DSIWG

SCSC Data Safety Initiative – WG Meeting 72

10th November 2022, Zoom

Minutes

Attendees

Rhiannon Chilton (RC) – Dstl, Oscar Slotosch (OS) – Validas, Mike Parsons (MP) – AAIP, Nick Hales (NH) – Consultant, Martin Atkins (MA) – MCA, Jennifer Kracht (JK) – TomTom, Roland Rosier (RR) - TomTom, Bob Oates (RO) – Blackberry, Paul McKernan (PMcK) – Consultant, Lina Travushkina (LT) – TomTom, Carl Tipton (CT) – JM, Paul Butcher (PB) - AdaCore

Apologies

Divya Atkins (DA) – MCA, Richard Garrett (RG) – SQEP, Dave Banham (DB) – Blackberry, Michael Green (MG) – Ecomergy, Andy Williams (AW) – Consultant, Paul Hampton (PH) – CGI, Mike Standish (MS) – Dstl, Mark Templeton (MT) - Qinetiq

Agenda

1. Welcome
2. Data Safety & Dashboards – Jennifer
3. Fuzz Testing - Paul
4. Standards to use as template - Carl
5. New Data Risk Types – Update
6. Content for next version of Guidance
7. DSITN (Data Safety in the News)
8. Update on Tooling
9. SCSC Seminars and SSS'23
10. Actions
11. Next meeting
12. AOB

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].*

The meeting slides are available at: https://scsc.uk/file/gd/72nd_DSIWG_Slides_v1-1467.pptx

1. Welcome

MP opened the meeting and welcomed those attending.

2. Data Safety and Dashboards

JK presented slides from TomTom outlining their approach to Data Safety including Data Risk Management and Safety Dashboards. The slides are available here: https://scsc.uk/file/gd/2022-11-10_DataSafety_at_TomTom-1469.pdf

MP noted that these showed a mature approach to managing data risks.

JK said that in using the Data Safety Guidance (DSG) some suggestions and ideas for improvements had been noted. These could be considered as candidate changes for the new version of the DSG.

Action 72.1 (JK) – Send MP the suggestions and ideas from TomTom application of the DSG for consideration in the new version

RR noted that there are some common features in standards documents such as lists of Work Products and Threads/Lifecycles which make them easier to work to. These features should be considered for the DSG.

Action 72.2 (RR) – Send MP the suggestions for improvements related to the typical content of standards documents

There was a discussion about the pros and cons of using categorization / levels in risk management, i.e. DSALS, or RGB categories for metrics reporting. It was thought that these are generally a good thing in that they allow comparisons, management reports, comparisons of systems, etc. but obviously create difficult decisions at the level boundaries.

3. Fuzz Testing

PB presented a set of WIP slides on Fuzz Testing as a precursor to the SCSC Seminar on Testing on 1st October (https://scsc.uk/e966). The full slide set will be available after this event.

This work created some discussion and clearly had many data aspects to it. There was a suggestion that it might also apply at higher and more complex data levels, not just at module or unit level (i.e. with data files/data sets). It was noted that Fuzz techniques are often used for security-related testing. A website 'The Fuzzing Book' was referenced, https://www.fuzzingbook.org/

CT noted that this sort of testing would be highly relevant to instrumentation and embedded systems. MP noted that the Boeing 737 MAX accidents might have been avoided if Fuzzing techniques for testing sensor inputs had been applied.

4. Standards to use as template

CT presented some slides (https://scsc.uk/file/gd/ISODatasafety-1470.pptx) covering standards which might provide templates to use for producing a data safety standard.

His conclusion was that the ISO/IEC 27001 series probably provides a good starting point.

5. New Data Risk Types

MP outlined the latest thinking on Dead Data Types, https://scsc.uk/file/gd/Dead_Data_Types_v3.1-1466.docx and explained that PH and MP were working on a taxonomy / ontology for these.

There will be a working meeting on these data risk types on 15/11/22. Please contact mike.parsons@scsc.uk if you want to attend.

