DSIWG

SCSC Data Safety Initiative – WG Meeting 79

20th September 2023, Zoom

Minutes

Attendees

Mike Parsons (MP) – Ebeni, Mark Templeton (MT) - Qinetiq, Richard Thomas (RT) – AtkinsRéalis, Dave Banham (DB) – Blackberry, Paul Hampton (PH) – CGI, Jennifer Kracht (JK) – TomTom, Michael Green (MG) – Ecomergy, Paolo Giuliani (PG) – EDF, Paul McKernan (PMcK) – Consultant, Divya Atkins (DA) - MCA.

Apologies

Richard Garrett (RG) - Garrett Associates Ltd, Melanie D'Mellow (MDM) – Adaptix, Dave Murray (DM) - BAE Systems, Mike Ainsworth (MAi) – Ricardo, Dave Smith (DS) – FNC, Ali Hessami (AH) – Vega, Roland Rosier (RR) – TomTom, Martin Atkins (MA) – MCA, Mike Standish (MS) – Dstl.

Agenda

1. Welcome
2. NATS Outage
3. Email from Oscar re: F-35
4. Email from Oscar re: Japanese Moon Lander
5. Data Affecting Data Update
6. Email from John Spriggs re: "Weight Carrying Competition"
7. Oldest Data Safety Error Paper
8. DSITN (Data Safety in the News)
9. Update on Tooling
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/79th_DSIWG_Slides_v1-1615.pptx

1. Welcome

MP opened the meeting and welcomed those attending.

2. NATS Outage

MP noted the recent NATS Air Traffic Management problem in the UK where a flight plan with duplicate waypoint data caused both primary and backup systems to fail, causing an outage in automatic flight plan processing. This led to major disruption of about a week, considerable distress for stranded passengers and approximately £300 million in costs. Some links:

https://www.bbc.co.uk/news/uk-66654338
https://www.bbc.com/news/uk-66685349
https://www.flightglobal.com/safety/coincidentally-identical-waypoint-names-foxed-uk-air-traffic-control-system/154824.article

This was discussed by the group. MP said that this polarized posts in LinkedIn and elsewhere with some people saying it was a simply an algorithmic software problem, others saying it was a systems issue with no diverse backups, etc. and others saying that the real issue was an incredibly 'brittle' or 'fragile' air traffic system with no contingency within the system, and that software outages must be expected.

MT noted that the flight plan processing system had been running for many years without error. There was surprise within the group that the backup system seemed to run with identical data, software and hardware – so very little backup in practice due to common-mode failures. MT said that in military aircraft care is taken to not present identical data feeds, including placing GPS receivers in different zones on an aircraft.

MP suggested this NATS problem was a good example of a common-mode failure involving identical data, and diversity should have been introduced, at least for software and hardware.

MG thought that this was essentially a business continuity problem and that there should have been more robust measures in place, and was symptomatic of an over-estimatation and over-confidence in the reliability of software systems.

Although the manual processes for flight plan processing were executed successfully (allowing a lower rate of flight plans), there were concerns that staff may have become stale or at least unfamiliar with what was required of them.

It was noted that this problem could easily have been more serious, as NATS have many duplicated legacy systems.

3. Email from Oscar re: F-35

OS communicated a data and software problem which was discussed by the group. This led to the complete loss of an F-35: "The bumpy air caused the F-35's flight controls to register incorrect flight data, and the jet stopped responding to the pilot's attempts at manual control."

https://www.defensenews.com/news/your-air-force/2023/07/27/software-glitch-during-turbulence-caused-air-force-f-35-crash-in-utah/

4. Email from Oscar re: Japanese Moon Lander

OS sent an email regarding the failed Japanese moon lander. In summary they changed the landing position to a place they did not simulate.

https://www.nytimes.com/2023/05/26/science/moon-crash-japan-ispace.html

Then it turned out that the surface there was too steep for their software and it wrongly concluded the height sensor must be defective… If they had simulated this place too, they probably would have detected and avoided it.

