Version 3.1 [SCSC-156C]

Service Assurance Guidance

by the SCSC Service Assurance Working Group [SAWG]

Published by the Safety-Critical Systems Club

SCSC Publication Number: SCSC-156C

ISBN: 9798785666429
Download at: scsc.uk/scsc-156C

Cover design by Alex King

Service Assurance Guidance

By the SCSC Service Assurance Working Group

Version 3.1, January 2023
SCSC-156C

This document is intended to provide guidance for the assurance of services in a safety context.
It was produced by the SCSC Service Assurance Working Group (SAWG), 2017-2023.

Comments or suggestions on this document should be sent to: sawg-comments@scsc.uk

What This Book is About

This book provides guidance on the assurance of services when there are safety implications of those services. Tangible examples of such services are air traffic control, a maritime satellite service handling emergency distress calls or an ambulance dispatch service. A set of principles for assuring services is given; guidance is then provided on how to apply the principles through objectives and how to address the challenges that may be encountered. Mitigation methods and techniques to address the specific risks of service situations are covered. Analyses are outlined for identifying undesired behaviours of services. The role of service assurance requirements is explained through the service definition, service architecture and the agreements made at service interfaces, often using Service Level Agreements (SLAs). The approach draws upon concepts from modular assurance and illustrates the use of supplementary assurance ('wrappers') to manage the variety of assurance positions presented by services.

Change History

Version	Brief Description	Date
1.0	First Version for SSS'20	February 2020
1.1	Relationship with BS EN 17371 Annex	December 2020
1.2	Covid-19 intro	January 2021
1.3	Various edits and updates	January 2021
2.0	Version for SSS'21	February 2021
2.1	Update to Service Analysis Techniques	September 2021
3.0	Version for SSS'22 download and hardcopy	January 2022
3.1	Version for SSS'23 download	January 2023

Foreword

"As far as service goes, it can take the form of a million things. To do service, you don't have to be a doctor working in the slums for free, or become a social worker. Your position in life and what you do doesn't matter as much as how you do what you do.."

Elisabeth Kubler-Ross

Rationale

Why is this guidance needed? It is now clear that many safety-related systems are now used in a service context, and this context is important to ensure safety. In particular:

- The collaborative working of systems, organisations, agreements, people and processes all contribute to the safety of the service.
- A service approach recognises the flexibility and encapsulation of services, and the time-limited nature of service contracts.
- A service-based approach is used in many areas of technology and commerce, for example in highways, healthcare and information technology.
- A service-based approach to assuring safety provides a different, useful and important perspective to that of more traditional systems-focussed approaches.

Services Business Context and Motivation

The case for using commercial services to construct a business solution is very compelling:

- Architects can easily develop safety-related capabilities using a Service Based Solution (SBS) building on existing solutions.
- Specialist and off-the-shelf services (e.g. cloud computing) have reached high levels of maturity. They are:
    a. Highly available and are resilient.
    b. Have rich and sophisticated functionality.
    c. Cheap, with the economies of scale and competition giving lower costs than in-house implementations.
    d. Dynamic, and have growing capabilities.
- The trend is set to continue and accelerate as these services expand and mature.
- Organisations are increasingly using the paradigms of Services and Service Oriented Architectures (SOA) to deliver their aims.
- Organisations can focus on the provision of in-house and customer-facing services. They buy-in generic, "commodity" services and so off-load the complexity, expertise and non-safety risk associated with providing those services to their suppliers via commercial relationships.

- This approach is generic, and the use of services can work in many different sectors, e.g. from hospital cleaning to train fleet maintenance.
- The SOA approach can be applied to many of the services that support an enterprise such as Facilities Management and Physical Security as well as Information Technology (IT) services such as Web Services, Cloud Computing, Cyber-Security and Network Services.
- Robust Cyber-Security is a particularly good example as it requires a very high level of sophistication and knowledge. Individual enterprises are increasingly unable to maintain the level of expertise in-house needed for effective protection, and so buy-in Cyber-Security services from expert providers.

This Document

This document provides guidance on the assurance of services when there are safety implications associated with the use of those services. These services we call 'Safety-Related Services'; typical examples might be an ambulance dispatch service or an air traffic control service.

This guidance is aimed at services that are genuinely safety-related. Excluded services, which are considered critical, but not safety-related, include services such as banking and public broadcasting.

A set of principles for assuring services (as opposed to systems) is proposed. The guidance explains how they may be applied in a service provision situation. These principles are domain agnostic and can be used across a wide range of service scenarios in diverse sectors.

Further guidance is provided on how to apply the principles through objectives and how to address the challenges that may be encountered.

Methods and techniques applicable to service situations are covered. Analyses are listed for identifying undesired behaviour where assurance is required.

Of particular significance is how to show that the intent of the service assurance requirements is maintained through the service definition, service architecture and the agreements made at service interfaces, e.g. through Service Level Agreements (SLAs), and that the principles are preserved through change.

The approach described in this guidance draws upon concepts from modular assurance and illustrates the different types of supplementary assurance (a "wrapper") that can be used to manage the variety of assurance positions presented by services.

The principles are linked to objectives and characteristics to show how high-level requirements can be established for assured services.

Quick Start Guide

"Profit in business comes from repeat customers, customers that boast about your project or service, and that bring friends with them.."

W. Edwards Deming

The main sections of the document are as follows:

1. Introduction

   This section provides rationale, i.e. why are services in a safety context a problem now (industry trends, etc.). It covers background aims and scope, and also the target audience. The overall approach is that this document is positioned as guidance; it may be used for developing (domain-specific) standards and further guidance for services. It discusses views of what a service is and what service characteristics are. It also introduces service terms used in this document.

2. Assurance of Services

   This section begins by introducing some of the challenges of assuring services, as a way to describe what is different about services (as opposed to systems) from an assurance view. It introduces further concepts and terms relevant to assurance of services. Finally, it lists some basic assumptions used in the document.

3. Service Assurance Principles

   This key part of the document states the six Service Assurance Principles, including brief supporting descriptions and explanations. It then defines objectives which support each principle; these are seen as a route of demonstrably meeting the principles. This section also includes a mapping of the principles to service characteristics.

4. Levels of Service Assurance

   The concept of Levels of Service Assurance (LSA) is introduced in this section. The levels are then used to scope the applicability of objectives, so tailoring what is required for each level of service risk.

5. Capturing justifications and evidence

   This section provides evidence tables covering aspects of service scoping, design, analysis, implementation and change. These tables suggest evidence techniques and containers for meeting the objectives. The concept of Assurance Wrappers is introduced and explained. Some further service assurance challenges and some solutions are discussed.

6. Analysis Techniques

   A brief discussion of a range of possible assurance techniques is given in this section with an indication of the perspective they provide, i.e., it examines the inner workings or structures of the service being analysed or it provides benefit by analysing the functionality of a service. There are also examples of the implementation of the techniques and details of the perceived benefits and disadvantages.

Supporting sections (Informative / Discursive)

7. Service 'Mode' Changes

   Services can evolve over time to account for increased or reduced demand or to account for a re-evaluation of the customer's use of the service. This section discusses how such service 'mode' changes should or can be managed in an assured way.

8. What Happens when Services Go Wrong?

   This discussion section covers the topic of degraded or contingent services, covering what typically happens to a service in fault conditions, and how to maintain an assurance position.

9. Services Across Boundaries

   Services often do not lie cleanly within a single boundary (e.g. geography, time zone) and span many boundaries. This section discusses some of the issues which arise when parts of a service are implemented across boundaries.

10. Further work

    Topics raised in SAWG meetings for future consideration are listed in this section.

Annex A: Provides a suggested set of Hazop-style guidewords for services.

Annex B: Gives a set of service-related Incidents and Accidents as identified from publicly available sources.

Annex C: Outlines a stepwise methodology for applying this guidance document, referencing an example

Annex D: Gives a brief overview of the relationship between this guidance and the emerging BS 17371: Provision of Services

Annex E: Discusses the service requirements from other standards and guidance.

Annex F: Provides a brief description of Service Blueprints and their Relevance

Annex G: Provides Terms and Acronyms.

Annex H: Gives the references used in this document.

Annex I: STPA Example for Highways Services

Annex J: Lists the contributors to this document.

Annex K: Presents the acknowledgements.

Table of Contents

Figures

Tables

This page is intentionally blank

1 Introduction (Informative)

"The best way to find yourself is to lose yourself in the service of others."

Mahatma Gandhi

Many current safety-critical and safety-related systems rely on functionality provided by services which are designed, developed, operated, and maintained outside the immediate boundaries of the system. In many cases, overall system design is essentially about managing the interactions between various service functionalities, which co-operate to enact some operational scenario. In this context, the term 'System of Systems' is actually 'System of Systems and Services'. Future developments in business and technology are likely to mean that this service paradigm will become increasingly prevalent in the next generation of safety-critical and safety-related technologies.

Examples of safety-related systems where a service-oriented approach might be used include the provision of data to support operations, such as aeronautical or defence systems, or the provision of commercial IT facilities for hosting, informing, or supporting end-user applications. A service-oriented view of safety may be able to identify and manage safety risks more effectively in many scenarios since it highlights the collaboration of various elements of the socio-technical situation (people, organisations, processes, maintenance, change, contracts and agreements, support and through-life aspects) and their contributions to the overall safety of the operation.

This service paradigm presents considerable challenges for safety engineering and assurance for a variety of technical and non-technical reasons, often extending beyond the traditional concerns of system safety engineering (e.g. into the realm of commercial contracts, service-level agreements and cross-organisational concerns).

This guidance – which has been produced by members of the SCSC Service Assurance Working Group (SAWG) from 2017-2023 – aims to characterize the challenges presented for safety assurance of services and proposes a process for the management of service safety.

The Working Group comprises members from a variety of safety-critical and safety-related industries, including safety consultancies and from academia, and the guidance offered is intended to be applicable to all domains.

1.1 Disclaimer

While the authors and the publishers have used reasonable endeavours to ensure that the information and guidance given in this work is correct, all parties must rely on their own skill and judgement when making use of this work and obtain professional or specialist advice before taking, or refraining from, any action based on the content of this work. Neither the authors nor the publishers make any representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to such information and guidance for any purpose, and they will not be liable for any loss or damage including without limitation, indirect or consequential

loss or damage, or any loss or damage whatsoever (including as a result of negligence) arising out of, or in connection with, the use of this work. The views and opinions expressed in this publication are those of the authors and do not necessarily reflect those of their employers, the SCSC or other organisations.

1.2 Intended Audience

It is anticipated that this guidance will be of interest to all those involved in the procurement, provision, through-life management, and assurance of service-dependent systems in a safety context. Potential interest groups include:

Service Providers – those who design, supply, manage, operate, and maintain services on which safety-critical and safety-related systems rely.

Service Buyers - those responsible for specification or procurement of services.

Service Integrators – those responsible for complete safety-critical and safety-related systems which rely on services for some aspect of their functionality.

Service Designers/Architects - those responsible for the design of services, and their interfaces to client systems.

Service Consumers (Service Users/Customers) – those who make use of or otherwise benefit from the safety-critical and safety-related services.

Sub-contractors and Suppliers – from the services perspective, sub-contractors may be a source of requirements on the service, or on its interfaces, or may provide particular functionality supporting the service.

Regulators – those responsible for approving safety-critical and safety-related systems or services for deployment for a defined purpose in a defined operational context.

Incident/Accident Investigators – those responsible for analysing incidents and accidents involving safety-critical and safety-related systems or services, for drawing conclusions about causation and blame and for recording lessons learnt.

Service Assurers - those who are required to make an assurance position for the service.

Support and Service Desk Staff – those at 'sharp-end' of receiving problem reports and progressing fixes in an operational environment.

The Guidance at present is aimed at Service Providers, Service Assurers and Service Designers/Architects. It will be expanded in future to cover the other stakeholders.

