

SCSC Data Safety Initiative – WG Meeting 41

11th July 2018, Highways England, Birmingham

Minutes and Actions

Attendees

Paul McKernan (PM) – DSTL, Nick Hales (NH) – ex-DE&S, Dave Banham (DB) Rolls–Royce PLC, Bernard Twomey (BT) – Rolls-Royce PLC, John Bragg (JEB) – MBDA, Louise Harney (LH) – Leonardo, Mark Simmonite (MS) – Highways England, Peter Smith (PS) – Highways England, Mike Parsons (MP) – NATS (Phone)

Apologies

Bill Blackburn (BB) – Process Renewal Group, Eric Bridgstock (EB) - Raytheon, Mark Templeton (MT) – QinetiQ, Dale Callicott (DC) – BAE/UKHO, Gordon Hurwitz (GH) – Thales, Martyn Clarke (MC) – SCSS, Vincent Martin (VM) – Raytheon, Robert Oates (RO) - Rolls Royce PLC, Paul Hampton (PH) – CGI, Martin Atkins (MaA) – Mission Critical Applications, Divya Atkins (DA) - Mission Critical Applications, Michael Aspurian (MAS) – EDF Energy, Ebby Joseph (EJ) – RINA, Phil Wright (PW) – DSTL, Fan Ye (FY) – ESC, Paolo Guiliani (PG) – EDF, Chris Hartgroves (CH) – Leonardo, Shaun Cowles (SC) – EDF, Paul Dart (PD) – NCC Group, Mark Nicholson (MN) - _ University of York, Sam Robinson (SR) – EDF Energy, Ged Lancaster (GL) – JLR, Carolyn Stockton (CS) – BAE, John Spriggs (JS) – NATS, Maria Kelly (MK) – Leonardo, Paul Caseley (PC) – DSTL, Andrew Eaton (AE) – CAA, Ashley Price (AP) - Raytheon

Agenda

1. Highways England Presentation (MS, PS)
2. Data Strategy Session (All)
3. Model for Data Risk Management – see doc link (DB)
4. Ligature problems in Guidance Document (MT/DB)
5. Overleaf status (MT)
6. Sales/Downloads Update (MP)
7. Tooling update (DA, MA)
8. Dissemination update (All)
9. Standards update (All)
10. Training course update (MC/MT)
11. Future Events (MP)
12. Minutes and actions status (All)
13. AOB (All)
14. Data Safety in the News (All)

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].*

Slides used in the meeting are available in [1].

1. Highways England Presentation

Highways England presented their view on data safety, and the slides have been uploaded to the DSIWG resources [TBD].

DB and PM questioned how Highways England are analysing the 'to be' scenario, as the presentation focusses on characterising the data currently used by or available to Highways England. A discussion was held around the group's suggestions for further work Highways England could do. BT asked how data which is not critical for safety would be filtered out from the assessment, and which new stakeholders might be identified when greater autonomy is involved. The 'ultimate safe state' of a motorway was discussed, as Highways England can't prevent people from driving. However, all data provided is advisory (i.e. Highways England inform, rather than control, drivers), so that could be switched off. NH commented that the 'tunnel problem' requires more detailed analysis. For instance, the scenario where signalling is used to group for example tankers together to pass through a tunnel before the tunnel is reopened to all other traffic.

2. Data Strategy Session

At the last meeting it was difficult to find enough information within the working group on these topics, so some actions were taken to try and find people to talk about these things. Unfortunately, it was not possible to achieve this for the current meeting, but the actions remain.

Internet of Things / Cyber Physical Systems and Operational Technology / IT Convergence

MP talked about the SCSC seminar on IoT, which had quite a big data angle in the healthcare presentation. MP will try to gather the slides from this event and distribute them at a later date. No case studies are currently available, so this appears to be an area where the risks have not yet been analysed in detail. It was suggested to improve awareness that another event should be held next year, and it would be necessary to partition the data issues from the IOT concepts. The presentation given by Stuart Harrison of NHS Digital is available here [2].

Cryptography

No update provided at this meeting.

Big Data

No update provided at this meeting.

Cloud / Service Agreements / Distributed Infrastructure

It was agreed to follow up with VM after the meeting to get an update.

Autonomy and Machine Learning / Self Learning and AI / Lack of Determinism and Geography Configuration / Challenge to Decision and Accident Investigation

BT provided information from the maritime perspective. The International Maritime Organisation (IMO) is analysing the regulations, but it could be a long time before they have concluded whether a regulatory reason exists to restrict fully automated systems. In the meantime, technology is being used where agreement from nation states is provided (e.g. Norway, Finland, Denmark) and the vessel is operating within their own territorial waters. Different levels of autonomy are defined for marine applications; e.g. part autonomous but still a manned vessel (e.g. propulsion systems). Different sets of requirements may apply if the remote control of a vessel is located in a different country to the vessel itself. In the legal framework, a ship would be covered by maritime law, but an office (including remote control centre) covered by HSE regulations. Bilateral or trilateral agreements between nation states are likely to be required, complicating the safety assessment.