5. Data Affecting Data Update

MP added two further cases to the existing list of examples:

1. A bad config parameter data item causes other items to be unused/unselected
2. Tuning/filter/selection data settings are incorrect (e.g. bad date range or RAG)
3. Tags or metadata are incorrect or lost causing the original data to be unused/wrongly used
4. Noisy or bad data (e.g. timestamps) causes correct data to be rejected (Dazzle Data L.3.2, 3.3, 3.4 etc)
5. Sentinel values are incorrect causing wrong data to be selected
6. NEW: Bad CRCs cause data items to be incorrectly rejected
7. NEW: Incorrect indices in arrays or tables cause the wrong data to be selected

DB wondered if analyses such as FTA might help to investigate this issue. MP thought that some sort of analysis based on 'knock-on level' or 'impact area' might help, possibly related to 'fan-out'. MT said that he had successfully used EBA or EBTA (Energy Barrier Trace Analysis, http://icma.org.uk/06-6_etba.html) to look at data transfer through systems.

ACTION 79.1 (MT) – Introduce EBA / EBTA with a short presentation at next meeting

JK thought it important to note that it is possible to have many users and uses of the same data

6. Email from John Spriggs re: "Weight Carrying Competition"

John Spriggs communicated a historic data safety issue:

> *"In August 1910, Bertram Dickinson, a well-known aviator at the time and recently retired from the Army, entered a competition at the Lanark Airshow. It was the "Weight Carrying Competition". To increase his aircraft's payload, he took the editor of The Aero magazine as passenger, and asked for some lead sheets to be added to both balance the aircraft and increase the overall weight. The account I read said that he calculated that he needed about 19kg, but for some reason the engineers added 44kg to his Farman biplane."*

So this appears to be units confusion: this was 1910; Mr Dickinson would have calculated in pounds - he needed about 44lb, the Farman engineers, who were French, added 44kg... The aircraft took off,

but soon crash landed, both occupants were thrown clear, uninjured. An image of Mr Dickinson's aeroplane is at: https://flic.kr/p/hb1wZ

MT noted that these sorts of errors are often not just due to units, but also language and cultural aspects also. He mentioned an English/French example where the understanding was exactly the opposite for both nationalities.

A more modern example of units confusion is the Air Canada Flight 143 (the 'Gimli Glider', https://en.wikipedia.org/wiki/Gimli_Glider) where there was confusion of imperial and metric units when fuelling, resulting in a Boeing 767 glider.

7. Oldest Data Safety Error Paper

MT, PG and PMcK agreed to help MP produce the paper for SSS'24.

MP explained that the bulk of the paper will be a set of data-related accidents / incidents with:

- A title, reference or link
- Ideally a picture, diagram or some sort of illustration
- Approx. two paragraphs of text describing the issue
- Approx. one or two sentences giving the 'read-across' to a modern context

This is expected to be about 1 page total for each accident.

As per the reviewer comments it was agreed that the paper would also include relevance to today's data problems and include mitigations where possible. The deadline for the paper is by the end October 2023, so the accident cases will need to be done by 15th October at the latest.

8. DSITN (Data Safety In The News)

MA sent through some topics with data aspects. These were briefly discussed. The ones not already covered earlier in the meeting were:

- Chandryan 2 moon lander crash, https://en.wikipedia.org/wiki/Chandrayaan-2
- More police data leaks, https://www.bbc.co.uk/news/uk-england-manchester-66843618 and https://www.theguardian.com/uk-news/2023/aug/26/met-police-on-high-alert-after-it-system-holding-officers-details-hacked
- Voter database leak (safety? Or "just" security?), https://www.theguardian.com/technology/2023/aug/08/uk-electoral-commission-registers-targeted-by-hostile-hackers
- Near loss of comms with voyager spacecraft, https://www.cbsnews.com/news/nasa-loses-communication-voyager-2-spacecraft-antenna-accident-earth/

ACTION 79.2 (DA) – Investigate the Chandryan 2 crash further and report back at next meeting

9. Update on Tooling

PH has used the RADISH tool[1] from MCA and has raised some comments based on a real example. He considered the assistance provided by the tool was very useful. He said that data safety work can produce a lot of requirements and these need combining or pruning. The requirements were all sensible, with some covered by existing design work. The work with RADISH has definitely identified things that need to be analysed.

PH said he would like to share his experience of using the tool.

ACTION 79.3 (PH) – Report on use of the RADISH tool at next meeting

DA said that MCA received some useful feedback from the recent healthcare seminars.

PG mentioned that he did some work on data safety in the nuclear arena several years ago, without any tool support. He thought it would be good to try the tool on this example and see if the work was easier.

ACTION 79.4 (PG) – Re-visit the earlier nuclear data safety work using the RADISH tool

10. Actions

77.1 was closed. See table at end.