1.3 Services

The term "Service" is much overloaded, its definition is much discussed. This section does not aim to provide a precise and constraining definition. Several standard definitions are presented, but more importantly, the section identifies characteristics of a service that may make the Service-Based

approach to safety assurance appropriate. Most safety standards do not provide a definition of service. Some common definitions are:

> *"**Services** are a means of delivering value to customers by facilitating the outcomes customers want to achieve **without the ownership of specific costs and risks**". **ITIL V3 2011***
>
> *"A **Service** is delivered by a combination of people, processes, products and partners." **ITIL V3 2011***
>
> *"A **Service** is a discrete unit of functionality that can be accessed remotely and acted upon independently." **Service Oriented Architecture concept***
>
> *"**Service**: a vehicle by which a consumer's need or want is satisfied according to a negotiated contract (implied or explicit) which includes Service Level Agreement, function offered, warranties, assurance or certification, etc." **Component-based Development and Integration (CBDI) concept***
>
> *"**Service**: The operation or usage of a system in a defined operating environment to achieve a specific purpose or purposes. A service can be any activity using a system, e.g. maintaining/updating military vehicles." **DEF STAN 00-056 (PART 1) issue 7***
>
> ***"Service:** intangible output and result of a process that includes at least one activity that is carried out at the interface between the supplier (provider) and the customer.*
>
> *Note 1 to entry: Service provision can take many forms. Service can be provided to support an organization's own products (e.g., warranty service or the serving of meals).*
>
> *Note 2 to entry: Conversely, a service can be provided for a product supplied by a customer (e.g. a repair service or a delivery service).*
>
> *Note 3 to entry: Service can also involve the provision of an intangible thing to a customer (e.g. entertainment, ambience, transportation, or advice)." **ISO 9000:2015***

1.4 Defining a Service

The way that a Service is normally described or defined is different from the specifications and descriptions more commonly used in safety-related systems. An individual Service (or Service Component) is typically described by the Service Provider via an entry in a Service Catalogue. The Service Catalogue usually describes the capabilities/functionality offered to a Consumer without providing much (or indeed any) implementation detail, in fact it is unusual for the design and implementation of the Service to be visible to the Consumer.

Service Level Agreements (SLA) are used to define the level of service being offered, this may include non-functional properties such as capacity, performance, and availability. SLAs often describe (commercial) penalties on the Service Provider for not meeting key elements of the agreements.

Service Contracts between the Provider and Consumer provide the overriding legal and commercial picture and typically refer to Service Catalogues, Statements of Work (SoW) and SLAs.

The boundary between a Service Consumer and a Service Provider is typically both an organisational and commercial boundary as well as a technical one. A Consumer may not be involved in the specification and development of a Service and instead may select a standardised Service (i.e.

something already available). Alternatively, they may be involved in the creation of new, tailored, or bespoke services.

1.5 Service Context and Service-Oriented Architecture

The following section introduces some key terms. Figure 1 gives the context:

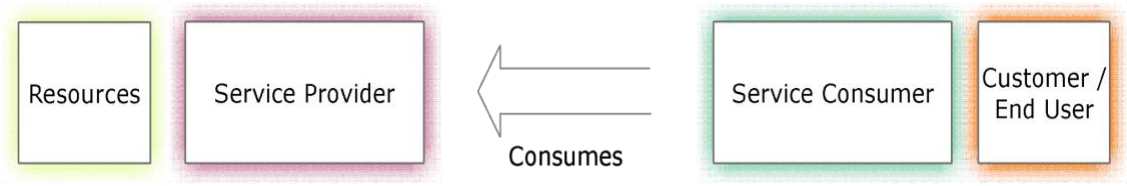


Figure 1 - Context of Service Providers and Consumers

Service Provider - provides one or more Services.

Service Consumer - consumes one or more Services.

Customer Facing Service - provides services facing directly to Customers, e.g. web service, warship maintenance, General Practice (GP) service, etc.

Resource Facing Service - delivers services consumed by other Services, e.g. electrical power, network services, X-Ray service, etc.

Service Definition - describes the Services available for consumption which may include technical and/or commercial aspects. It may include deliverables, prices, contact points, availability, ordering and processes to request Services. This may include a service catalogue.

Service Level Agreement (SLA) - the agreement between the Service Provider and Consumer that defines the level of service that the Consumer will receive. It usually specifies responsibilities of both parties and defines the penalties in the event the specific targets in the SLA are not met.

Service Contract - The contractual agreement between Service Provider and Service Consumer. Note that the Service Consumer may not be involved in defining the service or the SLAs at the outset; they may be provided pre-defined and pre-packaged by the Service Provider on a take-it-or-leave-it basis (see Figure 2).

A **Service Based Solution (SBS)** comprises the systems, organisations, processes and resources to deliver and manage the services through life. It may consume other services. An **SBS** delivers capabilities to its customers via a set of collaborating services.

A **Well-Formed SBS** has a hierarchy of services with specialised, domain-specific **Customer Facing Services** constructed from generic, reusable **Resource Facing Services** (see Figure 3).

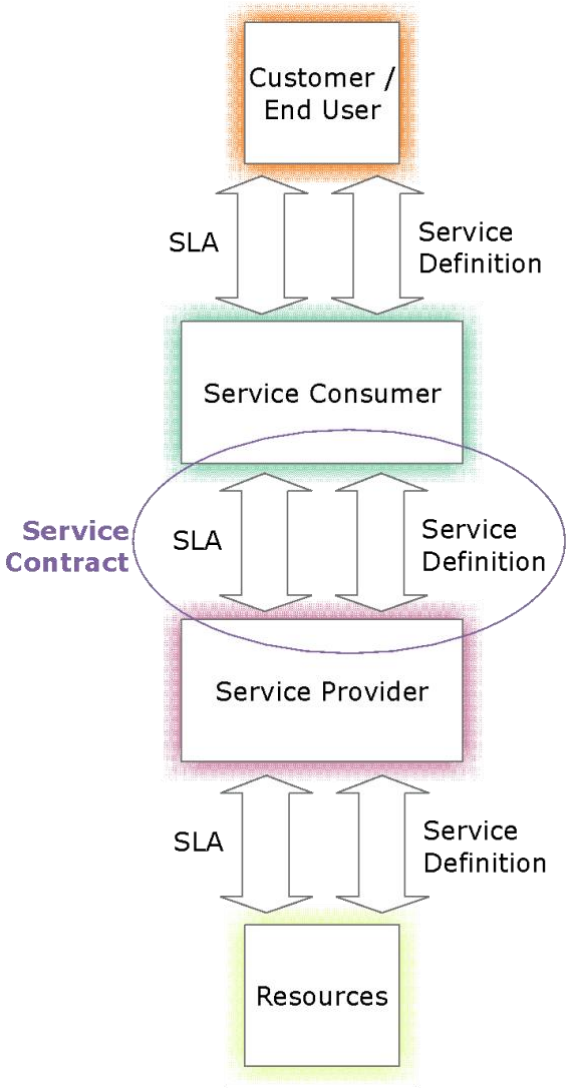


Figure 2 - Context of Service Contract

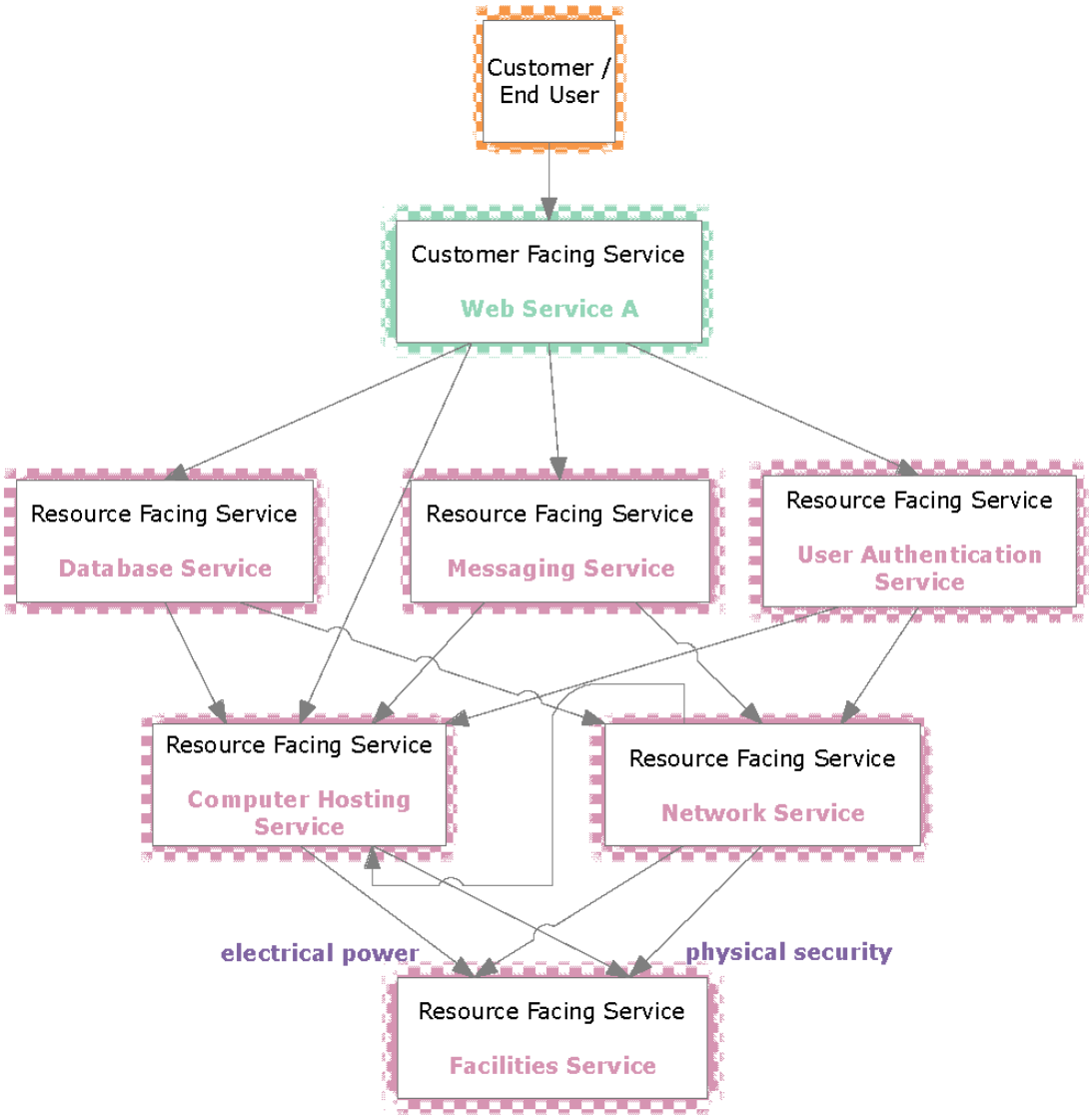


Figure 3 - Example Service Architecture Showing Customer and Resource Facing Services (arrows indicate service consumption)

1.6 Service Hierarchy and Decomposition

A key characteristic of the SBS approach is the flow-down of requirements and targets to services at different layers in the hierarchy.

Figure 4 represents a simplification of a service hierarchy. Not all organisations providing safety services in a service 'stack' will be willing or able to take part in safety activities. Note there is a distinction between service providers that have 'visibility' of the top-level (safety) risk and those, lower-down, that would have little or no visibility of system safety. These latter providers would only demonstrate that their service satisfied its specification. They would not necessarily receive, nor understand 'traditional' safety requirements; instead, what might be termed 'confidence demands' flow down, defining the rigour of the evidence needed. In many domains, this awareness is the result of the visibility of data relating to risk through the system hierarchy: such visibility is likely to be governed by contractual relationships, as well as by business expectations.

