SCSC Data Safety Initiative – WG Meeting 65

18th November 2021, Zoom

Minutes

Attendees

Divya Atkins (DA) - MCA, Martin Atkins (MA) - MCA, Dave Banham (DB) - BlackBerry, Dale Callicott (DC) - BAE, Sarah Dickens (SD) - Innovate Edge UK, Emrah Eminoglu (EE) – TomTom, Nick Hales (NH) - Rtd, Mike Parsons (MP) – AAIP, Andy Williams (AW) – Consultant, Richard Garrett (RG) – SQEP, Oscar Slotosch (OS) – Validas, Brent Kimberley (BK) – Durham, J Kracht (JK) - TomTom, Paul McKernan (PMcK) - Dstl, Arash Saberi (AS) - TomTom

Apologies

Paul Hampton (PH) – CGI, Michael Green (MG) – Ecomergy, John Bragg (JB) - MBDA

Agenda

1. Welcome
2. Opener
3. TomTom & Guidance
4. Dazzle Data Rename
5. Content of Guidance V3.4
6. Data Safety in the News
7. Covid-19 Data Systems
8. Planning for 2022/23
9. Data Safety Tooling
10. SSS'22
11. Actions
12. Next Guidance Version
13. 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].*

The meeting slides are available at: https://scsc.uk/file/gd/65th_DSIWG_Slides_v1-1279.pptx

1. Welcome

MP opened the meeting and welcomed the attendees: both physically present and remote via Zoom.

MP discussed briefly that he had been involved in a proposal for Service Assurance research arranged by Davy Pissort of KU Leuven involving funding from the EU Marie Curie Network. He wondered if the same sort of approach might work for Data Safety which would then fund a set of PhDs students to study across Europe (including the UK).

Action 65.1 (MP) – Contact Davy Pissoort and see if any interest in this funding route for Data Safety

2. Opener

MP presented a photo of a BACS bank transfer error which was for Prof. Harold Thimbleby's house move. The figure shown on the completed transfer document was nearly £80 million, rather more than he was expecting for his house sale! There was a discussion on how data is now everywhere and impacts on everything.

3. Presentation by TomTom

AS from TomTom gave a presentation. He explained that TomTom is now primarily selling location technology to other organisations, given the widespread adoption of 'free' services such as Google Maps, etc. They are here to understand how they can apply the Data Safety guidance to TomTom.

Why do they care about Data Safety at TomTom?

- OEMs are demanding safe development
- Liability and compliance – product liability and protect reputation
- Competition is positioning safety as USP

Further considerations include the Safety Assurance required for Autonomous vehicles. Also there is a reliance on accurate mapping information for Level 4+ autonomous driving solutions.[1]

TomTom use lots of different sources of map information – i.e. government sources, targeted surveys, "roadagrams" (real-time updates received from Vehicles)

Sources of map errors that could reduce safety:

- Reality change
- Errors made between capturing real-world observation and making map available
- Real-world change between observation and use of the map

MP noted that there is significant overlap between the concerns expressed by SA and work that is being conducted by himself in conjunction with the University of York related to research on autonomous vehicles within the AAIP (https://www.york.ac.uk/assuring-autonomy/).

DC explained the background to work on maritime charting at the UK hydrographic office (https://www.admiralty.co.uk/ukho/About-Us) and noted there is a significant overlap with the

[1] https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles

issues faced compiling maritime charts as for land mapping. He asked whether there is a standard used when collating charts in the TomTom world? AS explained there are standards applied to collation of the data, but no standard defined for how hazards are actually notified to the driver, etc. DC explained that a confidence level can be assigned to data elements to indicate how reliable the data is perceived to be with respect to the outside world. AS confirmed a similar technique is applied to the mapping data distributed by TomTom.

AS noted the use of real-time sensors in vehicles (and the driver) as additional sources of information and agreed that the data and hazard information supplied to the vehicle cannot be the only source of control (but noting that future autonomy may place more reliance on this data).

MP asked whether there is an attempt to state the confidence on location data – i.e. to apply a tolerance on positional data of elements – a measure of uncertainty.

BK mentioned a paper that outlined a proposal to apply to physical systems to ‘filter’ improbable step-changes in motion based on their known inertia.

