Why Data Safety?

The Airbus A400M aircraft crash shows, that data can impact on the safety of systems with catastrophic consequences.
This is now a growing problem as more systems become dependent on many types of data in safety-related and safety-critical applications.
Safety data is found in many sectors and systems: everything from patient records in a hospital through aircraft navigation data, to signal configuration files on a railway.
The DSIWG is the Safety-Critical Systems Club Working Group looking at the safety implications of data which, as of today, are not well covered by existing safety standards

Resources

1 Data Safety v3.0 – The Guidance Document, http://scsc.org.uk/scsc-127C

2 Working Group Flyer, http://scsc.org.uk/file/gd-main/Working-Group-Flyer-v12.pdf

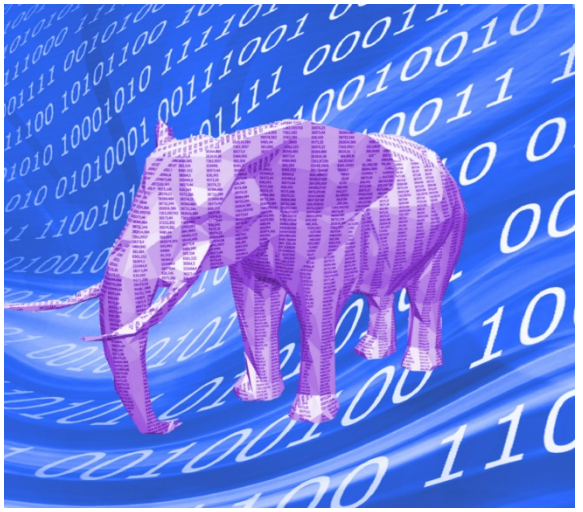
3 The Data Elephant, http://scsc.org.uk/file/gd/Hampton_-_The_Data_Elephant-339.pdf

4 Accidents and Incidents: Viewing the World through Data Eyes, http://scsc.org.uk/file/gd/Accidents_and_Incidents_-_Viewing_the_World_Through_Data_Eyes_v0.98-340.pdf

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

The Safety-Critical Systems Club



Information on Data Safety by the SCSC Data Safety Initiative Working Group (DSIWG)

February 2018

scsc.uk/groups.html

"Fatal A400M crash linked to data-wipe mistake"
- BBC News

"Config file wipe blunder caused deadly Airbus A400M crash"
– The Register

Data is here
Data is growing
Data is causing harm

The way that systems are designed and built is changing. Data was used simply to configure a system but its use is rapidly expanding and now has a huge influence on many systems. Organisations now make significant decisions based solely on data used by or held in systems. There is now a clear gap in the way data is (or is not) managed, controlled and processed. Key data properties that preserve safety are not actively managed. The use of data has grown, e.g. "Big Data" and in systems of systems, where data connects together the elements allowing a cohesive capability to be built. Mistakes introduced in data, or inappropriate use of data, are factors in a number of incidents and accidents.

Data Takes Many Forms

Data is everywhere: the configuration and adaptation files which determine system behaviour, test data used to verify a system, real-time sensor input data, application data in databases, and navigation data in the Cloud. The latest guidance document identifies no less than 23 types of safety data, plus an additional meta-type "trustworthiness".

Data Properties

There are 20 properties which need to be preserved in a safety system. These include: Integrity, Continuity, Format, Accuracy, Priority Completeness, Resolution, Traceability, History Consistency, Timeliness, Verifiability and Lifetime

The Working Group

The SCSC data safety working group is widely supported by industry, government agencies and academia, across many sectors. The main objective of the group is to develop and disseminate guidance providing recommendations and strategies on how the safety risks associated with data can be managed.
The latest technical guidance from the group can be accessed at http://scsc.org.uk/scsc-127C
The group welcomes members from organisations interested in making technical or strategic contributions. The ultimate aim is to ensure that data is properly considered alongside other contributing factors to system safety.

Key Points

- Data in safety systems presents risks - just like software and hardware
- These risks need to be managed
- Data has unique properties which need attention (e.g. lifetime and history)
- Use the data safety guidance document to help identify and control the risks

Contact Us

For further information, please contact:
Mike Parsons (mike.parsons@nats.co.uk)
Paul Hampton (paul.hampton@cgi.com)