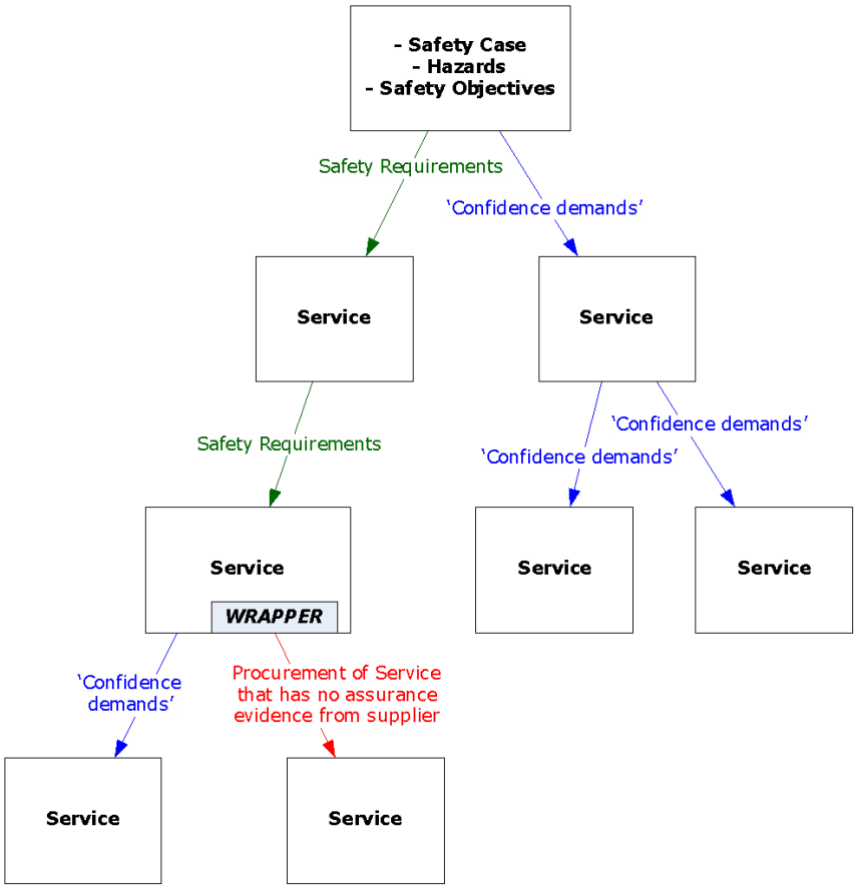


Figure 4 - Example Service Stack

This hierarchical flow down includes several aspects which need to be considered for safety assurance:

- The capability and willingness of Service Providers to engage with the safety assurance process, e.g. accepting safety requirements.
- Determining when an SLA approach rather than apportioning of safety requirements is appropriate.
- Analysis of SLAs to identify how a Service may relate to safety concerns.
- Establishing the level of confidence needed in a specific SLA and its targets.

The risks that arise from the services within the SBS need to be identified and managed. A lack of visibility of how services are delivered may challenge the way that failures are identified and impacts from changes are analysed. The risk of known hazards (and any emergent properties that may end up being hazardous) may be increased by using independent collaborating services with limited view of implementation and little visibility of the end-use.

1.7 Responsibilities

Ultimately it is the service consumer who must convince him/herself that the services being consumed are safe enough. However, some of this responsibility may be partly met by other parties, including the service providers. The questions to be answered are:

1. who is the individual or corporate/government body who is responsible for the service in question (i.e. the "Provider")?

2. who should sign the assurance case? And

3. who should be liable for any safety consequences?

Where users or consumers encounter risks through misuse or ignorance the provider should aim to identify the potential risks from misuse and explicitly provide consumer information, warnings or caveats. Some very unlikely circumstances may not be identified by the provider, and so the consumer must always be partly involved.

We can refine our 'knowing' and 'unknowing' service providers into several groups, where understanding and willingness to engage in safety activities are the distinguishing features. These are detailed in section 5.3.2.

1.8 Characteristics of Services

The term Service is widely used and as discussed has numerous variations in definition, scope and intent. It is considered more important to understand the key characteristics of a service and establish the distinct nature of that service as opposed to a system or product, especially with respect to assurance for safety. Some characteristics of a service are similar to systems or products and as such, much can be tailored from traditional assurance approaches. However, some characteristics can be different from, or even unique, to service provision thus requiring adaptation of existing approaches or completely new techniques.

Figure 1 showed typical aspects of a service within a service provision model. There is always at least one consumer of the service and at least one provider. There is also always a definition of the service which may be part of a contract, and there is usually some form of Service Level Agreement (SLA) detailing the contractual expectations of the services being provided. Typically, services have several levels or layers and may end up forming a service stack. It is important to note that a lower-level service in such a stack may be consumed by several independent higher-level services.

Some typical characteristics of services and a comparison with products are given in Table 1.

Table 1 - Typical Service Characteristics

ID	Service Characteristic	Service Context	Compared to Systems / Products
C1	Services are provided for the duration of a service contract	By definition, services provide features with a given performance for the duration of the contract between provider and consumer. The service consumer does not usually have to be concerned with the design, maintenance, or disposal of the service components.	Products persist beyond the contract end date. Products are usually provided with warranties but there may be no further involvement from the producer after product acquisition. The owner of the product is usually responsible for maintenance and disposal.

ID	Service Characteristic	Service Context	Compared to Systems / Products
C2	Services are often designed to meet the needs of a broad range of consumer needs	Providers want to attract a broad range of customers and may wish to avoid bespoke solutions. In a services context it can be easy to add or remove features for particular customers.	Products are often designed to exacting specifications, often for a broad set of customers but may be bespoke.
C3	Services are likely to be used by more than one consumer	Service providers usually desire to sell similar service offerings (via catalogues), so multiple consumers can be using the same service offering at the same time (or sharing resources of other services). However services may be tailored for particular consumers.	Products are often used by many different customers; it is less common to develop bespoke systems now. Products are increasingly able to involve some degree of tailoring and configuration.
C4	Services are implemented through a combination of elements	Service implementation typically requires the collaborative working of many elements including people, processes, products and other products, systems and services to deliver a set of features with the desired performance	Similar to complete systems that consider people procedures and equipment and all aspects of in-service operation. However, systems and product suppliers are not usually responsible for live system operation.
C5	Services may be designed without recognition of the full context of use	Providers may release the service before the full context is understood. The service may be designed to adapt to a context of use or may evolve over time to meet the emerging context of use. Services may be developed for specific purposes that other users exploit (i.e. there may be unexpected and unintended uses/users). New features are sometimes added to a service without the consumer's knowledge. Changes in the underlying provision increase the likelihood of undesired emergent properties.	Similar to off the shelf products and systems, however, once established and demonstrated within the context of use, products and systems are usually only changed under the direct control of the consumer.
C6	Service implementation details may not be visible to the consumer	Whilst the performance and features of a service should be clear to the consumer, the details of how the service is delivered may be kept confidential or be hidden within other lower-tier services.	Very similar to Commercial Off The Shelf (COTS) products / software. However, once established and demonstrated for a given installation, products and systems are usually only changed under the direct control of the owner.
C7	Service implementation may change frequently and significantly	Providers may be looking to maintain or obtain a commercial advantage, hence streamlining service provision, offshoring, reacting to other consumer requirements and external issues (e.g. new security threats), etc.	Very different from a typical product scenario where change is non-existent, limited, or the change is very much under the control of the product owner.

ID	Service Characteristic	Service Context	Compared to Systems / Products
C8	Services may include or provide features for the maintenance or monitoring of the service or other services	Services cover a broad range of scenarios e.g. from provision of a product through to a service to inspect an installation, audit another provider, dispose of a product, etc. The service could have a big impact on the consumer's product, systems or services if not provided properly.	Unusual for a system or product to involve such activities.
C9	Services are often multi-layered	Consumers may not be aware of all the services used by the service provider. Sub-layers of providers often become more generic and commoditised and can use common service suppliers. Sometimes requirements (e.g. for location and diversity) are often inadvertently and silently not met. The service consumer is unlikely to be aware of the full service hierarchy. This could increase the likelihood of undesired emergent properties.	Similar to off the shelf products and systems, however, once established and demonstrated within the context of use products and systems are usually only changed under the direct control of the consumer.
C10	Services may be created rapidly	New services can be very quickly constructed from existing services and products by using people and procedures as the 'glue'. There may be little design activity with components 'bolted together' with speed of service construction being the dominant factor.	Products and systems usually take significant time to develop and are subject to design and review activities.
C11	Services may change size and scope quickly	Services can be resized very rapidly due to the flexibility of the people involved. This can be scaling up or down or change of scope.	Complete systems may be resized in similar ways, but generally with more design activity.
C12	Services may be provided from frequently changing multiple locations	Services may utilise many sub-services which may be located in different locations or jurisdictions, anywhere across the world (e.g. web services), and these may change regularly (e.g. annually).	Although products and systems may utilise components sourced from multiple suppliers (which may be global), they generally keep the same source/supplier for as long as possible.

2 Assurance of Services (Informative)

"Anyone who works in the NHS [National Health Service] has superpowers. It's a miracle, it is magic."

Benedict Cumberbatch

The nature of services presents several challenges to established systems safety assurance methodologies and processes, and services are hardly mentioned in current guidance and standards. The section below lists some of these challenges.

2.1 Service Assurance Challenges

Some of the challenges with safety-related services that have been identified and will need due consideration are listed below. These are presented here to show some of the differences with traditional systems safety assurance. Further consideration of some of these is given in section 5.3.

Service Implementation Since the details of the implementation of the service are often hidden, the potential contribution of the service to system-level hazards may not be fully understood.

Management of Interfaces The complexity of the service hierarchy and the way that services are consumed may lead to issues of how interfaces are managed, and where hazards might emerge.

Service Data This is essential to support an assurance argument and may not flow easily through the development chain, and it may not be clear how to write service contracts in such a way as to ensure that appropriate data is available. The COTS nature of many service components further adds to this problem.

Service Change Changes to the service might not be visible to the system integrator or consumer. The safety impact of such changes might not be clear to the service provider, since there may be no clear understanding of the operational context or end use of the service. Contracting issues may contribute to this lack of visibility or understanding.

Service-Level Agreements Safety-related features of the service – such as availability, throughput, timeliness of data provision, data accuracy requirements etc. – are governed by service-level agreements. It is therefore essential that these agreements have a clear understanding of potential safety concerns, and that their importance is communicated across organisational boundaries.

Cloud Safety-related services may rely on generic cloud software and commercial hosting services (e.g. Amazon Web Services). Particular assurances are needed to ensure the suitability of these services for safety-related operations and content.

Service Interference Some services or consumed sub-services may unintentionally interfere with each other causing deterioration in service levels. This could be due to use of common infrastructure,

common personnel or complex, unintended interactions and behaviours. This also ties in with the need to investigate and analyse possible emergent behaviours of services.

Unintentional Service Provision For instance, services may be procured generically and include elements that come included in the package, and that are provided automatically or by default and are difficult to disable. A simple example may be the provision of WiFi to a wider area than intended.

Service Analyses It may be difficult to carry out assurance analyses such as common mode failure analysis, Failure Modes and Effects Analysis (FMEA) or analysis for emergent properties without visibility of a Service's implementation (see section 6).

Analysis of Contractual Documents Technical/legal analysis of SLAs and SoWs may be required, and conclusions for the assurance case produced. This may require specialist skills. There also needs to be a way of establishing the level of confidence required that a specific SLA will be met. It may be possible to do a "failure analysis" of the SLA itself (see section 6).

ALARP The United Kingdom (UK) 'As Low As Reasonably Practicable' (ALARP) principle may need to be considered for services. This is especially true when a service provider may not know which of their services (or specific characteristics of specific services) will subsequently be relied on to satisfy some higher-level safety claim.

Service Layers Is it reasonable to assume that the higher levels in a service stack take safety responsibility, i.e. "layer n looks after level n-1"? Does this always mean that the service consumer holds the overall risk? For assured services, there may need to be visibility through the layers.

Properties In the case of flowed-down safety requirements, we need to define a set of properties that the service (or service component) needs to exhibit (from the point of the consumer), involving specific properties and targets which can then be assured.

Constraints Consumers need to provide evidence that they are consuming the services within the defined constraints of use. Service agreements probably need to include specific constraints or limitations of use (and indeed what is not expected) as well as positive requirements.

Who Assures? It will be necessary to establish who is doing the assurance in a service stack as the picture could be complex – does each service provider or supplier just assure their "level" in the stack? Who has the overall picture? Note that failures may propagate across service layers, so there is a need to understand interactions on the margins, and also to capture and manage the notification chain. This may result in functional requirements for notification, including auditing, corrective actions, etc. This would need to be reflected in contractual arrangements.

