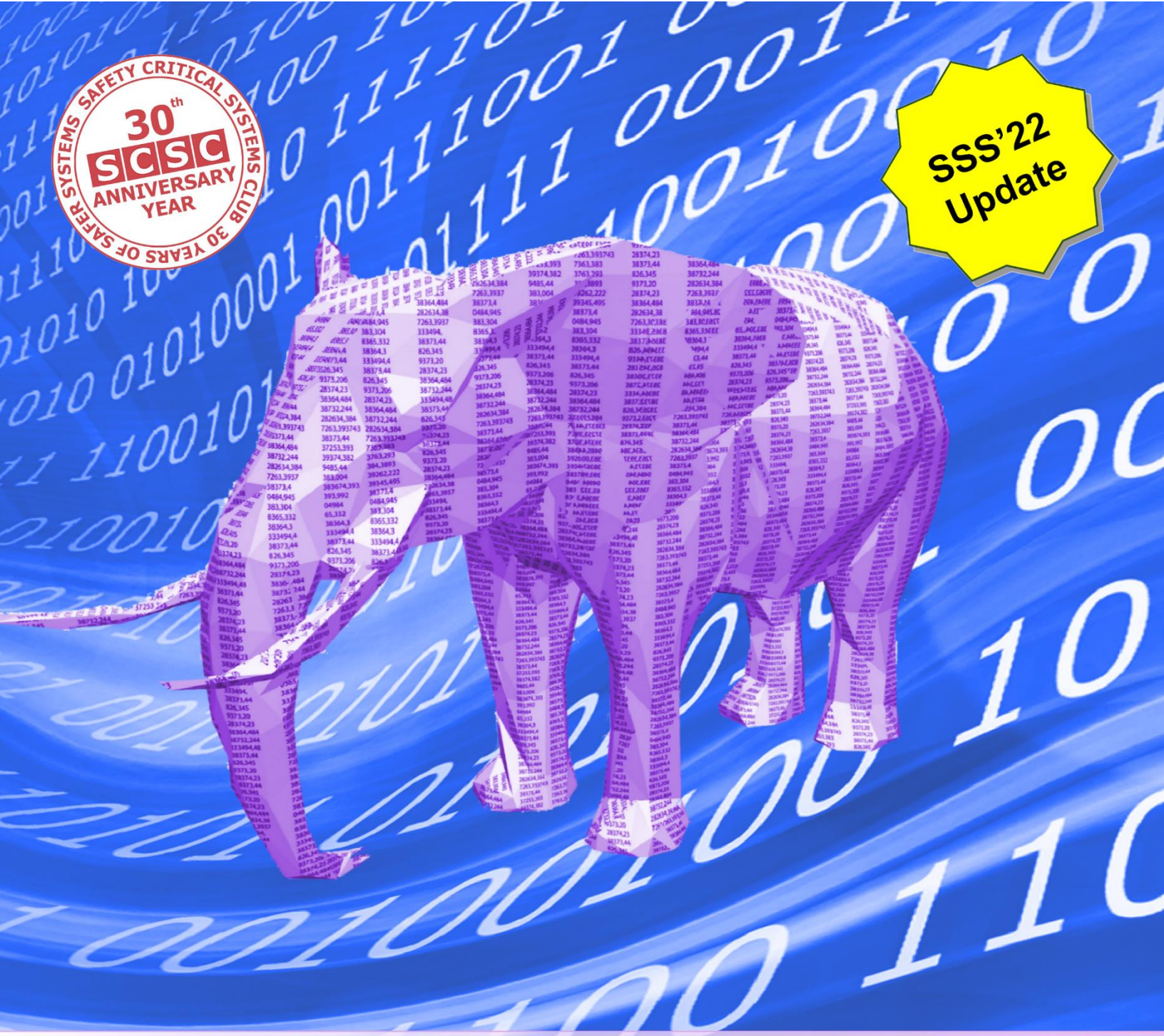


Data Safety Guidance

Version 3.4

The Data Safety Initiative
Working Group (DSIWG)

SCSC-127G

ISBN-13: 9798401357663

SCSC Publication Number: SCSC-127G

This document was prepared using the LaTeX 2_ε typesetting system.

Editing and typesetting by Mark Templeton.

Cover design by Paul Hampton.

The Safety-Critical Systems Club (SCSC) is the professional network for sharing knowledge regarding safety-critical systems. It brings together: engineers and specialists from a range of disciplines working on safety-critical systems in a wide variety of industries; academics researching the arena of safety-critical systems; providers of the tools and services that are needed to develop the systems; and the regulators who oversee safety. Through publications, seminars, workshops, tutorials, a web site and, most importantly, at the annual Safety-critical Systems Symposium (SSS), it provides opportunities for these people to network and benefit from each other's experience in working hard at the accidents that don't happen. It focuses on current and emerging practices in safety engineering, software engineering, and product and process safety standards.

This document was written by the Data Safety Initiative Working Group (DSIWG), which is convened under the auspices of the SCSC. The document supports the DSIWG's vision, which is to have clear guidance that reflects emerging best practice on how data (as distinct from software and hardware) should be managed in a safety-related context. This update takes account of the consensus that a process-based guidance document will complement existing safety management processes, making it more usable. It was formally released at SSS'22, 8–10 February 2022, details of which may be found at https://scsc.uk/e797.

Comments on this document are actively encouraged. These can be emailed to:

comments@data-safety.scsc.uk.

Alternatively, a comments submission form is available at:

data-safety.scsc.uk/comments.

Data Safety Guidance

The Data Safety Initiative Working Group [DSIWG]

February 2022

This page is intentionally blank

Change History

Version	By	Status	Date
1.0	The DSIWG Team	First draft for external review	31-JAN-2014
1.1	The DSIWG Team	(Internal edition for DSIWG use only)	09-DEC-2014
1.2	The DSIWG Team	For publication at SSS'15	23-JAN-2015
1.3	The DSIWG Team	For publication at SSS'16	29-JAN-2016
2.0	The DSIWG Team	For publication at SSS'17	30-JAN-2017
3.0	The DSIWG Team	For publication at SSS'18	26-JAN-2018
3.1	The DSIWG Team	For publication at SSS'19	01-FEB-2019
3.2	The DSIWG Team	For publication at SSS'20	11-FEB-2020
3.3	The DSIWG Team	For publication at SSS'21	09-FEB-2021
3.4	The DSIWG Team	For publication at SSS'22	08-FEB-2022

Changes Since the Last Edition

The updates incorporated within this version of the Guidance consist primarily of:

- Collection of accidents enhanced:
  - New subsection H.2: A configuration error in widely used logging software permitted remote execution of malicious code
  - New subsection H.3: 43,000 people with Covid-19 were mistakenly given negative Polymerase Chain Reaction (PCR) results
- New data category "Twinning data" added to Table 4 in section 6.1.6, and to Table 25 in Appendix E. Unfortunately, this addition has had the effect of causing the three entries for "Compliance and Liability" to be renumbered.
- Section 6.2.2 describes ways in which data can fail. The new data issue type "Distribution" has been added, to address the trend in some sectors away from the monolithic storage of data, and the move towards more distributed data storage.
- Enhancements have been made to the Guidance to address communication or messaging issues. These are:
  - New Goldilocks property added to list of data properties, to address the need for data quantity to be not too big, not too small, but just right. A brief explanation of the new property has been provided in section 6.2.3.1.
  - New HAZOP guideword "insufficient" added to HAZOP Table 7 and Table 26.
  - New Appendix L to address issues caused by obfuscation of data. This kind of data may be referred to as Dazzle Data, Distracting Data or Disruptive Data.
- Clarification paragraph added to section 6.3.1 to encourage the development of project-specific approaches, both to the assignment of Severity and Likelihood, and to their combination into a Data Safety Assurance Level (DSAL).
- Appendix J has been updated to reflect developments in machine learning governance and guidance.

- Table 28 of Appendix M has been updated to capture additional ways in which data management has been fundamental to the management of the Covid-19 virus.
- New Appendix N to suggest ways that project-specific approaches to the calculation of likelihood may be developed.
- A number of small adjustments were also made to the text, where further clarity had been recommended by users of the document.

To assist users of earlier 3.x versions of the Guidance in ensuring that their existing data safety arguments have not been impacted by this update, a version of this document is available which has been annotated with change bars. The annotated version is available at http://scsc.uk/scsc-127G.

Future work

An SCSC Ontology Working Group is currently developing a formal ontology for risk management. Once this model is sufficiently mature, the intention is to apply it to data safety risk management and thus formalise the terminology and conceptual relationships used in this Guidance. An introduction to the ontological modelling was provided in the proceedings to SSS'20 [1] and a progress update on the work was presented at SSS'22.

MCA Ltd has worked with the DSIWG to develop a prototype software tool to assist in the automation of the processes described in this Guidance document. A working version of the tool has been developed and organisations that could benefit from the use and further development of the tool are urged to contact MCA via the DSIWG.

In addition to improvements to the Guidance resulting from the work of these two sub-groups, a number of improvements to the Guidance are currently planned. These improvements are intended to clarify the application of the data safety process and include:

- the addition of a process flow diagram,
- further detail on the assurance of communications and data flows,
- aspects of data migration and importation,
- data safety considerations associated with distributed data sets and Blockchain,
- addition of new data properties, such as "Analysability", "Verifiability" and "Explainability",
- addition of new treatments to the tables in section 6,
- review of the tables of treatments, with the aim of making them easier to use,
- further explanation of some treatments, where their use or benefit is not immediately apparent,
- reordering of parts of the document to improve readability, especially as regards likelihood,
- further detail on tool assurance,
- harmonisation of language and guidance on how organisations may expand the tables to incorporate their own internal processes.
- guidance on the application of the Data Safety Culture Questionnaire,

Several of these changes are likely to cause parts of the document to be re-ordered — they have therefore been deferred to the next major update, in version 4.0 of the Guidance.

If you or your organisation are interested in learning more about the work of the DSIWG or joining either of the sub-groups, please visit the SCSC website, where more information including contact details may be found on the "Working groups" section of the site. For direct access to the DSIWG area of the site, please visit https://scsc.uk/gd

Related working groups — autonomous systems

Whilst this document aims to address data safety in as generic a manner as possible, other working groups address domain-specific safety — Autonomous Systems (AS) are the focus of the Safety of Autonomous Systems Working Group (SASWG). The goal of the SASWG is to produce clear guidance on how autonomous systems and autonomy technologies should be managed in a safety related context, throughout the lifecycle, in a way that is tightly focused on challenges unique to autonomy.

The SASWG has developed guidance on the development of the safety objectives associated with AS [2]. This document aims to provide clear, practical, guidance, including:

- There is a deliberate focus on aspects directly related to autonomy, and enabling technologies such as Artificial Intelligence (AI) and Machine Learning (ML),rather than more general safety engineering or system engineering, where it is assumed that relevant general standards, guidelines and best practice will be applied. The intent is to avoid duplicating existing guidance relating to these general topics.
- There is a deliberate focus on AS that use AI developed using ML. Although it is possible to envisage AS that do not use these technologies, AI and ML are considered to represent the greatest assurance challenges; they are also expected to be widely used.
- The guidance is intended to be widely applicable. It is not tied to any specific development approach, system lifecycle or safety argument structure.

This page is intentionally blank

Foreword

> *Data is here. Data is growing. Data is causing harm.*

Data is here: Data is becoming ever more important in our lives: influencing, managing and even controlling many critical aspects. Some of this data is related to our personal safety and well-being. Consider, for example, the importance of data defining the layout of Britain's railway signals, data which indicates the position of underwater obstructions in nautical channels or data that records a patient's treatment history. Organisations now make significant decisions (including safety-related decisions) based solely on data held in systems. Hence, organisations need to safely manage, control and process their data. In particular, key Data Properties that preserve safety must be actively managed.

Data is growing: There are at least two reasons why the use of data has grown and, equally important, why it is expected to continue to grow. The first relates to the rapid expansion of the area loosely termed "Big Data", including the use of large data sets to support machine learning and artificial intelligence applications. The second is the growing use of systems of systems, where data is the lifeblood that connects together disparate elements and allows a cohesive capability to be built. Put simply, the need to address data-related issues is a pressing problem and will continue to be so.

Data is causing harm: Strictly speaking, data can neither cause nor prevent harm. However, mistakes introduced in data, or the inappropriate use of data, within safety-related systems have been factors in a number of documented accidents and incidents. Examples include: aircraft attempting to take-off from the wrong runway (and consequently crashing); ships running aground; and patients being exposed to higher than planned doses of radiation.

Against this background, the DSIWG was established under the auspices of the SCSC. The DSIWG's aim is to develop clear, cross-sector guidance that reflects emerging best practice on how data (as opposed to software or hardware) should be managed in a safety-related context. For the most part, this guidance is based on well-established techniques, and it has been designed to be compatible with current safety standards and to integrate with existing safety management systems. What is new, however, is the explicit and relentless focus on data, making it a "first-class citizen" within system safety analyses. By doing so, this guidance should help organisations identify, analyse, evaluate and treat data-related risks, thus reducing the likelihood of data-related issues causing harm in the future.

This page is intentionally blank

Quick Start Guide

> *Data really powers everything that we do.*
> ***Jeff Weiner***

The following bullets provide a single-page introduction to Data Safety Guidance. For first-time readers this should help place individual sections within an appropriate context; it should also help returning readers quickly navigate the document's contents.

- Systems are changing. The role of data is becoming more prominent. Hence, data needs to be considered as a "first-class citizen" in system safety analyses. This will help mitigate organisational and system level risks associated with the use of data.
- A Data Safety Management Process has been developed. This is based on four phases:
  - Establish Context;
  - Identify Risks;
  - Analyse Risks; and
  - Evaluate and Treat Risks.
- The underlying principles and an overview of the process may be found in section 2.
- Definitions and abbreviations (associated with normative text) are listed in section 3.
- The objectives associated with, and the outputs produced by, each phase are provided in section 4.
- The activities of each phase (and associated tailoring information) are described in section 5.
- Additional guidance information for each phase is contained in section 6.
- A worked example is provided in section 7.
- A collection of Appendices provide more detail, including:
  - A discussion illustrating how the underlying principles link to the objectives (Appendix A);
  - An Organisation Data Risk assessment questionnaire (Appendix B);
  - A Data Safety Culture questionnaire (Appendix C);
  - A questionnaire to help assess "data maturity" of a supplier (Appendix D);
  - A list of Data Categories (Appendix E);
  - A collection of Hazard and Operability Study Guidewords (Appendix F);
  - The suggested contents of a Data Safety Management Plan (Appendix G);
  - A summary of accidents and incidents in which data was potentially a causal factor (Appendix H);
  - A discussion of topics loosely related to system lifecycles (Appendix I);
  - Considerations regarding Machine Learning (Appendix J);
  - An introduction to the concept of Dark Data (Appendix K);
  - An introduction to the concept of Dazzle Data (Appendix L);
  - Some of the data issues that made management of the Covid-19 virus difficult (Appendix M);
  - Examples of ways that DSALs may be customised, with particular focus on likelihood (Appendix N);
  - Lists of acronyms, definitions and glossary entries (Appendix O); and
  - A collection of references (Appendix P).

This page is intentionally blank

Contents

List of Tables

List of Figures

This page is intentionally blank

1 Introduction (Informative)

> *We're entering a new world in which data may be more important than software.*
> ***Tim O'Reilly***

1.1 Aim and Scope

This guidance document aims to:

- Describe the data safety problem;
- Provide methods for identifying and analysing levels of risk; and
- Recommend methods and approaches for evaluating and treating those risks.

This document has been written for a wide readership. Its target audience covers all those who have an interest in, or a responsibility for, safety-related data within systems, including: Managers, Developers, Safety Engineers, Assurers (including Independent Safety Auditors), Regulators and Operators.

The breadth of readership is also intended to cover a number of different sectors. As such, the document identifies a wide spectrum of safety-related data that exists in many forms within systems, from specification and requirements data, to maintenance and disposal data, and everything in between. In particular, this document is not just concerned with numerical or well-structured data used during system operation.

It should be noted that, whilst they are considered mature enough to be useful, the contents of the document represent current thoughts on what is a complex and evolving area. Furthermore, to allow it to be produced within a reasonable timescale, this edition focuses on key items; it is not intended to be exhaustive. For example, this guidance document does not consider issues relating to staff competence or organisational structure.

1.2 Intended Relationship to Other Documents

This document is intended to be used as a supplement to existing standards and norms that are relevant to the scope of the engineering work being undertaken. In such cases it may be used to provide a deeper insight into the risks that data poses to the project team's outputs, allowing them to produce credible improvements to the safety argument as a result. Where a standard or norm sets out specific data related objectives then, unless agreed otherwise with the regulator or safety duty holder, they shall take precedence over the guidance provided herein.

In the longer-term the hope is that future standards and norms will take up relevant concepts, approaches and methods from those described within this document. It is also hoped that organisations will include the concepts, approaches and methods in their own safety management processes.

1.3 Normative, Informative and Discursive Text

Three types of text are used within this guidance document:

- **Normative** text, which is prescriptive. Typically, this text is restricted to describing objectives and outputs.
- **Informative** text, which is descriptive text that is closely linked to the normative text. Typically, this text provides a suggested way by which compliance with the normative text may be achieved. Note, however, that alternative means of compliance are possible.
- **Discursive** text, which contains discussions that are relevant to the general topic of Data Safety, but which are not closely linked to the normative text. A discussion on the relationship between data and software is an example of such text; descriptions of historical incidents and accidents are another.

Each section (or appendix) of this guidance document contains a single text type. The relevant type is indicated in the section (or appendix) title.

1.4 Compliance

There may be occasions when it is desirable, or necessary, to make a claim of compliance against the objectives listed in this document. Such a claim may be required, for example, if this document is explicitly included as a normative reference from a formal standard. Alternatively, it may be required as part of an organisation's internal processes.

To facilitate compliance claims, the following terminology is used within the normative parts of this guidance document:

- **SHALL** denotes items where evidence of compliance must be provided in order to claim compliance with this guidance document.
- **SHOULD** denotes items where, in some circumstances, there may be valid reasons for not complying with a particular item. The full implications of non-compliance must be understood, documented and approved in order to claim compliance with this guidance document.
- **MAY** denotes items that are optional. These may be advantageous in some circumstances but not in others. Organisations are free to adopt any approach to these items without the need for further justification.

2 Principles and Process (Informative)

> *Errors using inadequate data are much less than those using no data at all.*
> ***Charles Babbage***

2.1 Data Safety Assurance Principles

Hawkins *et. al.* established some generic software safety assurance principles, which are commonly referred to as "4 + 1" [3]. Given the close links between software and data it is helpful to consider these principles from a data-safety assurance perspective. The results are detailed below, with each principle being considered in turn.

2.1.1 Principle 1: Data Safety Requirements shall be defined to address the data contribution to system hazards

Data pervades active system operation, as well as the system's specification, realisation, verification, validation, certification, maintenance, and retirement. Moreover, data may be passed from one system to another; sometimes over a significant period of time. Data may be assimilated, and converted from prior uses into new uses, or simply used as-is by many systems. It is stored in media whose storage integrity decays. The system context for Data Safety Requirements may be specific to a particular system's (or [safety] engineering process's) use of the data, or it may be generalised to a class of related systems. Hence Data Safety Requirements are needed for any safety-related system that interacts with data.

2.1.2 Principle 2: The intent of the Data Safety Requirements shall be maintained throughout requirements decomposition

Data Safety Requirements establish the system's safety properties for data, for the system's use of data, for the management of data and for the engineering lifecycle of both the system and its associated data. The system's requirements hierarchy must preserve the intent of the Data Safety Requirements (and hence the system's safety-related Data Properties). Moreover, the applied engineering process for both the system's realisation and subsequent lifecycle stages shall demonstrate that the data safety properties are preserved.

2.1.3 Principle 3: Data Safety Requirements shall be satisfied

Evidence is required that the system satisfies all of the Data Safety Requirements imposed on it for all anticipated operating conditions. Moreover, the Data Safety Requirements that pertain to the data's lifecycle outside of the system shall be evidentially demonstrated prior to the system acting on such data, or else the system shall be able to adequately defend against unmet Data Safety Requirements. In other words, either the data can be shown to demonstrate the required Data Properties prior to being used, or the system can implement adequate defences and mitigations against data that does not conform to the required safety properties.

2.1.4 Principle 4: Hazardous system behaviour arising from the system's use of data shall be identified and mitigated

This is an intentionally broad statement because data is conceptual and not physical; it is the contextualised use of data that could result in a system hazard. Data Safety Assurance Principle 1 deals with system level hazards arising from data, whereas Data Safety Assurance Principle 4 is concerned with hazards that arise from the way the system uses its data; that is, whether the system's design and implementation introduce further hazards. An example is a ship navigation system's display of hydrographic chart data, where a wide field display results in small shallow underwater features disappearing (due to image scale) when it is critical that situational awareness of such hazards is maintained.

2.1.5 Principle 4+1: The confidence established in addressing the Data Safety Assurance Principles shall be commensurate to the contribution of the data to system risk

The confidence in the evidence that demonstrates establishment of the first four Data Safety Assurance Principles shall be proportionate to the contribution data (or a particular Data Artefact) makes to the system hazards.

2.2 Data Safety Management Process

To assist organisations with integrating data safety considerations into their existing processes and, in due course, their Safety Management System, an outline Data Safety Management Process has been developed. This is structured around ISO 31000 [4], and takes into account the Data Safety Assurance Principles: links between the process objectives and the assurance principles are described in Appendix A. The adoption of ISO 31000 means that a relatively simple process, which focuses on data-related aspects, can be presented here and applied by individual organisations.

To simplify the presentation, the process is presented as a series of sequential phases. In practice, a degree of iteration is likely to be required (e.g., measures adopted to treat risks may lead to refined system design and revised risk analyses). Likewise, it may be appropriate for some parts of the process to run in parallel (i.e., a subsequent phase may start before a preceding phase has finished).

A key aim is that the Data Safety Guidance can be applied across all industry sectors and to a wide range of system types. This extensive coverage can only be achieved through tailoring: what is required for large-scale, safety-critical systems would be excessive for small-scale systems that pose significantly less risk. Suggestions for tailoring are included in this document. Alternative levels of tailoring may be adopted, if sufficient justification is provided.

Although the Data Safety Management Process is based on the structure of ISO 31000, there are some differences between the two. These include:

- The ISO standard's "Establish Context" phase is concerned with an organisation adopting a risk management system; within this guidance document that phase is extended to apply to specific projects;
- The ISO standard considers risk as being synonymous with uncertainty in outcome (i.e., some risks may be beneficial and hence it may be desirable to take actions to increase their likelihood); within

this guidance document all risks are considered to have adverse effects; and

- The ISO standard separates the "Evaluate Risks" and "Treat Risks" activities; within this guidance document it has been convenient to combine these into a single phase.

ISO 31000 also recommends two activities that run in parallel with risk assessment. These activities are: (1) monitor and review the risk assessment process; and (2) communicate and consult with the Stakeholders about the risk assessment process. Aspects like "monitor", "review", "communicate" and "consult" are taken to be part of normal project activities; items like the Organisational Data Risk (ODR) assessment and the Data Safety Management Plan (DSMP) are intended to assist from the perspective of data safety.

This page is intentionally blank

3 Definitions (Normative)

> *I love data. I think it's very important to get it right, and I think it's good to question it.*
> ***Mary Meeker***

3.1 Definitions

Table 1: Basic definitions

Term	Definition
Data Artefact	An item, or collection of items, that provides a useful perspective on data generated, processed or consumed by a system.
Data Owner	The individual or organisation responsible for a particular Data Artefact, or collection of Data Artefacts.
Data Property	A characteristic that can be exhibited by a Data Artefact.
Data Safety Assessment	The process of explicitly considering data as part of a system safety assessment, via the means of Data Artefacts, Data Properties and Data Safety Assurance Levels.
Data Safety Assurance Level	An indication of the level of rigour with which relevant Data Properties should be demonstrated for appropriate Data Artefacts.
Data Safety Requirement	A requirement to implement an approach specifically designed to achieve, maintain or demonstrate a Data Property (or Properties) for a given Data Artefact (or Artefacts).
Response	The way in which an identified risk is addressed; possible responses include avoid/eliminate, treat, or accept as sufficiently low.
Stakeholder	An individual or organisation that has some relationship to the system, possibly including a power of veto.
Treatment	An action taken to reduce or control risk.

This page is intentionally blank

4 Objectives and Outputs (Normative)

> *The goal is to turn data into information, and information into insight.*
> ***Carly Fiorina***

4.1 Establish Context

4.1.1 Objectives

1-1 System context and intended use SHALL be established.

1-2 Key Stakeholders SHALL be identified.

1-3 Data Artefacts SHALL be identified.

1-4 Interfaces SHALL be defined and managed.

1-5 A Data Safety Assessment SHALL be planned.

4.1.2 Outputs

- A description of the system and its intended use. This SHOULD include an estimate of the level of data-related risks.
- A list of key Stakeholders for data-safety activities.
- A collection of Data Artefacts, described at an appropriate level of detail.
- An interface control plan or list of control measures. This MAY include a list of Data Owners, linked to Data Artefacts.
- A plan for the remaining parts of the Data Safety Assessment.

4.2 Identify Risks

4.2.1 Objectives

2-1 Historical data-related accidents and incidents SHALL be reviewed.

2-2 Unintended behaviour resulting from data SHALL be identified and analysed.

2-3 Risks SHALL be identified and linked to Data Artefacts and Data Properties.

4.2.2 Outputs

- A description of the process used for risk identification.
- A list of risks, linked to Data Artefacts and Data Properties.
- An updated plan for the remaining parts of the Data Safety Assessment, if required.

4.3 Analyse Risks

4.3.1 Objectives

3-1 Data Safety Assurance Levels SHALL be established.

3-2 Data Safety Assurance Levels SHALL be justified.

3-3 Data Safety Assurance Levels SHALL be incorporated into system safety activities.

4.3.2 Outputs

- A Data Safety Assurance Level and supporting justification for each risk identified in the previous phase.
- An updated plan for the remaining parts of the Data Safety Assessment, if required.

4.4 Evaluate and Treat Risks

4.4.1 Objectives

4-1 Data Safety Requirements SHALL be established and elaborated.

4-2 Methods used to provide data safety assurance SHALL be defined and implemented.

4-3 Compliance with Data Safety Requirements SHALL be demonstrated.

4.4.2 Outputs

- A record of the agreed responses to each of the identified risks, along with supporting justification.
- A list of Data Safety Requirements that follow from these responses.
- A record of the treatment adopted for each of the identified risks, including evidence that the treatment has been successfully implemented.
- An assessment as to whether the risk has been suitably mitigated (and, if not, plans for further mitigation activities).

5 Activities and Tailoring (Informative)

> *It is a capital mistake to theorise before one has data.*
> ***Sherlock Holmes - "A Study in Scarlet" (Sir Arthur Conan Doyle)***

5.1 Establish Context

5.1.1 Overview

This phase involves developing: an understanding of the context within which the system development occurs; an understanding of the system requirements; and an understanding of the system design. These factors help determine the risk appetite; that is, essentially, how much effort will be devoted to making risks as low as practicable. In turn, this will inform the nature and scope of assessments that are conducted during system development, introduction to service and operation. The factors also help identify Stakeholders.

5.1.2 Activities

There are four activities associated with this phase.

5.1.2.1 Describe the organisational context

Part of this activity involves understanding the Stakeholders involved, or with an interest, in the system. It is important to define how the Stakeholders will interact and the derived requirements applicable to each Stakeholder through interface control, similarly to systems engineering interface control procedures already in place in many industries. Consideration of external (e.g., economic, social, regulatory) and internal (e.g., culture, processes, strategy) factors is key to defining appropriate interface control measures. Note that, similarly to requirements, interface control may be iterative throughout the Data Safety Assessment. In particular, interface control may need to be amended to take account of implemented data safety mitigations.

To form a high-level understanding of each organisation's risk, the Organisational Data Risk (ODR) assessment (Appendix B) can be used. The ODR assessment can be used at programme level to cover all Stakeholders, or used by each individual Stakeholder to determine the risk appropriate to their area. Note however that care should be taken when adopting such a formulaic approach to risk assessment to ensure that the resulting system can meet its cumulative requirements; that is, nothing has "fallen through the cracks". This is part of the requirements decomposition and verification / validation activities described later in the Data Safety Management Process.

Amongst other things, the ODR assessment includes: the severity of any potential accidents; organisational maturity; applicable legal and regulatory frameworks; and the size, complexity and novelty of the planned system. It results in a rating, from ODR0 (which corresponds to the lowest risk) to ODR4 (which corresponds to the highest risk). This rating provides an initial, top-level view of the magnitude of data-related risk. As such, it could form the basis for process tailoring; it also gives an indication of the proportionate magnitude of effort that may be required in the management of data safety risks.

To allow tailoring to be applied in cases where the ODR assessment has not been explicitly conducted, the

qualitative scale presented in Table 2 is also used.

Table 2: Qualitative definition of ODR

ODR Rating	Qualitative Description
ODR4	High-risk
ODR3	Medium-risk
ODR2	
ODR1	Low-risk
ODR0	Very low-risk

Note that, in the case of an ODR0, no further work is required.

In addition to the rating, the ODR can be used to facilitate the identification of key Stakeholders (i.e., those with an interest in the system) and necessary approvers (i.e., those who need to formally accept the system). Note that some approvers might be within the organisation, whilst others may represent external bodies. Likewise, approvers could also be customers or regulatory authorities.

Part of the process of establishing the internal context involves understanding organisational culture. A short Data Safety Culture questionnaire has been developed (Appendix C), which may help in this regard. This can be applied at an organisation level or, more likely, within an individual project team. The questionnaire could also be used to highlight the importance of data safety related issues within a project team. In addition, before and after measurements could be taken to establish the effectiveness of data safety related training.

5.1.2.2 Describe the system context

This activity is concerned with describing the system under analysis, as well as the key external influences on that system (examples of which include interfacing systems and human operators). There are obviously many aspects to this activity. For reasons of brevity only those aspects that are directly relevant to data safety are discussed here.

When describing the system it is often helpful to think in terms of producers and consumers of data. These may be external systems, or sub-systems, or a combination of both. In addition, it may be necessary to consider data supply chains, especially when there are a number of separate organisations involved. Note that the considerations discussed in this paragraph are intended to be addressed at a high level: the identification of specific pieces of data is a separate, but related, activity; the identification of required properties is another activity.

Also note that, as development progresses the system description is expected to be refined. This may enable the data safety system context to also be refined, supporting the Data Safety Assessment planning.

5.1.2.3 Plan the assessment

This activity involves scheduling the phases associated with the Data Safety Management Process and acquiring the necessary resources to complete them. This also involves tailoring the generic process to meet the specific needs of a particular system development.

Details of the planned assessment may be recorded in a Data Safety Management Plan (DSMP). This could also be used to capture the scope of the analyses and the associated context. Together, this information constitutes the first section of the DSMP structure. Note that if a DSMP is created, it would be expected to be updated with details from subsequent phases. Alternatively, if a Safety Management Plan has already been developed for the project, data safety aspects may augment the existing Safety Management Plan.

Planning of the Data Safety Assessment requires some knowledge of the quantity and complexity of data that requires assessment. Therefore, the DSMP (or Safety Management Plan) needs to be updated in subsequent phases once these details are known.

Planning of the assessment may be done through a procurement process. Procurers may wish to understand their potential supplier's understanding of data safety and plans to implement a Data Safety Assessment. A Data Safety Supplier Questionnaire (Appendix D) has been developed to support this analysis; this questionnaire may also be used for auditing purposes.

5.1.2.4 Identify Data Artefacts

Data Artefacts are the key pieces of data that are generated, processed or consumed by the system. They provide the foundation for the remaining phases of data-related risk management.

To support the identification of Data Artefacts, a wide variety of Data Categories have been enumerated. Cross-referencing these categories against the system description should highlight the relevant artefacts.

Another way of identifying Data Artefacts involves considering the functions that the system performs and establishing the data that is required to support these.

A further option for confirming that all relevant Data Artefacts have been identified is to consider the different phases of the system lifecycle. This approach should help prevent an inappropriate focus on operational use of the system at the expense of, for example, artefacts associated with system test and evaluation.

5.1.3 Tailoring

The level of stakeholder interface control required will depend heavily on the number of Stakeholders, complexity of their interactions, and the contractual controls already in place. Many programmes already require Interface Control Documents (ICDs) to be developed for systems or equipment. The level of detail required in other programme interface control plans may be used as a guide for the requirements of data safety interface control.

The guidance in this document is general in nature and so it is anticipated that it will need to be tailored to align with the organisation's attitude to risk, their existing processes and the relevant sector's regulatory environment. Thus the provided ODR, or a version customised to suit the organisation's needs, may provide a structured approach to assessment. The ODR assessment can be conducted at product line or individual product level, as appropriate for the organisation. It is generally not recommended to conduct the ODR without the context of a system type.

It is expected that the ODR assessment will be of most utility for organisations that do not have significant safety engineering experience and that are operating in less well-regulated industrial sectors. Organisations with considerable experience in the development of safety-critical systems in heavily regulated environments may also find it of use in defining the context from a data perspective and

augmenting existing safety standards which have no explicit data considerations. Note that if this assessment is not conducted, some high-level qualitative estimate of risk may still be required (e.g., to support process tailoring); likewise, there will also be a need to identify key Stakeholders and necessary approvers.

It is also expected that the Data Safety Culture questionnaire will be of most use for low-risk (i.e., ODR1) systems. In particular, it is expected that developers of higher risk systems will have extant processes to develop, maintain and monitor safety cultures, although the data-oriented questionnaire could help inform those existing processes.

The approach of including data-related aspects within a Safety Management Plan is recommended for complex or highly safety-critical systems. In this case the structure of the Safety Management Plan may be maintained, with the Data Safety Assessment process being tailored to align to the overall safety assessment process.

The questionnaire that helps establish the level of "data maturity" in potential suppliers is expected to be of most use when new organisational relationships are being formed. Conversely, it may offer little value in situations where both organisations are familiar with each other, they have worked on data-related projects together before and there are suitable audit / review arrangements in place.

Data Artefacts may be defined at a number of levels. An artefact associated with a medical system could be described as "patient data". Alternatively, this could be split into smaller parts (e.g., "blood group"). Generally speaking, the highest possible level consistent with the system description should be used; this prevents an excessively long list of artefacts being developed. If necessary, those artefacts where further detail is needed can be refined as part of an iterative process that is focused on key issues.

Not every Data Category will be relevant to every system. Furthermore, for low-risk (ODR1) systems it may be sufficient to simply consider the groupings of categories (e.g., "context", "implementation", etc.). Conversely, high-risk (ODR4) systems might need to consider every category, even if this results in a conclusion that a specific category is not relevant for the system in question.

A function-based approach to identifying Data Artefacts is likely to be enabled by design processes that also adopt a function-based perspective. If information from a function-based perspective is readily available then it should be used to support the identification of Data Artefacts. If this information is not readily available, it is recommended that it be generated for medium and high-risk systems (i.e., ODR2 to ODR4, inclusive).

Considering data across the system lifecycle is a relatively simple activity, which is applicable to all systems (i.e., ODR1 to ODR4, inclusive).

5.2 Identify Risks

5.2.1 Overview

This phase involves identifying sources of risk and understanding the potential consequences; it should result in a comprehensive list of risks. From a system development perspective, these activities are likely to be concurrent with the development of more detailed system designs.

5.2.2 Activities

There are three, complementary, activities that can be used to identify risks. There is also an activity associated with updating planning documents.

5.2.2.1 Review the general, historical perspective

Some insight into potential risks may be gained by reviewing historical accidents and incidents, a collection of which is included in Appendix H of this guidance document. It is expected that each domain would have its own catalogue of historical incidents, which can be consulted during a data-focused review.

5.2.2.2 Conduct a top-down approach

If the system under consideration has clearly identified functions then data-related risks can be assessed by considering each function in turn and analysing what Data Artefacts and, more particularly, what Data Properties the function depends on.

If there are a limited number of safety-related functions, this is usually the simplest approach. This approach also has the advantage that it integrates well with other function-based, top-down approaches to assessing system safety.

5.2.2.3 Conduct a bottom-up approach

This approach starts from the Data Artefacts and explores the effects of data errors. In this context an error is a situation where a required Data Property is not exhibited. This may be achieved by a variety of methods, including a Hazard and Operability study (HAZOP).

5.2.2.4 Update planning documents

Once the data safety risks have been identified, the Data Safety Management Plan (or Safety Management Plan) requires review to determine if it needs updating to take account of the quantity and complexity of the analysis and mitigation activities needed to address the risks. While the DSMP may be updated throughout the Data Safety Assessment, updates may not be required for all projects.

5.2.3 Tailoring

The general, historical perspective review is a simple activity that does not require significant resources. Hence, it is recommended for all systems, regardless of risk level.

When conducting a bottom-up approach, it may not be appropriate to explicitly consider every possible property for every single artefact. In particular, for low-risk (ODR1) and medium-risk (ODR2 / ODR3) systems some form of tailoring may be expected: this may, for example, take the form of pre-selecting the properties that are most relevant, or limiting the layer of abstraction at which the system is considered.

Tailoring of the bottom-up approach may also be appropriate for some high-risk (ODR4) systems, but in this case an explicit argument that the tailoring has not adversely affected system safety would be expected. Furthermore, the risk identification process for high-risk (ODR4) systems is expected to be

a highly structured affair. To support this, a number of data-related HAZOP Guidewords have been determined and are presented in section F.

The top-down and bottom-up approaches provide different perspectives when attempting to identify data-related risks. For low-risk (ODR1) systems it may be appropriate to consider just one of these perspectives. Conversely, both perspectives would be expected to be considered (to some degree) for medium-risk (ODR2 / ODR3) and high-risk (ODR4) systems.

5.3 Analyse Risks

5.3.1 Overview

This part of the risk management process involves developing an understanding of the consequences and likelihood of each risk. From the perspective of safety-critical and safety-related systems this understanding allows System (or Safety) Integrity Levels or Development Assurance Levels to be determined. Likewise, this understanding should be used to allocate Data Safety Assurance Levels (DSALs).

5.3.2 Activities

There are two activities associated with this phase.

5.3.2.1 Establish DSALs

The key activity in this phase is to establish the (untreated) likelihood and severity of each risk identified in the preceding phase.

To analyse risks and, more particularly, to align data safety with other risk management processes, there is a need to overcome problems stemming from the use of the term "likelihood" in situations where there may be no failure rates. For this reason the DSAL was developed. The DSAL metric is not a statistical measure of likelihood, or a literal numeric measure of integrity. Instead, the DSAL metric is an indicator for the level of rigour that an assurance argument requires. As such, DSALs share a common theoretical basis with concepts like Item Development Assurance Levels [5] and development process systematic capability [6].

DSALs are measured on a scale of DSAL0 (lowest-assurance) to DSAL4 (highest-assurance). They are typically allocated as indicated in Table 3.

Table 3: DSAL "risk" matrix

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

Definitions for Severity and Likelihood associated with Table 3 may be customised for a specific application. A default approach to the assessment of Likelihood is presented in section 6.3.1 and Table 8, whilst default definitions for Severity are presented in Table 9.

Although this allocation of DSALs is typically used, it is acknowledged that there are some situations where a different allocation matrix may be more appropriate. Hence, it may be appropriate for a tailored allocation matrix to be used. Regardless of whether tailoring is used, the matrix should be reviewed and confirmed as being suitable for the intended application.

As their name suggests, DSALs are focussed on safety concerns. However, the framework of Data Artefacts, Data Properties, and so on, developed in this document could also be applied to other concerns. It could, for example, be used for to control data-related financial risks, or data-related reputational risks. In these types of approach, the severity terms would obviously relate to financial and reputational consequences, rather than safety ones.

It is possible that the additional understanding developed during this part of the process may mean some previously identified Data Artefacts are no longer of consequence; similarly, it is possible that this process may identify additional artefacts or a need to refine the description of existing artefacts.

5.3.2.2 Analyse DSALs as part of system safety activities

Allocating a DSAL is a significant part of controlling data safety risks, but it is not the only part. It is important that DSALs are considered as part of wider system safety activities, rather than being viewed as a separate item.

For medium-risk (ODR2 / ODR3) and high-risk (ODR4) systems it is likely that integrity, or assurance, levels will be calculated from perspectives other than data safety. Possible examples include Item / Function Development Assurance Levels from Aerospace Recommended Practice (ARP) 4754A [5] and Safety Integrity Levels from IEC 61508 [6]. Where such an approach is used, the mapping to DSALs should be included within the DSMP.

