SCSC Data Safety Initiative – WG Meeting 33

25th April 2017, MBDA, Bristol

Minutes and Actions

Attendees

Mike Parsons (MP) – NATS, Eric Bridgstock (EB) – Raytheon, Rob Ashmore (RA) – DSTL, Mark Templeton (MT) – QinetiQ, Dale Callicott (DC) – BAE & UKHO, Dave Banham (DB) – Rolls-Royce PLC, Paul Hampton (PH) – CGI, Louise Harney (LH) – PA, Martyn Clarke (MC) - ALS, Nick Hales (NH) – DE&S, John Bragg (JEB) – MBDA, Gordon Hurwitz (GH) – Thales, Steve Clugston (SC) – Consultant.

Apologies

Alistair Faulkner (AF) – Abbeymeade, Ali Hessami (AH) – Vega, Fan Ye (FY) – ESC, John Spriggs (JS) – NATS, Bob Oates (RO) - Rolls-Royce PLC, Janette Baldwin (JB) - Thales, Andrew Eaton (AE) - CAA, Amira Hamilton (AH) - CGI, Chris Hartgroves (CH) - Leonardo, Shaun Cowles (SC) - EDF Energy, Paolo Giuliani (PG) – EDF Energy, Michael Aspaturian (MAs) – EDF Energy, Sam Robinson (SR) – EDF Energy, Victor Malysz (VM) - Rolls-Royce PLC, Clive Kelsall (CK) – BAE, Tim Kelly (TK) – University of York, Des Burke (DeB) – BAE Systems, Ashley Price (AP) - Raytheon, Simon Brown (SB) - Qinetiq, Ged Lancaster (GL) - Jaguar Land Rover, Carolyn Stockton (CS) - BAE, Ashraf El-Shanawany (AES) - CRA Risk

Agenda

1. Objectives & Requirements, decision on new structuring of guidance document, etc. Sales/Downloads Update
2. SCSC December event & SSS'18 CFA
3. Network Rail Update
4. Health Guidance
5. Where to send next 10 copies of the guidance
6. Sales/Downloads Update
7. LinkedIn / Social Media Update
8. Classification?
9. Move to LaTeX update
10. Analysing of the Uberlingen Accident Simulation
11. Formal modelling activity update
12. Dissemination update
13. Standards update
14. Future Events – IET
15. Minutes and actions status
16. AOB, etc.
17. Data Safety in the News
18. Further work: Falsification of Data, Testing Data

19. 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].*

1. Objectives & Requirements, decision on new structuring of guidance document, etc.

RA discussed progress on reworking the guidance into normative/guidance/informative and presented the possible new structure [1]. The group was supportive of the proposed reorganisation.

RA asked the group if each section should declare its content type: normative/informative etc. NH was concerned that people may cherry pick from the informative parts of the text but the group agreed to the marking of sections in this way.

Action 33.1 [RA] Restructure the document into informative/normative/guidance sections as proposed.

Action 33.2 [MC/MP] Review the guidance objectives, outputs and definitions.

RA presented an update [2] on action 32.3 to identify how principles can be satisfied and presented initial conclusions. He noted that at least 2 objectives cover each of the principles apart from Principle 4 which doesn't have any explicit objectives around checking whether any new hazards have been introduced by applying the first few principles.

It was agreed that a new objective should be added stating that any new data mitigations should be passed up to the system team; also any new data mitigations should be checked to see if they have compromised any other data properties.

Action 33.3 [LH] Consider adding new objectives to cover Principle 4.

RA noted that we say little about decomposition arising from Principle 2. DB noted these were originally derived from software assurance principles and from a data perspective shouldn't be trying to tell people how to do decomposition.

RA also noted with principle 3 that the guidance document does not describe how to demonstrate satisfaction of requirements, i.e. evidencing that they have been implemented. MP thought this was achieved through linkage to the tables.

The modelling of the data argument was discussed and the need for a GSN structured argument of the guidance document was reasserted.

Action 33.4 [JEB] Review work MBDA has done in GSN and correlate with the work that RO is doing.

2. SCSC December event & SSS'18 CFA

MP noted that there is an SCSC event on 15th June 2017 "Risk, Proportionality and ALARP: How do we do enough for safety?" which may be relevant to data safety. MP showed the list of speakers.

There is also an SCSC event in London in December discussing healthcare crossover that will be relevant to the group [Healthcare is very data-intensive].

