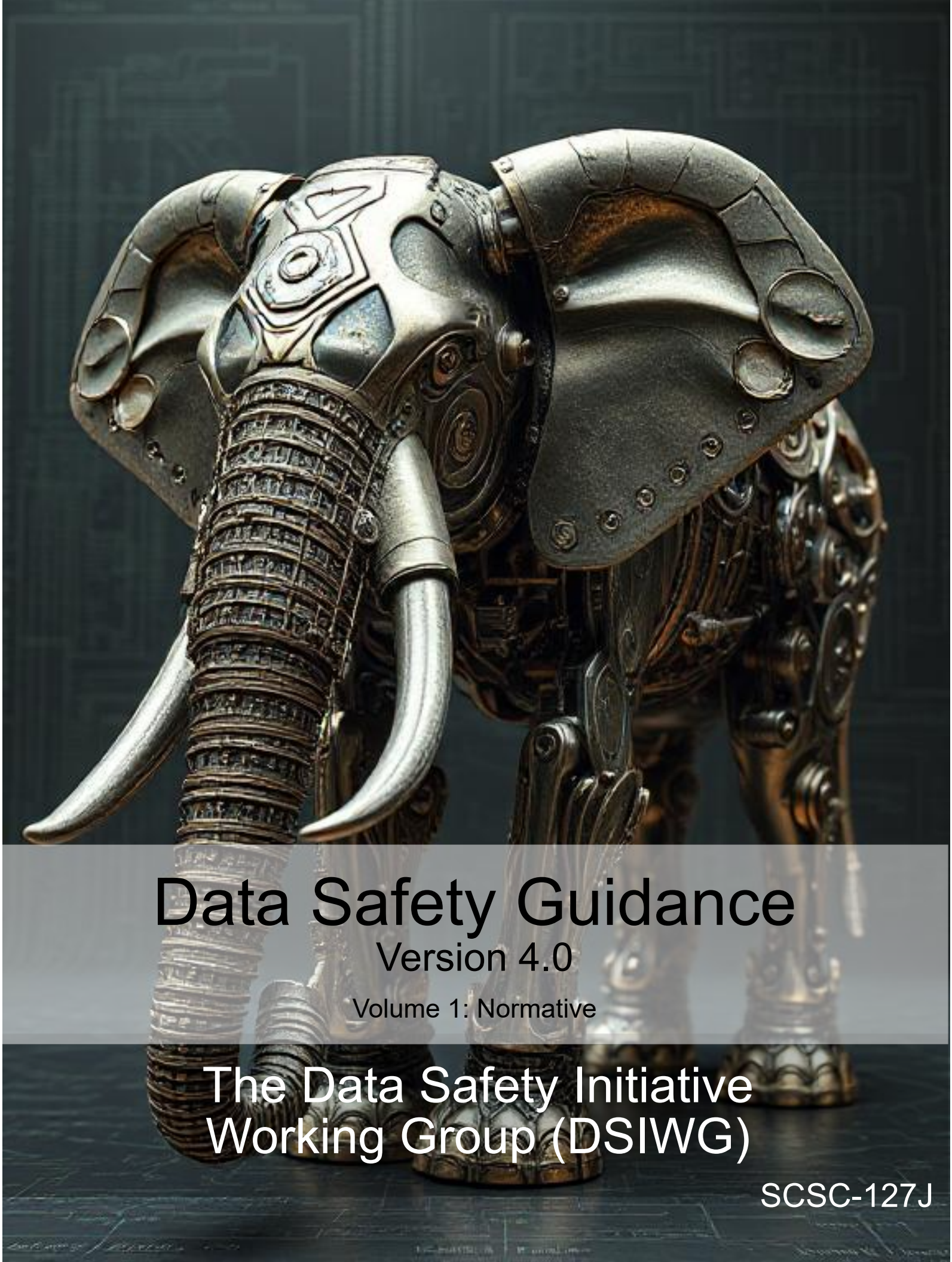

Data Safety Guidance

Version 4.0

Volume 1: Normative

The Data Safety Initiative Working Group (DSIWG)

SCSC-127J

SCSC Publication Number: SCSC-127K

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

Editing and typesetting by Mark Templeton and Tim Rowe.

Front cover design by DeepAI.org and Tim Rowe, based on an original by Paul Hampton. Back cover design by vector_corp on Freepik and Tim Rowe

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'26, 10–12 February 2026, details of which may be found at .