This activity involves comparing DSALs with these other integrity, or assurance, levels. Assuming a typical scenario of a system processing or manipulating data flowing through it, there are two cases to consider:

1. Can the data affect the software? In particular, this question is concerned with whether the data can affect the software such that the safe operation of the system is jeopardised. Obviously an ideal system would be able to handle any data fed into it safely without problems, but this is often not the case. An example might be a legacy system which has limited error checking and so may fail in unsafe ways if fed with data which is outside of the expected range. Formally this question can be stated as: *Given a system containing software written to a particular Software Assurance Level (which may be none), what should the DSAL of the processed data be to preserve correct operation of the system?*
2. Can the software affect the data? In particular, this question is concerned with whether the system's software can affect the data being processed or manipulated in such a way that Data Properties that are important for safety might be lost. Some examples might be systems which transform messages, losing any associated checksum protections, thereby possibly affecting the integrity of the data within the message; as a minimum, this removes a means of checking data integrity. Another example might be a system that can delay data flowing through it, (e.g., due to buffering) when timely delivery of the data is critical. Formally, this question can be stated as: *Given data at a particular DSAL, what should the Software Assurance Level of the software in the system be in order to preserve the DSAL of the data?*

5.3.3 Tailoring

DSALs can be applied at different levels and to different constructs. For example, in the case of simple, low-risk systems it may be appropriate to apply a single DSAL to an entire system. Alternatively, it may be appropriate to apply DSALs to sub-systems, for example, to match the level at which other integrity, or assurance, levels have been determined.

Another option is to apply DSALs to Data Artefacts rather than directly to risks. This approach has the advantage that treatments are often related to artefacts; it can work well where there is a simple relationship between artefacts and risks.

5.4 Evaluate and Treat Risks

5.4.1 Overview

This phase involves deciding, at a generic level, what action (if any) should be taken for each of the risks identified in preceding phases. This decision will be influenced by the organisation's risk appetite and other factors determined as part of the Establish Context phase. From some perspectives it may seem strange that requirements are identified at such a late phase. This is a consequence of explicitly linking Data Safety Requirements to risks associated with Data Properties of Data Artefacts, and the use of Data Safety Assurance Levels to describe levels of rigour.

This phase also involves identifying, implementing and verifying treatments for the risks emerging from the previous phase. Part of verifying the treatment involves checking technical details of the chosen approach; another part involves re-assessing the post-treatment risk to determine whether it is now acceptable.

5.4.2 Activities

This phase involves reviewing each risk, including the associated DSAL, and determining the appropriate response. Essentially, this phase aims to answer the question: can we accept this risk or does some action need to be taken? This is likely to require discussion amongst a number of Stakeholders. From a system-safety perspective, there is nothing intrinsically special about data-related risks. Hence, it is recommended that evaluation of data-related risks be conducted alongside the evaluation of other system risks, as part of an organisation's standard risk evaluation process.

Risks may be managed in different ways, for example:

- Avoid

  Risk avoidance can be employed where a risk can be eliminated by using different approaches to the design and / or operation of the system. It may also be the case that very significant risks cannot be adequately treated and the only option is to avoid the untenable risk by not proceeding with the project.

- Accept

  For low likelihood and low severity risks (e.g., those ranked as DSAL 0), where the cost of further risk reduction is judged to be unacceptable, the risk may be accepted as-is and managed as such. Appropriate justification is likely to be required for acceptance of risks ranked higher than DSAL 0.

- Transfer

  In this case ownership of the risk's consequence is transferred to another organisation. This can be achieved, for example, by taking out an insurance policy. It is important that any such risk transfers are formally documented, understood and agreed by both parties.

- Treat

  In this case there is a desire to reduce the risk. This can be achieved by reducing the severity, or the likelihood or both. Choosing this response often involves having an outline view of how the risk may be reduced.

In addition to deciding on and documenting the appropriate response to each risk, this phase also includes gaining approval for these decisions.

In cases when a decision is made to treat a risk, suitable methods and approaches should be identified. To assist in this process, a range of potential methods and approaches are included in this guidance. These are mapped against DSALs, Data Properties and a selection of lifecycle data categories.

Once a treatment strategy has been established and implemented there is, of course, a need to determine whether the expected risk reduction has been achieved. Equivalently, there is a need to consider whether the residual risk may now be accepted (or whether another one of the responses identified above is necessary).

5.4.3 Tailoring

It is expected that records will be kept of the discussions that occur as part of risk evaluation. For low-risk (ODR1) systems, this may be in the form of a brief memo. Conversely, for high-risk (ODR4) systems, a detailed, structured record, which is placed under formal control, may be expected; in this case these discussions may be recorded as part of the system's Hazard Log or as part of a Data Safety Management Plan.

As outlined in section 5.3.3, DSALs can be applied at varying levels of abstraction. For small-scale or low-risk (ODR1) systems it may be appropriate to consider treatments at higher levels of system abstraction. For example, this could involve applying a single DSAL to a sub-system or even to the system in its entirety and implementing risk treatment techniques at that level. The latter approach could be appropriate where the data in the system interacts in complex ways and the associated safety risk does not warrant a detailed investigation of these interactions.

A significant amount of tailoring is implicit in the way the tables of methods and approaches are constructed. At best a method / approach may be Highly Recommended as a way of maintaining a required Data Property at a given DSAL. In addition, the tables are not exhaustive; additional, or alternative, methods and approaches can be used.

This page is intentionally blank

6 Guidance (Informative)

> *I wanted to separate data from programs, because data and instructions are very different.*
> ***Ken Thompson***

6.1 Establish Context

6.1.1 Interface control

The interfaces between Data Owners, and indeed data ownership itself, can be much more complicated than for hardware or software, where the owner can be clearly identified. Indeed, when combining items from various sources it is possible to create data for which there is not an "owner" in any traditional sense. In such circumstances it may be appropriate for the overall system owner to take responsibility for the collected data and, where appropriate, pass specific, formally-recorded requirements onto original data suppliers.

The Data Owners throughout the lifecycle of data within the system should be identified, or the lack of an owner highlighted where applicable, including where data is merged or modified through the system operation. This will facilitate a greater understanding of the "controllability" of data safety issues within the assessment at a particular organisational level.

6.1.2 Organisational Data Risk Assessment Form

The Organisational Data Risk (ODR) Assessment Form was generated to capture a high-level perspective on the risk posed to an organisation by data safety issues within a specific project. How it integrates with an organisation's existing risk (or safety) management processes is the responsibility of the implementing organisation. However, it is anticipated that the form could be used to facilitate tailoring of the data safety guidance process. To facilitate this integration, the following paragraphs describe the connections between the ODR and the ISO 31000 [4] standard for risk management. The ODR itself is presented in Appendix B.

Establishing the context of a risk assessment ensures that the system being considered and the scope of any assessment is well defined. This helps prevent an overrun of the assessment's boundaries and allows those items that are out of scope to be explicitly communicated to all Stakeholders. In addition, it is the role of this activity to produce the criteria that a system will be judged on. The ODR assessment links directly to the sub-tasks identified by ISO 31000 for establishing the risk assessment context and introduces aspects to guide the assessor into focusing on data-specific risks.

Questions 2, 3 and 4 of the ODR align directly with establishing the external context of the risk assessment (Activity 6.3.3 from ISO 31000). They guide the assessor into judging the risk appetite of external Stakeholders, the level of risk that is allocated to the organisation and the regulatory environment within the project will operate.

Question 5 is concerned with establishing the internal context of the risk assessment (Activity 6.3.3), inviting the assessor to comment on the maturity of the organisation in terms of their attitude not just to risk, but specifically to data-driven risks.

Question 6 explores data ownership through the use cases of the system. This is related to the legal frameworks explored in Question 4, but also acts to lay the foundations of Activity 6.3.4, "Defining Risk

Criteria", which requires an assessor to identify "the nature and types of causes and consequences that can occur and how they will be measured". This is expanded upon by Questions 1, 7 and 8 which go into data-driven specifics about failure consequences and the issues raised by data complexity, boundary complexity and system complexity for the project.

Finally, the scoring system of the ODR provides a heuristic for defining the risk criteria (Activity 6.3.4) which handles how to combine these different aspects of risk into a single, high-level estimate of the data-related risks associated with a given project. This means that the ODR can, for example, provide some guidance on Data Safety Assurance Principle "4 + 1"; that is, it provides some guidance on the amount of effort that should be directed towards the management of data safety issues.

It is of note that whilst the completion of an ODR fits within the context establishment activity it also augments the ongoing "communication and consultation" activity both by providing a standardised format for capturing the relevant information and securing endorsement.

6.1.3 Data Safety Culture Questionnaire

Part of the ODR assessment relates to assessing the organisation's maturity in managing data safety risks; responses are aimed at establishing the depth of awareness of data safety and the associated management processes within the organisation. However, measuring the level of awareness of processes and concepts in an organisation is not always easy. There may be sufficient high-level knowledge of this for the purposes of the ODR but it still may be an area that warrants further investigation.

To support this, a separate questionnaire has been developed to explore the specific area of measuring the data safety culture for a particular activity; whether this be for the organisation as a whole or for a particular project, service or activity. However, here the focus is on a personal view rather than a project or company view so the questionnaire would be completed by all, or a significant subset of, staff. Responses can be aggregated to give an overall data safety culture value. A key aspect of this approach is that it can be periodically repeated to determine trends: for example, if overall scores are declining, this may suggest that further training and briefings will be required.

More details on the Data Safety Culture Questionnaire are provided in Appendix C.

6.1.4 System Definition

The system under consideration should be understood and documented, including interfaces and safety-related data aspects. The process of documenting the system of interest furthers the understanding of Stakeholders and approvers so they can make sensible judgements about the system. It also formally declares assumptions that are being made whilst assessing the system and clearly defines the limits of the assessment. In addition, different levels of risk may be associated with composites of safety-related data, which may be easier to manage than individual artefacts, or where independence cannot be demonstrated or maintained. Hence, the partitioning of data sets should also be considered during this phase.

6.1.5 Supplier Data Maturity

As noted above, a number of usage scenarios involve data being supplied by subcontracted organisations. It is expected that some formal process will be used to select these suppliers. A questionnaire has been developed to help ensure that the supplier has suitable processes in place to manage data safety-related

issues. This is available in Appendix D.

6.1.6 Data Categories

The full set of Data Categories which can have safety implications is large: to date more than twenty categories (and one meta-category) have been identified.

The table below gives the current view of the categories of safety-related data that contribute to, are used by, produced by or affected by safety-related systems. They are roughly organised into a number of categories, which aim to cover all aspects of the system lifecycle. Note that the list in Table 4 is non-exhaustive. Also note that a more detailed version of this table is available at Appendix E, where further detail on each entry is provided.

Table 4: Categories of safety-related data: concise definitions

No.	Category	Description
Context		
1	Predictive	Data used to model or predict behaviours and performance
2	Scope, Assumption and Context	Data used to frame the development, operations or provide context
3	Requirements	Data used to specify what the system has to do
4	Interface	Data used to enable interfaces between this system and other systems: for operations, initialisation or export from the system
5	Reference or Lookup	Data used across multiple systems with generic usage
Implementation		
6	Design and Development	Data produced during development and implementation
7	Software	Data that is compiled (or interpreted) and executed to achieve the desired system behaviour
8	Verification	Data used to test and analyse the system, specifically to determine whether it has been built as intended
Configuration		
9	Machine Learning	Data used to train the system
10	Infrastructure	Data used to configure, tailor or instantiate the system itself
11	Behavioural	Data used to change the functionality of the system
12	Adaptation	Data used to configure to a particular site
Capability		
13	Staffing and Training	Data related to staff training, competency, certification and permits
The Built System		
14	Asset	Data about the installed or deployed system and its parts, including maintenance data
15	Performance	Data collected or produced about the system during trials, pre-operational phases and live operations
16	Release	Data used to ensure safe operations per release instance

Continued on next page

Table 4: Category of safety-related data: concise definitions (continued)

No.	Category	Description
17	Instructional	Data used to warn, train or instruct users about the system
18	Evolution	Data about changes after deployment
19	End of Life	Data about how to stop, remove, replace or dispose of the system
20	Stored	Data stored by the system during operations
21	Dynamic	Data manipulated and processed by the system during operations
22	Twinning	Data used to create and maintain a digital counterpart of a physical object or process
Compliance and Liability		
23	Standards and Regulatory	Data that governs the approaches, processes and procedures used to develop safety systems
24	Justification	Data used to justify the safety position of the system
25	Investigation	Data used to support accident or incident investigations (i.e., potential evidence)
Meta-Property		
+1	Trustworthiness	(Meta) data which tells us how much the system can be trusted

6.2 Identify Risks

6.2.1 Historical Accidents and Incidents

Ideally, data safety risks would be identified and mitigated before they led to an accident or incident. However, this is not always the case. Historical occurrences can provide an indication of the data safety risks present in planned or existing systems. In particular, accidents and incidents can be analysed to identify potential contributory causes relating to data.

To support this type of analysis a number of previous accidents and incidents have been collected in Appendix H. These include cases which relate to a number of Data Properties (see section 6.2.3), for example the properties of completeness, integrity and timeliness. They also highlight the importance of the adaptation Data Category and dangers associated with the inappropriate use of default data values.

Most of the current collection of accidents and incidents fall into three categories: aviation; maritime; and medical. However, the lessons that can be learned span a much wider range of application areas.

6.2.2 Ways that Data Can Cause Problems

There are some risk-inducing issues that are different or more prevalent for data than for other system elements. An incomplete collection of examples is provided below. This list may provide a quick way of identifying risks, which could be especially useful at an early stage of a project:

- **Fluidity** Hardware and software can undergo significant amounts of product assurance and once assured may change relatively infrequently. Where change is required to hardware or software, it can be carefully managed and the impact on the safety case appraised. This is not always the case for data, which is often much more fluid; indeed the ease with which data can be changed is one motivation

for the move towards data-driven systems. This fluidity means that it is not always possible to revisit safety cases when data changes — for example, the safety case for an autonomous vehicle cannot be updated every time that the vehicle acquires new knowledge during operation. Instead, the fact that data can change, along with any associated safety impacts, may need to be captured in the system safety case. Fluidity can also provide a temptation for unscrupulous operators to falsify data, for example, after an incident has occurred. Rigorous configuration control procedures can help protect against this type of behaviour.

- **Reuse** For the purposes of this discussion, "reuse" is interpreted as use of the same data in a different system or system context (e.g., lifecycle phase). Just because data was valid for use in a particular system, it does not immediately follow that it can be reused again in a similar system. Many considerations associated with data reuse are similar to those of software reuse, for example: similarity of requirements; similarity of role in system; and similarity in required integrity / assurance level. One consideration that is different is that of timeliness: data that was valid for use in a particular system at a particular time is not necessarily valid for reuse in the same system at a different time.
- **Ageing** As highlighted above, all safety-related data has a lifetime and this needs to be explicitly managed. This can involve, for example, purging, deletion and alerting. It is also important to note that ageing can occur as a result of changes external to the system (for example, records of the positions of other aircraft, newly discovered drug interactions, or new software patches) or it can result from internal changes (e.g., valves gradually becoming less responsive, configuration data becoming out of date, or data schemas evolving over time).
- **Transformation** Data is often filtered, mapped or aggregated as it moves through systems, sometimes creating new data sets as a result. Data Properties are not necessarily preserved by these processes — sometimes data is filtered too much or only some of the data is selected (either deliberately or inadvertently through accident or unintended bias), such as by the selection of only the test runs that succeeded. The main issues are loss of heritage / history / source information; data can also appear to become something else. Without careful management the integrity may become lowered to the lowest common denominator and this needs to be recognised. Additional checks (e.g., validation checks, sanity checks) or assurance measures may need to be put in place to ensure that required integrity / assurance is maintained.
- **Ownership** The transformation of data can result in a lack of clarity regarding who has ownership of, and responsibility for, the data (if anyone). It is important that responsibility for errors can be tracked, for example, to determine whether they were present in the initial data or whether they arose as part of the transformation process. Establishing clear roles within the data supply chain can help mitigate these issues.
- **Archiving and Retrieval** Safety-related data needs to be available when required. There is thus a need to think about data accessibility over the complete system lifetime. It is also important to consider what properties of the data need to be preserved and how this affects the choice of storage medium.
- **Biasing** This is a systemic inaccuracy in data due to the characteristics of the process employed in the creation, collection, manipulation, presentation and interpretation of data. It is usually an unintentional distortion in the data set — one example of this is the confirmation bias that may be applied to safety claims, whilst another example is that synthetic autonomous vehicle training databases can have issues with artificial data if not realistic. Although there is no perfect way of checking for this within the system, completeness, statistical and validity checks on data sets may help.

- **Falsification / Misinformation** This issue arises where data is created, modified or deleted either accidentally or deliberately so as to mislead or misinform potential consumers of that data. Examples from policing and criminal justice might be: notes taken with fabricated times or dates; or accidentally adding or removing a crime from the wrong individual in a database. Another example might be a supplier falsifying quality records for materials or goods. There have been many cases of misinformation related to the Covid-19 pandemic (for example on social media) where people have been deliberately misled and sometimes this has led to harm (drinking bleach as a cure for instance). Some mitigations involve digitally signing transmitted data, strong access controls, independent fact-checking and audit records.

- **Defaulting** Many systems use default or initial values for data items; sometimes in data sets and sometimes embedded in software. Often these default values are designed to be neutral (e.g., "0") or unrealistic (e.g., "VOID"). There are essentially two cases: (i) initialisation data which may persist and be mistakenly taken as a real value when in fact it should have been changed; (ii) data that is used when no meaningful value has been assigned (e.g., during data migration or data exchange between systems). These issues can often be managed through good design of data structures, for example by the inclusion of a validity flag.

- **Sentinels** A sentinel value is a data value that is used to indicate a special action needs to be taken, typically indicating the end of a record or a data set. The sentinel value should be one that is not allowable in the data set itself, but often is not properly considered and may use common sequences (e.g., five zeroes). Sentinels can cause problems in two ways: (i) where they are not recognised and so, for example, processing continues past the sentinel; (ii) where the data itself somehow contains the sentinel value and so processing is erroneously interrupted. Sentinels can be a particular risk in long-lived systems and data sets. As with the issue above, the management or elimination of this issue may often be achieved through improved data structures.

- **Aliasing** This is an effect that causes different data to become indistinguishable when accessed; that is, there is only one record when there should be several — for example, two patients with similar names inadvertently sharing a single set of medical records. This could be due to the way the data is filtered, sampled, indexed, stored or retrieved. The data issues are typically related to loss of resolution leading to similar data points appearing to be identical. Hence, methods to maintain resolution, including use of unique indexes, may be beneficial.

- **Disassociation** This effect is, in some senses, the opposite of aliasing; there are several records when there should only be one. This could occur, for example, if two records are created for the same individual using slightly different names. It could also arise if different systems use different indexing methods and the association between the indexes becomes corrupted. Again, methods to maintain data resolution can be beneficial.

- **Masking** This issue can arise if a notable proportion of a data set is of a poor quality, for example, if sensors producing the data are faulty or measurements are taken from the wrong source. This poor quality data can mask errors in the way that the system handles the good quality data. One way of protecting against this issue is the generation and use of test sets of appropriate size and quality, although for some applications this may be a non-trivial task.

- **Incompleteness** Not all the data that is needed is always available; there may be known, and sometimes, unknown gaps or missing data points. The missing data points ("Dark Data" — see section K) can be critical and in some cases, more important than the data that is available. Incomplete data can arise, for example, from limitations on how much data can be physically captured (eg. sampling frequencies, storage/time constraints) or from the unintentional or deliberate darkening of data (eg. for privacy, security, political or commercial reasons).

- **Volume** Data can be so large and unstructured that it is not manageable in practicable timeframes. For example, video records of rail track could take days to inspect manually.
- **Interpretation** Data can be misinterpreted — too much or too little deduced from available data, or data extrapolated incorrectly to derive unsound results. An example is Machine Learning data, especially real or recorded data that may not contain critical edge/corner cases.
- **Distribution** Data can be decentralised, decomposed or distributed across many sources (e.g. channels, databases, websites) and needs to be consistently integrated to make a coherent picture. In the health sector often many IT systems have to work together feeding in different parts of a patient medical record to make a complete health picture. If parts of this distributed data are missing (for instance diagnostic test results) then it is difficult if not impossible to obtain the complete picture, and mistakes may be made.

Further examples of how data may cause issues in many scenarios is given in a recently published book [7].

6.2.3 Data Properties

Data Properties are used to establish what aspects of the data (e.g., timeliness, accuracy) need to be guaranteed in order that the system operates in a safe manner.

James Inge's work [8] produced a useful taxonomy of data categories, and went on to look at faults in data. He concluded that a rigid taxonomy of data categories was unhelpful due to various properties, or characteristics, of the data which vary independently. In short, it is the combination of Data Category with the required Data Properties that facilitates safety analysis.

Data Categories were discussed in the preceding phase. A collection of Data Properties has been produced; this is documented in Table 5. Typically speaking, it is the loss of one of these properties that presents a hazard. Note that, this notion of "loss" is dependent on the intended use: for example, what is "timely" for one use may not be for another. Also note that this list is non-exhaustive.

6.2.3.1 The Goldilocks Property

The "Goldilocks" property has been added to address appropriate sizing and quantity of data. A number of issues have been found to arise when there is too much or too little data. Whilst it is particularly relevant to communications links, it may have relevance to other areas, such as databases and also when people are involved in reviewing or checking data. The property is named "Goldilocks" as it refers to the need to have not too much, not too little, but just the right amount of data[1].

The Goldilocks property is related to the "Volume" problem of data discussed in section 6.2.2, however given the importance of data sizing, and the experience of real-world incidents this is now a separate property.

[1] A system where the property was lost involved a high speed bus that connected several safety critical systems. A transiever of that bus failed and transmitted random noise. The receivers employed parity checks and cyclic redundancy check, but the system had been designed to eliminate occasional errors. When random noise filled the bus, several apparently valid messages were created every second, resulting in potentially lethal behaviour.

In a HAZOP carried out during 2020, based upon the HAZOP guidewords within previous versions of this document, the facilitator realised that certain failure modes had not been identified by the HAZOP team. In addition to the issue of system overload already discussed, those omissions also concerned system behaviour following data rejection. In these cases, bad data was detected and rejected, but the consequences of data rejection over an extended period had not been considered.

Table 5: Properties of data

Property	Abbreviation	Description
Integrity	I	The data is correct, true and unaltered
Completeness	C	The data has nothing missing or lost
Consistency	N	The data adheres to a common world view (e.g., units)
Continuity	Y	The data is continuous and regular without gaps or breaks
Format	O	The data is represented in a way which is readable by those that need to use it
Accuracy	A	The data has sufficient detail for its intended use
Resolution	R	The smallest difference between two adjacent values that can be represented in a data storage, display or transfer system
Traceability	T	The data can be linked back to its source or derivation
Timeliness	M	The data is as up to date as required
Verifiability	V	The data can be checked and its properties demonstrated to be correct
Availability	L	The data is accessible and usable when an authorised entity demands access
Fidelity / Representation	F	How well the data maps to the real world entity it is trying to model
Priority	P	The data is presented / transmitted / made available in the order required
Sequencing	Q	The data is preserved in the order required
Intended Destination / Usage	U	The data is only sent to those that should have access to it
Accessibility	B	The data is visible only to those that should see it
Suppression	S	The data is intended never to be used again
History	H	The data has an audit trail of changes
Lifetime	E	When does the safety-related data expire
Disposability / Deletability	D	The data can be permanently removed when required
Goldilocks	G	The data is just the right size — not too much and not too little

Table 6 illustrates where the data issues discussed in section 6.2.2 can result in loss of one or more Data Properties (x = potential loss of property).

Table 6: Properties that can be lost through issues

	Integrity	Completeness	Consistency	Continuity	Format	Accuracy	Resolution	Traceability	Timeliness	Verifiability	Availability	Fidelity/Representation	Priority	Sequencing	Intended Destination/Usage	Accessibility	Suppression	History	Lifetime	Disposability/Deletability	Goldilocks
Issue	**I**	**C**	**N**	**Y**	**O**	**A**	**R**	**T**	**M**	**V**	**L**	**F**	**P**	**Q**	**U**	**B**	**S**	**H**	**E**	**D**	**G**
Fluidity								x		x		x						x			x
Reuse		x				x		x	x	x		x			x		x	x	x	x	x
Ageing		x				x			x			x			x	x	x	x	x	x	
Transformation	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Ownership								x		x	x				x	x		x			
Archiving / Retrieval															x	x	x	x	x	x	
Biasing	x	x	x	x		x			x	x		x	x	x							
Falsification / Misinformation	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Defaulting	x	x	x	x		x						x									
Sentinels	x	x		x		x								x							
Aliasing	x	x		x		x	x	x		x	x	x									
Disassociation	x			x		x		x	x	x	x	x	x	x	x	x	x	x	x	x	
Masking	x	x	x	x		x				x		x									
Incompleteness	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Volume										x											x
Interpretation	x	x	x		x	x	x		x	x		x									
Distribution	x	x	x	x				x			x		x	x	x	x		x		x	

6.2.4 HAZOP Guidewords

A Hazard and Operability study (HAZOP) [9] provides a structured approach for identifying hazards. It involves a multidisciplinary team collaborating to identify potential hazards and operability problems. Structure and completeness are supported through the use of guideword prompts, for example, considering the implications if software components perform functions early, late or not at all. These prompts are intended to stimulate imaginative thinking, to focus the study and to elicit ideas and discussion.

Table 7 lists a set of guidewords for a data-focused HAZOP, based upon the properties defined in Table 5. The intent here is to assess the impact of each guideword on the property under consideration. For example, the first row considers *loss* of integrity, *partial loss* of integrity, and so on. The list is non-exhaustive. Other guidewords may be useful for particular systems, or may be used to ensure the Data Safety Assessment is fully integrated within the system safety assessment. Note that a more detailed version of this table, including specific HAZOP Data Considerations, is available at section F.

Table 7: HAZOP guidewords: concise guide

Property	HAZOP Data Guidewords
Integrity	Loss, partial loss, incorrect, multiple
Completeness	Loss, partial loss, incorrect, multiple, insufficient
Consistency	Loss, partial loss, incorrect, multiple, too early, too late, loss of sequence
Continuity	Loss, partial loss, incorrect, late, loss of sequence
Format	Loss, partial loss, incorrect, multiple
Accuracy	Loss, partial loss, incorrect, multiple, insufficient
Resolution	Loss, partial loss, incorrect, multiple, insufficient
Traceability	Loss, partial loss, incorrect, multiple, too early, too late, loss of sequence
Timeliness	Loss, partial loss
Verifiability	Loss, incorrect, partial loss, multiple, too early, too late, loss of sequence
Availability	Loss, partial loss, multiple, too early, too late
Fidelity / Representation	Loss, incorrect, partial loss, multiple, too early, too late
Priority	Loss, incorrect, partial loss, multiple, too early, too late
Sequencing	Loss, incorrect, partial loss, multiple
Intended Destination / Usage	Loss, incorrect, partial loss, multiple, too early, too late, loss of sequence
Accessibility	Loss, incorrect, partial loss, multiple, too early, too late
Suppression	Loss, incorrect, partial, too early, too late, too much, too little
History	Loss, incorrect, partial loss, multiple
Lifetime	Loss, too early, too late, incorrect, multiple, loss of sequence
Disposability / Deletability	Loss, incorrect, partial, too early, too late
Goldilocks	Loss, incorrect, partial, too early, too late, too much, too little

6.3 Analyse Risks

6.3.1 Establishing DSALs

Section 5.3.2.1 presented a method for the assignment of DSALs, by combining Severity and Likelihood through a risk matrix, such as Table 3. This section describes approaches that may be used to determine the Severity and Likelihood appropriate to the loss of any given property. In principle, Table 8 and Table 9 are used together with Table 3 to determine a DSAL. However it must be emphasised that the methods presented within this document to determine Severity and Likelihood, and to combine them to determine a DSAL should not be slavishly followed, but should be defined based upon the overall safety requirements of the system being assessed. Examples of situations that may require such alternate approaches are described in section 5.3.2.2, whilst potential approaches to customisation are described in section N. Such customisation is encouraged, but it is essential that any customised approach is recorded in the DSMP.

The likelihood of a data-safety related risk is qualitatively determined by consideration of the significance of a data error, along with the defences currently in place against such errors. These factors may be addressed by considering the following characteristics:

1. **Proximity**: how directly a data failure will lead to an accident;
2. **Dependency**: how dependent the application is on the data set;
3. **Prevention**: the ability of the systems architect / developers to guard against errors;
4. **Detection**: the likelihood of being able to detect a data failure prior to an accident; and
5. **Correction**: the ability of the system to work around or correct errors.

For example, errors that are easy to guard against are associated with low likelihoods. Conversely, errors that are difficult to detect are associated with high likelihoods. Table 8 illustrates how aspects of these characteristics map to three, qualitative likelihoods.

Table 8: Calculation of likelihood

	Likelihood		
	High	**Medium**	**Low**
Proximity	A known use of the data is highly likely to lead to an accident.	A possible use of the data could lead to an accident.	All currently foreseen uses of the data could lead to harm only via lengthy and indirect routes.
Dependency	Data is completely relied upon.	Data is indirectly relied upon.	Little reliance on data.
Prevention	Difficult or impossible to guard / barrier against errors.	Possible to guard / barrier against errors.	Easy to guard / barrier against error.
Detection	Low or no chance of anything else detecting an error.	Some other people / systems are involved in checking the data.	Many other people / systems are involved in checking the data.
Correction	Difficult or impossible to correct or workaround errors.	Possible to correct or workaround errors.	Easy to correct or workaround errors.

When applying this table to a specific data-related risk it is likely that consideration of different characteristics will result in different likelihoods. In order to provide an overall likelihood, it is assumed that the actions implied in the above table are taken. For example, a low likelihood for the "prevention" characteristic is only valid if the easy guard / barrier is actually implemented. Similarly, it is assumed that if an error is found, under the "detection" characteristic, an appropriate response is implemented. With those assumptions in place, the overall DSAL is associated with the lowest likelihood of any characteristic.

Note that the approach described above in the determination of likelihood may seem non-intuitive, as we look for the **lowest** likelihood, not the highest. However in doing so, it is important to only apply those rows of the table which are valid for the issue under consideration. Thus, for example, if it would be easy to implement a guard against a given error, but that guard is not actually in place, it would not be valid to claim that the likelihood is Low, on the basis of the Prevention row. In general, it should always be possible to determine likelihood based upon Proximity and Dependency, however the benefits of Prevention, Detection and Correction will not always be present.

Risk severity is estimated against a five-point scale, as indicated in Table 9.

Table 9: Definition of severity

Severity	Description
Minor	Minor injury or temporary discomfort for one or two people. Minor environmental impact.
Moderate	An accident resulting in minor injuries affecting several people or one serious injury. Some environmental impact.
Significant	An accident resulting in minor injuries affecting many people or a few serious injuries. Significant environmental impact.
Major	A serious accident resulting in serious injuries affecting a number of people, or a single death. Major environmental impact.
Catastrophic	An accident resulting in several deaths. The accident could affect the general public or have wide and catastrophic environmental impact.

As noted earlier, DSALs have some commonality with things like (Item / Function) Development Assurance Levels (IDALs / FDALs). However, this commonality does not extend across all aspects. For example, there is an accepted calculus of FDALs in which two independent lower-integrity functions can be used to replace a single higher-integrity function. There are two reasons why this type of calculus is not appropriate for DSALs:

1. The definition of a DSAL already caters for interactions. For example, using two independent Data Artefacts to provide similar information to a system function reduces the "dependency" of each artefact.
2. These types of consideration are most closely related to system architecture, from which Data Artefacts, associated Data Properties and risks are derived. Hence, rather than applying any calculus at the DSAL tier it is more appropriate to apply this to, for example, FDALs, with DSALs changing as a consequence of the revised system definition.

6.3.2 Analysing DSALs

When considering the possibility of data affecting software or software affecting data, the degree of contribution and existing mitigation position are important. The mitigations should be proportionate and full credit for existing mitigations may reduce or obviate the need for additional work. A particular case is the use of strong checksums to "wrap" the data. If these are preserved through processing and can be checked later on, then undetected corruption situations can be largely discounted.

With regards to the first case (i.e., **data affecting software**) the issue is that the data used by the system may affect the software execution in a way that could credibly lead to hazards, but only where this data-induced effect is not easily detected or mitigated by other means. If this is the situation then appropriate measures need to be put in place *within the data* to mitigate this risk. Alternatively (or additionally), if the software within the system can be modified, mitigations could be placed *within the software* to achieve or enhance the mitigation needed:

1. **Mitigation within the data** In many cases the best or only option is to improve the quality of the data to avoid the issue. This can be done by introducing a DSAL for the data, related to the severity of the hazard which may be induced, and thereby addressing the issue at cause. In this case, the DSAL is bearing a large amount of responsibility. This may mean that a greater number of the "Recommended" risk treatment methods and approaches (identified in the following phase) need to be implemented.
2. **Mitigation within the software** If the data cannot be assured to a DSAL (e.g., if it is supplied by a third party or legacy system), sometimes changes can be made to the software in the system to improve the situation. These mitigations could be functional (e.g., introduction of better range checking, rejection of illegal combinations of data values). This requires not only specific software changes but also associated verification of these new features and any software changes will have to be implemented to an appropriate Software Assurance Level. However there may be no particular functional mitigation or set of mitigations that can be targeted at the particular issue (e.g., testing for illegal combinations of values is too complex). In this latter case, potentially the complete set of software within the system responsible for manipulating the data should be developed (or re-developed) to a suitable Software Assurance Level. This level should be related to the severity of hazards it is mitigating.

With regards to the second case (i.e., **software affecting data**) the issue is that the software may affect (e.g., corrupt, delete) the data in a way that key safety properties may be lost and, furthermore, that loss may not be easily detected. In general the key Data Properties should be considered to see if any important ones for this data may be jeopardised. If so, a Software Assurance Level from an appropriate standard or guideline should be introduced that mitigates this risk of undetected property loss. This Software Assurance Level should be determined by the hazards that could be caused, and may be localised to the software that can cause the problem.

However there are specific functional and architectural approaches that may reduce or avoid the need for a Software Assurance Level, including use of strong checksums and digital signatures, as well as techniques such as storing multiple copies, independent channels and so on. However it is important that the software performing the check of the Data Property will itself need to be developed to the introduced Software Assurance Level. The key is to establish what the software in the system is doing to the data: if the operations are simple and non-changing, then the risk is lower; if the operations are complex involving transforming the data, using the data to calculate and insert new values, or reformatting the data then the risk is higher.

It is necessary to decide how effective the functional mitigations are in reducing impact to the particular Data Properties, e.g., a strong checksum may be very effective at detecting unwanted change and therefore lower

the Software Assurance Level (from the perspective of data-related requirements). However a checksum may not help at all if the issue is one of timely message delivery. More information on the use of checksums in the aviation domain is available in [10]; this information is likely to be applicable to other domains as well.

6.4 Evaluate and Treat Risks

6.4.1 Risk Treatment

There are a range of approaches that could be used to treat data-related risks. One option might be to redesign part of a system, either to remove the risk or to incorporate safety devices. Alternatively, ways of mitigating (or, more generally, treating) the risk could be devised. Another option could be to conduct further analysis, for example to better understand the likelihood of a risk occurring. In extreme cases, risk evaluation may lead to a recommendation to cancel a project.

It is apparent that some of these approaches involve repeating activities (or part of activities) discussed in earlier sections of this document. This type of repetition is to be expected given the iterative nature of risk management.

Discussion is an important part of risk evaluation, allowing a variety of different perspectives to be brought to bear. Documentation is also important, partly to allow these discussions to occur on an even footing and partly to ensure that decisions and supporting rationale are recorded.

6.4.2 Mitigating Data Safety Risks

A range of methods and approaches can be used to mitigate the identified data safety risks. Since mitigation can be a complex process, requiring collaboration with all system engineering elements, a collection of high-level mitigation measures is provided; these may particularly assist those attempting to explain the process to non-practitioners, or those conducting assessments in less regulated environments. For practitioners assessing systems which do not have a high safety criticality, these high-level mitigation measures may prove sufficient.

For practitioners conducting assessments in highly regulated environments, or for highly safety-critical systems, sets of appropriate mitigation measures should be derived from the high-level table. To assist these practitioners, suggested methods and approaches are provided in a series of more detailed tables. These methods and approaches have been developed through cross-industry collaboration, but they may not be complete, especially for different types of system.

The practitioner should always consider whether the mitigation measures used to mitigate the data safety risks are sufficient for their purposes. In highly safety-critical systems, each data safety risk can be linked to a system-level hazard (or a new system-level hazard identified). Each hazard is tracked in accordance with the existing system safety method and mitigations are reviewed in terms of their feasibility, potential to introduce new or amended hazards, and effectiveness.

6.4.2.1 High Level Mitigation Measures

Table 10 presents a number of generally applicable mitigaton measures. Each of these mitigation measures should be reviewed to establish whether it is relevant to the system under assessment.

For each Data Safety Assurance Level, the tables indicate whether the method / approach is:

- Highly Recommended (HR);
- Recommended (R); or
- No recommendation for or against being used (-).

Table 10: High level mitigation measures

Ref	Mitigation Measure	DSAL				Comment
		1	2	3	4	
M.01	Documentation of data context and suitability for use	HR	HR	HR	HR	e.g., data flow diagram to document and agree how data is handled in the system, recording the impact of design decisions on the data aspects of the safety case
M.02	Definition of data ownership through the data lifecycle in the system	R	R	HR	HR	e.g., governance model, interface control document
M.03	Definition and traceability of data requirements	HR	HR	HR	HR	e.g., requirements management, use of test data / test cases
M.04	Recorded trustability of the data source(s)	R	R	HR	HR	e.g., source of the data is trusted (with 'trusted' to be defined in detail for the system), or there are multiple sources of data which are correlated
M.05	Editing limitations	R	R	HR	HR	e.g., encapsulation[2] of data, access limitations
M.06	Diverse and / or redundant manipulation of data	R	R	HR	HR	e.g. data partitioning separation of data that is managed differently (architectural decisions)
M.07	Automatic system checking functionality	-	R	HR	HR	e.g., Built-In Test (BIT), heartbeat functionality
M.08	Monitored, controlled, or redundant manipulation of data	-	-	R	HR	e.g., redundant channels processing the data as hot standby
M.09	Diverse and / or redundant storage of data	R	R	HR	HR	e.g., redundant storage of data, multiple different media types used to back-up the data
M.10	Data recovery mechanisms	R	R	HR	HR	e.g., backward recovery, error correcting codes
M.11	Tracking of data	R	R	HR	HR	e.g., digital signatures, sequence numbers, logging of data processing events, using metadata, configuration management
M.12	Recorded derivation of test data	R	R	HR	HR	e.g., test data derived from an established system and supported by field evidence, or from another 'trusted' source
M.13	Documented compliance against the data requirements	HR	HR	HR	HR	e.g., use of test data / test cases

6.4.2.2 Detailed Methods and Approaches

The following collection of tables details methods and approaches which may be used by practitioners conducting safety assessments. The tables map the methods and approaches to Data Categories. To aid

[2] Sometimes referred to as "data hiding", encapsulation hides the physical representation of data.

both legibility and usability, these data categories are abbreviated using the scheme shown in Table 11.

It should be noted that the five Data Categories presented in Table 11 are a subset of those presented in Table 4, which presents a comprehensive list of Data Categories. The five presented in Table 11 have been used to populate the tables within this document which are used for the selection of methods and approaches. The addition of further Data Categories to Table 11 is likely to be associated with expansion or customisation of the methods and approaches tables. Future versions of this guidance may incorporate these enhancements — however users of the guidance are also encouraged to do this as part of the customisation process associated with their own organisations or projects.

Table 11: Data category abbreviations

Data Category	Abbreviation
Verification	V
Infrastructure	I
Dynamic	D
Performance	P
Justification	J

The tables also map the methods and approaches to the Data Properties. To aid legibility, the properties which were defined in Table 5 have been assigned abbreviations using the scheme shown in Table 12.

Table 12: Data property abbreviations

Data Property	Abbreviation
Integrity	I
Completeness	C
Consistency	N
Continuity	Y
Format	O
Accuracy	A
Resolution	R
Traceability	T
Timeliness	M
Verifiability	V
Availability	L
Fidelity / Representation	F
Priority	P
Sequencing	Q
Intended Destination / Usage	U
Accessibility	B
Suppression	S
History	H

Continued on next page

Table 12: Data property abbreviations (continued)

Data Property	Abbreviation
Lifetime	E
Disposability / Deletability	D
Goldilocks	G

In an attempt to aid usability, these detailed methods and approaches tables have been organised into eight, loosely-defined categories:

- System Design;
- Data Design;
- Data Implementation;
- Data Migration;
- Data Testing;
- Test Data;
- Media - Paper; and
- Media - Electronic.