6. Content for Next Version of Guidance

MP outlined the proposals for the next version of the document:

- W3W (What3Words) issues. In fact there may well have been real safety incidents already, see https://www.grough.co.uk/magazine/2022/08/31/dont-rely-solely-on-what3words-app-say-lakeland-rescuers-sent-to-wrong-side-of-lake#
- Data Risk Cygnology, see article in the latest SCSC Newsletter: https://scsc.uk/scsc-177
- Add Homophones/Homonyms explicitly to the guidance (related to W3W issues above)
- Add data properties from Thor Mykelbust: Analysability', 'Explainability', 'Verifiability'
- MT/MA were going to do some work on aggregation which could be included?
- MP to update and enhance the migrating/porting already in the guidance with the content presented at meetings
- JK with experience on applying the DSG at TomTom
- RR with suggestions from other standards documents
- Any other accidents / incidents mentioned in the Data Safety in the News sections of minutes
- Other material related to actions (see below) that have a target version of "4.0"
- Possibly on the new work that MP and PH are doing an ontology for data risks, but it is recognized that this work is not yet mature

7. Data Safety in the News (DSITN)

It was thought the UK government breaches of email security could have safety implications, https://www.theguardian.com/politics/2022/oct/31/braverman-admits-personal-email-work-six-times-apology-secret

The UK government handling of migrants in processing centres has become slow and many are held in very poor conditions, partly due to data handling, *"… the Home Office's decision-making was incredibly slow. It relied on unmanageable computer systems and massive spreadsheets: it could take each case worker up to 40 minutes just to carry out the simple task of booking an asylum seeker in for an interview."*, see https://www.bbc.co.uk/news/uk-63477371

8. Update on Tooling

MA said that an update on recent contract wins will be made at next meeting.

9. SCSC Seminar and SSS'23

MP mentioned the upcoming December seminar on Testing: https://scsc.uk/e966 which has a data aspect.

Also SSS'23 takes place in February 2023 in York: https://scsc.uk/e898 - bookings are open and there are still spaces for posters. If you would like to present a poster, please contact mike.parsons@scsc.uk

10. Actions

Not discussed during the meeting, but updated below:

11. AOB

None

12. Next Meeting

Next meeting will be held mid-December probably by Zoom. MP to arrange.

13. Thanks

Thanks to JK and PB for making presentations.
Thanks to MP for taking the minutes.
Thanks to MP for chairing.

Summary of Open Actions

Actions greyed out are considered closed and will be removed from the list at next issue.

Ref	Owner	Description	Target Guidance Version
42.9	MP	Work out a matrix of data categories (previously 'types') and data properties (as per DB discussion)	N/A
43.4	MP	Write up a data focussed FMEA approach.	4.0
44.2	MP	To discuss with AK on how to get the Wikipedia article published	N/A
46.1	MP	Review the application of DSALs to higher level forms of aggregation	N/A
49.6	MT	Review Overleaf briefing material and aim to hold a briefing before end of March 2021 in the use of Overleaf in the production of the guidance.	N/A
53.1	MP	To talk to Kevin King about what we need to do in the guidance for digital twins.	4.0
61.2	AW	Research the relevance of digital currencies and report back to the group (with MA and MT)	N/A
63.1	CT	Look at both Dark Data and Dazzle Data for sensors (e.g. when a sensor is saturated, in noisy environment or when readings are below the detection level floor)	4.0
64.1	MP	Contact Thor and establish the details of the guidance proposals in the paper.	4.0
66.6	MT	Add these three properties ['Analysability', 'Explainability', 'Verifiability'] to the user-visible further work section. If time allows then develop into the guidance further.	4.0
68.2	MP/MT	Develop the migration work further and present at next meeting	4.0

Ref	Owner	Description	Target Guidance Version
69.1	CT	Establish a list of similar / related TRs that we could use as examples.	
69.2	RR	Explore the issue of data / software compatibility issues and to what extent data can impose requirements on software	4.0
69.3	PMcK	Develop a scoping diagram that shows how the DSG fits into the overall lifecycle process and other standards	4.0
69.4	MA	Write a short note on the issues of aggregation	4.0
69.6	MA/DA	Update the data safety tool to use the latest version of the guidance document	-
70.1	MA/DA	Investigate feasibility of creating searchable web database of data safety-related accidents.	-
71.1	MP	Add Homophones/Homonyms explicitly to the guidance.	4.0
71.2	MP/PH	Consider these additional data risk types (Abandoned/Derelict/Magic Numbers) in the list of types and in the articles	4.0
71.3	PH/DA/RO	Develop security properties thinking further for next DSIWG	4.0
71.4	PH/DA/RO	Present security properties work to next SISWG meeting	-
71.5	AM	(i) Establish if any of this can be published within the DSIWG and (ii) Consider a structuring similar to that used in security standards or ISO26262	-
71.6	RO	See if an expert can be found to give a presentation on Fuzz Testing to next meeting	-
71.7	MP/CT	Consider impact of FAIR data on the guidance	4.0
72.1	JK	Send MP the suggestions and ideas from TomTom application of the DSG for consideration in the new version	4.0
72.2	RR	Send MP the suggestions for improvements related to the typical content of standards documents	4.0