

SCSC Data Safety Initiative – WG Meeting 62

30th June 2021, Zoom

Minutes

Attendees

Mike Parsons (MP) – AAIP, Divya Atkins (DA) – MCA, Martin Atkins (MA) – MCA, Paul Hampton (PH) – CGI, Andy Williams (AW) – NewTechNo, Carl Tipton (CT) – Johnson Matthey, Dale Callicott (DC) – BAE, Mark Templeton (MT) – Qinetiq, Paolo Giuliani (PG) – EDF, Tim Rowe (TR) – GTR Safety Management Ltd, Richard Garrett (RG) – SQEP, Paul Mayo (PM) – SQEP, Jim Mateer (JM) – SQEP, Michael Green (MG) – Ecomergy, Nick Hales (NH) – ex-MOD, Gordon Hurwitz (GH) - Thales

Apologies

Emma Taylor (ET) - SCSC, Paul McKernan (PMcK) – Dstl, Oscar Slotosch - Validas

Agenda

- Welcome
- Buncefield, PNC & Data
- Sufficiency Issue
- Recent Accidents/Incidents
- Covid-19 and Data
- Porting of Data
- SCSC Events
- The Boeing 737 Max 8 MCAS and Nimrod MRA4 SAS – two similar solutions – two very different approaches (Talk by GH)
- 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/62nd_DSIWG_Slides_v1-1201.pptx

1. Welcome and Update

MP welcomed the group.

2. Buncefield Explosion

MP presented an update on the issue of the Buncefield explosion causing data loss. MA suggested it might make a good war story for the next guidance issue. Ref, https://web.archive.org/web/20070819153935/http://www.channel4.com/news/articles/politics/domestic_politics/buncefield+fire+destroyed+crime+data/683952

Action 62.1 (MA): Create war story for the next issue of the guidance on the Buncefield data loss

3. Sufficiency Issue

There was further discussion on the issue raised by MT around the possibility of a missing HAZOP guide word related to "Sufficiency".

For the Hazop we may need guidewords such as "Spurious", "Erroneous", "Incorrect timing" or "Unwanted duplication".

The problem could be termed "Spuriocity" or "Spuriousness" or "Unexpected" or "Unsolicited". In the end "Unexpected" is probably the best phrasing.

MP suggested that there may be parallels with 'Dark Data' which need to be explored.

Action 62.2 (MP): Consider a 'Dark Data' type of treatment for unwanted or unexpected data

It was thought that a new guidance section on messaging issues may be required, including aspects such as timing, noise, masking, CRC defeat. There are really two aspects: delivery of the unexpected message itself and then unexpected payload within the message.

Note that we can also get issues with continuous data feeds. A fundamental issue is the breaking the 'contract' between sender and receiver (as often documented in Interface Control Documents).

It was also noted that some of the existing property definitions probably need a refresh.

It was agreed to continue Action 61.1 on this matter.

4. Recent Accidents/Incidents

Some recent data-related incidents discussed were:

1. Failures in England's Test and Trace system are partly responsible for a surge in the Indian variant, <https://www.bbc.co.uk/news/uk-politics-57186059>
2. NASA Study Sheds Light On F-35 Oxygen Deprivation Symptoms, <https://aviationweek.com/awin/company/19991>
3. Deletion of Police records from legacy systems, <https://www.bbc.co.uk/news/uk-politics-57242885> and <https://www.itpro.co.uk/business-strategy/digital-transformation/359673/deleted-police-records-were-on-a-70s-it-system>
4. Woman dies after Scottish cancer screening error, <https://www.bbc.co.uk/news/uk-scotland-57596250>

5. Boeing 737 MAX and Nimrod MRA4

GH presented on the common issues and differences of the two systems designed and implemented for the two different aircraft, with the Nimrod system apparently much more engineering and safety-led, and the Boeing apparently more commercially driven. The slides are at:

[https://scsc.uk/file/gd/Safety_Forum_Presentation_130421_\(3\)-1202.pptx](https://scsc.uk/file/gd/Safety_Forum_Presentation_130421_(3)-1202.pptx)

[GH note: a key element of the SAS design was the voter monitoring logic of the data where it would start out using quadruplex logic and then following removal of one of the inputs, would start applying a triplex logic. This could be a subject for a further talk.]