Supply Chains Service stacks and service supply chains could get long and obfuscated; how do we assure more complex Services of Services? How much trust do we put in a 3rd party service provider's assurance? Could a significant safety event / service failure flow up the supply chain?

Emergent Properties Provision of services may exhibit emergent properties and often behave in ways not envisaged by the original service designer. Further work is required here to fully understand the kinds of mechanisms with service provision that could lead to emergent properties that may have

a safety impact. It will be necessary to analyse and manage emergent properties arising from the service. An added complication is the emergent behaviours that services may cause in people.

Security There is a need to feed in outputs of security analyses into the service safety analysis to give "security informed safety services".

Safety Arguments Different types of assurance argument (product, service or a mix) could support a top-level Safety Case, and a number of 'frameworks' (i.e. a limited number of patterns) for Service Assurance Arguments need to be established. There also needs to be generic advice on how safety cases could be structured to reflect the service-based safety assurance approach.

Legal Considerations If a service is consuming another (more generic) sub-service to fulfil its aims, what it the legal position if the consumed sub-service fails in a way to cause a safety issue? It may make no claims about its suitability for the safety-related use in which it has been put by the consuming service. In the UK, who would face corporate manslaughter charges and claims?

2.2 Assumptions

The following assumptions have been made for this issue of the guidance document to help frame the guidance:

- A Service can be modelled as hierarchy (or network) of layered sub-services.
- Only safety is considered (i.e. this document is only interested in safety assurance), other aspects, such as reliability, liability and security assurance are not covered (however, a similar approach may work with these types of attributes).
- Not all the organisations in a service stack will be willing or able to take part in safety activities.
- Assurance may be derived from several evidence items including non-traditional aspects such as the Service Level Agreement and Service Definition.
- Internal service assurance (i.e. that used within a specific service) may not be visible to the Service Consumer.
- Assurance evidence can be supplemented (that is, "wrapped") with additional activities and artefacts which provide additional argument / evidence. The organisation providing the supplementary "assurance wrapper" may be the service consumer, service provider or a third party.

This page is intentionally blank

3 Service Assurance Principles (Normative)

"Softbank has always been a service firm, and with the Internet, services became the center of the technology industry."

Masayoshi Son

This section introduces the concept of Service Assurance Principles, using a similar approach to that used for software safety assurance.

3.1 Introduction to Principles

Table 2 presents the 6 Service Assurance Principles proposed as a way of structuring the service assurance activity, and of checking that completeness and consistency has been achieved in this guidance. Similar principles have been found to be useful in safety-related software development, data safety, development of autonomous systems and other areas.

Table 2 - Service Assurance Principles

1	Service assurance requirements shall be defined to address the service-based solution's contribution to both desirable and undesirable behaviours
	There must be an overall definition of what the service is trying to achieve (formulated as requirements) and this must be within an expected usage scenario (e.g. concept of operations). There must be requirements addressing known behaviours that are unwanted or unsafe.
2	The intent of the service assurance requirements shall be maintained through the service definitions, service levels, the service architecture and the agreements made at service interfaces
	This relates to the way the service hierarchy and service decomposition is constructed. It is saying that the intent of the assurance requirements must be shown to be met by the service elements comprising the service, and that the overall service architecture or hierarchy supports this flow down (i.e. that all service elements together meet the overall intent, and nothing is missing). Service elements can be of various types, including other services, systems, subcontracts, and agreements.
3	Service assurance requirements shall be satisfied
	Service assurance requirements must be satisfied, i.e. verified as-is or decomposed into further requirements which are subsequently verified in some way. The methods by which service assurance requirements are verified are wider than traditional systems, often including extensive use of proven-in-use (service history) and commodity-usage arguments, and also some specific contractual mechanisms. This principle (together with (4) below) creates the need for assurance "wrappers". (A *wrapper* is an assurance augmentation which addresses the assurance deficit inherent in the consumed service in some way.)
4	Unintended behaviours of the service-based solution shall be identified, assessed and managed
	All undesired or unintended behaviours which may impact safety properties or safe behaviour of the overall system must be identified and assessed within the usage context. They must be appropriately managed (e.g. mitigated, avoided or accepted in some way). This is not always possible to the extent desired, especially when commercial "commoditised" services are involved. Hence this may create the need for additional wrappers to make up the assurance gaps (see also principle (3) above).

5	The confidence established in addressing these principles shall be commensurate with the level of risk posed by the service-based solution
	This is the proportionality principle: the level of (safety) risk must be used to determine the amount of effort (resources, time, etc.) put into assurance and mitigation activities. This principle can be used to underpin a set of levels of service assurance, where applicable activities are defined in bands derived from the risk level.
6	These principles shall be established and maintained throughout the lifetime of the service-based solution, resilient to all changes and re-purposing
	Services may have a long lifetime and the service offering may evolve significantly over this time. These principles must be established and maintained throughout life: through e.g. usage change, technical change, subcontractor change, supplier or process and personnel change. This principle must also hold in service failure scenarios (contingency situations) where the service might temporarily employ manual or procedural activities to achieve its aims. It might be thought that this principle is implied by the others, but continuous evolution and change is a key property of services; in this they are different to (largely) static systems.

3.2 Service Principles and Service Characteristics

Table 3 shows the linkage between the Service Assurance Principles and Service Characteristics.

Table 3 - Mapping of Service Assurance Principles to Service Characteristics

Characteristic ⇒ Principle ⇓	C1 - Services are provided for the duration of the service contract	C2 - Services are often designed to meet the needs of a broad range of consumer needs	C3 - Services are likely to be used by more than one consumer	C4 - Services are implemented through a combination of people, procedures, products and other services
Principle 1	Requirements need to be in place and implemented at the start of any contract. There may need to be assurance in the transition from old service provider to a new one. There will need to be a continuous assurance approach.	Services may not meet all requirements and may exhibit undesired behaviours. The overall SBS needs to be designed to tolerate or make up for specific service shortcomings.	Services may exhibit undesired behaviours. The overall SBS needs to be designed to tolerate or make up for specific service shortcomings	Assuring that requirements are met through the SBS will involve assessment of technical, process and people aspects.
Principle 2		Services may have more features than required. Unused features may introduce interference with features that are safety related. Ideally unused services would be removed or disabled.	Potential for service interference or disruption must be analysed where exclusivity is not provided.	
Principle 3	Service assurance requirements need only be satisfied for the duration of the service contract. However, the consumer may need to define alternate service provision in case of significant service failure or sudden contract termination.	Generic requirements or service capabilities may need to be mapped to specific use cases.	Requirements for one consumer may not necessarily meet those of another. Changes may impact existing consumers. Service level agreements may need notification clauses.	Requirements will have to be produced and verified for the SBS (including staff and suppliers) and may be of different forms.
Principle 4				
Principle 5	Confidence needs to be provided proportionate to the risk exposure involved. Shorter contracts may reduce overall exposure but may leave out important assurance.	Confidence levels for most consumers may not be sufficient for specific safety-related usage, see section 4.	Confidence in the adequacy of non-interference measures must be established, see section 4.	Depending on the assurance level required specific assurance needs will have to be met including those on people and process, e.g. there may need to be additional vetting, training and monitoring of staff.
Principle 6	Assurance needs to be maintained throughout the contract period. Changes must be addressed, key performance indicators monitored, and any issues rectified through life. Service level agreements are in effect for the entire contract period. Changes cannot be made without both parties agreement.	Services often evolve over time or are implemented differently to accommodate new consumers. Assurance must be maintained or re-worked for changes, especially if new non-safety consumers are in the majority.	Services often change to accommodate new consumers. Assurance must be maintained or re-worked for changes.	Evidence will need to be continuously or routinely monitored to ensure the assurance is still current, e.g., through process or procedure changes or when staff or a supplier change.

Characteristic ⇒ Principle ⇓	C5 - Services may be designed without recognition of the full context of use	C6 - Service implement-ation details may not be visible to the consumer	C7 - Service imple-mentation may change frequently and significantly	C8 - Services may include or provide features for the maintenance or monitoring of the service or other services
Principle 1	Services may not meet all requirements and may exhibit undesired behaviours for a specific usage. Generic behaviours may need to be tailored. The overall SBS needs to be designed to tolerate or make up for specific service shortcomings.	How a service requirement is met may not visible to the service consumer. The Service level agreement may establish that the service provider is responsible for assuring the service assurance requirements are met	Changes may occur without the knowledge of the consumer. The first awareness may come with failure of the service	Service assurance requirements must address all aspects of service provision, including aspects affecting other services.
Principle 2				
Principle 3	The service may not be compatible for a specific context of use or may change over time. Compatibility needs to be assessed prior to service activation and changes need to be managed with the consumer	There may be limits on verification, e.g. simply that the performance / features are achieved / provided. It may not be possible to assess robustness easily. The service provider may be independently regulated.	Frequent changes may degrade or undermine confidence over time, see section 4, e.g., change of supplier every 12 months.	The monitoring service needs appropriate verification and assurance itself.
Principle 4				
Principle 5	Generic services are common and may be used for unexpected or unintended uses. It is important to establish confidence in behaviours related to the safety-related usage.	The service consumer needs to be sufficiently confident in what is not visible. Some knowledge and details of the implementation may be required to build enough confidence.	The service consumer needs to be sufficiently confident especially when it changes frequently. Where changes are not under the control of the consumer, they will need to maintain awareness of changes.	The monitoring needs to be appropriate for the level of safety delivered by the monitored services.
Principle 6	Over the service lifetime many changes and evolutions may occur which may change the offered functionality considerably. Service offerings may become more generic over time.	There may be many changes in the underlying service implementation during the lifetime of the service. These need to be visible to the service consumer and assurance formed where necessary.	There may be many changes in the underlying service implementation during the lifetime of the service. Most will have no impact, but some may.	The monitored services are likely to evolve, and the monitoring service may need to adapt over time with new tools and technologies.

Characteristic ⇒ Principle ⇓	C9 - Services are often multi-layered	C10 - Services may be created rapidly	C11 - Services may change size and scope quickly	C12 - Services may be provided by frequently changing multiple locations
Principle 1	Requirements must flow down appropriately through the layers. It can be difficult to assure changed consumed services and suppliers many levels down in the hierarchy.	Assurance requirements should be created for the new service.	Assurance requirements should be reviewed and updated for the changed scope.	Requirements must flow down to all consumed sub-services, wherever they are located. This flow down must be maintained throughout life.
Principle 2	Layers in the hierarchy may interact in unexpected ways or use common resources thus undermining assurance claims made by the SBS.	Requirements should be flowed down through the new service structure, including new suppliers and contracts.	Requirement flow down should be checked down through the updated service structure, including changed suppliers and contracts.	Layers of service implementation must maintain requirements flow wherever they are located.
Principle 3	Efforts should be made to establish that lower levels of the SBS hierarchy will satisfy flowed down assurance requirements.	The new service should be verified in an appropriate way and any unexpected behaviours due to rapid creation explored.	The new service should be verified in an appropriate way and any unexpected behaviours due to size or scope change explored.	Verification evidence should be refreshed if parts of a service are moved. New wrappers may be needed on any change.
Principle 4				Changes in implementation (e.g. offshoring) may introduce unintended behaviours.
Principle 5	Assurance effort should be proportionate i.e. may be stopped at a certain level or layer, replaced by wrappers.	Assurance effort should be proportionate to the newly created service risk. Waivers may be needed initially where assurance is lacking.	Assurance effort should be proportionate to the changed service risk.	Assurance effort should be proportionate to the changed service implementation risk.
Principle 6	Assurance must be maintained through multiple layers and when the service hierarchy is changed.	All initial changes and teething problems should be analysed, and updates made.	All changes need to be checked for impact on service assurance.	All changes (which may be frequent e.g. change of service provider on annual basis) require a reassessment of assurance. Wrappers may be needed, especially when service provision is across national boundaries.

