DSIWG

SCSC Data Safety Initiative – WG Meeting 63

18th August 2021, Zoom

Minutes

Attendees

Mike Parsons (MP) – AAIP, Andy Williams (AW) – NewTechNo, Carl Tipton (CT) – Johnson Matthey, Dale Callicott (DC) – BAE, Mark Templeton (MT) – Qinetiq, Paolo Giuliani (PG) – EDF, Tim Rowe (TR) – GTR Safety Management Ltd, Richard Garrett (RG) – SQEP, Jim Mateer (JM) – SQEP, Michael Green (MG) – Ecomergy, Nick Hales (NH) – ex-MOD, Oscar Slotosch - Validas

Apologies

Emma Taylor (ET) - SCSC, Paul McKernan (PMcK) – Dstl, Paul Hampton (PH) - CGI

Agenda

- Welcome
- Def Stan 00-055 update
- Recent Accidents/Incidents
- Ongoing Debate about Covid-19 Data
- PBL Communications
- 'Dazzle' Data
- SSS'20 Abstracts
- Version 3.4 of the Guidance
- Covid-19 Data-Reliant Systems
- 'Pingdemic'
- SCSC Events
- AOB, etc.

NOTE: All comments or opinions in these notes are attributed only to individual attendees of the meeting, not to their respective organisations.

*[Note that actions are presented in the form **N.Mx** where **N** is the meeting number, **M** a reference number for the action raised in that meeting and **x** is an optional letter that differentiates related actions arising from the same discussion point].*

The meeting slides are available at: https://scsc.uk/file/gd/63rd_DSIWG_Slides_v2-1248.pptx

1. Welcome and Update

MP welcomed the group.

2. Def Stan 00-055 Update

MP mentioned an update received from PMcK explaining the update to Def Stan 00-055:

The Def Stan 00-055 Part 1 Issue 5 has been updated and Annex I (Data Safety) continues to reference the DSIWG:

Notes

2. Some domain Open Standards address Data Safety Requirements when applied within their domain regulatory constraints. The UK Safety Critical System Club Data Safety Initiative Working Group has provided generic Data Safety Guidance, compatible with the Def Stan 00-056 principles, which identifies:

a) Different data types (verification, infrastructure, performance, dynamic and justification) that may have a bearing on system safety;
b) Data properties that may need to be established and maintained;
c) Processes and methods that can be used to identify and analyse risks;
d) Processes, methods and approaches that can be used to evaluate and treat risks and manage data safety requirements.

3. Recent Accidents and Incidents

The following were discussed:

1. Warship positions faked including UK aircraft carrier, https://www.bbc.co.uk/news/technology-58027363
   The safety issue here is that other vessels do not know the true positions and hence may have a collision.
   MG also mentioned the Wired article: Phantom Warships Are Courting Chaos in Conflict Zones, https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/
2. Confusing NOTAMs led overrun 747 crew to use short runway leading to loss of aircraft, https://www.cbc.ca/news/canada/nova-scotia/cargo-jet-overrun-tsb-report-2018-halifax-airport-1.6084155

4. Covid-19 and Data

David Perrin communicated the following sources and ongoing debate about Covid-19 data reliability:

1. "John Dee's Almanac" on Facebook
2. Joel Smalley https://twitter.com/RealJoelSmalley
3. Dr Jessica Rose recently gave a presentation on analysis of VAERS data, https://youtu.be/bMY2tdFNkRU . https://i-do-not-consent.netlify.app/)
4. Dr Robert Malone (https://twitter.com/RWMaloneMD)

The issue of Covid-19 data was discussed, and many issues raised, including the data supporting the vaccination of children. MP mentioned that this was a really good example of Dark Data (missing data about vaccine effectiveness in those groups being a factor).