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

comments@data-safety.scsc.uk.

Data Safety Guidance

The Data Safety Initiative Working Group [DSIWG]

February 2026

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
3.5	The DSIWG Team	For publication at SSS'23	07-FEB-2023
3.6	The DSIWG Team	For publication at SSS'24	13-FEB-2024
3.7	The DSIWG Team	For publication at SSS'25	04-FEB-2025
4.0	The DSIWG Team	For publication at SSS'26	10-FEB-2026

Changes Since the Last Edition

This is a major rewrite of the guidance. The document has been split into three volumes, each giving progressively more detail.

The process remains substantially the same. The intention is that conformance with this version does imply conformance with earlier versions , but some material that was informative in earlier versions has been made normative, so conformance with earlier versions of the guidance does not guarantee conformance with this version.

Future work

Proposed future work includes elaboration and expansion of scenarios to enable different routes into this guidance. An appendix of scenarios is included as a starting point at Vol. 2 Appendix A.

MCA Ltd has continued to work 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 organizations that could benefit from the use and further development of the tool are urged to contact MCA at Mission Critical Applications Limited (radish@mca-ltd.com).

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:

- further detail on the assurance of communications and data flows;
- data safety considerations associated with distributed datasets and Blockchain;
- further explanation of some treatments, where their use or benefit is not immediately apparent; and

- further elaboration of issues related to machine learning, large language models (LLMs) and generative artificial intelligence (AI).

Related working groups

Related SCSC working groups include:

- Assurance Cases,
- Security Informed Safety,
- Safe AI Working Group,
- Safer Complex Systems.

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. The use of AI systems is a new, exciting, but potentially hazardous use of data. LLM based systems are trained on data, and it is this data which enables them to be useful. Although machine learning (ML) systems tend to be trained on specifically curated data, these can also be subject to issues such as bias, poisoning and omission.

Some of this data is related to our personal safety and well-being. Consider, for example, the importance of data defining the layout of railway signals, data that indicates the position of underwater obstructions in nautical channels, or data that is used to train a vision recognition system to detect tumours in medical images. Organizations now make significant decisions (including safety-related decisions) based solely on data held in systems. Hence, organizations need to safely manage, control and process their data. In particular, they must actively manage key data properties that preserve safety.

Data is growing: There are many 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 AI, particularly LLMs which are trained on vast amounts of data. A second area is "Big Data". A further area 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.

Data is causing harm: Strictly speaking, data can neither cause nor prevent harm. However, mistakes in data or inappropriate uses 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. Because of this focus, this guidance should help organizations identify, analyse, evaluate and treat data-related risks, thus reducing the likelihood of data-related issues causing harm in the future.

Quick Start Guide

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

This section provides a single-page introduction to data safety guidance (DSG). 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 organizational and system-level risks associated with the use of data.

The guidance is in three volumes, published as separate documents.

Volume 1 (this volume) contains the normative material. It describes the "what" of the guidance and states what is needed to ensure conformance with this guidance, if required. It should be of use to those establishing processes and procedures for data safety assurance and for those doing the actual assurance;

Volume 2 contains the informative material. It describes the "how" of the guidance and should be of particular value to data safety practitioners;

Volume 3 contains the discursive material. It describes the "why" of the guidance and gives background and supporting material intended to improve practitioner's understanding of the data safety management processes and of issues relating to data safety management.

- The data properties that need to be guaranteed to ensure system safety are described in Chapter 2
- The underlying principles of the guidance are described in Chapter 3.
- The objectives and outputs to satisfy the principles are described in Chapter 4.
- Definitions and abbreviations are described in Chapter 5.
- A possible data safety management process is outlined in Vol. 2 Chapter 2
- The activities of each phase (and associated tailoring information) are described in Vol. 2 Chapter 3.
- More detailed guidance is given in Vol. 2 Chapter 4
- A worked example is provided in Vol. 2 Chapter 5.
- Guidance for the assignment of data safety assurance levels (DSALs) is given in Vol. 2 Chapter 6.
- Tool qualification is addressed in Vol. 2 Chapter 7.
- Issues relating to AI and ML are considered in Vol. 2 Chapter 8 and Vol. 2 Chapter 9.
- Additional information on lifecycle data categories is given in Vol. 2 Chapter 10.
- Issues that may arise when migrating, porting, importing or exporting data are discussed in Vol. 2 Chapter 11).
- Rare events are addressed in Vol. 2 Chapter 13.

