Data Safety Assurance – The Emerging Challenge

Modern Systems use data to make safety-critical decisions. Errors in, or 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. The risks from data will only increase as our systems become more inter-connected, autonomous, and driven by data-intensive technologies such as Internet of Things, Artificial Intelligence and Machine Learning.

Accidents are happening…

There have already been a number of accidents and incidents, where data, as distinct from purely software and hardware, has been a major contributory factor. Some recent examples include:

0
101
01100
Caution
Data in use

Air: 2018/19 – Boeing 737MAX

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

No redundancy of critical data source, inadequate training materials, missing in-service problem reporting, etc.

Rail: 2017 – Cambrian Line

Risk to pedestrians, track-side workers

Speed restriction data not available to drivers, data was not re-loaded after system reset

Air: 2017 – Irish Search and Rescue Helicopter

Lost with all crew

Incorrect map data used

Space: 2017 – Russian Soyuz-2-1b Rocket

Fregat-M rocket and satellites destroyed

Incorrect launch site coordinates used

Health: 2008/9 – Cedars Sinai Medical Centre

206 Patients were over exposed to radiation

Incorrect use of default configuration

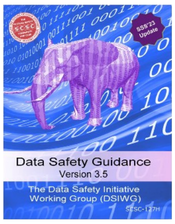
Military: 2002 – Fort Drum: Artillery range

2 shells hit mess, 2 killed, 13 injured

Artillery piece moved, but elevation not re-initialised correctly

The Data Safety Guidance

Cross-Sector best practice, has been published in the "Data Safety Guidance" (scsc.uk/scsc-127H) from the Data Safety Initiative Working Group of the Safety Critical Systems Club (SCSC). The Guidance describes a Data Safety Management Process, which can be integrated into an overall Safety Management System.



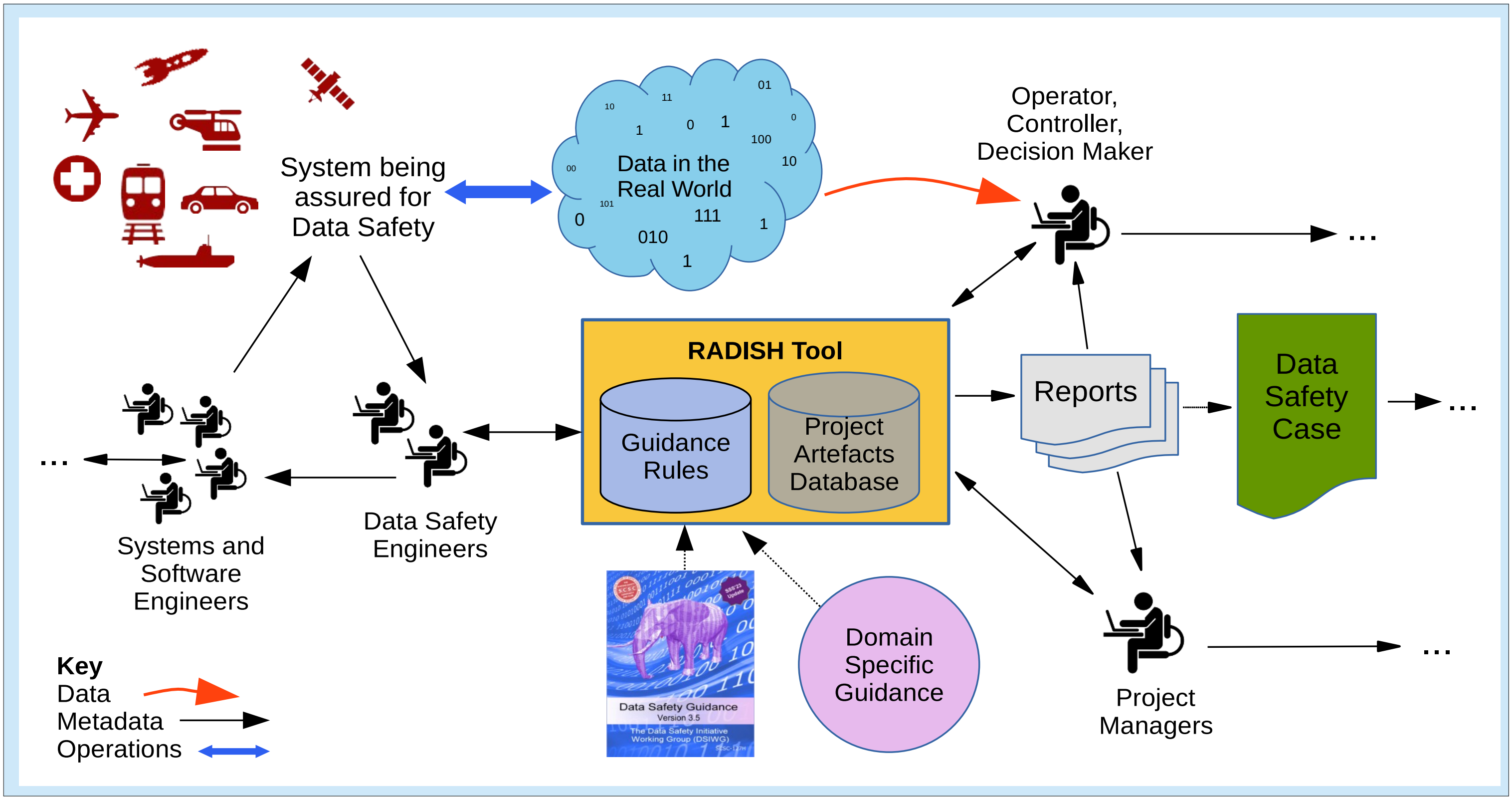
RADISH - Risk Assessor for Data Integrity and Safety Hazards

