DSIWG

SCSC Data Safety Initiative – WG Meeting 36

11th October 2017, Thales, Crawley

Minutes and Actions

Attendees

Mike Parsons (MP) – NATS, Rob Ashmore (RA) – DSTL, Martin Atkins (MaA) – Mission Critical Applications, Eric Bridgstock (EB) – Raytheon, Des Burke – BAE, Martyn Clarke (MC) – SCSS Ltd, Robin Cook – Thales, Nick Hales (NH) – DE&S, Gordon Hurwitz (GH) – Thales.

Apologies

Michael Aspaturian (MAs) – EDF Energy, Divya Atkins (DA) – Mission Critical Applications, Janette Baldwin (JB) – Thales, Dave Banham (DB) – Rolls–Royce PLC, John Bragg (JEB) – MBDA, Dale Callicott (DC) – BAE, Steve Clugston (SC) – JLR, Shaun Cowles (SC) – EDF Energy, Andrew Eaton (AE) – CAA, Paolo Giuliani (PG) – EDF Energy, Robert Green (RG) – NATS, Amira Hamilton (AH) – CGI, Paul Hampton (PH) – CGI, Louise Harney (LH) – Leonardo, Chris Hartgroves (CH) – Leonardo, Ali Hessami (AH) – Vega, Clive Kelsall (CK) – BAE, Clive Lee (CL) RINA, Bob Oates (RO) – Rolls–Royce PLC, Ashley Price (AP) – Raytheon, Bernard Twomey (BT) – Rolls Royce, Fan Ye (FY) – ESC, Derek Fowler (DF) – JDF, Mike Ainsworth (MA) – Ricardo, Alastair Faulkner (AF) – Abbeymeade, Duncan Dowling (DD) – DARD, Paul Ensor (PE) – Boeing, Julian Lockett (JL) – FNC, Sam Robinson (SR) – EDF, Ged Lancaster (GL) – JLR, Dave Lunn (DL) – Thales, Carolyn Stockton (CS) – BAE, Sean White (SW) – NHS Digital, Matthew Twiselton (MTw) – MOD.

Agenda

1. Guidance Document: New structure, Version number, Objectives, Accidents, DSALs, Compliance
2. Updates from DSIWG members
3. Note from DF on objectives & comments
4. SCSC Update, including data–related poster and paper abstracts for SSS'18
5. Review of 2017/8 plans, including changes, new topics and improvements
6. Move to LaTeX update (including collaboration platform and DocuWiki issues)
7. Sales/Downloads Update
8. Formal modelling activity update
9. Dissemination update
10. Standards update
11. Future events
12. Minutes and actions status
13. AOB, etc.
14. Data Safety in the news
15. Further work

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].*

1. Guidance Document: New structure, Version number, Objectives, Accidents, DSALs, Compliance

RA explained the new structure of the guidance, which explicitly distinguishes between normative, informative and discursive text. MP and RA exhibited hardcopies showing this new structure, as well as the results of transitioning to LaTeX. The results of previous actions (for example, introducing comments about claiming compliance, revising the appendix detailing accidents and incidents) were highlighted. One action resulted:

Action 36.1 [RA] Remove the phrase "in some circumstances" from the description of the SHOULD term.

Suggestions for revising the objectives were discussed (including some pre–meeting comments by MP, LH and input from DF).
It was agreed that the objectives do not explicitly need to mention stakeholders; that "unintended behaviour" was a better phrase than "failure"; and that "established" and "justified" were two separate objectives. For ease of reference, the full set of revised objectives is available in this document (see Appendix A).

It was agreed that the next edition would be numbered v3.0 (rather than v2.1 or similar).

It was also agreed that the next edition would remain as "guidance"; that is, the title would not include the word "standard".

2. Updates from DSIWG members

MP presented updates from:

- MaA, who provided an update (in person) on progress with regards to obtaining funding for the production of tools to support the implementation of Data Safety Guidance. He also noted his willingness to support LaTeX–related activities.

- CL, who noted that a colleague from RINA, Ebby Joseph, may be able to attend future meetings.

- DC, who offered to support the production of training material. The group agreed that such material would be valuable and that training may be a notable objective for work in Calendar Year 2018.

Other updates were covered under the relevant agenda item.

3. Note from DF on objectives & comments

This note was discussed in relation to the revised objectives under agenda item 1.

4. SCSC update, including data related abstracts submitted for SSS'18

MP showed the planned programme for SSS'18, highlighting the sessions which include data safety: (i) Two presentations on the 3rd day, (ii) Updates from Working Groups, and (iii) "Birds of a Feather".

5. Review of 2017/2018 plans, including changes, new topics and improvements

The intention is for v3.0 of Data Safety Guidance to last two years; that is, there will not be an update for SSS'19 (in February 2019). Although detailed plans were not discussed, the current intent is to focus on training and researching new topics (for example, data safety for machine learning) in 2018.

6. Move to LaTeX update

MT provided input prior to the meeting. He noted that the transition to LaTeX was complete. However, the free version of Overleaf (the collaborative editing system) allows anonymous edits, which is not desirable. A Pro+ version, which does not allow this, is available at US$12 per month. This is being trialled. There are volunteers who will fund some of this but, ideally, these costs should be borne by the SCSC.