- The relationship between typical risk-inducing issues and the data properties most likely to be affected are discussed in Vol. 2 Chapter 14
- Various supplemental material is given in appendices to Volume 2.
- Lifecycle considerations are addressed in Vol. 3 Chapter 2.
- The data safety tool RADISH is described in Vol. 3 Chapter 3.
- Some of the data issues that made management of the Covid-19 virus difficult are discussed in Vol. 3 Chapter 4.
- A summary of accidents and incidents in which data was potentially a causal factor is given in Chapter Vol. 3 Chapter 5;

This page is intentionally blank

Contents

List of Tables

1 Introduction

> *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.

It has been written for a wide readership. Its target audience is 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 document is also intended to cover a number of different sectors. It 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.

There are various understandings of the word "safety". Traditionally, these are limited to physical harm to the person: "The state of being protected from or guarded against hurt or injury; freedom from danger" ([1]) or "Freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment." ([2]). However, data safety needs to consider more general harm such as societal harm and indirect harm caused by misinformation and so on. This guidance concentrates on the former but is applicable more widely, and from time to time other types of harm will be considered, particularly but not exclusively in the examples of incidents and accidents (Vol. 3 Chapter 5).

1.2 Structure of the Guidance Documents

The guidance is in three parts, published as separate documents.

Volume 1 contains the normative material. It describes the "what" of the guidance and states what is needed to ensure conformance with this guidance, if required. It should be of use to those establishing processes and procedures for data safety assurance and for those doing the actual assurance work;

Volume 2 contains the informative material. It describes the "how" of the guidance and should be of particular value to data safety practitioners;

Volume 3 contains the discursive material. It describes the "why" of the guidance and gives background and supporting material intended to improve practitioner's understanding of the data safety management processes and of issues relating to data safety management.

1.3 Intended Relationship to Other Documents

This guidance is intended to be used as a supplement to existing standards and norms that are relevant to the scope of the work being undertaken. It may be used to provide a deeper insight into the risks that data poses, to improve coverage of the safety argument. 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 this guidance. The DSIWG also hopes that organizations will include the concepts, approaches and methods in their own safety management processes.

1.4 Normative, Informative and Discursive Text

Three types of text are used within this guidance document:

Normative text, which is prescriptive and can be used for claims of conformance. Typically, this text is restricted to describing methods 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 conformance with the normative text may be achieved, but alternative means of conformance 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 volume of the guidance document contains a single text type.

1.5 Conformance

There may be occasions when it is desirable or necessary to make a claim of conformance to 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 organization's internal processes.

To facilitate conformance claims, the following terminology is used within the Volume 1 of this guidance document. The terms have their normal English meanings volumes 2 and 3.

SHALL denotes items where evidence of conformance must be provided in order to claim conformance with this guidance document.

SHOULD denotes items where, in some circumstances, there may be valid reasons for not conforming to a particular item. The implications of non-conformance must be understood, documented and approved in order to claim conformance with this guidance document.

MAY denotes items that are optional. These may be advantageous in some circumstances but not in others. Organizations are free to adopt any approach to these items without the need for further justification.

2 Data Properties

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

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.

Table 2.1 documents a non-exhaustive collection of data properties. Typically, it is the loss of one of these data properties that presents a hazard. This notion of "loss" is dependent on the intended use; for example, what is "timely" for one use may not be for another.

Table 2.1: 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 authorized 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

Continued on next page

Table 2.1: Properties of data (continued)

Property	Abbreviation	Description
Analysability	Z	The data (including any metadata) is of a suitable size, type and format to enable it be usefully analysed
Explainability	X	The data can be meaningfully explained,by a suitable mechanism, to those who need to understand it
Clarity	K	The data is visible, unmasked, not hidden or obscured and not camouflaged

2.1 Recently Added Properties

2.1.1 The Goldilocks Property

The "Goldilocks" property[1] addresses appropriate sizing and quantity of data. A number of issues have been found to arise when there is too much or too little data. While it is particularly relevant to communications links, it may have relevance to other areas such as databases and 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[2] [3]

The Goldilocks property is related to the data volume problem mentioned in Vol. 2 Chapter 14, however, given the importance of data sizing and the experience of real-world incidents this is now a separate property.

