SCSC FOR EVERYONE WORKING IN SYSTEM SAFETY

DSIWG

SCSC Data Safety Initiative – WG Meeting 39

3rd April 2018, CGI, London

Minutes and Actions

Attendees

Martin Atkins (MaA) – Mission Critical Applications, Divya Atkins (DA) - Mission Critical Applications, Michael Aspaturian (MAs) – EDF Energy, Paul McKernan (PM) – DSTL, Mike Parsons (MP) – NATS, Vincent Martin (VM) – Raytheon, Robert Oates (RO) - Rolls Royce PLC, Paul Hampton (PH) – CGI, Nick Hales (NH) – DE&S, Mark Templeton (MT) - QinetiQ

Apologies

Bill Blackburn (BB) – Process Renewal Group, Ebby Joseph (EJ) – RINA, Dave Banham (DB) Rolls–Royce PLC, Eric Bridgstock (EB) - Raytheon, Robin Cook (RC) - Thales, Rob Ashmore (RA) – DSTL, John Bragg (JEB) – MBDA, Louise Harney (LH) – Leonardo, Mike Ainsworth (MA) – Ricardo, Phil Wright (PW) – DSTL, Fan Ye (FY) – ESC, Julian Lockett (JL) – Frazer Nash, Paolo Guiliani (PG) – EDF, Janette Baldwin (JB) – Thales, Chris Hartgroves (CH) – Leonardo, Shaun Cowles (SC) - EDF.

Agenda

1. Comments / reception of new version of guidance document
2. Data Strategy Session
3. Paolo’s Example
4. New trifold
5. Sales/Downloads Update
6. Dissemination update
7. Future Events
8. Minutes and actions status
9. AOB, etc.
10. Data Safety in the News
11. 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. Comments / reception of new version of guidance document

MP discussed reception of the guidance at SSS'18, and reported the comments from the evaluation forms:
"Excellent publications with the latest version of the data safety guidance a nice surprise addition."
"Excellent way to present the material in a take away format for future reference"
"The DSIWG guidance is leading the field in supporting data safety and is an invaluable support to those working in the field."
"…they are well manufactured and definitely good to have and will be referred to in the future."
"Not sure yet if the DSG book is of relevance to me."
"Data book is becoming a go to guide for many of us."
"The DSIWG material is too complex. Book is well presented, but the material is not really usable."
"I will certainly read Data Safety Data safety guidance is a great document, focused on application, clear to understand and able to refer clients to it."

He also showed the DSIWG Data Safety slide [1] that was presented as a progress update at the symposium.

RO noted that he had shared it on Yammer and there was a lot of positive feedback.

MT said he had given an internal trial of a training course on the guidance (which was being used to develop a more formal course for the MOD). MP showed the feedback from development and running of the course [2] with the following few key points emerging:

- it wasn't obvious quite how the tables work based on 'pattern matching' of the 3 different fields;
- The audience felt they needed more of a process diagram to explain its use;
- It was concluded that a 4-hour session is a minimum to cover the whole guidance;
- Some confusion arose with the use of the *lowest* likelihood to determine the overall risk likelihood.

It was discussed how comments on the guidance should be managed e.g. as a formally controlled review records that need to be considered and responses recorded and agreed. It was thought that the group doesn't need an overly rigorous process as it is not a formal standards body.

MP thought that we could issue a 3.1 or a 3.0.1 that corrects minor issues, but RO thought that might harm uptake of 3.0. The group thought that associated guidance or FAQs could be published to help support its use.

Action 39.1 [MT] Look at what overleaf can do in terms of version control
Action 39.2 [MP] Collate and be the custodian of all comments received on the guidance.

MP showed LH's email [3] covering her ideas and suggestions for the future of the guidance.

2. Data Strategy Session

A number of specific areas were discussed. It was thought that these areas could be covered as supplements rather than trying to incorporate into the main guidance as these are specialised areas and are relatively new and fast-moving.

Internet of Things and Operational Technology/ IT Convergence/Cyber Physical Systems (a)
Noted that OT is where factories are adopting office-like technology automation.

It was noted that Cyber Physical systems are software centric not necessarily internet connected.