NH mentioned the Jeremy Farrar and Anjana Ahuja book, "Spike: The Virus vs. The People - the Inside Story" and provided summary notes:
https://scsc.uk/file/gd/Nick_Hales_-_Notes_on_J_Farrar_book_-_Spike_the_virus_versus_the___people-1249.docx
(Farrar's book can be found on Amazon at: https://www.amazon.co.uk/Spike-Virus-People-Inside-Story/dp/1788169220)

5. PBL Communications

MP mentioned two communications from Peter Ladkin:

a) The first on the use of AI & ML in healthcare related to the pandemic, with poor results. A quote from the MIT Technology Review was: *"This pandemic was a big test for AI and medicine...But I don't think we passed that test. Because patients scanned while lying down were more likely to be seriously ill, the AI learned wrongly to predict serious covid risk from a person's position. Some AIs were found to be picking up on the text font that certain hospitals used to label the scans. As a result, fonts from hospitals with more serious caseloads became predictors of covid risk.",* MIT Technology Review by William Douglas Heaven: "Hundreds of AI tools have been built to catch covid. None of them helped", https://www.technologyreview.com/2021/07/30/1030329/machine-learning-ai-failed-covid-hospital-diagnosis-pandemic/

b) An update on the status of IEC 61508 Ed 3. He says there is a still a reference to the Data Safety Guidance but that we need a thorough check when the draft comes out (later this year possibly).

6. Dazzle Data

MP mentioned the work he was doing on 'Dazzle Data' i.e. *'Data which is spurious, superfluous or unexpected which masks and confuses the picture and reduces your ability to see details and often the whole picture.'* His notes are available at:
https://scsc.uk/file/gd/Words_for_Dazzle_Data_for_DSIWG_Guidance_3.4_v0.4-1246.docx
He explained that 'Dark Data' and 'Dazzle Data' are essentially opposites but can have the same impact. The typical Dark Data matrix can be re-interpreted as:

	Recognised as Spurious	Not Recognised As Spurious
Data We Are Aware Of	**Known Knowns** Data which we are aware of and know to ignore	**Known Unknowns** Data which we are aware of but don't know to ignore
Data We Are Not Aware Of	**Unknown knowns** Data which we are not aware of but know to ignore	**Unknown Unknowns** Data which we are not aware of and don't know to ignore

He then explained some of the categories identified within safety engineering. There are 11 categories found to date:

1. Data We Know are Superfluous or Unneeded: "Known Extras"

This case is common in safety where there are extra, irrelevant details that can mask the position. It can be a problem in large safety documents or detailed safety analyses, e.g. those with many rows or columns, e.g. FMECAs.

In this case, the data is recognised as superfluous and is ignored. Examples include:

- Information is included for items which are not part of solution in use at that site or situation
- Data about old or legacy components is included but these are now not in service
- Information is included for every low-risk element
- ML training data contains many cases which are duplicates or closely related, so adding nothing to the learned behaviour

This case can be mitigated in several ways, including: careful filtering, review and use of argumentation notations (e.g. GSN) to make arguments concise. In this case the issue is then the effort required and the accuracy of the removal.

2. **Data We Don't Know Are Unneeded or Spurious: "Unknown Extras"**

This is the most serious case, where the additional data is not recognised as unneeded and may be processed, analysed or left in place when it should be removed. Some examples are:

- Dead code in software where nobody understands its function, or how it relates to the used code and so is reluctant to remove it. The Ariane 4 Inertial Reference function left in place in the Ariane 501 launch disaster might be such a case.
- Parts of the safety case or safety argument are supplied separately (e.g. by a subcontractor or 3rd party) and are obscure. In this case it will not be known which parts are relevant to the particular situation. Some information may be irrelevant or worse, misleading.
- Poor structuring of the safety argument or use of evidence that it is hard to establish if it is relevant to the claim/argument
- ML training data containing too many outliers, which are not recognised as such

Mitigations include review, static analysis and data analysis.

3. **Data Obscuration: Missing What Matters**

This is where the meaning of the overall data set becomes obscured due to the extra unnecessary data. Examples might be:

- Measuring the wrong things due to excessive noise or too much data to deal with
- Processing involving sampling only picks bad data elements
- Being too close to the data, i.e. the "wood for the trees". This is when the extra data masks the overall issue with the data, e.g. a slow trend or bias.