2.1.2 The analysability property

The analysability property recognizes that data is now highly complex and extensive, often large scale, and distributed. And yet, for safety purposes we need to make sure it is of suitable quality and able to support system goals. We therefore need to ensure that it is possible to analyse it for key characteristics and establish meaningful results using tools or other means. This property is related to explainabilty and may be performed by the same set of tools or techniques.

2.1.3 The explainability property

Explainability describes the ability to establish what the purpose and effect data (and especially changes to data) has on a system and explain this to relevant stakeholders in terms that they can understand. It is

[1] The authors are aware that some of the names of categories are very culturally dependent. For example, we are informed that the folk-tale of Goldilocks is not well known in Chinese culture but the idiom guòyóubùjí, interpreted as "doing too much is just as bad as not doing enough" is well known. The intention of the names is simply to evoke the associations, so users of this guidance are encouraged to use names for the categories that are more appropriate to their cultures.

[2] A system where the property was lost involved a high-speed data bus that connected several safety-critical systems. A transceiver 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 data errors. When random noise filled the bus, several apparently valid messages were created every second, resulting in potentially lethal behaviour.

[3] In a hazard and operability study (HAZOP) carried out during 2020, based upon the HAZOP guidewords in this guidance, 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.

particularly important for learning and AI-based systems. This could be, for example, ML training data or system configuration data. This property is related to analysability and may be performed by the same set of tools or techniques.

2.1.4 The clarity property

The clarity property recognises the case where although data might be available it might not be clear to those who need it that it *is* available or where it can be found.

This page is intentionally blank

3 Principles

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

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.

3.1 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, training, 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 the use of the data by a particular system or process, 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.

3.2 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 should demonstrate that the data safety properties are preserved.

3.3 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 should be evidentially demonstrated prior to the system acting on such data, or the system should be able to adequately defend against unsatisfied 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. Sufficient resilience against unknowns, e.g. dark data, needs to be demonstrated.

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

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 features disappearing (due to image scale) when it is critical that situational awareness of such hazards is maintained. The associated objectives and outputs are shown in Table 4.4.

3.5 Principle 5: The confidence established in addressing the data safety assurance principles shall be commensurate to the contribution of the data to system risk

(Called Principle 4+1 by Hawkins.) The confidence in the evidence that demonstrates satisfaction of the first four Data Safety Assurance Principles should be proportionate to the contribution data (or a particular data artefact) makes to the system hazards.

3.6 Principle 6: All principles SHALL be established and maintained through all changes, reuse, re-deployment and re-purposing.

(New.) It is recognised that systems involving data are always subject to change. This could be change to the system or the data involved, or may be a change of use. Data may grow in size, evolve or change in many ways e.g. increased or decreased accuracy from sensor data. A new use of the system could impose different constraints on data properties and require production of new or updated evidence.This means that the applicable principles and objectives, and conformance to them, may have to be reviewed after any change. A process to detect and review changes needs to be in place.

4 Objectives

> *Management by objective works – if you know the objectives. Ninety percent of the time you don't.*
> ***Peter Drucker***

4.1 General

The data safety assurance principles (Chapter 3) provide the underpinning philosophy for this guidance. Conformance to this guidance could be based around these principles. This section identifies the objectives to satisfy the principles.

4.2 Principle 1

***Data safety requirements* SHALL be defined to address the data contribution to system hazards.**

The objectives and outputs supporting this principle are shown in Table 4.1.

Table 4.1: P1 Objectives and Outputs

Id	Objectives	Outputs	Reference
1.a	System context and intended use SHALL be established.	A description of the system and its intended use e.g. in a Concept of Operation (CONOPS). This SHOULD include an estimate of the level of data risks.	Vol. 2 Section 3.1
1.b	Legal and regulatory obligations and requirements SHALL be incorporated.	A record of all applicable laws and regulations.	Vol. 2 Section 3.1
1.c	Applicable standards and relevant guidance SHALL be incorporated	A record of all applicable standards and relevant guidance.	External
1.d	Existing data quality and data assurance requirements and constraints SHALL be identified	A record of applicable existing quality and data assurance requirements and constraints.	External
1.e	Data safety artefacts SHALL be identified	A collection of data artefacts, described at an appropriate level of detail.	Vol. 2 Section 3.1
1.f	Risks SHALL be identified and linked to data safety artefacts	A list of risks, linked to data artefacts and data properties; A description of the process used for risk identification	Vol. 2 Section 3.2
1.g	Data safety activities SHALL be defined and documented	A plan for covering all data safety relevant aspects needs to be created.	Vol. 2 Chapter 3

