SCSC Data Safety Initiative – WG Meeting 35

11th July 2017, Rolls-Royce, Bristol

Minutes and Actions

Attendees

Mike Parsons (MP) – NATS, Rob Ashmore (RA) – DSTL, Dave Banham (DB) – Rolls-Royce PLC, Paul Hampton (PH) – CGI, John Bragg (JEB) – MBDA, Nick Hales (NH) – DE&S, Gordon Hurwitz (GH) – Thales, Bob Oates (RO) - Rolls-Royce PLC, Martin Atkins (MCA) - Mission Critical Applications, Dale Callicott (DC) – BAE, Bernard Twomey (BT) – Rolls Royce, Michael Aspaturian (MAs) – EDF Energy.

Apologies

Louise Harney (LH) – PA, Divya Atkins (DA) - Mission Critical Applications, Davin Crowley-Sweet (DCS) - Network Rail, Ashley Price (AP) – Raytheon, Ali Hessami (AH) – Vega, Martyn Clarke (MC) – ALS, Fan Ye (FY) – ESC, 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, Clive Kelsall (CK) – BAE, Steve Clugston (SC) – JLR, Robert Green (RG) – NATS, Eric Bridgstock (EB) - Raytheon.

Agenda

1. New structuring of guidance document inc. Guidance vs. Requirements
2. Marine Data Safety – Bernard Twomey
3. Feedback from hardcopy document recipients
4. SCSC update, including data related abstracts submitted for SSS’18
5. Review of 2017/2018 plans, including changes, new topics and improvements
6. Move to LaTeX update
7. Sales/downloads update
8. Formal modelling activity update – feedback on Concept Model for Data Risk Management
9. Tooling update
10. Social Media update
11. Dissemination update
12. Standards update
13. Future events, including IET
14. Minutes and actions status AOB, etc.
15. AOB, Book dedication, etc.
16. Data Safety in the News – recent articles on BA data centre outage, Police data, EASA initiative etc.
17. Further work: Falsification of Data, Testing Data, etc.
18. 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].*

(Meeting slides can be found in [7].)

1. New structuring of guidance document inc. Guidance vs. Requirements

RA presented the new structure of the guidance [1] that shows the content split between normative and informative and is now generated from LaTeX. RA noted objectives are specified as shalls and shoulds. The question was therefore raised as to whether the document should be termed as Guidance or should be now Guidance and Requirements. There was concern that as Guidance, it does not compel organisations to implement it in the same way that a Requirements document may do. The use of the word Interim was discussed; it was thought that the question might be asked on what authority the requirements document was produced; Interim allows a level of consultation with organisations and markets. The most promising proposal considered was to use Data Safety at the main title and have a sub title "Interim Requirements and Guidance" and include a section on compliance. However further consideration needs to be given to this. It was also thought that a section on compliance and justifying non-compliance should be added.

Action 35.1 [MP] Work with the group to establish a new title and subtitle for the guidance document
Action 35.2 [RA] Add a paragraph on context of compliance and include justification of non-compliance

MAs noted that the ONR nuclear regulator is starting to look into this area and identifying data as a separate entity to software and hardware and moving to a standard would help promote more formal adoption by the regulator.

2. Marine Data Safety – Bernard Twomey

BT gave a presentation on Insurance implications arising from Cyber attacks on Maritime vessels [2]. BT noted that for autonomous ship systems there are no regulations or standards for regulators. He highlighted a safety incident where remote access of a ventilation system by an OEM caused the ship's engine to shut down during manoeuvring due to oxygen starvation. He also noted that there is exclusion clause (CL380) for malicious breaches where there is intent to cause harm. This therefore means there is an insurance gap and so additional insurance is offered by underwriters.

A new Insurance Act of 2015 introduced a duty of 'fair presentation' so ship owners (or those taking out the insurance, e.g. charterer) need to disclose the level of risk to the underwriter (e.g. unusual facts and concerns). Answer is to err on side of utmost caution, and encourage rule makers to mandate disclosure of cyber and 'off ship' capability.

BT said that IACS have set up a Cyber Systems Panel to provide recommendations for activities such as physical security, procedures for software updates and data assurance. He highlighted some emerging guidance documents for cyber security in the maritime domain. BT noted also that the boundary of the whole system is not just constrained to the ship as there are on-shore components that are also part of the overall system that needs to be protected.