Mission Critical Applications, under grant funding from the Lloyd's Register Foundation and Innovate UK, and have developed a proof-of-concept software tool to demonstrate the **Data Safety Assurance** process. We are inviting expressions of interest from organisations who could benefit from the use, and further development of the tool.

data-safety@mca-ltd.com

www.mca-ltd.com

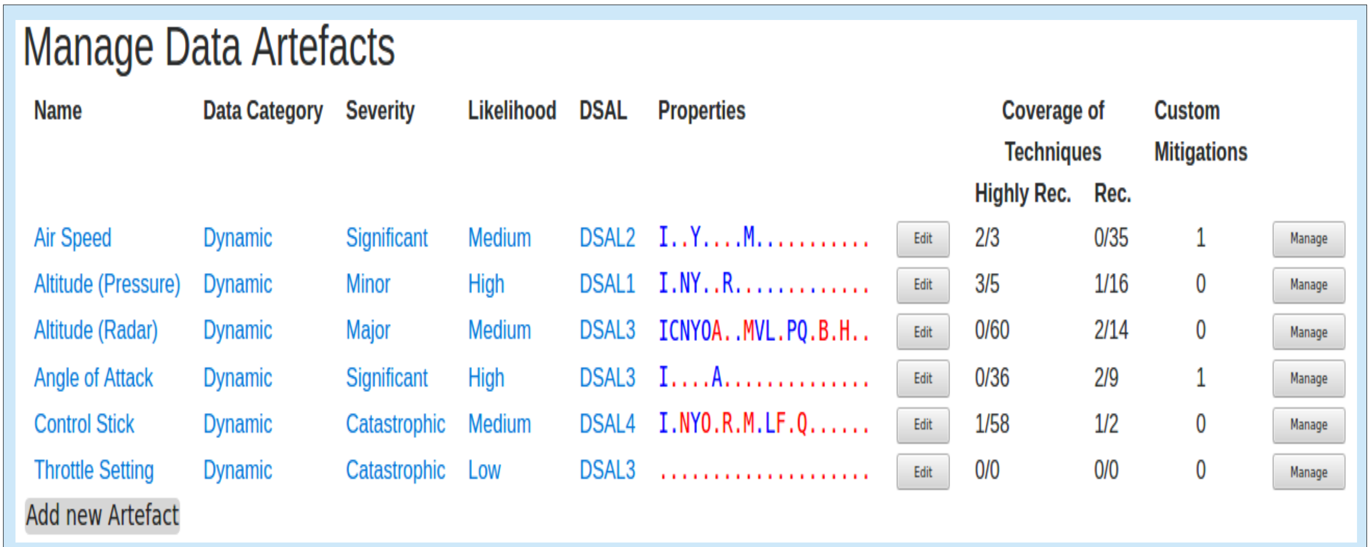
RADISH in a Project Context



RADISH stores safety properties of data artefacts, applies guidance rules to the properties, and suggests ways of mitigating the risks posed by the data. Data safety engineers identify the properties of the data artefacts, and feedback safety improvements to the systems engineers. Managers assess progress, and manage residual risk. Reports provide status and become the core of the Data Safety Case. Operators and decision makers can assess the trustworthiness of live data by querying the data safety properties stored in the tool.

RADISH

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



Manage Data Artefacts

Name	Data Category	Severity	Likelihood	DSAL	Properties		Coverage of Techniques		Custom Mitigations	
							Highly Rec.	Rec.		
Air Speed	Dynamic	Significant	Medium	DSAL2	I..Y....M...........	Edit	2/3	0/35	1	Manage
Altitude (Pressure)	Dynamic	Minor	High	DSAL1	I.NY..R.............	Edit	3/5	1/16	0	Manage
Altitude (Radar)	Dynamic	Major	Medium	DSAL3	ICNYOA..MVL.PQ.B.H..	Edit	0/60	2/14	0	Manage
Angle of Attack	Dynamic	Significant	High	DSAL3	I....A..............	Edit	0/36	2/9	1	Manage
Control Stick	Dynamic	Catastrophic	Medium	DSAL4	I.NYO.R.M.LF.Q......	Edit	1/58	1/2	0	Manage
Throttle Setting	Dynamic	Catastrophic	Low	DSAL3	....	Edit	0/0	0/0	0	Manage

An example Data Artefact Dashboard

Contact us at data-safety@mca-ltd.com for information about using RADISH.