Continued on next page

Table 4.1: P1 Objectives and Outputs (continued)

Id	Objectives	Outputs	Reference
1.h	Key data stakeholders SHALL be identified	A list of key stakeholders for data safety activities, including those affected by the data.	Vol. 2 Section 3.1
1.i	Missing, hidden, and obscured data SHALL be considered for safety impact	A plan to address potential relevant missing (Dark Data) and obscured data (Dazzle Data).	Vol. 2 Chapter 12
1.j	External interfaces SHALL be defined. This MAY include a list of data owners, linked to data artefacts.	An interface control plan.	External
1.k	A complete list of data assurance requirements SHALL be compiled, based on all the legal and regulatory needs, external inputs, known risks, etc.	A complete list of data assurance requirements.	Vol. 2 Section 3.1
1.l	Relevant historical data-related accidents and incidents SHOULD be reviewed for additional requirements	A documented review of relevant historical data-related accidents and incidents.	Vol. 2 Chapter 4
1.m	DSALs SHALL be established and justified.	A list of DSALs assigned to components and their justifications.	Vol. 2 Chapter 4
1.n	The risk appetite of stakeholders regarding data risks SHALL be established.	The data safety management plan (DSMP)	Vol. 2 Appendix B

4.3 Principle 2

The intent of data safety requirements SHALL be maintained throughout requirements decomposition.

This principle is based on standard systems engineering practices 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 data artefacts MAY be defined at a number of levels of increasing detail. The objectives and outputs supporting this principle are shown in Table 4.2.

Table 4.2: P2 Objectives and Outputs

Id	Objectives	Brief Explanation and Deliverables	Reference in the Guidance
2.a	Levels of abstraction of the data SHALL be defined.	Levels of Abstraction report. This MAY be in diagrammatic form. There MAY be several levels of data abstraction, presenting different relevant perspectives.	Vol. 2 Subsection 4.1.5

Continued on next page

Table 4.2: P2 Objectives and Outputs (continued)

Id	Objectives	Brief Explanation and Deliverables	Reference in the Guidance
2.b	DSALs SHALL be flowed through levels of the design	Traceability records showing the flow of DSALs through the design.	Vol. 2 Appendix B
2.c	Data assurance requirements SHALL be established for each level of system design.	Requirements documents.	Vol. 2 Appendix B
2.d	Data assurance requirements SHALL be traced between each level of system design	Traceability report	Vol. 2 Appendix B
2.e	Data-related interactions between components SHALL be considered.	Interactions report.	Vol. 2 Appendix C
2.f	Data-related interactions with other systems SHALL be considered.	Interactions report.	Vol. 2 Appendix C
2.g	Techniques and approaches for mitigating data risks SHALL be identified	Mitigation report.	Vol. 2 Chapter 4
2.h	Unintended interactions affecting data SHALL be identified.	Interactions report.	Vol. 2 Appendix C
2.i	Techniques and tools used for data analysis SHALL be justified.	Technique and tool justification.	Vol. 2 Chapter 7

4.4 Principle 3

***Data safety requirements* SHALL be satisfied.**

The objectives and outputs supporting this principle are shown in Table 4.3.

Table 4.3: P3 Objectives and Outputs

Id	Objectives	Brief Explanation and Deliverables	Reference in the Guidance
3.a	Methods and techniques used to verify data safety requirements SHALL be documented and justified	A record of the treatment adopted for each of the identified risks	Vol. 2 Chapter 4; Vol. 2 Appendix B
3.b	Data safety requirements SHALL be verified.	Verification reports	Vol. 2 Chapter 4
3.c	Methods and tools used to provide supplemental and supporting assurance SHALL be documented.	A description of the addition processes, methods and tools which provide backing assurance.	Vol. 2 Appendix B
3.d	DSALs SHALL be satisfied.	Conformance to DSALs by reference to the mitigation tables.	Vol. 2 Section 4.4
3.e	Trusted tools SHALL be used to produce verification evidence	Tools used to produce verification evidence should be appropriately qualified and justified.	Vol. 2 Chapter 7

Continued on next page

Table 4.3: P3 Objectives and Outputs (continued)

Id	Objectives	Brief Explanation and Deliverables	Reference in the Guidance
3.f	Verification evidence SHOULD include evidence acquired from field or historical usage where available	Ideally, real-world usage evidence should be used to support verification. The usage scenarios SHOULD accurately reflect the intended usage of the system being verified.	External
3.g	Conformance with data safety requirements SHALL be documented.	Conformance matrix	Normal engineering process
3.h	Data safety requirements which are partially or not met SHALL be identified and justified		Normal engineering process
3.i	Data which is missing or hidden SHALL be assessed for impact.	A missing and hidden data resilience report.	Vol. 2 Chapter 12

4.5 Principle 4

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

The objectives and outputs supporting this principle are shown in Table 4.4.