Mitigations include review, statistical checks and "taking a step back" to look at the bigger picture.

4. **Data Masking in Specific Cases**

This is where the extra data specifically masks, obscures or hides particular data elements (but not all). A difficult case of this is where filters are put in place to remove unwanted data values, but those filters actually remove less (or more) than they should (i.e. don't remove all unwanted cases or remove valid values as well). Some examples might be:

- The number of successful test runs vastly outweighs failed runs and so the failures are not investigated
- Selective sampling from sensors, or where the sampling intervals are chosen badly
- Incorrect filtering of the data, leaving in some cases that should have been excluded

Mitigations include use of review and completeness checks. Note that over-aggressive filtering would create cases of Dark Data.

5. **Masquerade or Fraudulent Data**

This is where data has been constructed to fool the system consuming it, hiding, overlaying or replacing the correct data. Often this will be malicious and should be filtered or rejected by the target system, but of course may not be.

- Intentional fraud
- Some security attacks

Mitigations include audit, monitoring, intelligent profiling of data and detection of changes.

(see: https://scsc.uk/file/gd/Words_for_Dazzle_Data_for_DSIWG_Guidance_3.4_v0.4-1246.docx for the full list):

There was a good discussion about this topic. Newspapers were highlighted as a particular case of both Dazzle Data (i.e. use of 'filler' articles and images to make up an edition to the correct size which are not really valuable, and also Dark Data, i.e. things left out if there is no more room). NH mentioned that the LEDSM technique may help[1].

Action 63.1 (CT): Look at both Dark Data and Dazzle Data for sensors (e.g. when a sensor is saturated, in noisy environment or when readings are below the detection level floor)

7. SSS'22 Abstracts

MP mentioned RG's accepted abstract for SSS'22: *Addressing Data Integrity for Safety Critical Equipment – A Real Life Example:*

> *"Data Systems are increasingly relied upon to provide a user with information to make decisions that have a potential to influence the safety of a system. It is therefore essential that the criticality of information being handled is fully considered and appropriate methods of risk mitigation are implemented. Assessing the impact of information is difficult; particularly ascertaining a measurable correlation between Data and system risk. This is particularly true when the contributory effects of information are very loosely coupled within an accident chain. During the derivation of data safety requirements, particularly for applications that are not stringently regulated, it is difficult to determine a justifiable level of data integrity rigour that is in proportion to the safety risk. If traditional safety techniques are applied this can lead to protracted accident sequences to justify that the residual risk, associated with Data, represents a level which can be argued to be ALARP. This paper discusses the approaches to, and the challenges experienced when applying current recognised good practice data safety*

[1] SCSC forthcoming publication: A GUIDE TO THE LAYERED ENTERPRISE DATA SAFETY MODEL, (LEDSM), Nick Hales: *"Kermit Tyler was warned of the approach of a large flight of aircraft toward Pearl Harbour. The radar operators were tracking Japanese planes coming to attack the base, but the operator, failed to make clear the size of the formation and Tyler did not pass on an alarm of "attack imminent.". In the case of the 9/11 attack on New York's Twin Towers, the intelligence agencies did not share relevant information. These problems and many more like them are caused by a lack of planning of the communication network in advance. There is a need to plan horizontal protocols to communicate with other organisations and vertical protocols to communicate effectively within organisations. LEDSM is a way to develop safer networks of communication of any type, verbal, telephone, internet, etc., or a mix of types, so that the risks of failures to communicate are considerably reduced. This booklet develops the initial idea, taken from the Open Systems Interface. It takes the reader from initial concepts through 10 chapters of increasing learning. The chapters show how, even with increasing complexity, the principles involved provide increased confidence that risks are minimised. Worked examples are provided to increase insights into the numerous possible applications"*

management processes, to a real-world large-scale commercial application and the solutions that have been derived to overcome those challenges."

