.docx))
3. Mapping terminology and language between safety and security ([remit](https://scsc.uk/file/gi/Task_Group_Objectives_-__Mapping_terminology_and_language_between_safety_and_security_v2-1216.docx))

These task groups each aims to provide guidance on their area of interest, within the overall remit of the SISWG. A link to the current remit of each task group is provided above.

# Agenda

This was the agenda for the meeting:

1. Challenges with terminology – discussion of the challenges of terminology, following feedback on the TG2 guidance – how can we achieve something which will be accessible and meaningful to as wide a range of people as possible (TG2, with support from Paul)
2. Co-assurance guidance (TG1) – discussion of revised (much abbreviated and restructured) guidance being prepared by Nikita (Nikita envisages two sets of guidance, one for engineers and the other for regulators – it is the engineers’ guidance which will be circulated for the meeting.)
3. Recent incidents in safety / security arena – thoughts on their implications (open to suggestions from group members)
4. Next steps – intention to focus on items 1 and 2 above – can we reform the existing groups (with any further volunteers) to support these aims?
5. SCSC business:
	1. Forthcoming events – see <https://scsc.uk/events?tab=scsc>
	2. SSS’23 – can you write a paper? (about SISWG or anything else) … see <https://scsc.uk/file/898/SSS22-Call-for-Abstracts-v3.pdf>

# Minutes

## Challenges with terminology

*We have received feedback on the TG2 guidance document. The overarching comment is that the document felt too ICS-specific and some reviewers did not see how the document applied to their area. The main reasons for this due to us not using their industry specific terminologies or referencing industry specific standards. We plan on addressing this by revising the document to a form which a reader is more easily able to see how it applies to them no matter what their field. However, to achieve this, we will need to decide upon a set of terms which are easily understood pan industry along with a method of keeping it generic while also considering the industry specific standards.*

A couple of attendees gave additional positive feedback about the current TG2 guidance document.

Further improvement to the document was discussed, with the following being key points:

1. We need a sector-agnostic term for the technical system which is the subject of the assurance: IACS is felt be some to be too specific to particular sectors. Suggested terms included “target system”, “target of co-assurance”, “programmable electronic system”, “system under consideration”, “security target”. Some were concerned about use of “target” because of connotations in military environment. *Note: it would be good to make the language as accessible as possible to intended readers, especially as the language used gives an important first impression to new readers.*
2. There was wider concern that the guidance is too focussed on a particular subset of industry sectors and / or system architectures. It was suggested that we abstract the (normative) guidance to make it generic across as many architectures as possible and then provide (informative) examples to ground it in specific industry sectors.

We agreed that the next step should be for people from as many industry sectors as possible (e.g. civil aviation, military aviation, rail, nuclear, maritime, …) to review the guidance against the following specific questions:

1. What terms in this guidance are not used in the sector? What alternative term is more natural in my sector? (In some cases there may not be a simple answer to this question, because the concept is not familiar in the sector in question: in these cases, it would be helpful if the reviewer could explain in as much detail as possible.)
2. What assumptions does the guidance make which are not valid in the sector? These may be assumptions about development processes, system failure modes, fail safe states … What affect does this have on the risk assessment processes described?
3. Does the guidance describe processes which are not used in the sector? In these cases, it would be helpful if the reviewer could explain what processes are used instead.
4. Does the guidance miss (significant) processes which are used in the sector? Please give details. What is lost by omitting these processes?

This feedback will identify the parts of the guidance which need to be refined in order to be widely useful: this will help to set a direction for further development of the TG2 material.

**Action 22/2-1**: Representatives from different industry sectors to comment on usefulness for their sector – using the above questions as a basis. Please add comments to the collaborative working version of the document, which can be found on Google Drive [here](https://drive.google.com/drive/folders/1WnxVzvWRJEekISP8cQmOqshyWVNpf8x0). Individuals will need to ask Nikita Johnson to grant access. *If you intend to review the material* ***please let TG2 know*** *via either of the email addresses at the end of this document, including a note of which industry sector(s) you cover. Deadline for comments: 17th July 2022.*

Note: the version published for review is unchanged from that published for SSS’22. TG2 will work on addressing existing comments in parallel, but this additional input in answer to the questions above will inform the review.

## Co-assurance guidance (TG1)

Nikita presented the [updated version](https://scsc.uk/file/gi/SISWG_Engineering_Co_Assurance-1397.pdf) of the TG1 guidance, which is significantly slimmed down from the version published in February.