Table 4.4: P4 Objectives and Outputs

Id	Objectives	Brief Explanation and Deliverables	Reference in the Guidance
4.a	Key properties of the data SHALL be analysed for failures which lead to safety risks.	Data-focussed Functional Failure Analysis.	Vol. 2 Appendix C. Future work to develop this further.
4.b	Unintended behaviour resulting from data SHALL be identified, analysed and addressed.	Unintended Behaviours Report.	Vol. 2 Appendix D and Vol. 2 Appendix C
4.c	Unintended behaviour resulting from hidden or absent data SHALL be identified and analysed.	Unintended Behaviours Report.	Vol. 2 Appendix D and Vol. 2 Chapter 12
4.d	Emergent and unanticipated effects due to data SHALL be investigated.	Unintended Behaviours Report.	Vol. 2 Appendix D and Vol. 2 Appendix C
4.e	Resilience measures to deal with unknowns of the data SHALL be considered.	Unintended Behaviours Report.	Vol. 2 Appendix D and Vol. 2 Appendix C
4.f	Unintended behaviour resulting from malicious data SHALL be identified and analysed.	Unintended Behaviours Report.	Vol. 2 Appendix D and Vol. 2 Appendix C

4.6 Principle 5

The confidence established in addressing the data safety assurance principles SHALL be commensurate to the contribution of data to system risk.

The objectives and outputs supporting this principle are shown in Table 4.5.

Table 4.5: P5 Objectives and Outputs

Id	Objectives	Brief Explanation and Deliverables	Reference in the Guidance
5.a	DSALs SHALL be appropriately applied.	The application and conformance to DSALs needs to be appropriate for the level of risk presented by the system.	Vol. 2 Chapter 3 and Vol. 2 Section 4.4
5.b	Assurance artefacts SHALL be produced with a level of rigour commensurate with the DSAL and data safety requirements.	Artefacts used to demonstrate the safety of the system need to be produced in an appropriate way for the system risk.	Vol. 2 Chapter 3 and Vol. 2 Section 4.4
5.c	Activities, methods, analyses, and tools used to provide assurance SHALL be appropriate for the DSAL and stakeholder group.	This is addressed in the safety management plan (SMP).	Vol. 2 Appendix B and Vol. 2 Chapter 7
5.d	Specific confidence demands from stakeholder groups regarding data SHALL be addressed.	This is addressed in the SMP	Vol. 2 Appendix B
5.e	Residual risks regarding conformance to the data safety principles SHALL be documented.	Residual conformance risks would typically be recorded in an overall system safety justification document such as a safety case.	External

4.7 Principle 6

All principles SHALL be established and maintained through all changes, reuse, re-deployment and re-purposing.

The objectives and outputs supporting this principle are shown in Table 4.6.

Table 4.6: P6 Objectives and Outputs

Id	Objectives	Brief Explanation and Deliverables	Reference in the Guidance
6.a	All changes that impact these principles and objectives SHALL be assessed and managed.	The DSMP continues to apply through system life.	Vol. 2 Appendix B
6.b	Assurance artefacts SHALL be maintained.	The DSMP continues to apply through system life.	Vol. 2 Appendix B
6.c	Measures SHALL be in place to monitor the behaviour of the SCS at appropriate intervals throughout its life.	The DSMP continues to apply through system life.	Vol. 2 Appendix B

Continued on next page

Table 4.6: P6 Objectives and Outputs (continued)

Id	Objectives	Brief Explanation and Deliverables	Reference in the Guidance
6.d	Use SHALL be monitored for change and an assurance impact analysis undertaken where necessary.	The DSMP continues to apply through system life.	Vol. 2 Appendix B
6.e	Evolution and incremental change SHALL be considered.	The DSMP continues to apply through system life.	Vol. 2 Appendix B
6.f	Longevity and obsolescence of data SCS SHALL be considered.	The DSMP continues to apply through system life.	Vol. 2 Appendix B
6.g	Lessons learned from successful operation, failures and incidents SHOULD be reviewed	The DSMP continues to apply through system life.	Vol. 2 Appendix B

