

SCSC Data Safety Initiative – WG Meeting 76

4th May 2023, CGI Reading and Zoom

Minutes

Attendees

Mike Parsons (MP) – AAIP, Tim Rowe (TR) – Consultant, Paul Hampton (PH) – CGI, Nick Hales (NH) – Consultant, Mike Standish (MS) – Dstl, Mark Templeton (MT) – Qinetiq, Divya Atkins (DA) – MCA, Martin Atkins (MA) – MCA, Jennifer Kracht (JK) – TomTom, Dave Banham (DB) – Blackberry, Gordon Hurwitz (GH) – Thales, Paolo Giuliani (PG) – Atkins, Carl Tipton (CT) – Johnson Matthey, Brent Kimberley (BK) – Durham

Apologies

Oscar Slotosch (OS) – Validas, Rhiannon Chilton (RC) – DSTL, Susan Perriam (SP) – Atkins, Paul McKernon – Consultant, Richard Garrett (RG) – SQEP, Bob Oates (RO) – Consultant, Michael Green (MG) – Ecomergy, Daniel Clegg (DC) – BAE Systems, Andy Williams (AW) – Consultant, Alastair Faulkner (AF) – Consultant.

Agenda

1. Welcome
2. Data Hazard Labels
3. Oldest Data Safety Error
4. How TomTom tried to assure Data Safety
5. ISO/IEC 25012 summary
6. AI / ML and security
7. Recent Webinars
8. DSITN (Data Safety in the News)
9. Actions
10. Next meeting
11. 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].*

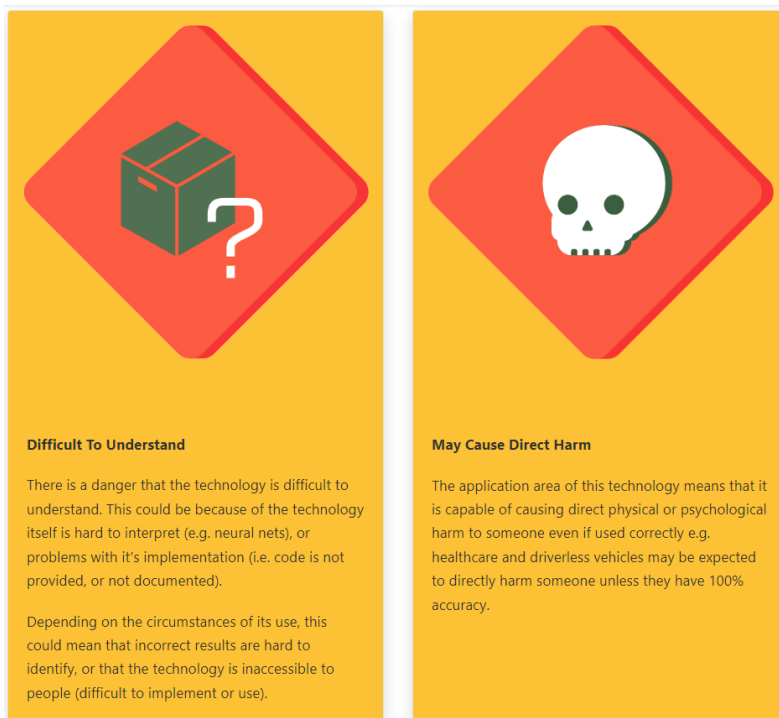
The meeting slides are available at: https://scsc.uk/file/gd/76th_DSIWG_Slides_v2-1557.pptx

1. Welcome

MP opened the meeting and welcomed those attending.

2. Data Hazard Labels

MP introduced the meeting to data hazard labels, and the concept was discussed. The idea was found interesting, although it was less clear where data hazard labels might be beneficial. The meeting agreed to try the concept in the Guidance. Examples are:



MP suggested it might work for the identified data issues. Further detail is available at <http://datahazards.com>. There were some comments in the meeting chat¹


3. Oldest Data Safety Error

Contributions on this topic were received from RC, AF and TR.

¹ 11:10:59 From martin To Everyone: Visual version of Guide words?

11:11:31 From Jennifer Kracht - TomTom To Everyone: is there a label for data that is shared insecure?

11:12:58 From Tim Rowe To Everyone: There is a label for "Risk to privacy" which would overlap with data that is shared insecure.