MP noted that the SSS'18 will be in York next year and there is a call for abstracts for SSS'18 (submissions by end May) and also for the IET conference on systems safety and cyber-security.

MP also noted that for SSS'18, an alternative engagement opportunity will be available through the use of a poster. Speakers would at various points in the conference stand by their poster and present their ideas to those interested. [This is significantly less effort than preparing a paper and presenting it.]

MP also noted that at SSS'18 each of the SCCS working groups (including this one) will be asked to present an update on progress.

3. Network Rail Update

MP sent an unsolicited copy of the guidance to a suggested contact at Network Rail (Davin Crowley-Sweet) and the response was very positive. The Home Office was proposed as another potential contact.

MP noted that CreateSpace has been able to link the two document issues on Amazon so the new guidance document is promoted and highlighted as the latest but it is still possible to buy the old version.

MP noted that in future versions the version needs to be in the CreateSpace title to avoid any problems with inadvertent copyright infringement concerns.

4. Health Guidance

PH gave an update on the status of the healthcare guidance and said he had updated it to reflect version 2.0 of the guidance and had had some comments. It was agreed that once comments are addressed it can be sent to NHS Digital for review and publication.

5. Where to send next 10 copies of the guidance

MP has approval to send 10 more unsolicited copies (paid for by the SCSC) and asked the group to suggest further contacts who might benefit from being made aware of the content.

6. Sales/Downloads Update

MP showed the current sales statistics for hardcopies (206) and downloads (438) for the Data Safety Guidance.

7. LinkedIn / Social Media Update

LH presented progress on the LinkedIn page. LH suggested adding a couple of posts before making it public.

It was agreed to add everyone to the distribution list once it is ready to be made public.

Action 33.5 [LH] Add a couple of posts before making the LinkedIn page public.

Action 33.6 [LH] Add everyone on the DSIWG distribution list to the LinkedIn page.

There was no progress on setting up a Facebook page although it was thought that this was not as valuable as LinkedIn and it was thought that the group should concentrate primarily on LinkedIn moving forward.

It was agreed that posting to LinkedIn should be a standing agenda item in the DSIWG meetings.

8. Classification?

MP raised a point as to whether document protection markings idea could be applied to data safety (c.f. BS10010). However, it was agreed that this was not an area the group thought could be transferred easily.

It was noted that there is an Aviation standard that now that links safety and security viz. DO-326A / ED-202A.

9. Move to LaTeX update

MT has talked to the University of York and they said they would allow the group to have a collaborative environment. This will be as a minimum the LaTeX environment and configuration management. MT noted that Overleaf might be an alternative LaTeX environment which is web based and free for up to 40 people. MT noted that Overleaf shows a WYSIWYG view and also what changes other people have done who are working on the same document.

JEB showed the work he and MT had done already on porting the guidance to the LaTeX format. JEB said he is trying to make it as simple as possible to work with.

10. Analysis of the Uberlingen Accident Simulation

NH presented ideas on applying the 7 layer model in the Data Safety Guidance to the Uberlingen Disaster [3]. He noted that structuring against the model helped highlight issues. He went on to show the colour coded sequence of events and the use of animation to illustrate issues. NH asked whether some form of animation for data interactions could be useful. JEB noted the similarities with STAMP and highlighted some work called XSTAMP[1] (http://www.xstampp.de/) related to STAMP. It was agreed that using a simulation tool that could handle data faults would be useful avenue to explore.

SC noted that FRAM (Functional Resonance Analysis Method) is a methodology[2] that may be of use.

Action 33.7 [All] Investigate what simulation tools may be appropriate for data safety modelling in their sector.

[1] An extensible modelling environment for STAMP/STPA analysis. As it is extensible it's possible that an 'animator' could be developed for it.

[2] FRAM is not a tool but a methodology, however a tool (FMV) does exist for visualising FRAM models (http://functionalresonance.com/FMV/index.html)

11. Formal modelling activity update

DB presented an update on the formal modelling following on from his paper in SSS'16. DB noted the move from the original assurance bias to one that is more risk-centric. He noted work done for the OMG relating to threat and risk and how that has been used to inform his work. There was discussion around the term Cyber and the concept of separating out digital data as distinct from other types of data. MP suggested as an ambition, the next version of the document is informed by the model (it is unlikely to be in a position to claim it is completely consistent with the model). [Note the updated model may be downloaded from [13]. DB would welcome any feedback.]