3.3 Objectives for each principle

The principles form the high-level "mission statement" of service assurance. These can then be mapped to a lower-level set of objectives which can be used to tie into a service lifecycle. Objectives form the next level of specification. Tied to a principle, if the objectives for a principle are satisfied, then it can be stated that the principle is met.

3.4 Mapping of Principles to Service Objectives

Table 4 shows how the principles may be mapped to lower-level objectives phrased as requirements. This then gives a flow-down to more tangible deliverables and outputs which can be verified using appropriate techniques for production of evidence.

Table 4 - Mapping of Service Assurance Principles to Service Objectives

1	Service assurance requirements shall be defined to address the service-based solution's (SBS) contribution to both desirable and undesirable behaviours
	a. Context and intended use of the SBS SHALL be established b. States of the SBS SHALL be defined including normal, abnormal and degraded modes, as well as transitions between the states c. Key stakeholders of the SBS SHALL be identified d. Service assurance requirements for desirable behaviours, including service and performance levels, of the SBS SHALL be defined e. Service assurance requirements to mitigate undesirable behaviours of the SBS SHALL be defined f. A high-level service architecture SHALL be defined g. Historical accidents and incidents related to the service offering SHOULD be assessed and any relevant recommendations considered
2	The intent of the service assurance requirements shall be maintained through the service definitions, service levels, the service architecture and the agreements made at service interfaces
	a. Service assurance requirements SHALL be decomposed and assigned to service elements within the service architecture of the SBS b. The service architecture including sub-services SHALL be defined c. Service assurance requirements SHALL be defined for each sub-service d. The agreements made at service interfaces SHALL be defined e. Service assurance requirements tracing through the service architecture SHALL be established f. Methods and techniques used to provide service assurance within each level of the service architecture SHALL be defined and implemented g. Assurance wrappers SHALL be identified and defined for service elements to make good any known assurance shortfalls
3	Service assurance requirements shall be satisfied
	a. Verification evidence SHALL be produced to show that service assurance requirements are met by the architecture and the elements of the SBS b. Assurance wrappers SHALL be implemented and verified c. Evidence SHOULD include proven in use and service history evidence
4	Unintended behaviours of the service-based solution shall be identified, assessed and managed
	a. Residual risks SHALL be identified and linked to service artefacts and service properties b. The residual risk of the SBS SHALL be reduced to an acceptable level c. Unintended behaviours resulting from the service architecture and service elements SHALL be identified, assessed and managed d. Unintended behaviours resulting from fault-free cases SHALL be identified, assessed and managed e. Service-service interactions SHALL be considered f. Service assurance artefacts SHALL be identified and produced

5	The confidence established in addressing these principles shall be commensurate with the level of risk posed by the service-based solution
	a. Levels of Service Assurance (LSAs) SHALL be established based on the level of risk that the service presents to the service users b. LSAs SHALL be decomposed and assigned to service elements within the service architecture of the SBS c. Service assurance artefacts SHALL be produced according to the LSA d. Activities, methods, analyses, and tools used to provide service assurance SHALL be appropriate for the LSA
6	These principles shall be established and maintained throughout the lifetime of the service-based solution, resilient to all changes and re-purposing
	a. All changes to the SBS that impact these objectives SHALL be assessed and managed b. Service assurance artefacts SHALL be maintained c. Use of the SBS SHALL be monitored for change and a safety impact analysis undertaken where necessary d. Use of the SBS for a new purpose, or changed scope SHALL cause a re-evaluation of the compliance with the objectives e. Degraded and contingency modes of the SBS SHALL maintain a defined subset of these objectives to a specific level f. Lessons learnt from successful operation, failures and incidents SHALL be reviewed and considered for incorporation in the SBS

Note: not all objectives may need to be met to fulfil the requirements; it depends on the level of risk involved. Further sections introduce a scoping or modulation of objectives depending on the level of service assurance required.

3.5 Note about Responsibilities

The overall responsibility for specifying and showing complete achievement of these objectives sits with the organisation consuming the service, however the objectives will typically be met by other organisations within the service provision (which can be the service provider, or a third party contracted to provide service assurance).

4 Level of Service Assurance (LSA) (Normative)

"Eighty-five percent of the reasons for failure are deficiencies in the systems and process rather than the employee. The role of management is to change the process rather than badgering individuals to do better."

The concept of Level of Service Assurance is an important one. It is acknowledged that, in a services world, differing amounts of assurance are required for different types and instances of service usage. What the Level of Service Assurance does is formalise this approach, so it becomes explicit as to what is required to meet a particular level of safety risk inherent in the service.

The LSA is defined by the level of risk in using the service (i.e., defined by the consumer of the service). Five levels are proposed in Table 5.

Table 5 - Levels of Service Assurance

Level of Service Assurance	Definition (Service **Consumer** View)
LSA 0	No safety aspects present in service so no objectives assigned to services assessed to be at LSA0
LSA 1	Minor safety aspects with little impact of failures (minor injury possible but unlikely)
LSA 2	Safety aspects with some impact of failures (several injuries possible)
LSA 3	Significant safety aspects with service with major impact (could indirectly lead to multiple injuries or a single death)
LSA 4	Service is safety-critical: service failures could have catastrophic impact (could directly lead to multiple deaths)

Notes:

The definition refers to harm to people. This could be extended to cover other aspects if required, e.g. environment, assets or platforms.

The LSA is allocated in a top-down fashion, starting with the highest-level service element (i.e. the service visible to the consumer). It then flows down through the hierarchy. The allocation rule is that at least one of the subsidiary elements inherits the highest LSA above it[1].

The flow down of LSA, where used, must be justified, i.e. there must be an explanation as to why the flow of LSA levels through the hierarchy preserves the overall safety goals. Also there must be no 'dumping' of a high LSA level onto an irrelevant subsidiary component; the overall safety picture must be preserved and justified through flowdown.

[1] So for example if the top-level service is LSA3, then at least one of the next-level down services in the hierarchy is also LSA3 (or possibly LSA4).

4.1 Influences on Level of Service Assurance

The level of service assurance assigned may be influenced by several factors, including:

- The faults that may occur in the service and how easily they may be detected and corrected.
- Importance of timeliness, i.e. the time criticality of the service.
- Ease of mitigation and management of problems, failures and issues that arise, e.g. can someone or something easily take over.

For faults, one might consider a range of possibilities from a situation where a fault is easily detected by human or automatic means through to the situation where a fault may be undetected for an extended period, or indeed is not possible to detect by any reasonable means. If fault detection is hard, then it sensible to err the LSA on the side of caution, i.e., where there is doubt choose a higher LSA.

For time criticality, the lowest level might be where the service has no specific timeliness involved or long periods (weeks or months) available to recognise problems and take mitigating actions. The highest would be where the service is highly time-critical and there is no time to recognise problems and take mitigating actions.

For ease of mitigation, the range is from a situation where service problems are easily mitigated by human or automatic means, up to the case where a problem is not easily mitigated or indeed impossible to mitigate.

4.2 Objectives and Applicability

Table 6 links the objectives to a set of methods and techniques tables, giving suggested approaches to satisfying the objectives.

Each objective is considered applicable (i.e. required) at a certain LSA or higher.

Key: o - Optional, ● - Required

Table 6 - Levels of Service Assurance Applicability

#	Principle and Objective	Needed for LSA				Ref.
1	Service assurance requirements shall be defined to address the service-based solution's (SBS) contribution to both desirable and undesirable behaviours	1	2	3	4	Sect. 5 table rows
	a. Context and intended use of the SBS SHALL be established	●	●	●	●	SP-1 to SP-8
	b. States of the SBS SHALL be defined including normal, abnormal and degraded modes, as well as transitions between the states	o	o	●	●	SP-7
	c. Key stakeholders of the SBS SHALL be identified	o	●	●	●	SP-4
	d. Service assurance requirements for desirable behaviours, including service and performance levels, of the SBS SHALL be defined	o	●	●	●	SP-3
	e. Service assurance requirements to mitigate undesirable behaviours of the SBS SHALL be defined	o	●	●	●	SP-3; SA-1to SA-12

#	Principle and Objective	Needed for LSA				Ref.
	f. A high-level service architecture SHALL be defined	●	●	●	●	SD-1 to SD-9
	g. Historical accidents and incidents related to the service offering SHOULD be assessed and any relevant recommendations considered.	o	o	o	o	SA-11; SF-5
2	The intent of the service assurance requirements shall be maintained through the service definitions, service levels, the service architecture and the agreements made at service interfaces	1	2	3	4	Sect. 5 table rows
	a. Service assurance requirements SHALL be decomposed and assigned to service elements within the service architecture of the SBS	o	●	●	●	SP-3; SP-7; SD-1 to SD-9
	b. The service architecture including sub-services SHALL be defined	o	●	●	●	SD-1 to SD-9
	c. Service assurance requirements SHALL be defined for each sub-service	o	o	●	●	SP-3; SP-5; SP-8
	d. The agreements made at service interfaces SHALL be defined	o	●	●	●	SP-5; SP-8; SC-6
	e. Service assurance requirements tracing through the service architecture SHALL be established	o	o	●	●	SP-3; SP-5; SD-3 to SD-6; SY-4 to SY-5
	f. Methods and techniques used to provide service assurance within each level of the service architecture SHALL be defined and implemented	o	●	●	●	SA-1 to SA-12; SS-1 to SS-9; SV-1 to SV-13
	g. Assurance wrappers SHALL be identified and defined for service elements to make good any known assurance shortfalls	o	●	●	●	SS-3 to SS-5
3	Service assurance requirements shall be satisfied	1	2	3	4	Sect. 5 table rows
	a. Verification evidence SHALL be produced to show that service assurance requirements are met by the architecture and the elements of the SBS	o	●	●	●	SV-1 to SV-13
	b. Assurance wrappers SHALL be implemented and verified	o	●	●	●	SS-4 to SS-5; SV-1 to SV-13
	c. Evidence SHOULD include proven in use and service history evidence	o	o	o	o	SV-14
4	Unintended behaviours of the service-based solution shall be identified, assessed and managed	1	2	3	4	Sect. 5 table rows
	a. Residual risks SHALL be identified and linked to service artefacts and service properties	o	●	●	●	SS-1 to SS-9
	b. The residual risk of the SBS SHALL be reduced to an acceptable level	●	●	●	●	SS-1 to SS-9

#	Principle and Objective	Needed for LSA				Ref.
	c. Unintended behaviours resulting from the service architecture and service elements SHALL be identified, assessed and managed	o	●	●	●	SA-1 to SA-13
	d. Unintended behaviours resulting from fault-free cases SHALL be identified, assessed and managed	o	o	●	●	SA-1 to SA-13
	e. Service-service interactions SHALL be considered	●	●	●	●	SA-6; SF-4
5	The confidence established in addressing these principles shall be commensurate with the level of risk posed by the service-based solution	1	2	3	4	Sect. 5 table rows
	a. Levels of Service Assurance Levels (LSAs) SHALL be established based on the level of risk that the service presents to the service users	●	●	●	●	SS-10
	b. LSAs SHALL be decomposed and assigned to service elements within the service architecture of the SBS	o	●	●	●	SD-1 to SD-9
	c. Service assurance artefacts SHALL be produced according to the LSA	●	●	●	●	SS-1 to SS-10
	d. Activities, methods, analyses and tools used to provide service assurance SHALL be appropriate for the LSA	●	●	●	●	SS-1 to SS-10
6	These principles shall be established and maintained throughout the lifetime of the service-based solution, resilient to all changes and re-purposing	1	2	3	4	Sect. 5 table rows
	a. All changes to the SBS that impact these objectives SHALL be assessed and managed	●	●	●	●	SH-1 to SH-4
	b. Service assurance artefacts SHALL be maintained	●	●	●	●	SS-2; SS-5 to SS-10
	c. Use of the SBS SHALL be monitored for change and a safety impact analysis shall be undertaken where necessary	●	●	●	●	SS-6 to SS-10; SH-1 to SH-4
	d. Use of the SBS for a new purpose, or changed scope SHALL cause a re-evaluation of the compliance with the objectives	●	●	●	●	SS-6 to SS-10; SH-1 to SH-4
	e. Degraded and contingency modes of the SBS SHALL maintain a defined subset of these objectives to a specific level	o	●	●	●	SS-2, SS-5; SF-1 to SF-4
	f. Lessons learnt from successful operation, failures and incidents SHALL be reviewed and considered for incorporation in the SBS	o	●	●	●	SS-9; SV-14; SF-5; SR-1 to SR-5

Hence the LSA defines the quantity, breadth and rigour of the service assurance required from the assurance provider.

