SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY

DSIWG

SCSC Data Safety Initiative – WG Meeting 51

17th March 2020, Webex/Teleconf

Minutes

Attendees

Mike Parsons (MP) – CGI, Paul Hampton (PH) – CGI, Tim Rowe (TR) – GTR Safety Management Ltd, David Dowe (DD) - Lloyds Register Foundation, Dale Callicott (DC) – BAE Systems, Mark Templeton (MT) – Arcade Experts, Divya Atkins (DA) – Mission Critical Applications, Martin Atkins (MA) – Mission Critical Applications, Paul McKernan (PM) – DSTL, Nick Hales (NH) - Consultant, David Sykes (DS) - Consultant, Brent Kimberley (BK) - Region of Durham, Canada

Apologies

Dave Banham (DB) – Blackberry, Chris Harper (CH) - University of the West of England, Fan Ye (FY) – ESC, Sam Robinson (SR) – EDF, Paul Mukherjee (PMu) – Astellas, Ali Hessami (AH) – Vega, Paolo Giuliani (PG) – EDF, Andy Williams (AW) – Newtechno, John Bragg (JB) – MBDA, Alastair Faulkner (AF) – Abbeymeade, Louise Harney (LH) – Leonardo, Xinwei Zhou (XZ) – Atkins, Andrew Eaton (AE) – CAA, Miguel Rodrigues (MR) – Eurocontrol, Ashley Price (AP) – Raytheon

Agenda

- Coronavirus / COVID-19
- Updated on SSS
- Update on Guidance Document V3.2
- Sales/Downloads Update
- Intro from David Dowe of Lloyds Register Foundation
- Tooling Update
- Aims for 2020/2021
- Future Events
- Minutes and action status
- AOB, etc.
- Data Safety in the News
- Next Meeting

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 [1].

1. Coronavirus / COVID-19

MP noted how much the current COVID-19 pandemic is relying on models and data to make significant safety-related decisions affecting the health of large volumes of people. MT expressed concern that some countries may have different practices in testing and reporting data, and so the data on which decisions are being made may be distorted and not reflect the true situation. There were questions as to whether the data was being considered as safety-related and being treated as such to address the types of issues the guidance is meant to address. MT suggested that the guidance should be used to retrospectively see if it would apply to this particular novel scenario. MP referred the group to a recent article he has posted in LinkedIn "Coronavirus is a systems safety issue!" [2].

2. Update on SSS'20

MP showed the slides that he presented at SSS'20 discussing the progress the working group has made to date and included other details such as the data aspects of the Boeing 737 MAX accidents [5]. PM however expressed concern that there is still not widespread acknowledgment of data as a source of hazards, as distinct from hardware and software. MP said that there has been good progress in healthcare, but regulators will need to be targeted in the future to get real traction within industry.

MP said the paper *"Safety Critical Integrity Assessments in Large Datasets"* given at SSS'20 was of particular relevance to data safety and machine learning [3]

3. Update on Guidance Document V3.2

MP said that version 3.2 of the data safety guidance was issued at SSS'20 [6] and highlighted the main changes in this version of the document as follows:

- clarifications arising from the tooling project;
- "data type" now called "data category";
- a new section on future work;
- unique serial numbers added to the tables in section 6.4;
- high level mitigations in Table 9 references have been amended;
- new war story covering Being 737 MAX and Soyuz rocket;
- a new section on Machine Learning.

4. Sales/Downloads Update

MP said there were 101 downloads of the PDF version of the Data Safety Guidance v3.2 [6] to date.

PH said there were 2 purchases of the Data Safety Guidance v3.2 hard copy last month.

5. Intro from David Dowe of Lloyds Register Foundation

DD said the LRF was a charity established in 2012 whose mission is to engineer a safer world and funds various projects to this end, working with organisations and consortia to establish best practices. Recent grants have been looking at the safety of food and analysing global attitudes to risk, the quality of safety data and the provision of real evidence to support clinical decision making.

DD said that the LRF have funded an initial demonstrator tool for Data Safety, but for the next phase, they would be looking for end-user engagement with demonstrable commitment, before providing further funding. There are several models of how to do this under discussion.

6. Tooling Update

DA presented an update on tooling and said that:

- A 'Z' specification Poster was presented at SSS'20 [4].
- There is now a complete Demo Tool with flyers including tool screenshots;
- The Tooling Sub-group (TSG) will be initiated today (as a plenary to this meeting) and invites to register will be sent out the following week;
- They are looking for pilot projects/case studies from user organisations to use this demonstrator tool, to elicit feedback for future updates.

DA highlighted that the tool currently allows only a single risk for any data artefact. Allowing multiple risks could lead to large data-sets, requiring management of the resulting complexity in the tool. It was acknowledged that there is absence of any guidance on managing such complexity in the current guidance document. [Post meeting note: This is a key issue - it is suggested that this is added as a new section for next issue.]

[Post meeting note: Managing complexity is a key issue - it is suggested that this is added as a new section for next version, showing how the work can be scaled.]

DA showed the poster that was presented at SSS'20, which presented the relationships between the properties and the issues around the complexities as there are many properties that can be lost for a given artefact, and hence can cause data-related hazards.

MT said we should understand and try the tool ourselves before trying to roll out and educate others in the need for the tool. MP thought the tools should have an attractive user interface in order to successfully promote the adoption of the tool.