8. Version 3.4 of DSG Update

There was agreement to produce a v3.4 update of the guidance for SSS'22. This will include:

- Additional accident case studies ('war stories')
- Sufficiency Issue and Hazops
- Possibly something on Dazzle Data

9. Covid-19 Data-Reliant Systems

The table of identified data-reliant Covid-19 systems was reviewed. A new issue has arisen with fake vaccination cards being used in the US. There was a general discussion about the safety issues of faking certification documents (e.g. in aviation spare parts).

10.Pingdemic

It was noted that NHS phone App has been changed from 5 days to 2 days history. There was a suggestion that this was an app configuration error and was not originally specified, but there is some debate, see: https://www.theguardian.com/world/2021/aug/17/covid-app-pinged-close-contacts-in-prior-five-days-not-two-says-source

11.SCSC Events

Future SCSC events (see https://scsc.uk/events) were described and are shown below:

Seminar: Can we quantify risk?
September 23, 2021 - Radisson Blu Edwardian Bloomsbury Street Hotel, London, UK and Virtually Online
In many areas of safety attempts are made to quantify risk. Some of these are apparently more successful than others, but some areas are notoriously difficult to quantify, especially those which ... »

Seminar: Safe Use of Multi-Core and Manycore Processors
November 11, 2021 - London, UK and blended online
This is the event postponed from 2020. It will be held in London as a blended online / in-person event
Confirmed speakers are:
Lee Jacques, Leonardo - WG Activities Overview
Oliver ... »

Seminar: Managing 'Black Swans': Handling Rare and Severe Events Now and in the Future
December 2, 2021 - London, UK and blended online
This seminar will consider how to manage recovery from 'Black Swan' events in a safety context, ie. events which are rare, unexpected and have high impact. Events such as Fukushima ... »

Symposium: Safety-Critical Systems Symposium (SSS'22)
February 8 - 10, 2022 - Bristol, UK and blended online
The Safety-Critical Systems Symposium 2022 (SSS'22) will be held 8-10th February 2022 in person in Bristol, UK and as an online (blended) event.
It is our 30th Symposium and as such will ... »

12.AOB

None noted.

13.Actions, etc.

See table at end.

62.2 was closed

14.Next Meeting

Next meeting will be held 6th October 2021 by Zoom 3:30-5:00 BST. MP to arrange.

It may be possible to hold a blended (in-person / online) meeting in November/December.

15.Thanks

Thanks to all participants. Thanks to MP for chairing the meeting and taking the minutes.

16. Summary of Open Actions

Actions greyed out are considered closed and will be removed from the list at next issue.

Ref	Owner	Description	Target Guidance Version
42.6	PH	Define the process to publish a document developed in Overleaf via Amazon	3.4
42.9	MP	Work out a matrix of data categories (previously 'types') and data properties (as per DB discussion)	N/A
43.4	MP	Write up a data focussed FMEA approach.	3.4
44.2	MP	To discuss with AK on how to get the Wikipedia article published	N/A
46.1	MP	Review the application of DSALs to higher level forms of aggregation	N/A
49.6	MT	Review Overleaf briefing material and aim to hold a briefing before end of March 2021 in the use of Overleaf in the production of the guidance.	N/A
53.1	MP	To talk to Kevin King about what we need to do in the guidance for digital twins.	3.4
56.2	DA	Consider impact of Dark Data on the Data Safety Tool	N/A
61.1	MP, PH, MT	Check existing data property definitions and add a case related to "Unexpected" data	3.4
61.2	MA, MT, AW	Research the relevance of digital currencies and report back to the group	3.4
62.1	MA	Create war story for the next issue of the guidance on the Buncefield data loss	3.4
62.2	MP	Consider a 'Dark Data' type of treatment for unwanted or unexpected data	3.4
62.3	MP/MT	Consider issues of porting and importation of legacy data	3.4
63.1	CT	Look at both Dark Data and Dazzle Data for sensors (e.g. when a sensor is saturated, in noisy environment or when readings are below the detection level floor)	3.4