5 Capturing Justifications and Evidence (Discursive)

"People love our products. They love using our services. All of this, to me, equals great opportunity."

Tim Cook

5.1 Evidence Tables

The following section lists example techniques for production of evidence against each objective. These are examples only; other ways of meeting the objectives may be acceptable. These are listed in the following tables:

SP - Service Scope

SD - Service Design

SA - Service Analysis

SC - Service Contracting

SY - Service Delivery

SS - Service Assurance

SV - Service Verification

SH - Service Change

SR - Service Regulation

SF - Service Staffing

Table 7 - SP - Service Scope

#	Technique	Typical Container
SP-1	Service context and usage scenarios / use cases defined	Consumer requirements document
SP-2	Service Concept of Operations (CONOPS) defined	CONOPS/Service Catalogue
SP-3	Service requirements established	Service Requirements Specification
SP-4	Stakeholders established	Consumer requirements document
SP-5	Interfaces established	Service Architectural Design
SP-6	Consumers established	CONOPS
SP-7	States of the SBS (including degraded modes) established	CONOPS
SP-8	Consumed services, systems and contracts established	Service Architectural Design

Table 8 - SD - Service Design

#	Technique	Typical Evidence
SD-1	Industry accepted norm service design methodology employed	Service Architectural Design
SD-2	Reference to existing similar service design	Service Architectural Design
SD-3	Appropriate redundancy in design	Service Architectural Design
SD-4	Appropriate diversity in design	Service Architectural Design
SD-5	Appropriate failover/standby instances in design	Service Architectural Design
SD-6	Degraded modes of operation of the service covered by design	Service Architectural Design
SD-7	Description of service components offered	Service Catalogue
SD-8	Description of consumed services (internal to organisation)	Operational Level Agreement
SD-9	Description of consumed services (external to organisation)	Sub-service level agreements

Table 9 - SA - Service Analysis

#	Technique	Typical Containers
SA-1	Service Functional Failure Analysis	SFFA report
SA-2	Service Failure Modes and Effects Analysis	SFMEA, SCM/CCA reports
SA-3	Service Hazard Analysis	SHA report
SA-4	Service Process Modelling Notation	SPMN report
SA-5	Service Decision Analysis	SDA report
SA-6	Service Metrics and Contracts Analysis	SMCA report
SA-7	Service Structure Analysis (Inc. subcontracts, suppliers, outsourcing, offshoring, gap analysis, etc.)	SSA report
SA-8	Service Focussed Organisational Risk Analysis (business risk, enterprise risk, supply chains, logistics, competence, etc.)	SFORA report
SA-9	Service Bow-Tie Analysis	SBTA report
SA-10	Service-Focussed Systems Analyses (e.g. System-Theoretic Accident Model and Process /Systems Theoretic Process Analysis	SFSA report
SA-11	Service-Related Historical Accident and Incident Report analysis	SHAIR report
SA-12	Service Functional Resonance Analysis Method	SFRAM Report

Table 10 - SC - Service Contracting

#	Technique	Typical Containers
SC-1	Simple Statement of Work	Memos, Emails
SC-2	Formal Statement of Work	SoW document
SC-3	Informal contract	Memos, Emails
SC-4	Formal Contract documentation set	Contract
SC-5	Specific penalties for non-conformance	SLA, SoW
SC-6	Service Level Agreement (SLA)	SLA, Contract
SC-7	Key Performance Indicators (KPIs) defined	Contract
SC-8	Informal supplier check	Emails, personal reference
SC-9	Formal supplier evaluation - may include assessments of several suppliers	Supplier evaluation report
SC-10	Supplier references	Supplier evaluation report

#	Technique	Typical Containers
SC-11	Financial checks	Supplier evaluation report
SC-12	Experience in this sector	Supplier evaluation report
SC-13	Certifications / accreditations (for services)	Supplier certificates / formal accreditation
SC-14	Compliance to industry standard or guidance (for services)	Supplier certificates / formal accreditation

Table 11 - SY - Service Delivery

#	Technique	Typical Containers
SY-1	Informal or commercial service delivery models	Service Design Document
SY-2	Recognised industry-standard service delivery model (e.g. ITIL)	Conformance / Compliance Reports
SY-3	Metrics collected and used to improve service	Monthly Service Reports
SY-4	Service Level Agreements	Contract
SY-5	Operational Level Agreements	Company Internal Agreements

Table 12 - SS - Service Assurance

#	Technique	Typical Containers
SS-1	Informal assurance position made	Technical documents
SS-2	Service Assurance Case established	Assurance / Safety Case Report
SS-3	Assurance gaps / deficiencies identified and managed	Hazard Logs, Assurance / Safety Case Report
SS-4	Assurance wrappers defined and implemented where needed	Assurance / Safety Case Report
SS-5	Supplementary assurance activities defined and implemented	Assurance / Safety Case Report
SS-6	Assurance position reviewed after any change	Change Review
SS-7	Assurance position regularly updated	Assurance / Safety Case Report
SS-8	Assurance dashboard shows current position	KPIs / Dashboards
SS-9	Assurance position reviewed after incident / accident	Assurance / Safety Case Report
SS-10	Derivation of LSA and justification	LSA Report

Table 13 - SV - Service Verification

#	Technique	Typical Containers
SV-1	Informal Testing	Spreadsheets
SV-2	Testing performed and documented	Test Specifications Test Reports
SV-3	Extensive functional testing	Test Specifications Test Reports
SV-4	Hazard-based testing	Test Specifications Test Reports
SV-5	Basic performance testing	Spreadsheets
SV-6	Extensive performance testing	Test Specifications Test Reports
SV-7	Basic stress testing	Spreadsheets
SV-8	Extensive and extended stress testing	Test Specifications Test Reports
SV-8	Basic failover testing	Spreadsheets

#	Technique	Typical Containers
SV-9	Extensive Failover and service restoration / fail-back testing	Test Specifications Test Reports
SV-10	Degraded mode testing	Test Specifications Test Reports
SV-11	Extensive and extended degraded mode testing	Test Specifications Test Reports
SV-12	Regression testing	Regression Test Suites Test Specifications Test Reports
SV-13	Highly automated testing, regularly run on scheduled basis	Tooling documents Automation Scripts Test Specifications Test Reports
SV-14	Historical Verification Trend Analysis	Trend Analysis Reports

Table 14 - SH - Service Change

#	Technique	Typical Containers
SH-1	Informal service change process	Technical Documents
SH-2	Formal service change process including sign-off	Change Management Process, Change Documents
SH-3	Change impact analysis	Change Documents
SH-4	Update to service analyses for change	Analysis Documents

Table 15 - SR - Service Regulation

#	Technique	Typical Containers
SR-1	Informal review	Technical Documents
SR-2	Audit and review (by same organisation)	Internal Audit Reports
SR-3	Audit/review by 3rd party organisations	External Audit Reports
SR-4	Light-touch industry regulation	Regulator Review
SR-5	Formal industry regulation (legal basis)	Regulator Reviews / Audit Reports

Table 16 - SF - Service Staffing

#	Technique	Typical Containers
SF-1	Trained staff	Training records
SF-2	Demonstrably competent staff	Competency assessment records
SF-3	Staff Monitoring	Performance reviews
SF-4	Defined staff handover / changeover procedures	Call Logging Instructions Procedures document
SF-5	Lessons learnt influence training	Lessons Learnt Report

5.2 Service Assurance Wrappers

Typical services comprise several components and consumed services, the integration of which allows the overall SBS to achieve its intent. Where that intent includes control of safety risk, assurance in terms of claims, arguments and evidence is typically provided for each component to provide sufficient confidence that the:

- Behaviours required, with respect to the SBS behaviour, have been correctly specified (including any specific safety targets).
- Behaviour includes consideration of the component's interactions with others and/or the operational environment.
- Component will behave as specified, and only as specified.

The assurance is used at the point of the component's integration into the overall architecture, reconciling what the component offers (both functionally, as well as in terms of any assurance evidence that may be presented for the component's behaviour) with the specific 'needs' of the wider system. When presented for one or more services to be consumed by the parent system, this assurance is referred to as a 'service assurance wrapper'. Hence in a typical service hierarchy, the assurance wrapper is the specific assurance that enables the lower-level service to be safely used by the consuming service. The scope and complexity of a service assurance wrapper will vary to accommodate service characteristics including:

- Criticality of the service (i.e. related to the consequences of the service failing to behave as specified.)
- Service providers being unable or unwilling to provide any or all of the required assurance evidence.
- Change to the service implementation over its lifetime (e.g. due to the service provider's organisation or technology, or due to the replacement of one service provider with another).

A taxonomy for broad categories of service assurance wrapper types is proposed in Table 17. Then, a hierarchical architecture of integrated services, each with an assurance wrapper conforming to one of these declared types, is illustrated in Figure 5.

This taxonomy currently only considers safety explicitly, not other service assurance properties such as business resilience or liability, etc. However, the same approach may well work with these types of attributes.

Note that a wrapper may also need to flow down requirements to the sub-service, which will generally not be safety requirements, but may be other types of requirements. For example, a wrapper may "map" a safety requirement into something else that the sub-service can provide (e.g. compliance to a code of practice).

Figure 5 uses different circle line weights to illustrate how some wrappers may be 'thicker' (more complex, more in-depth) than others. This illustration serves to reflect that wrapper complexity is not a simple function of the class of wrapper (see Table 17), as it will also be influenced by the degree of dependence on the consumed service and the nature of its integration into the overall architecture.

It should be noted that an organisation that develops an assurance wrapper may be the service consumer itself, the service provider, or a third party. However, the consumer of a service remains accountable for the claims made in the associated assurance wrapper. At the highest level of the architecture, where safety risk can be understood, this will be the 'Duty Holder' for the overall system. Finally, note further that different services from the same provider may well require wrappers of different classes.

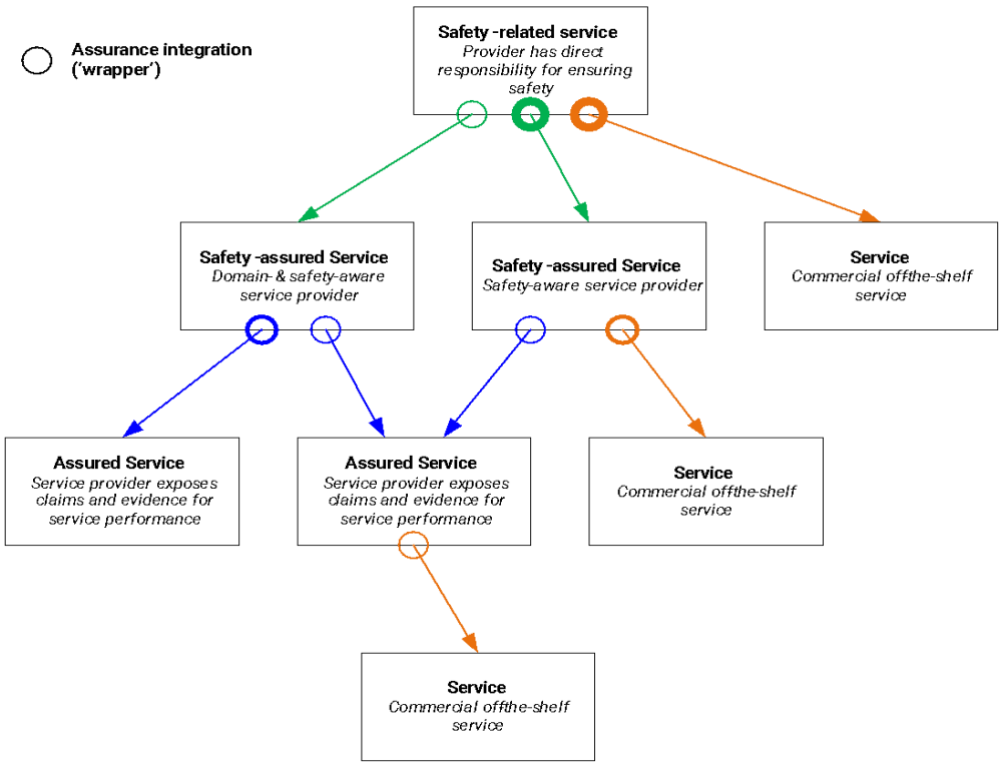


Figure 5 - Assurance Wrappers in Context

(thicker circles denote more "substantial" wrappers)

Notes on wrappers:

- Wrappers bridge the gap between what is required to support an argument of achievement of Service Assurance Level with the assurance available. Some variation cases are apparent:
    - Services can evolve / devolve and may or may not be transparent – needs a different kind of wrapper to protect against unknown changes.
    - If the voracity of any evidence provided cannot be verifiable and/or trustworthy – then it needs a wrapper.
    - A service may provide "different" evidence (e.g. right data but wrong environment) – in this case there is a need for a wrapper.
    - A wrapper may need to impose requirements and/or additional activities on the subsidiary service. These will generally not be safety requirements. They may need to be phrased in terms and concepts that the subsidiary provider can understand and implement.