The method for using these tables when considering any given data artefact, is as follows:

- Determine the DSAL applicable to the artefact, using Table 3 in association with Table 8 and Table 9.
- Determine the Data Category, using the abbreviations in Table 11.
- Determine the list of applicable Data Properties, using the abbreviations in Table 12. This will generally provide a list of several applicable abbreviations.

Then consider each row in each table (or each table that you wish to use for this assessment). For each row, if:

- The Data Category matches the Data Category for this artefact and
- At least one of the Data Properties listed in that row matches a Data Property for the artefact

then the row is likely to be applicable to the artefact. The result for that row is therefore found from the DSAL column, since if:

- The relevant DSAL entry is “HR”, then use of the Technique on this row is Highly Recommended.
- The relevant DSAL entry is “R”, then use of the Technique is Recommended.
- The relevant DSAL entry is “-”, then the technique should be considered, as it may be relevant in certain application domains, but this Guidance document is unable to take a view on its application in a generic context.

To give a specific example, consider the row corresponding to the first Technique in Table 13. This Technique will apply to data artefacts where:

- The Data Category is Dynamic ("D" from Table 11) and
- The data artefact holds one or more of the properties Integrity, Completeness or Verifiability ("I", "C" or "V" from Table 12).

In such a case, the Technique would be Highly Recommended if the data artefact were of DSAL 3 or 4, Recommended is the DSAL were 2, or should merely be considered if the DSAL were 1.

Many dots have been placed in the table to indicate Data Categories and Data Properties which are not applicable to the Technique under consideration. The dots enable the tables to be assessed very quickly, as they enable the letters representing specific Data Categories and Data Properties to always be presented in the same position within the table. For example, the Data Property Verifiability ("V" from Table 12 can easily be seen to appear against the first two Techniques of Table 13, whereas it does not appear in the next seven Techniques — this can be seen without actually reading the text, but merely looking at the pattern presented by the letters and dots.

Within each table, the "Serial" column lists a unique serial number for each technique. The serial numbers simply provide a unique reference which aligns with those implemented within the toolset.

6.4.2.3 System Design

Table 13: Mitigation methods: system design

Serial	Technique	Data Category	DSAL				Notes	Data Property
			1	2	3	4		
SD.01	Built-in-Test / Built-in-Test Equipment (BIT / BITE)	..D..	-	R	HR	HR	Application tests the data (e.g., at start-up or when requested by an operator).	IC.......V..........
SD.02	Cyclic / Continuous BIT	..D..	-	-	R	HR	Application applies tests to the data it is processing continuously (e.g., for a live data stream) or periodically (e.g., every nth message, every hour).	IC.Y.....VL..........
SD.03	Backward recovery	..D..	R	R	HR	HR	If a fault in data has been detected, the system resets to an earlier internal data set, which has been proven consistent.	IC..................
SD.04	Parity Checks	..D..	R	R	HR	HR	Within data, e.g., Hamming codes, Reed-Solomon, Hagelbarger.	I...................
SD.05	Automatic Error Correction	..D..	R	R	HR	HR	Detected errors are corrected automatically.	IC..................

Continued on next page

Table 13: Mitigation methods: system design (continued)

Serial	Technique	Data Category	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
SD.06	Checksums / Cyclic Redundancy Checks (CRCs) / Hashes	..D..	-	R	HR	HR	Digests of data sets are produced, included with the data set and checked to provide confidence that the data is unaltered.	IC.....G
SD.07	Digital Signatures	..D..	-	R	HR	HR	For non-repudiation and integrity of data.	I.....T.....U.....G
SD.08	Sequence Numbers	..D..	R	R	HR	HR	Data bears sequence numbers so the integrity of a data stream can be checked (e.g., monotonic increase, duplicate detection).	ICN.....PQ.....
SD.09	Automatic Repeat Request	..D..	R	R	HR	HR	Automatic Repeat-reQuest (ARQ) to repeat transmission of data which has not been received correctly.	IC.Y.....G
SD.10	Auditing Facilities	..DP.	-	R	HR	HR	Changes to Data Properties are audited so the before and after values are recorded and also other related information such as the author and the time of the change.	.....T.V.....H...
SD.11	Logging Facilities	..DP.	R	R	HR	HR	Data processing events are logged to allow support staff to monitor the health of the system and provide diagnostic information.	.....T.....H...
SD.12	Encapsulation	..D..	R	R	HR	HR	The hiding of data so that it is only accessible through well defined interfaces.	.....UB.....
SD.13	Multiple Stores	..D..	-	-	R	HR	The same instance of a data set or data items is stored in multiple locations.	.....B.H...
SD.14	Homogeneous Redundancy	..D..	-	-	R	HR	Data is processed using homogeneous redundant channels; detected faults in data of one channel cause processing to switch to another channel.	IC.Y....M.....

Continued on next page

Table 13: Mitigation methods: system design (continued)

Serial	Technique	Data Category	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
SD.15	Heterogeneous Redundancy	..D..	-	-	R	HR	Data is processed using heterogeneous redundant channels; detected faults in data of one channel cause processing to switch to another channel.	IC.Y....M.....
SD.16	Data Integrity Sampling	..D..	HR	HR	R	R	The integrity of subsets of data is periodically checked, in accordance with a given selection criteria (e.g., random, critical records).	IC..O.....L.....
SD.17	Sanity / Reasonability Checks	V.D..	R	R	HR	HR	Dedicated processing implemented to check that data is within reasonable tolerances and / or logically / semantically consistent (e.g., range checks, date checks, record counts, record sizes, special values - NaN).	I...O.............G
SD.18	Data Correlation	..D..	R	R	HR	HR	Data from a number of sources exists to permit a cross-correlation of the data supplied from one source (the master) with other sources.	ICNY.............
SD.19	Data Partitioning	..D..	R	R	HR	HR	To separate data that is managed differently, creating independence so that a whole data set does not require validation after a change.	.............B.....
SD.20	Syntax Checks	VID..	R	R	HR	HR	Semantic checking of data values and sequences based on defined rule sets.	I.N.O.............G
SD.21	Feedback testing	..D..	HR	HR	R	R	To check output data by comparing it with the input source.	IC.Y...T.V.........G
SD.22	Information Redundancy	..D..	HR	HR	R	R	Additional redundant information is supplied from diverse sources. The validity of the data coming from the diverse sources can be checked against each other.	IC.................G

Continued on next page

Table 13: Mitigation methods: system design (continued)

Serial	Technique	Data Category	DSAL				Notes	Data Property
			1	2	3	4		
SD.23	Reverse Translation	..D..	-	R	HR	HR	To verify data output of a process is correct, by attempting to create the source data from the output data and comparing this with the original source.	IC.Y...T.....
SD.24	Meta-data	..DP.	-	R	HR	HR	Auditable data are sent with the data that is about the data (e.g., source, issue state, expiry date).	..N....T.V..PQ....E..

6.4.2.4 Data Design

This table addresses design aspects, including the construction of data storage structures and methods.

Table 14: Mitigation methods: data design

Serial	Technique	Data Category	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
DD.01	Governance Model	VI..J	R	R	HR	HR	A governance model is established that defines, e.g., data ownership, processing roles and responsibilities, processing authorisations and permissions.	I....A.T......U.S..D.
DD.02	Data Process Definition	VIDPJ	-	R	HR	HR	Documented and agreed process definitions for how data is handled.	.......T......U.....G
DD.03	Data Flow Diagram	VIDPJ	HR	HR	HR	HR	To describe the data flow in a diagrammatic form.	.............U......
DD.04	Data Model	VIDPJ	HR	HR	HR	HR	To articulate how data is organised.	..N.O..............
DD.05	Client Sign-Off	VI.PJ	R	R	HR	HR	Agreement from the client that the data is appropriate.	......R..V..........
DD.06	Data Quality Correction Mechanisms	...P.	-	R	HR	HR	A process, strategy and tooling for data that breaches a given data quality criteria.	IC.Y..............
DD.07	Configuration Management	VIDPJ	HR	HR	HR	HR	The recording of the production of every version of every "significant" deliverable and of every relationship between versions of the different deliverable.	.......T.........H...
DD.08	Data Dictionary	VIDPJ	HR	HR	HR	HR	A collection of descriptions of the data objects or items in a data model for the benefit of data users.	..N.O.R....F.........
DD.09	Formal Methods	..D..	-	R	R	HR	To specify data (or data formats) in a precise, mathematical manner.	.CN.O..T....PQ......G
DD.10	Update Comparison	VIDPJ	-	R	R	HR	Updated data is compared to its previous version (e.g., so the list of changed elements can be compared with a supplier-generated list).	.......T.........H..G

6.4.2.5 Data Implementation

A number of issues need to be considered during the implementation phase of a programme, to ensure that at any point in the programme we know how much we can rely upon the data. Table 15 addresses those mitigations relevant to this whole programme phase, not just from data capture or generation. It therefore includes aspects of data management, checking and expiry.

Table 15: Mitigation methods: data implementation

Serial	Technique	Data Category	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
DI.01	Review / Inspection	VIDPJ	HR	HR	HR	HR	Manual review / inspection of data possibly involving data visualisation tools.	IC..O.....L.....
DI.02	Statistics-Based Sampling	VIDPJ	-	R	HR	HR	More appropriate for real-time large and / or volume data. Could be manual selection, a form of random selection or comparison against statistical norms.	I.NY.A.....
DI.03	Ground-Truth Check	VIDPJ	R	R	HR	HR	Inspection against physical measurements (e.g., lengths, positions, heights) taken in the real world.	ICN..AR..V.F.....
DI.04	Auditing	VIDPJ	R	R	HR	HR	A period of comprehensive internal and external testing of the data quality process.	ICNYO....V.....
DI.05	Tracing	VIDPJ	-	R	HR	HR	Ability to trace data from source across multiple participants in the data supply chain.	.......T.V.....
DI.06	Defined Verification Frequency	VIDPJ	-	R	HR	HR	Data should contain an indicator of how often it should be revalidated against other (e.g., real world) source.	.........V........E..
DI.07	Defined Data Lifetime(s)	VIDPJ	R	R	HR	HR	Information showing when data validity expires.	..................E..
DI.08	Data Quality Trend Analysis	VIDPJ	-	-	R	HR	Checking that a data set is consistent with a model of the expected data behaviour (e.g., vibration data increases over time).	IC.Y.....V.F.....
DI.09	Authorisation	VIDPJ	R	R	HR	HR	A security model is established to control who is authorised to create, view, edit, delete the data.	.............UBS..D.
DI.10	Authentication	VIDPJ	R	R	HR	HR	Data is authenticated to validate its provenance.	.......T.V.....

Continued on next page

Table 15: Mitigation methods: data procedures (continued)

Serial	Technique	Data Category	DSAL				Notes	Data Property
			1	2	3	4		
DI.11	Defined Confidence / Trust Levels	VIDPJ	R	R	HR	HR	Criteria are established to provide an objective measurement of the confidence or trust in a given data set.	IC.Y.....V.F.....
DI.12	Independent Check	VIDPJ	-	-	R	HR	A separate person or system is used to check the data independently.	I........V.....

6.4.2.6 Data Migration

This table addresses migration from one implementation to another, as opposed to the movement or gradual corruption of data.

Table 16: Mitigation methods: data migration

Serial	Technique	Data Category	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
DM.01	Manual Load	..D..	R	R	-	-	Data is entered into the system manually relying on human validation and verification.	ICNYOA.....F.....
DM.02	Dedicated Translation and Loading Platform	..D..	-	R	HR	HR	For example, using mature enterprise migration Commercial Off-The-Shelf (COTS) products.	ICNYOA.T...F.....
DM.03	Existing / Established System Transfer	..D..	-	R	HR	HR	Use of an existing / established proven transfer mechanism.	ICNYOA.T...F.....
DM.04	Client Supervision	VIDPJ	-	R	HR	HR	The client provides independent supervision of activities checking processes, inputs and outputs at agreed points.	ICNYOA.....F.....
DM.05	Client Sign-Off	VIDPJ	-	R	HR	HR	Formal acceptance of the migrated data sets in the target system.	ICNYOA.....F.....
DM.06	Incremental switch-over	..D..	-	R	HR	HR	Users are incrementally switched over to the new system rather than as a “big bang”.	ICNYOA.....F.....
DM.07	Parallel Load With Existing System	..D..	-	R	HR	HR	Parallel running of the new system alongside the existing system with data crosschecks between the two systems.	ICNYOA.....F.....
DM.08	Shadowing	..D..	-	R	HR	HR	Parallel running of the new system alongside the existing system, only data from the existing system is used operationally, with an experienced user crosschecking between the two systems.	ICNYOA.....F.....
DM.09	End to End Import-Export Verification	..D..	-	R	HR	HR	Data is traced and verified at all stages through the entire end to end migration process.	ICNYOA.T...F.....

6.4.2.7 Data Checking

Table 17: Mitigation methods: data checking

Serial	Technique	Data Category	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
DC.01	Limited / Pre-Operational Deployment	.IDP.	-	R	HR	HR	A period of monitored operation in a specially chosen environment.	ICN..A.....F.....
DC.02	Client Sign-Off of Data	VI.PJ	-	R	HR	HR	Agreement from the client that the data is appropriate.	......R..V.....
DC.03	Non-Critical Trialling	..D..	-	R	HR	HR	Monitored operation in an operational, but non-critical, environment.	.....A.....F.....
DC.04	Beta Testing	V....	-	R	HR	HR	Testing with a small group of specially chosen users.	ICN..A.....F.....
DC.05	Parallel Running	.IDP.	-	R	HR	HR	Running two systems in parallel and crosschecking between them.	ICN..A..M..FP.....
DC.06	Checklists	.IDP.	R	R	HR	HR	Using a checklist to verify that system behaviour is correct, prior to use. This approach can also be effective for detecting otherwise dormant failures and reduces time at risk.	ICN.O....VLFP.....
DC.07	Widespread Distribution to User Community	.IDP.	-	R	HR	HR	Large-scale distribution to all users.	ICN.OAR.M.LFP.....

6.4.2.8 Test Data

Table 18: Mitigation methods: test data

Serial	Technique	Data Category	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
TD.01	Using Informal / Ad-hoc Means	V....	R	R	-	-	Data is generated by simple means (e.g, spreadsheets, scripts, basic assumptions). There is no formal checking or review of the method of generation.	ICNY.A.....F.....
TD.02	Using Testbed	V....	-	R	HR	HR	A dedicated testbed is a good way to produce test data. It may require configuration and tailoring for the particular application, and this configuration should be managed.	ICNY.A.....F.....
TD.03	Using Simulator	V....	-	R	HR	HR	Simulators (software or hardware) may be able to produce very good test data, obviously depending on how close and detailed a simulation they can achieve.	ICNYOAR....F.....
TD.04	Using Prototype	V....	-	R	HR	HR	Prototypes are often a good way of generating test data for the real system. However they may not produce data with the appropriate range, accuracy or precision.	ICNY.A.....F.....
TD.05	Using Manual Means	V....	R	R	-	-	Simple test data can be produced by manual means, although this may be prone to human error.	ICNY.A.....F.....
TD.06	Using Dedicated Platform	V....	-	R	HR	HR	For complex and critical systems a dedicated test platform is required which can produce realistic test data for all interfaces and inputs.	ICNY.AR..V.FPQ.....
TD.07	Using Existing / Established System	V....	-	R	HR	HR	Where a new system replaces an old one, then data can often be extracted from the old system to test the new one. Data formats may change so translation may be required.	ICNYOAR.MV.FPQU.....

Continued on next page

Table 18: Mitigation methods: test data (continued)

Serial	Technique	Data Category	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
TD.08	Using Initial Runs of New System	V....	R	R	R	R	This method is often used where the system is breaking new ground and there is no prototype or legacy system to produce test data. Initial operations may differ from eventual usage, so test data must evolve.	ICNYOAR.MV.FPQ.....
TD.09	Derived from Real Data	V....	R	R	HR	HR	Where real data is available this is usually a good basis for generating test data (e.g., by modification to increase the test space coverage).	ICNY.A.....F.....
TD.10	Statistical Profiling Post-Production	V....	-	-	R	HR	If a statistical analysis of the data can be produced then greater confidence in the quality of the test data can be obtained.	ICNY.A...V.F.....
TD.11	Produced by Client	V....	R	R	R	HR	Ideally the client is involved in producing or at least checking the test data.	ICNY.A...V.F.....
TD.12	Client Sign-Off	V....	R	R	HR	HR	Where possible, the client should formally agree and sign-off the test data as appropriate.	ICNY.A...V.F.....
TD.13	Error Seeding	V....	R	R	HR	HR	This is where errors are deliberately inserted into the data set to demonstrate the effectiveness of data validation.	ICNYOAR.MV.F.....G
TD.14	Data Reuse	V....	R	R	HR	HR	Reusing data for one project that was created and thoroughly assured for another project. This can be effective but the read-across should be established.	ICNY.A.....F.....G
TD.15	Feedback Testing	V....	R	R	R	R	To check output data by comparing it with the input source.	ICNY.A.....F.....

6.4.2.9 Media - Paper

Table 19: Mitigation methods: data media handling — paper / physical storage

Serial	Technique	Data Category	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
MP.01	Photographic Copies	VIDPJ	R	R	HR	HR	Photocopy and store separately.	.C.....B.H...
MP.02	Scan to Electronic Format	VIDPJ	R	R	HR	HR	Retain both paper and electronic copies.	.C.....B.H...
MP.03	Copies Held at Different Locations	VIDPJ	-	R	HR	HR	Meaning of "different" depends on data criticality and similarity of location-based risks.	.....VL....B.....
MP.04	Limited Access	VIDPJ	-	R	HR	HR	Control (e.g., by procedure) who can access the data.	.....U.....
MP.05	Secure Storage	VIDPJ	-	R	HR	HR	Physical measures to prevent unauthorised access.	.....U.....
MP.06	Manual Inspection	VIDPJ	-	R	HR	HR	Used to check data when generated and periodically thereafter.	IC.....
MP.07	Suitable Physical Environment	VIDPJ	-	R	HR	HR	For example, prevent water ingress, control temperature.	I.....L.....E..
MP.08	Defined Handling Procedures	VIDPJ	-	R	HR	HR	To ensure that changes to the data can be attributed.	I.....UB.H...
MP.09	Repair / Restoration Programme	VIDPJ	-	-	R	HR	To protect against degradation and to ensure availability.	I.....L.....
MP.10	Indexing / Cataloguing	VIDPJ	R	R	HR	HR	To support efficient accessibility.	.....L.....
MP.11	Lifetime Planning	VIDPJ	-	-	R	HR	For example, to avoid gradual quality reduction by repeatedly "copying a copy".	.....ED.

6.4.2.10 Media - Electronic

Table 20: Mitigation methods: data media handling — electronic storage

Serial	Technique	Data Category	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
ME.01	Regular Refresh / Rewrite	VIDPJ	R	R	HR	HR	Of magnetic media or flash memory.	I.....E..
ME.02	Suitable Physical Environment	VIDPJ	R	R	HR	HR	Store media in a clean, low-humidity environment at a steady temperature, cool but not cold.	I.....L.....E..
ME.03	Copies at Different Locations	VIDPJ	R	R	HR	HR	Physically separate to cover natural disasters, accidental or malicious damage.	.....VL....B.....
ME.04	Backups / Duplication	VIDPJ	R	R	HR	HR	Backups are essential. Frequency of backup depends on rate of change. The number of generations to keep relates to the impact of data loss.	.....L.....
ME.05	Sample Restores	VIDPJ	R	R	HR	HR	Sample restores should be performed at intervals to ensure that the backups are readable and retrievable.	.....L.....
ME.06	Multiple Copies	VIDPJ	-	R	HR	HR	At least two backups should be kept, preferably in diverse formats.	.....VL.....
ME.07	Copy to Latest Media Format	VIDPJ	-	R	HR	HR	Anticipate obsolescence and plan a smooth transition to new technologies.	.....L.....
ME.08	Media Physically Secured	VIDPJ	-	R	HR	HR	Access to, and removal of, media should be controlled by suitable procedures. Access permissions should be reviewed at intervals.	.....T.....U..H...
ME.09	Resilient / Redundant Format	VIDPJ	-	-	R	HR	This may involve less use of compression, use of error detection and correction protocols, and (at the highest level) two or more redundant data servers.	IC.....L.....
ME.10	Long-Lifetime Format	VIDPJ	-	-	R	HR	The best formats should be adopted where available.	.....L.....E..
ME.11	Easily Translatable / Convertible Format	VIDPJ	-	-	R	HR	Adopt widely-used, well-documented, general-purpose formats in preference to specialist proprietary formats.	....O.....L.....

Continued on next page

Table 20: Mitigation methods: data media handling — electronic storage (continued)

Serial	Technique	Data Category	DSAL 1	DSAL 2	DSAL 3	DSAL 4	Notes	Data Property
ME.12	Copy to Cloud Storage	VIDPJ	-	R	HR	HR	Must specify whether a private cloud or a public cloud shall be used. Cloud storage may not be suitable for highly confidential data.	.....L.....
ME.13	Copy to Archiving Organisation	VIDPJ	-	R	HR	HR	Consider the required level of data integrity and confidentiality; also, the integrity and long-term viability of the archiving organisation, and plans in case it ceases to function.	.....L.....

6.4.2.11 Recording the Data Safety Risk Mitigation

The Data Safety Management Plan can be used to document:

- The tables of mitigation measures (or methods and approaches) used for the system, context, and planned implementation under assessment;
- Any specific mitigation measures identified for the system and their source / justification;
- Planned compliance with the tables; and
- Confirmation that the mitigation measures are sufficiently complete and consistent.

The overall safety justification for the given project/service/operational context must then provide evidence of compliance against the plan.

7 Worked Example (Informative)

> *There is a forest of data and we need to create a path through.*
> ***Tom Adams***

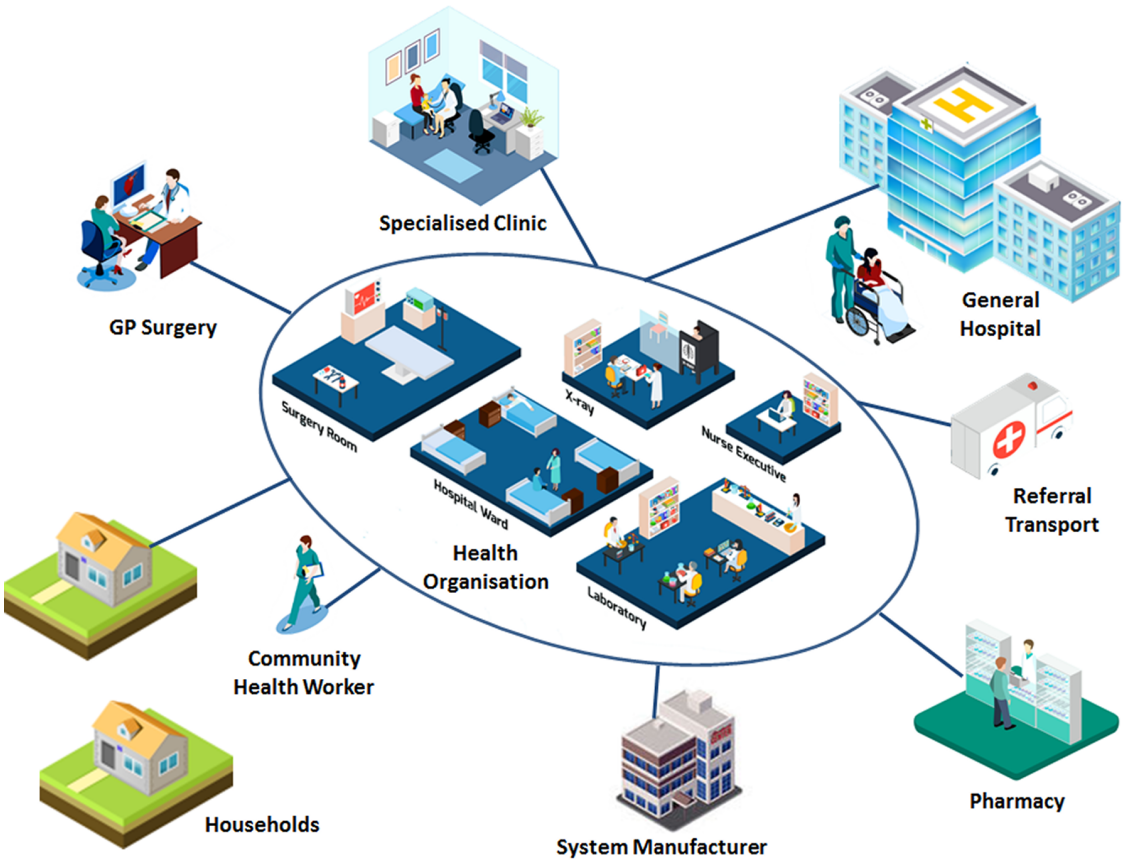
7.1 Purpose

This section provides a worked example of applying the Data Safety guidance to a hypothetical system in the Healthcare sector. Although some aspects of the example have been simplified, it is intended to be sufficiently realistic to allow key features of the guidance to be illustrated.

7.2 Establish Context

7.2.1 Background

A Manufacturer is building a new integrated health and social care system to support holistic care for community health services. The system supports clinical workflows for aspects such as referrals, tracking clinical encounters, appointment scheduling, outcome measures through to letter and report generation. The system follows a typical development lifecycle as a series of phases: business modelling; requirements; analysis and design; implementation; test; and deployment.



The system is being targeted to meet the requirements of a Health Organisation who are procuring a solution to help their clinicians maintain a high level of quality of care in the face of increasing volumes of patients and pressure to reduce staff costs.

From a data perspective, fundamental to fulfilling these requirements is establishing the context within which the use of data in system development, enhancement, introduction, integration or operation is occurring. This should establish the risk appetite: essentially, how much effort is devoted to making data risks as low as practicable. In turn, this will inform the nature and scope of assessments that are conducted during system development and, furthermore, its introduction into operational service. To meet the 'Establish Context' objectives set out in the guidance the following activities are recommended:

- Describe the organisational context;
- Describe the system context;
- Plan the assessment; and
- Identify Data Artefacts.

The Manufacturer decides to use an Organisational Data Risk (ODR) Assessment form to understand in broad terms the level of risk it will have to manage in developing and supporting this system. This will allow the Manufacturer to ***Describe the organisational context*** and ***Describe the system context.***

System Manufacturer

7.2.2 Organisational Data Risk (ODR) Assessment

The Manufacturer considered each of the questions within the ODR form, which is presented in Appendix B of this document. The following list identifies the questions in the ODR, along with the assessments for the Manufacturer's system.

Q1:	How severe could an accident be that is related to the data? Could it be caused directly by the data?

Failings in the system could give rise to non-optimal treatment plans for a patient that might delay detection of a more serious condition or prolong the recovery for a known condition. The system is not solely relied upon however, and there are other people and systems in play involved in checking data. On balance, this question is assessed as: **1c**; Score **4**.

Q2:	What would be the impact on the organisation, client or public if an accident occurred related to the data?

Unfortunately, accidents in the health domain are relatively frequent. There are many injuries and deaths attributed to medical errors but these are largely tolerated by the public and grievances are usually settled through financial settlements through the courts. The Manufacturer believes through their contractual arrangements that the Health Organisation would be liable for any claims even if it was attributed to an error in the Manufacturer's system's handling of data. On balance, this question is assessed as: **2b**; Score **2**.

Q3:	How much responsibility does this organisation have for data safety?

The Manufacturer is responsible for building the system in compliance with DCB0129 [11] and so is responsible for executing the associated safety management system to manage risk. The Manufacturer however plans to sell the product with a condition of use that places end responsibility for patient safety on the client. On balance, this is question is assessed as: **3b**; Score **2**.

Q4:	What legal and regulatory environment will this work be subject to?

The work will be contracted under UK law and subject to the Data Coordination Board (DCB) standards for Health IT Systems. However, there is no special regulator who is currently empowered to intervene in the delivery of healthcare systems, i.e., the standards are not currently enforced through law. The Health Organisation however will make compliance with the standards a contractual requirement. On balance, this question is assessed as: **4c**; Score **4**.

Q5:	How mature is this organisation regarding data safety?

The Manufacturer has a good understanding of data as a source of safety risk. Many of their systems are data intensive to support clinical decision making. There is good support and funding for the identification and resolution of data-related risks. On balance, this question is assessed as: **5b**; Score **2**.

Q6:	How widely used is the data and who by?

The data will be used in multiple clinical settings and by many clinicians and other support staff. There are several data supply chains and public web access to data. On balance, this question is assessed as: **6c**; Score **4**.

Q7:	What is the scale, sophistication and complexity of the data and its manipulation?

The data is complex and although transmitted through industry standard data structures, these require knowledge of the associated abstract clinical data model. Some data manipulations are required to map between different encodings for data held in the various heterogeneous systems. Some legacy systems transfer data in unstructured format. On balance, this question is assessed as: **7c**; Score **4**.

Q8:	How well defined and understood are the boundaries and interfaces for this data scenario?

The boundaries of the supply are well understood and although the interfaces are complex and mixed formats, these will be defined and agreed formally through Interface Control Documents. Most of the integrating systems are established Commercial Off-The-Shelf (COTS) based systems but some of the legacy systems still need to be investigated and working assumptions have been made by the Manufacturer. On balance, this question is assessed as: **8c**; Score **4**.

The final score is **26**, which corresponds to **ODR2**. The Manufacturer therefore concludes that there is low to medium risk that loss of properties of data in the system can contribute to or give rise to harm.

The Manufacturer has an internal policy for engagements based on the ODR level that dictates how the organisation shall ***Plan the assessment***; this policy dictates the amount of proportional effort it needs to spend on safety data management and the level of rigour to be employed. In this case, the policy dictates, amongst other requirements, that a separate section covering Safety Data Management is required in its Clinical Risk Management Plan.

The Manufacturer aims now to ***Identify Data Artefacts*** that are potential sources of safety hazards. The Manufacturer also knows that the safety dependency of data is dictated by the context in which it is used so it now develops an understanding of when in its process lifecycle the data will be used and relied upon. The Manufacturer plans to build an early prototype to show to clients to help elicit requirements definition. To support this, the Manufacturer plans to create a test data set that comprises a typical range of scenarios that the system will encounter. This form of data is identified as **Verification Data**. The system also needs to be configured to support deploying Health Organisations' policies. This data is **Infrastructure Data** and, for the prototyping phase, the Manufacturer plans to use largely default values.

In later phases when the system functionality is specified and the system is being built, the Manufacturer plans to create a test data set that will be key to demonstrating the correct functioning of the system and hence acceptance by the deploying Health Organisation. This still involves the use of **Verification Data** and **Infrastructure Data** but there will be far greater dependency on these data sets than the prototyping case. The Manufacturer therefore documents the planned use of each of the data categories during the entire delivery lifecycle in the Clinical Risk Management Plan.

The procuring Health Organisation will have a different perspective of the IT system that they will deploy into their organisation. They will already have many integrated systems in live operation and as part of establishing the context for the system's deployment they will need to consider many different types of data sets:

- **Infrastructure Data**: how the system will be configured in the specific environment;
- **Verification Data**: the test data sets to be used to support certain deployments such as integration testing and training; and
- **Dynamic Data**: the data entered or fed into the system and the data presented to the user, generated in the form of reports or data passed to other systems.

The Health Organisation decides to complete an Organisational Data Risk Assessment so it can ***Describe the organisational context*** and ***Describe the system context***. The scoring is similar to the Manufacturer with the following notable differences:

Q2:	What would be the impact on the organisation, client or public if an accident occurred related to the data?

The Health Organisation would bear the brunt of any publicity and litigation in the event of an accident and so assess this question as **2c**, Score **4**.

Q3:	How much responsibility does this organisation have for data safety?

The Health Organisation is responsible for deploying systems in compliance with DCB0160 [12] and is

ultimately responsible for patient safety. The Health Organisation assesses this as **3e**, Score **12**.

Q5:	How mature is this organisation regarding data safety?

The Health Organisation has only recently acquired the expertise to apply DCB0160 and is still developing its capability. Safety Data Management is new to the organisation and it anticipates some resistance from senior management after the expenditure incurred in rolling out a DCB0160 compliant safety management system. This question is assessed as **5d**, Score **7**.

The resulting score for the Health Organisation is **43**. This is **ODR3**; medium to high risk. The Health Organisation aims to ***Plan the assessment*** through a Clinical Risk Management Plan. This plan defines the organisation and system context in more detail and lays out the planned activities for identifying, evaluating and treating data safety related risks.

As with the Manufacturer, the Health Organisation needs to ***Identify Data Artefacts*** that are potential sources of safety hazards and understand the context of their use in its lifecycle. Post acceptance, the procuring Health Organisation plans to run a series of user training sessions for clinicians. Once users are trained, the system will be integrated into live operations. The Health Organisation identifies the Infrastructure, Verification and Dynamic Data Categories to be used during these phases. The Health Organisation also realises that the system will form part of a data supply chain as a number of external organisations and departments within their own organisation engage in the procurement and use of safety-related data. For example, it will receive referral data from a number of other General Practitioner (GP) systems, it will receive outcome measures from hospitals and clinical data acquired from remote workers visiting patients in the community and also from the patients themselves using the system's online portal. The system also produces data for other external systems such as electronic prescriptions for pharmacies.

The Health Organisation sees that by using the new system it will become a Commissioning User as it will require and be a **Consumer** of data from a variety of sources; these sources are: GP's systems, hospital systems, systems used by remote workers in the community and the system's portal capturing data entered by the patients themselves, each of these acting as **Data Provisioners**. Those health care professionals (and the patient themselves) gathering patient data through physical inspections and measurement are the **Data Acquirers**.

The Health Organisation defines the data supply chain relevant to the system including the roles and interfaces involved in its Clinical Risk Management Plan. This will therefore show where there are dependencies on **Dynamic Data** used and produced by the system.

Questions the Health Organisation will need to address when establishing the context are:

- Have all the dependent interfaces been identified?
- Have the roles of Commissioning User / Data Provider / Data Acquirer been established and acknowledged?
- What 'service levels' or contracts exist for the delivery of the data?
- What level of assurance do Data Providers/Data Acquirers provide for their data?

7.3 Risk Identification

The Manufacturer aims to carry out the following activities to meet the guidance objectives for the Risk Identification phase.


System Manufacturer

- Review the general, historical perspective;
- Conduct a top-down approach;
- Conduct a bottom-up approach; and
- Update planning documents.

Before embarking on any hazard analysis, the Manufacturer ensures that Stakeholders ***Review the general, historical perspective***. This takes the form of a refresh briefing to raise awareness of issues that are specific to data such as ageing, biasing and defaults.

The Manufacturer of the Health IT System decides that during the prototyping phase there is little safety dependency of the test and configuration data sets as no clinical decisions will be made based on their content; the data is simply being used to support the elaboration of requirements.

In later phases however, when the system functionality is specified and the system is being built, the Manufacturer will want to create a test data set that will be instrumental in demonstrating the correct functioning of the system. This still involves the use of **Verification Data** and **Infrastructure Data** but there is far greater dependency on these data sets than the previous case. For example, if the verification or configuration data is not sufficiently diverse or insufficiently models real world scenarios, it is possible that erroneous and unsafe functional behaviour is present in the system during live operation despite this system having passed factory and site acceptance testing.

To analyse the risks in more detail the Manufacturer uses a ***Top-down approach*** and a ***Bottom-up approach***. In the first approach it considers each of the system functions (such as clinical screens) and analyses where there is a dependency on data and the properties that need to be preserved. In the second, as much of the functionality is driven by data flows in and out of the system, the Manufacturer also looks at specific data flows and assesses the impact if there are loss of properties for the data in those flows.

On completion of the risk identification phase the Manufacturer ***Updates planning documents*** such as the Clinical Risk Management Plan to reflect the outcome of the analysis.


Health Organisation

The Health Organisation will likewise need to conduct risk identification relevant to their deployment context. Hazards arising from data sources that are to be delivered into the new system from existing systems need to be assessed for data risks. As with the Manufacturer, a briefing to Stakeholders to ***Review the general, historical perspective*** is first conducted to cover generic data safety issues but also to highlight lessons learnt from previous accidents and incidents that have occurred in the Health Organisation itself.

As with the Manufacturer, both a ***Top-down approach*** and a ***Bottom-up approach*** is adopted. From the Health Organisation's perspective, one key focus for hazard identification is in the use of **Dynamic Data**, i.e., data that will be delivered into the new system from existing system data sources, and the data presented to the user. For the interactions identified in the supply chain, the Health Organisation needs to consider the risks associated with loss of properties of the data it will receive. Questions the Health Organisation will need to consider and address more formally in the Clinical Risk Management Plan are as follows:

- Which data sets or items being received from other systems have Data Properties (such as timeliness, completeness, consistency, fidelity etc.) that are significant to patient safety?
- What data presented to the user has Data Properties (such as availability, format, resolution, etc.) that are significant to patient safety?
- What existing barriers or mitigations (physical, technical, procedural) exist to reduce the risk of loss of Data Properties?
- Will any existing barriers be lost as a consequence of the new system?

On completion of the Risk Identification phase the Health Organisation will ***Update planning documents*** such as the Clinical Risk Management Plan to reflect the outcome of the analysis.

7.4 Risk Analysis

In this phase identified hazards are assessed to determine their likelihood and severity. To meet the guidance objectives the following activities are carried out:

System Manufacturer

- Establish DSALs; and
- Analyse DSALs as part of system safety activities.

The Manufacturer will ***Establish DSALs*** by considering cases where the use of specific categories of data could give rise to hazards. In the first, the prototyping phase, the Manufacturer sees no use of the data that can give rise to credible clinical risk and assessing the DSAL for that data set as **DSAL0**.

In the second phase of the development lifecycle, where **Verification Data** and **Infrastructure Data** is being used to demonstrate the correct functioning of the system, the Manufacturer considers that loss of any of the Data Properties of **Integrity, Completeness, Consistency, Continuity, Format, Accuracy, Resolution, Timeliness, Availability, Fidelity / Representation, Sequencing, Intended Destination / Usage** of this data could give rise to hazards.

For example, if the verification data set selected is not representative of the eventual diversity experienced in practice (loss of Fidelity / Representation), then it is possible that the system may contain latent software errors that could give rise to harm. However, the Manufacturer acknowledges that the system will be subject to further testing and trials in the clinical setting and so there will be other opportunities to detect errors in the system. Overall:

- The likelihood of the data use gives rise to an accident is **Medium** as other systems and processes are in place that would detect errors; and
- The severity is **Moderate**; failings in the system could give rise to non-optimal treatment plans for a patient that might delay detection of a more serious condition or prolong the recovery for a known condition.

The Manufacturer therefore assesses these data categories as **DSAL1** in this particular context of use.

The Manufacturer takes care to ***Analyse DSALs as part of system safety activities*** by documenting these assessments along with other hardware and software safety considerations, for example those arising from DCB0129, in the Clinical Risk Management Plan.

From the Health Organisation's perspective, the main focus for risk assessment to ***Establish DSALs*** is in the use of ***Dynamic Data***. For the interactions identified in the supply chain the Health Organisation needs to consider the risks associated with loss of properties of the data it will receive and present to the user. Questions the Health Organisation will need to consider and address more formally in the Clinical Risk Management Plan are as follows:

- How likely is it that there would be a loss of the given Data Property?
- How would such a loss of a Data Property be detected?
- How would such as loss be isolated to prevent further risks of harm?
- What recovery action would be required to resolve the issue to maintain patient safety?

Concerns were raised about the vulnerability of the system to inadvertent data overload from the large number of potential data sources, and possibly from malicious activity. This led to the addition of the **Goldilocks** property to the list of Data Properties applicable to the live system.

In considering the receipt of outcome measures data received from a clinic or hospital, the Health Organisation considers that it is likely that some credible errors would not be readily detected by their new system; if the hospital system confused a result or there were errors in the precision of data then there would be few chances to catch these once received by the system.

- The Health Organisations assesses the likelihood of this loss of property as **High**; and
- The impact of such errors, although not realistically likely to lead to death, could result in delays to treatment that could result in serious injury and hence **Moderate** impact.

The data received from this data source is therefore classed as **DSAL2** in this particular context of use.

The Health Organisation takes care to ***Analyse DSALs*** as part of system safety activities by documenting these assessments along with other hardware and software safety considerations (e.g., arising from DCB0160 requirements) in the Clinical Risk Management Plan.

