SCSC FOR EVERYONE WORKING IN SYSTEM SAFETY

DSIWG

SCSC Data Safety Initiative – WG Meeting 46

10th June 2019, CGI London/Webex

Minutes

Attendees

Mike Parsons (MP) – CGI, Paul Hampton (PH) – CGI, Gordon Hurwitz (GH) – Thales, Martin Atkins (MCA) – Mission Critical Applications, Divya Atkins (DA) – Mission Critical Applications, Dave Banham (DB) – Rolls–Royce PLC [Webex], Chris Barnes (CH) – Highways England, Dale Callicott (DC) – Consultant.

Apologies

Mark Templeton (MT) – Arcade Experts, Nick Hales (NH) – ex. MOD, Paul McKernan (PM) – DSTL, Mike Ainsworth (MA) – Ricardo, Amira Kawar (AK) – CGI, Fan Ye (FY) – ESC, Andrew Eaton (AE) – CAA, John Bragg (JEB) – MBDA, Martyn Clarke (MC) – Consultant, Paolo Giuliani (PG) – EDF Energy, Rob Ashmore (RA) – Dstl, Sam Robinson (SR) – EDF Energy, Alastair Faulkner (AF) – Abbeymeade, Steve Clugston (SC) – Consultant, David Smith (DS) – FNC, Louise Harney (LH) – Leonardo, Paul Mukerjee – Astellas, Graham Sutherland (GS) – Consultant, Jeanette Baldwin (JBa) – Thales, Jenny Brain (JB) – Wood PLC, Julian Lockett (JL) – FNC

Agenda

1. Introduction and Status
2. SSS Abstract on data
3. Outputs from OWG
4. Tooling Status & Funding
5. Tool demo
6. Heatherbury Community Health Case Study
7. Updates for Guidance Document 4.0
8. Discussion of data in Boeing 737 MAX accidents
9. Training Course Update
10. Overleaf status
11. Sales/Downloads Update
12. Dissemination update
13. Standards update
14. Future Events
15. Minutes and actions status
16. AOB, etc.
17. Data Safety in the News

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 [4].

1. Introduction and Status

MP provided a summary of the status of the working group and noted that although the guidance is relatively mature now, there are some gaps and areas for improvement. The intention is therefore to produce a version 4.0 for the next SCSC symposium in Feb 2020 (SSS'20).

2. SSS Abstract on Data

MP noted that a number of abstracts have been submitted for SSS'20 which have content related to data safety.

3. Output from OWG

DB gave an overview of progress of the Ontology Working Group (OWG). The group was established in January 2019 and has been working on refining the ontological model and to suggest changes that would be necessary to make the guidance consistent with the model. DB said the ontology model itself has now been reviewed and revised and some sections of the guidance have proposed updates to align with the ontology. The process has however uncovered a number of issues, which the group discussed.

DSAL

DB said the guidance is unclear on how DSAL are applied as the guidance conflates the risk assessment and the level of assurance rigour required when mitigating risks. The guidance suggests the DSAL is the risk score but DB questioned whether the DSAL should be related to the risks score as directly as this.

DB also said that the DSAL relate to data properties but when defining mitigating techniques, the guidance aggregates these up to the covering systems, which therefore, may apply to many other data artefacts and properties. MP said assurance techniques tend to be broad brush and not just dealing with specific risks (c.f. software DALs and SILs).

One of key questions arising from the discussion was how DSAL assessments on individual Data Artefacts are rolled up and applied to higher level aggregations. The group discussed whether the guidance should establish a calculus for aggregating DSALs; this might, for example, be as simple as taking the highest applicable DSAL, but this would need further investigation. It was noted that ARP4754 provides a calculus for aggregating assurance levels and it was thought that this might usefully inform a similar process for DSALs. For example, in ARP4754, a DAL A level can be claimed if the function is implemented by two [independent] DAL B components. It was however acknowledged that data may be different. For example, in ARP4754 you can only lower the required assurance level when you can show independence of components; how independence of data artefacts could be claimed was unclear.

It was agreed that a section should be added to the guidance to explain the issue and provide guidance on the aggregation of DSALs.

