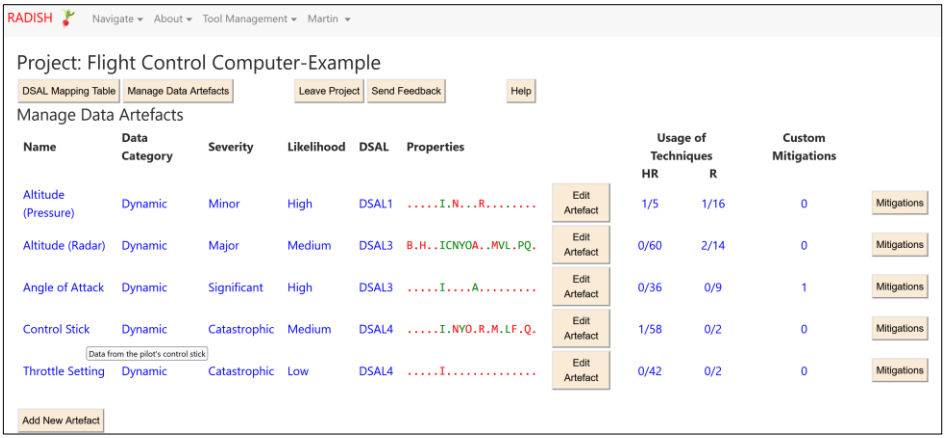
Data Safety Analysis using RADISH



The Data Safety Initiative Working Group (DSIWG) is now in its 10th year of operation and its Data Safety Guidance document has been helping engineers assess and manage data safety risks. Divya and Martin Atkins discuss a new tool that they are developing to help practitioners implement the guidance by automating many of the processes in the guidance itself.

The Data Safety Initiative Working Group (DSIWG) was the first working group to be set up under the Safety Critical Systems Club (SCSC), in 2013. With 88 members and 74 meetings later, it is still going strong, as data becomes increasingly important in safety-critical systems with every passing year. Over this period, the DSIWG has published and refined the Data Safety Guidance (Guidance) – now at version 3.5 [1], into a mature and well-regarded document, which is increasingly used in industry, and referred to by industry-specific guidance, such as the UK National Health Service's clinical risk management standards: DCB0129 [2] and DCB0160 [3], and some international safety standards, such as the upcoming version of IEC 61508 [4].

RADISH (Risk Assessor for Data Integrity and Safety Hazards) is a software tool being developed by Mission Critical Applications Limited (mca-ltd.com), to assist a data safety practitioner developing a data safety case using the Guidance, by:

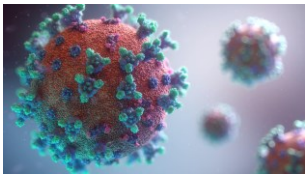
- recording the decisions that are made
- automating parts of the data safety assessment process
- helping the practitioner to choose between the risk mitigations that are recommended by the guidance, given the nature of each risk

This article provides an overview – for more information, and access to the RADISH tool, visit data-safety.tech/tooling

Data Safety

Modern Systems use data to make safety-critical decisions. Errors in, or the incorrect use of such data, can cause harm to life and the environment. Ensuring the safe use of data is a complex challenge faced by all industries, but some industries, such as healthcare, are particularly reliant on data. The risks from data will only increase as our systems become more inter-connected, autonomous, and driven by data-intensive technologies such as the Internet of Things, Artificial Intelligence and Machine Learning.

Accidents are happening...



2019 - Immensa Labs False Negative Covid-19 PCR Tests

- An estimated 1,000 deaths.

False-negative Covid test results meant that 43,000 people were not told to quarantine, further propagating the virus.

2018/19 – Boeing 737 MAX

- Lion Air Flight 610, 189 lives lost
- Ethiopian Airlines Flight 302, 157 lives lost

No redundancy of critical angle-of-attack data to the MCAS system. Also inadequate training materials, missing in-service problem reporting, and inadequate responses to failed test reports.

2017 – Irish Search and Rescue Helicopter

- Lost with all crew

Flying in zero visibility, the helicopter flew into a hill that was not in the map data loaded into its Enhanced Ground Proximity Warning System.

The Data Safety Guidance

The DSIWG publishes cross-sector best practice in the Data Safety Guidance. The Guidance describes a Data Safety Management Process, which can be integrated into an overall Safety Management System. A major part of the process involves considering appropriate mitigation techniques for each safety-related data artefact, based on the criticality and other metadata characterizing each data artefact.

RADISH: Risk Assessor for Data Integrity and Safety Hazards

Mission Critical Applications have been members of the DSIWG since 2017. They realised that the highly table-driven process to choose mitigation techniques for risks was difficult (and error-prone) to apply, and very suitable for automation. This was the basis of the development of the RADISH tool to guide a data safety practitioner through this part of the data safety process.

The formalisation of the Data Safety process needed to implement RADISH is also feeding back clarifications to the Guidance, and formalising aspects of the process.