7.5 Risk Evaluation and Treatment

The Manufacturer carries out the following activities to meet the guidance objectives:

- Review each risk and either: Avoid; Accept; Transfer; Treat;
- Establish treatment methods for relevant risks; and
- Implement and verify treatment methods.

The Manufacturer decides to ***Review each risk and either: Avoid; Accept; Transfer; or Treat the risk***. It decides to **Accept** the **DSAL0** risk but as it has determined there is some, albeit low, risk (**DSAL1**) associated with its use of data at a specific point of its lifecycle, it decides to **Treat** that risk. The Manufacturer evaluates this risk and considers that the risks should be reduced further by taking some reasonably practicable steps.

Having decided that further risk reduction is necessary, the Manufacturer needs to ***Establish treatment methods for relevant risks*** that are appropriate for DSAL1 data and in doing so demonstrate that reasonably practicable steps have been taken to reduce the risk. The Manufacturer therefore refers to the tables in the Data Safety Guidance document. The Manufacturer then documents in its Clinical Risk Management Plan:

- Planned compliance with the tables;
- The interpretation for the given method/technique (e.g. depth of checking); and
- Justification in the case where a technique is not to be adopted.

For **DSAL1** Verification Data, the tables show that the following are recommended (R) or highly recommended (HR) where loss of Data Properties **Integrity, Completeness, Consistency, Continuity, Format, Accuracy, Resolution, Timeliness, Availability, Fidelity / Representation, Sequencing, Intended Destination / Usage, Goldilocks** can give rise to a number of hazards. The extracts below indicate the mitigation techniques identified from the tables which should form the basis of the data safety requirements.

Table 21: Worked example: Filtered Techniques tables

Ref	Technique	R/HR	System Design (extracted from Table 13)
SD.17	Sanity / Reasonability Checks	R	Dedicated processing implemented to check that data is within reasonable tolerances and / or logically / semantically consistent (e.g., range checks, date checks, record counts, record sizes, special values - NaN).
SD.20	Syntax Checks	R	Semantic checking of data values and sequences based on defined rule sets.

Ref	Technique	R/HR	Data Design (extracted from Table 14)
DD.01	Governance Model	R	A governance model is established that defines, e.g., data ownership, processing roles and responsibilities, processing authorisations and permissions.
DD.03	Data Flow Diagram	HR	To describe the data flow in a diagrammatic form.
DD.04	Data Model	HR	To articulate how data is organised.
DD.05	Client Sign-Off	R	Agreement from the client that the data is appropriate.
DD.08	Data Dictionary	HR	A collection of descriptions of the data objects or items in a data model for the benefit of data users.

Ref	Technique	R/HR	Data Implementation (extracted from Table 15)
DI.01	Review / Inspection	HR	Manual review / inspection of data possibly involving data visualisation tools.
DI.03	Ground-Truth Check	R	Inspection against physical measurements (e.g., lengths, positions, heights) taken in the real world.
DI.04	Auditing	R	A period of comprehensive internal and external testing of the data quality process.

Ref	Technique	R/HR	Data Implementation
DI.09	Authorisation	R	A security model is established to control who is authorised to create, view, edit, delete the data.
DI.11	Defined Confidence / Trust Levels	R	Criteria are established to provide an objective measurement of the confidence or trust in a given data set.

Ref	Technique	R/HR	Data Migration (extracted from Table 16)
No relevant techniques			

Ref	Technique	R/HR	Data Checking (extracted from Table 17)
No relevant techniques			

Ref	Technique	R/HR	Test Data (extracted from Table 18)
TD.01	Using Informal / Ad-hoc Means	R	Data is generated by simple means (e.g, spreadsheets, scripts, basic assumptions). There is no formal checking or review of the method of generation.
TD.05	Using Manual Means	R	Simple test data can be produced by manual means, although this may be prone to human error.
TD.08	Using Initial Runs of New System	R	This method is often used where the system is breaking new ground and there is no prototype or legacy system to produce test data. Initial operations may differ from eventual usage, so test data must evolve.
TD.09	Derived from Real Data	R	Where real data is available this is usually a good basis for generating test data (e.g., by modification to increase the test space coverage).
TD.11	Produced by Client	R	Ideally the client is involved in producing or at least checking the test data.
TD.12	Client Sign-Off	R	Where possible, the client should formally agree and sign-off the test data as appropriate.
TD.13	Error Seeding	R	This is where errors are deliberately inserted into the data set to demonstrate the effectiveness of data validation.
TD.14	Data Reuse	R	Reusing data for one project that was created and thoroughly assured for another project. This can be effective but the read-across should be established.
TD.15	Feedback Testing	R	To check output data by comparing it with the input source.

Ref	Technique	R/HR	Media - Paper (extracted from Table 19)
MP.01	Photographic Copies	R	Photocopy and store separately.

Ref	Technique	R/HR	Media - Paper
MP.02	Scan to Electronic Format	R	Retain both paper and electronic copies.
MP.10	Indexing / Cataloguing	R	To support efficient accessibility.

Ref	Technique	R/HR	Media - Electronic (extracted from Table 20)
ME.01	Regular Refresh / Rewrite	R	Of magnetic media or flash memory.
ME.02	Suitable Physical Environment	R	Store media in a clean, low-humidity environment at a steady temperature, cool but not cold.
ME.03	Copies at Different Locations	R	Physically separate to cover natural disasters, accidental or malicious damage.
ME.04	Backups / Duplication	R	Backups are essential. Frequency of backup depends on rate of change. The number of generations to keep relates to the impact of data loss.
ME.05	Sample Restores	R	Sample restores should be performed at intervals to ensure that the backups are readable and retrievable.

From these tables the Manufacturer decides on a series of activities to implement the recommendations that are applicable to its particular endeavour. These activities are expressed as a series of requirements that can be placed on the Manufacturer's delivery organisation and tracked through to completion.

Table 22: Worked example: Derived data safety requirements

Ref	Requirement	Guidance Reference
R1	The verification data shall be carefully controlled in the Manufacturer's configuration management system. There shall be a configuration management plan that shall define who has responsibility for the data and who is authorised to create and amend it.	DD.01, DI.09
R2	The verification data shall be held on an industry standard file share that is regularly backed up with copies moved periodically to offsite storage. The Backup / Recovery plans shall include periodic sampling of restores.	ME.01, ME.02, ME.03, ME.04, ME.05
R3	The data shall be modelled as a series of patient "journeys" that cover the entire lifecycle of data from first encounter through to archival and deletion of data. The complete set of journeys shall be chosen to exercise all the functionality of the system. The modelling shall include a data dictionary, data flow diagrams and a data model.	DD.03, DD.04, DD.08
R4	To model data from external systems, the Manufacturer shall use manual data entry and spreadsheet based records to hold the data.	TD.01, TD.05

Continued on next page

Table 22: Worked example: Derived data safety requirements (continued)

Ref	Requirement	Guidance Reference
R5	The Manufacturer has a set of clinical standing data that was used for another system and derived from real data. It includes encounter codes, clinical terms, consultant names, surgery and hospital addresses etc. and can be reused for this system. The Manufacturer's Clinical Safety Officer has reviewed the data and agreed its suitability for reuse.	TD.09, TD.14
R6	Some of the verification data sets shall include errors deliberately inserted to check the effectiveness of data validation.	TD.13
R7	The controlled verification data set shall be subject to review and analysis against defined confidence/trust criteria. Scripts shall be written to check for syntax and semantic consistency of the data and provide a basic sanity check. The scripts themselves shall be validated and verified before use.	SD.17, SD.20, DI.01, DI.03, DI.11
R8	The project shall be subject to an internal delivery quality assurance audit.	DI.04
R9	Data loaded from external system into the system and displayed to the user shall be crosschecked against the original source data, using manual spot-checks.	TD.15
R10	The level of rigour employed in verifying all the above requirements shall be commensurate with the DSAL criticality and so an ISO9001 compliant quality management system shall be adopted.	All

The following guidance recommendations were not adopted by the Manufacturer for the reasons given. Note that some may however become relevant in the future so actions are set, where appropriate, to review the applicability of the recommendation when the given condition is met.

Table 23: Worked example: Rejected data safety requirements

Ref	Guidance Reference	Justification	Action
E1	TD.08	The data will be used before any initial run of the system.	Review when data from initial runs is available.
E2	DD.05, TD.11, TD.12	The system is a new development with no contracted client, so it will not be possible to get the client to create or signoff data.	Review when contracting with a client.
E3	MP.01, MP.02, MP.10	There are no paper based resources for this system.	No further action.

Having determined the requirements arising from the data safety analysis the Manufacturer ensures these are included along with other system requirements as part of the overall delivery and operation of the system. It then remains for the Manufacturer to ***Implement and verify treatment methods***, that is, as well as defining requirements the Clinical Risk Management Plan needs to ensure activities are in place to verify and evidence that treatments have actually been implemented.

Likewise, the Health Organisation has identified DSAL2 data and in deciding to Treat the risk, it aims to ensure risks are reduced as low as reasonably practicable.

Appendix A Linking Principles and Objectives (Informative)

> *I'm a bit of a freak for evidence-based analysis. I strongly believe in data.*
> ***Gus O'Donnell***

A.1 General

The Data Safety Assurance Principles provide the underpinning philosophy for Data Safety Guidance (DSG). Conversely, an implementation of the guidance would be based around the objectives. It is thus appropriate to consider how meeting the objectives results in the Principles being satisfied. To that end, each Principle is considered in turn in the following paragraphs.

A.2 Principle 1

Data Safety Requirements shall be defined to address the data contribution to system hazards.

This Principle asks that requirements be defined. Hence, it is related to the Objective that:

- 4-1 Data Safety Requirements SHALL be established and elaborated.

However, that relationship does not tell the full story. In particular, the Principle is focussed at a system-level, whereas the above Objective is most likely to apply at more detailed levels of design. The following two objectives provide a system-level perspective on risks (from which specific requirements are developed) and hence both objectives directly support this Principle:

- 1-3 Data Artefacts SHALL be identified.
- 2-3 Risks SHALL be identified and linked to Data Artefacts and Data Properties.

A.3 Principle 2

The intent of Data Safety Requirements shall be maintained throughout requirements decomposition.

This Principle is based on standard systems engineering practises whereby a system is gradually developed at increasing levels of design detail. In order to cater for a wide range of systems, across a wide range of economic sectors, DSG does not specifically require an explicit hierarchical decomposition of requirements. However, it does note that, if necessary, Data Artefacts may be defined at a number of levels of increasing detail. Hence, the following two objectives are related to Principle 2:

- 1-3 Data Artefacts SHALL be identified.
- 2-3 Risks SHALL be identified and linked to Data Artefacts and Data Properties.

At a more fundamental level, this Principle is concerned with translating from high-level requirements to something that can be implemented. Data Safety Assurance Levels are a key element of this translation. As such, the following three objectives are also relevant:

- 3-1 Data Safety Assurance Levels SHALL be established.
- 3-2 Data Safety Assurance Levels SHALL be justified.
- 3-3 Data Safety Assurance Levels SHALL be incorporated into system safety activities.

Note that the third of these objectives could also provide a direct link to hierarchical decomposition, if that activity is part of the system safety activities conducted by the organisation implementing DSG.

As noted earlier, this Principle is about identifying low-level design descriptions that, firstly, satisfy the intent of the high-level requirements and, secondly, are described in sufficient detail to allow them to be implemented (and for this implementation to be verified). From the perspective of DSG these low-level items are Data Safety Requirements. Consequently, the following Objective also supports this Principle:

- 4-1 Data Safety Requirements SHALL be established and elaborated.

A.4 Principle 3

Data Safety Requirements shall be satisfied.

This Principle is straightforward. It involves implementing the low-level design descriptions and verifying these implementations. As such, it is directly supported by the following objectives:

- 4-2 Methods used to provide Data Safety assurance SHALL be defined and implemented.
- 4-3 Compliance with Data Safety Requirements SHALL be demonstrated.

A.5 Principle 4

Hazardous system behaviour arising from the system's use of data shall be identified and mitigated.

From one perspective this Principle is about looking bottom-up to determine whether the detailed design decisions have introduced any new system-level risks. A HAZOP is one way this can be achieved. Similarly, a HAZOP is one of several techniques that DSG suggests can be used to achieve the following objectives, which consequently may support Principle 4:

- 2-2 Unintended behaviour resulting from data SHALL be identified and analysed.
- 2-3 Risks SHALL be identified and linked to Data Artefacts and Data Properties.

More generally, identifying potential new system-level hazards introduced by detailed design decisions involves looking at the system from a variety of perspectives. One perspective that is useful is provided by historical accidents and incidents; another useful perspective is provided by top-level generic data-related issues, distilled from experience across a wide range of systems and activities. Hence, the following Objective also supports Principle 4:

- 2-1 Historical data-related accidents and incidents SHALL be reviewed.

In addition, understanding the system context and intended use, as well as perspectives provided by a suitably wide collection of Stakeholders can inform risk considerations. Likewise, potential issues can also be identified by considering the boundaries of the system. It follows that the following three objectives are also relevant to Principle 4:

- 1-1 System context and intended use SHALL be established.
- 1-2 Key Stakeholders SHALL be identified.
- 1-4 Interfaces SHALL be defined and managed.

A.6 Principle 4 + 1

The confidence established in addressing the Data Safety Assurance Principles shall be commensurate to the contribution of data to system risk.

This Principle provides a means of balancing available effort against risk. From the perspective of DSG, this is provided by Data Safety Assurance Levels. As such, this Principle is directly supported by the following three objectives:

- 3-1 Data Safety Assurance Levels SHALL be established.
- 3-2 Data Safety Assurance Levels SHALL be justified.
- 3-3 Data Safety Assurance Levels SHALL be incorporated into system safety activities.

A.7 Summary Table

For ease of reference, Table 24 summarises links between the Principles and objectives; these are shown by an "X" in the relevant cell. For completeness, this table shows the phase associated with each group of objectives.

Two things are apparent from this table. Firstly, each Principle is supported by at least two objectives. Secondly, with one exception, each Objective supports at least one Principle. The exception is the Objective that "A Data Safety Assessment SHALL be planned", which acts as an overarching Objective to ensure there is sufficient resource to meet the other objectives. For this reason it is loosely associated with each Principle; this is shown by an "o" in relevant cells.

Having each Principle supported by at least two objectives, along with the descriptive text above, provides confidence that meeting the objectives will satisfy the Principles; equivalently, it provides confident that the collection of objectives is *sufficient* to satisfy the Principles.

In addition, every Objective supporting at least one Principle (with the exception noted above) indicates that there is value in each Objective being included in DSG. This observation is not quite enough to demonstrate that the collection of objectives is *necessary* to satisfy the Principles. However, given the small number of objectives and the apparent lack of overlap between them, it is sufficient to suggest the necessity of the objectives.

Table 24: Principles and objectives: summary table

	Principle				
	P1	**P2**	**P3**	**P4**	**P4+1**
Establish Context					
1-1 System context and intended use SHALL be established.				X	
1-2 Key Stakeholders SHALL be identified.				X	
1-3 Data Artefacts SHALL be identified.	X	X			
1-4 Interfaces SHALL be defined and managed.				X	
1-5 A Data Safety Assessment SHALL be planned.	o	o	o	o	o
Identify Risks					
2-1 Historical data-related accidents and incidents SHALL be reviewed.				X	
2-2 Unintended behaviour resulting from data SHALL be identified and analysed.				X	
2-3 Risks SHALL be identified and linked to Data Artefacts and Data Properties.	X	X		X	
Analyse Risks					
3-1 Data Safety Assurance Levels SHALL be established.		X			X
3-2 Data Safety Assurance Levels SHALL be justified.		X			X
3-3 Data Safety Assurance Levels SHALL be incorporated into system safety activities.		X			X
Evaluate and Treat Risks					
4-1 Data Safety Requirements SHALL be established and elaborated.	X	X			
4-2 Methods used to provide Data Safety assurance SHALL be defined and implemented.			X		
4-3 Compliance with Data Safety Requirements SHALL be demonstrated.			X		

Appendix B Organisational Data Risk Assessment (Informative)

> *Data is becoming the new raw material of business.*
> ***Craig Mundie***

Note: this questionnaire only provides an initial organisational data risk level assessment. Further work is required to establish the safety data risks in detail such as determining a Data Safety Assurance Level (DSAL) for relevant data sets.

Organisational Data Risk (ODR) Assessment Form			
This form is used to determine the safety risk related to data for a particular organisation and usage. *This form must be completed from the perspective of **one** of the organisations involved; typically this will be the organisation using the data or the contractor supplying the system that handles the data. This form needs to be completed for each instance / application / scope / risk profile and should consider a defined boundary for the analysis, e.g. the scope of supply for the contractor or the limit of the data user's operational responsibility. It may be useful for both contracting parties to complete the form from their respective positions to check the data risk responsibilities and apportionment.* *It is anticipated that this form will be used during early phases of a procurement or supply and also for changes to existing supplies. It can also be used to assess existing legacy scenarios.* *Answer the questions as they apply in the context of the scope of supply. Mark the response with the "best" fit for the given scenario. Note that not all elements have to be satisfied. For each response also add a brief justification for that particular selection as opposed to any other choice.* *If the answer to a question is completely unknown at this stage; it is suggested that the middle value or higher is chosen and an explanation added to the justification.* *When all the relevant questions have been answered and justified, add the scores together to give a final total and record the value in the appropriate field. Use this total to determine the final ODR level based on the stated ranges.* *The ODR level determined may be used to support process tailoring and to determine the management regime required to mitigate the risk associated with the data.*			
Data Scenario/Context Name:			
Data Scenario/Context Description:			
Scope/Data Boundary and Perspective:			
Completed By:		Date Completed:	

Organisational Data Risk (ODR) Assessment Form
Answer each question using the response that forms the best match for the particular scenario. Not all statements have to be satisfied and some judgement is required; it is expected that the majority of statements in the selected response can be satisfied with some interpretation. The use of multiple criteria in each question enables a smaller and manageable set of questions to be posed to provide a holistic view of the overall risk.

QUESTION 1 — SEVERITY AND PROXIMITY			
How severe could an accident be that is related to the data? Could it be caused directly by the data? *This question considers the safety consequence, the proximity and contribution of the data to the accident sequence.*			
1a	All currently foreseen uses of the data could not contribute to an accident. The data is not relied upon for safe operation. Negligible environmental impact.	1	❑
1b	A possible use of data could contribute to a minor accident, but only via lengthy and indirect routes. Could lead to minor injury or temporary discomfort for 1 or 2 people. Many other people/systems are involved in checking the data. Some aspects of safe operation rely very indirectly on the data. Minor environmental impact only via indirect routes.	2	❑
1c	A use of the data could lead to a significant accident resulting in minor injuries affecting several people or one serious injury. Several other people/systems are involved in checking the data. There is a dependency on the data for safe operation. Environmental impact is possible.	4	❑
1d	A likely use of the data could directly lead to a serious accident resulting in serious injuries affecting a number of people, or a single death. One human or independent check is involved for all data. There is major dependency on the data for safe operation. Major environmental impact is possible.	8	❑
1e	An intended use of the data could lead to an accident resulting in death for several people. The accident could be caused by the data with little chance of anything else detecting and mitigating the data issues. The accident could affect the general public or cause catastrophic environmental impact.	16	❑
Justification:			

QUESTION 2 — ORGANISATIONAL AND SOCIETAL IMPACT			
What would be the impact on the organisation, client or public if an accident occurred related to the data? *This question considers the tolerability within this industry sector and the general public. How much would it affect the organisation or society? Would a claim be likely? Would it generate press interest? Would a formal investigation ensue?*			
2a	Little interest, accidents happen all the time in this sector; very high societal tolerability. Negligible chance of claims or investigations. No adverse publicity likely.	1	❑
2b	Some concern from the client, but accidents happen occasionally; high societal tolerability. Small chance of claim against the organisation. Local or specialist press interest. Minor investigation or audit.	2	❑
2c	Public would be concerned, accidents are rare in this sector; some societal tolerability. Significant chance of claim against the organisation. Regional press interest. Client inquiry or investigation likely.	4	❑

QUESTION 2 — ORGANISATIONAL AND SOCIETAL IMPACT			
2d	Public would be alarmed and consider the accident a result of poor practice; little societal tolerability. Claims very likely. National press or media coverage a possibility. Legal or independent inquiry may follow.	8	❑
2e	Public would be outraged and consider such an accident unacceptable; almost no societal tolerability. Multiple claims/fines from regulators or courts are likely. International press or media coverage. Official and / or public enquiry possible.	16	❑
Justification:			

QUESTION 3 — RESPONSIBILITY			
How much responsibility does this organisation have for data safety? *This question considers how much legal and other responsibility and ownership the organisation has for data safety aspects within this scenario. What liabilities for consequential losses/3rd party claims does the organisation have via the contract or other means? What is the scale of the organisation's contribution to the overall scope?*			
3a	The organisation is not responsible for any data safety aspects. No liabilities for accident claims related to the data lie with the organisation. Client or other party has accepted full data safety responsibility. The organisation is fully covered and indemnified by the client or a 3rd party.	1	❑
3b	The organisation is a small part of a large consortium. It has minimal liability for data safety via the contract. It is partly covered by explicit client or 3rd party protections. All safety data is managed by subcontractors, the organisation only reviews and monitors.	2	❑
3c	The organisation is a significant part of the consortium team. It has some share of the data safety responsibility. Specific data safety liabilities to the client via the contract are mentioned. There are no indemnities in the organisation's favour. All key safety data obligations are explicitly flowed down to subcontractors.	4	❑
3d	The organisation is prime for a small programme or has the bulk of the data safety responsibility within a team. Specific accident-related liabilities in the contract are significant. The organisation provides some indemnities to others via the contract. Some significant data safety obligations are not flowed down to subcontractors.	7	❑
3e	The organisation is priming a major programme or has total data safety responsibility. Specific accident-related liabilities in the contract are large (or unlimited). The organisation provides explicit indemnities in favour of the client/3rd parties for accidents. Safety data obligations have not been discussed or are not flowed down to subcontractors.	12	❑
Justification:			

QUESTION 4 — LEGAL AND REGULATORY FRAMEWORK			
What legal and regulatory environment will this work be subject to? *This question considers the legal and regulatory obligations that this work will have to conform to. How well is the legal framework defined and understood? Is there an established standards culture? Is there a regulator and certification process?*			
4a	Well understood and tested legal framework, one jurisdiction. Highly regulated sector with one overseeing body. Well established industry guidelines and standards for safety data. Formal certification processes.	1	❑
4b	Understood and established legal framework, a few related jurisdictions. Regulated sector, more than one overseeing body. Industry guidelines and standards for safety data. Some formal certification processes.	2	❑
4c	Some understanding of legal position, several jurisdictions. Partially regulated sector, several possible overseeing bodies. Some industry guidelines and standards that refer to data. Informal certification processes.	4	❑
4d	Complex, poorly defined legal position, multiple different jurisdictions. Largely unregulated sector with no established overseeing body. Some industry guidelines and standards that mention data. Some informal certification processes.	6	❑
4e	Very complex, untested and unclear legal position, many diverse jurisdictions. Unregulated sector with no overseeing body. No industry guidelines or standards for data. No certification processes.	10	❑
Justification:			

QUESTION 5 — ORGANISATIONAL MATURITY			
How mature is this organisation regarding data safety? *This question considers the maturity of the organisation in relation to awareness and management of the risks associated with safety data. Are staff trained, managed and resourced to enable proper handling of data safety risk?*			
5a	Explicit recognition of data as a source of safety risk. Formal and established processes and procedures in place for the identification and control of safety data. Staff trained and fully aware of safety data risks. Senior management fully aware and supportive of data safety management activities. Management of safety data risks fully supported and funded.	1	❑
5b	Awareness of data as a source of safety risk. Informal processes and procedures in place for the identification and control of safety data. Staff awareness of safety data risks. Senior management awareness of data safety management issues. Good support and funding for management of safety data risks.	2	❑
5c	Some awareness of data as a source of safety risk. Some ad-hoc processes and procedures in place for the identification and control of safety data. Some staff awareness of safety data risks. Some senior management awareness of data safety management issues. Some support or partial funding for management of safety data risks.	4	❑

QUESTION 5 — ORGANISATIONAL MATURITY			
5d	Little awareness of data as a source of safety risk. Minimal processes or procedures in place for the identification and control of safety data. Little staff awareness of safety data risks. Little senior management awareness of data safety management issues. Little support or minimal funding for management of safety data risks.	7	❑
5e	No recognition of data as a source of safety risk. No processes or procedures in place for the identification or control of safety data. No staff training or awareness of safety data risks. Senior management not aware or in denial of safety data risks. No support or funding for management of safety data risks.	10	❑
Justification:			

QUESTION 6 — OWNERSHIP AND USAGE			
How widely is the data used and who by? *This question considers how much usage and what type of users there are likely to be of the data. How complex is the data supply chain? In what geographies is it used? How many owners and interfaces are there?*			
6a	Minimal or infrequent usage. One Data Owner, a specialist highly trained user group. Single organisation or recipient usage only.	1	❑
6b	A number of operational data users. Simple linear supply chain. More than one Data Owner. Specialist user or limited public access. Small scale operation. No general web access. Few user organisations or recipients.	2	❑
6c	Regional usage. Some public or mainstream usage. A few supply chains. A few Data Owners. Some web access. Several user organisations or recipients.	4	❑
6d	National usage. Public or mainstream usage. Several supply chains. Several Data Owners. Web access. Some or varied user organisations or recipients.	7	❑
6e	International usage. Extensive public or mainstream usage. Extensive web access. Many complex supply chains. Many and diverse Data Owners. Many and diverse user organisations or recipients.	12	❑
Justification:			

QUESTION 7 — SIZE, COMPLEXITY AND NOVELTY			
What is the scale, sophistication and complexity of the data and its manipulation? *This question considers the nature of the data, its lifecycle and how easy it is to detect errors in the data.*			
7a	Simple data structures. Mature and established data storage and manipulation techniques and technologies. One or two interfaces. No timeliness aspects. No transformations. Data is easily verifiable. Data is easily traceable to original source.	1	❑

QUESTION 7 — SIZE, COMPLEXITY AND NOVELTY			
7b	Varied data structures. Mainstream data storage and manipulation techniques and technologies. Several interfaces. Few timeliness aspects. Few data transformations. Data is verifiable. Data is traceable to original source.	2	❑
7c	Complex with some unstructured data. Current data storage and manipulation techniques and technologies. Multiple interfaces. Some timeliness aspects. Some data transformations. Data is difficult to verify. Data is difficult to trace back to original source.	4	❑
7d	Complex, varied or partially unstructured data. Novel storage and manipulation techniques and technologies. Multiple complex interfaces. Time critical. Complex data transformations. Data is very difficult to verify. Data is very difficult to trace back to original source.	7	❑
7e	Highly complex, varied or unstructured data. Highly novel storage and manipulation techniques and technologies. Many and complex, ill-defined or dynamic interfaces. Highly time critical. Many and complex data transformations. Data is infeasible to verify. Data is impossible to trace back to original source.	10	❑
Justification:			

QUESTION 8 — BOUNDARIES AND INTERFACES			
How well defined and understood are the boundaries and interfaces for this data scenario? *This question considers the number, complexity and definition status of the boundaries and interfaces where data is exchanged. How well understood are the boundaries and interfaces? Are standard formats and protocols used? Is data exchange time critical? Are all assumptions and ambiguities relating to the data exchange resolved?*			
8a	One well-understood boundary and few, well-defined interfaces. Standard interface formats and protocols. No timeliness aspects to data exchange. No remaining ambiguities, TBCs or TBDs. No assumptions.	1	❑
8b	A few, understood boundaries and several defined interfaces. Mainly standard interface formats and protocols. Few timeliness aspects to data exchange. Few areas of ambiguity, few TBCs and TBDs. Few assumptions.	2	❑
8c	Several, established boundaries, some defined, some undefined and some ambiguous interfaces. Mixture of standard and non-standard interface formats and protocols. Some timely data exchanges. Some areas of ambiguity, some TBCs and TBDs. Some assumptions.	4	❑
8d	Many, poorly understood boundaries, many undefined or ambiguous interfaces. Mostly non-standard interface formats and protocols. Time sensitive data exchange. Many areas of ambiguity, many TBCs and TBDs. Many assumptions.	6	❑
8e	A large number of unclear boundaries; a large number of unknown and undefined interfaces. Completely non-standard, complex interface formats and protocols. Real-time data exchange. Large areas of ambiguity, a large number of TBCs and TBDs. A large number of assumptions.	10	❑

QUESTION 8 — BOUNDARIES AND INTERFACES
Justification:

ORGANISATIONAL DATA RISK LEVEL	
Record the total score and use it to determine the ODR level based on the ranges given below. If the first 3 questions' scores sum up to 6 or less then disregard the scores for the remaining questions.	
Score 14 or less	ODR0
Score 15 to 21	ODR1
Score 22 to 37	ODR2
Score 38 to 47	ODR3
Score 48 and above	ODR4
Total Score for this scenario/context:	
ODR Level for this scenario/context:	

Appendix C Data Safety Culture Questionnaire (Informative)

> *Data is the fabric of the modern world: just like we walk down pavements, so we trace routes through data and build knowledge and products out of it.*
> ***Ben Goldacre***

This form helps an organisation appreciate the data safety culture. It can be applied at various levels, including at the project level and at the organisational level.

Data Safety Culture Questionnaire Form			
This form is used to assess the safety culture related to data for a particular programme. **You play a key role in protecting the organisation from data safety risks and your views are important. This self-assessment survey is designed to assess our current level of data safety culture within the programme. The output can help us to improve our safety position.** Please tick the box which reflects your view and answer as honestly as possible. Space is provided for explanatory comments. Your response will only be of value if it reflects what you actually believe is the case, rather than what you believe should happen. If you would like to remain anonymous please print and send this form by post. The survey should take no longer than 10 minutes. It is anticipated that this form will be used on a regular basis (e.g. annually).			
Programme Name:			
Data Scenario/Context Description:			
Completed By:		Date Completed:	
Answer each question as you see it - there is no right answer!			

QUESTION 1 — MY VIEW OF OUR SUPPLY							
		Don't Know	Strongly Disagree	Disagree	Maybe	Agree	Strongly Agree
1a	I see data as an important factor in the safety of my programme.	❑	❑	❑	❑	❑	❑
1b	I am familiar with the safety aspects of our data.	❑	❑	❑	❑	❑	❑
1c	I understand how data in our solution can contribute to an accident.	❑	❑	❑	❑	❑	❑
1d	I think we could be blamed if there were an accident due to our data.	❑	❑	❑	❑	❑	❑
Comments:							

QUESTION 2 — WHAT WE'RE DOING							
		Don't Know	Strongly Disagree	Disagree	Maybe	Agree	Strongly Agree
2a	I think that the programme is aware of data safety risks.	❑	❑	❑	❑	❑	❑
2b	I believe we need to implement measures to manage data safety risks.	❑	❑	❑	❑	❑	❑
2c	I think that the programme meets its obligations (e.g. has a Data Management Plan in place and a role with specific responsibilities in this area).	❑	❑	❑	❑	❑	❑
Comments:							

QUESTION 3 — MY ROLE							
		Don't Know	Strongly Disagree	Disagree	Maybe	Agree	Strongly Agree
3a	I know my role relates to the management of data and associated safety risks.	❑	❑	❑	❑	❑	❑
3b	If I had a safety concern about our data I would report it.	❑	❑	❑	❑	❑	❑
3c	I know who the data safety representative is on my programme.	❑	❑	❑	❑	❑	❑
3d	I have received adequate training regarding data safety for my role.	❑	❑	❑	❑	❑	❑
3e	I feel supported in dealing with data safety risks.	❑	❑	❑	❑	❑	❑
3f	I have adequate time to address any data safety issues.	❑	❑	❑	❑	❑	❑
Comments:							

Appendix D Supplier Data Maturity (Informative)

> *The most valuable thing you can have as a leader is clear data.*
> ***Ruth Porat***

This questionnaire may be used for two purposes:

1. To support a procurement process - distributed by an organisation looking for a company that can handle safety-critical development, because the system they require to be developed is known to have safety-critical requirements
2. Internal audits - used internally by a company developing systems with safety-related data which needs to assure itself of its capability to fulfil customer needs.

Organisation

1. For each software development involving data, is there a designated data safety manager?
2. If so, does the data safety manager report directly to the project manager?
3. Are the management reporting channels for data assurance and software development separate?
4. Is data subject to a formal configuration control process?
5. Is data engineering represented on the system design team?
6. Is data engineering process improvement part of the company quality systems?

Resources, Personnel and Training

1. Are personnel specified as responsible for data safety as a separate role from software and system design and development?
2. Is there a required training programme for data specialists?
3. Is training on data safety issues part of the training for managers or management teams?
4. Is there a formal training programme for data safety design and review leaders

Data Issues Growth Management

1. Is a mechanism employed for maintaining awareness of the state of the art in data safety technology?
2. Is a mechanism employed for comparing the company approach to data safety with external processes for data safety practised elsewhere in the industry?
3. Is a mechanism used for introducing new technologies and processes into system development?
4. Is a mechanism in place for identifying and replacing obsolescent processes related to data safety?

Documented Standards and Procedures

1. Describe any formal procedures adopted at each periodic management review to assess the status of data related to the system.
2. Describe the methods used for ensuring that the data development team understands each data requirement.
3. Is a data risk assessment method used for assessing the use of existing data in new applications?
4. Are data test cases developed formally with a company standard?
5. Is there a document which describes how the customer is to be consulted over data issues?
6. Is particular care taken to capture requirements, design, review and test data for user interfaces?
7. Is there a data risk monitoring and tracking to closure procedure practised?

Process Metrics

1. Are statistics of failures due to data errors during development kept to feedback and learn from in future development?
2. Are data issue action items tracked to closure and reports maintained of causes?
3. Is configuration data separately developed from everyday operational data?
4. Is data test coverage measured and recorded?
5. Are all states, from which configuration data will be required, tested, (including emergency reboot), and results recorded?
6. Are analyses of errors due to data conducted to determine their process related causes?
7. Are the process causes reviewed and changes to processes implemented where appropriate?

Process Control

1. Is regression testing routinely performed when errors are discovered?
2. Is the adequacy of regression testing subject to an assurance process to ensure new errors are not introduced?
3. Is a mechanism used for identifying and resolving system engineering issues that affect data?
4. Is a mechanism used for ensuring traceability between the data requirements and the top level design?
5. Is the importance of data in the system engineering process reviewed to maintain processes at an adequate level to cope with the expanding role of data in the Internet of Things?

Appendix E Data Categories – Detail (Informative)

> *It's difficult to imagine the power that you're going to have when so many different sorts of data are available*
> ***Tim Berners-Lee***

Table 25 provides additional information, in the form of explanations and lists of typical containers, for the identified Data Categories.

Table 25: Categories of safety-related data: detailed definitions

No.	Category	Description	Explanation	Typical containers
			Context	
1	Predictive	Data used to model or predict behaviours and performance	Data for studies, models, prototypes, initial risk assessments, etc. This is the data produced during the initial concept phase which subsequently flows into further development phases.	Prototype results, evaluations, analyses
2	Scope, Assumption and Context	Data used to frame the development, operations or provide context	Restrictions, risk criteria, usage scenarios, etc. explaining how the system will be used and any limitations of use.	Concepts of operation, Safety Case Report Part 1
3	Requirements	Data used to specify what the system has to do	Data encompassing requirements, specifications, internal interface or control definitions, data formats, etc.	Formal specifications, interface control documents, user requirements documents, Safety Case Report Part 1
4	Interface	Data used to enable interfaces between this system and other systems: for operations, initialisation or export from the system	Data that exists to enable exchange between this system and other external systems. Covers start-of-life operations (data import or migration), end-of-life operations and ongoing operational exchange of data between systems.	Protocols, schemas, interface control documents, transition plans, Extract-Transform-Load tool specifications, cleansing and filtering rules
5	Reference or Lookup	Data used across multiple systems with generic usage	Data comprising generic reference information sets used by multiple systems (i.e., not produced solely for this system). Typically updated infrequently, and not specific to this system.	Dictionaries, materials information, sector data reference sets, encyclopedias

Continued on next page

Table 25: Categories of safety-related data: detailed definitions (continued)

No.	Category	Description	Explanation	Typical containers
			Implementation	
6	Design and Development	Data produced during development and implementation	Data encompassing the design and development process artefacts: everything from design models and schemas to document review records. It also includes test documents (specification and results) but not the test data itself.	Design documents, review records, hardware, software, test scripts, code inspection reports, Safety Case Report Part 2
7	Software	Data that is compiled (or interpreted) and executed to achieve the desired system behaviour	From some perspectives it is helpful to consider software (e.g., source code) as another category of data.	Text files, configuration management systems
8	Verification	Data used to test and analyse the system	Data comprising the test values and test data sets used to verify the system. It may include real data, modified real data or synthetic data. It includes data used to drive stubs, and any data files used by simulators or emulators.	Test data sets, stub data, emulator and simulator files
			Configuration	
9	Machine Learning	Data used to train the system to enable it to learn from the characteristics of the data	Data used to train, set up or adapt the system for a particular purpose or configuration. May be subsets of real data or synthetically produced. May have to include or exclude corner cases.	Images for pattern recognition analysis
10	Infrastructure	Data used to configure, tailor or instantiate the system itself	Data used to set up and configure the system for a particular installation, product configuration, or network environment.	Network configuration files, initialisation files, hardware pin settings, network addresses, passwords
11	Behavioural	Data used to change the functionality of the system	Data to enable / disable or configure functions or behaviour of the system.	XML configuration files, Comma Separated Variable (CSV) data, schemas
12	Adaptation	Data used to configure to a particular site	Data used to tailor or calibrate a system to a particular physical site or environment, incorporating physical or environmental conditions.	Configuration files

Continued on next page

Table 25: Categories of safety-related data: detailed definitions (continued)

No.	Category	Description	Explanation	Typical containers
			Capability	
13	Staffing and Training	Data related to staff training, competency, certification and permits	Data which allows staff to perform a function within the wider context of the safety-related system. This may include training records, competency assessments, permits to work, etc.	Human Resources records, training certificates, card systems
			The Built System	
14	Asset	Data about the installed or deployed system and its parts, including maintenance data	Data related to location, condition and maintenance requirements of the system under consideration. This may cover hardware, software and data.	Inventory, asset and maintenance database systems
15	Performance	Data collected or produced about the system during trials, pre-operational phases and live operations	Data produced by and about the system during introduction to service and live service itself. Includes fault data and diagnostic data. This may be the results of various phases of introduction and may include trend analysis to look for long-term problems.	Field data, Support calls, bug reports, non-compliance reports, Defect Reporting And Corrective Action System (DRACAS) data
16	Release	Data used to ensure safe operations per release instance	Explanation of particular features or limitations of a release or instance. May include specific time-limited workarounds and caveats for a release.	Release notes, Certificate of Design (CoD), Transfer documents, Safety Case Report Part 2 or Part 3
17	Instructional	Data used to warn, train or instruct users about the system	Data that explains to users the risks of the systems and gives any mitigations that may be required to be implemented by users, e.g., by process, procedure, workarounds, limitations of use.	Manuals, Standard Operating Procedures (SOPs), on-line help, training courses, Safety Case Report Part 3
18	Evolution	Data about changes after deployment	Data that covers enhancements, formal changes, workarounds, and maintenance issues. It also covers data produced by configuration management activities, such as baselines or branch data.	Change requests, modification requests, issue and version data, configuration management system outputs
19	End of Life	Data about how to stop, remove, replace or dispose of the system	Data covering all activities related to taking the system out of service or mothballing / storage / dormant phases.	Transition, disposal and decommissioning plans

Continued on next page

Table 25: Categories of safety-related data: detailed definitions (continued)

No.	Category	Description	Explanation	Typical containers
20	Stored	Data stored by the system during operations	Data stored or utilised within the system which has end-user meaning. It may be displayed and used within the system or may be for transfer and distribution to other systems or downstream users. It is data that has some real domain meaning.	May be stored internally within the system (e.g., in databases or text files), or transferred into or out of the system through interfaces (e.g., Ethernet)
21	Dynamic	Data manipulated and processed by the system during operations	Data processed, transformed or produced by the system which has end-user meaning. It may be displayed and used within the system or may be for transfer and distribution to other systems or downstream users. It is data that has some real domain meaning.	May be manipulated within the system in data structures or transferred into or out of the system through interfaces
22	Twinning	Data used to create and maintain a digital counterpart of a physical object or process	The digital twin is an up-to-date and accurate model when supplied with accurate and up-to-date data. This may be a model of a physical object's properties and states, including position, status and motion or of a process flow. A digital twin also can be used for monitoring, diagnostics and prognostics to optimize asset performance and utilization. Intelligent maintenance system platforms can use digital twins to find the root cause of problems.	Tooling / modelling environments and bespoke software implementations
Compliance and Liability				
23	Standards and Regulatory	Data that governs the approaches, processes and procedures used to develop safety systems	Data predominantly in the form of documents that describe and dictate the activities, processes, competencies etc. to be used for a particular development in a particular sector.	Standards documents, guidelines, legal directives and laws
24	Justification	Data used to justify the safety position of the system	Data used to justify, explain and make the case for starting or continuing live operations and why they are safe enough. Often passed to external bodies (e.g., regulators, Health and Safety Executive, Independent Safety Auditors) for their review.	Safety Case Report, certification case, regulatory documents, COTS justification file, design justification file

Continued on next page

Table 25: Categories of safety-related data: detailed definitions (continued)

No.	Category	Description	Explanation	Typical containers
25	Investigation	Data used to support accident or incident investigations (i.e., potential evidence)	Data collected or produced during an incident or accident investigation which may be used in investigation reports, lessons learnt or prosecutions. This can be process data, trace data, site data (e.g., photographs of crash site) or may be derived (accident simulations, analyses, etc.).	Incident/accident investigation reports and supporting documents
Meta-Property				
+1	Trustworthiness	(Meta) data which tells us how much the system can be trusted	Data which provides assurance or confidence about the other data within or about the system under consideration. This may be some of the data mentioned in the other categories, but may be different.	Data audits, data quality index measures, sign-off sheets traceability records, model database

This page is intentionally blank

Appendix F HAZOP Guidewords – Detail (Informative)

> *I don't see the logic of rejecting data just because they seem incredible.*
> ***Fred Hoyle***

Table 26 expands upon the HAZOP guidwords presented in Table 7 by adding Data Considerations which may be helpful in determining how to apply the guidewords to a specific instance of a Property.