For IOT it is the scale that is the issue – there are large numbers of devices that can generate data. RO said he has done a demo on a remotely controlled vessel using IoT devices.

RO noted concern that people bolt systems together using things like Stringify. RO gave an example of a connected home that allows Amazon Alexa service to send a command to Hive to switch a light on. Stringify is a similar technology and there could be many people now doing ad-hoc integrations like this.

RO said that in November this year there will be aviation guidance on embedding cyber security. These are being produced by EUROCAE as ED-201 through to ED-205 but these have missed operational monitoring aspects and this might be an area that the group could focus on.

MP showed the flyer for the SCSC IOT Safety seminar in June 2018: https://scsc.uk/e560 .

Areas to consider:

- Scale – volume of devices
- Stakeholders and Data Ownership
- Transformative Services
- Variation in standard/technologies
- Simplicity of devices/safety has to be managed externally
- RFID tags

Cryptography (b)
Typical hazards were noted as:

- accidental locking out
- consumption of bandwidth
- loss of IFF systems broadcast
- unique data – use once numbers
- inappropriate randomisation sources (entropy)
- more vulnerable to corruption
- inadvertent disclosure

Big Data (c)
MP noted that there may possibly be funding in this area if we can link in with the Turing Institute who cover data analytics and data science.

- Data provenance
- Scale is too immense for humans to check
- When used as reference data prone to selectivity, bias etc.
- Non-structured format can make it difficult to check
- Lack of provenance, context, demographic, reapplication issues.

RO said one of the Rolls-Royce data analytics experts is going to look at the guidance.

Cloud Computing/Service Agreements/Distributed Infrastructure (d)

- Service provision may not have safety SLAs
- Lack of validation of activities/unknown geographic distribution/processing
- Shared tenancies/inadvertent sharing/cross contamination/data leakage
- Jurisdictional conflicts/constraints/inheritance of legislative jurisdiction

Autonomy (e)

- Blindspots where there is no data for some areas
- Geo positioning/ Geofencing
- Conflicting Data
- Repositioning of autonomous systems in new/unexpected contexts
- Data configured failsafe e.g. whether it's safe to conduct an emergency stop or drop anchor in maritime.
- Lack of human in the loop to prevent unsafe conditions
- Distribution/aggregation of different learnt behaviour

NH noted that Mark Douthwaite and Tim Kelly had published a paper in this area. Reference email from Nick Hales of 14th March 'Data Safety Initiative Woking Group' Safety-Critical Software and Safety-Critical Artificial Intelligence: Integrating New Practices and New Safety Concerns for AI systems (Mark Douthwaite, Tim Kelly). JC has issued a response. References [4][7][8].

It was noted that in the military it was thought that there would always be a man in the loop or at least *on* the loop so the human can intervene. However, some autonomy may be required for example, to take an evasive action where the human would not have enough time to react otherwise.

It was noted in general that it may not be that practicable for a human to intervene in a timely manner e.g. to intervene prior to a car about to collide with an object.

Machine Learning / Self-Learning & AI (e)

RO presented a paper (Machine Learning Safety and Assurance) discussing hazards associated with training data:

- Training data insufficient types of data
- Sample is too small
- Errors treated equally - coverage of the safety cases
- Undertrained (not familiar with all scenarios)
- Over trained (only able to work on training data)
- Reward Hacking (biasing/unintended optimisation)
- Certainty of decision (probability based decisions doesn't mean certainty)
- Training based on synthetic data (simulator)
- Survivorship (loss of data during accidents)
- Paradigm shift in the balance of configuration/software (traditional projects software centric, ML is configuration centric)
- Lack of determinism (training algorithms may use random data)
- Geographies

MP thought that the DSIWG should be well positioned to provide guidance on how to generate training data for safety applications, initially as guidelines, although there was some concern that this might demand the acquisition of specialist knowledge.

RO showed the video on Rolls-Royce on the use of intelligent data to improve maritime safety.

Wireless Communications (f)
This relates to use of wireless comms for redundancy and energy harvesting technology.