It was agreed that this complex area needs further analysis, including questions around whether certain ships may be forbidden from entering some territorial waters (in a similar way to some airspace restrictions) if they are deemed not to be safe, and issues around identification and tracking of military vessels using remote control centres.

MP mentioned a presentation he did for the University of York on test coverage for autonomous systems which included “Data Coverage” [3].

It was agreed to post about these topics on the LinkedIn page, and email round members asking for people who know about these topics. Two actions were raised.

Wireless Communications (GPS, energy-harvesting sensors, etc)

No update provided at this meeting.

Blockchain

No update provided at this meeting.

3. Model for Data Risk Management

DB presented his updated ontological model. A summary report was provided for review in advance of this meeting, and is available [4].

The full report of the ontology modelling is available [5]. The model includes an incomplete attempt to unify terms for safety and security to avoid the need for two separate models.

DB requests that group members validate the ontology in their domain of work. The DSIWG then needs to take ownership of the terms described by the modelling, and ensure that the Data Safety Guidance consistently uses these terms as described (and agreed) via the modelling. Two actions were raised.

DB is using PTC Integrity Modeler, which is not a tool available to all DSIWG members. DB agreed to try exporting the document as html to see if that allows linkage between diagrams.

It was recommended that members read BS 31100:2011, *“Risk management – Code of practice and guidance for the implementation of BS ISO 31000”*, as it has useful content relevant to the Data Safety Guidance.

An action was raised for BT to find out who updates each of the standards the modelling is based on, so we can feed back anything we think could be improved based on difficulties with the modelling and understandability of the standards.

An action was raised for LH to speak to TK about the possible impact on standards through the SCSC SG, with the view to raise a standing SCSC SG agenda item.

An action was raised for MP to think of how to better to broadcast the ontological model within the wider world, including the SCSC and outside.

4. Ligature problems in Guidance Document

Ligature problems are being sorted in the guidance document and existing PDFs with problems could be replaced with the fixed versions. An action was raised for MP / BJ to update the PDFs.

[Post meeting note: JEB and MT have understood how the Ligature problem occurred. The current v3.0 document that is available for download from the SCSC website could be updated without a version number change since no material content will be changed, but this will require JEB and MT to do it. (NB BJ made a “display resolution” version from the supplied “printer resolution” PDF and care will be required that such a post production activity does not create problems.)]

5. Overleaf Status

MT needs to share information on how to use this because others have found it difficult to see change tracking. Overleaf is a collaborative environment, which makes it difficult to show what is a locked in change, rather than what is a temporary fix. An action was raised to follow up with MT after this meeting. It may be possible to add his guidance directly to Overleaf.

6. Sales/Downloads

MP provided an update on sales, which is included in [1].

7. Tooling Update

Possible tool support was briefly discussed, but feedback from DA and MA was that funding has not been secured to build their tooling as desired. It was discussed that building on UML modelling already used may be too complicated.

8. Dissemination update

It was agreed to ask PH to put NHS logo, if approved, on the healthcare trifold and arrange its distribution at relevant healthcare events. An action was raised.

An action was also raised on BT to provide key event dates that he is aware of, at which dissemination may be useful / welcomed.

9. Standards update

The SCSC may wish to seek direct influence on UK representations body for IEC 61508, and an action has already been placed for this at a previous meeting.

10. Training course update

Updates have been received from MT and MC via email. Some progress has been made in getting the training course approved for an external audience but further approvals are still required, so it is not anticipated that the course will be available in 2018.

11. Future Events

The call for abstracts for SSS'19 Bristol, February 19, <https://scsc.uk/e569>, is now closed. An abstract has been received from Nick Hales relates to Data Safety in the context of maintenance [Post meeting note: This abstract as been accepted for SSS'19]. An abstract received from Brian Stevens (DSTL) also includes data safety. DB will also provide a poster on the data safety ontological model.

12. Minutes and actions status

The following action statuses were updated:

- Action 33.5 was closed post-meeting. LH has made the LinkedIn page public, but related Action 33.6 is still ongoing.
- Action 37.7 was closed as DB has provided his updated ontological model.
- Action 37.9 was closed as MP has organised working group leader meetings with TK.
- Actions 39.3, 39.4, 39.5, 39.6, 39.7, and 39.8 were all closed as a standing agenda item has been added to discuss strategy for each new area.
- Action 39.10 was closed as Paul has updated the healthcare trifold and it is uploaded to the web here: https://scsc.uk/file/gd/Working_Group_Trifold_Healthcare_Example_v3-463.docx
- Action 40.5 has been closed.
- Action 40.6 has been closed as MT has emailed an update of the internet searches leading to the Data Safety Guidance, but recommendations have been raised which need to be dealt with in the next meeting. A new action is therefore raised to cover this.
- Action 40.7 has been closed as the map of downloads has been made available by BJ here: <https://clustrmaps.com/site/1a81n>
- Action 40.8 has been closed as MC has provided the 00-970 references to the DSIWG.
- Action 40.11 has been closed as it has been agreed that the reduced day rate for SCSC events can also be made available to retired personnel.