5 Definitions

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

artefact, data

An item, or collection of items, that provides a useful perspective on data generated, processed or consumed by a system.

property, data

A characteristic that can be exhibited by a data artefact.

safety assurance level, data

An indication of the level of rigour with which relevant data properties should be demonstrated for appropriate data artefacts.

safety requirement, data

A requirement to implement an approach specifically designed to achieve, maintain or demonstrate a data property (or data properties) for a given data artefacts (or Artefacts).

stakeholder

An individual or organization that has some relationship to the system, possibly including a power of veto.

treatment

An action taken to reduce or control risk. This might be mitigation of the risk or elimination of the hazard.

This page is intentionally blank

6 Acronyms, Definitions and Glossary

> *The plural of anecdote is not data.*
> ***Mark Berkoff***

6.1 Acronyms

AI	artificial intelligence
CONOPS	Concept of Operation
DSAL	data safety assurance level
DSG	data safety guidance
DSIWG	Data Safety Initiative Working Group
HAZOP	hazard and operability study
LLM	large language model
ML	machine learning
OED	Oxford English Dictionary
SCSC	Safety-Critical Systems Club
SSS	Safety Critical Systems Symposium

6.2 Definitions and Glossary

accessibility

Property that the data is visible only to those that should see it.

accuracy

Closeness of agreement between a measured quantity value and a true quantity value of a measurand. [4]

analysability

The data (including any metadata) is of a suitable size, type and format to enable it be usefully analysed

artefact, data

An item, or collection of items, that provides a useful perspective on data generated, processed or consumed by a system.

availability

The property of being accessible and usable upon demand by an authorized entity. ISO 27001:2013 [5]

clarity

The property that the data is visible, unmasked, not hidden or obscured, and not camouflaged

completeness

- Property of having every necessary part or element.
- Completeness of the data provided. RTCA/DO-200A

configuration data

- Data that configures a generic software system to a particular instance of its use. (EC) No 482/2008 [6]
- 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 [7]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 [7]

consistency, data

The property that the data adheres to a common world view (e.g., units).

continuity, data

The property that the data is continuous and regular without gaps or breaks.

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 [8]

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

dataset

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 [9]

disposability / deletability

The property that the data can be permanently removed when required

error, data

- Discrepancy with the universe of discourse. ISO 19138:2006 [10]
- Discrepancy between a data value and the true, specified or theoretically correct value or condition. P. Ensor [11]

explainability

The property that the data can be meaningfully explained, by a suitable mechanism, to those who need to understand it.

fidelity / representation ,data

The property describing how well the data maps to the real world entity it is trying to model.

format

The property that data is represented in a way which is readable by those that need to use it.

Goldilocks

The property that the data is just the right size – not to much and not too little

hazard, data

> Use of data (in the context of a system) that could lead to harm. SCSC DSIWG

history

Property that the data has an audit trail of changes.

information

- Knowledge communicated concerning some particular fact, subject, or event; that of which one is apprised or told - intelligence, news - as contrasted with data. OED
- Knowledge that has a contextual meaning. ISO/IEC 2382 [8]

integrity, data

- 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 [12]
- 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 [13]
- 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 [14]
- The property of protecting the accuracy and completeness of assets, i.e., that which has value to the organization. ISO 27001:2013 [5]

intended destination / usage

Property that the data is only sent to those that should have access to it

lifetime

The property of when the safety-related data expire

metadata

Data that represents information about data itself. Note that one should distinguish between "Structural Metadata", which is data about the design and specification of data structures (and is more properly called "data about the containers of data") and "Descriptive Metadata", which is about individual instances of application data, the data content. J. Inge [15]

mitigation

Steps taken to control or prevent a hazard from causing harm and reduce risk to a tolerable or acceptable level. [16]

owner, data

The individual or organization responsible for a particular data artefact or collection of data artefacts.

priority

The property that data is presented / transmitted / made available in the order required.

property, data

A characteristic that can be exhibited by a data artefact.