Table 26: HAZOP guidewords: detailed definitions

Property	Description	HAZOP Data Guidewords	HAZOP Data Considerations
Integrity	The data is correct, true and unaltered	Loss, partial loss, incorrect, multiple	Correctness, truth, original, trustworthy, coherency, stability, perfect, unquestionable, faithful, certain, ordered, unadulterated, unmodified, unchanged, clean, uncontaminated, untainted, proper, flawless, organized, exact, undistorted, faultless, guided, connected, linked, traced, unbiased.
Completeness	The data has nothing missing or lost	Loss, partial loss, incorrect, multiple, insufficient	Whole, complete, entire, finished, done, stable, qualified, certified.
Consistency	The data adheres to a common world view, e.g., units	Loss, partial loss, incorrect, multiple, too early, too late, loss of sequence	Coherent, compatible, congruent, congruous, harmonious, deconflicted, consistent, appropriate, suitable, sound, cleansed.
Continuity	The data is continuous and regular without gaps or breaks	Loss, partial loss, incorrect, late, loss of sequence	Smooth, continuous, regular, gapless, whole, complete, entire, unfragmented.
Format	The data is represented in a way which is readable by those that need to use it	Loss, partial loss, incorrect, multiple	Conformant, suitable, valid, configured, well-formed, setup, composed, well structured, arranged, compliant, organised, exact, unaliased, migrated, transformed.
Accuracy	The data has sufficient detail for its intended use	Loss, partial loss, incorrect, multiple, insufficient	Accurate, true, correct, undistorted, unbiased, faultless.
Resolution	The smallest difference between two adjacent values that can be represented in a data storage, display or transfer system	Loss, partial loss, incorrect, multiple, insufficient	Exact, untruncated, retention of detail, clarity, determination, distinguishable, clear, within range, distinct, separated, discernible, discriminatable, unconfused, divisible, unaliased, granularity, precision.

Continued on next page

Table 26: HAZOP guidewords: detailed definitions (continued)

Property	Description	HAZOP Data Guidewords	HAZOP Data Considerations
Traceability	The data can be linked back to its source or derivation	Loss, partial loss, incorrect, multiple, too early, too late, loss of sequence	Traceable, verifiable, indexed, linked, connected, justified, proven, evidenced, substantiated, continuous, unfragmented, complete, networked.
Timeliness	The data is as up to date as required	Loss, partial loss	Timely, early, ready, expected, unique, appropriate, opportune, ordered, organised, anticipated, seasonable, converging, settling, on-time, latency, lag, lead time, time slots, real-time, determinism, predictable.
Verifiability	The data can be checked and its properties demonstrated to be correct	Loss, incorrect, partial loss, multiple, too early, too late, loss of sequence	Verifiable, provable, checkable, supportable, demonstrable, sustainable, certifiable, defensible, excusable, justifiable, undisputable, irrefutable, validated.
Availability	The data is accessible and usable when an authorized entity demands access	Loss, partial loss, multiple, too early, too late	Ready, available, obtainable, reachable, accessible, serviceable, operable, functional, usable, capable, released, issued, disseminated, distributed.
Fidelity / Representation	How well the data maps to the real world entity it is trying to model	Loss, incorrect, partial loss, multiple, too early, too late	Representative, accurate, faithful, trustworthy, characteristic, normal, standard, real, expected, natural, typical, regular, fit for purpose, validated, separable, associated, correct units/dimensions, stable, unbiased.
Priority	The data is presented / transmitted / made available in the order required	Loss, incorrect, partial loss, multiple, too early, too late	Current, ordered, included, precedence, hierarchy, pre-eminence, retained, ahead, readiness.
Sequencing	The data is preserved in the order required	Loss, incorrect, partial loss, multiple	Ordered, contiguous, unique, ordered, clear, continuous, successive, uninterrupted, sequential.
Intended Destination / Usage	The data is only sent to those that should have it	Loss, incorrect, partial loss, multiple, too early, too late, loss of sequence	Directed, delivered, copied, sent, transmitted, correct recipient, unintercepted, unseen, integral, received, acknowledged, forwarded, filtered.
Accessibility	The data is visible only to those that should see it	Loss, incorrect, partial loss, multiple, too early, too late	Secure, open, visible, reachable, seen, usable, accessible, obtainable, uncompromised, secure, encrypted, preserved.
Suppression	The data is intended never to be used again	Loss, incorrect, partial, too early, too late, too much, too little	Hidden, encrypted, private, confidential, erased, unlinked, unavailable, unaccessible, redacted.

Continued on next page

Table 26: HAZOP guidewords: detailed definitions (continued)

Property	Description	HAZOP Data Guidewords	HAZOP Data Considerations
History	The data has an audit trail of changes	Loss, incorrect, partial loss, multiple	Justifiable, traceable, provable, supportable, demonstrable, sustainable, certifiable, defensible, excusable, justifiable, undisputable, irrefutable.
Lifetime	When does the safety-related data expire	Loss, too early, too late, incorrect, multiple, loss of sequence	Expiry date, age, validity, currency, applicability, durability, duration, lifespan, stretch, tenure, half-life, longevity, span, in-date, best-before, window, established.
Disposability / Deletability	The data can be permanently removed when required	Loss, incorrect, partial, too early, too late	Unavailable, unaccessible, redacted, hidden, filtered, lost, deleted, destroyed, backup, archive, locked, secured, unlinked.
Goldilocks	There is exactly the right amount of data - not too much, not too little and arrives at the right time	Loss, incorrect, partial, too early, too late, too much, too little (insufficient), spurious	Manageable data rate, manageable error rate, expected, within acceptable limits, without system overload

This page is intentionally blank

Appendix G Data Safety Management Plan (Informative)

> *Things get done only if the data we gather can inform and inspire those in a position to make a difference.*
> ***Mike Schmoker***

This section gives a suggested Data Safety Management Plan (DSMP) table of contents. It is expected that this will be needed only for aspects not already covered in a Safety Management Plan (SMP), or similar. It can be merged with an SMP, if appropriate. However it may be useful to consider the distinct data perspective by using a DSMP as well as an SMP. Regardless, a close connection should be maintained between the SMP and the DSMP.

Data Safety Management Plan suggested contents:

1. Introduction:
    - Scope and Context (Sets the scene, describes the project, scenario, concept of operations, etc.);
    - Boundaries and Interfaces (Describes the main interfaces and exchanges, with a scope boundary diagram.);
    - Derived requirements (System level requirements which impact the data safety process);
    - Owners (Who owns the data under consideration as it progresses through the system?);
    - Producers / Consumers (Who are the producers and consumers of the data the system inputs and outputs?);
    - Assumptions;
    - References; and
    - Abbreviations and Acronyms.
2. Analysis of Assigned DSAL and ODR Level (Implications of the data analyses.):
    - System Integrity Level (SIL), etc., Implications (What impact does the DSAL have on the required SIL, or similar measure, and vice versa?);
    - Development Implications (Are there any special development considerations? Derived from the SIL if there is one, otherwise what is deemed necessary for this system.);
    - Verification Implications (Derived from the SIL if there is one, otherwise what is deemed necessary for this system.);
    - Assurance Implications (Derived from the SIL if there is one, otherwise what is deemed necessary for this system.); and
    - Process / Procedure Implications (Derived from the SIL if there is one, otherwise what is deemed necessary for this system.).
3. Categories of Safety Data in Scope (A list of all the categories to be considered in the system context.).
4. Data Requirements Analysis:
    - Lifecycles (What data lifecycles are to be used?);
    - Specific Targets (Are there any qualitative or quantitative targets for the data?); and
    - Security Considerations (How will security be managed in this context? Are there any security / safety conflicts? Are there any security-related causes of data hazards?).

5. Management Approach (How will the organisation manage the data safety risks?):
    - Organisation;
    - Responsibilities;
    - Authorisations; and
    - Approvals and Signoffs.
6. Justification Approach (How will the safe usage of the data be justified, e.g., as part of the Safety Case Report?).
7. Analyses / Verifications to be Performed (What analyses or checks are to be performed on the data?).
8. Documents to be Produced (The list of documents to be produced related to data aspects.).
9. Appendix: DSAL Guidelines Response (Tailored version of the tables from this document. What is considered applicable / useful and what is not?).

Appendix H Incidents and Accidents (Discursive)

> *Hiding within those mounds of data is knowledge that could change the life of a patient, or change the world.*
> ***Atul Butte***

H.1 General

The following 'War Stories' describe incidents and accidents in which data is considered to have been a contributory factor. A data perspective has been taken to demonstrate the need for data to be given equal footing alongside software, hardware and human factors. The items described here have been arbitrarily selected; the collection is not intended to be exhaustive.

Note: The analysis presented here has no legal standing whatsoever. The purpose of this section is not to discredit, contradict or undermine any existing accident analysis; the aim is simply to view these incidents from a data perspective. Where possible accident reports have been referenced with the role of data highlighted. All references have been taken at face value and not independently verified.

Table 27 provides a summary of the items considered in this appendix. More information on each item is then presented in the following paragraphs.

Table 27: Incidents and accidents

Ref.	Title	Summary	Domain	Year	Data Property
H.2	log4j Java library vulnerability	Critical zero-day vulnerability affecting Apache Log4j2 java library	Internet	2021	Integrity
H.3	Immensa False Negative Covid-19 PCR Tests	43,000 people with Covid-19 mistakenly given negative PCR results	Medical	2021	Integrity, Accuracy, Traceability, Verifiability
H.4	Covid-19 test results silently deleted by Excel	Importing Covid-19 test results into an Excel file truncated the data after 65536 records	Medical	2020	Integrity, Completeness, Timeliness, Availability, Fidelity / Representation
H.5	Boeing 737 MAX 8 crashes	On two occasions a single faulty Angle-of-Attack sensor repeatedly commanded the nose down, leading to the aircraft flying into the sea/ground	Air	2018 & 2019	Integrity, Completeness, Accuracy Availability, Verifiability, Fidelity / Representation

Continued on next page

Table 27: Incidents and accidents (continued)

Ref.	Title	Summary	Domain	Year	Data Property
H.6	Loss of Soyuz-2.1b rocket carrying Meteor-M 2-1 weather satellite	The launch vehicle and satellite were lost because programmers gave coordinates for the wrong cosmodrome	Space	2017	Fidelity / Representation, Integrity, Verifiability
H.7	Cambrian Line Data Loss	Speed restriction data failed to be passed to trains, placing pedestrians on level crossings at risk.	Rail	2017	Availability, History
H.8	Loss of Irish Rescue Helicopter	At the time of writing, the investigation is continuing; possible controlled flight into terrain; possible issues with terrain / obstacle databases. Four fatalities.	Air	2017	Fidelity / Representation, Completeness, Accuracy
H.9	Loss of Schiaparelli Mars Lander	High rates led to the saturation of the Inertial Measurement Unit (IMU); the lander prematurely believed it was on the ground and released its parachute; the lander was lost. The high rates should have been expected, but were not due to modelling deficiencies.	Space	2016	Fidelity / Representation, Integrity
H.10	Interception of Communications	Incorrect data was disclosed during an investigation into indecent images. A welfare check was delayed on a child believed to be in crisis.	Policing	2015	Integrity
H.11	A400M Torque Calibration Parameters	A software update apparently wiped the engine torque control parameters. Aircraft crash; four fatalities.	Air	2015	Completeness
H.12	Royal Navy Submarine, Trawler *Karen*	A Royal Navy submarine snagged the fishing gear of the trawler *Karen*. The trawler was dragged backwards at about 7 knots and suffered structural damage.	Maritime	2015	Resolution, Integrity
H.13	Turkish Airlines A330	Inaccurate navigation data, relating to runway location, led to touchdown with left main gear off the paved surface. Aircraft written off.	Air	2015	Accuracy, Timeliness, Verifiability
H.14	Dallas Hospital Ebola Incident	A man suffering from Ebola was mistakenly sent home from a Dallas hospital. He later returned to hospital, was diagnosed but died; two nurses contracted Ebola but survived.	Medical	2014	Completeness, Format
H.15	Qantas Boeing 737 Take-Off	Two independent and inadvertent data entry errors meant weight used when calculating take-off performance was 10 tonnes less than actual weight. Tail strike.	Air	2014	Integrity, Verifiability

Continued on next page

Table 27: Incidents and accidents (continued)

Ref.	Title	Summary	Domain	Year	Data Property
H.16	Qantas Boeing 737 Loading	Default settings meant that children were incorrectly recorded as adults, resulting in incorrect aircraft weight and balance. Take-off safety speed was exceeded by about 25 knots.	Air	2014	Completeness, Fidelity / Representation
H.17	Grounding of *Navigator Scorpio*	The *Navigator Scorpio* was sailing with out of date charts, the planned route was not checked and positional fixes were not taken as often as required. The vessel was grounded, but refloated on the rising tide, with no damage. After the event, false information was added to the navigation chart.	Maritime	2014	Timeliness, Verifiability
H.18	Loss of MQ-9 Reaper	The ground control station was mis-configured following a change from MQ-1 to MQ-9 operations. The misconfiguration was not spotted. It caused any throttle position aft of full forward to command negative thrust. The aircraft decelerated below stall speed and impacted ground in unpopulated area.	Air (Defence)	2012	Consistency, Verifiability
H.19	Boeing 737-33A at Chambery Airport, France	Misuse of Electronic Flight Bag results in tail strike	Air	2012	Timeliness, Suppression, Lifetime
H.20	Loss of Hermes 450	Whilst attempting an automatic landing the Unmanned Air System (UAS) self-aborted. This abort was due to an incorrect set-up parameter that had been loaded by the crew. The crew elected to intervene rather than let the UAS self-recover. The air vehicle hit a new, unoccupied hangar; it was ultimately deemed "non-repairable".	Air (Defence)	2011	Integrity
H.21	Advocate Lutheran Hospital	An infant boy died after a series of medical errors: incorrect information was entered into an electronic intravenous order; automatic alerts had been turned off; and a bag was mislabelled.	Medical	2010	Integrity, Verifiability.
H.22	Grounding of *Sichem Osprey*	Anti-collision radar thresholds were apparently set incorrectly; there were also sizeable discrepancies between positions plotted on a chart and those displayed on the radar. The vessel grounded at more than 16 knots; no pollution occurred.	Maritime	2010	Integrity, Accuracy

Continued on next page

Table 27: Incidents and accidents (continued)

Ref.	Title	Summary	Domain	Year	Data Property
H.23	Near Collision of Trains, Cootamundra	Following a signalling system design error, a passenger train had to unexpectedly apply its brakes; it stopped just 5 m short of a goods train.	Rail	2009	Integrity, Completeness
H.24	Cedars Sinai Medical Centre Scanner	A software misconfiguration led to 206 patients receiving radiation doses approximately 8 times higher than intended; the error persisted for 18 months.	Medical	2008	Verifiability
H.25	Grounding of *The Pride of Canterbury*	An unapproved electronic chart system was apparently being used as the primary means of navigation for the passenger ferry *The Pride of Canterbury*. Due to user settings a charted wreck would not have been displayed on this system. The vessel grounded on the wreck, causing severe damage to her port propeller system.	Maritime	2008	Accuracy, Completeness, Intended Destination / Usage
H.26	LOT Flight 282	Incorrect data input to the Flight Management System, 'E' rather than 'W', meant loss of instruments. Aircraft had to return to Heathrow.	Air	2008	Integrity, Fidelity / Representation
H.27	Annabella container ship — Baltic Sea	Software developed loading plan using incorrect container specifications	Maritime	2007	Integrity, Verifiability, Fidelity / Representation
H.28	COMAIR Flight 5191	Inaccurate (out of date) aerodrome charts led to take-off being attempted from the wrong runway. Aircraft overran the runway; 49 fatalities.	Air	2006	Timeliness, Completeness
H.29	Überlingen Mid-Air Collision	Contradictory advice from Traffic Collision Avoidance System (TCAS) and an air traffic controller led to a mid-air collision between two TCAS-equipped aircraft. 71 fatalities.	Air	2002	Consistency, Availability, Timeliness
H.30	Fort Drum Artillery Incident	Movement of an artillery site led to errors in targeting. Artillery shells were fired more than a mile off target: 2 soldiers killed; 13 injured.	Defence	2002	Integrity, Verifiability
H.31	Early Release from Washington State Prison	A software update led to miscalculation of the time an inmate was due to serve in prison. Although the results of the calculation could easily be checked, the problem persisted for 13 years and over 2,000 offenders were released early.	Policing	2002	Integrity, Verifiability

Continued on next page

Table 27: Incidents and accidents (continued)

Ref.	Title	Summary	Domain	Year	Data Property
H.32	Mars Climate Orbiter	A mismatch in the units used by two software teams led to errors in the Flight Management System and, ultimately, the loss of a multi-million dollar space mission.	Space	1998	Consistency
H.33	Crash into Nimitz Hill, Guam	Controlled flight into terrain; the ground-based minimum safe altitude warning designed to alert air traffic controllers had been inhibited. 228 fatalities; 26 serious injuries.	Air	1997	Continuity, Fidelity / Representation
H.34	San Bernardino derailment and pipeline rupture	Criticality of train weight not recognised, resulting in multiple fatalities	Rail	1989	Integrity, Completeness, Accuracy, Timeliness, Verifiability, Fidelity / Representation, Lifetime
H.35	Lake Peigneur Drilling Accident	Whilst drilling a test well, a rig crew inadvertently caused a flood in a nearby salt mine. The previously freshwater lake became a salt water lake and the flow of a river was reversed.	Oil and Gas	1980	Verifiability

H.2 log4j Java library vulnerability

On Dec 10th 2021 a new critical zero-day vulnerability was detected that affected Apache Log4j 2 Java library. It adversely impacted the digital domain and security systems worldwide.

The vulnerability, when exploited, permited remote code execution on the vulnerable server with system-level privileges.

Log4j is a highly configurable logging mechanism for Java (“log4j”) that is used for documentation and debugging. Although originally developed for the Apache web server, it has been used part of many commercial applications, including network monitoring tools and even games such as Minecraft.

The exploit was a combination of the Java code that contains different logging functions (typically error(), warn(), info(), debug(), …) and a configuration file. The configuration file specifies which information shall be added to the log-file, the associated format, and how to “interpret” the logged data.

The security risk was that the logging mechanism was by default configured in a way such that it interpreted the logged data, and that the logged data that the user entered could be used to attack the server. For example if a user were to enter into the name field of a html-page instead of his name a “delete *.*” command, along with certain escape sequences, it might cause huge damage on the server — if this data were logged from the software and interpreted from the configuration file.

Data Property involved: *Integrity.*

Links

- Apache provides details on security issues with the log4j library, including available fixes, on its website https://logging.apache.org/log4j/2.x/security.html (Accessed: 09/01/2022)
- Further details may be found at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228 (Accessed: 09/01/2022)

H.3 Immensa False Negative Covid-19 PCR Tests

Failings at the Immensa lab in Wolverhampton led to an estimated 43,000 people with Covid-19 being mistakenly given negative Polymerase Chain Reaction (PCR) results; they thought they were in the clear, but were actually positive for Covid-19. This contributed to soaring rates of infection across the South West and Wales.

It took the Government almost a month to identify the issue and to stop sending PCR tests there.

It is unknown how much the virus spread in that time, but the effects of this mismanagement are potentially huge. Professor Deepti Gurdasani, a senior lecturer in epidemiology at Queen Mary University, estimates that the false negatives may have caused up to 200,000 further Covid-19 infections, and more than 1,000 avoidable deaths.

On Monday, November 1st 2021 the Good Law Project launched legal proceedings against the Secretary of State Sajid Javid over the Immensa testing scandal, citing the lack of a proper system to monitor the accuracy of tests at such labs breached the Department of Health and Social Care's duty to protect life, and the human rights of those affected.

Data properties involved: *Integrity, Accuracy* and possibly *Traceability* and *Verifiability.*

Links

- BBC programme Inside Science containing discussion with Professor Gurdasani: https://www.bbc.co.uk/programmes/m0010q9x (Accessed: 09/01/2022)
- https://goodlawproject.org/news/immensa-update/ (Accessed: 09/01/2022)
- https://www.gov.uk/government/news/testing-at-private-lab-suspended-following-nhs-test-and-trace-investigation (Accessed: 09/01/2022)
- https://www.theguardian.com/world/2021/dec/21/immensa-lab-month-delay-before-incorrect-covid-tests-stopped (Accessed: 09/01/2022)

H.4 Covid-19 test results silently deleted by Excel

In early October 2020 the British Government announced that 15841 positive Covid-19 test results had not been reported in the totals for England between 25 September and 2 October. This also meant that the contacts of those people were not traced, or asked to self-isolate, meaning that the virus might have spread further than it would otherwise have done, and possibly have taken additional lives.

The results were silently discarded as they were imported into the Public Health England database. Results were delivered as a "Comma separated Values" (".csv") file, which was imported into an Excel spreadsheet "template", using the ".xls" format, which was then in turn imported into the national database. The ".xls" format has a limit of 65536 (2^{16}) rows, and rows beyond this limit in the ".csv" file were silently discarded. (Data Category: Dynamic, Properties lost: *Integrity, Completeness, Timeliness, Availability, Fidelity/Representation*)

The newer ".xlsx" file format would have increased the row limit to 1048576 (2^{20}) rows before suffering the same problem, but the ".csv" file format has no limit on the number of rows.

This demonstrates the danger of using COTS software for safety-related functions without fully analysing its limitations. A decision had already been made to replace this system, but had not been acted upon. It is also an example of Dark Data, where it comes under the *Data we don't know are missing: "unknown unknowns",* and the *Missing What Matters* categories.

Finally, it is an example of where an error is known to the system, but not reported (adequately) to the user (Data Category: Dynamic, Properties lost: *Timeliness, Availability*).

Links

- https://www.bbc.co.uk/news/technology-54423988 (Accessed: 11/01/21)
- https://www.bbc.co.uk/news/uk-54422505 (Accessed: 12/01/21)

H.5 Boeing 737 MAX 8 crashes

On October 29th 2018, Lion Air flight 610 was lost with all on board when it flew into the sea. On March 10th 2019, Ethiopian Airlines flight 302 flew into the ground. In each case the aircraft was a Boeing 737 MAX 8 — the latest modernised iteration of the 737 airframe design, and in each, a software system called the Manoeuvring Characteristics Augmentation System (MCAS) has been established as the principle cause of the crashes.

The MCAS system was introduced because bigger, and hence more fuel efficient, engines are used on the 737 MAX 8, which had to be positioned higher on the wing and further forward (to ensure sufficient ground clearance for the larger engines). This changed the aerodynamic properties of the aircraft and meant the 737 MAX 8 tended to pitch up during high angles of attack. MCAS was introduced to counter this effect by taking input from an Angle-of-Attack (AoA) sensor and commanding the horizontal stabiliser control surfaces to bring the nose down. Although the aircraft has two AoA sensors, only one sensor gave input to MCAS at any one time, meaning that a single sensor failure could cause the nose to be forced down incorrectly. The design of MCAS allowed this to happen repeatedly, which if left unchecked would eventually force the aircraft into an unrecoverable dive.

MCAS did not compare data from the two sensors in order to detect a discrepancy between them, and hence indicate that the sensor data was not trustworthy (Data Category: Dynamic; Properties lost: *Integrity,*

Accuracy, Fidelity/Representation; Mitigations unused: Redundancy). Furthermore, the function (outside MCAS) to report a discrepancy between the sensors to the pilots was not enabled, reducing the crew's ability to respond appropriately (Data Category: Dynamic; Properties lost: *Availability*).

Several other data safety related failures can also be found in the report on flight 610:

- The MCAS system was not described in the pilot's manual and training materials (Data Category: Staffing & training, Properties lost: *Availability*)
- There was no indication to the pilots that MCAS was active (Data Category: Dynamic; Properties lost: *Availability*).
- The AoA sensor fitted to flight 610 was incorrectly calibrated during a previous repair, reporting an angle 21° higher than the correct value. But this was not detected during the repair (Data Category: Justification; Properties lost: *Availability, Fidelity/Representation, Verifiability*).
- The evidence of the testing of the AoA sensor after fitting to flight 610 by the maintenance crew was erroneous (Data Category: Justification; Properties lost: *Integrity, Availability, Verifiability*)
- 31 pages were missing from the maintenance log-book for flight 610, including the records of the testing of the AoA sensor after fitting to the aircraft (Data Category: Asset; Properties lost: *Completeness, Availability, Verifiability*)
- During the previous flight of the aircraft on flight 610, the pilots experienced repeated activation of the stick shaker, and other alarms, which were caused by the faulty AoA sensor. However they did not fully report all the issues in the flight logs, and so the maintenance crew's remediation activities did not lead them to suspect an issue with the sensor. (Data Category: Performance, Properties lost: *Availability*)
- During flight testing, adaptation was changed to give MCAS more authority, without a new safety impact assessment (Data Category: Adaptation; Properties lost: *Verifiability*).

Links

- http://knkt.dephub.go.id/knkt/ntsc_aviation/baru/ 2018 - 035 - PK-LQP Final Report.pdf (Accessed: 20/12/19)
- https://en.wikipedia.org/wiki/Boeing_737_MAX_groundings (Accessed: 20/12/19)
- https://en.wikipedia.org/wiki/Lion_Air_Flight_610 (Accessed: 20/12/19)
- https://en.wikipedia.org/wiki/Ethiopian_Airlines_Flight_302 (Accessed: 20/12/19)
- https://www.businessinsider.in/thelife/boeing-reportedly-made-the-flight-control-system-that-mistakenly-activated-during-2-deadly-crashes-4-times-stronger-while-creating-the-737-max/articleshow/68840690.cms (Accessed: 03/01/20)
- https://www.theverge.com/2019/5/2/18518176/boeing-737-max-crash-problems-human-error-mcas-faa (Accessed: 04/01/20)
- The design, development & Certification of the Boeing 737 MAX, September 2020, The House Committee on Transportation & Infrastructure. https://transportation.house.gov/committee-activity/boeing-737-max-investigation (Accessed 22/01/2021)

H.6 Loss of Soyuz-2.1b rocket carrying Meteor-M 2-1 weather satellite

On November 28th, 2017, the second launch took place from Russia's new launch site at Vostochny, carrying the Meteor-M No.2-1 polar-orbiting weather satellite, and 18 small satellites flying as secondary payloads. The launch appeared successful, but several hours later it was announced that it had not been possible to establish communications with the weather satellite, because it was not in its target orbit. An unconfirmed report claimed that the rocket was in the wrong orientation during its initial burn, and crashed into the Atlantic ocean. The following January, Russian deputy prime minister Dmitry Rogozin reported that the 2.6bn-rouble ($45m) satellite was lost because the Soyuz-2.1b launch vehicle had been programmed to take off from Baikonur, and not from the actual launch site at Vostochny. This is an example of a problem with data in the Adaptation category, which did not map correctly to the real-world entity that it was modelling, and hence lost the *Fidelity/Representation* property. Other properties that were lost include *Integrity and Verifiability.*

Links

- https://www.theguardian.com/world/2017/dec/28/russian-satellite-lost-wrong-spaceport-meteor-m (Accessed: 14/01/20)
- https://www.space.com/39270-russian-weather-satellite-doomed-human-error.html (Accessed: 22/01/20)
- https://www.space.com/38918-russian-satellites-lose-contact-after-launch.html (Accessed: 22/01/20)

H.7 Cambrian Line Data Loss

In the United Kingdom, railway signalling is primarily implemented through trackside signals. In 2011, a trial system was installed in the Machynlleth signalling control centre, which enabled suitably equipped trains travelling over the part of the rail network that it controlled (the Cambrian lines) to acquire data relating to speed restrictions and display these to the driver. The Cambrian lines are a collection of rail tracks which run along the Welsh coast and as far inland as Shrewsbury. On 20th October 2017, a driver reported that his train had failed to display speed restriction data.

The initiating event was just after 23:00 hrs on 19th October 2017, when a train automatically requested a movement authority (permission to travel on a specified part of the rail network) which had already been allocated to another train. This error condition is known to occur several times per year and causes an automatic software reset to be invoked. A well established set of processes are used by the signalling centre staff to return the rail system to normal operation. The staff followed their processes, and once the system was functional, allowed the final three trains of the day to complete their journeys. On the following day, it was the driver of the fourth train of the day who noticed the error and reported the failure.

Subsequent investigation revealed that speed restriction data had been unavailable since the software reset, resulting in six trains completing their journeys without that data, before the driver of the seventh train observed the problem.

The most significant risk identified thus far by the Rail Accident Investigation Board is that a number of the speed restrictions which were in place on the Cambrian lines had been invoked to allow pedestrians at level crossings sufficient time to take action, when observing an approaching train. Luckily the failure did not result in an accident — but this was due to luck, not failsafe systems on the railway.

This incident highlights the importance of the *availability* Data Property, as the data had been silently unavailable to trains. In addition, much of the digital audit trail relating to the failure was lost during repeated attempts to correct the problem and get the rail network running again, a loss of the *history* Data Property.

Links

- Interim report: https://assets.publishing.service.gov.uk/media/5bc871d5e5274a0956564a41/IR012018_181018_Cambrian_TSRs.pdf (accessed 31 December 2018).
- Final report: https://www.gov.uk/government/news/report-172019-loss-of-safety-critical-signalling-data-on-the-cambrian-coast-line (accessed 14 January 2020).

H.8 Loss of Irish Rescue Helicopter

On 14 March 2017, an Irish Search And Rescue (SAR) helicopter apparently suffered Controlled Flight Into Terrain (CFIT); all four crew members were killed. *Note: At the time of writing the investigation is continuing. The following discussion is based on a preliminary report from the Air Accident Investigation Unit, Ireland*.

The SAR helicopter was responding to a medical emergency on board a fishing vessel. It left Dublin and requested a route to Blacksod to refuel. The flight data recorded on the Health and Usage Monitoring System (HUMS) showed the helicopter was in stable level flight until the final few seconds, when it pitched up rapidly and impacted with terrain at the western end of Black Rock.

The helicopter was equipped with an Enhanced Ground Proximity Warning System (EGPWS). This is designed to decrease instances of CFIT by increasing pilot situational awareness, including the use of alerts and warnings: it is not intended to be used for aircraft navigation. The EGPWS can provide terrain alerting using look ahead algorithms, which take information from the aircraft (e.g. position., attitude, heading) and use this in conjunction with internal terrain and obstacle databases. Neither the Black Rock lighthouse nor the island's terrain were included in the EGPWS databases; these databases had been sourced from external suppliers by the EGPWS manufacturer.

The preliminary investigation also notes that the flight crew were following an operator-specific route guide: a review of such guides has been recommended.

This incident potentially illustrates the importance of the *fidelity / representation* and *completeness* Data Properties, with respect to the EGPWS databases, and the *accuracy* Data Property, with respect to the route guides.

Links

- http://www.aaiu.ie/sites/default/files/report-attachments/REPORT%202017-006%20PRELIMINARY.pdf (accessed 29 November 2017).

H.9 Loss of Schiaparelli Mars Lander

The Schiaparelli module, also known as the Entry Demonstrator Module (EDM), was part of the European Space Agency (ESA)'s ExoMars 2016 mission. The objective was to validate and demonstrate entry, descent and landing on Mars in preparation for the ExoMars 2020 mission.

On 19 October 2016, the EDM entered the Mars atmosphere at 14:42:07 (UTC). During its entry and descent it constantly transmitted telemetry. Its signal was lost at 14:47:22 (UTC), about 43 seconds before expected touchdown. On 20 October, a camera on NASA's Mars Reconnaissance Orbiter imaged the planned landing site and observed crash debris.

During entry, a parachute was deployed as planned. This triggered oscillations that saturated the IMU. Integration of this saturated value caused a significant error in predicted attitude. As the descent continued, a Radar Doppler Altimeter (RDA) was turned on. The significant attitude error led to large discrepancies between the IMU and the RDA. The nature of the guidance and navigation control software meant that this discrepancy led to a premature declaration of touchdown. As such, the parachute was jettisoned too early, causing the EDM to crash into the planet's surface.

The investigation determined the rates that saturated the IMU could have been predicted. Limitations in the modelling of parachute dynamics meant they were not. The investigation also noted issues with the persistence of the flag used to denote IMU saturation, as well as inadequate handling of this saturation by the guidance software.

This incident illustrates the importance of the *fidelity / representation* Data Property, with respect to the modelling, and the *integrity* Data Property, with respect to the persistence time of the saturation flag.

Links

- http://exploration.esa.int/mars/59176-exomars-2016-schiaparelli-anomaly-inquiry/ (accessed 29 November 2017).

H.10 Interception of Communications

In July 2015, it was reported that a public authority was undertaking an investigation into the uploading of indecent images of children and requested details of the account connected to the IP address used to upload the images. Issues with a new upgrade of the communication provider's system resulted in incorrect data being disclosed. Investigations revealed that a further five requests had resulted in incorrect data being disclosed. Data was acquired in six cases that related to individuals unconnected with the investigations. In one of these cases a welfare check was delayed on a child believed to be in crisis.

Under the Regulation of Investigatory Powers Act 2000, Internet Service Providers and indeed other communication service providers (e.g. mobile phone network providers) are required to provide data to investigatory bodies such as the Police. This data can be used to support criminal investigation and prosecutions and in the protection of vulnerable children and adults. The data clearly has the potential to be safety related, but there is no obligation for data providers to treat it as such. In this case the data errors led to a child being exposed to additional risk of harm.

This incident highlights the importance of the *integrity* Data Property. It also shows the applicability of Data Safety Guidance to areas that are not traditionally encompassed by safety engineering.

Links

- https://www.ipco.org.uk/docs/iocco/2015%20Half-yearly%20report%20(web%20version).pdf (accessed 9 January 2019).

H.11 A400M, Torque Calibration Parameters

On 9 May 2015, just minutes into a routine, pre-delivery test flight an Airbus A400M military plane crashed in Spain, killing four of the six crew. Three of the four engines had become stuck at high power and initially did not respond to the crew's attempts to control the power setting in the normal way. Pilots then succeeded in reducing power only after selecting the thrust levers to idle. The engines subsequently remained stuck in this mode. In an attempt to return to the airport, the aircraft struck power lines and crashed.

Although not confirmed, reports suggest the torque calibration parameters for the engines were wiped during a software installation. The torque calibration data is needed to measure and interpret information coming back from the A400M's engines, and is crucial for the Electronic Control Units (ECUs) that control the aircraft's power systems.

This accident highlights the importance of the *completeness* Data Property, specifically with respect to the torque calibration parameters.

Links

- http://www.bbc.co.uk/news/technology-33078767 (accessed 29 November 2017).
- http://www.reuters.com/article/us-airbus-a400m-idUSKBN0OP2AS20150609 (accessed 29 November 2017).

H.12 RN Submarine, Trawler Karen

On 15 April 2015, a submerged Royal Navy submarine snagged the fishing gear of the UK registered trawler *Karen*, 15 miles south-east of Ardglass, Northern Ireland. *Karen* had been trawling for prawns on a westerly heading at 2.8 knots when its fishing gear was snagged and it was dragged backwards at about 7 knots. *Karen*'s crew managed to release both winch brakes, freeing the trawl warps; the starboard warp ran out completely but the port warp became fouled on the winch drum, causing the vessel to heel heavily to port and its stern to be pulled underwater. *Karen* broke free from the submarine when the port warp parted; there was structural damage to the vessel but it returned to Ardglass safely under its own power. Evidence of the collision on board the submarine was either not observed or misinterpreted.

The nature of sub-surface operations requires the use of sonar technology to detect collision hazards. Detection in this way is reliant on noise emanating from contacts. In this instance the fishing trawler was detected but misidentified as a merchant vessel rather than a fishing vessel because the submarine's sonar operators did not detect or report hearing trawl noise. Given the number of vessels operating in the area, it is almost certain that the noise levels being generated would have been extremely high, with noise from one vessel masking the noise from another. Such a situation would make it very difficult for the sonar operators to methodically identify and analyse each contact, in particular to identify discrete acoustic classification clues such as trawl noise. As a result the trawler was assessed to be that of a small merchant vessel and the command team's perception would have been that no risk of collision could exist between a submarine at safe depth and a merchant vessel.

Review concluded that the submarine was operating near to the limit of its capability. Given that all the submarine's systems were reported to be functioning properly, it was apparent that the submarine's limit of capability had, in reality, been exceeded, with its sonar and command teams becoming cognitively overloaded, leading to degraded situational awareness and poor decision-making.

In conclusion, the Maritime Accident Investigation Board (MAIB) report stated, "The collision happened

because the submarine's command team believed *Karen* to be a merchant ship, so they did not perceive any risk of collision or need for avoiding action."

This incident highlights the importance of the *resolution* Data Property, specifically with regards to resolving a trawler and a merchant vessel. It also highlights the importance of the *integrity*, specifically with regards to the information provided from the sonar team to the command team.

Links

- https://www.gov.uk/maib-reports/collision-between-the-stern-trawler-karen-and-a-dived-royal-navy-submarine (accessed 29 November 2017).

H.13 Turkish Airlines A330

During March 2015, an Airbus A330-303, operated by THY Turkish Airlines, suffered a runway excursion accident upon landing at Kathmandu-Tribhuvan Airport (KTM), Nepal.

Flight TK726 was a regular passenger service from Istanbul-Atatürk International Airport (IST) to Kathmandu, Nepal. The flight was the first international flight to arrive that morning. After descending from cruising altitude, it entered a holding pattern. It was subsequently cleared for a VHF Omnidirectional Range (VOR) / Distance Measuring Equipment (DME) approach to Runway 02.

This approach was abandoned at about the Missed Approach Point at 1DME and the aircraft performed a go around. The aircraft circled and positioned for a second approach to Runway 02. The aircraft touched down to the left of the runway centre line with the left hand main gear off the paved runway surface. It ran onto soft soil and the nose landing gear collapsed. Following the accident the aircraft was written off.

The aircraft touched down to the left of the centreline because the Flight Management Guidance System (FMGS) navigation database contained threshold coordinates for a proposed displacement of the Runway 02 threshold. This was later withdrawn through a Notice To Airmen (NOTAM), but had not been updated by the airline in the database. Additionally, the coordinates that were initially published were inaccurate, causing the threshold coordinates to be offset to the left of the actual threshold. This had been noticed and reported by a previous Turkish Airlines flight on March 2. The changes had not been performed by the time TK726 landed at Kathmandu.

Among the safety recommendations stated in the accident report were:

- "The operator must ensure that the correct navigation data are uploaded on Flight Management Guidance System";
- "The operator should establish a system of verifying the quality of charts prepared by the service provider";
- "The operator should establish a system of checking the validity of the Flight Management System database"; and
- "Civil Aviation Authority of Nepal must ensure that raw aeronautical information/data are provided by the aerodrome authorities taking into account of its accuracy and integrity requirements for aeronautical data as specified by ICAO Annex 15 and its Aeronautical Information Service Manual."