12. Dissemination update

LH said she has sent the PDF of the guidance document to some old colleagues but has had no feedback yet.

Action 33.8 [MP] Check with Brian Jepson to see if it is possible to find out who has actually downloaded the data safety guidance and consider whether any are worth following up.

13. Standards update

Issue 7 of 00-056 has been published now in 2 parts. EB said he is no longer on the standards committee. Guy Barratt of BAE SYSTEMS has taken his place, and they are in frequent contact.

14. Future Events – IET

MP said that the IET are interested in holding a full or half day event on Data Safety.

15. Minutes and actions status

The status of the previous actions was agreed, as follows:

Action 28.5 Ongoing.
Action 29.2 Ongoing.
Action 29.9 Ongoing.
Action 30.12 Closed – MAs will let us know when.
Action 30.16 Closed – work has been done and there are other actions to cover this activity.
Action 31.8 Ongoing.
Action 31.10 Action superseded.
Action 31.11 MP did pursue this but has not heard back.
Action 31.12 MP did email Roger Rivett and talk to him but no response yet. Changed to David Ward.
Action 31.13 MP did email Tim and Mark but there has not been any significant response. Action Closed.

It was noted that Lancaster University do entertain visiting lecturers so this might be a more fruitful angle to pursue but no one knew anyone to approach.

Cranfield was also noted as a possible University to approach.

Action 33.9 [GH] Forward on a contact from Cranfield University who MP can approach for introducing data safety as an academic module.

Action 33.10 [MC] Propose some contacts to approach for introducing data safety as an academic module.

Action 33.11 [MP] Send copies of the guidance to Simon Place, Ray Cherry, Audrey Canning and Daz Stephenson.

Action 31.14 Ongoing.
Action 31.15 no update.
Action 31.16 MP did talk to Graham and spoke to the events coordinator. Action Closed.
Action 31.17 Ongoing
Action 31.18 Ongoing
Action 31.19 Reworded to be achieved by passing action on to Tim Kelly.
Action 31.21 Ongoing
Action 32.1 Action complete. Changed to just reflect last part.
Action 32.2 Ongoing.
Action 32.3 Action complete.
Action 32.4 Action complete.
Action 32.5 Ongoing.
Action 32.6 No update.
Action 32.7 Action complete – 10 copies have been approved.
Action 32.8 EB said they have agreed in principle but need to work out how to place the order through the company.
Action 32.9 Action complete.
Action 32.10 Action complete.

It was agreed that for document acknowledgements, those that have worked on the current version will be listed with affiliation and anybody else who has ever worked on the guidance listed as acknowledged without affiliation [as per the MISRA C Guidelines approach].

16. AOB, etc.

It was discussed whether some of the war stories should age and the list be refreshed with new stories.
Action 33.12 [RA] Update the "Incidents and Accidents" section of the document

[Other documents received were:
Data Integrity for Marine and Offshore Operations – ABS [12]
MHRA GP Symposium: Data Integrity – MHRA [11]
]

17. Data Safety in the News

- Life was ruined by a typo [4]
- How fake data could lead to failed crops and other woes [5]
- 2017 Irish Coast Guard Rescue 116 crash [6] and [7] (note also quotation on page 14 of [8])

SC provided an example of where an accident investigation was impeded through mishandling of recording sensor data.

18. Further work: Falsification of Data, Testing Data

Not discussed.

19. Next Meeting

DSIWG #34, 7th June 2017 (TBC – awaiting confirmation), PA Consulting, London.

20. Thanks

Thanks to PH for taking the minutes and actions, and JEB for hosting the meeting.