- Jamming
- Frequency sharing issues
- Environmental issues
- Low power/drop outs
- Interference

Blockchain (g)

- Decentralisation/Consistency
- Trust through consensus
- Delays/latency in distribution
- Scalability – the ledgers can be gigabytes
- Immutability (undeletability) of the ledger when undesirable data is capture

It was agreed that these bullets should be used as the basis for supplementary guidance (potentially only a few pages). The initial aim is to get a list of identified issues as they relate to data, e.g. documented in three columns: **Hazards**, **Causes** and **Mitigations** in a simple table format. Then use this to progress into a subsequent positioning paper.

Action 39.3 [MP] Act as champion for production of IOT (a) positioning table.

Action 39.4 [DA] Act as champion for production of Cryptography (b) positioning table.

Action 39.5 [PM/RO] Act as champion for production of Big Data (c) positioning table.

Action 39.6 [VM] Act as champion for production of Cloud (d) positioning table.

Action 39.7 [RO/NH] Act as champion for production of Autonomy and ML (e) positioning table.

Action 39.8 [MA] Act as champion for production of Blockchain (g) positioning table.

The group agreed to leave the Wireless topic for time being.

3. Paolo’s Example

PH explained the worked example that PG produced [6] in the nuclear domain relating to assessment of data risk associated with modelling pressures in fuel pins. He said it was a good in its own right and a well written example but did not go as far as indexing into the methods and techniques tables.

Action 39.9 [PH] To feed comments back to PG on the worked example.

[MAs had distributed a case study of a nuclear incident “Control System Network Error Causes Reactor Trip” before the meeting which has a strong data element to it [13].]

4. New trifold

PH showed the Healthcare specific tri-fold that he has developed. RO said that the front page should be more focussed on data safety and content of the tri-fold rather than the SCSC.

Action 39.10 [PH] Rework the Trifold to change front page so it focuses more on data safety rather than SCSC.

PH also noted that he and Sean White (NHS Digital) are writing an article for the SCSC Newsletter to raise awareness of the healthcare specific guidance produced to support. He also said he has been invited to submit a paper for DICOH'18 to discuss this healthcare guidance.

5. Sales/Downloads Update

MP noted that there have been 186 sales on the v3.0 of DSG hard copy via Amazon, and 165 downloads of the PDF from the SCSC website to date.

6. Dissemination update

MP reported on a meeting with Lloyds Register Foundation who expressed interest in the Data Safety Guidance and especially the accidents/war stories sections. He said they do fund some work if the group can tag the work with one of their niche areas and funding could be substantial. They suggested the Turing Institute as a possibility for interest / collaboration but they may be more academic than industry focussed.

DA said she had been in touch with several companies including Lloyds Register Foundation to pursue funding for the data safety tool but they have declined. DA also asked the group to consider what they would like to get out of the tool i.e. what functionality would add the greatest value to managing data safety risk.

MA said there is a route through the Nuclear Sector area where they can sponsor a company applying for innovation funding.

Action 39.11 [MA] To look at what funding routes may be available from Nuclear Sector for tooling.

7. Future Events

MP showed the SCSC events list https://scsc.uk/diary.html?opt=SCSC including SSS’19 and the Safety and Security Integration in April.

[Note: abstracts on a data theme (either presentation or poster) are welcome for SSS’19, see the call for abstracts: https://scsc.uk/e569]

8. Minutes and actions status

The following actions were closed: 36.3, 37.6, 37.8, 37.12, 37.15, 38.1, 38.2, 38.3, 38.5 and 38.6.
RA’s action 37.2 was reassigned to PM.
EB’s action 37.10 was reassigned to VM. [Now closed, see 12]

9. AOB, etc.

None.

10.Data Safety in the News

- Uber fatality [9]

- Boeing lost their manufacturing site because of ransomware [10]
- Sewage plant lost control during to a generic crypto-mining [11]

11. Next Meeting

Friday 1st June 2018 at NATS, Brettenham House, London, 11:00-17:00.