This incident highlights the importance of three Data Properties, specifically: *accuracy*; *timeliness*; and *verifiability*. All of these apply to data describing the runway's location.

Links

- http://www.tourism.gov.np/downloadfile/TURKISH_AIRLINE_Final_Report_finalcopy4.pdf (accessed 29 November 2017 — no longer available from this location, but on 9 January 2019 was still available through archive.org).

H.14 Dallas Hospital Ebola Incident

On 26th September 2014, a Dallas hospital mistakenly sent home a man who had the Ebola virus having missed what would have appeared to be an obvious potential case: a Liberian citizen with fever and abdominal pain who said he had recently travelled from Liberia. The man later returned to the hospital, was eventually diagnosed with the illness, but subsequently died. Two nurses that had treated the man also contracted the virus but later recovered.

There have been mixed reports on the cause of the problem, but it is clear that external social phenomena such as the Ebola outbreak, which are outside the hospital's Electronic Health Record (EHR) system and processes, can change the safety significance of data held in the EHR. If the importance of the data is not recognised and elevated appropriately in the support tools and processes, then the risk of unintended harm can increase. This conclusion is reinforced by system vendors who subsequently updated their systems to reflect the Ebola crisis in light of the Dallas incident.

This incident highlights the importance of the *completeness* and *format* Data Properties, in that information about the Ebola outbreak was apparently either not available, or not available in a usable form, to decision makers.

Links

- http://www.nbcnews.com/storyline/ebola-virus-outbreak/texas-hospital-makeschanges-after-ebola-patient-turned-away-n217296 (accessed 29 November 2017).

H.15 Qantas Boeing 737 Take-Off

On 1 August 2014, a Qantas Boeing 737-838 aircraft commenced take-off from Sydney Airport, New South Wales. The flight was a scheduled passenger service from Sydney to Darwin, Northern Territory.

While the aircraft was climbing to cruise level, a cabin crew member reported hearing a "squeak" during rotation. Suspecting a tail strike, the flight crew conducted the tail strike checklist and contacted the operator's maintenance support. With no indication of a tails trike, they continued to Darwin and landed normally. After landing, the captain noticed some paint was scraped off the protective tailskid. This indicated the aircraft's tail only just contacted the ground during take-off.

The Australian Transport Safety Bureau (ATSB) found the tail strike was the result of two independent and inadvertent data entry errors in calculating the take-off performance data. As a result, the take-off weight used was 10 tonnes lower than the actual weight. This resulted in the take-off speeds and engine thrust setting calculated and used for the take-off being too low. Hence, when the aircraft was rotated, it overpitched and contacted the runway.

The ATSB also identified that the Qantas procedure for conducting a check of the Vref40 speed could be

misinterpreted. This negated the effectiveness of that check as a defence for identifying data entry errors. In this case, uncorrected errors affected the integrity of the data used to calculate take-off parameters.

This incident highlights the importance of the *integrity* and *verifiability* Data Properties, with respect to the data used to calculate take-off performance data.

Links

- http://www.atsb.gov.au/publications/investigation_reports/2014/aair/ao-2014-162.aspx (accessed 29 November 2017).

H.16 Qantas Boeing 737 Loading

On 9 May 2014, a Qantas Boeing 737 was preparing for departure from Canberra to Perth. There were 150 passengers, 87 of which were primary school children. These children were all seated together at the rear of the cabin.

A 'name template' was completed by a travel agent on behalf of the school group. This group was travelling from Perth to Canberra and returning back to Perth. Despite being marked as mandatory, the "Gender Description" field in this template was left blank; options for this field were "Adult", "Child" and "Infant".

As per company procedures, two days before the Perth-Canberra leg of their journey this group was 'advance accepted' into the booking system. Since the fields recording the number of children and young passengers in the group were blank, the Customer Service Agent assumed all of the group were adults. No loading-related issues were experienced during this flight.

Two days before the return flight the group was again "advance accepted" as all adults. This meant they had all been assigned an 'adult weight' of 87 kg. They were checked in at Canberra Airport and assigned seats at the rear of the aircraft. During take-off the aircraft appeared nose heavy. Significant back pressure was required to rotate the aircraft and lift off from the runway. The aircraft exceeded the calculated take-off safety speed by about 25 kt. The aircraft rose at a higher initial climb speed than usual, but the crew did not receive any warnings. No further issues were experienced during the flight.

This incident demonstrates the importance of the *completeness* Data Property (i.e., ensuring that the mandatory "Gender Description" field was completed) and the *fidelity / representation* Data Property (i.e., ensuring the calculated aircraft loads and balances reflect the real situation). It also illustrates some potential difficulties associated with the use of default data.

Links

- http://www.atsb.gov.au/publications/investigation_reports/2014/aair/ao-2014-088.aspx (accessed 29 November 2017).

H.17 Grounding of Navigator Scorpio

On 3 January 2014, the liquefied gas carrier *Navigator Scorpio* ran aground on Haisborough Sand in the North Sea. The vessel was undamaged, no pollution occurred and after two and a half hours the vessel refloated on the rising tide.

The schedule for the *Navigator Scorpio* was changed close to the time of its departure. This change meant that additional North Sea coastal charts were required. These charts were delivered to the vessel shortly before its departure. However, they were not up to date with the latest corrections and they were not corrected prior to sailing. In addition, the passage plan (i.e., vessel route) was not checked by the master before sailing.

When the master checked the passage plan, which had been drawn up by the second officer (2/O), he suggested a change to a portion of the route. After discussion with the 2/O the route was left unchanged, but with a requirement that position fixes be obtained every five minutes rather than every fifteen. Whilst acting as the sole bridge watchkeeper the 2/O was distracted by further passage planning activities and lost positional awareness. This led to the grounding of the vessel. After the grounding false information was added to the navigation chart to give the appearance that five minute positional fixes had been taken.

This incident highlights the importance of the *timeliness* Data Property, with respect to both the additional North Sea charts and the master's check of the passage plan.

In addition, the fluidity of the chart data allowed the 2/O to make false post-grounding additions to create an incorrect impression. According to the MAIB's report, such actions are not uncommon. These actions affect the *verifiability* of the chart data, which makes post-accident investigations more complicated.

Links

- https://assets.publishing.service.gov.uk/media/547c6f1740f0b6024100000d/NavigatorScorpio.pdf (accessed 29 November 2017).

H.18 Loss of MQ-9 Reaper

On 5 December 2012, an MQ-9 Reaper remotely piloted aircraft crashed in an unpopulated area three miles north-east of Mount Irish, Douglas County, Nevada. The crash occurred due to a stall, which was the result of an unrecognised reverse thrust condition. The aircraft and a number of pieces of ancillary equipment were destroyed. The total damage to United States government property was assessed at over $9 million.

The investigation board concluded that the throttle settings of the Ground Control Station (GCS) were incorrectly configured. This misconfiguration arose as the GCS was converted from supporting MQ-1 operations to supporting MQ-9 operations. It persisted despite the presence of a checklist, the completion of which should have identified the error. The misconfiguration meant that reverse thrust was commanded whenever the pilot's throttle was in any position except full forward.

This incident highlights the importance of the *consistency* Data Property, with respect to the differences between the GCS settings and the aircraft it was meant to be controlling. It also highlights the importance of the *verifiability* Data Property, with respect to the GCS settings (and, in particular, the limitations of using checklists to verify data).

Links

- http://www.airforcemag.com/AircraftAccidentReports/Documents/2013/120512_MQ-9_Nevada_full.pdf (accessed 29 November 2017).

H.19 Boeing 737-33A at Chambery Airport, France

On the 14 April 2012 and prior to departing Chambery Airport in France, the crew of a Boeing 737 used an Electronic Flight Bag (EFB) computer to calculate the aircraft's take-off performance. During the use of the software application the commander omitted to input the aircraft's take-off weight and it defaulted to the previous flight's data. Compounding the issue was that none of the crew undertook a cross-check of the EFB's output and the pilot subsequently employed incorrect speed and thrust information for the take-off. The consequence of using the incorrect information was that the calculation of the required airspeed for rotation was too low and the pilot continued to increase the aircraft's pitch angle to the point whereby the tail hit the runway. There were no injuries sustained in this incident but the aircraft suffered damage.

Following its investigation, which examined the wider employment of computers to derive aircraft performance information, the Air Accident Investigation Branch (AAIB) identified that there had been "a number" of previous accidents and incidents attributable to the "incorrect calculation of take-off performance"; and that due to the potential for degraded climb performance a catastrophic outcome could be envisaged. The AAIB also recognised that "take-off under-performance" is subtle and many other events of this nature may have been experienced but never reported. In its conclusions the AAIB acknowledged that using computers has "brought about improvements in accuracy and ease with which aircraft performance requirements can be made". However, there are "continued vulnerabilities" associated with the use of incorrect data that it is essential to control through "appropriately designed software and hardware". Although there were no injuries in this instance, this incident and the conclusions of the AAIB highlight some important points for "Safety Related Information Systems".

A clear chain of events was established that involved the use of incorrect information as a causal factor leading to an incident, which had the potential to be of a catastrophic nature;

- This was not an isolated incident;
- The crew did not appreciate the criticality of the EFB's information and it was used without validation;
- The AAIB recognised the essential need for appropriate system development.

It is often recognised that data must be up to date, but the explicit need to prevent the use of old data can be omitted from the safety requirements. This incident illustrates the importance of the properties *Timeliness, Suppression* and *Lifetime*.

Links

- *Air Accident Investigation Branch April Bulletin 4/2013* [on line] available at http://www.aaib.gov.uk/publications/bulletins/april_2013.cfm (accessed 17 January 2021).

H.20 Loss of Hermes 450

On 2 October 2011, a Hermes 450 UAS crashed at Bastion Airfield, Afghanistan. The aircraft was unrepairable.

The aircraft sortie was terminated early due to rising engine temperature. Due to the presence of vehicles and people in the vicinity of the runway, the GPS Take Off and Landing System (GTOLS) was selected to land the aircraft. Shortly after the approach had been initiated, the landing was self-aborted by the UAS. This abort occurred as a result of an incorrect data parameter in the GTOLS set-up loaded by the crew.

Moments after the self-abort, due to the urgency of the situation and the addition strain on the engine caused by the aborted landing, the crew chose to abbreviate the pre-programmed go-around GTOLS route. Instead, they issued a 'fly to coordinate' command. As the aircraft was climbing, the engine temperature rose rapidly, before the engine failed completely. On its descent the aircraft initially impacted an unoccupied hangar, before striking the ground upside down. It eventually came to rest on an empty aircraft dispersal pan.

The Service Inquiry determined that the cause of the accident was engine failure, as a result of overheating caused by oil starvation. Like many incidents, there were a considerable number of interacting factors. In total, thirteen contributory factors were identified, including the error in the GTOLS data.

This incident highlights the importance of the *integrity* Data Property, with respect to the GTOLS data loaded by the crew.

Links

- https://www.gov.uk/government/publications/service-inquiry-investigating-the-accident-involving-unmanned-air-system-uas-hermes-450-zk515-on-02-oct-11 (accessed 29 November 2017).

H.21 Advocate Lutheran Hospital

A Chicago hospital paid $8.25 million to settle a lawsuit brought by the parents of an infant boy who died at the institution in October 2010 after a series of medical errors.

The mother gave birth to her son 4 months prematurely. She stayed by his side with her husband for the next six weeks while the boy remained in the hospital's care. On 15 October, the baby suddenly died after coming out of a heart operation without any clear complications.

The hospital determined that a pharmacy technician had entered information incorrectly when processing an electronic Intravenous (IV) order for the baby. This resulted in an automated machine preparing an IV solution containing a massive overdose of sodium chloride, more than 60 times the amount ordered. The problem would have been identified by automated alerts in the IV compounding machine, but these were not activated when the customised bag was prepared for the baby. That is, adaptation data had been used to change the behaviour of the machine.

Investigations also found that the outermost label on the IV bag administered to the baby did not reflect its actual contents. Furthermore, although a blood test on the infant had shown abnormally high sodium levels, a lab technician assumed the reading was inaccurate. This highlights a different perspective on the dangers of defaulting, in this case a default assumption rather than a numerical default value.

Since the incident, staff have been activating alerts for similar IV compounders used in the system's hospitals and strengthened "double check" policies for all medications leaving pharmacies.

This incident highlights the importance of the *integrity* and *verifiability* Data Properties, for example with regard to: the information in the IV order; the bag label; and the blood test results.

Links

- http://articles.chicagotribune.com/2012-04-05/news/chi-parents-awarded-825-million-in-infants-death-20120405_1_clear-complications-lab-technician-double-check-policies (accessed 29 November 2017).

H.22 Grounding of Sichem Osprey

On 10 February 2010 at 0436 (local), the chemical tanker *Sichem Osprey*, on her way from Panama to Ulsan (South Korea) stranded at more than 16 knots on the north-easterly part of Clipperton Island. An Officer Of the Watch and a lookout were on the bridge at the time and no damage had been reported prior to the accident. A 100 metre fore part of the vessel had been grounded. No pollution was observed.

Anti-collision radar alarm thresholds were apparently not set according to the Captain's instructions. There were also sizeable discrepancies between the fixes plotted on the chart and those displayed on the radar.

This incident highlights the role of the *integrity* Data Property, with respect to the chart plots, and the *accuracy* Data Property, with respect to the alarm thresholds which did not reflect the Captain's wishes.

Links

- https://www.nautinst.org/download.cfm?docid=F9DA081F-6C1E-40F0-A71F0A89B10F426C (accessed 5 December 2017).
- http://www.bea-mer.developpement-durable.gouv.fr/IMG/pdf/RET_SICHEM_OSPREY_05-2010_Site.pdf (in French) (accessed 29 November 2017).

H.23 Near Collision of Trains, Cootamundra

On 12 November 2009, a passenger train was being routed into Number 1 Platform Road at Cootamundra, New South Wales. The driver of the passenger train received a signal indicating that the route was clear. However, as he approached, he noticed that the last wagon of a freight train was blocking his path. He applied the train brakes and stopped just short of a collision.

The investigation determined that a signalling system design error had allowed the incorrect signal to occur. The error happened despite the staff involved being suitably qualified and experienced. Working against a tight timescale, they were simultaneously developing a control table and associated software, rather than adopting the normal sequential approach. The control table contains information on points, signal and level crossing interlocking logic. The tight timescale also compromised the normal testing process. In addition, the quality control process was somewhat lacking: for example, not all identified queries and issues were appropriately closed out.

This incident illustrates the importance of the *integrity* Data Property, with respect to the control table data, and the *completeness* Data Property, with respect to data produced by the testing and the quality control processes.

Links

- http://www.atsb.gov.au/publications/investigation_reports/2009/rair/ro-2009-009.aspx (accessed 29 November 2017).

H.24 Cedars Sinai Medical Centre Scanner

A software misconfiguration in a Computed Tomography (CT) scanner used for brain perfusion scanning at Cedar Sinai Medical Center in Los Angeles, California, resulted in 206 patients receiving radiation doses approximately 8 times higher than intended. This error persisted for an 18 month period, starting in February 2008. Some patients reported temporary hair loss and erythema.

The problem reportedly arose from an error made by the hospital in resetting the CT machine after it began using a new protocol for the procedure in February 2008. The error was not detected until one of the patients reported patchy hair loss in August 2009. "There was a misunderstanding about an embedded default setting applied by the machine," according to a statement from Cedars-Sinai. "As a result, the use of this protocol resulted in a higher than expected amount of radiation."

This incident highlights the importance of the *verifiability* Data Property, especially with regards to default (and adaptation) data.

Links

- http://articles.latimes.com/2009/oct/10/local/me-cedars-sinai10 (accessed 29 November 2017).

H.25 Grounding of The Pride of Canterbury

On 31 January 2008, the roll-on roll-off passenger ferry, *Pride of Canterbury* grounded on a charted wreck while sheltering from heavy weather in an area known as 'The Downs' off Deal, Kent. The vessel suffered severe damage to her port propeller system but was able to proceed unaided to Dover, where she berthed with the assistance of two tugs.

The vessel had been in the area for over 4 hours when, while approaching a turn at the northern extremity, the bridge team became distracted by a fire alarm and a number of telephone calls for information of a non-navigational nature. The vessel overshot the northern limit of the identified safe area before the turn was started. The Officer Of the Watch (OOW) became aware that the vessel was passing close to a charted shoal, but he was unaware that there was a charted wreck on the shoal. The officer was navigating by eye and with reference to an electronic chart system which was sited prominently at the front of the bridge, but he was untrained in the use and limitations of the system. The wreck would not have been displayed on the electronic chart due to the user settings in use at the time. A paper chart was available, but positions had only been plotted on it sporadically and it was not referred to at the crucial time.

Although the Voyage Management System (VMS) was loaded with Electronic Navigational Charts (ENCs) for the vessel's area of operation, the system had not been approved by the Maritime and Coastguard Agency (MCA) as the owner's policy was for the VMS to be used as an aid to navigation only, with *Pride of Canterbury*'s paper charts being utilised as the primary means for navigation. Relevant admiralty charts were supplied to the vessel for this purpose.

Despite the VMS being unapproved for use as the primary means of navigation, the officers on *Pride of Canterbury* were apparently using it as if it was. Furthermore, many of the officers, including the Chief Officer, who was in charge at the time of the accident, were not fully trained in the use of the system.

This incident highlights the importance of the *accuracy* Data Property, with regards to the information displayed on the electronic chart. It also highlights the importance of the *completeness* Data Property, with regards to training (and training records) and the *intended destination / usage* Data Property, with regards

to the inappropriate use of the VMS data.

Links

- https://assets.publishing.service.gov.uk/media/547c700ded915d4c0d000071/PrideofCanterburyReport.pdf (accessed 29 November 2017).

H.26 LOT Flight 282

On 4 June 2007, just after take-off from Runway 09R at London Heathrow Airport (LHR), the pilots noticed that most of the information on both of the Electronic Attitude Director Indicators and Electronic Horizontal Situation Indicators had disappeared. The aircraft entered Instrument Meteorological Conditions (IMC) at about 1,500 feet Above Aerodrome Level (AAL), and the co-pilot had no option but to fly using the standby attitude indicator and standby compass. He experienced difficulty in following radar headings. The aircraft returned to land at LHR after a flight of 27 minutes.

A single error made by the co-pilot during the pre-flight preparation caused the subsequent problems. This was the use of 'E' instead of 'W' when the longitude co-ordinates were entered into the Flight Management System (FMS).

The airports around London, because of their proximity to the Prime Meridian, can lead flight crews to make co-ordinate entry errors of this nature. It is of note that the operator's route network is such that there are few destinations to the west of the Prime Meridian and hence the majority of longitude co-ordinates that need to be entered would be eastings. Inertial Reference System (IRS) alignment warnings should have alerted the crew but may have been dismissed.

This incident highlights the importance of the *integrity* and *fidelity / representation* Data Properties, specifically with respect to co-ordinates.

Links

- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384859/Bulletin_6-2008.pdf (accessed 29 November 2017).

H.27 Annabella container ship — Baltic Sea

On the evening of the 25 June 2007 the container ship the Annabella was subjected to heavy seas causing the vessel to pitch and roll heavily. The following morning the ship's crew discovered that, due to the induced stresses, a "stack of seven 30 ft cargo containers" had collapsed resulting in crushing damage to the lowest containers. A number of these containers were transporting Class 2 Dangerous Goods in the form of Butylene gas.

The Marine Accident Investigation Branch (MAIB) concluded that the container stack had been "piled too high both for the particular hold location and the stacking limits of the containers". The MAIB identified that one of the incident's contributing factors had been an incorrect loading plan which had been produced by planning software used by the cargo company. The software application should have taken account of the stability and stowage information pertinent to the vessel (as provided by its manufacturer). The application, however, had unknowingly converted the container's dimensions from 30 ft to 40ft resulting

in the wrong stacking limits being detailed. The cargo company passed the loading plan to the shipping terminal prior to it being inputted to the vessel's on-board loading computer. The computer did not recognise the error and the 40 ft limits were applied. Amongst the MAIB's conclusions it was noted that, although the master is responsible for the final loading plan, appropriate oversight is difficult in practice in light of the "pace of modern container operations". The MAIB made the following recommendations in relation to the Information System:

- Loading computer programs should incorporate the full requirements of a vessel's cargo securing manual and be properly approved to ensure that officers can place full reliance on the information provided;
- The availability of a reliable and approved loading computer programme is a factor to be considered in determining an appropriate level of manning for vessels on intensive schedules;
- Cargo planning software should be able to recognise and alert planners to the consequences of variable data, such as non-standard container specifications.

This incident involved incorrect data, that could have been identified if the software had highlighted the unusual aspects of the data such as the container dimensions to the operator. From a data perspective, the properties that needed to be maintained were *Integrity, Verifiability* and *Fidelity / Representation.*

Links

- Marine Accident Investigation Branch Report 21 — *Report on the Investigation of the Collapse of Cargo Containers Annabella Baltic Sea 26 February 2007* [online] available at https://assets.publishing.service.gov.uk/media/547c7032e5274a429000007d/AnnabellaReport.pdf (accessed 17 January 2021).

H.28 Comair Flight 5191

On 27th August 2006, Comair flight 5191 crashed during take-off from Blue Grass Airport, Lexington, Kentucky. The flight crew was instructed to take-off from runway 22, but instead lined up on runway 26 and began the take-off roll. The airplane ran off the end of the runway and impacted the airport perimeter fence, trees, and terrain. The captain, flight attendant and 47 passengers were killed.

The National Transportation Safety Board determined that the probable cause of the accident was the flight crews' failure to use available cues and aids to identify the airplane's location on the airport surface during taxi and their failure to cross-check and verify that the airplane was on the correct runway before take-off.

The Airport Charts used by the crew were inaccurate. The airport was under construction, and the charts were not kept current with the rapid changes that were taking place during the construction work. The chart did not accurately reflect either the taxiway identifiers or a taxiway that was closed on the day of the accident.

Due to a previously unrecognised software problem, any information the chart provider received after normal work hours on Fridays was not included in their regular updates. Furthermore, the chart provider modified the Blue Grass Airport chart after the accident to include a note that Runway 8/26 is "daytime VMC use only", even though this information had been published since 2001. Additionally there was a local NOTAM issued advising of taxiway closures due to construction work. However the crew was not provided with this information in their dispatch paperwork.

This incident highlights the importance of the *timeliness* Data Property, specifically with regards to the charts. The *completeness* Data Property is also relevant, given that neither the "after hours" changes on Fridays nor the local NOTAM were communicated appropriately.

Links

- http://libraryonline.erau.edu/online-full-text/ntsb/aircraft-accident-reports/AAR07-05.pdf (accessed 29 November 2017).
- http://en.wikipedia.org/wiki/Comair_Flight_5191 (accessed 29 November 2017).

H.29 Überlingen Mid-Air Collision

On 1 July 2002, a passenger jet (Bashkirian Airlines Flight 2937) and a cargo jet (DHL Flight 611) collided in mid-air. The collision happened over the south German town of Überlingen; it occurred despite both aircraft being equipped with TCAS.

The two aircraft were in airspace that was controlled from Zürich and were on a collision course. A single controller was on duty and they were responsible for controlling two workstations. This arrangement was against regulations, but was tolerated by management and had become accepted practice. Initially, the controller did not appreciate the dangerous situation that was developing.

Maintenance was being conducted on the main radar system, which meant that the controller was reliant on a backup system. This delayed the presentation of radar information. In addition, a ground-based optical system that would have provided warning of the impending collision was turned off, also for maintenance: the controller was unaware of this.

Less than a minute before the collision the controller became aware of the situation. He instructed Flight 2937 to descend. Seconds after initiating this decent, the TCAS on Flight 2937 requested a climb, with the corresponding system on Flight 611 requesting a descent. Flight 2937 continued to follow the controller's direction, meaning that both aircraft were descending.

Unaware of the TCAS instructions the controller repeated the request for Flight 2937 to descend; he also provided Flight 2937 with misleading information on the relative location of Flight 611. The planes collided, resulting in the deaths of all 69 people on Flight 2937 and both people on Flight 611.

One of the actions resulting from the accident was a clarification from International Civil Aviation Organization (ICAO) of how pilots should respond to contradictory information from a controller and TCAS.

This incident illustrates the importance of the following Data Properties: *consistency*, with regards to the instructions provided to Flight 2937; *availability*, with regards to information from the ground-based optical system; and *timeliness*, with regards to information from the radar system.

Links

- https://en.wikipedia.org/wiki/Überlingen_mid-air_collision (accessed 29 November 2017).

H.30 Fort Drum Artillery Incident

Two artillery shells were fired more than a mile off target during an Army firing exercise at Fort Drum in Northern New York in March 2002. The shells landed near a mess tent where a Battalion were having breakfast. Two soldiers were killed, 13 were injured.

The initial artillery site was unsuitable so the unit had to move to a different location nearly a mile away. The unit then had trouble setting up its digital and wire communications. The movement of the unit was not taken into account when programming the firing coordinates. Also, in what was termed a 'software behavioural shortfall' the system was designed to reset the gun elevation to zero. The correct altitude for the new site was not entered into the safety calculations, and the mistakes were not captured by the data review process.

This incident highlights the importance of the *integrity* and *verifiability* Data Properties, specifically with respect to the location and elevation data.

Sources

- http://www.apnewsarchive.com/2002/Army-Reports-on-Ft-Drum-Accident/id-539bf2ea24b8dd66009c6efee2be926c (accessed 29 November 2017).

H.31 Early Release from Washington State Prison

For over 13 years the Washington State Department Of Corrections (DOC) had been releasing certain prison inmates earlier than their sentences allowed.

In 2002 the Supreme Court ruled that the DOC was erroneously denying offenders credit for early release time earned during pre-sentence detention. In attempting to address that issue the DOC incorrectly reprogrammed its computer tracking system. This resulted in the early release of offenders with sentencing enhancements. The programming error went undetected for over ten years, with more than 2,000 offenders being released early.

The error was detected when the family of an assault victim hand-calculated the assailant's release date. The family notified the DOC that it appeared as if the assailant would be released earlier than warranted by statute. It took a further three years before the programming error was finally corrected.

This incident illustrates the importance of the *integrity* Data Property, with respect to calculated release dates. The *verifiability* Data Property is also relevant, noting that the calculation of the release date was readily verifiable (as shown by the actions of the family of the assault victim).

Links

- http://www.governor.wa.gov/sites/default/files/documents/2016-02-25_DOC_Report.pdf (accessed 29 November 2017).

H.32 Mars Climate Orbiter

The Mars Climate Orbiter was a spacecraft launched aboard a Delta II rocket by NASA from Cape Canaveral on 11th December 1998. Its intended mission was to study the Martian atmosphere and climate, whilst acting as a communications relay for other spacecraft on or near Mars.

The plan was that the rocket would place the spacecraft into a transfer orbit to Mars, which would be optimised along the way by a series of four trajectory correction manoeuvres. Insertion into Mars orbit was to take place at an altitude of 226 km, but during the week after the final correction manoeuvre, calculations predicted that it would be between 150 km and 170 km; revised to 110 km the day before insertion. The orbiter was able to survive atmospheric stresses down to about 80 km. On 23rd December 1999, the spacecraft passed behind Mars, and so out of radio contact, earlier than expected; communications were never regained.

Final calculations placed the spacecraft in a trajectory that would have taken it within 57 km of the Martian surface, but it is likely to have disintegrated before getting to that point.

It transpires that the orbiter's FMS software was designed to work with metric Newton seconds, whereas a FMS data-file generated by ground system software used pound-force seconds. A Newton is about 22.5% of a pound-force or a factor of 4.45.

The cost of the mission was stated by NASA to have been $327.6 million in total ($193.1 million to develop the spacecraft, $91.7 million for launch and $42.8 million for mission operations).

This incident highlights the importance of the *consistency* Data Property.

Links

- http://en.wikipedia.org/wiki/Mars_Climate_Orbiter (accessed 29 November 2017).

H.33 Crash into Nimitz Hill, Guam

On 6 August 1997, Korean Air Flight 801 crashed at Nimitz Hill, Guam. This is high terrain approximately 3 miles southwest of Guam International Airport, where the aircraft had been cleared to land. Of the 254 people on board, 228 were killed and 26 survived with serious injuries.

Probable causes of the accident were the captain's failure to adequately brief and execute a non-precision approach and the first officer's and flight engineer's failure to effectively monitor and cross-check this approach. Contributing factors included fatigue and inadequate flight crew training.

Another contributing factor was the intentional inhibition by the Federal Aviation Administration (FAA) of the Minimum Safe Altitude Warning (MSAW) system at Guam, and the agency's failure to adequately manage the system.

The MSAW system uses a terrain database. It is designed to alert a controller if an aircraft equipped with a Mode C transponder descends below, or is predicted to descend below, a predetermined safe altitude.

In 1990, the Guam terminal MSAW was installed to provide protection within a 55 nm radius. In 1993, a new software package was produced in which warnings were inhibited within a 54 nm radius; this left a 1 nm annular region within which warnings could be generated. The motivation behind the new configuration was to reduce false alarms. The software became operational in February 1995. A further software update

became operational in April 1996. This also had the 54 nm inhibition.

This incident illustrates the importance of the *continuity* Data Property, with respect to the MSAW coverage, and the *fidelity / representation* Data Property, regarding the terrain database used by the MSAW system.

Links

- https://www.ntsb.gov/investigations/AccidentReports/Reports/AAR0001.pdf (accessed 29 November 2017).

H.34 San Bernardino derailment and pipeline rupture

In May 1989 a Southern Pacific Transportation Company freight train derailed in San Bernardino, California. The train derailment accounted for seven fatalities and two serious injuries; however, that accident also damaged a fuel pipe and less than a fortnight later it ruptured causing a further two deaths and three serious injuries.

One of the causal factors of the train's derailment, as reported by the National Transportation Safety Board, was a "failure to determine the weight of the train" and in summary, the operator thought it weighed less than it actually did, resulting in the dynamic braking being insufficient to deal with the downhill gradient it was travelling on. The Company had used a computer to determine the train's weight and because the actual weights had not been entered the system made its calculations based upon estimated weights, which were lower. Clearly this was not a systematic failure of the computation algorithm but again potentially a failure to appreciate the criticality of the weight information and its potential as a causal factor within an accident sequence.

From the criticality of the weight information, derived safety requirements could be developed for the various data sources that were used to derive the weight. Such requirements could be expected to highlight the properties of *Integrity, Completeness, Accuracy, Timeliness, Verifiability, Fidelity / Representation* and *Lifetime*.

T Hardy, *Software and System Safety — Accidents, Incidents and Lessons Learned,* Bloomington, Author House, 2012, ISBN 978-1-4685-7470-8

H.35 Lake Peigneur Drilling Accident

Lake Peigneur is located in Louisiana, United States of America. It was a ten-foot deep freshwater lake popular with sportsmen. On 20th November 1980, an exploration rig drilling for oil in the lake bed was evacuated as it began to sink; this was perceived by the crew as a structural collapse. Meanwhile, the nearby Jefferson Island salt mine was being evacuated due to the sudden onset of flooding.

The rig crew had been drilling a test well into deposits alongside a salt dome under Lake Peigneur. By some miscalculation, the assembly drilled into the third level of the nearby salt mine. Fresh water from the lake soon began trickling into the mine. Over the course of the morning, the fresh lake water began dissolving the salt and enlarging the hole until water was literally flooding into the mine.

The whirlpool created as the lake drained into the mine sucked in the drilling platform, eleven barges, trees and soil. The Delcambre Canal, which usually drains from the lake into a bay on the Gulf of Mexico, had its flow reversed. This resulted in Lake Peigneur becoming a salt water lake. Fortunately, no injuries or loss of human life were reported.

Federal experts from the Mine Safety and Health Administration were not able to determine the cause of the accident due to confusion over whether the rig was drilling in the wrong place or whether the mine's maps were inaccurate.

This incident highlights the importance of the *verifiability* Data Property, specifically with regards to the location of the rig. Note that this property was relevant both when the rig started to drill and also during the post-incident investigation.

Links

- http://en.wikipedia.org/wiki/Lake_Peigneur (accessed 29 November 2017).

This page is intentionally blank

Appendix I Lifecycle Considerations (Discursive)

> *Failure is an amazing data point that tells you which direction not to go.*
> ***Payal Kadakia***

I.1 Usage Scenarios

If safety-related data is incorrect it can become dangerous when used, either by making a computer or control system perform incorrect actions, or by misleading human users into making incorrect decisions. Since the danger can only be determined when the usage of the data is understood, risk assessment should involve both the consumer of the data and the producer.

Figure 1: Consumer-focused integrity requirements

The consumer assesses the use of the safety-related data. (In later phases of the Data Safety Management Process this information is used to define the required Data Properties: for example, how accurate a particular safety-related Data Artefact must be.)

The producer investigates how the safety-related data is collected and what errors might occur. (Building on activities in later phases of the Data Safety Management Process, the producer can provide some form of guarantee, or level of confidence, that the safety-related data meets the specific data-related requirements.)

In some cases a producer will be providing safety-related data without any knowledge of a specific user (e.g., mapping data or generic databases that are sold to many users). In these cases the producer will need to make some assumptions about possible users, and then clearly state what level of integrity the data has been produced to. It is then up to the users to check whether the declared integrity matches their need.

I.2 Data in System Lifecycles

Like other components of a safety-related system, the safety dependency of data is dictated by the context in which it is used and the causal links that become established where loss of one or more of the required properties can contribute to hazardous system states. For example, a given data set (say configuration data) could be used in a number of separate contexts such as:

- prototyping a system to demonstrate solution feasibility of a safety-related system;
- development testing of a safety-related system; and
- live operational use of a safety-related system.

In these cases, the data set is the same but the context of its use changes the safety significance and therefore the level of assurance that it may require. It follows that the assessed assurance level of a data set is also predicated on where and when in the lifecycle the data set will be applied.

To illustrate this concept, a number of generic model lifecycles are discussed below. Note that these are not intended to be prescriptive or mandate the use of any particular model. Instead, they are being used to illustrate how the Data Safety Management Plan could articulate these lifecycle considerations.

Development The diagram in Figure 2 represents a typical development lifecycle using an iterative development approach[3]. In this model there are key phases as the system transitions from concept through to testable executable code. The process is iterative in that several cycles of functional elaboration, design, development and test may be run and these typically will focus on the areas of the system that bear most technical risk or comprise the key functional use cases so the client gets early visibility of the system. This early awareness allows feedback to be provided into the next iteration to help steer the solution to the client's actual needs. Traditional waterfall implementation can map onto this model on the basis that there is only one iteration in each phase and all activities in one phase need to be completed before progressing to the next.

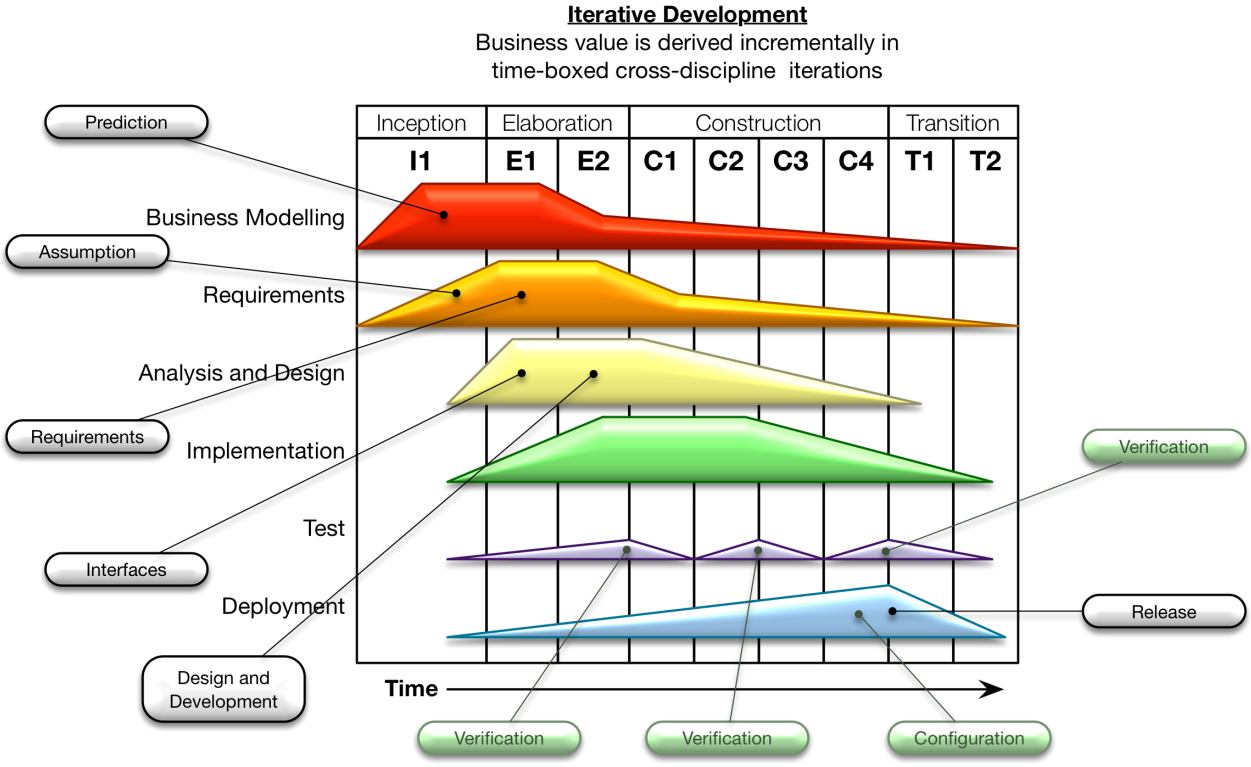


Figure 2: Development lifecycle

The model itself may vary depending on the specific needs of the project but the diagram illustrates that different Data Categories become significant at different points of the process.

Operational Once a system has been developed it will move into an operational lifecycle or indeed, if data safety has not previously been considered for an enterprise, then the system could already be in operational use. These operational lifecycles tend to be cyclical in nature; the diagram in Figure 3[4] illustrates a typical model.

[3] The diagram is based on IBM's Rational Unified Process, an iterative software development process framework. The original diagram is in the public domain.

[4] ITIL is a registered Trade Mark of AXELOS Limited. All rights reserved.

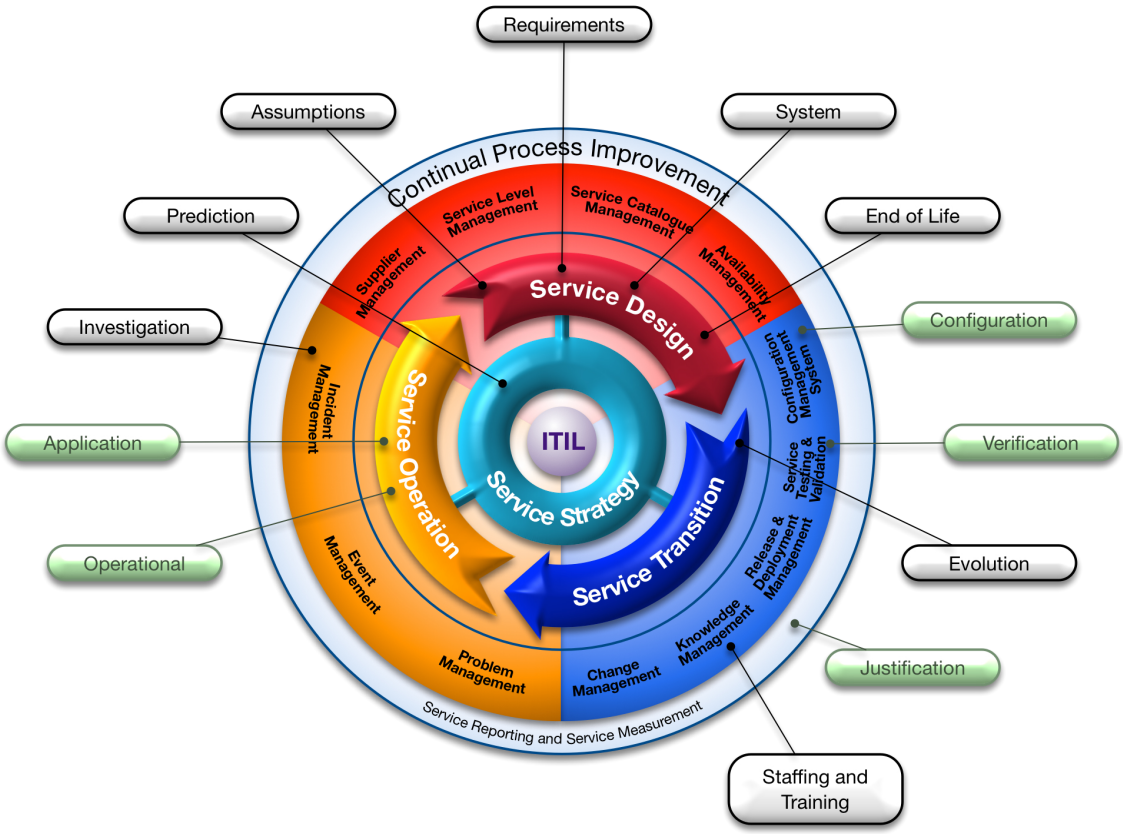


Figure 3: Operational lifecycle

Again, specific Data Categories will come into play at different periods in the process. Documenting the relationship between process steps and Data Categories will therefore give clarity as to when a particular assurance technique needs to be applied.

