DSIWG

SCSC Data Safety Initiative – WG Meeting 43

21st November 2018, Thales, London

Minutes and Actions

Attendees

Wayne McNeill (WM) - NATS, Paul McKernan (PM) – DSTL, Dave Banham (DB) - Rolls–Royce PLC, Louise Harney (LH) – Leonardo, Mike Parsons (MP) – NATS, Gordon Hurwitz (GH) – Thales, Martin Atkins (MCA) – Mission Critical Applications, Divya Atkins (DA) - Mission Critical Applications, Paul Hampton (PH) – CGI, Peter Smith (PS) – Highways England, Jenny Brain (JB) - Wood.

Apologies

Nick Hales (NH) – Consultant, Ali Hessami (AH) – Vega, Mike Ainsworth (MA) – Ricardo, Paul Mukherjee (PM) – Astellas, Amira Kawar (AK) – CGI, Duncan Dowling (DD) – DARD, Phil Wright (PW) – DSTL, Fan Ye (FY) – ESC, Chris Hartgroves (CH) – Leonardo, Shaun Cowles (SC) – EDF, Paul Dart (PD) – NCC Group, Maria Kelly (MK) – Leonardo, Andrew Eaton (AE) – CAA, John Bragg (JEB) – MBDA, Martyn Clarke (MC) – Consultant, Paolo Giuliani (PG) – EDF Energy, Rob Ashmore (RA) – Dstl, Sam Robinson (SR) – EDF Energy, Ged Lancaster (GL) – JaguarLandRover, Janette Baldwin (JB) – Thales, Nick Holmes-Mackie (NHM) – RINA, Alastair Faulkner (AF) – Abbeymeade, Marinos Panayiotou (MaP) - CRARisk

Agenda

1. Presentation: Data Risks in Cloud Systems (WM)
2. Presentation: Command & Control Links in Remotely Piloted Aircraft over Satcomms: Standards Developments (PH)
3. Continuation of the planning / strategy (for V4 content), assessing the data risks in: IoT and OT/IT Convergence; Cryptography; Big Data; Cloud Computing; Cyber Physical Systems; Machine Learning and Autonomy; Wireless Communications; Multicore; FPGA
4. Training Course Development Update
5. SSS'19 Update
6. Overleaf Status
7. Move to Amazon/KDP and Sales/Downloads Update
8. Formal Modelling Activity Update
9. Tooling / LRF Update
10. Dissemination Update
11. Standards Update
12. Future Events
13. Minutes and Actions
14. AOB, etc.
15. Data Safety in the News

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. Presentation: Data Risks in Cloud Systems (WM)

WM presented slides on data risks in cloud systems. This introduced the concepts of Cloud services, the different types of services, and illustrated some case studies where problems have given rise to catastrophic impact with the cloud provision. It was noted that an Air Traffic Services Provider is aiming to move systems to a Cloud based infrastructure but were intending to build their own private cloud as they could not build a sufficient assurance argument for the use of public cloud services [1].

2. Presentation: Command & Control Links in Remotely Piloted Aircraft over Satcomms: Standards Developments (PH)

PH presented initial findings on the RTCA standards development on command and control safety and performance requirements for unmanned aerial vehicles [2].

3. Continuation of the planning / strategy (for V4 content), assessing the data risks in:

- IoT and OT/IT Convergence
- Cryptography
- Big Data
- Cloud Computing
- Cyber Physical Systems
- Machine Learning and Autonomy
- Wireless Communications
- Multicore
- FPGA

It was noted that although there is an ambition to include all these topics in the Data Safety Guidance v4 for 2020 publication timeframe, there is a lead time for developing print ready material and so it was agreed that the primary focus should be on: (i) Cloud, (ii) IoT, and (iii) Machine Learning and Autonomy.

It was thought that even if recommended tools and techniques in these new areas are not fully elaborated, there would still be value in raising awareness of the data contribution for each of these topics; especially if supported by 'war stories' highlighting real world cases where data has contributed to an accident.

Action [DB] 43.1 Ask John Fitzgerald at Newcastle University if he would be interested in contributing to the guidance on Cyber Physical Systems from a data perspective.

Action [DA] 43.2 Ask John Clarke at Sheffield University if he would like to contribute to the guidance material developed on Machine Learning.

Action [GH] 43.3 Speak to Stephen Boyle & James Weston on Cyber security aspects of IT/OT to see if they could contribute.

DB asked whether we should provide additional analysis techniques for data over and above the Hazop guidance already in the document.

Action [MP] 43.4 Write up a data-focussed FMEA approach.

4. Training Course Development Update

No updates.