12. Thanks

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

13. Summary of Open Actions

Ref	Owner	Description	Target Guidance Version
32.6	DeB	Generate a database of historical incidents and accidents where data is considered to have been a contributory factor.	3.0
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
36.4	MC	Coordinate the production of training material (based on v3.0).	N/A
37.2	PM	Add comments/open issues to the document as a section after the v3.0 version of the document is published. [Closed by 39.1 and 39.2].	3.1
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
37.7	DB	Produce a baseline model for review including any outstanding issues.	N/A
37.9	MP	Speak to Tim Kelly to coordinate working group leader meetings to ensure there is no overlap	N/A
37.10	EB	Distribute draft DEF STAN 00-051 to the group if possible for information [Now closed, see reference [12] below]	N/A
37.13	MP	Prompt MT, SC, MaM, on actions 31.8, 31.19, 33.7	N/A
37.14	MP	Update all SCSC website links for the new version of the document	N/A
38.4	DC	Review IEC61508 and investigate where a link to the management of data safety could be best introduced into the standard	N/A
39.1	MT	Look at what overleaf can do in terms of version control and comments tracking	N/A
39.2	MP	Collate and be the custodian of all comments received on the guidance.	3.1
39.3	MP	Act as champion for production of IOT (a) positioning table	3.1
39.4	DA	Act as champion for production of Crytography (b) positioning table.	3.1
39.5	PM/RO	Act as champion for production of Big Data (c) positioning table.	3.1
39.6	VM	Act as champion for production of Cloud (d) positioning table.	3.1
39.7	RO/NH	Act as champion for production of Autonomy and ML (e) positioning table.	3.1
39.8	MA	Act as champion for production of Blockchain (g) positioning table.	3.1
39.9	PH	To feed comments back to Paolo on the worked example.	3.1
39.10	PH	Rework the Trifold to change front page so it focuses more on data safety rather than SCSC.	N/A
39.11	MAs	To look at what funding routes may be available from Nuclear Sector for tooling.	N/A

14. References

Ref	Title	Location
[1]	DSIWG Data Safety slide from SSS'18	https://scsc.uk/file/gd/DSIWG_slide-413.pptm

[2]	Mark Templeton's comments as a result of feedback	https://scsc.uk/file/gd/Mark_Templeton_Inputs-411.txt
[3]	Louise Harney's email	https://scsc.uk/file/gd/Louise_Harney_Inputs-410.txt
[4]	Safety-Critical Software and Safety-Critical Artificial Intelligence: Integrating New Practices and New Safety Concerns for AI systems (Mark Douthwaite, Tim Kelly)	http://scsc.uk/r140%2f6 http://scsc.uk/res?res=e503/6 http://scsc.uk/rv503.7
[5]	Meeting #39 Slides	https://scsc.uk/file/gd/39th_DSIWG_MP_Slides-409.pptx
[6]	Nuclear worked Example	https://scsc.uk/file/gd/DSIWorkedExample_v4_(3)-412.doc
[7]	Email from Nick Hales	https://scsc.uk/file/gd/Nick_Hales_Email-415.txt
[8]	Email from John Carter responding to [7]	https://scsc.uk/file/gd/John_Carter_Email-414.txt
[9]	Uber fatality	https://www.theguardian.com/technology/2018/mar/22/self-driving-car-uber-death-woman-failure-fatal-crash-arizona
[10]	Boeing hit by WannaCry	https://www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/
[11]	Generic Crypto-mining	https://www.theregister.co.uk/2018/02/11/browsealoud_compromised_coinhive/
[12]	DEF STAN 00-151: Environmental Management Requirements for Defence Systems [Action 37.10]	https://scsc.uk/file/gd/DRAFT_DEF_STAN_00-051_Part_1_Issue_1-416.pdf https://scsc.uk/file/gd/DRAFT_DEF_STAN_00-051_Part_2_Issue_1-417.pdf https://scsc.uk/file/gd/DRN_Def_Stan_00-51_Draft_Issue_1_Raytheon_UK-418.doc
[13]	Control System Network Error Causes Reactor Trip	https://scsc.uk/file/gd/EB-18-COR-014_Control_System_Network_Error-419.pdf
-	Mike's photos from the meeting location	https://500px.com/photo/252215335/walkie-talkie-view-1-by-mike-parsons?ctx_page=1&from=user&user_id=7332433 https://500px.com/photo/252293083/view-from-the-walkie-talkie-building-3-by-mike-parsons?ctx_page=1&from=user&user_id=7332433