Data supply chains The previous models relate to typical system supply and operate perspectives but there are also other data supply chains where a number of organisations engage in the procurement and use of safety-related data. These processes may include the development and operational lifecycles but a different model is required to fully represent the wider processes that are being employed. The diagram in Figure 4 shows such a model representing a data acquisition lifecycle.

This model represents the interactions between three key organisations:

- The Commissioning User: the organisation that has the need for the data;
- The Data Provisioner: the organisation that will fulfil that need for data; and
- The Data Acquirer: the organisation employed by the Data Provisioner to carry out physical collection of data.

Note that these may be three separate organisations, or they may be separate business units within the same, larger, organisation.

In this supply chain, the Commissioning User is a Consumer of the data and the Data Acquirer is a Producer of data. The Data Provisioner acts both as a Consumer (from the Data Acquirer) and Producer (to the Commissioning User) of data. Similarly, an organisation that augments data sets is both a Consumer and Producer of data in the supply chain.

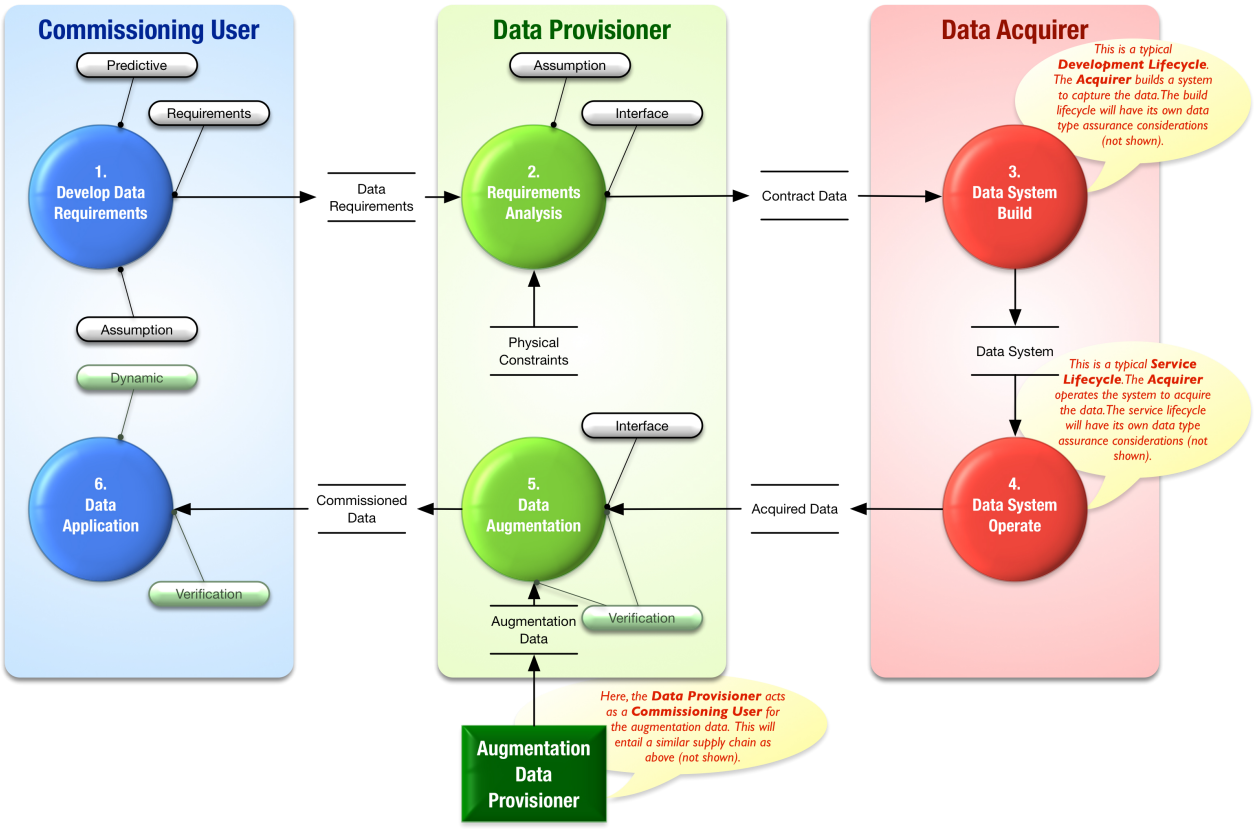


Figure 4: Data supply chain

The Commissioning User Requirement Analysis is the key process step where the Commissioning User's expectations for data (including fidelity levels for associated properties) are agreed with the Data Provisioner. The requirements may be adjusted because of physical constraints (e.g., loss of precision because of physical measuring device constraints) and may include additional requirements to augment the captured data with additional information (e.g., airport codes added to a measurement of a given runway length).

The Data Provisioner may employ a Data Acquirer to capture the data (e.g., to carry out a physical survey of a site). The acquisition phase may itself require a specialised system to be built to perform the capture and data refinement to meet the Data Provisioner's specifications. Such systems will then themselves be subject to the Development lifecycle model considerations discussed above. Likewise, the data augmentation phase may require further system development processes or indeed, could trigger an instance of the model again as the Data Provisioner acting as a Commissioning User.

Acquired and augmented data is then fed into the operational system that has been built for providing the service of generating the commissioned data. This system in its service provision role would then typically follow the Operational Lifecycle process model discussed earlier.

I.2.1 Tool Assurance

Tools in this context are considered anything that automates all or part of a process, for example, data creation or data transformation. Test tools are also included (i.e., the term is not limited to parts of an operational system).

Tools can impact data safety in different ways, depending on both their function and how they are to be used. For tools to be considered fit for purpose it is necessary to show that the tool meets its requirements in the context in which it is to be used. The activity to ensure a tool is fit for purpose is usually called "tool qualification".

The first step is to define the purpose for which the tool is required to be fit. Once that is done, and the tool's requirements are specified, there are three main strategies available for qualification:

- Use evidence of a previous certification of the tool by a trusted third party (unlikely to be available in most industry sectors);
- Base tool qualification on the practices used when designing and developing the tool (only practicable for tools developed within the organisation); and
- Use one of the available industry-specific guidance documents that admit Commercial-Off-The-Shelf solutions, e.g., EUROCAE Document ED-215 (RTCA/DO-330) [13].

There is an alternative, risk-based and perhaps more feasible, approach. This involves assessing the potential risks presented by use of the tool and providing assurance that these risks are adequately managed. The method proceeds as follows:

- Draft a procedure for the use of the tool to achieve the stated purpose;
- Identify threats to data safety associated with using the tool;
- Specify adequate mitigations for each identified threat;
- Augment and formally issue the tool requirements and the usage procedure to implement the specified mitigations;
- Demonstrate that the tool and its mitigations perform as expected; and
- Provide a compelling assurance argument based on the previous steps and any other evidence that will improve confidence; for example:
  - reputation of the supplier;
  - configuration management of the tool, its settings and its documentation;
  - competence of the tool user; and
  - checks that are made on the tool's output.

I.2.2 Test Data

The generation of suitable test data is critical to verification of a safety system. The test data must include both representative "normal" values based on intended usage and also values which push at, and beyond, normal use to provoke hazards that the system might produce. This latter type of test data is particularly hard to generate: generally it must be credible, yet it must stress the system to react in a way that the preservation of safety properties can be assessed.

In general, all the properties of the test data should be considered and an assessment made as to whether breaking a property (e.g., introducing corrupt or late data) would cause a problem to the system. If it does, then specific test data should be produced to facilitate testing of this potential problem.

Some suggestions for test data for safety-related systems are:

- Use of values on or around boundaries;
- Use of extreme values, way beyond what could be reasonably expected;
- Use of typical "everyday" values / sets;
- Some realistic but unexpected values;
- Try combinations of data values or items that are problematic together (e.g., inconsistent);
- If possible, use some values known to have caused problems in the past;
- Where appropriate, use values related to timing, rollover or date boundaries;
- Where possible, use white-box values (i.e., those derived from an understanding of the system);
- Use a set of values with drift or bias over time;
- Use data sets with particular statistical properties (e.g., distribution, patterns etc.);
- Use data which has incorrect formatting, ordering, or out of sequence, etc.; and
- Try data which has repeated sets of values or pseudo-random characteristics.

Typically very complex test data is derived from recorded live feeds of real data flows. While this data can be extremely useful for regression purposes, it should be recognised that it is unlikely to contain many outlying or boundary data items. Therefore it may need to be modified to test any hazardous situations; this modification can be difficult and may require sophisticated tools to both ensure correct properties and injection of the intended faults (for instance to introduce a statistical bias to the data).

Simulator / emulator derived values can be useful, but again the issue is how realistic the values are: often the accuracy, resolution or timing of simulated values may be different to real data.

Coverage with test data is something to consider. Sometimes the same data set is used for multiple test scenarios, when in fact it is not stressing all of them to the same degree. Test data coverage can be collected over requirements, code or design, but it is important not to forget hazards: coverage of the hazards and mitigations identified in the hazard log is a key aim.

In general some measure of the quality and suitability of the test data can be useful. This could be based on statistical properties, coverage of hazards or coverage of requirements.

Test data must show continued relevance, through systems evolution and over time. It is good practice to build up extensive regression suites containing coverage of all detected problems to date.

I.2.3 Interfaces with Existing Assessments

I.2.3.1 Data and Software

Although most people feel they have an intuitive understanding of the difference between software and data, upon closer examination the boundary is not always as clear as it may first appear.

Consider, for example, Java bytecode, which is operated on by a Java Virtual Machine. From one perspective, it could be argued that the Java bytecode is simply data. By extension, it could also be argued that the Java source code is also just data. This type of argument can be extended to suggest that any software can, at least from one viewpoint, be considered as data. Conversely, think about the data used in a 3D printer,

perhaps to produce a part for an aircraft. This data could be viewed as a program for the printer; that is, it could potentially be viewed as software. This type of argument can easily be extended across a range of situations, especially those relating to configuration data.

Whilst they are interesting, and potentially important, these philosophical considerations should not detract from the practical issue: there are some aspects of data (using the term in a generic sense) that are often not explicitly addressed in standards. These are a consequence of features that are more readily apparent in data than in software. Examples include:

- It is easy for data to be reused in a range of contexts and despite appearances it is not trivial to translate an assurance argument that the data is fit-for-purpose from one context to another.
- It is not always clear who owns or is responsible for data, especially when data is shared and processed amongst a collection of disparate systems.
- Data often has a lifetime, that is a time after which it is no longer valid. This may be a strict cut off, or a more gradual degradation in the utility (or applicability) of the data.
- There is often a default value for data. Whilst this can make systems easier to use and hence more productive it can be difficult to identify a default value that is appropriate for all circumstances.
- It can be easy to change data. In some circumstances this can give rise to a temptation to make uncontrolled and potentially untested changes. It can also allow data to be fraudulently changed after an accident.

In summary, data and software are closely related and, as such, need to be considered together in system engineering activities, including system safety analyses. However, data and software emphasise different facets of risk and they are susceptible to different mitigation approaches; this means there is also a need to adopt a data-focussed perspective. It also means that assurance levels related to software cannot be mapped directly to Data Safety Assurance Levels.

I.2.3.2 Data Safety and Security

When generating high-level processes and techniques to manage the risks posed by data, it is worthwhile understanding the difference between the safety risks posed by accidental failure to preserve Data Properties and the security risks posed by actors maliciously undermining the properties of data.

The relationship between safety and security, as engineering concepts, can be summarised by their relationships to cultural, developmental and aspirational properties of systems development.

Culturally, embedding both safety and security into an organisation is seen as a key strategic goal for creating systems that are both safe and secure. Developmentally, safety and security are quality factors, generating transverse requirements that impact the entire system. Most importantly, at the aspirational level, both safety and security have the common goal of preventing harm from accidental and malicious interventions respectively.

For an organisation aiming to create systems that are both safe and secure, these connections can be both a benefit and a burden. The shared goal of preventing harm means that both quality factors seek to identify routes to harm through analysis of the system being developed. This can result in shared processes and tools, which in turn can save time and money during systems development. However, safety and security interact in a more volatile way at the functional level. Security failings can undermine the safety

case for a system and, conversely, safety requirements can prevent the implementation of standard security solutions. For example, the German government published a report in 2014 into a fire at a steel works caused by a cyber attack that resulted in the control system being placed into an unsafe state and the safety system being unable to intervene (Section 3.3.1 of [14] - in German). In addition, "fail-safe" states can often leave a system with exposed security vulnerabilities.

These links between safety and security infer that there are connections between the sub-categories of data safety and information security: both attempt to take a data-centric view of the system of interest in order to improve the associated quality factor; and both attempt to prevent harm through the preservation of the properties of data within that system.

In the security domain, the three key properties of data considered are confidentiality, integrity, and availability. Confidentiality, the failure of which is termed "Information Disclosure" in the Microsoft Security Model, [15] is typically not a safety concern as, without malicious intent, information sharing is not inherently unsafe. However, when considering systems where confidentiality is an important property, the interaction between data safety and security cannot be trivially resolved. For example, accidental disclosure of information can form part of a causal chain which leads to harm from a malicious actor.

Data integrity is a critical property for both domains. The Microsoft Security Model describes malicious removal of the property of integrity as "tampering". Whether by accident or through malicious intent, the potential harm from loss of data integrity can be disastrous to a safety-critical system, from the values of drug dosages to control system parameters.

Data availability is also important to both domains. Loss of availability, or "denial of service" in the Microsoft Security Model, is another property that can be lost accidentally or through malicious intervention. Loss of availability prevents systems from functioning properly and can result in undefined behaviour if not mitigated by design.

Further guidance on the integration of safety and security can be found in a Code of Practice published by the IET [16]. The Code of Practice is written for engineers and engineering management to support their understanding of the issues involved in ensuring that the safety responsibilities of an organization are addressed, in the presence of a threat of cyber attack.

Appendix J Machine Learning (Informative)

> *Learning never exhausts the mind.*
> ***Leonardo da Vinci***

J.1 Machine Learning Training Data

A complete discussion about the assurance of Machine Learning /Artificial Intelligence algorithms is beyond the scope of this document. However, as such algorithms are inherently data-driven, the Data Safety Guidance provides the following notes on good practice for data sets used for Machine Learning / Artificial Intelligence applications.

The data for real-world machine learning scenarios may be effectively infinite (for example, with self driving cars, where the environment is largely unbounded) and can only be approximated by finite number of scenarios. Therefore it is crucial to have an extension process in place to extend the system when previously unknown situations are experienced. ISO 21448 [17] captures this process by introducing the term "Safety Of The Intended Functionality" (SOTIF) and requires the systematic handling of unknowns. Although specifically aimed at road vehicles, SOTIF may be of interest to other domains.

For more general guidance on managing the safety of Autonomous Systems, please refer to the safety assurance objectives guidance produced by the SCSC Safety of Autonomous Systems Working Group (SASWG) [2].

J.2 Data Categories

Three data categories are discussed: training data (the data used to train the machine learning model), test data (used to provide a measure the trained model's accuracy), and validation data (used to independently verify the trained model).

J.3 Real World Data

It is important to obtain sufficient quantities of data for the training data. It is generally assumed that this is sufficiently representative of situations that could be encountered to allow the algorithm to generalise the appropriate behaviour for all encountered situations. However, there are problems with real-life training data. Firstly, it is possible that rare, hazardous cases are never encountered during the capture of a data set (as those events have been engineered to be statistically unlikely) and are too dangerous, or expensive, to generate deliberately. Poor representation of rare cases in training data will result in a model that is insufficiently prepared to handle those important scenarios. Poor representation (or weighting) of rare cases in test data or validation data can result in error heuristics that do not provide adequate insight into the system's performance in rare situations. A second issue with real-world data is that amassing, understanding, verifying and validating it at scale is resource intensive. Hence it is not just a case of more testing, a more cost-effective approach is needed. Some possible techniques are: artificial test data set generation, data fault injection and simulation. It may well be more practicable to use simulated training data during the training phase to give more control and avoid the cost and effort of real-world testing. The issue then is how realistic the simulated data (and the associated simulation) can be. Note that artificial data sets can also be used to increase the frequency of rare events, thus biasing the algorithm to managing those

rare events effectively, but doing so, could impair the "sunny day" performance of the system.

J.4 Sensor Data

In many cases sensors will be on-board and embedded (e.g. on an automated vehicle) and will be subject to many real-world influences. Sensor data may be changed or degraded by both internal influences, e.g. system environment temperature, and external factors e.g. humidity, ambient light, weather conditions such as snow or fog, and rarely encountered extremes such as lightning or flood. Sensors may also suffer degradation due to ageing and specific faults due to their positioning, construction or configuration. Sensors may need to be diverse to increase resilience and give an overall more reliable output. Realistic data variations, informed by an understanding of likely sensor failure modes, need to be incorporated in the training data set (c.f. the AoA sensor in the Boeing 737 MAX 8, discussed in subsection H.5). Sensor fusion can effectively create "composite data", e.g. from merging of Lidar, Radar and Camera data; this will have different (and possibly hard to predict) properties compared to the individual sensors.

J.5 Data Coverage

Some notion of data coverage, that is, how well the training data covers the intended operational domain, is needed: this could be based on use of all known data sets, all known hazardous situations or some other measure. "White box" techniques involved in exercising all connected sensors or coverage of nodes in a neural network may have some value. Regardless, it will be essential that the training data covers all required safety test scenarios.

J.6 Data Set Assurance

There is a need to have assurance about the data sets themselves, including their configuration management. Assessment of the quality and suitability of the training data sets should be included in the safety argument.

The University of York has developed a method for the Assurance of Machine Learning for use in Autonomous Systems (AMLAS) [18]. The University's approach is intended to assist in the development of a compelling argument about a Machine Learning model, to feed into a system safety case.

J.7 Data Diversity

The degree of data diversity is important. Common data items across data sets need to be avoided, especially across training and validation data. Common data may include data derived from the same sources, environments, simulators, tools, techniques or mathematical models.

J.8 Data Properties

Bias, sufficiency and accuracy are all concerns with the data. Fidelity may also be a problem as modelling real-life sensor data is difficult. Errors should be introduced for training: this may be by analytical means, by random, automated sampling of data to determine the degree of similarity between samples, or by means

of deliberate insertion of known edge-cases. It is suggested that all the data properties mentioned in this guidance document are considered.

J.9 Data Set Management

Data sets will be large and complex and ensuring quality and consistency will be difficult. Measures will have to be taken to control, manage and archive large amounts of data. Data sets should be subject to formal change control and monitoring. Tools will be needed to manage the data.

J.10 Optimisation

What is an optimal size of a training or validation data set? A data set may contain many repeated or redundant values. If these do not add to the training outcome it is possible that some values may be removed. Also if there are ways in which the data set could be compressed or optimised then these should be considered to assist management and curation.

J.11 Compliance

A "safety by compliance" strategy for such data is difficult to implement as there are currently few existing standards and little guidance for data in this area. It is therefore difficult to quantify data sufficiency and as a result, no generally agreed "ALARP" principle for data.

It may be possible to demonstrate Data Safety through statistical methods, such as when millions of representative miles have been driven. However such approaches have generally been found insufficiently robust to support safety critical systems in other domains such as aviation, and so must be treated with caution. The demonstration of compliance for the data is likely to require a compliance argument for the tools that produced the data, the preservation of data properties as described within this document, and an update process such as that specified in ISO 21448 (SOTIF) [17].

J.12 References

This appendix provides only a brief overview of the issues around the application of data safety techniques to machine learning. It is based upon information in the following documents, which should be consulted for further details:

- Assuring the Machine Learning Lifecycle: Desiderata, Methods, and Challenges [19]
- Quantifying Data set Properties for Systematic Artificial Neural Network Classifier Verification [20]
- Safety Critical Integrity Assurance in Large Data sets [21]

This page is intentionally blank

Appendix K Dark Data and Safety (Informative)

> *…we can be blind to missing data … that can lead us to conclusions and actions that are mistaken, dangerous, or even disastrous.*
> ***David Hand***

K.1 Introduction

This appendix outlines some of the safety implications arising from the issues identified by Prof. David Hand in his work on "Dark Data" presented in his book: "Dark Data: Why What You Don't Know Matters" [22] and website [23]. Dark Data relates to data that is not available, but nevertheless is important, and indeed, in some cases, more important than the data that is available.

Unintentionally Donald Rumsfeld popularised the concept of Dark Data with his famous speech:

> *"…there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know…"*

Figure 5 neatly shows the dark categories in grey:

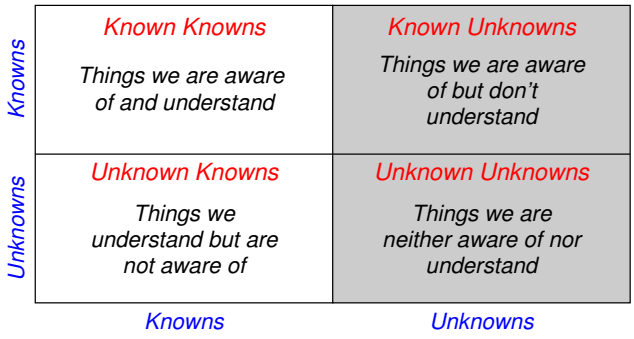


Figure 5: Categories of dark data

K.2 Dark Data Example

A meeting was held prior to the fatal Challenger disaster in January 1986, to decide whether the flight should go ahead due to the prevailing cold weather and concerns over the performance of O-ring seals at low temperatures. The decision to launch was made on the basis of the following data points that show the temperature at which previous O-ring problems had occurred.

On this basis, it was concluded that: "there is nothing irregular in the distribution of O-ring 'distress' over the spectrum of joint temperatures at launch between 53 degrees Fahrenheit and 75 degrees Fahrenheit." However, there was Dark Data in this dataset — the data points that show the temperatures for successful launches when there were no O-ring problems were left out. These are shown as the red points in Figure 7.

When the Dark Data is included, there is an obvious correlation between temperature and O-ring failures and it is possible the decision to launch may have been different if this additional data had been presented.

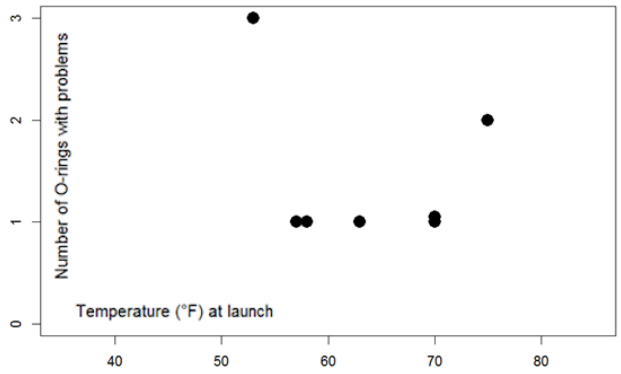


Figure 6: O-ring Failures by Temperature

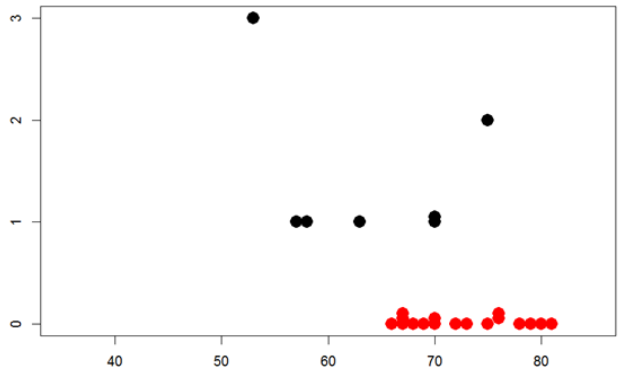


Figure 7: O-ring Performance by Temperature

K.3 Dark Data Categories and Safety Examples

In his book, David introduces a taxonomy of 15 categories of Dark Data. This section discuses each of these from a data safety perspective.

K.3.1 Data We Know Are Missing: “Known unknowns”

This case is very common in safety justifications where assurance information may be withheld for commercial reasons or does not exist, but we know, or are informed, that it isn’t available. Common examples include:

- Assurance information for COTS components is unavailable
- Information about legacy systems was never produced or is now lost
- ML training data restricted to a particular context of use

If this is the case, it can be mitigated in several ways, including use of warnings, training, restrictions of use, etc. Evidence can also be substituted with other more indirect assurance e.g. established organisational track-record in the sector, or audit reports.

K.3.2 Data We Don't Know Are Missing: "Unknown unknowns"

This is the most serious and far-reaching case. Occurrence is hopefully less common than case K.3.1, but it is important to acknowledge that it does happen. Some examples are:

- The recent Covid-19 Track and Trace data loss (subsection H.4), where the organisation handling the data was unaware that rows were missing from a spreadsheet for some time is illustrated in Figure 8
- Somebody knows a problem with a system but does not tell
- Machine Learning training data missing edge / corner cases
- Key safety requirements missed
- Change of use never anticipated
- Data loss which may be discovered after some period (or indeed never)
- Test cases never thought of, so never created or executed

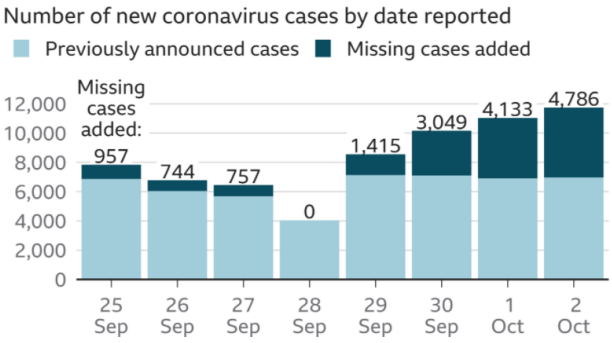


Figure 8: Covid-19 Track and Trace Data Loss

In many cases the loss may be discovered after some time, and it is incumbent on the organisation involved to analyse the impact of the missing data over the time period, including subsequent decisions and actions. Its effects should not be underestimated. This case can fundamentally change the safety picture and is probably in the highest safety risk category.

Data that was missing can subsequently be found. The following options show possible approaches to handling this "rediscovered data":

i) Apply the missing data

ii) Ignore the missing data

iii) Mention that the data was missing but not take it into account, and

iv) Perform an impact analysis on the missing data and then act according to the results

K.3.3 Choosing Just Some Cases

This is where something or somebody has been selective. Examples might be:

- Selection of test runs that succeeded (ignoring failed runs and their diagnostics)

- Selective sampling from sensors, or where the sampling intervals are chosen badly
- Incorrect filtering of the data, leaving out more cases than intended

Note that with complex or informal criteria the effects could be as case K.3.2, i.e. you don't know what has been left out.

Mitigations include use of peer review, independent teams, and audits. It is important to ask questions and challenge the data selected to be sure it can be justified.

K.3.4 Self-Selection

This is considered to be similar to case K.3.3, but could be even more informal or ambiguous. Again mitigations include: use of peer review, independent teams, and audits.

K.3.5 Missing What Matters

This was considered similar to case K.3.2 in impact terms, and might well be considered the "Elephant in the Room". Examples might be:

- Measuring the wrong things, e.g. poor safety metrics / indicators
- Too much data to deal with or analyse, so some is ignored
- Too much filtering or processing, so losing information along the way
- Being too close to the data, i.e. the "wood for the trees". This is when the detail masks the overall issue with data, e.g. a slow trend or bias masked by peaks.

Mitigations include independence as K.3.3 and K.3.4 but also "taking a step back" to look at the bigger picture.

K.3.6 Data Which Might Have Been

This is where it is impossible to obtain the relevant data as a consequence of how the system/scenario is constructed. This was considered an interesting and important case.

This could for example, be due to an inappropriate system architecture e.g. single data channel when a multiple channel approach should have been used, such as in the Boeing 737 MAX 8 accidents (see section H.2). It is therefore important that Mitigations are in place at design time, as they are often very difficult to retro-fit.

Mitigations include assessing the data collection opportunities gained or lost from the design or architectural approach — at design time.

K.3.7 Changes with Time

This is a common problem in a safety context. Data in safety systems often becomes obsolete or out-of-date and may still be mistakenly used. Some examples are:

- System configuration data not kept up to date as software or hardware changes
- Medical drug interaction databases
- Software patches requiring updates to configuration or system data, which is not always done

Mitigations include keeping critical data up-to-date and regularly refreshed, and knowing how old the data is in the first place.

K.3.8 Definitions of Data

This was considered a common case for systems with databases or those exchanging data with external systems, e.g.

- Taxonomies e.g. in machine learning categorisation schemes
- Data schemas in medical record systems
- Interface specifications and data definitions, which often evolve over time. These can render old data obsolete / subject to misinterpretation, and often needing migration/translation or re-interpretation.

Mitigations include keeping a list of known changes / incompatibilities and documenting the changes or fixes that have to be applied to make the data usable or consistent.

K.3.9 Summaries of Data

This is often seen in data about safety systems and projects:

- Safety metrics or indicators where data is aggregated to create a composite value
- Data fusion across multiple sensors Summaries can be misleading or cause "boundary reactions", e.g. Red-Amber boundary.

Mitigations include thinking about what missing data could cause (i.e. performing sensitivity analysis) — for instance, what decisions might be made erroneously due to certain data values being omitted, late or slightly perturbed.

K.3.10 Measurement Error and Uncertainty

Sensors can degrade and fail over time, especially in harsh environments such as automotive, marine or aviation:

- Sensors may feed faulty or biased data into systems
- Sampling techniques can cause some artefacts in themselves
- Interval polling interval can lead to misleading readings
- Data fusion can be impacted if multiple sensor values are combined

Hence sensors need to be regularly maintained and calibrated or replaced, and their interfaces need to be able to detect any problems and report faults.

K.3.11 Feedback and Gaming

This can often happen in safety justifications or test case production:

- Early production of a safety argument could lead to only those artefacts that support the claim being generated, e.g. requirements-based testing vs. stress testing
- Confirmation bias in safety justifications and can cause over-optimism

Mitigations include the use of dialectic argument approaches (where both positive and negative cases can be considered). It is also useful to get a second opinion, independent review or a 'fresh pair of eyes' to check the justification.

K.3.12 Information Asymmetry

This is common where there are multiple stores or sources of the same data:

- Multiple / backup databases where they are not kept in sync
- Image recognition systems that learn, but fail to share data
- Issues of divergence of data across multiple sources.

Comparisons, reviews and data audits may help in these cases. In general the issue of divergence across multiple data sources needs to be recognized and addressed in the most appropriate technical, and ideally automated, way.

K.3.13 Intentionally Darkened Data

This can and does happen, e.g.

- Defence, security and government sectors where data is purposefully hidden or destroyed
- Records intentionally deleted after an accident to cover up what really happened

This can be mitigated using appropriate technical measures (e.g. blockchain, digital signatures, off-site backups), and also robust procedures with oversight.

K.3.14 Fabricated and Synthetic Data

Fabrication (i.e. making up the data) is surprisingly common, e.g. in medical, policing and maritime sectors. Sometimes it is created with the best of intentions as it was not produced or collected at the right time and is now required (e.g. for an audit), but sometimes it is created to mask a problem. Synthetic data is often used where there are difficulties in producing enough real data with the right characteristics:

- Data is retrospectively entered / patched to make a "clean" record
- Synthetic autonomous vehicle training databases can have issues with artificial data if not realistic

Possible mitigations include comparisons with current real-world data and checking with historical data.

K.3.15 Extrapolating Beyond Your Data

Systems, especially machine learning systems (see Appendix J) have to cope with values outside of their training data, but the outcomes may be unexpected:

- Bizarre results from recognition / detection systems may result

Mitigations include use of machine learning training data containing edge/corner cases, boundary cases, and testing well beyond normal or acceptable ranges to give insight into the system degradation behaviour.

K.4 Summary

Dark Data is a very useful way of thinking about problems and solutions. It is important to always think of the bigger picture, considering what information is not known:

- What might have been left out, intentionally or otherwise?
- What might be missing due to the way things are done (or the way those things are being executed)?
- Could missing items cause any safety problems?
- What is outside of the defined operational domain?
- Can you present your results / outputs in a way that shows the dark data?

K.5 Further Reading

A number of resources are available for further information on how Dark Data relates to data safety:

- The October 2020 edition of the SCSC Newsletter [24] contains articles both by David Hand and on Dark Data Safety.
- A presentation on Dark Data given by David Hand to the DSIWG [25];
- A presentation by Mike Parsons given at the University of York [26].

This page is intentionally blank

Appendix L Dazzle Data and Safety (Informative)

> *Camouflage is a game we all like to play, but our secrets are as surely revealed by what we want to seem to be as by what we want to conceal*
> ***Russell Lynes***

L.1 Introduction

This appendix outlines some of the safety implications arising from the issues identified by "Dazzle Data" in contrast to "Dark Data" presented in David Hand's book: "Dark Data: Why What You Don't Know Matters" [22] and website [23]. Dark Data relates to data that is not available but nevertheless is important.

"Dazzle Data" refers to spurious, superfluous or unexpected data that masks and confuses the picture and can reduce your ability to see details, and indeed the whole picture — a bit like noise or camouflage.

> It is data you don't want, didn't ask for, arrives more frequently than expected, is redundant, or data that arrives at an unexpected or inconvenient time or in the wrong format or sequence, so requiring extra resources to deal with…

At first sight it might be thought this is just an annoyance rather than a problem, however Dazzle Data can mask, distort or prevent usage of the real or desired data. It can hide the true picture as in "wood for the trees" and in the worst case create real problems.

Some examples of such false positive alerts that cause real alerts to be ignored are:

- The classic case of "Crying Wolf".
- Denial of Service Attack, when servers can be blocked with useless requests that cannot be distinguished from the real requests.

Data which is truly spurious and believable (e.g. generated by extensive electrical noise, or fabricated to mask a fraud) may be accepted as valid data, leading to potentially hazardous results.

Dazzle Data may be categorised in the same grid manner as Dark Data, as shown in Figure 9, where the yellow areas indicate potential dazzle data.

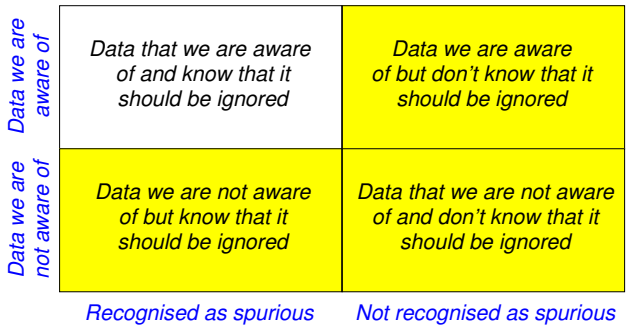


Figure 9: Dazzle data categorisation

L.2 Dazzle Data Examples

L.2.1 Data We Are Aware Of — Recognised as Spurious

Repeated false positive alerts (e.g. from faulty sensors or alarms). These tend to be annoying irritants rather than safety issues, however they can lead to alarms being permanently switched off, masking true problems. An example from everyday life might be removing the battery from a badly place smoke alarm in a kitchen which repeatedly sounds when the toaster is used.

L.2.2 Data We Are Aware Of — Not Recognised as Spurious

Electromagnetic interference (EMI) affecting transmitted data is a good example of this case; we know it exists as a possibility but don't know how it might affect data in a system or a communications path, and this could be in different ways at different times or days.

L.2.3 Data We Are Not Aware Of — Recognised as Spurious

In many cases we do not know what changes or corruptions may affect the data, but we have strong correction mechanisms to cope with the problems regardless. A good example is data stores on a spacecraft which have redundancy and error correcting codes built-in and so can deal with the majority of corruptions caused by cosmic rays.

L.2.4 Data We Are Not Aware Of — Not Recognised as Spurious

An example of this is where data is mistakenly added to a machine learning training data set resulting in bizarre and possibly hazardous behaviours of the system using it (e.g. an autonomous road vehicle). It is paramount that data used for such image recognition systems filters and excludes potentially dangerous extraneous data arising from unanticipated situations

L.3 Data Categories and Safety Examples

In his book, David Hand introduces a taxonomy of fifteen categories of Dark Data. This section discuses each form of Dazzle Data and considers it from a systems and safety assurance perspective. Some of the categories are the same as Dark Data, but some are very different.

L.3.1 Data We Know are Superfluous or Unneeded: "Known Extras"

This case is very common in systems where an interface may be flooded with unsolicited messages. It is also common in safety justifications where assurance information may be padded out with extra, irrelevant information that can mask the underlying safety argument (which may or may not be intentional). It can be a serious problem in large, complex safety documents or detailed safety analyses. Luckily, in this case, the data is recognised as superfluous and can be ignored. Common examples include:

- Mailboxes filled with spam mail, preventing important messages being read
- Repeated stall warnings when the aircraft is under control

- Assurance information in a safety case is included for components which are not part of the solution in use at that site or situation
- Assurance information about old or legacy components is included but these are now not in service
- Machine learning training data contains many cases which are duplicates or very closely related, so adding nothing to the learned behaviour but making the set hard to deal with

This case can be mitigated in several ways, including careful filtering, review, use of concise notations (such as Goal Structuring Notation) to extract the essence, and periodic audits and cleans.

L.3.2 Data We Don't Know Are Unneeded or Spurious: "Unknown Extras"

This is the most serious and far-reaching case, where the additional data is not recognised as unneeded and may be processed, analysed or be left in place when it should be removed. Some examples are:

- Legacy code in software where nobody understands its function, or how it relates to the current code and so is reluctant to remove it. The Ariane 4 Inertial Reference function left in place in the Ariane 501 launch disaster might be such a case. Note that code whose function is known would be under the first case, discussed in L.3.1
- Parts of the safety case or safety argument are supplied separately (e.g. by a subcontractor or 3rd party) and they are obscure. In this case it will not be known which parts are relevant to the particular situation. Some information may be irrelevant or worse, misleading.
- Machine learning training data containing too many outliers, which are not recognised as such

In many cases the extra data may be discovered after some time, and it is incumbent on the organisation involved to analyse the impact of the complete set of data which may have been used over the time period, including subsequent decisions and actions. The effect of spurious data should not be underestimated, as it may have masked, prevented or distorted the intended use of the nominal data for some time. This case can fundamentally change the safety picture and is probably in the highest safety risk category.

Data found to be erroneous (i.e. it should not ever have been in the system or in the safety argument) is a problem. The following options show possible approaches to handling this data:

i) Delete the erroneous data

ii) Accept the erroneous data, i.e. continue using it

iii) Report that the data was erroneous but take no further action

iv) Establish under what circumstances and situations the erroneous data would have had an effect

v) Perform a full impact analysis on the effects of the erroneous data and then act according to the results

L.3.3 Data Obscuration: Missing What Matters

This is where the meaning of the overall data set becomes obscured due to the extra unnecessary data. Examples might be:

- Measuring the wrong things due to excessive noise or too much data to deal with
- Processing involving sampling only picks bad data elements
- Being too close to the data, i.e. the "wood for the trees". This is when the extra data masks the overall issue with the data, e.g. a slow trend or bias hidden by large local variations.

Mitigations include review, statistical checks and "taking a step back" to look at the bigger picture.

L.3.4 Data Masking in Specific Cases

This is where the extra data specifically masks, obscures or hides particular data elements (but not all). A particularly nasty case of this is where filters are put in place to remove unwanted data values, but those filters actually remove less (or more) than they should (i.e. don't remove all unwanted cases or remove valid values as well). Some examples might be:

- The number of successful test runs vastly outweighs failed runs and so the failures are not investigated
- Incorrect filtering of the data, leaving in some cases that should have been excluded

Mitigations include use of review and completeness checks. Note that over-aggressive filtering would create cases of Dark Data.

L.3.5 Masquerade or Fraudulent Data

This is where data has been constructed to fool the system consuming it, hiding, overlaying or replacing the correct data. Often this will be malicious and should be filtered or rejected by the target system, but of course may not be.