5. SSS'19 Update

MP presented the programme for the symposium in Feb 2019 https://scsc.uk/e569 , which features (i) a 30 minute report on the activities of the DSIWG (ii) a paper using data techniques to analyse the Uberlingen accident by NH and (iii) a poster on the ontology model presented by DB.

6. Overleaf Status

No updates.

7. Move to Amazon/KDP and Sales/Downloads Update

MP presented sales figures from the guidance publication and noted that the publishing platform has been migrated from Amazon CreateSpace to Kindle Direct Publishing. MP said there have been some issues with getting historical sales information, but a new set of (beta) tools look promising.

8. Formal Modelling Activity Update

There is a now a Draft B model and DB is looking for a basic sanity check of the model. Once this is done DB can look at writing formal definitions, for example, defining terms such as "Undesirable Situation" in a way that references are consistent with other defined terms.

[Note: terms which require formal definitions, or which we need to check the consistency of their use within the guidance, need to be updated within the Data Safety Guidance as well.]

It was thought that the Data Safety Guidance v4 version could incorporate the data model in some capacity and have links to other resources such as the actual detailed model. It was agreed that a separate dedicated workshop would help facilitate a review of the model.

Action [DB] 43.5 Set up a Webex meeting to specifically discuss the data model in January 2019.

9. Tooling / LRF Update

DA and MA presented progress on the tooling for implementing the guidance. DA said there have been several attempts to get funding. The most promising was the Lloyds Register Foundation but they have said that they would like to see customer engagement before investing. DA also spoke to NHS Digital and they are supportive so this might be the catalyst to getting Lloyds Register funding. DA/MA have prepared a 'Collaborator Business Case' [4] and presented the content of this in the meeting.

[Post-meeting note: see email from EDF [9] on possible funding opportunities]

LH recommended adding the list of standards and guidance that have been influenced by data safety but it was thought this might be counterproductive as it might give the impression that users could wait for the standards to be updated before taking any action.

[Note: The purpose of adding standards to the outline business case is to provide businesses with a reason to invest. LH made the point that the basis of a business case for her organisation would be that the work is either essential to fufil a duty of care or that it is required by a standard which is part of the contract (already the case, via the Defence Standards, for example). So rather than just standards 'influenced by' data safety, it is standards which require or recommend a data safety assessment already.]

PM suggested that an alternative selling point might be to say the data guidance could be used as demonstrating compliance (in a similar way to a guidance document such as DO-178C).

MP suggested the document uses Tim Kelly's concepts of Conformance, Risk and Confidence [5].

Areas raised in the meeting for consideration were:

- tool qualification as the tool may need to be subject to some form of verification, if, for example used in aviation project where DO-178C and DO-330 would be applicable;
- providing an ability to export data to say Microsoft Excel.

MA then demonstrated an early prototype of the tool.

Action [DA/MA] 43.6 Send the request for support document to MP for publication and general review by the group.

10. Dissemination Update

No update.

11. Standards Update

MP said that Phil Williams of the SCSC Steering Group is now in the IEC 61508 UK representation committee and he is willing to promote data safety in the group [10]. MP has forwarded thoughts on how IEC 61508 could be changed to reflect data safety based on work originally done by Dale Callicott [6]. DB said he had a first draft of his survey of IEC61508 Ed2 for references to "Data" and this is now on the WG resources area [11].

12. Future Events

MP noted a few future SCSC events that could have data content:
(https://scsc.uk/diary.html?opt=SCSC)

- Seminar: COTS, Legacy and Reuse on 6th Dec 2018;
- Seminar: Evolution of Assurance Case Practice on 4th April 2019;
- Seminar: Learning from Accident Investigations on 13th June 2019.

MP suggested we should have a dedicated seminar based on v4 of data safety guidance in April 2020.

JB provided an update of the human factors seminar that took place in Barrow: Operating beyond the edge: Safety critical systems and human factors 29th October 2018.

LH attended the High Integrity Software 2018 conference on 6th November 2018.

MP presented an initial version of a matrix linking data properties to data types but said further work is required [7].

13. Minutes and Actions

The following actions were closed:

39.9: PH provide comments to PG.
40.1 MP got WM from NATS who presented at the meeting
40.2 WM presented this in the meeting
40.3: this will become specific actions on individuals drafting sections.
40.4: Big Data not a topic that will be a focus for the guidance now
40.9: there is now representation on the IEC 61508 committee.
41.1
41.2: superseded by actions on individuals to write specific sections

Action [DA/MA] 43.7 Review the Data Safety Guidance and the ontological model against the tool to identify inconsistencies.

