



RADISH - Risk Assessor for Data Integrity and Safety Hazards

Errors in, or inappropriate use of data, can lead to accidents and incidents in safety-related systems. Mission Critical Applications have developed a demonstrator software tool, to manage the data risks of a system. The demonstrator conforms to current best practice, as described in the "Data Safety Guidance" (scsc.uk/scsc-1271), published by the [Safety Critical Systems Club](#). We invite you to trial the demonstrator for managing and assuring the data safety of your systems.

Features of RADISH

RADISH is a web-based application for managing safety information about the data assets of a project. It records the risks from data, and suggests appropriate mitigation techniques to improve the trustworthy use of the data. The analysis is recorded with justifications, thus providing the evidence for producing a Data Safety Case.

DSAL Mapping Table

	High	Medium	Low
Minor	DSAL1	DSAL0	DSAL0
Moderate	DSAL2	DSAL1	DSAL1
Significant	DSAL3	DSAL2	DSAL1
Major	DSAL4	DSAL3	DSAL2
Catastrophic	DSAL4	DSAL4	DSAL3

Edit

Initialise Project

Custom Data Safety Assurance Levels (DSAL)

New Artefact

Name:

Blood Pressure

Data Category:

Dynamic(D)

Severity:

Major

Likelihood:

Medium

Properties:

☒ I☒ C☐ N☐ Y☐ O☐ A☐ R☐ T☐ M☒ V☐ L☐ F☐ P☐ Q☐ U☐ B☐ S☐ H☐ E☐ D☐

Description:

The blood pressure is key...

Add New Artefact

Discard New Artefact

Data Artefacts, Categories, and associated Risks

☒ I☒ C☐ N☐ Y☐ O☐ A☐ R☐ T☐ M☒ V☐ L☐ F☐ P☐ Q☐ U☐ B☐ S☐ H☐ E☐ D☐

Control Stick

Dynamic

Catastrophic

Medium

DSAL4

I.NY0.R.M.LF.Q.....

Properties of interest for each Data Artefact

Calculated DSAL for a Data Risk

Manage Artefact:

Name:

Altitude (Radar)

Data Category:

Dynamic

Severity:

Major

Likelihood:

Medium

DSAL:

DSAL3

Properties of Interest:

ICNYOA.MVL.PQ.B.H...

Properties Covered:

ICNYO.T.VL.PQ.....

Mitigation

Technique

Properties Covered

Name	Used	Serial	Lifecycle	Name	Recommendation
CRC	Yes	SD.02	System Design	Cyclic / Continuous BIT	Recommended IC.Y.....VL.....
Formal methods	Yes	DD.09	Data Design	Formal Methods	Recommended .CN.O..T....PQ.....

Create Mitigation From Guidance

Create Custom Mitigation

Techniques used, and Properties "covered"

Create Mitigation From Guidance

Name:

Backward Recovery

☒ Used

Discussion:

We will implement this by...

Review Status:

I believe this is OK, because...

Add New Mitigation

Discard New Mitigation

Highly Recommended Techniques not used

Serial	Lifecycle Stage	Name	Properties	Select
SD.01	System Design	Built-in-Test / Built-in-Test Equipment (BIT/BITE)	IC.....V.....	<input type="radio"/>
SD.03	System Design	Backward recovery	IC.....	<input checked="" type="radio"/>
SD.04	System Design	Parity Checks	I.....	<input type="radio"/>
SD.05	System Design	Automatic Error Correction	IC.....	<input type="radio"/>
SD.06	System Design	Checksums / Cyclic Redundancy Checks (CRCs) / Hashes	IC.....	<input type="radio"/>

Selection of a Technique from a filtered list



Create Mitigation From Guidance

Name: Parity Checks Used

Discussion: This won't help because...

Review Status: Ask Fred about this...

Add New Mitigation Discard New Mitigation

Highly Recommended Techniques not used

Serial	Lifecycle Stage	Name	Properties	Select
SD.01	System Design	Built-in-Test / Built-in-Test Equipment (BIT/BITE)	IC.....V.....	<input type="radio"/>
SD.03	System Design	Backward recovery	IC.....V.....	<input type="radio"/>
SD.04	System Design	Parity Checks	I.....V.....	<input checked="" type="radio"/>
SD.05	System Design	Automatic Error Correction	IC.....V.....	<input type="radio"/>

Decision **not** to use a Recommended Technique

Create Custom Mitigation

Name: Blockchain Used

Discussion: This is a powerful technique...

Review Status: Yes, very helpful...

Add New Mitigation Discard New Mitigation

Properties Asserted: ☒ I ☐ C ☐ N ☐ Y ☐ O ☐ A ☐ R ☐ T ☐ M ☐ V ☐ L ☐ F ☐ P ☐ Q ☐ U ☐ B ☐ S ☐ H ☐ E ☐ D

Custom or Domain-specific Technique

Project Flight Control System

Leave Project

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	ICNYO...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

Add new Artefact

Dashboard of Project Data Risks

ICNTYORIMVLPFQUBSHED

DSAL Filter:

DSAL1 DSAL2 DSAL3 DSAL4

R HR R HR R HR R HR

(No current filters)

Techniques List

Serial	Lifecycle Stage	Name	Data Category	DSAL1	DSAL2	DSAL3	DSAL4	Data Properties
SD.01	System Design	Built-in-Test / Built-in-Test Equipment (BIT/BITE)	..D..	-	R	HR	HR	IC.....V.....
SD.02	System Design	Cyclic / Continuous BIT	..D..	-	-	R	HR	IC.Y.....VL.....
SD.03	System Design	Backward recovery	D	R	R	HR	HR	IC.....

Browsing and Filtering of Mitigation Techniques from Guidance

Future developments include domain-specific customisation, multiple risks for data artefacts, and much more!

Would you like to find out how to manage your data risks using our demonstrator tool?

Contact us at data-safety@mca-ltd.com



This work was supported by the [Lloyds Register Foundation](#), and [Innovate UK](#)