- Intentional fraud
- Some security attacks

Mitigations include audit, blockchain, monitoring, intelligent profiling of data and detection of changes.

L.3.6 Incorrect Definitions of Data

This is considered a common case for systems exchanging data with external systems, where they may duplicate, translate or incorrectly send multiple messages. They may be time-separated, for instance if communications are lost and then regained, leading to confusion.

- Data sent in the wrong rate or units (e.g. every millisecond rather than second)
- Data given for the wrong range or duration (e.g. for a month rather than a day
- Data sent for the wrong domain or scale (e.g. national values rather than regional)
- Text messages re-sent to a mobile phone when coverage restored

Mitigations include making sure interface specifications are clear and ambiguous, rejecting incorrect size or scale data sets, keeping a list of known changes / incompatibilities and documenting the changes or fixes that have to be applied to make the data usable or consistent.

L.3.7 Summaries of Data

Spurious data can affect summaries in a significant way if composite values are calculated, e.g.

- Calculations of averages or other statistics affected by duplicates
- Spurious outliers can lead to overfitting when analysing data trends

Mitigations include audit and assessing what extra data could cause (i.e. performing sensitivity analysis) and establishing what decisions might be made erroneously due to certain data values being present.

L.3.8 Information Asymmetry

This is common where there are multiple stores or sources of the same data. If one has erroneous duplicate values (i.e. many null values used for padding) then comparisons between them may fail.

- Multiple / backup databases where they are not kept in sync
- Issues of divergence of data across multiple sources.

Comparisons, reviews and data audits may help in these cases. In general the issue of divergence across multiple data sources needs to be recognised and addressed in an automated way.

L.3.9 Intentionally Dazzled Data

This might happen in a secure context where key data is effectively "camouflaged" by hiding within large data items (e.g. images) or the use of large amounts of apparently routine data to mask the secure data.

- Defence, security and government sectors where data is purposefully hidden
- An organisation may provide copious amounts of safety case collateral to hide a weak safety case

L.3.10 Extrapolating Beyond Your Data

Machine learning systems have to cope with values outside of their training data, but the outcomes may be unexpected if the training data contains many spurious values:

- Bizarre results from recognition / detection systems due to out of range values
- Image components mislabelled leading to strange results

Mitigations include checking of the values that are used in training, analysis of outliers and repeats, deletion of duplicates and use of machine learning validation data containing edge/corner cases and boundary cases.

L.3.10.1 A Note on Sensors

Sensors can degrade and fail over time, especially in harsh environments such as automotive, marine or aviation. In such cases sensors may feed erroneous or additional data into systems (e.g. if an out of normal range situation is detected), leading to misleading processing or false alarms. The Boeing 737 MAX 8 accidents might fall into this category as the angle of attack sensor erroneously generated high values, and certainly the systems/processing which passed on the values created spurious data. Some examples are:

- Faulty sensors
- Multiple sensors that do not have their values properly combined
- Sampling techniques which generate additional data
- Interval polling interval can lead to misleading readings
- Data fusion can be impacted if multiple sensor values are combined

Mitigations include independent monitoring of sensors and regular maintenance, calibration or replacement of hardware. Their interfaces need to be able to detect any problems and report faults. In particularly critical applications, it may be necessary to minimise the potential for common mode failures by utilising disparate tecnologies, or at least sensors from different manufacturers.

An example may be found in https://en.wikipedia.org/wiki/Qantas_Flight_72 where:

> …the CPU of the ADIRU corrupted the angle of attack (AOA) data. The exact nature of the corruption was that the ADIRU CPU erroneously re-labelled the altitude data word so that the binary data that represented 37,012 (the altitude at the time of the incident) would represent an angle of attack of 50.625 degrees. The FCPC then processed the erroneously high AOA data, triggering the high-AOA protection mode, which sent a command to the electrical flight control system (EFCS) to pitch the nose down.
>
> The FCPC algorithm was very effective, but it could not correctly manage a scenario where there were multiple spikes in either AOA 1 or AOA 2 that were 1.2 seconds apart — i.e., if the 1.2-second period of use of the memorised value happened to end while another spike was happening.

L.4 Summary

Dazzle Data is a very useful way of thinking about data problems and solutions. It is important to always think of the bigger picture, considering what information is superfluous and may be distorting or masking the real picture:

- What might be hidden intentionally or otherwise due to the extra values?
- Could the extra items cause any safety problems, e.g. change a numerical calculation?
- How would a system cope if it received data it was not expecting?
- How do you characterise the nature of unexpected data so as to ensure it can be handled if it does occur?
- Can you present your results / outputs in a way that shows the extra data?

Appendix M Covid-19 (Informative)

> *The public health community wants a safe and effective [COVID-19] vaccine as much as anybody could want it. But the data have to be clear and compelling.*
> ***Michael Osterholm***

M.1 Covid-19 and Data

The Covid 19 crisis has highlighted a number of areas where better data and data management could have improved outcomes and hence reduced the death toll. Such pandemic-related data is therefore very much safety-related data.

Some issues related to Covid-19 data are:

1. The lack of consistency and standardisation in handling the data, e.g:
    a. In predictive models where many assumptions may be wrong, or the algorithms inappropriate
    b. Presentation of statistics in a selective or misleading way
    c. Methods of data collection which may be selective or incomplete. For instance reporting on the number of positive test cases is always misleading, as many people may be asymptomatic with the virus so never get tested.
    d. Calculations and filtering
    e. Allowances for delays in collection or processing
    f. Intentional and unintentional bias
    g. Use of averaging (e.g. moving averages) and smoothing of plots hiding sudden increases
    h. Loss of data (e.g. in the recent UK Test and Trace system due to old versions of Excel)

    All of which have prevented any meaningful comparisons internationally, even between countries in Western Europe. They also lead to public confusion; this in turn leads to mistrust and a refusal to abide by guidance and regulations.
2. The poor data within the Test and Trace systems is a major factor in the failure of these systems. If data is not accurate, timely or complete then contacts cannot be traced in time, and the effort put into the activity is wasted. These systems in the UK need huge improvement as there is currently low contact performance and hence very poor outcomes. Background reading on this may be found at this link: https://www.bbc.co.uk/news/health-55008133

M.2 Systems Involved with Covid-19 Data

Many systems have been created or re-deployed to help manage the pandemic. These systems consume and produce vast amounts of data, some of which is critical and could affect safety of individuals or the general population. Some identified systems are shown in Table 28. For each of these, it is worth thinking through some basic data failure modes, e.g. data is lost, late, incorrect or incomplete. For instance if we are running an infection / spread model and we feed it with stale data, then its predictions will clearly be inaccurate.

Table 28: Systems involving data used to manage the pandemic

Analysis of air flow and particles	Satellite imagery (Wuhan)	Video conferencing	Risk assessment systems
Infection / spread models (inc new variants)	Itinerary systems	Remote consultation systems	Computational bioinformatics tools
Infra-red / thermal cameras	Infection testing systems	Ventilators / other patient management devices	Appointment systems
Track and Trace apps	Antibody testing systems	Personal risk profiling apps / systems	Border Control / Quarantine systems
Track and Trace back office systems	Drug trials systems / data	Allocation / reservation / booking systems	Risk profiling / prioritising for vaccination
Track and Trace service	Ventilation models & UV sterilisers	Models of built environments	Digital Twins (systems and biological: lungs, etc.)
Supply chain systems	Behavioural models	Safety analyses (STAMP/STPA), etc.	(Automatic) cleaning systems
Virus aerosols modelling	Analysis of delays in system of reporting / actions	Modelling / public perception of the disease	Virus shedding models
Vaccination booking / tracking / monitoring	Sanitiser systems	Lockdown easing models	Vaccination Passports
Vaccination production data	Vaccination trials and reporting data	Vaccination "Yellow Card"	Cross-system data sharing
PPE testing results	Data used to inform public perceptions	No coordination across international boundaries — incompatible systems	Use of blockchain to validate Covid and vaccination status

M.3 Falsification/Misinformation of Data

One serious and perhaps unexpected aspect of the pandemic is that of misinformation. There are people either in denial of the virus's dangers, refusing to socially distance or refusing vaccinations. Reasons for these behaviours have generally been driven by intentional misinformation, ignorance, superstition, or economics. Marianna Spring, the BBC's specialist reporter covering disinformation and social media put the problem of misinformation succinctly when she stated "The problem with misinformation is that it is popular." See Barack Obama: One election won't stop US 'truth decay' — BBC News at https://www.bbc.co.uk/news/election-us-2020-54910344. Methods need to be devised or improved to prevent this effect, and to restore trust in carefully managed data.

M.4 Rumsfeld's known unknown and unknown unknown data conundrum

It is clear that until China reported to the world that Covid 19 had emerged as a threat, that data about the virus was an unknown unknown. However, we know there are thousands of viruses in animals that could pose a threat. These all need analysis and it may be possible to use massive computer analysis of genetic data to identify likely new threats.

A paper was given by Nick Hales as part of the 2021 Safety-Critical Systems Symposium which gives more detail on this topic *"Data Safety in Virus Outbreaks — Lessons learnt and Recommendations"* [27].

M.5 Learning

It is important to learn from these deficiencies because, while Covid 19 has brought tragedies with it, it is unlikely to be the last, or indeed, the most dangerous virus we will face. We must do better next time.

This page is intentionally blank

Appendix N DSAL customisation (Informative)

> *One size does not fit all*
> ***Frank Zappa***

N.1 Introduction

Within the body of this document, a method has been provided for the assignment of DSALs. However it is anticipated that, as with the methods used for the assignment of safety criteria within system safety analysis, some programmes may find it desirable to develop alternate approaches. This section presents some possible methods for the determination of likelihood. These methods are intended to serve as approaches for consideration when developing project-specific criteria, as these approaches are less generic than that presented through Table 8, so it is highly likely that customisation will be required.

N.2 Significance factors

A method of determining likelihood from the different characteristics is to implement a scoring scheme that apportions a quantitative value for each of the characteristics, with the sum giving the total likelihood score. The total score is then compared against a scale, and that in turn determines the overall low, medium or high assessment.

For example, consider the modified version of Table 8 illustrated in Table 29

Table 29: Calculation of likelihood — option 1

	Score		
	2	**1**	**0**
Proximity	A known use of the data is highly likely to lead to an accident.	A possible use of the data could lead to an accident.	All currently foreseen uses of the data could lead to harm only via lengthy and indirect routes.
Dependency	Data is completely relied upon.	Data is indirectly relied upon.	Little reliance on data.
Prevention	Difficult or impossible to guard / barrier against errors.	Possible to guard / barrier against errors.	Easy to guard / barrier against error.
Detection	Low or no chance of anything else detecting an error.	Some other people / systems are involved in checking the data.	Many other people / systems are involved in checking the data.
Correction	Difficult or impossible to correct or workaround errors.	Possible to correct or workaround errors.	Easy to correct or workaround errors.

For each of the characteristics, the applicable assessment of likelihood is then selected and scored. So for example, if it is "Possible to guard/ barrier against errors" for Prevention, then the score for that characteristic would be 1. Each characteristic is then scored and they are then summed to give a total score. The range of possible values will run from 0 (all choices in the far right column, favouring low likelihood

aspects) through to 10 (all choices in the far left column, favouring high likelihood aspects).

The overall likelihood in the assessed against a scale such that shown in Table 30.

Table 30: Likelihood assessment

Low	Medium	High
0–2	3–6	>6

N.3 Weighted characteristics

The method presented in section N.2 may be enhanced to provide a more holistic overall assessment of the likelihood based on all characteristics. Note that the scheme in section N.2 allocated equal significance to each of the characteristics. This method could be further refined if necessary to apply weightings to each of the characteristics, as shown in Table 31.

Table 31: Calculation of likelihood — option 2

		Score		
	Weighting	2	1	0
Proximity	1.5	**A known use of the data is highly likely to lead to an accident.**	A possible use of the data could lead to an accident.	All currently foreseen uses of the data could lead to harm only via lengthy and indirect routes.
Dependency	1.0	Data is completely relied upon.	**Data is indirectly relied upon.**	Little reliance on data.
Prevention	1.3	**Difficult or impossible to guard / barrier against errors.**	Possible to guard / barrier against errors.	Easy to guard / barrier against error.
Detection	0.7	Low or no chance of anything else detecting an error.	Some other people / systems are involved in checking the data.	**Many other people / systems are involved in checking the data.**
Correction	0.5	Difficult or impossible to correct or workaround errors.	Possible to correct or workaround errors.	**Easy to correct or workaround errors.**

The total score is then calculated by first multiplying the individual characteristic's score by the weighting before summing all the values. For example, if the selections highlighted in bold were made, then the score would be

$$(1.5 \times 2) + (1.0 \times 1) + (1.3 \times 2) + (0.7 \times 0) + (0.5 \times 0) = 6.6$$

resulting in a *High* assessment rather than the *Medium* that would result with no weighting. This is because Proximity and Prevention are considered (in this particular example) more important than Detection and Correction. The weightings within a project-specific version of this table would be chosen by the organisation to suit the particular scenario under consideration.

Appendix O Acronyms, Definitions and Glossary (Discursive)

> *The plural of anecdote is not data.*
> ***Mark Berkoff***

O.1 Acronyms

Acronym	Expansion
AAL	Above Aerodrome Level
ARP	Aerospace Recommended Practice
ARQ	Automatic Repeat-reQuest
ATM	Air Traffic Management
ATSB	Australian Transport Safety Bureau
BIT(E)	Built-In Test (Equipment)
CFIT	Controlled Flight Into Terrain
CNS	Communications, Navigation, Surveillance
CoD	Certificate of Design
COTS	Commercial Off-The-Shelf
CRC	Cyclic Redundancy Check
CSV	Comma Separated Variable
CT	Computed Tomography
DCB	Data Coordination Board
DME	Distance Measuring Equipment
DOC	Department Of Corrections
DRACAS	Defect Reporting And Corrective Action System
DSAL	Data Safety Assurance Level
DSG	Data Safety Guidance
DSIWG	Data Safety Initiative Working Group
DSMP	Data Safety Management Plan
ECS	Electronic Chart System
ECU	Electronic Control Unit
EDM	Entry Demonstrator Module
EGPWS	Enhanced Ground Proximity Warning System
EHR	Electronic Health Record
ENC	Electronic Navigational Chart
ESA	European Space Agency
FAA	Federal Aviation Administration
FMGS	Flight Management Guidance System

Acronym	Expansion
FMS	Flight Management System
FDAL	Function Development Assurance Level
GCS	Ground Control Station
GP	General Practitioner
GPS	Global Positioning System
GTOLS	GPS Take Off and Landing System
HAZOP	Hazard and Operability Study
HSE	Health and Safety Executive
HUMS	Health and Usage Monitoring System
ICD	Interface Control Document
ICAO	International Civil Aviation Organisation
IDAL	Item Development Assurance Level
IMC	Instrument Meteorological Conditions
IMU	Inertial Measurement Unit
IRS	Inertial Reference System
ISO	International Organisation for Standardisation
IV	Intravenous
LHR	London Heathrow
MAIB	Maritime Accident Investigation Board
MCA	Maritime and Coastguard Agency
MSAW	Minimum Safe Altitude Warning
NaN	Not a Number
NOTAM	Notice to Airmen
ODR	Organisational Data Risk
OOW	Officer Of the Watch
OSI	Open Systems Interconnection
RDA	Radar Doppler Altimeter
SAR	Search And Rescue
SCSC	Safety-Critical Systems Club
SIL	Safety Integrity Level
SMP	Safety Management Plan
SOP	Standard Operating Procedure
SSS	Safety-critical Systems Symposium
TCAS	Traffic Collision Avoidance System
UAS	Unmanned Air System
USB	Universal Serial Bus
VMS	Voyage Management System
VOR	VHF Omnidirectional Range
XML	eXtensible Markup Language

O.2 Definitions & Glossary

	Definition	Source
A		
Accuracy	Closeness of agreement between a test result and the accepted reference value. Note that a test result can be observations or measurements.	ISO 19113:2005 [28]
	A degree of conformance between the estimated or measured value and the true value.	(EU) No 73/2010 [29]
Accuracy (temporal)	Correctness of the temporal references of an item (reporting of error in time measurement). Correctness of ordered events or sequences, if reported. Validity of data with respect to time.	ISO 19138:2006 [30]
(data) Assurance Level	The required assurance level for the aeronautical data process is identified, based on the overall system architecture through allocation of risk determined using a preliminary system safety assessment.	RTCA/DO-200A [31]
	An indication of how much assurance is required (commensurate to risk) before deploying software into an operational system.	J Spriggs, based on (EC) No 482/2008 [32]
Adaptation Data	Data used to customise elements of the Air Traffic Management System for their designated purpose. Adaptation data is utilised to customize elements of the CNS / ATM system for its designated purpose at a specific location. These systems are often configured to accommodate site-specific characteristics. These site dependencies are developed into sets of adaptation data. Adaptation data includes data that configures the software for a given geographical site, and data that configures a workstation to the preferences and / or functions of an operator. Examples include, but are not limited to: 1. Geographical Data - latitude and longitude of a radar site. 2. Environmental Data - operator selectable data to provide their specific preferences. 3. Airspace Data - sector-specific data. 4. Procedures - operational customisation to provide the desired operational role. Adaptation data may take the form of changes to either database parameters or take the form of pre-programmed options. In some cases, adaptation data involves re-linking the code to include different libraries. Note that this should not be confused with recompilation in which a completely new version of the code is generated.	ED-153 [33]
Aeronautical Data	A representation of aeronautical facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing.	(EU) No 73/2010 [29]
	Data used for aeronautical applications such as navigation, flight planning, flight simulators, terrain awareness, and other purposes.	RTCA/DO-178C [34]
Availability	The property of being accessible and usable upon demand by an authorized entity.	ISO27001:2013 [35]
B		

	Definition	Source
C		
Completeness	Completeness of the data provided.	RTCA/DO-200A [31]
Configuration Data	Data that configures a generic software system to a particular instance of its use.	(EC) No 482/2008 [32]
	Data that configures a generic software system to a particular instance of its use (e.g., data for flight data processing system for a particular airspace, by setting the positions of airways, reporting points, navigation aids, airports and other elements important to air navigation).	ED-153 [33]
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	ISO27001:2013 [35]
(data) Correctness	Completeness, self-consistency, protection against alteration or corruption and consistency with the functional requirements of the data driven system.	IEC 61508 Part 3 [6]
(data) Coupling	The dependence of a software component on data not exclusively under the control of that software component.	RTCA/DO-178C [34]
(data) Criticality	Classification of data by the potential effect of erroneous data on the expected operation that is supported by that data.	RTCA/DO-200A [31]
Critical Data	Data with an integrity level as defined in Chapter 3, Section 3.2 point 3.2.8(a) of Annex 15 to the Chicago Convention, i.e., integrity level one in one hundred million: there is a high probability when using corrupted critical data that the continued safe flight and landing of an aircraft would be severely at risk with the potential for catastrophe.	(EU) No 73/2010 [29]
Customisation (data)	Data used to configure a system or component.	Def(Aust)5679 [36]
D		
Data	A thing given or granted; something known or assumed as fact, and made the basis of reasoning or calculation; an assumption or premiss from which inferences are drawn.	Oxford English Dictionary (OED)
	A reinterpretable representation of information in a formalized manner suitable for communication, interpretation or processing.	ISO/IEC 2382 [37]
Database	A set of data, part or the whole of another set of data, consisting of at least one file that is sufficient for a given purpose or for a given data processing system.	RTCA/DO-178C [34]
Data Chain	An 'Aeronautical Data Chain' is a conceptual representation of the path that a set, or element of aeronautical data takes from its creation to its end use. An aeronautical data chain is a series of interrelated links wherein each link provides a function that facilitates the origination, transmission and use of aeronautical data for a specific purpose.	RTCA/DO-200A [31]
	A collection of organisational data processing functions, where data is transferred from one chain participant to another between data origination and end use.	P. Ensor [38]
	Any combination of two or more data elements, data items, data codes, and data abbreviations in a prescribed sequence to yield meaningful information; for example, "date" consists of data elements year, month, and day.	McGraw-Hill Dictionary [39]

	Definition	Source
(data) Dictionary	The detailed description of data, parameters, variables, and constants used by the system.	RTCA/DO-178C [34]
Data Driven Systems	System which relies upon configuration data or lookup tables to define the functionality of the system.	IEC 61508 Part 4 [40]
Data Intensive System	Systems which make extensive use of large amounts of data.	N. Storey [41]
E		
(data) Error	Discrepancy with the universe of discourse.	ISO 19138:2006 [30]
	Discrepancy between a data value and the true, specified or theoretically correct value or condition.	P. Ensor [38]
Essential Data	Data with an integrity level as defined in Chapter 3, Section 3.2 point 3.2.8(b) of Annex 15 to the Chicago Convention, i.e., integrity level one in one hundred thousand: there is a low probability when using corrupted essential data that the continued safe flight and landing of an aircraft would be severely at risk with the potential for catastrophe.	(EU) No 73/2010 [29]
F		
G		
H		
(data) Hazard	Use of data in the context of a system that could lead to an accident.	SCSC Data Safety Initiative Working Group
Hazard Log	A Hazard Log records all hazard analysis, safety risk assessment and safety risk reduction activities for the “whole-of-life” of a safety-related system.	
I		
Information	Knowledge communicated concerning some particular fact, subject, or event; that of which one is apprised or told - intelligence, news - as contrasted with data.	Oxford English Dictionary (OED)
	Knowledge that has a contextual meaning.	ISO/IEC 2382 [37]
Information (aeronautical)	Information resulting from the assembly, analysis and formatting of aeronautical data.	(EU) No 73/2010 [29]
(data) Integrity	The assurance that a data element retrieved from a storage system has not been corrupted or altered in any ways since the original data entry or latest authorised amendment.	RTCA/DO-200A [31]
	The degree of assurance that a data item and its value have not been lost or altered since the data origination or authorised amendment.	(EU) No 73/2010 [29]
	The degree of undetected (at system level) non-conformity of the input value of the data item with its output value.	(EU) No 1207/2011 [42]
	The property of protecting the accuracy and completeness of assets, i.e., that which has value to the organisation.	ISO27001:2013 [35]
(data) Item	Single attribute of a complete data set, which is allocated a value that defines its current status.	(EU) No 73/2010 [29]
J		
K		

	Definition	Source
L		
M		
Meta-data	Data that represents information about data itself. Note that one should distinguish between "Structural Meta-data", which is data about the design and specification of data structures (and is more properly called "data about the containers of data") and "Descriptive Meta-data", which is about individual instances of application data, the data content.	J. Inge [8]
N		
O		
(data) Origination	Creation of a new data item with its associated value, the modification of the value of an existing data item or the deletion of an existing data item.	(EU) No 73/2010 [29]
P		
(data) Product	Dataset or dataset series that conforms to a data product specification.	BS EN ISO 19131:2008 [43]
Q		
(data) Quality	A degree or level of confidence that the data provided meet the requirements of the user. These requirements include levels of accuracy, resolution, assurance level, traceability, timeliness, completeness, and format.	RTCA/DO-200A [31]
	Process by which the Electronic Chart Systems (ECS) Database is produced, the source materials, the resolution and reproduction accuracy of chart features, and the correctness and completeness of data.	ISO 19379:2003 [44]
	A degree or level of confidence that the data provided meets the requirements of the data user in terms of accuracy, resolution and integrity.	(EU) No 73/2010 [29]
(data) Quality Attributes	Accuracy, resolution, assurance level, traceability, timeliness, completeness and format.	RTCA/DO-200A [31]
R		
Resolution	The smallest difference between two adjacent values that can be represented in a data storage, display or transfer system.	RTCA/DO-200A [31]
	A number of units or digits to which a measured or calculated value is expressed and used.	(EU) No 73/2010 [29]
Routine Data	Data with an integrity level as defined in Chapter 3, Section 3.2 point 3.2.8(b) of Annex 15 to the Chicago Convention, i.e., integrity level one in one thousand: there is a very low probability when using corrupted routine data that the continued safe flight and landing of an aircraft would be severely at risk with the potential for catastrophe.	(EU) No 73/2010 [29]
S		

	Definition	Source
(data) Set	Identifiable collection of data. Note that a dataset may be a smaller grouping of data which, though limited by some constraint such as spatial extent or feature type, is located physically within a larger dataset. Theoretically, a dataset may be as small as a single feature or feature attribute contained within a larger dataset. A hardcopy map or chart may be considered a dataset.	BS EN ISO 19131:2008 [43]
Software Lifecycle Data	Data that is produced during the software lifecycle to plan, direct, explain, define, record, or provide evidence of activities (including the software product itself). This data enables the software lifecycle processes, system or equipment approval and post-approval modification of the software product.	ED-153 [33]
T		
Timeliness	A measure of the time delay between a change in the real world and the associated database update being available to the user.	P. Ensor [38]
	The difference between the time of output of a data item and the time of applicability of that data item.	(EU) No 1207/2011 [42]
Traceability	Ability to determine the origin of the data.	RTCA/DO-200A [31]
Trace (data)	Data providing evidence of traceability of development and verification processes software lifecycle data without implying the production of any particular artifact. Trace data may show linkages, for example, through the use of naming conventions or through the use of references or pointers either embedded in or external to the software lifecycle data.	RTCA/DO-178C [34]
U		
V		
(data) Validation	The activity whereby a data element is checked as having a value that is fully applicable to the identity given to the data element, or a set of data elements that is checked as being acceptable for their purpose.	RTCA/DO-200A [31]
	Process of ensuring that data meets the requirements for the specified application or intended use.	(EU) No 73/2010 [29]
Validity (period of)	Period between the date and time on which aeronautical information is published and the date and time on which the information ceases to be effective.	(EU) No 73/2010 [29]
(data) Verification	Evaluation of the output of an aeronautical data process to ensure correctness and consistency with respect to the inputs and applicable data standards, rules and conventions used in that process.	(EU) No 73/2010 [29]
W		
X		
Y		
Z		

This page is intentionally blank

Appendix P References (Discursive)

> *Data opportunities multiply as the data is transformed.*
> ***Sun Tzu misquoted***

[1] D Banham. Formalising the language of risk. In *Assuring Safe Autonomy, Proceedings of the 28th Safety-Critical Systems Symposium (SSS'20)* [45]. ISBN 9781713305668.

[2] The Safety of Autonomous Systems Working Group [SASWG]. *Safety Assurance Objectives for Autonomous Systems*. Number SCSC-153A. SCSC, January 2020. ISBN 978-1654029050.

[3] R Hawkins, I Habli, and T Kelly. *The Principles of Software Safety Assurance*. Boston, Massachusetts, USA, 2013.

[4] Risk Management — Guidelines. Standard ISO31000:2018, International Standards Organisation, February 2018. Second Edition.

[5] Society of Automotive Engineers. *SAE Aerospace Recommended Practice 4754A: Guidelines for development of civil aircraft and systems*. 2010.

[6] Functional safety of electrical/electronic/ programmable electronic safety-related systems: Software requirements. Standard BS EN 61508-3:2010, International Electrotechnical Commission, June 2010.

[7] Alastair Faulkner and Mark Nicholson. *Data-Centric Safety: Challenges, Approaches, and Incident Investigation*. Elsevier, June 2020. ISBN 978-0128207901. Available from https://www.amazon.co.uk/dp/0128207906?ie=UTF8&n=341677031. Accessed 30 January 2021.

[8] J Inge. *Improving the Analysis of Data in Safety-Related Systems*. September 2008.

[9] Hazard and operability studies (HAZOP studies) — Application guide. Standard IEC 61882:2016, International Electrotechnical Commission, March 2016. ISBN 978-2-8322-3208-8. Second edition.

[10] P Koopman, K Driscoll, and B Hall. *Selection of Cyclic Redundancy Code and Checksum Algorithms to Ensure Critical Data Integrity*. US Department of Transportation, 2015.

[11] *DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems*. NHS Digital, May 2018. Version 4.2.

[12] *DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems*. NHS Digital, May 2018. Version 3.2.

[13] Software Tool Qualification Considerations. Standard RTCA/DO-330, EUROCAE/ED-215, Radio Technical Commission for Aeronautics / European Organisation for Civil Aviation Equipment, January 2012.

[14] Die Lage der IT-Sicherheit in Deutschland 2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf, December 2014. Accessed: 27 January 2021.

[15] D LeBlanc and M Howard. *Writing secure code*. Microsoft Press, December 2002.

[16] *Cyber Security and Safety Code of Practice*. IET, 2020. ISBN 978-1-83953-318-8.

[17] Road vehicles — Safety of the intended functionality. Standard ISO/PAS 21448:2019, International Standards Organisation, 2019.

[18] University of York. Website: Assurance of Machine Learning for use in Autonomous Systems (AMLAS). https://www.york.ac.uk/assuring-autonomy/guidance/amlas/. Accessed: 25 January 2022.

[19] R Ashmore, R Calinescu, and C Paterson. *Assuring the Machine Learning Lifecycle: Desiderata, Methods, and Challenges*. 2019. https://arxiv.org/pdf/1905.04223.pdf. Accessed: 27 January 2021.

[20] D Hond, A White, and H Asgari. Quantifying dataset properties for systematic artificial neural network classifier verification. In *Assuring Safe Autonomy, Proceedings of the 28th Safety-Critical Systems Symposium (SSS'20)* [45]. ISBN 9781713305668.

[21] GS Sutherland and A Hessami. Safety critical integrity assurance in large datasets. In *Assuring Safe Autonomy, Proceedings of the 28th Safety-Critical Systems Symposium (SSS'20)* [45]. ISBN 9781713305668.

[22] David J Hand. *Dark Data: Why What You Don't Know Matters*. Princeton University Press, January 2020. ISBN 069118237X. Available from https://www.amazon.co.uk/dp/069118237X. Accessed: 27 January 2021.

[23] David Hand. Website: Home — Dark Data. https://darkdata.website/. Accessed: 27 January 2021.

[24] SCSC Systems Safety Newsletter. https://scsc.uk/scsc-160, October 2020. vol.28-3. Accessed: 27 January 2021.

[25] David Hand. Presentation on Dark Data given to the DSIWG. https://scsc.uk/file/gd/DARK_DATA_David_Hand_DSIWG_talk-863.pptx, 2020. Accessed: 27 January 2021.

[26] Mike Parsons. Presentation on Dark Data given at the University of York. https://scsc.uk/file/gd/Dark_Data_ABC_Slides_v2-963.pptx, December 2020. Accessed: 27 January 2021.

[27] *Systems and Covid-19, Proceedings of the 29th Safety-Critical Systems Symposium (SSS'21)*, number SCSC-161. SCSC, 2021. ISBN 979-8588665049. Available from https://www.amazon.co.uk/dp/B08RRMSBTN. Accessed 30 January 2021.

[28] Geographic Information. Quality Principles. Standard BS EN ISO 19113:2005, International Standards Organisation, 2005.

[29] Commission Regulation (EU) No 73/2010 of 26 January 2010 laying down requirements on the quality of aeronautical data and aeronautical information for the single European sky. URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:023:0006:0027:EN:PDF, January 2010. Accessed: 27 January 2021.

[30] Geographic Information. Data Quality Measures. Standard ISO/TS 19138:2006, International Standards Organisation, 2006.

[31] Standards for processing aeronautical data. Standard RTCA/DO-200A, EUROCAE/ED-76, Radio Technical Commission for Aeronautics / European Organisation for Civil Aviation Equipment, September 1998.

[32] Commission Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system, as amended. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008R0482&qid=1611781633022, May 2008. Accessed: 27 January 2021, but no longer in force.

[33] Guidelines for ANS software safety assurance. Standard EUROCAE/ED-153, European Organisation for Civil Aviation Equipment, August 2009. Used for definitions only.

[34] Software Considerations in Airborne Systems and Equipment Certification. Standard RTCA/DO-178C, EUROCAE/ED-12C, Radio Technical Commission for Aeronautics / European Organisation for Civil Aviation Equipment, January 2012.

[35] Information Technology — Security Techniques — Information Security Management Systems — Requirements. Standard BS ISO/IEC 27001:2013, International Standards Organisation, 2013.

[36] *DEF(AUST)5679, Issue 2, Safety Engineering for Defence Systems — Standard*. October 2008.

[37] Information Technology. Vocabulary. Part 1: Fundamental terms. Standard ISO/IEC 2382-1:1993, International Standards Organisation, 1993.

[38] P Ensor. *Safety Analysis of Navigational Data*. September 2009.

[39] *McGraw-Hill Dictionary of Scientific and Technical Terms, 6th Edition*. McGraw-Hill, November 2002. ISBN 007042313X.

[40] Functional safety of electrical/electronic/ programmable electronic safety related systems: Definitions and abbreviations. Standard BS EN 61508-4:2010, International Electrotechnical Commission, June 2010.

[41] N Storey and A Faulkner. *The Characteristics of Data in Data-intensive Safety-related Systems*. 2003. 396-409 pp. Lecture Notes in Computer Science, Volume 2788.

[42] Commission Implementing Regulation (EU) No 1207/2011 of 22 November 2011 laying down requirements for the performance and the interoperability of surveillance for the single european sky. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:305:0035:0052:EN:PDF, November 2011. Accessed: 27 January 2021.

[43] Geographic Information. Data Product Specifications. Standard BS EN ISO 19131:2008, International Standards Organisation, 2008.

[44] Ships and Marine Technology. ECS databases. content, Quality, Updating and Testing. Standard BS ISO 19379:2003, International Standards Organisation, 2003.

[45] *Assuring Safe Autonomy, Proceedings of the 28th Safety-Critical Systems Symposium (SSS'20)*, number SCSC-154. SCSC, 2020. ISBN 9781713305668.

This page is intentionally blank

Appendix Q DSIWG History (Discursive)

> *If we have data, let's look at data. If all we have are opinions, let's go with mine.*
> ***Jim Barksdale***

The task of developing generally applicable, pan-sector guidance for data safety issues was taken on by the Data Safety Initiative Working Group (DSIWG) of the Safety-Critical Systems Club (SCSC). The DSIWG's work started with a seminar *"How to Stop Data Causing Harm"*, which was held in December 2012; material from this seminar is available at: (http://scsc.org.uk/e209) (accessed 30 October 2017). The first meeting of the group agreed the following vision:

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

The group, comprising industry, academics, government and independent consultants, produced an initial guidance document in January 2014. A subsequent version of the document was released in January 2015, with a second seminar *"How to Stop Data Causing Harm: What You Need to Know"* held in December 2015; material from this seminar is available at: (http://scsc.org.uk/e343) (accessed 30 October 2017). To help disseminate information, members of the DSIWG have presented papers relating to data safety in a number of fora, including the Safety-critical Systems Symposium (SSS).

Further revisions of the guidance document, which include new material generated during and as a consequence of DSIWG meetings, were issued in January 2016, January 2017 and in January 2018.

The January 2018 release was version 3.0 and the DSIWG decided to keep this version "current" for several years, to enable users to demonstrate compliance against a fixed target. However it was also necessary to keep the document up to date and address user feedback, particularly where this could improve the usability of the document. The next two versions were therefore kept in alignment with version 3.0, with all section numbers in the body of the document remaining constant.

This latest update is version 3.4, the fourth update of the January 2018 version 3.0, and was released in February 2022.

This page is intentionally blank

Appendix R Contributors (Discursive)

> *Without data, you're just another person with an opinion.*
> ***W. Edwards Deming***

This document has had the benefit of contributions from a large number of people, who work for a variety of organisations, which collectively span a range of different sectors. Note that contributions have been made on an individual basis and, in particular, the inclusion of an organisation in the following list does **not** necessarily mean that organisation agrees with the entire contents of the document.

Updates to the most recent version of the document were written by:

- Paul Hampton, CGI IT UK Ltd
- Mike Parsons, AAIP and SCSC
- Oscar Slotosch, Validas AG
- Mark Templeton, Arcade Experts Ltd

Review comments were gratefully received from the following:

- Oscar Slotosch, Validas AG
- Andy Williams

In addition to the above, contributors to earlier versions upon which this document is based include the following (the organisations listed were correct at the time of their contribution) :

- Mike Ainsworth, Ricardo
- Rob Ashmore, Dstl
- Michael Aspaturian, EDF Energy
- Divya Atkins, Mission Critical Applications
- Martin Atkins, Mission Critical Applications
- Janette Baldwin, Thales UK
- Dave Banham, Blackberry QNX
- Ian Bingham
- John Bragg, MBDA UK Ltd
- Jennifer Brain, Wood plc
- Eric Bridgstock
- Simon Brown, QinetiQ
- Dermot Martin Burke, BAE Systems

- Dale Callicott, DKCSC Ltd
- John Carter, General Dynamics
- Martyn Clarke, SCSS Ltd
- Steve Clugston, TSC
- Robin Cook, Thales
- Davin Crowley-Sweet, Highways England
- Dijesh Das, AMEC / BAE Systems
- Duncan Dowling, DARD
- Andrew Eaton
- Ashraf El-Shanawany, CRA Risk Analysis
- Paul Ensor, Boeing
- Alastair Faulkner, Abbeymeade
- Ken Frazer, KAF
- Richard Garrett, SQEP
- Paulo Giuliani
- Ian Glazebrook, Atkins
- Rob Green, NATS
- Nick Hales
- Louise Harney, Leonardo
- Ali Hessami, Vega Systems
- David Higgins
- Gordon Hurwitz, Thales
- Pete Hutchison, RPS
- Gavin Jones
- Amira Kawar, Kawar Engineering Consultancy Ltd
- Tim Kelly
- Andrew Kent
- Brent Kimberley, Durham, Canada
- Julian Lockett, Frazer-Nash Consultancy Ltd
- David Lund, David Lund Consultants
- Dave Lunn, Thales UK
- Nasser Al Malki, University of York

- Victor Malysz, Rolls-Royce
- Jim Mateer, SQEP
- John McDermid, University of York
- Paul McKernan, DSTL
- Thor Myklebust, Sintef
- Mark Nicholson, University of York
- Yvonne Oakshott
- Robert Oates
- David Perrin, Virtual PV
- Ashley Price, Raytheon UK
- Andrew Rankine
- Felix Redmill, SCSC
- Sam Robinson, EDF Energy
- Tim Rowe, EC Harris
- Mark Simmonite, Highways England
- Alan Simpson, Ebeni
- Dave Smith, Frazer-Nash Consultancy Ltd
- Peter Smith, Highways England
- John Spriggs, NATS
- Carolyn Stockton, BAE Systems
- Lesley Winsborrow
- Fan Ye, ESC

This page is intentionally blank

Appendix S Acknowledgements (Discursive)

> *Our ability to do great things with data will make a real difference in every aspect of our lives.*
> ***Jennifer Pahlka***

The document contributors would like to thank:

- The Safety-Critical Systems Club (SCSC).
- The SCSC Covid-19 Working Group for providing some of the data used in the Covid-19 Appendix.
- Brian Jepson of the SCSC for web hosting support and technical help with the SCSC web site.
- Mark Templeton for editing this edition.
- Paul Hampton and Mark Templeton for managing the publication processes.
- Paul Hampton, Mike Parsons, Oscar Slotosch and Mark Templeton for developing the additional text for this edition.
- Martin Atkins and Divya Atkins for driving the development of tooling and obtaining the necessary grant from Lloyds Register Foundation.
- Mike Parsons for chairing the Working Group meetings.
- All those who have taken minutes at Working Group meetings.
- All the organisations that have hosted Working Group meetings.
- All the organisations that have provided support to the document's contributors.
- Those that have been unable to attend meetings but have made supporting contributions.

DATA IS HERE. DATA IS GROWING. DATA IS CAUSING HARM.

The unintended loss and poor presentation of COVID-19 data during the Coronavirus pandemic has shown that data, as distinct from software and hardware, can be a critical contributing factor in many accidents and incidents. The inclusion of data as a potential cause of harm is therefore a crucial part of a thorough system safety assessment.

This book has been developed by the Safety-Critical Systems Club Data Safety Initiative Working Group (DSIWG) to provide guidance on how data, such as COVID-19 data, should be managed in a safety-related context.

This is the 4th minor update since version 3.0 and paragraph numbering within the body of the document remains aligned with that major release. Thus users of any previous 3.x release of the Guidance document will find migration to this edition takes little effort.

This updated document clarifies some sections in response to user feedback, includes a new 'Goldilocks' property, new HAZOP guidewords, clarification of likelihood evaluations, updates on COVID-19 and a new Appendix covering the concept of 'Dazzle' data.

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

SAFER SYSTEMS SAFETY CRITICAL SYSTEMS CLUB 30 YEARS OF

30th SCSC ANNIVERSARY YEAR