3. Feedback from hardcopy document recipients

MP said that more copies have been sent out and one set of feedback has been received from Ray Cherry [8]. Ray said he had noted the document and would include it in future courses. MP thought that regulators should also be the focus of future copies of the guidance.

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

MP said that two papers relating to data have been accepted for SSS'18. LH's paper on "A system engineering approach to data risk" and MP/PH (et al) paper "Data in Police and Criminal Justice systems". MP noted that there will be a requirement for a short update from the group at the symposium and MP asked for volunteers to give this update. Also "Birds of a Feather" sessions will also be held where working groups can get together.

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

MP noted that there had not been any progress with IET in hosting a data safety focussed event, despite showing interest initially. A SCSC tutorial/worked example in around September 2018 was proposed and agreed as something the group should work towards. It was thought that if the group moves to a 2 year document update cycle it could focus on generation of tutorial material in the interim publishing years. NH noted that the tutorial should be repeatable but it was agreed that the group needs to be realistic about how much effort can be devoted to it.

DB said that there is a need to describe how data can give rise to harm. RO referred to a similar Microsoft method called STRIDE. DB noted that linkage between data properties and accidents/incidents is not as well defined in the model at the moment. There were also comments raised about the textual descriptions of properties, which some thought were too abstract.

Action 35.3 [RO/MAs] Suggest rewording of the data properties table definition where these are unclear.

It was discussed whether the group should add current trending topics to the guidance such as machine learning, big data analytics, etc. The concern would be that the guidance may become out of date as new trends emerge. It was thought that these could be covered in ancillary guidance documents/pamphlets so it was agreed that these would not be covered in the main document.

6. Move to LaTeX update

JEB said that v2.0 guidance has been put into LaTeX but there was no update on hosting yet. The University of York have said they could host, but Overleaf may be better (although it is restricted to 5 named users). It was discussed whether the configuration control of the LaTeX environment could be held centrally in, for example, GitHub or SVN. Action 31.17 was therefore modified to include MCA.

7. Sales/downloads update

MP presented the sales/download updates: For the V2 guidance, there have been 215 copies sold and 768 downloads to date.

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

DB said he has updated the model document to address review comments to date. DB said the original OMG risk/threat model has been updated but mainly reflecting more refinement of their model. The question arose as to whether to include the model into the guidance document. DB said that decision should be made by the reviewers as it is still a work in progress and it still needs to be checked that it aligns with the document. MP felt that including the model, even an incomplete one would be worthwhile and may encourage wider review and contribution from the wider community.

Action 35.4 [All] Provide input on what are considered the important aspects of the guidance that should be in the model.

9. Tooling update

MCA presented progress on tooling for those intending to use the data safety guidance. MCA said DA has been in touch with DCS at Network Rail and a contact involved in NHS Digital research who have expressed an interest. MCA presented a context diagram [3] [updated after the meeting in [3a]]. Comments on the diagram were that:

- The individuals at the top should have defined roles, e.g. data safety engineers;
- There is a need to clarify which phase of the lifecycle the context apply to – it was agreed that it was predominantly for the development lifecycle but could be used for operational and maintenance phases.
- It was thought that a monitoring process or engine could be part of the tooling if actual data properties are checked from live data feeds;
- It would be useful to include use cases to clarify how the tool would be used.

MCA said he is still looking for funding to help progress effort on developing the tooling. Ideally it would be useful to have a version for use by the group for the tutorial in Sep 2018. It was noted that the tool may require qualification itself.

10. Social Media update

Members were encouraged to like and follow the Facebook page.

11. Dissemination update

MAs noted that ONR have now taken an interest in data safety and starting to acknowledge that it is separate from software and hardware and needs consideration in its own right.

RO has pointed the IMarEST (Institute of Marine Engineering, Science & Technology) Cyber Security Group Special Interest group at the guidance and also to the ATI (Aerospace Technology Institute).

PH said he has sent the Healthcare guidance to NHS Digital for final review before publication and also to Farah Magrabi (an associate professor at Macquarie University) who has an interest in healthcare standards.

12. Standards update

Nothing significant to record.

13. Future Events – IET

The possibility of future events with the IET was discussed and MP said that there has been no further progress on organising a national event. It was thought that a local IET event may be more promising.

Action 35.5 [MAs] Contact local IET to get a presentation slot then let the group know and it will identify someone to present

14. Minutes and actions status

NH noted that in the previous notes and actions to meeting #34, the sentence: *"issues are more to do with confidence in data rather than quality*", in the Network Rail data management section could be interpreted as implying that data quality was not important. However, this was clearly not the case from the process information DCS presented. The point was noted and agreed that this interpretation did not reflect DCS's intention. The rest of the notes and actions were otherwise agreed.