See also PH's Newsletter article on the 737 MAX: <https://scsc.uk/r162:1>

6. Covid-19 and Data

The data-related aspects of the systems used to manage the virus were discussed. It was noted that Malta was refusing to use electronic records of vaccination status. Again much Covid-19 data was thought to be misleading (or misunderstood). Four new items were added to the table:

Systems involving data used to manage the pandemic			
Analysis of air flow and particles	Satellite imagery (Wuhan)	Video conferencing	Risk assessment systems
Infection / spread models inc. new variants	Itinerary systems	Remote consultation systems	Computational bioinformatics tools
Infra-red / thermal cameras	Infection testing systems	Ventilators / other patient management devices	Appointment systems
Track and Trace apps	Antibody testing systems	Personal risk profiling apps / systems	Border Control / Quarantine systems
Track and Trace back office systems	Drug trials systems / data	Allocation/reservation/ booking systems	Risk profiling / prioritising for vaccination
Track and Trace service	Ventilation models & UV sterilisers	Models of built environments	Digital Twins (systems and biological: lungs, etc.)
Supply chain systems	Behavioural models	Safety analyses (STAMP/STPA)	(Automatic) cleaning systems
Virus aerosols modelling	Analysis of delays in the system of reporting / actions	Modelling / public perception of the disease	Virus shedding models
Vaccination booking / tracking / monitoring	Sanitiser systems	Lockdown easing models	Vaccination Passports
Vaccination production data	Vaccination trials and reporting data	Vaccination 'Yellow Card'	Cross-system data sharing
PPE testing results	Data used to inform public perceptions	No coordination across international boundaries – incompatible systems	Use of blockchain to validate Covid and vaccination status

7. Porting of Data

There was a discussion of the issues of porting / importing data especially from legacy systems where there may be endian issues, format issues, translation, character set, tagging or sentinel issues. There may also be issues with being able to read the old data (i.e. media devices long gone) as well.

Action 62.3 (MP/MT): Consider issues of porting and importation of legacy data

8. Version 3.3 of DSG Update

MP said there have been 616 downloads of the DSG v3.3.

9. SCSC Events

Future SCSC events are shown below:

MP mentioned that the call for abstracts is out for SSS and he would welcome any data-related abstracts.

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

July 1, 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 ... »*

Seminar: Can we quantify risk?

September 23, 2021 - London, UK and blended online

In many areas of safety attempts are made to quantify risk. Some of these are apparently more successful than others, but some areas are notoriously difficult to quantify, especially those which ... »

Seminar: Safe Use of Multi-Core and Manycore Processors

November 11, 2021 - London, UK and blended online

This is the event postponed from 2020. It will be held in London as a blended online / in-person event

Confirmed speakers are:

Oliver Charrier, WindRiver - Multicore Processors usage ... »

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

December 2, 2021 - London, UK and blended online

This seminar will consider how to manage recovery from 'Black Swan' events in a safety context, ie. events which are rare, unexpected and have high impact. Events such as Fukushima ... »

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 ... »

10.AOB

MG noted that STAMP and associated analyses take a more holistic view and can include data elements. The STAMP workshop is currently in progress.

11.Actions, etc.

See table at end.

MP has made contact with the ISO 8000 WG lead and has joined the group.

CT provided a note and list of process-related incidents and accidents:

[Flixborough disaster - Wikipedia](#)

[Bhopal disaster - Wikipedia](#)

[Texas City Refinery explosion - Wikipedia](#)

*(nice OSA video and more detailed reports - [BP America Refinery Explosion | CSB](#))
(this is definitely a data one, persevere past the advert for the new app)*

[Buncefield fire - Wikipedia](#)

[Deepwater Horizon oil spill - Wikipedia](#)

[Piper Alpha - Wikipedia](#)

[Plant explosion in Apex, North Carolina - Wikinews, the free news source](#)

The US chemical safety board does some great videos after the investigations – all of these videos correspond to an event that could be added to the list

[U.S. Chemical Safety and Hazard Investigation Board | CSB](#)

This is a link to all of them

<https://www.csb.gov/videos/>

I find it an interesting thought process to put my data/information flow spectacles on all of them.

Eg. Poor maintenance is normally due to poor communications with management for example

Eg. Poor design can be thought of as a information flow problem. (there are nearly always better design and information available if one looks hard enough)

12.Next Meeting

Next meeting will be held 18th August by Zoom 3:30-5:00 BST.

It may be possible to hold a blended (in-person / online) meeting in September.

13.Thanks

Thanks to all participants. Thanks to MP for chairing the meeting and taking the 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
42.6	PH	Define the process to publish a document developed in Overleaf via Amazon	3.4
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	3.4
61.2	MA, MT, AW	Research the relevance of digital currencies and report back to the group	3.4
61.3	MP	Respond to Jeanette Baldwin re: ISO 8000.	N/A
61.4	CT	Send the list of process-related accidents to MP	N/A
62.1	MA	Create war story for the next issue of the guidance on the Buncefield data loss	3.4
62.2	MP	Consider a 'Dark Data' type of treatment for unwanted or unexpected data	3.4
62.3	MP/MT	Consider issues of porting and importation of legacy data	3.4