11. AOB

Review of DSG

An independent review of the DSG was thought to be really valuable, particularly the accident list in Appendix H to avoid sector bias. However it should be noted that the current set was drawn from accidents that are well documented, and not all sectors do this (e.g. automotive). Also some newer technologies, e.g. offshore wind turbines, may not yet have independent accident reporting in place.

ACTION 79.5 (MP) – Review the DSG accident list in Appendix H and see if a better sector spread can be achieved

Data-Related Accidents in Automotive

DB mentioned his request for examples of data-related accidents and incidents in the automotive sector to assist positioning regarding the update of ISO 26262. MP sent emails to various people and Phil Koopman provided a really useful resource:

https://betterembsw.blogspot.com/p/potentially-deadly-automotive-software.html

A search for 'configuration' or 'calibration' gives several useful data-related incidents, e.g.

Rivian / May 2022

[1] Note RADISH is "Risk Assessor for Data Integrity and Safety Hazards"

- Incorrect calibration data in the front passenger seat **air bag controller does not deactivate with child seat or child occupant** as required due to incorrect weight threshold setting.

Rearview image blanking / failed OTA update (Subaru) / Dec 2020

- "The August 2020 **over-the-air software update may have timed out** without completing the installation, corrupting the data, and causing the **rearview display to shutoff intermittently**."

Improper Air Bag Deployment (Jaguar) / Sep 2020

- "A concern has been identified with certain Jaguar XJ 2010 to 2011MY vehicles and one 2017MY vehicles where, when connected to Jaguar Land Rover's Symptom Driven Diagnostics (SDD) device and an update to the Restraint Control Module (RCM) is unsuccessfully undertaken, the **calibration may default to a pre-set condition**."

Missing Instrument Panel Information (Honda) / July 2020

- "Many in-cabin system interfaces are linked to a central network, including the instrument panel, display audio, and rearview camera display. Due to **inappropriate software programming, increased data traffic on the central network may exceed the computing threshold of the instrument panel control module. Once exceeded, the instrument panel cannot display certain information** required by FMVSS 101; Controls and Displays, such as the engine oil pressure, speedometer, and gear selector position until the next ignition cycle. An overloaded instrument panel control module also prevents the rearview camera image from displaying, which does not comply with the requirements of FMVSS No. 111; Rear Visibility"

ECM may disable fuel injectors (GM Malibu) / Sep. 2019

- "Under certain conditions, an error in the vehicles' engine control module (ECM) software can cause data used by the ECM to become corrupted. When this occurs, the ECM may send a signal **disabling the engine's fuel injectors**."

It was noted that autonomous vehicles will be very data-intensive.

Post meeting note from MG:

My M2M Direct To Satellite communication project (weightless.space) and I have recently been accepted into the UK Space Agency's (UKSA) 'Accelerator' programme.

As such, given the added commitment of time for UKSA related work plus their online meetings schedule, I will find it increasingly hard to participate meaningfully in the SCSC & the DSIWG going forward.

Please accept, therefore, my withdrawal from the DSIWG and pass my apologies to the other members (perhaps as an addendum to the minutes). Participation has provided a fascinating insight to data safety issues, causes, effects and lessons. Insights I expect to incorporate into my own system designs.

Thank you for enabling me to participate and my best regards, Michael

12. Next Meeting

The next meeting will be held 20th October 2023 16:00-17:30 via Zoom, https://scsc.uk/gd

13. Thanks

Thanks to all who provided contributions.
Thanks to MP for chairing and taking minutes.

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
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
69.3	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	-
75.3	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
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.	-

Ref	Owner	Description	Target Guidance Version
77.1	OS	Investigate this moon landing accident further	
77.2	MP, PH, MT	Review proposed updates and add to list of changes to version 4.0 of the guidance	4.0
78.1	MP/MA	Investigate representation / format issues further. Consider adding another issue to the next version of the guidance on representation.	4.0
78.2	MP	Investigate data-data interactions further.	4.0
79.1	MT	Introduce EBA / EBTA with a short presentation at next meeting	
79.2	DA	Investigate the Chandryan 2 crash further and report back at next meeting	
79.3	PH	Report on use of the RADISH tool at next meeting	
79.4	PG	Re-visit the earlier nuclear data safety work using the RADISH tool	
79.5	MP	Review the DSG accident list in Appendix H and see if a better sector spread can be achieved	4.0