DSIWG

SCSC Data Safety Initiative – WG Meeting 31

11th January 2017, NATS, London

Notes and Actions

Attendees

Rob Ashmore (RA) – DSTL, Paul Hampton (PH) – CGI, Steve Clugston (SC) - TSC, Louise Harney (LH) – PA Consulting (Part), Mike Parsons (MP) – NATS, John Bragg (JEB) – MBDA, Eric Bridgstock (EB) – Raytheon, Mark Templeton (MT) – QinetiQ, Ali Hessami (AH) – Vega (Part).

Apologies

Bob Oates (RO) - Rolls-Royce, Dave Banham (DB) - Rolls-Royce, Nick Hales (NH) – DE&S, Janette Baldwin (JB) - Thales, Andrew Eaton (AE) - CAA, Amira Hamilton (AH) - CGI, Chris Hartgroves (CH) - Leonardo, Julian Lockett (JL) - FNC, Simon Burwood (SB) – ESC, Ashraf El-Shanawany (AES) – CRA Risk Analysis, Shaun Cowles (SC) - EDF Energy, Paolo Giuliani (PG) – EDF Energy, Clive Lee (CL) - Edif ERA, Michael Aspaturian (MAs) – EDF Energy, Robin Cook (RC) – Qinetiq, Sam Robinson (SR) – EDF Energy.

Agenda

1. Guidance Document status report
2. Check of Hardcopy book
3. Book delivery to SSS'17
4. Future publishing routes
5. Review of 2017 plans
6. SSS'17 Preview
7. Future Events
8. Move to LaTeX
9. Formal modelling activity update
10. Standards Update
11. Minutes and actions status
12. AOB, etc.
13. Data Safety in the News.
14. Further work: Falsification of Data, Testing Data

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 status report

The Data Safety Guidance document was published in colour over the Christmas period and is now available for purchase online at Amazon at a cost £10.50. [Post-meeting note: a problem with the appendices meant that the publication was withdrawn for corrections. This is currently being checked. The latest PDF version is in the group resources area [3].]

2. Check of Hardcopy book

Hard copy versions of the guidance document were reviewed and were positively received. The group thanked all those involved in the production of the document in the run up to Christmas.

3. Book delivery to SSS'17

The group discussed when the wider community should be notified that the Data Safety Guidance document has been published. It was agreed that a forward notification should be given but to also state that a free version will be available at SSS'17. [Post-meeting note: MP will announce when again available on Amazon.]

Action 31.1 [MP] Forward announce that the Data Safety Guidance PDF will be available at SSS'17 but also say it is available for hardcopy purchase now.

The availability of the PDF version was also discussed. It was agreed that it would be made available at SSS'17 as a free PDF download [within the publications area of the SCSC website].

Action 31.2 [MP] Make the PDF available as a PDF download at SSS'17.

It was noted that the SSS'17 hotel will not take delivery of the books prior to the conference so RA said he would get them delivered to him and he would drive up with them. RA agreed to order 150 for the conference.

Action 31.3 [RA] Order 200 copies of the Data Safety Guidance and make 150 of these available for the conference on Monday for welcome packs.

4. Future publishing routes

MP and SC noted that there might be other publishing routes such as the BSI. MP also noted that it may be possible to also publish via IEEE although the BSI may be a swifter route than IEEE. The group thought that if it did go down alternative routes they would still want to reserve the right to publish further changes. It was noted that there may be additional cost associated with going down these alternative publishing routes. It was agreed that any cost should be kept low to make it accessible to the practitioners that need it. The group would also want to avoid having to maintain two branched versions, but it should be possible to have a formally published version via a standards body and continue on development of a new version outside the publication body. It was agreed that if any such publishing route was followed, the group would need to be careful about what rights they retained as the authoring organisation and where copyright belongs.

5. Review of 2017 plans

Plans [1] for further development of the guidance for 2017 were discussed.

Rollout and integration

MP thought an important aspect to develop was a Business Benefit Guide.

Action 31.4 [MP] Make a first draft of the Business Benefit Guide.

It was thought that now there is a guidance document, the focus should be more on dissemination to ensure the message is delivered as effectively as possible. It was also suggested that the focus could be more on conferences attended by managers (i.e. decision makers, budget holders) rather than engineers.

Action 31.5 [SC] Try to find out which conferences could be targeted to disseminate the guidance to managers within BEIS (Department for Business, Energy and Industrial Strategy).

SC noted that there may be data protection considerations with gathering data such as publically identifiable data. DPA and general privacy laws could therefore affect the application of the guidance. It was thought that a paragraph should be added to recognise these issues but to reflect them in a positive way as far as possible.

Action 31.6 [RA] Produce a first draft of an assessment of how legislation could impact the Data Safety Guidance.

MP also noted that people (e.g. the Police) may use data for legal purposes. It was agreed that a future meeting could discuss how these wider aspects could be documented and they relate to similar sections such as security, etc.

Improving the Guidance

It was agreed that a Normative/Informative split would be good perhaps as a Part A and Part B (A being the specific requirements and B being the history and guidance implementation) – one of the best examples being the recent Healthcare IT standards (SCCI0129 [4], SCCI0160 [5]).