21. Summary of Open Actions

Ref	Owner	Description	Target Guidance Version
28.5	DB	Publish an agreed version of the data model whitepaper.	2.1
29.2	NH	Publicise the data safety guidance via social media such as Facebook.	N/A
29.9	PG	Look into adding a worked example in the civil nuclear sector	2.1
31.8	MT	Look at applying the guidance to the autonomous aircraft airworthiness example previously used to assess the dataware framework report.	2.1
31.11	MP	Talk to John McDermid to see if he can help write to various regulators to make them aware of the guidance and ask them to review/comment.	N/A
31.12	MP	Talk to David Ward about how to disseminate the guidance into the automotive sector.	N/A
31.14	All	After SSS'17, make contact with at least one international colleague or contact and let them know about the new publication and invite them to participate in the group.	N/A
31.15	AH	Raise with IEEE standards about seeking more international participation with the group.	N/A
31.17	MT	To set up a subgroup including JEB, MT and RA to decide on how best to manage the implementation of the move to LaTeX. [Including hosting and collaborative environment issues.]	2.1
31.18	MP	Ensure legal and liability of the group's work is given due consideration by Tim Kelly in future meetings (disclaimers etc.), including production of WG terms of reference.	N/A
31.19	SC	Write some text about sampling rate issues and consider where in the guidance this could be included.	2.1
31.21	MP	Write some text on Falsification and submit this for review within the group.	2.1
32.1	PH	Identify a unique document name for the next version.	2.1
32.2	MP	Arrange a follow on meeting to discuss NR's approach further and look to involve them (Davin Cowley-Sweet) in the DSIWG	N/A
32.5	RA	Collate the feedback from reviews conducted against the latest version of the Data Safety Guidance document	2.1
32.6	DeB	Generate a database of historical incidents and accidents where data is considered to have been a contributory factor.	2.1
32.7	MP	Discuss with the SCSC the potential of purchasing and distributing more free copies of the Guidance document, using the revenue generated from sales.	2.0
32.8	EB	Discuss the potential of Raytheon supplying funds for the publication of the next version of the Guidance document.	2.0
33.1	RA	Restructure the document into informative/normative/guidance sections as proposed.	2.1
33.2	MC/MP	Review the guidance objectives, outputs and definitions.	2.1
33.3	LH	Consider adding new objectives to cover Principle 4.	2.1
33.4	JEB	Review work MBDA has done in GSN and correlate with the work that RO is doing.	2.1
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	All	Investigate what simulation tools may be appropriate for data safety modelling in their sector.	N/A
33.8	MP	Check with Brian Jepson if it is possible to find out who has actually downloaded the data safety guidance and consider whether any are worth following up.	N/A

Ref	Owner	Description	Target Guidance Version
33.9	GH	Forward on a contact from Cranfield University who MP can approach for introducing data safety as an academic module.	N/A
33.10	MC	Propose some contacts to approach for introducing data safety as an academic module.	N/A
33.11	MP	Send copies of the guidance to Simon Place, Ray Cherry, Audrey Canning and Daz Stephenson.	N/A
33.12	RA	Update the "Incidents and Accidents" section of the document	2.1

References

[1] 20170301 – PossibleNewStructure http://scsc.org.uk/file/gd/20170301-PossibleNewStructure-245.docx

[2] Progress against action 32.3 http://scsc.org.uk/file/gd/20170413-ObjectivesToPrinciples_DRAFT-275.docx

[3] Analysis of the Uberlingen Accident Simulation. <TBD>

[4] My life was ruined by a typo http://www.bbc.co.uk/news/uk-39328853

[5] How fake data could lead to failed crops and other woes http://www.bbc.co.uk/news/business-38254362

[6] 2017 Irish Coast Guard Rescue 116 crash https://en.wikipedia.org/wiki/2017_Irish_Coast_Guard_Rescue_116_crash

[7] Irish Coast Guard helicopter crash: 'We're gone' - last words from cockpit of Rescue 116 http://www.belfasttelegraph.co.uk/news/republic-of-ireland/irish-coast-guard-helicopter-crash-were-gone-last-words-from-cockpit-of-rescue-116-35621770.html

[8] PRELIMINARY REPORT ACCIDENT Sikorsky S-92A, EI-ICR Black Rock, Co. Mayo, Ireland 14 March 2017 http://www.aaiu.ie/sites/default/files/report-attachments/REPORT%202017-006%20PRELIMINARY.pdf

[9] Meeting Slides http://scsc.org.uk/file/gd/33rd%20DSIWG%20MP%20Slides-271.pptx

[10] Input to NHS Digital for data guidance http://scsc.org.uk/file/gd/Clinical%20Risk%20Management%20-%20Data%20Safety%20v4%20DRAFT-256-273.pdf

[11] MHRA slides on data integrity http://scsc.org.uk/file/gd/MHRA%206-data-integrity-270.pdf

[12] Data Integrity for Marine and Offshore Operations http://scsc.org.uk/file/gd/CyberSafety_V3_Data_Integrity_GN_e-272.pdf

[13] Tidied up version of concept model for http://scsc.org.uk/file/gd/Proposal%20for%20a%20model%20of%20data%20risk%20management%20v

	data risk management	A.2-276.pdf.