AS and EE outlined one of the difficulties they experienced trying to apply the Data Guidance to their application. Initial concern is that process for determining DSAL is highly subjective, particularly when trying to assess likelihood – high, medium, low etc

There was a discussion on clarity of the system boundary when applying the guidance. For TomTom, it was suggested that the boundary is the interface with the driver (i.e. hazards arise on the display screen or other devices, e.g. audible warnings). The boundary has to be here as we cannot be sure that driver will react to the information being presented.

MP suggested that it is best to avoid being too mechanistic when applying the process of likelihood and DSAL assignment. Sometimes it requires application of intuition and best engineering judgement to determine a DSAL.

DB contributed much to the discussion and explained some of the history of the guidance development, and that the data properties (e.g. integrity) were the real step forward. He suggested that TomTom should look at the properties of the data they are trying to preserve (e.g. timeliness)

AS explained some further observations. It was noted the tables of methods are meant to be applied selectively (with justification) so it is not necessary to apply all applicable methods, for example use of checksums and then hashes.

4. Dazzle Data Rename

MP opened a discussion on renaming ‘Dazzle data’,
https://scsc.uk/file/gd/Words_for_Dazzle_Data_for_DSIWG_Guidance_3.4_v0.7_clean-1280.docx
A number of options were considered but it was felt that Dazzle Data or possibly Distracting Data would be the best name. A ‘Where’s Wally’ picture was used as an illustration of one of the types of Dazzle Data.

5. New Guidance Document Version 3.4

MP discussed what may go into the next edition of the guidance v3.4 – due for publication next year (February, so has to be ready in January 2022) to support SSS’22. Mike listed four items for consideration:

1. Inputs/clarifications/corrections from the TomTom work
2. More accident examples (MA is preparing one)
3. Sufficiency Issue (need MA/PH agreements)
4. Distracting/Dazzle Data (Appendix is ready)

6. Data Safety in the News

MP highlight some recent news stories where data was a factor:

1. Data Integrity and Whistle-Blowing, Pfizer vaccine trial BMJ: https://www.bmj.com/content/375/bmj.n2635
2. Woman died after benefits mistakenly cut, Benefits and Data [thanks to PH]: https://www.theguardian.com/politics/2021/nov/03/capita-pays-compensation-family-woman-who-died-after-benefits-cut-philippa-day
3. The current Covid-19 Data-Dependent Systems were discussed (see table in meeting slides)
4. Peter Ladkin inputs on Covid-19, Articles on Data Science/AI and CoVID-19: https://scsc.uk/file/gd/20210807NoteOnDataScience&Covid19-1278.pdf

7. Planning for 2022/23

MP outlined some areas where future work of the group could be focussed:

1. Machine Learning data sets
2. Post COVID-19 data issues
3. Blockchain / authentication data
4. Fraudulent data / masquerade data
5. Digital currencies

8. Data Safety Tooling

MA provided a live demonstration of the prototype Data Safety Analysis tool to TomTom using a simple example of a Flight Control System. AS/EE expressed some interest in the potential to have access to the toolset.

Action 65.2 (DA/MA) – See if access to the tool can be given to TomTom for evaluation

DA provided some background (history) on development of the tool to date.

SD then joined the meeting and led a session via a Jamboard where we all considered sectors where the tool could have the most potential impact – and who is within reach from a communication perspective.

AS noted that the tool needs to be able to import data from an existing system with a view to then identifying the mitigations that need to be deployed to manage that data, rather than provide a toolset that simplifies facilitates navigation of the Data Safety Guidance document.