Action 31.7 [RA] Look at how the guidance could be structured into normative and informative guidance.

It was noted that the Section 7 tables still seem disconnected and haven't really had enough critical review and this should be a key focus for the next version. It was thought that it should be tied up with the formal modelling.

Having more worked examples was also thought to be a good idea e.g. from Defence, Automotive and Aviation.

It was noted that the splitting out of the normative part could become the starting point for a standards approach for publication, hence the language needs to be appropriately worded.

Action 31.8 [MT] Look at applying the guidance to the autonomous aircraft airworthiness example previously used to assess the dataware framework report.

It was agreed that the group should aim for another version (2.1) for SSS'18 being an incremental update.

Action 31.9 [RA] Look at minutes and produce a candidate list for activities for the next version of the document.

Action 31.10 [JEB] Look at how GSN can be added to the guidance to support the data aspects of a safety argument, i.e. give an example data safety argument in GSN.

Engagement

RA suggested that someone with well-established standing in the safety community, e.g. John McDermid (or similar) could be asked to formally write to various regulators (e.g. Aviation, Rail, Nuclear) to ask them to review the guidance.

Action 31.11 [MP] Talk to John McDermid to see if he can help write to regulators to make them aware of the guidance and ask them to review/comment.

It was thought that the automotive and autonomous vehicle groups may be a good area to explore for disseminating the guidance.

Action 31.12 [MP] Talk to Roger Rivett or Ged Lancaster about how to disseminate the guidance into the automotive sector.

Training

Data Safety as part of an academic module was discussed. It was thought that data safety was poorly covered at the moment. It was decided that the group should approach various universities to see if data safety could be included in the academic curriculum in some way (e.g. as a guest lecture session). Possible target universities could be York, Cranfield, Lancaster and University of West England.

Action 31.13 [MP] Talk to Tim Kelly / Mark Nicholson about introducing data safety into an academic module [E.g. on the York MSc. This could involve a member of the DSIWG].

DSIWG

Coordination with other groups that are being set up (e.g. Autonomy and Service Assurance) was thought to be covered as there is some common membership with members of the DSIWG.

There was a discussion as to whether the group should seek participation and/or international collaboration.

Action 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.

Action 31.15 [AH] Raise with IEEE standards about seeking more international participation with the group.

6. SSS'17 Preview

The SSS'17 programme was discussed briefly and it was noted that there are three data safety related papers being presented.

7. Future Events

Other channels for engaging with the community were discussed and it was thought that running seminars/tutorials through the IET would be a useful area to explore.

Action 31.16 [MP] Talk to Graham Jolliffe about organising an IET event (seminar/tutorial).

8. Move to LaTeX

JEB presented slides [2] on the pros and cons of moving from the current wiki based document production approach to LaTeX. The current scheme has some benefits in terms of collaboration and WYSIWYG aspects but has downsides in terms of the post processing and the dependency on plugins.

JEB said MT had trialled the process of moving to LaTeX, which uses a similar style of mark up, and have recreated the guidance in a satisfactory manner. There are some additional benefits with this approach in terms of referencing, indexing and captioning.

LaTeX presents a more streamlined way of production that is less error prone as 'production ready' output comes straight out of LaTeX. LaTeX is not a content management environment so the group would still need to have a way of collaborating on the content. Some special tooling is required to be able to edit the document in LaTeX form.

Action 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].

The group agreed that this would be the mechanism for generating the next version of the document.

A question was raised about how well the document could transfer to other standards groups, e.g. could it be converted to Word as there are standard templates for some of the groups? It was thought that as long as the document was produced as PDF it could be imported to other formats.

The legality and liability aspects were discussed and the question arose as to whether the group itself or its members could be exposed to litigation if someone claimed that following the guidance had contributed to an accident.

Action 31.18 [MP] Ensure legal and liability of the group's work is given due consideration in future meetings (disclaimers etc.), including production of WG terms of reference.

Technical Content

SC discussed the issues around sampling rates for vehicle signal logging and how the data could be used in accident investigation. Some sampling rates could potentially cause data to misrepresent the actual real signal profiles.

Action 31.19 [SC] Write some text about sampling rate issues and consider where in the guidance this could be included.

The group discussed whether ALARP [as it might apply to data-based mitigations] should be explicitly documented in the guidance. There is mention that post mitigation risk should be assessed to see if it is acceptable but doesn't discuss what acceptable [for data] actually means. It was agreed that this would stray more into core safety engineering, which is not the main purpose of the document. It was noted however that there is some reference to 'as low as reasonably practicable' in the document (but not the acronym ALARP).

Action 31.20 [MP] Consider how best to resolve the issue of ALARP in the context of data.

9. Formal modelling activity update

No specific update.

10. Standards Update

No specific update.

11. Minutes and actions status

The last minutes and actions were agreed.

Action 26.4 No update.

Action 27.1 MP has emailed twice with no response. Superseded by further actions 31.13 and 31.17. **Action Closed.**

Action 28.5 No update.

Action 28.10 MP asked – no response. **Action Closed.** Superseded by further action (see 27.1 above).