resolution

- The ability of a device to respond to small differences in input and to indicate or represent them accurately in output; a measure of this, expressed as the smallest difference so distinguishable. OED.
- The smallest difference between two adjacent values that can be represented in a data storage, display or transfer system. RTCA/DO-200A [12]
- The number of units or digits to which a measured or calculated value is expressed and used. (EU) No 73/2010 [13]

response

The way in which an identified risk is addressed; possible responses include avoid / eliminate, treat, or accept as sufficiently low.

safety

- The state of being protected from or guarded against hurt or injury; freedom from danger. OED
- Freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. [2]

safety assessment, data

The process of explicitly considering data as part of a system safety assessment, via the means of data artefacts, Data Properties and DSALs.

safety assurance level, data

An indication of the level of rigour with which relevant data properties should be demonstrated for appropriate data artefacts.

safety requirement, data

A requirement to implement an approach specifically designed to achieve, maintain or demonstrate a data property (or data properties) for a given data artefacts (or Artefacts).

sequencing

The property that the data is preserved in the order required.

stakeholder

An individual or organization that has some relationship to the system, possibly including a power of veto.

suppression

Property that the data is intended never to be used again

tailoring

Adaptation of processes etc. to be appropriate for a specific system and context

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 [11]
- The difference between the time of output of a data item and the time of applicability of that data item. (EU) No 1207/2011 [14]

traceability

Ability to determine the origin of the data. RTCA/DO-200A [12]

treatment

An action taken to reduce or control risk.

validation, data

- 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 [12]
- Process of ensuring that data meets the requirements for the specified application or intended use. (EU) No 73/2010 [13]

verifiability

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 [13]

verification, data

Evaluation of the output of a process to ensure correctness and consistency with respect to the inputs and applicable data standards, rules and conventions used in that process. Based on (EU) No 73/2010 [13]

The normative list of definitions is at chapter 5. Normative definitions have been repeated here for convenience.

This page is intentionally blank

7 References

> *Data opportunities multiply as the data is transformed.*
> ***Sun Tzu misquoted***

Bibliography

[1] Safety, n., i.1.a. In *OED Online*. Oxford University Press.

[2] System safety. standard Mil-Std-882E, Department of Defense, 2012.

[3] R Hawkins, I Habli, and T Kelly. *The Principles of Software Safety Assurance*. International System Safety Society, Boston, Massachusetts, USA, 2013.

[4] ISO/IEC. Information technology — data governance — data collaboration framework. https://www.iso.org/obp/ui#iso:std:iso-iec:25642:ed-1:v1:en:term:3.9. Accessed: 2 October 2025.

[5] Information Technology — Security Techniques — Information Security Management Systems — Requirements. Standard BS ISO/IEC 27001:2013, International Standards Organisation, 2013.

[6] Commission Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system, as amended. URL 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.

[7] Guidelines for ANS software safety assurance. Standard EUROCAE/ED-153, European Organisation for Civil Aviation Equipment, August 2009. Used for definitions only.

[8] Information Technology. Vocabulary. Part 1: Fundamental terms. Standard ISO/IEC 2382-1:1993, International Standards Organisation, 1993.

[9] Geographic Information. Data Product Specifications. Standard BS EN ISO 19131:2008, International Standards Organisation, 2008.

[10] Geographic Information. Data Quality Measures. Standard ISO/TS 19138:2006, International Standards Organisation, 2006.

[11] P Ensor. *Safety Analysis of Navigational Data*. University of York, September 2009.

[12] 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.

[13] 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.

[14] 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. URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:305:0035:0052:EN:PDF, November 2011. Accessed: 27 January 2021.

[15] J Inge. *Improving the Analysis of Data in Safety-Related Systems*. University of York, September 2008.

[16] Use of safety management systems by ATM service providers. Standard ESARR3, EUROCONTROL, 2011.

This page is intentionally blank

Index

Data is here. Data is Growing. Data is Causing Harm

This guidance has been developed by the Safety-Critical Systems Club Data Safety Initiative Working Group (DSIWG) to assist with the management of data, as distinct from hardware and software, in a safety-related context.

"If you torture the data long enough, they confess – even to crimes that were never committed.

Nihat Bülent Gültekin

This is a major rewrite of the version 3 guidance, to improve the structure, clarify the workflow, improve the consistency of the normative content and to move much of the appendix material of version 3 into the body of the text. Although the fundamental process has not changed, conformance to previous versions does not guarantee conformance to this version.

SCSC

For Everyone Working in System Safety