41.5: BT has notified MP/LH on who updates the standards.
41.6: LH spoke to TK.
41.7
41.13
42.1: superseded by new actions.
42.2
42.3
42.8
42.10

Changes were made to the following actions:
41.8 the action owner was changed to JEB/BJ
41.10: changed action to make the trifold colour consistent with the NHS Logo

14. AOB, etc.

None.

15. Data Safety in the News

MP presented the recent data related Flybe incident where an autopilot had been incorrectly configured [8] to take the aircraft to a height of 0ft, resulting in a sudden drop.

DB noted that 'Checklist' should be added to the v4 guidance as a result of the Flybe incident. MP sent MT an email during meeting to inform him that this needs to be included.

16. Next Meeting

The next meeting date is planned for January 2019 as a Webex and then a face to face will be held in Feb 2019 location TBD.

17. Thanks

Thanks to PH for taking the minutes.
Thanks to MP for chairing the meeting.
Thanks to GH and Thales for hosting.

18. Summary of Open Actions

Ref	Owner	Description	Target Guidance Version
33.6	LH	Add everyone on the DSIWG distribution list to the LinkedIn page and create a Wikipedia 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
40.10	MT	To ask if his Qinetiq course can be released to DSIWG and be presented at SSS'19	N/A
41.3	ALL	Review ontological model in own domain and provide review comments for DSIWG Meeting #44	N/A
41.4	ALL	Review Data Safety Guidance and identify where ontological model has highlighted inconsistencies, for discussion at the DSIWG Meetings	4.0
41.7	MP	Think of how to better to broadcast the ontological model within the SCSC and wider	N/A
41.8	JEB/BJ	Update Data Safety Guidance PDFs with ligature problems fixed	N/A
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 colour, 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	N/A
42.4	LH	Get an update from RO on cyber-data properties mapping, which has been published.	N/A
42.5	MT	Make a PDF of the guidance document version 3.0.1 available for SSS'19 to support reporting of progress	N/A
42.6	PH	Define the process to publish a document developed in Overleaf via Amazon	N/A
42.7	MP	Ask John Spriggs to write a template data safety argument for the next guidance update	N/A
42.9	MP	Work out a matrix of data categories (previously 'types') and data properties (as per DB discussion)	N/A
42.11	MP	Ask BJ how to ensure a search for the correct key words such as data safety finds the material created by the DSIWG on the first page of search results.	N/A
43.1	DB	Ask John Fitzgerald at the Newcastle University if he would be interested in contributing to the guidance on Cyber Physical Systems from a data perspective.	4.0
43.2	DA	Ask John Clarke (Sheffield University) if he would like to contribute to the guidance on Machine Learning.	4.0
43.3	GH	Speak to Stephen Boyle & James Weston on Cyber security aspects of IT/OT to see if they could contribute.	4.0
43.4	MP	Write up a data focussed FMEA approach.	4.0
43.5	DB	Set up a webex meeting to specifically discuss the data model in January 2019.	N/A
43.6	DA/MA	Send the request for support document to MP for publication and general review by the group.	N/A
43.7	DA/MA	Review the Data Safety Guidance and the ontological model against the tool to identify inconsistencies.	N/A

19.References

Ref	Title	Location
[1]	Data Risks in Cloud Systems	https://scsc.uk/file/gd/WM_Cloud_and_Data_Presentation_(1)-508.pptx
[2]	Developments in RPAS C2 standardisation	https://scsc.uk/file/gd/RPAS-510.pptx
[3]	Proposal for a model of data risk management	https://scsc.uk/file/gd/Proposal_for_a_model_of_data_risk_management_(full_report)_vB.1-464.pdf
[4]	Request to Support: Data Safety Tool Collaborator Business Case	https://scsc.uk/file/gd/20181126_Collaborator_Business_Case-509.pdf
[5]	Tim Kelly Conformance, Risk and Confidence presentation	https://scsc.uk/file/404/Kelly---Risk-Confidence-Compliance-Arguments.pdf
[6]	Updating IEC 61508 for data safety aspects	https://scsc.uk/file/gd/Note_from_DC-502.txt
[7]	Data properties versus data type matrix table	https://scsc.uk/file/gd/Matrix_v1-501.docx
[8]	Plane drops 500ft in 18 seconds after error	https://www.bbc.co.uk/news/uk-46137445
[9]	Note from MA, EDF	https://scsc.uk/file/gd/Note_from_MA-503.txt
[10]	Note from PW on IEC 61508 representation	https://scsc.uk/file/gd/Note_from_PW-504.txt
[11]	First draft of DB survey of IEC61508 Ed2 for references to “Data”	https://scsc.uk/file/gd/IEC%2061508%20and%20data%20safety-47.doc