We discussed the use of the term “co-assurance”: we questioned whether this is a useful term, given that the end result of the process is “assurance”: in many ways the co-assurance is just a way of achieving this. However, we use the term to emphasise that we are considering joint assurance of more than one domain – in this case safety and security. For some this implies optimisation over multiple criteria, and implies the need to find a way of trading off between those criteria. At the moment our guidance is not really doing this because we are focussed solely on the effect (of risks from multiple disciplines) on safety.

We discussed the use of “interaction risk” and questioned whether it should, instead, be “integration risk”. “Integration risk” in particular has potential for misunderstanding because it could be interpreted as “risk arising during integration activities” which is not what is intended here.

We discussed whether it is helpful to consider co-assurance as a separate activity at all (and whether it should be shown as a separate leg of the assurance argument). The alternative would be to properly integrate concerns within the individual safety and security workstreams. It may be that “co-assurance” (as a separate activity) is the best that we can aim for at the moment, given how safety and security teams are often separate. Fuller integration may be something to aim for in future!

We also noted that our current remit is only considering issues which eventually give rise to a safety risk. There is a whole different set of risks (e.g. loss of confidentiality) which (in some domains) do not directly give rise to safety risk, but which are still of a concern for the security discipline.

The next step is to develop “case studies” which illustrate co-assurance in different sectors. This will help to explore whether the co-assurance process works in those sectors, and how it may need to be extended. Nikita will publish an aerospace example, and would like group members to provide similar examples for their own domains.

**Action 22/2-2**: Nikita to update the TG1 guidance document to include aerospace example of co-assurance synchronisation points.

**Action 22/2-3**: All group members to comment on the updated TG1 guidance document and provide examples of co-assurance from their own sectors. Collaborative working documents can be found Google Drive [here](https://drive.google.com/drive/folders/1WnxVzvWRJEekISP8cQmOqshyWVNpf8x0). Individuals will need to ask Nikita Johnson to grant access.

Another area of the guidance which needs development is the “organisation and people” section. It was suggested that we may be able to develop what Reuben MacDonald (HS2) presented at SSS’22. **Action 22/2-4** Stephen Bull to make contact with Reuben to investigate what we can use.

## Recent incidents

There was not time in the meeting to discuss recent incidents in the news.

Group members can post incidents and comment on posts by others here: <https://scsc.uk/f190>

## SCSC Business

Stephen Bull reminded attendees that SCSC runs a programme of seminars. For more information see the website: <https://scsc.uk/events?tab=scsc> Please take a look and see whether any is of interest.

SCSC is also looking for papers for next year’s symposium (SSS’23): please get in touch if you have any suggestions for a paper. (More information here: <https://scsc.uk/file/898/SSS22-Call-for-Abstracts-v3.pdf>)

## AOB

Dave Banham requested that we put material on a collaboration site so it is easier to make comments. TG2 already works in this way. (The SCSC website is not set up to allow this.)

In the interim, Nikita has agreed to host on a Google Drive site. Access will need to be granted on an individual basis. This would only be used for collaborative working documents.

Stephen Bull will look at longer term alternatives.

# Actions

| Action | Owner(s) | Status |
| --- | --- | --- |
| 20/4-2: Identify cyber security experts who may be able to support development by SISWG.*It is great to welcome new cyber experts to our group, but more are welcome.* | All | Open |
| 21/2-2: Meet to improve structure of war story recording*Meeting to involve SB, PH, RR and Oliver Carrigan* | SB | Open |
| 22/2-1: Review TG2 material applying the specific questions about applicability in individual industry sectors*If you intend to review the material please let TG2 know via either of the email addresses below, including a note of which industry sector(s) you cover.* | All | Open until 17/7/2022 |
| 22/2-2: Publish aerospace co-assurance case study | NJ | Open |
| 22/2-3: Comment on new co-assurance guidance and provide co-assurance case study examples for other sectors | All | Open until 17/7/2022 |
| 22/2-4: Explore whether HS2 examples can inform development of organisation and people for co-assurance.*SB to contact Reuben MacDonald* | SB | Open |
| 22/2-5: Explore whether a collaboration site can be used to improve efficiency of commenting on documents*E.g. is this something which can be done via the SCSC website; or hosted by Ebeni?* | SB | Open |

Response to actions can be added to the collaborative working documents on [Google Drive](https://drive.google.com/drive/folders/1WnxVzvWRJEekISP8cQmOqshyWVNpf8x0) where appropriate; any additional comments can be emailed to siswg-comments@scsc.uk

Output from all actions should be emailed to Stephen Bull at stephen.bull@ebeni.com

# Next Meetings

We aim to have another meeting in early September to discuss feedback on TG1 and TG2 material.

1. Affiliation and primary sector of interest listed for each attendee; those marked \* identified specific cybersecurity experience. [↑](#footnote-ref-1)