Action 29.2 No update.

Action 29.9 No update.

Action 30.1 **Action Complete.**

Action 30.2 **Action Complete.**

Action 30.3 **Action Complete.**

Action 30.4 AH said he could get funding from the IEEE for training material for example computer based training perhaps even leading to some form of certification. This normally takes the

form of giving the document to a 3rd party suitably competent to generate computer based training material for free distribution via IEEE. The group could retain the IPR and even act as approver of any future training providers.

Action 30.5 **Action Complete.**

Action 30.6 **Action Complete.**

Action 30.7 **Action Complete.**

Action 30.8 **Action Complete.**

Action 30.9 **Action Complete.**

Action 30.10 **Action Complete.**

Action 30.11 Action Ongoing.

Action 30.12 Action Ongoing.

Action 30.13 Action Ongoing.

Action 30.14 No Update.

Action 30.15 Action superseded by new action 31.17 raised in this meeting.

Action 30.16 Action ongoing. LH said she needs a logo. Action wording amended to add notification to DSIWG members when complete.

12. AOB, etc.

None.

13. Data Safety in the News

Ambulance response times were delayed over the New Year in London after technical problems hit the ambulance control room systems [6]. It is understood the computer system crashed, so calls had to be recorded by pen and paper for nearly five hours on one of the busiest nights of the year. There may well be data aspects to this failure, possibly related to the leap-second added at midnight.

14. Further work: Falsification of Data, Testing Data

MP reiterated that he was keen to have data falsification covered as this is a known issue in sectors such as Healthcare and Marine sectors where people try to cover their tracks after incidents/accidents. Test data is also a big area that needs more guidance.

Action 31.21 [MP] Write some text on Falsification and submit this for review within the group.

15. Next Meeting

DSIWG #32, Raytheon, Harlow, Thursday 16th March 2017 11:00-17:00.

DSIWG #33, MBDA, Bristol, Tuesday 25th April 2017 11:00-17:00.

16. Thanks

Thanks to PH for taking the notes and actions.

17. Summary of Open Actions

Ref	Owner	Description	Target Guidance Version
26.4	TK	Provide some initial suggestions on how to better organise the concepts in the current model.	2.1
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
30.11	RO	Collate a list of activities to be considered for the Data Safety Guidance in 2017.	N/A
30.12	MAs	Consider how the group could be involved in applying for funding in the future.	N/A
30.13	PH	Update the data safety guidance for healthcare to reflect version 2.0 updates and send to NHS Digital for publication.	N/A
30.14	RO	Include PH's observations on applying the guidance as part of the wider list of things to consider for next year.	N/A
30.16	LH	Create a data safety page on LinkedIn and invite DSIWG members when it is set up.	N/A
31.1	MP	Forward announce that the Data Safety Guidance PDF will be available at SSS'17 but also say it is available for purchase now.	N/A
31.2	MP	Make the PDF available as a digital download at SSS'17.	N/A
31.3	RA	Order 200 copies of the Data Safety Guidance and make 150 these available for the conference on Monday for welcome packs.	N/A
31.4	MP	Make a first draft of the Business Benefit Guide.	N/A
31.5	SC	Try to find out which conferences could be targeted to disseminate the guidance to managers within BEIS.	N/A
31.6	RA	Produce a first draft of an assessment of how legislation could impact the Data Safety Guidance.	N/A
31.7	RA	Look at how the guidance could be structured into normative and informative guidance.	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
31.9	RA	Look at minutes and produce a candidate list for activities for the next version of the document.	2.1
31.10	JEB	Look at how GSN can be added to the guidance to support the data aspects of a safety argument.	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 Roger Rivett or Jed Lancaster about how to disseminate the guidance into the automotive sector.	N/A

Ref	Owner	Description	Target Guidance Version
31.13	MP	Talk to Tim Kelly / Mark Nicholson about introducing data safety into an academic module [E.g. on the York MSc. This could involve a member of the DSIWG].	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
31.16	MP	Talk to Graham Jolliffe about organising an IET event (seminar/tutorial).	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 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
31.20	MP	Consider how best to resolve the issue of ALARP in the context of data	2.1
31.21	MP	Write some text on Falsification and submit this for review within the group.	2.1

References

[1] Plans for 2017 http://scsc.org.uk/file/gd/31st%20DSIWG%20MP%20Slides-231.pptx

[2] Move to LaTeX http://scsc.org.uk/file/gd/31st%20DSIWG%20LaTeX%20Slides-233.pdf

[3] Latest PDF of the Guidance Document http://scsc.org.uk/file/gd/SCSC-127B%20Data%20Safety%20Guidance%20-%20Version%202_0%20(Corrected%20Appendices)-230.pdf

[4] Clinical Risk Management: its Application in the Manufacture of Health IT Systems http://content.digital.nhs.uk/media/20984/0129392012spec/pdf/0129392012spec.pdf

[5] Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems http://content.digital.nhs.uk/media/20988/0160382012spec/pdf/0160382012spec.pdf

[6] London Ambulance Systems Failure http://www.bbc.co.uk/news/uk-38482746