29.9	PG	No Update – MA to chase
31.8	MT	No Update
31.11	MP	MP did get in touch but no further update. Action Closed
31.17	MT	Ongoing
31.18	MP	Ongoing
31.19	SC	No Update
31.21	MP	Ongoing
32.1	PH	Ongoing
32.6	DeB	No Update
33.1	RA	Action Complete
33.2	MC/MP	Ongoing
33.3	LH	Ongoing
33.5	LH	Ongoing
33.6	LH	Ongoing
33.7	All	To be reassigned to MCA
33.9	GH	Action Complete
33.10	MC	No Update
33.12	RA	Ongoing
34.1	PH	Action Complete.
34.2	RA	Ongoing
34.3	RA	Ongoing
34.4	DA	Ongoing

15. AOB, Book dedication, etc.

It was decided not to provide any book dedication in the next version.

16. Data Safety in the News – recent articles on BA data centre outage, Police data, EASA initiative etc.

- False earthquake alarm that was triggered 92 years after it happened [4] (note false alarms can actually give rise to accidents as people can be hurt during evacuations);
- Police in Durham introducing an AI system to help decide whether individuals should stay in custody or not [5];
- Vulnerability in Intel chips [6].

17. Further work: Falsification of Data, Testing Data, etc.

Due to time limitations, this agenda item was not discussed.

18. Next Meeting

DSIWG #36 mid-September. Possibly at Network Rail, Thales in Crawley or NHS Digital Leeds.

19. Thanks

Thanks to PH for taking the minutes and actions.

Thanks to RO and Rolls-Royce for hosting the meeting.

20. Summary of Open Actions

Ref	Owner	Description	Target Guidance Version
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
31.17	MT	To set up a subgroup including JEB, MT, RA and MCA 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
32.6	DeB	Generate a database of historical incidents and accidents where data is considered to have been a contributory factor.	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
33.5	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	MCA	Investigate what simulation tools may be appropriate for data safety modelling in their sector.	N/A
33.10	MC	Propose some contacts to approach for introducing data safety as an academic module.	N/A
33.12	RA	Update the "Incidents and Accidents" section of the document	2.1
34.1	PH	Get in touch with Dr Farah Magrabi to share the work being done on the Healthcare Data Guidance	N/A
34.2	RA	Add text to the guidance to say the safety criteria for DSAL's can be tailored, and indeed should be reviewed and updated for each context	2.1
34.3	RA	Add text to the guidance to say the guidance can be applied to other areas not just safety, e.g. reputational damage, financial loss, etc.	2.1
34.4	DA	Develop a proposed way forward for developing concept demonstrator tools to support the implementation of Data Safety Guidance.	N/A
35.1	MP	Work with the group to establish a new title and subtitle for the guidance document	2.1
35.2	RA	Add a paragraph on context of compliance and include justification of non-compliance	2.1
35.3	RO/MAs	Suggest rewording of the data properties table definition where these are unclear.	2.1

Ref	Owner	Description	Target Guidance Version
35.4	ALL	Provide input on what are considered the important aspects of the guidance that should be in the model	2.1
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

References

[1] Restructured Guidance Document http://scsc.org.uk/file/gd/Restructured%20Guidance%20Document-322.pdf

[2] Ship Intelligence/Marine 4.0 Insurance Interface http://scsc.org.uk/file/gd/Ship%20Intelligence%20-Marine%204.0%20mtg%2005072017-320.pptx

[3] Tooling Context Diagram http://scsc.org.uk/file/gd/Martins%20image-321.jpg

[3a] Updated Tooling Context Diagram http://scsc.org.uk/file/gd/Tool%20Diagram%202-323.png

[4] California earthquake alarm sounded - 92 years late http://www.bbc.co.uk/news/technology-40366816

[5] Durham Police AI to help with custody decisions http://www.bbc.co.uk/news/technology-39857645

[6] About the Intel manageability firmware critical vulnerability https://www.intel.co.uk/content/www/uk/en/architecture-and-technology/intel-amt-vulnerability-announcement.html

[7] Meeting slides http://scsc.org.uk/file/gd/35th%20DSIWG%20MP%20Slides-318.pptx

[8] Book feedback http://scsc.org.uk/file/gd/Book%20feedback-319.txt