Action MP [46.1] Review the application of DSALs to higher level forms of aggregation

Application ODR
The role of the Organisational Data Risk (ODR) assessment form was discussed. It was noted that the form was originally intended to simply raise awareness of data safety issues within an organisation predominantly for new projects. However, it has since been appropriated as a useful means of determining the level of rigour to be applied in managing data safety risks and therefore as a means of defining the organisation's risk appetite. For example, one organisation may decide not to do any further work in reducing data safety risks for DSAL1 or DSAL2 whereas another, more risk averse, organisation may decide to apply the guidance at all levels.

PH noted that Mark Thomas [NHS Digital] had developed this idea and promoted the concept in a healthcare workshop for clinicians in York [1]. Mark's idea was that an organisation should tailor the guidance to define what activities would be undertaken at each step of the risk assessment process (called principles in the slideset). PH said he thought this could be a useful addition to the guidance as the tables in the guidance simply establish the techniques to be used, not the rigour by which they are applied. There were however concerns with this approach. Firstly, it was argued that it is the detailed technical safety assessment that should drive the level of rigour to be applied to reducing the associated risks and the ODR top down approach would not be sufficiently rigorous. It was thought that this approach might be more suited to those sectors where there are no safety standards, but might otherwise be confusing to those sectors that are subject to formal safety standards. It was also debated whether the questions were correct if the ODR was to be used for this purpose and it was thought they may therefore need to be revisited.

Action PH [46.2] Put together a positioning paper on how ODRs, tailoring and DSALs operate together.

Likelihood as a parameter of risk
DB discussed the concept of *Causality Sensitivity*, a term coined as a result of the OWG updates. The term is used to allow the quantification of likelihood of the loss of a data property and likelihood as a probability is otherwise difficult to determine for data.

Data Categories
MCA noted that there are only 6 out of 31 data categories mentioned in the techniques tables and there is no detailed explanation of why only these properties have been selected for discussion in the guidance over the other categories, and whether it is intended to add to the list of categories in future.

Action MP [46.3] Make it more obvious why a handful of data categories have been selected for the guidance when there are over 30 in the appendices.

4. Tooling Status & Funding

DA gave an update on the Data Safety Tooling [5]. MCA and DA have been working on a prototype tool and looking for funding to continue this work. DA said that they resubmitted an application to the Lloyds Register Foundation (LRF) in April, after discussion with the allocated case officer. The revised proposal structures the development over 2 phases of work: an initial 6-month proof of concept phase, followed by a 2nd phase covering the formal development of the tool over a 15 month period. DA noted that the LRF's main concern is that they are a charity and don't want to fund something that would not end up being used and hence want assurances that organisations will use it. DA said the application was going to be considered by a grants committee and there should be a go/no go decision soon.

DA appealed to members to ask their organisations to submit a letter of interest for collaboration either in a Level 1 / Level 2 capacity. The letter would confirm the organisation's intent to use the product, and to commit up to 35 days of collaboration effort to the project.

5. Tool demo

MCA gave a demo of the prototype tool in current development. He showed a browser for the techniques table, and it was suggested that in the longer term, the tool might become the master of the techniques list and extracts could then be provided for the guidance document.

6. Heatherbury Community Health Case Study

PH presented the Heatherbury Case Study [6] to illustrate the use of the guidance to derive data safety requirements. This illustrated the bottom up approach of deriving data safety requirements directly from DSAL assessments of data artefacts.

7. Updates for Guidance Document 4.0

Not discussed specifically.

8. Discussion of data in Boeing 737 MAX Accident

The events surrounding the recent Boeing 737 MAX accidents were discussed [2]. In summary, in order to compete with Airbus, the old 737 airframe had been adapted to accommodate more fuel efficient engines. This led to a change in the aerodynamic characteristic of the aircraft. To avoid having to retrain all 737 pilots with the new behaviour, a Manoeuvring Characteristics Augmentation System (MCAS) was added. The MCAS sensed the aircraft's angle of attack (AOA) and modified flight controls to give similar handling behaviour to earlier models. There were a number of issues identified:

- The MCAS used the data from a single sensor and so was prone to a single point of failure;
- There was a feature to alert pilots to erroneous sensor readings but this was a costed optional extra (again, to avoid having to retrain pilots);
- Pilots were not made aware of the MCAS system;

It was noted that there are strong parallels with the Sidney Dekker's presentation at SSS'19 [3]

GH mentioned a previous project on the Nimrod aircraft that had a similar MCAS function as has been implemented in the Boeing 737 MAX aircraft. However, he said it was acknowledged that the system could cause the aircraft to nosedive so multiple techniques were used to mitigate the risk, such as 3 sensors with a voting design pattern and other monitoring systems that checked correct operation. This level of rigour and protection did not seem to have been implemented on the 737 MAX, which had a single channel input.