- Evidence applicability to end user varies.
- Assurance across the service boundary needs to meet LSA, how much of the assurance characteristics are met by supplier and how much by consumer will inform the 'thickness' of the wrapper

Table 17 - Wrapper Classes

Class	Case	Consumer Perspective	Key Functions for Wrapper	Service Provider Response	Notes
Transparent (have visibility downwards)	W1a	Can flow down assurance requirements to a capable, 'safety-aware' supplier that fully understands the consumer's domain.	• Demonstrate safe integration of the service into the consumer's architecture, may include management of any limitations or shortcomings declared for the service. • Demonstrate adequate review of service provider's assurance deliverables. • Demonstrate service provider's compliance with consumer's safety requirements, including standards and legislation • Justify mechanisms by which the provider will alert the consumer to planned and unplanned service changes.	Safety Case (or equiv.)	Can likely justify requirements remaining very high level, as the supplier will fully understand their customer's context.
	W1b	Can flow down assurance requirements to a safety-aware service provider, albeit one that may not fully appreciate the context of use of their service in the consumer's domain.	• As above, but with more robust arguments regarding clarity of requirements & for management of assumptions, to compensate for supplier's lack of domain familiarity. Latter is likely to rely more heavily than would otherwise be the case on the consumer's review processes, to capture any implicit assumptions made by the provider regarding use of their service.	Safety Case (or equiv.)	Example: service providers supported by safety consultancy, or where the provider supports safety of services in other domains

Class	Case	Consumer Perspective	Key Functions for Wrapper	Service Provider Response	Notes
Translation (need to map / translate assurance position)	W2	Can flow down assurance requirements to the service provider, albeit the provider will not respond to them cognisant of the safety implications for their potential misbehaviour.	• As above, with additionally: • Demonstration that evidence provided for the service behaving as specified is sufficient in the context of the dependencies on it. • More robust reporting / control mechanisms for changes to service provision, as the service provider is unlikely to recognise / fully appreciate safety significance of unintended consequences.	SLA, supported by contracted assurance deliverables	The consumer will require a robust specification for all activities the supplier is expected to conduct as well as to set out expectations for the evidence to be provided to demonstrate SLA satisfaction. The service consumer may need to spend time / cost reviewing a service provider's key processes to ensure they are fit for purpose (e.g. change management, performance monitoring, etc.).
Total (may be no visibility)	W3	Assurance Requirements are not flowed down to the provider.	• Wrapper has to (effectively) provide the Assurance Case for both the service and its use. • Claims will inevitably rely on evidence of service performance from extant use (either by the consumer or wider industry). • Wrapper will need particularly robust arguments regarding how the consumer adequately controls impact from changes to the service provision.	SLA	

5.3 Service Assurance Challenges and Solutions

Some further details and discussions are provided below on selected topics.

5.3.1 Service catalogues

The service catalogue offers up a set of defined services for consumption. It is seen as important for assurance purposes as it gives an obvious interface and will include references to Service Level Agreements (SLA), Statements of Work (SoW) or contract requirements that can be used to derive assurance targets. It may turn out to be a key assurance element going forward.

Hence (for IT services, and probably for other services), it is suggested that an approach based on assurance of service catalogues, is a promising step forward. This assurance would then be based on assuring each individual service component or element being offered. The proposed way forward is to define certain key properties from the SLA's (e.g. availability or performance) and then verify that these properties (quantified if possible) are actually achieved and will continue to be achieved. There

may need to be an extended list of candidate properties from which a subset of interest is chosen. Some aspects of the properties are:

- Properties should be defined from the point of view of the service consumer (i.e. based on functional behaviour).
- Properties may be generic to other services.
- Evidence is required (e.g. by testing) that the property is met and will continue to be met. The degree of confidence (e.g. testing thoroughness and rigour) is also important.
- Levels of Service Assurance may help to determine the number of properties considered and the level of verification required.

5.3.2 Types of service provider

Four types of service provider have been identified in a service safety context to date, with their understanding and willingness to engage in safety activities the distinguishing features:

- Those that understand safety, may understand the domain, and likely to be at or near the top-level and/or at the 'sharp end' of delivering safety.
- Those that don't understand safety but can support the service consumer's safety claims.
- Those that don't understand safety now but are interested in developing capability in this area and hence developing safety expertise.
- Those that don't want to, or are uninterested in safety, so provide the service as a 'take it or leave it' or off the shelf basis (i.e. largely 'black box' approach), for example a network provider.

5.3.3 Transfer of Safety Risk

One benefit of using a Service is reduced ownership of specific costs and risks. However, it needs to be decided who is responsible for managing a risk? (it probably depends on the nature of risk and who controls the risk mitigations).

It is recognised that in many cases it may not be possible to hand over ownership of risks to a service provider.

There are many different types of risk including commercial, legal, safety, and regulatory risks. When considering the safety of a system (or product) the primary concern is that all risks to the safety of those exposed to the system are identified and acceptably mitigated. Who is responsible for managing a risk depends on the nature of that risk and the extent to which they have control over the risk mitigations? For example, the manufacturer of a vehicle is responsible for ensuring that the vehicle can be driven safely, but the driver takes responsibility for driving safely, and the vehicle owner takes responsibility for conducting scheduled checks, arranging repairs, etc. Many of the responsibilities for managing risks are set out in regulations or legislation.

One of the defined aims of a service is to facilitating outcomes "without the ownership of specific costs and risks". However, depending on the nature of the risk it may not be possible to hand over ownership, through the service architecture, to a service provider unless they have legal responsibility for or full managerial control over the risk mitigation. A consumer of a service does not necessarily need to know how a service is implemented. For example, as a consumer of electricity in a building I

may need assurance that the supply is highly available and provide mitigation (e.g. in the form of Uninterruptible Power Supply) as part of assuring the safety of my service. But as a consumer I do not have to know about the electricity supply chain, contracts, wiring, etc. or that any of these meet particular standards, so long as I choose reputable suppliers, i.e. those suppliers who claim compliance with the various relevant regulations.

There is clearly a need to define who is responsible for managing risks and to what extent throughout the service architecture. Risk mitigation responsibility will flow up and down the service stack and will need to be captured as part of the service contacts, and the commercial framework needs to provide for this. However, it needs to be recognised that many of the services used in a safety context are generic services, e.g. operating systems, with a variety of consumers (many not safety-related), and the providers may be unwilling to accept the flow down of any responsibilities related to safety risk mitigation. Issues such as availability of generic services, updates, patching, obsolescence, through-life support (especially where the service is a component in a wider system with a very long lifecycle, e.g. defence systems) need to be managed.

5.3.4 Example: What3words

What3words (https://what3words.com) is a free service to the general public that enables individuals to pinpoint their location to a 3m x 3m square anywhere in the world. This leads to 57 trillion squares around the world, with around 25 billion squares just in the UK. Each square is identified by three unique words, with 25,000 words utilised for land and 15,000 words for sea. Both singular and plural forms of words are utilised.

It is acknowledged by what3words (what3words: How does what3words handle similar combinations of words?, Available at https://what3words.medium.com/how-does-what3words-handle-similar-combinations-of-words-d480c94483c7, accessed January 2023) that there is potential for singular and plural forms of words to be confused and also that potential homophones (words spelt differently but pronounced the same) are further compounded by regional accents. Hence, there is potential for errors to be introduced either by the person reading the words out incorrectly (that person is likely to be stressed given what3words is commonly used in an emergency situation), or by the person mis-hearing the words spoken to them (background noise, wind noise, poor signal quality, all compounded by regional accents). There is a further source of error in terms of accuracy of the sender's device (normally a mobile phone) to pinpoint their position utilising GPS etc., although this is commonly only a matter of metres (worse in an indoor location), resulting in location within a neighbouring what3words square. The above errors need to be considered in the context of the alternative of reading out location in the form of latitude and longitude where a long string of numbers can be misread (numbers transposed or omitted) or misheard.

What3words is an accepted form of location identification for the UK Emergency Services. For example, Staffordshire Police (*Guide for emergency call handlers: How what3words helps locate callers and save time,* https://www.staffordshire.police.uk/SysSiteAssets/foi-media/staffordshire/2021-published-foi-requests/august/foi-13491-what3words-data-3.pdf, accessed January 2023) clearly document the process their call handlers follow to establish the location of a caller.

Step 2 of that process involves verification of the identified location by other means (e.g. visual landmarks) - which is a straightforward example of what this guidance document refers to as a "Service Wrapper", i.e. an additional layer of assurance provided by the service consumer.

6 Analysis Techniques (Discursive)

"More and more major businesses and industries are being run on software and delivered as online services - from movies to agriculture to national defense."

Marc Andreessen

6.1 Possible Service Analyses

Can services be analysed using existing traditional safety analysis methods, or is there a need to modify existing or invent new analyses? It is recognised that service failure analyses need to cover people, processes, contracts, and agreements, not just equipment or products. Hence, they could look very different to traditional safety analyses, e.g., use of service blueprint, activity/sequence or Business Process Model and Notation (BPMN) diagrams to find failures. The use of service Hazard and Operability study (HAZOP) keywords for services could be useful to develop and a base set is proposed in Annex A. The analyses need to consider a holistic socio-technical view (e.g. integrating human factors, system safety and security analyses). Table 9 introduced some analyses based on established techniques, as adapted, or modified for services. Note it is not suggested that all of these are performed for every service; a subset will be selected based on the specific service scenario. These techniques are summarised below:

Key

Summary – A high level of summary of the technique.

Applicability – The facets of a service to which the technique would be most beneficial.

Perspective – Whether the technique is "Transparent", i.e., it examines the inner workings or structures of the service being analysed or "Opaque", whereby it provides benefit by analysing the functionality of a service.

Intended Outputs – How the results of the analysis would expect to be presented.

Example – A sample from a worked example of how the technique would be presented.

Benefits – Identifies the benefits from the application of the technique.

Disadvantages – Identifies the disadvantages from the application of the technique.