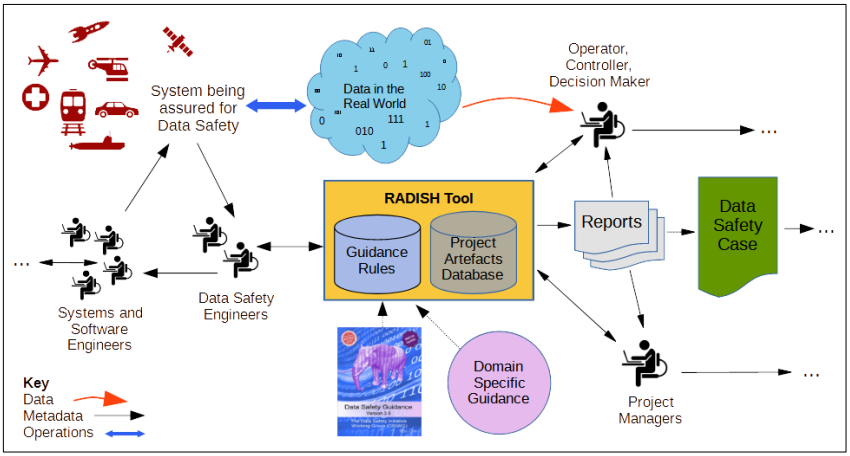
Grant funding from the Lloyd's Register Foundation made it possible to produce a proof-of-concept tool, and that is now being progressed by funding from Innovate UK.

The RADISH Tool in the context of a large development project

The RADISH tool is a central repository of information about the Data Safety case for a development project. Data Safety engineers following the Guidance, identify the data artefacts in the system, and the safety properties that are important for each artefact. The engineer chooses which mitigation techniques to use out of those recommended, or highly recommended by the guidance, adding those to the requirements of the system.

During the design and development process, RADISH can generate reports showing the risks that have mitigations, and those where more work is needed, giving project management a view of the state of the data safety process.

When the analysis is complete, RADISH can generate a report that can be included in a Data Safety Case to support the safety argument.

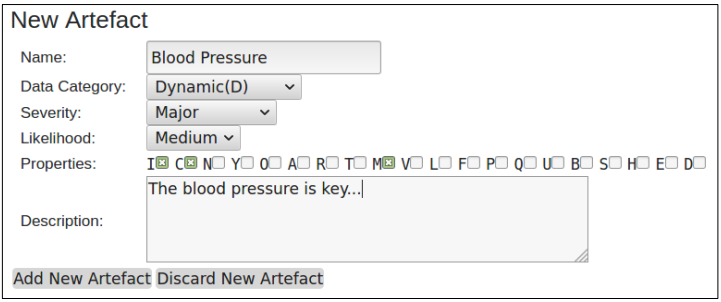


RADISH in Practice

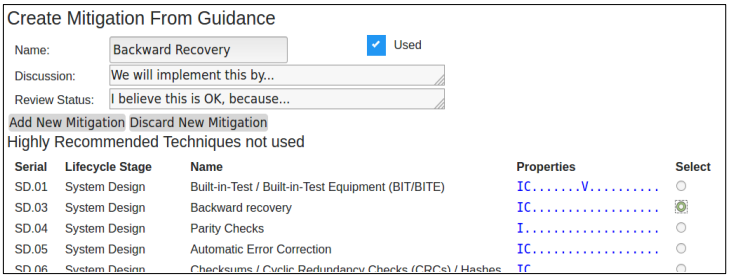
RADISH is a web-based application supporting the collection, management and maintenance of information about the safety of the data assets of a project. It records the identified data safety risks from each data artefact.

The tool also *suggests* mitigation techniques available from the Guidance, to improve the trustworthiness of the data. All risk mitigation decisions are captured along with supporting *justifications*, for inclusion in the Data Safety Case.

These steps can be seen in the screenshots below:



The first shows the creation of a new data safety artefact along with the properties of the data that need to be maintained for safety. The second shows an example of a recommended mitigation arising from the Guidance and automatically displayed by the tool.



References

[1] Data Safety Guidance, SCSC DSIWG, Version 3.5, available to download at scsc.uk/scsc-127H
[2] DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems
[3] DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems
[4] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems

Image attributions
Covid © Fusion Medical Animation | unsplash.com
Lion Air Flight 610 © PK-REN, CC BY-SA 2.0 | wikipedia.org,
Ethiopian Airlines Flight 302 © LLBG Spotter, CC BY-SA 2.0 | wikipedia.org
Irish SAR Helicopter © Riatsnapper, CC BY-SA 3.0 | wikipedia.org

Dr Divya Atkins, Managing Director, Mission Critical Applications Limited

Divya Atkins (née Prasad) has a background in Computer Science, and has conducted research in formal methods, high-integrity and real-time systems and software metrics. Her experience includes safety-critical development, and project management, and she is interested in computer and network security.

Dr Martin Atkins, Technical Director, Mission Critical Applications Limited

Martin has a research background in Object-Oriented languages, and software development experience in operating systems, embedded, safety-critical systems, and software tools. He has also managed large networks, developed hardware, taught courses and undertaken technical authoring.