9. Training Course Update

No update.

10. Overleaf status

No update.

11. Sales/Downloads Update

MP showed the download statistics from the SCSC website.
PH said there were no purchases of the Data Safety Guidance v3.1 hardcopy from Amazon in the last 90 days.

12. Dissemination update

No update.

13. Standards Update

No update.

14. Future Events

MP showed the up and coming events at SCSC:

- Learning from Accident Investigations on 13th June 2019, https://scsc.uk/e594
- Tutorial on Safety Assurance of Autonomy and Machine Learning 26th Sep 2019, https://scsc.uk/e624
- Creating and Maintaining an effective Safety Culture 5th Dec 2019, https://scsc.uk/e631

15. Minutes and action status

The actions table was updated during the meeting.

16. AOB, etc.

None.

17. Data Safety in the News

None.

18. Next Meeting

The aim is to hold a conference call 3rd week in July 2019.

19. Thanks

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

20. 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
36.4	MC	Coordinate the production of training material (based on v3.0).	N/A
40.10	MT	To ask if his Qinetiq course can be released to DSIWG and be presented at SSS'20	N/A
41.8	MT/BJ	Ensure Data Safety Guidance PDFs have no ligature problems. Note that this also affects copy-and-paste from the low-resolution PDFs.	N/A
41.10	PH	To update the healthcare trifold to include the NHS logo colour, if approved, and arrange distribution of the trifold at key healthcare events	N/A
42.4	LH	Get an update from RO on cyber-data properties mapping, which has been published.	N/A
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

Ref	Owner	Description	Target Guidance Version
43.3	GH	Speak to Stephen Boyle & James Weston on Cyber security aspects of IT/OT to see if they could contribute.	4.0
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
44.3	MT/MP	Make contact with Martyn Clarke to see if there is any progress on Action 36.4 (production of training material)	N/A
45.1	MP	MP to invite Mark Thomas to join the DSIWG. Also ask if his paper could be forwarded to MT.	N/A
45.2	MCA	MCA to send MT details of the serial numbers applied to treatments within the demonstrator. This is to ensure that numbering within the Guidance and tooling can be aligned.	4.0
45.3	MP	MP to insert a pointer from v3 to v3.1 of the Guidance, to ensure users will become aware that the later version is now available.	3.1
45.4	MP	MP to provide link to Facebook page in the minutes.	4.0
46.1	MP	Review the application of DSALs to higher level forms of aggregation	N/A
46.2	PH	Put together a positioning paper on how ODRs, tailoring and DSALs operate together.	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.	4.0

21. Names for the Data Elephant

The previous meeting established **"Delphi"** and **"Dharma"** as the most popular names for the real "Data Elephant".

22. AOB

None.

23. References

Ref	Title	Location
[1]	Mark Thomas healthcare workshop slides	https://files.digital.nhs.uk/BA/3B70DF/Data%20Safety%20March%202019.pdf
[2]	Boeing 737 MAX accidents	https://en.wikipedia.org/wiki/Boeing_737_MAX_groundings

[3]	Automation Surprise in the 21st Century: Culture, Collaborative Cognition, Complexity and Legacy Systems	https://scsc.uk/e569prog
[4]	Meeting slides	https://scsc.uk/file/gd/46th_DSIWG_Slides-564.pptx
[5]	Update on Data Safety Tooling	https://scsc.uk/file/gd/Mission_Critical_Applications_Slide_-_DST-565.pptx
[6]	Heatherbury Case Study	https://scsc.uk/file/gd/Heatherbury_Community_System_v2_(1)-540.docx