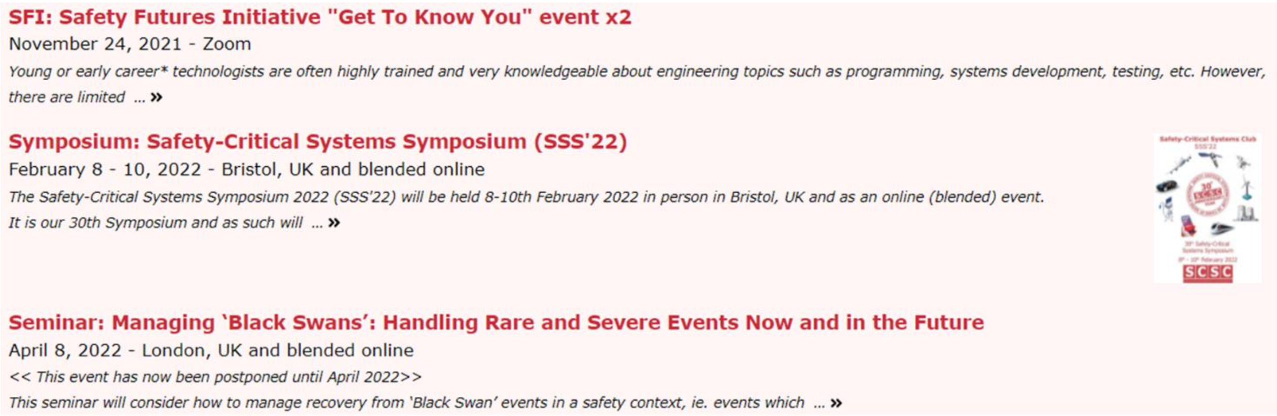
MP noted that Healthcare is probably one sector where there an obvious issue with Data Safety compared to other sectors such Aerospace/Rail. These latter sectors are already quite well regulated, and Data Safety tends to get considered as part of overall Software Safety Case.

[Post Meeting Notes:

1. DA/MA: Recognise that the tooling needs further development, however, without an obvious need (customer) for the tooling, obtaining funding to bring it to a releasable state is difficult. Whilst technical (data safety) specialists recognise potential benefits it is proving very difficult to obtain traction with senior management(s).
2. PMcK: However, one thing we did not discuss, which may be useful, is to understand how much time/money would be required to bring the toolset to a releasable form (at least in beta), knowing this and, ideally, the cost for working to a full release would give us a much better idea of the cost benefit of proceeding. I remain convinced that there is a place for this tool in the general assurance case development domain.]

9. SCSC Events

Future SCSC events (see https://scsc.uk/events) were described and are shown below:



SFI: Safety Futures Initiative "Get To Know You" event x2

November 24, 2021 - Zoom

Young or early career technologists are often highly trained and very knowledgeable about engineering topics such as programming, systems development, testing, etc. However, there are limited ... »*

Symposium: Safety-Critical Systems Symposium (SSS'22)

February 8 - 10, 2022 - Bristol, UK and blended online

The Safety-Critical Systems Symposium 2022 (SSS'22) will be held 8-10th February 2022 in person in Bristol, UK and as an online (blended) event. It is our 30th Symposium and as such will ... »

Seminar: Managing 'Black Swans': Handling Rare and Severe Events Now and in the Future

April 8, 2022 - London, UK and blended online

<< This event has now been postponed until April 2022>>

This seminar will consider how to manage recovery from 'Black Swan' events in a safety context, ie. events which ... »

10. AOB

NH discussed his work on the Layered Data Safety Model. This looks at the chain of why, what, because, therefore and can be used to support a-priori examination of mitigation effectiveness.

MP recommended that NH put his publication for consideration in the SCSC journal [or perhaps serialized in the SCSC Newsletter].

11. Actions, etc.

Action 64.2 was closed.

12. Next Meeting

Next meeting will be held mid-January 2022 in person and by Zoom. MP to arrange.

13. Thanks

Thanks to DA and MA for hosting the meeting in Bath (great location!).
Thanks to AA and PMcK for taking the minutes.
Thanks to MP for chairing.

14. 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.	3.4
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.	3.4
56.2	DA	Consider impact of Dark Data on the Data Safety Tool	N/A
61.1	MP, PH, MT	Check existing data property definitions and add a case related to "Unexpected" data [Related to 'Sufficency' issue – suggest encompasses this as well.]	3.4
61.2	AW	Research the relevance of digital currencies and report back to the group (with MA and MT)	3.4
62.1	MA	Create war story for the next issue of the guidance on the Buncefield data loss	3.4
62.3	MP/MT	Consider issues of porting and importation of legacy data	3.4
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)	3.4
64.1	MP	Contact Thor and establish the details of the guidance proposals in the paper.	3.4
64.2	MP	Process the Dazzle Data comments from PH and produce updated version	3.4
65.1	MP	Contact Davy Pissoort and see if any interest in this funding route for Data Safety	-
65.2	DA/MA	See if access to the tool can be given to TomTom for evaluation	-