11:14:20 From Jennifer Kracht - TomTom To Everyone: Reacted to "There is a label for..." with 

11:22:09 From Tim Rowe To Everyone: ISO 3864-2:2016 Graphical symbols — Safety colours and safety signs — Part 2: Design principles for product safety labels

Various early data issues were considered, including longitude errors leading to shipwrecks. The lack of the Marine Chronometer caused the data error (in Longitude), one factor in the Scilly Naval Disaster of 1707:

https://en.wikipedia.org/wiki/Scilly_naval_disaster_of_1707

Discussion also included John Harrison's H4 Chronometer, https://en.wikipedia.org/wiki/John_Harrison and also errors introduced by astrolabes. However, it was considered difficult to tie these early navigation issues to specific well-documented accidents.



Due to many ships being unstable and sinking when loaded, the Plimsoll Line was introduced (...a report at the time found that *...nearly a thousand British sailors lose their lives due to the uninformed overloading*, <https://www.marineinsight.com/maritime-law/what-is-plimsoll-line-on-ships/>), but found to be relatively recent (1860s).

The Charge of the Light Brigade (1854) was considered as the catastrophic error leading to the losses was caused by ambiguity or incomplete data:

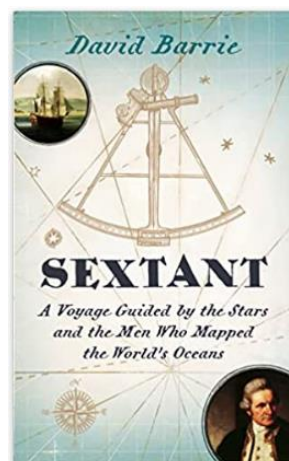
https://en.wikipedia.org/wiki/Charge_of_the_Light_Brigade

RC communicated by email that "...there must be some early battle/war examples. Misjudging location information, opposition numbers, weapon capability etc. The Battle of Agincourt, 25 October 1415, being won in part due to 'The French, however, made a ruinous mistake, miscalculating the accuracy, range and firing rate of the English longbows.'

<https://www.historyhit.com/military-mistakes-in-history> (although I've struggled to find information to substantiate this)."

She also mentioned that exploration of the Solomon Islands was fraught with problems due to inaccurate longitude (See Preface of a book called 'Sextant', by David Barrie):

<https://www.amazon.co.uk/Sextant-Voyage-Guided-Mapped-Worlds/dp/0007516568>



MS also found an article saying that the Great Pyramid of Giza contains an alignment error. "Great Pyramid of Giza Was Lopsided Due to Construction Error" – the key will be what caused the construction error of course! <https://www.ancient-origins.net/news-history-archaeology/great-pyramid-giza-was-lopsided-due-construction-error-006161>

There were some comments in the chat². The hunt for the oldest data error continues...

[Post meeting note: MP wondered if Lloyds Register Foundation might provide grant funding through their established schemes for someone to look at the extensive records in London to find definite examples of maritime data errors which had safety implications. Contact MP if interested.]

4. How TomTom tried to assure Data Safety

JK presented her findings on applying the Guidance at v3.3 to a product under development by TomTom, as a Proof of Concept. A separate paper has been provided:

https://scsc.uk/file/gd/How_TomTom_tried_to_assure_Data_Safety-1558.pdf

JK thought that the diagram in this page was helpful: <https://lakefs.io/blog/what-is-data-lifecycle-management/> Some points of note are:

- Some proposed Treatments do not deserve the title, as they apply after the fact - "follow up meetings", for example.
- Notes from the Treatment tables were better reworded as Requirements.
- A big jump was found between the compliance requirements for DSAL 2 and 3, leading to a project decision to apply DSAL 3, to err on the side of caution.
- The weighting given by the number of Treatments associated with each DSAL is uneven, with very few HRs in DSAL2. We should review the allocation of HRs and Rs, to see whether a more even approach can be achieved, possibly by downgrading some DSAL 3 HRs to R.
- It was not obvious that the Guidance builds up in subsequent chapters from Objectives through high level explanations, to detailed approaches - a "how to read this document" might be helpful.
- More mapping and cross referencing between chapters would be useful.
- There was no guidance on how to measure success. Some form of Key Performance Indicator or other metrics would be useful.
- There was some discussion about data safety metrics. DA pointed out that you don't reduce SILs in software development, so we should probably not be looking at a reduction in DSAL. However MP pointed out that a DSAL could be considered as a risk level, rather than just a means to work out what to do about the risk.