13. AOB

It was agreed that any other influential conferences at which data safety should have a presence should be identified by the group. Members should identify any such conferences, so an action was raised.

It may be possible for future meetings to include WebEx to facilitate wider participation, and this will be decided on a case-by-case basis.

14. Data Safety in News

No news articles were raised involving data safety.

15. Next Meeting

The next meeting date is TBC [Post meeting note: This is now arranged for 28th September 2018 at NATS Brettenham House, London]. An action is raised to organise this.

Future meetings may be held at UKHO, Taunton or Thales, London; DC and GH to investigate. BT also offered at the Rolls-Royce offices in Bristol

16. Thanks

Thanks to Highways England for hosting the meeting.

Thanks to LH for chairing the meeting and taking the minutes.

17. Summary of Open Actions

Ref	Owner	Description	Target Guidance Version
33.6	LH	Add everyone on the DSIWG distribution list to the LinkedIn page.	N/A
36.4	MC	Coordinate the production of training material (based on v3.0).	N/A
37.3	DB	Ensure the model is included in the next version of the document	4.0
37.5	MP	To coordinate with BJ on the close down old docuwiki, remove content, and refer future authors to MP	N/A
39.9	PH	To feed comments back to Paolo on the worked example.	3.1
39.11	MAs	To look at what funding routes may be available from Nuclear Sector for tooling.	N/A
40.1	MP	To get an expert from NATS to brief the WG on the configuration data challenges of cloud.	N/A
40.2	VM	To better define 'Cloud' in the context of data safety and cloud. What level (scope) should this be defined at?	N/A
40.3	All	Specific domain owners to identify experts to brief the DSIWG on their domain so as to identify the hazards and issues	N/A
40.4	PM	To contact RO and/or DB about real world examples of big data applied to data safety.	N/A
40.9	MP	To check with Audrey Canning on access to IEC 61508/update cycle. May be better to have SCSC as a permanent representative on 61508 committee	N/A
40.10	MT	To ask if his Qinetiq course can be released to DSIWG and be presented at SSS'19	N/A
41.1	ALL	Post on LinkedIn about new topics discussed under Data Safety Strategy	N/A
41.2	MP	Email around members asking for any input on the topics discussed under Data Safety Strategy	N/A
41.3	ALL	Review ontological model in own domain and provide review comments for DSIWG Meeting #42	N/A
41.4	TBD	Review Data Safety Guidance and identify where ontological model has highlighted inconsistencies, for discussion at the DSIWG Meetings <i>Note: owner TBD dependent on time available.</i>	4.0
41.5	BT	Find out who updates each of the standards the ontological model is based on and provide information to MP / LH	N/A
41.6	LH	Speak to TK about the possible impact on standards through the SCSC SG, with the view to raise a standing SCSC SG agenda item	N/A
41.7	MP	Think of how to better to broadcast the ontological model within the SCSC and wider	N/A
41.8	MP / BJ	Update Data Safety Guidance PDFs with ligature problems fixed	N/A

Ref	Owner	Description	Target Guidance Version
41.9	JB	Follow up with MT on how change tracking works in Overleaf and whether guidance can be added directly to Overleaf	N/A
41.10	PH	To update the healthcare trifold to include the NHS logo, if approved, and arrange distribution of the trifold at key healthcare events	N/A
41.11	BT	Provide key event dates at which data safety dissemination may be useful / welcomed	N/A
41.12	ALL	DSIWG members to identify any influential conferences in their domain for discussion at DSIWG meeting #42	N/A
41.13	MP	Agree date and location for next DSIWG meeting [Done: 28 th Sep, NATS, London]	N/A

18. References

Ref	Title	Location
[1]	Slides from the meeting	https://scsc.uk/file/gd/41st_DSIWG_MasterSlides-465.pptx
[2]	IoT Healthcare slides	https://scsc.uk/file/564/05---Stuart-Harrison---SCSC-Clinical-Risk-Management-IoT---0.1-1.pdf
[3]	Autonomous Systems Test Coverage presentation	https://scsc.uk/file/gd/York_Presentation_-_Test_Coverage_for_Autonomous_Systems_0.3-466.pptx
[4]	Updated ontological model summary report	https://scsc.uk/file/gd/Proposal_for_a_model_of_data_risk_management_(short_report)_vB.1-462.pdf
[5]	The full report of the ontology modelling	https://scsc.uk/file/gd/Proposal_for_a_model_of_data_risk_management_(full_report)_vB.1-464.pdf