Action 36.2 [MP] Determine whether the SCSC will fund the costs associated with Overleaf Pro+ (details of what this provides are available at: https://www.overleaf.com/plans).

7. Sales/downloads update

MP presented the sales/download updates: For the V2 guidance, there have been 221 copies sold and 954 downloads to date.

8. Formal modelling activity update – feedback on Concept Model for Data Risk Management

DB provided input prior to the meeting. He noted that he had made some progress on the document modelling. This had identified some inconsistencies, which had been passed to RA. (RA noted that these had been addressed in the latest draft.) Unfortunately, other commitments have prevented a revised version of the model being completed.

9. Dissemination update

NH noted he had publicised the Facebook page. This attracted some interest.

10. Standards update

Current versions of key defence standards (00-056 and 00-055) were noted. These are both now on a standard four year review cycle.

11. Future events

It was noted that there will be papers related to Data Safety at: High Integrity Software (HIS) in October 2017, the IET System Safety and Cyber Security conference (October/November 2017) and SSS'18 (February 2018).

It was suggested that there would be value in having an updated trifold to distribute at these (and future SCSC) events.

Action 36.3 [MaA] Update the trifold (based on material to be provided by MP).

12. Minutes and actions status

The following actions were closed: 29.9, 31.17, 31.18, 31.21, 33.2, 33.3, 33.10, 33.12, 34.2, 34.3, 34.4, 35.1, 35.2, 35.4.

13. AOB, etc.

MC noted the existence of the "Data For Safety" initiative (https://www.easa.europa.eu/newsroom-and-events/press-releases/easa-and-aviation-partners-launch-data4safety). He undertook to write to the leader of that initiative, mentioning the importance of Data Safety.

14. Data Safety in the news

MP highlighted a report about detention letters being sent in error: http://www.bbc.co.uk/news/uk-41027671. Although this is not necessarily a safety issue, it is one where distress was caused.

15. Further work

The intent is to provide a final draft of v3.0 by the end of November. This will allow two weeks for DSIWG members to proof read, before starting the publication process.

MC volunteered to coordinate the production of training material. Although this will be based on v3.0, there is sufficient information for the work to start now.

Action 36.4 [MC] Coordinate the production of training material (based on v3.0).

16. Thanks

Thanks to GH (and Thales) for hosting the meeting.

Thanks to RA for taking the minutes.

17. Summary of Open Actions

Ref	Owner	Description	Target Guidance Version
31.8	MT	Look at applying the guidance to the autonomous aircraft airworthiness example previously used to assess the dataware framework report.	3.0
31.19	SC	Write some text about sampling rate issues and consider where in the guidance this could be included.	3.0
32.1	PH	Identify a unique document name for the next version.	3.0
32.6	DeB	Generate a database of historical incidents and accidents where data is considered to have been a contributory factor.	3.0
33.5	LH	Add a couple of posts before making the LinkedIn page public.	N/A
33.6	LH	Add everyone on the DSIWG distribution list to the LinkedIn page.	N/A
33.7	MaA	Investigate what simulation tools may be appropriate for data safety modelling in their sector.	N/A
34.1	PH	Get in touch with Dr Farah Magrabi to share the work being done on the Healthcare Data Guidance.	N/A
35.3	RO/MAs	Suggest rewording of the data properties table definition where these are unclear.	3.0
35.5	MAs	Contact local IET to get a presentation slot then let the group know and it will identify someone to present.	N/A
36.1	RA	Remove the phrase "in some circumstances" from the description of the SHOULD term.	3.0

Ref	Owner	Description	Target Guidance Version
36.2	MP	Determine whether the SCSC will fund the costs associated with Overleaf Pro+ (details of what this provides are available at: https://www.overleaf.com/plans).	N/A
36.3	MaA	Update the trifold (based on material to be provided by MP).	N/A
36.4	MC	Coordinate the production of training material (based on v3.0).	N/A

18. References

Meeting Slides	http://scsc.org.uk/file/gd/36th_DSIWG_MP_Slides-336.pptx
Current draft of next version	http://scsc.org.uk/file/gd/Guidance_Doc_051017-338.pdf
MAA minutes of meeting (SMAG 10)	http://scsc.org.uk/file/gd/20170831-SMAG_10_Minutes___FOR_APPROVAL-O-337.pdf

APPENDIX A - REVISED OBJECTIVES

Establish Context

1. System context and intended use SHALL be established.
2. Key stakeholders SHALL be identified.
3. Interfaces SHALL be defined and managed.
4. A Data Safety Assessment SHALL be planned.
5. Data Artefacts SHALL be identified

Identify Risks

1. Historical data-related accidents and incidents SHALL be reviewed.
2. Unintended behaviour resulting from data SHALL be identified and analysed.
3. Risks SHALL be identified and linked to Data Artefacts and Data Properties.

Analyse Risks

1. Data Safety Assurance Levels SHALL be established.
2. Data Safety Assurance Levels SHALL be justified.
3. Data Safety Assurance Levels SHALL be incorporated into system safety activities.

Evaluate and Treat Risks

1. Data Safety Requirements SHALL be established and elaborated.
2. Methods used to provide Data Safety assurance SHALL be defined and implemented.
3. Compliance with Data Safety Requirements SHALL be demonstrated.