² 11:35:21 From Carl Tipton To Everyone: <https://www.123helpme.com/essay/Lack-Of-Communication-And-The-Collapse-Of-526961>

11:36:27 From Carl Tipton To Everyone: My son told me that one the other day, the collapse of the Roman Empire was because it was too big to get information from one side to the other in a timely fashion, hence rule became impossible

11:38:01 From martin To Everyone: That is the reason for many of Caesar's writings - they were reports back to Rome about what he had done, etc

11:39:21 From Tim Rowe To Everyone:

"On 22 July, the Prime Minister, Benjamin Disraeli, announced that the bill would be dropped. Plimsoll lost his self-control, applied the term "villains" to members of the House, and shook his fist in the Speaker's face.[1]

"Disraeli moved that he be reprimanded, but on the suggestion of Lord Hartington agreed to adjourn the matter for a week to allow Plimsoll time for thought.

"Eventually Plimsoll made an apology. Many people, however, shared his view that the bill had been stifled by the pressure of the shipowners, and popular feeling forced the government to pass a bill which in the following year was amended into the Merchant Shipping Act." https://en.wikipedia.org/wiki/Samuel_Plimsoll

11:39:39 From martin To Everyone: So that is about the communication of "red lines" from design to operation.

5. ISO/IEC 25012 summary

TR presented his findings from a comparison of IEC 25012 with the Guidance. The detail is in the slides [https://scsc.uk/file/gd/ISO25012_Summary_\(1\)-1559.pptx](https://scsc.uk/file/gd/ISO25012_Summary_(1)-1559.pptx) but in addition:

- IEC 25012 defines data, whilst the Guidance does not. However the definition in IEC 25012 is of limited benefit to this DSIWG.
- Metadata was identified as something that deserves further consideration, as it can cause data to be misinterpreted.
- It may be helpful to compare IEC 25012 "characteristics" to Guidance Properties, to ensure that nothing has been missed.
- IEC 25012 characteristics appeared to be at different levels, in some cases aligning with our Properties, but others being high level objectives.
- IEC 25012 presents examples, but not solutions. We could consider developing a mapping from the "requirements" of IEC 25012 to the lower-level detail of "how to meet requirements" within the Guidance. However, PH pointed out that there are many data quality standards, and that we should consider whether it is beneficial to focus on this specific one.
- IEC 25012 does not provide a process - it's just a model.

The discussion around IEC 25012 led to two actions:

Action 76.1 (MP, PH, MT): Consider whether Guidance Annexes can be integrated into the main body of the document.

Action 76.2 (TR): Look further at IEC 25012 to consider whether a new Annex to the Guidance would be beneficial.

6. AI / ML and security

MP explained that he had received a document from RO, "AI SECURITY CONCERNS IN A NUTSHELL", https://scsc.uk/file/gd/BSI_AI_Security_Concerns-1560.pdf which outlined some of the ways in which AI/ML systems can be subverted by malicious intent. He said that many of the mechanisms appear to be data-related so it something we should look at.

Discussion was deferred to a future meeting, as RO was not present.

7. Recent Webinars

PH and MP reported that there had been two SCSC webinars on Clinical Data Safety recently (<https://scsc.uk/e1001> and <https://scsc.uk/e1000>). These were seen as a success with a lot of attendees and some participation (particularly in the second one). The first one had some technical problems. The NHS speaker in the second webinar, Charles Olowosuko, was thought to be very good. It was noted that PH presented some diagrams in the webinar that could help in the Guidance document.

MA and DA spoke about data safety tooling at the Webinars.

8. DSITN (Data Safety in the News)

The Government's safety alert to mobile phones was considered not very effective, as many phones remained silent (also people can turn off the alerts if desired). However, it was a test, so it could be regarded as successful.

A smear test issue in Scotland involved the incorrect classification of data, but it was unclear whether this was caused by a data error, or a misuse of data, <https://www.bbc.co.uk/news/uk-scotland-65299210>. The problem became apparent in 2021, but recently, 13,000 more people have been identified as potentially affected.

9. Actions

See table at end.

10. AOB

NH pointed out that Geoffrey Hinton had resigned from Google over concerns with AI. NH is looking at aviation issues, and can see that in many cases where human error had been identified as the cause, it could be read across to AI making the same mistakes in the future. Miscommunication remains a classic issue.

JK mentioned this image which fools vehicle AI:

https://www.fairkehr-magazin.de/fileadmin/_processed_/csm_6_2017_3D_Zebrastreifen_8c0535e054.jpg

as the crosswalk is painted in 3d. Apparently the vehicle recognizes this as barriers on the road.

MS stated that questions given to ChatGPT are not currently used as training data, but eventually they may be. Should there be a warning on ChatGPT about the dangers of inadvertently giving away Intellectual Property? There was further discussion about ChatGPT and TR added this question and ChatGPT response to the chat:

"Produce a chatbot similar to ChatGPT but that only produces verifiably correct results."