7. Aims for 2020/2021

MP asked what the priorities should be for the guidance for the 2020/2021 period. PH said the Ontology Work has revealed several issues with the guidance that should be addressed as a priority, as they are fundamental to the structure of the guidance. Other aspects such as Machine Learning should also be advanced, but it was thought this would be better kept as an appendix for the next release.

8. Ontology Working Group

PH presented the progress of the Ontology Working Group. He said that a new SCSC working group has now been set up that will have a wider role in promoting an ontology for general risk management of which data safety is a particular aspect. He also presented the 3 main issues that have arisen from trying to formalise the language of risk in the data safety guidance.

Organisational Data Risk Assessment Form (relationship with DSALs)

The ODR is a simple tool for assessing organisation risk exposure to data safety concerns in their product systems. The DSG (v3.2) "extrapolates" this assessment into specific product system data-safety process tailoring without consideration for the specific hazards and harms that product system might create.

DSALs defined as a target for assurance rigour but used as a risk score

It is therefore unclear what the purpose of the DSAL columns are for in the techniques tables. Moreover, it is not at all clear how an assurance based DSAL is determined, or how assurance rigour is verified (i.e. what is the required objective evidence?)

Alignment with the 4+1 data safety principles
The overall data-safety process does not currently align strongly with the 4+1 data safety assurance principles. This alignment needs to be undertaken and the result used to revalidate these data safety assurance principles in light of our improved understanding.

9. Tooling Working Group

DA led a plenary meeting to kick off the Tooling Working Group. See separate minutes.

10. Future Events

Not discussed.

11. Minutes and action status

See table at end [Not discussed - some amendments made post-meeting.]

12. AOB, etc.

PH noted that there is a NHSX consultation on a new NHS Digital Health Technology Standard (https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-data-and-technology-standards). This is a wider standard that will encompass the existing NHS standards for Health IT (such as DCB0129) and include other aspects such as Ethics.

13. Data Safety in the News

The following were briefly discussed:

1. https://nakedsecurity.sophos.com/2020/02/14/self-driving-car-dataset-missing-labels-for-pedestrians-cyclists/

2. https://arstechnica.com/science/2020/02/boeings-starliner-problems-may-be-worse-than-we-thought/

3. https://www.flightglobal.com/news/fokker-50-crash-crew-ignored-multiple-alerts-during-take-off-roll/136871.article

4. https://www.businessinsider.com/amtrak-new-ceo-safety-concerns-atlas-amazon-air-crash-2020-3?r=US&IR=T

5. https://assets.nhs.uk/prod/documents/NHS_Digital_Health_Technology_Standard_draft.pdf

6. https://dhsc.surveyoptic.com/NHS-DHTS

14. Next Meeting

A WebEx/Teleconf meeting in May is suggested. MP to arrange.

15. Thanks

Thanks to all for taking part.
Thanks to PH for taking minutes.
Thanks to MP for chairing the meeting.

Summary of Open Actions

Rows have been greyed-out to indicate that the actions were closed during this meeting. Those entries will be deleted from future versions of the action log.

Ref	Owner	Description	Target Guidance Version
42.6	PH	Define the process to publish a document developed in Overleaf via Amazon	4.0
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.	4.0
44.1	MT	Review last 12 months of DSIWG minutes and put any actions referring to v4.0 into Appendix O.	4.0
44.2	DB/LH	To develop the Wikipedia article to get it into a position where it can pass review and be published.	N/A
46.1	MP	Review the application of DSALs to higher level forms of aggregation	N/A
46.3	MP	Make it more obvious why only a handful of data categories have been selected for the guidance when there are over 30 in the appendices.	3.2
49.6	MT	Review Overleaf briefing material and aim to hold a briefing Webex (between 16th and 20th December 2019) in the use of Overleaf in the production of the guidance.	N/A
49.9	PH	Suggest some wording on how the ODR relates to risk appetite.	3.2
49.11	DA/MP	Prepare an introductory email to send out to the DSIWG group inviting people to join the tooling subgroup.	N/A
50.1	PH	Issue updated cover picture for review	3.2
50.2	MT/PH	Produce review copy by 24/01/20 and upload to KDP (with PH) by 01/02/20.	3.2
50.3	MA	Produce a war story on the Soyuz launch failure.	3.2
50.4	PG	Arrange meeting at EDF to demonstrate the tool	N/A
50.5	DA	Start up the sub-group and initiate first teleconf	N/A

16. References

Ref	Title	Location
[1]	Meeting slides	https://scsc.uk/file/gd/51st_DSIWG_Slides-659.pptx
[2]	COVID-19 and data	https://www.linkedin.com/feed/update/urn:li:activity:6645266900311961600
[3]	Assuring Safe Autonomy	Proceedings of the Twenty-eighth Safety-Critical Systems Symposium, York, UK. https://scsc.uk/scsc-154
[4]	Z Data Safety Guidance Poster	https://scsc.uk/file/gd/SSS20_Poster_Z_Spec-670.pdf
[5]	WG Slides at SSS'20	https://scsc.uk/file/gd/DSIWG_-_Parsons_-_DSIWG_slide_v4-660.pptm
[6]	V3.2 of Guidance Document	https://scsc.uk/scsc-127E