SCSC Data Safety Initiative Kick-Off Meeting

24th January 2013, Logica Kings Place, London

Notes and Actions

Attendees

Mike Ainsworth (Altran Praxis)	Alastair Faulkner (Abbeymeade)	Andrew Rankine (NATS)
Ian Bingham (Logica)	Derek Fowler (JDF Consultancy)	Felix Redmill (SCSC)
Simon Brown (QinetiQ)	Ken Frazer (KAF Consulting)	Tim Rowe (CSE International)
Dale Callicott (UKHO)	Gavin Jones (Raytheon)	Alan Simpson (Ebeni)
Paul Hampton (Logica)	Andy Kent (HP)	
Ali Hessami (Vega Systems)	Julian Lockett (Frazer-Nash Consultancy)	
Mike Parsons (Logica)	Mark Nicholson (University of York)	

Apologies: Martyn Clarke (RPS Group), Duncan Dowling (DARD Consulting), Ron Pierce (CSE International)

Statement of the Problem

It was agreed that data in safety related systems is not currently sufficiently addressed in current safety management practices and standards. It is acknowledged that data has been a contributing factor in several incidents to date. There are clear business and societal benefits, in terms of reduced harm, reduced commercial liabilities and improved business efficiencies, in investigating and addressing outstanding challenges related to safety of data.

Agreed Vision

To have clear guidance on how data (as distinct from the software and hardware) should be managed in a safety related context, which will reflect emerging best practice.

Agreed Objectives of Group for 2013

1. Produce cross-sector guidance by end of the year including a clear statement on handling of data as a separate component within safety related systems
2. Produce a high level strategic plan by the end of the year for fuller adoption e.g. into existing standards or a new standard
3. Influence standard updates currently in progress where we can
4. Actively promote and disseminate objectives and outcomes of the initiative to the wider community, professional bodies, etc.

Submissions to the Meeting

1. Email from Ron Pierce, CSE International, containing document: “Some initial thoughts from Ron Pierce, CSE International Ltd “, 23rd January 2013

2. Email from Ian Bingham, Logica, "Re: Suggested Agenda", 23rd January 2013
3. Email from Martyn Clarke, RPS Group, "Re: Provisional Agenda for Tomorrow", 23rd January 2013
4. Email from Duncan Dowling, DARD, "Fw: Kick-off meeting for SCSC Data Safety Initiative", 23rd January 2013

Key Challenge Areas

How do we define the scope of our concern?

1. What is the scope of our concern?
2. What should be included and excluded?
3. How do we take appropriate account of existing standards – should we duplicate or reference out?

Structure of the Guidance Note

1. What should the structure of the guidance note be?
2. Who is the audience for the guidance?
3. Appendix A can include the war stories

Producing the business case for adoption of the guidelines and any related standard updates

1. We need to produce war stories of previous accidents and incidents related to data
2. How do we engage and educate clients who may not understand the need for safety management on data?
3. We should focus on future known risk, emerging risks and past accidents?
4. How do we incorporate guidance – into each sector standard or publish a standalone generic standard?

Terminology and Taxonomy - how do we categorise safety related data and its properties?

1. Can we produce a universally acceptable set?
2. How do we separate data out as a separate component – do we call it 'dataware'?
3. How do we distinguish and label different categories of data such as certification data, test data, application data, configuration data, etc?
4. What are the properties of data that may affect safety e.g. performance, timeliness, integrity, accuracy, availability, etc.
5. How should use affect the definition, e.g. data used in testing?
6. The document should be generic – it may need to be tailored for specific implementations

How do we categorise and define data criticality and assurance levels?

1. How should the data criticality relate to the criticality of other components of the system?
2. What can we learn from existing practices of aeronautical data?
3. Need to understand use and the context not just the data
4. How do we handle user operational data that changes functionality?
5. How do we handle deployment configuration data changes that affect operational behaviour?

6. How do we map data criticality to data assurance methods?
7. How do you apportion assurance categorisation taking into account of architecture and other tactics – once allocated what actions should be taken?
8. Should we use a matrix style method for defining strategies for different criticalities?

What should the guidance be?

1. We should produce a strawman for what we need to do for each data assurance level
2. What can we learn from the aeronautical means of compliance work?
3. What legal caveats do we need?

How do we define ownership and responsibility and accountability across data supply chain interfaces?

1. The landscape is changing – eg. Hydrographic paper charts to electronic navigation products displayed on screens – how do we manage this increasing separation?
2. How do we deal with data confidence across interfaces and data lifecycle and ageing concerns?
3. How do we define the interfaces (architectural and people), wrappers and escalation points across boundaries?
4. How do we specify the valid configuration parameter data set?
5. How do we control data change management and ensure process integrity?
6. How do we manage the link with security?
7. How do we ensure a consistency of approach?

Other Issues

1. What specific challenges will 'big data' present in terms of aggregation and ability to verify?
2. Sectors are moving quickly to share data and move to paperless operations
3. How do we handle data lifecycles, deletion ageing, retention, etc.
4. What can we say about test data tools and data preparation tools?

What do we have already?

1. James Inge taxonomy (safety.inge.org/project.htm)
2. Dave Lunn MSc
3. Alistair Faulkner's thesis and papers
4. Some standardisation – eg. Annex 15
5. Wording in Eurocontrol website - ADQ mandate
6. Implicit assumptions in 61508
7. What else is out there to help us?
8. What data challenges and problems are there
9. What existing strategies approaches and mitigations are available now?
10. What funding vehicles are there?

Approach

1. We're not defining a software standard as such but we will eventually define mitigation strategies for specific integrity levels

2. Need to understand priorities – terminology needs to come early to base further work on
3. Need working groups to tackle specific issues with a leader to report back in 6 weeks

Actions

1. What do we have already? **(All – Andy Rankine to collate)**
2. How do we define the scope of our concern? **(All – Mike Parsons to collate)**
3. Terminology and Taxonomy - how do we categorise safety related data and its properties **(All to research – Mark Nicholson to collate)**
4. Who else needs to be involved in the initiative, eg. Automotive, Process Control, Health, Nuclear? **(All – recommendations to Mike Parsons)**
5. Can we investigate what opportunities there may be for funding this initiative? **(All)**

Topics for Future Meetings

1. Producing the business case for adoption of the guidelines and any related standard updates
2. Structure of the Guidance Note
3. What should the guidance be?
4. How do we categorise and define data criticality and assurance levels
5. How do we define ownership and responsibility and accountability across data supply chain interfaces

Next Meeting

20th March 2013, 10am – 5pm, same location, i.e. Ford Room, Logica (now part of CGI), 7th Floor, Kings Place, London, N1 9AG

References

Health standards mentioned:

- ISB 0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems, (DSCN14/2009), http://www.isb.nhs.uk/documents/isb-0129
- ISB 0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems, (DSCN18/2009), http://www.isb.nhs.uk/documents/isb-0160