As an AI language model, my responses are based on probabilities and statistical analysis of a large corpus of text. While I strive to provide accurate and reliable information, there is always a chance that my responses may not be completely correct.

However, to create a chatbot that produces verifiably correct results, it would require a significant amount of time and resources to ensure that the information provided is accurate and up-to-date. One possible approach would be to have a team of subject matter experts review and verify each response generated by the chatbot to ensure its correctness.

This chatbot could be designed to only provide information on topics that have been extensively researched and verified, such as scientific facts, historical events, or mathematical equations. Any response that is not verifiably correct could be flagged and reviewed by the team of experts to ensure its accuracy.

Action 76.3 (MT): Provide slides from last October's SQEPtember presentation (an introduction to data safety) to MP.

MP pointed out that presentations from previous meetings such as SSS and Data Safety seminars were available on the SCSC website (on the Catch Up tab at left). MT asked whether we should provide a webpage with links into this collection of data, to make it easier for people to find introductory material, actual experience in applying the Guidance, and so on. MP and NH discussed the possibility of generating a DSIWG App, or other Social-Media based access to DSIWG data.

JK mentioned that we need to cover all data risk aspects: safety, security, privacy, quality and compliance and manage this in its whole lifecycle.

MS stated that DSTL has created a hyperlinked version of a document, that has been thoughtfully produced, as navigation of the document had been an issue. We could consider it as a model for improving our own offering. An example is:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1120270/MASAAG_Paper_124.pdf

MS added via email:

[We need] Information to allow the DSG to be understood in a 'digestible' format. At the moment there is information on generic data safety and why it is important and then there is the full DSG. I've talked to people in Dstl and MOD about data safety / the DSG but there doesn't appear (to me at least) to be something which provides a short 1-2 page summary of the DSG itself (the process and it's benefits) rather than why data safety is important. Perhaps a 1-2 pager or other 'sales' literature could work? Something akin to the INCOSE Z Guides (https://incoseuk.org/Normal_Files/Publications/zGuides), although the tri-fold format possibly isn't suitable for reading electronically. The data safety videos we looked at yesterday were useful, possibly have something on the 'public facing' site of the DSIWG?

He also asked if there are any use cases / success stories from projects that have used the DSG? These could highlight it's benefits and the impact it has had? This information could be 'published' on the DSIWG website or via LinkedIn etc? Are there any training packages that can be provided as slides or as a 1/2 day course on applying the DSG? I know Mark put some slides together and Mark ran a successful event for DE&S but is there a training reference which users could access?

11. Next Meeting

The next meeting will be held in around 6 weeks (so mid-end June) via Zoom. MP to arrange.

12. Thanks

Thanks to all who provided contributions.

Thanks to PH for providing the venue.

Thanks to MT 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.

61.2: MA stated that AW has started development of some slides on digital currencies and may be ready to present it at the next meeting.

69.4: The action was "Write a short note on the issues of aggregation". MA said that he had been considering the risks of aggregating data, such as loss of privacy. MP pointed out that the Action was originally intended to address the aggregation of DSALs. However both aspects are useful.

69.6: The tool has been updated to align with Guidance v3.4. MT asked whether we should have a "security" Annex in the Guidance. The general principles of customisability and extensibility in the tool would be a good thing - after all, we encourage users to add their own Treatments to the tables.

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
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
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	-
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	-
71.7	MP/CT	Consider impact of FAIR data on the guidance	4.0
73.1	JK, RR	Consider production of a short note which could be used as an appendix to the guidance on lessons learnt using the guidance at TomTom	4.0
73.2	MT	Consider how the guidance fits with different lifecycles considering 'V', Continuous Service, Agile and 'Data Pipeline'	4.0
73.4	DA	See whether any of the DSITN entries from previous minutes and slides could be used to enhance the list of accidents	-
75.1	MT	Produce a short presentation on approach to updating IEC 61508 to include data safety aspects	
75.2	TR	See if access to the ISO 25000 standards can be obtained through the IEE / IET and, if so, have a quick look at how it related to our guidance.	4.0

Ref	Owner	Description	Target Guidance Version
75.3	MT	Fix the minor typos that have been reported with v3.5 and prepare updates for both the online version and also the KDP/Amazon hardcopy.	3.5 Update
75.4	MP	Create a challenge to find the earliest documented data safety error	
76.1	MP, PH, MT	Consider whether Guidance Annexes can be integrated into the main body of the document.	4.0
76.2	TR	Look further at IEC 25012 to consider whether a new Annex to the Guidance would be beneficial.	4.0
76.3	MT	Provide slides from last October's SQEPtember presentation (an introduction to data safety) to MP.	-