Table 18 – Service Analysis Techniques

SA-1	Service Functional Failure Analysis (SFFA)
Summary	A high-level analysis which starts with a list of the offered services (e.g. as described in the Service Catalogue), and assesses (i) what typical failures might occur and (ii) the impact of those failures. The emphasis is not on the detailed causes here, but on the visible effect on the offered services. The most effective way of establishing the service failures is by using a team consisting of service delivery experts and the potential service consumer(s). A set of guidewords or failure scenarios may be useful here, such as "Loss", "Delay", "Temporary Outage", "Reduced Throughput", etc. The effect of contractual devices (e.g. penalties in the SLA) can be factored in. This is an important analysis which is conducted early.
Applicability	Applicable to all services
Perspective	Opaque
Intended Outputs	A short tabular analysis akin to Functional Failure Analysis, where each service offered is listed together with its typical failures and their impact on the service consumer.
Example	See Figure 6
Benefits	Identifies the major problems quickly and facilitates early identification of possible wrapper or SLA requirements. Cost effective – good "bang for the buck". Relatively easy to do as largely 'black box' i.e. not concerned with detailed causes, more concerned with effects and impacts.
Disadvantages	Needs inputs from those who consume the service to assess impact; this may not always be clear. May not find the more obscure failures (e.g. common mode) as these require knowledge of the service implementation.
SA-2	**Service Failure Modes and Effects Analysis (SFMEA)**
Summary	This is a more detailed tabular analysis which starts with a list of the offered service elements or components and assesses (i) what typical failures might occur based on the implementation of the service i.e. the sub-services, systems, suppliers or sub-components and (ii) the impact of those failures, at various levels. This technique requires visibility of the service constituent components which may not always be available. The emphasis here is more on the detailed causes. Causes will typically be related to specific deliverables or actions that a sub-component is providing. To enable development of this analysis, service implementation experts and also the service architect are useful people to consult. The resulting impacts of the failure should be compared with the High-Level Service Functional Failure Analysis above.
Applicability	Higher-criticality services (LSA 2+)
Perspective	Largely Opaque
Intended Outputs	A detailed tabular analysis (ideally in a suitable tool) showing the type of failure modes considered and their impact on the service.
Example	TBD
Benefits	Thorough if done properly. Can be expected to identify and analyse many potential problems that arise from single-cause failures.
Disadvantages	Can become very large with hundreds of rows. This can make maintenance and update difficult. Can be difficult to keep the assessment team interested. Won't necessarily find complex cause failures where multiple failures contribute across different components.
SA-3	**Service Hazard Analysis (SHA)**
Summary	This analysis uses a suitable analysis technique (e.g. STAMP/STPA, Fault Tree Analysis) to investigate more complex interactions leading to hazards. Hazards are identified and assessed at the service boundary. Each hazard has a unique identifier. Hazards are assessed on a defined scale of severity and likelihood. A risk classification scheme is used to assign an overall risk level. It may be helpful to use a hazard/sub-hazard approach with two levels (broad-specific).
Applicability	Higher-criticality services (LSA 2+)
Perspective	Transparent
Intended Outputs	Analysis of the service delivery with potential hazards identified.

Example	TBD
Benefits	TBD
Disadvantages	TBD
SA-4	Service Process Model and Notation (SPMN)
Summary	Where the business processes in a service are formally defined using a notation such as BPMN or other formal model, more detailed process analysis can be performed. This systematically considers each element described in the model or notation and asks the "What If?" questions. The results are compiled in a table together with the likely service impacts.
Applicability	Higher-criticality services (LSA 2+)
Perspective	Transparent
Intended Outputs	Table of service failures identified together with their likelihood and severity.
Example	TBD
Benefits	TBD
Disadvantages	TBD
SA-5	Service Decision Analysis (SDA)
Summary	Seen as a high-level technique that considers the types of decisions that are made in scope of the service being provided and how they might affect the overall service provision. This can be used to identify weaknesses in the organisational structure supporting the service provision. It employs the service architecture diagram to systematically consider decisions made by the provider of each service element and decisions impacting across component boundaries (sub-service, subcontractor, supplier, system). The results are then assessed and tabulated.
Applicability	Higher-criticality services (LSA 2+)
Perspective	Opaque
Intended Outputs	Tabular output based on service decision types and their assessment.
Example	TBD
Benefits	TBD
Disadvantages	TBD
SA-6	Service Metrics and Contracts Analysis (SMCA)
Summary	A high-level review of the controlling contractual documents, looking for incentives, instructions or clauses which may impact the safety of the defined service. Typically, these are in the form of penalties for loss of service or drop in performance which are inadvertently linked to a safety issue. An example might be service credits associated with loss of service in a highly data-sensitive service (e.g. prescribing drug data provision in a hospital) but when data is lost or corrupted the safest thing to do is not to bring the service back up, but to investigate and repair the data problem first. The service credit regime should not penalise a proper investigation and careful re-introduction of service. This technique should also consider what behaviours may result in proportion to the penalties applied to service failure/degradation, i.e. committing to a safe service provision because of financial penalties rather than it being the right thing to do.
Applicability	Higher-criticality services (LSA 2+)
Perspective	Opaque
Intended Outputs	Tabular outputs listing i) possible issues / conflicts in the contractual documents where safety could be an issue together with an assessment of the impact, ii) potential behaviours that could be exhibited and their impact on the service provision.
Example	TBD
Benefits	TBD
Disadvantages	TBD

SA-7	Service Structure Analysis (SSA) (Inc. subcontracts/ suppliers/ outsourcing/ offshoring/ gap analysis etc.)
Summary	This analysis considers if the way the service has been constructed could lead to possible problems and issues related to safety. In particular, the way the service has been decomposed into sub-services, systems, and suppliers. Any of the subcomponents could be a weak link and this analysis looks at the levels of the service in turn and assesses any problems (e.g. supplier does not conform with required standards, use of commercial service provider, offshored subcontract, lack of visibility deeper levels of subcontracts). This technique also encompasses consideration of the interactions between services (particularly common sub-services) which might affect the overall service and potential single-point failures in the service through the use of common sub-components (e.g. two different suppliers apparently providing separate services may use the same network provider) or sub-services and suppliers that may fail in the same manner. Elements of this analysis should be considered akin to Common Cause Analysis
Applicability	All services
Perspective	Transparent
Intended Outputs	Report assessing the way the service has been put together and identifying any weaknesses with subcomponents. This would ideally include a tabular consideration of potential service interaction failures, structural failures and single point failures – potential for guidewords alluding to typical interaction failures here, e.g. early/late handshake, unrelated information on an interface.
Example	TBD
Benefits	TBD
Disadvantages	TBD
SA-8	Service-Focussed Organisational Risk Analysis (SFORA)
Summary	This analysis is concerned with the risks related to organisational aspects, i.e. the way that service providers and suppliers run their operation and what might go wrong (so related to business risk / enterprise risk / supply chains / logistics / competence, etc.). It considers weaknesses in the way they are constructed and can assess aspects which might contribute to a service risk such as financial stability, staff turnover, etc.
Applicability	All services
Perspective	Opaque
Intended Outputs	Report on identified issues related to the organisations involved in delivering the service.
Example	TBD
Benefits	TBD
Disadvantages	TBD
SA-9	Service Bow-Tie Analysis (SBTA)
Summary	Traditional Bow-Tie Analysis presents a single visualisation of each main system risk. Shaped like a bow-tie, it shows clear differentiators between proactive and reactive risk mitigations and provides an overview of various credible scenarios in a single picture. In the context of Service Assurance each bow-tie is centred on a hazard resulting from one or more service failures with the mitigations considering the service components. These can include aspects such as human factors, whole system safety and security as well as more traditional component level or control failures. This technique will also support inductive analysis of events in an approach akin to Event Tree Analysis.
Applicability	All services
Perspective	Transparent
Intended Outputs	Service Bow-Tie diagrams showing the analysis for the key service elements. Conclusions and recommendations drawn from the diagrams.
Example	See Figure 7
Benefits	Bow Ties are a useful approach, clear, graphical approach for concentrating the mind on the important safety-related issues of a potential service failure, indicating to engineers and operators alike which facets of the service are Safety Critical.

Disadvantages	Service Bow Ties suffer from the same main issues as traditional system Bow Ties. They represent the risk reduction mitigations akin to layers in James Reason's Swiss Cheese Model but not the specific holes in the cheese, and consequently can be seen to paint an overly optimistic picture of the service risks. Equally, representing the mitigating facets of the service being provided (the green bordered boxes above) in this way can give the impression that they are both independent and effective when real systems rarely have mitigations that can be considered entirely independent. It is also important to recognise that the quantity of mitigating facets to a service do not equate directly with a level of confidence in that overall service being delivered safely.
SA-10	Service-Focussed Systems Analyses (SFSA)
Summary	This is the use of established analysis techniques in a service setting. Some work has been done on STAMP/STPA, which shows promise but more needs to be done. See an initial example in Annex I.
Applicability	Potentially all services
Intended Outputs	Appropriate analysis report
Example	TBD
Benefits	TBD
Disadvantages	TBD
SA-11	Service-Related Historical Accident and Incident Report Analysis (SHAIR)
Summary	This report identifies significant historical accidents and incidents related to this service (so for example, considering the problems for the same or similar service has been provided by the same service provider in another setting). Significant events are then analysed to see if they could occur in this service instance. This obviously relies on access to data from service providers and suppliers which may be hard to obtain. Non-disclosure agreements may be required. It is likely this approach will link to many of the other techniques listed herein based on the type(s) of service being analysed.
Applicability	All services
Perspective	Opaque
Intended Outputs	Report considering related incidents and accidents and an assessment as to whether they could occur within this service setting.
Example	TBD
Benefits	TBD
Disadvantages	TBD
SA-12	Service Functional Resonance Analysis Method (SFRAM)
Summary	Looking at analysis of functions undertaken relating to a service either retrospectively or prospectively.
Applicability	All services
Perspective	Opaque
Intended Outputs	Event tree diagrams showing the likely impact of failures within the service together with an assessment of severity and likelihood.
Example	TBD
Benefits	TBD
Disadvantages	TBD

Example SFFA worksheet: Provision of Accurate Timing Signal

Identification				Service Provider						Contract and SLA		Service Consumer(s)					Risk
Service Catalogue ID	Service (Component) Name	Potential Failure of Service	Service Failure Type	Possible cause(s)	Estimated Likelihood	Typical Duration	Service Restoration Time	Detection Methods	Possible Mitigations / Workarounds	SLA Weaknesses	SLA Strengths	Immediate Effect	Detection Methods	Possible Mitigations / Workarounds	Assurance Wrapper Considerations	Impact on Higher-Level Consumers	Service Risk Level
1.1	UTC Time	Time drift away from UTC	Accuracy	Jamming; Receiver develops fault out of maintenance contract; Service out of contracted support hours	Once a month	Few minutes	< 10 minutes	Large drift would be detected by other systems	Small drifts are within the SLA limits. Redundant time server architecture with voting.	Problem may occur outside of contracted support hours.	Quantified accuracy, drift and restoration time clauses may be explicit in SLA; Remedies may be payable	Service Consumer receives drifted time	Large drift would be detected by other systems	Small drifts are acceptable and can be managed. Backup time service provider can take over in slower time.	Need to establish and assure (i) Jamming susceptibility; (ii) Maintenance contract provision; (iii) Support contract hours	Could be many; all functions and services that need accurate time could be affected	Low
1.1	UTC Time	Complete loss of time service	Availability	Hardware problem; Software bug; Mis-maintenance; Bad patching; Security problem; Hardware or software out of maintenance contract; Service out of contracted support hours	Once a year	Some time if outside contracted support hours	< 1 day	Many other systems and services would detect the failure	None at individual Service Provider level.	Problem may occur outside of contracted support hours.	Quantified availability clauses may be explicit in SLA; Remedies may be payable	No timing service available to Service Consumer	Many other systems and services would detect the failure	Backup time service provider can take over in slower time.	Need to establish and assure (i) Patching process; (ii) Security processes; (iii) Maintenance contract provision; (iv) Support contract hours; (v) Supplier hardware quality processes	Could be many; all functions and services that need time could be affected	Medium
1.1	UTC Time	Incorrect time given by time service	Integrity	Operator error; Software bug; Mis-maintenance; Bad patches; Security problem	Once evey 10 years	Some time if outside contracted support hours	< 1 day	Many other systems and services would detect the failure	Redundant time server architecture with voting.	Problem may occur outside of contracted support hours.	Quantified integrity clauses may be explicit in the SLA; Remedies may be payable	Incorrect time given to Service Consumer	Many other systems and services would detect the failure	Backup time service provider can take over in slower time.	Need to establish and assure (i) Change processes; (ii) Operator compentencies; (iii) Maintenance contract provision; (iv) Support contract hours; (v) Supplier software and hardware quality processes	Could be many; all functions and services that need the correct time could be affected	Medium

Figure 6 – Service Functional Failure Analysis Example

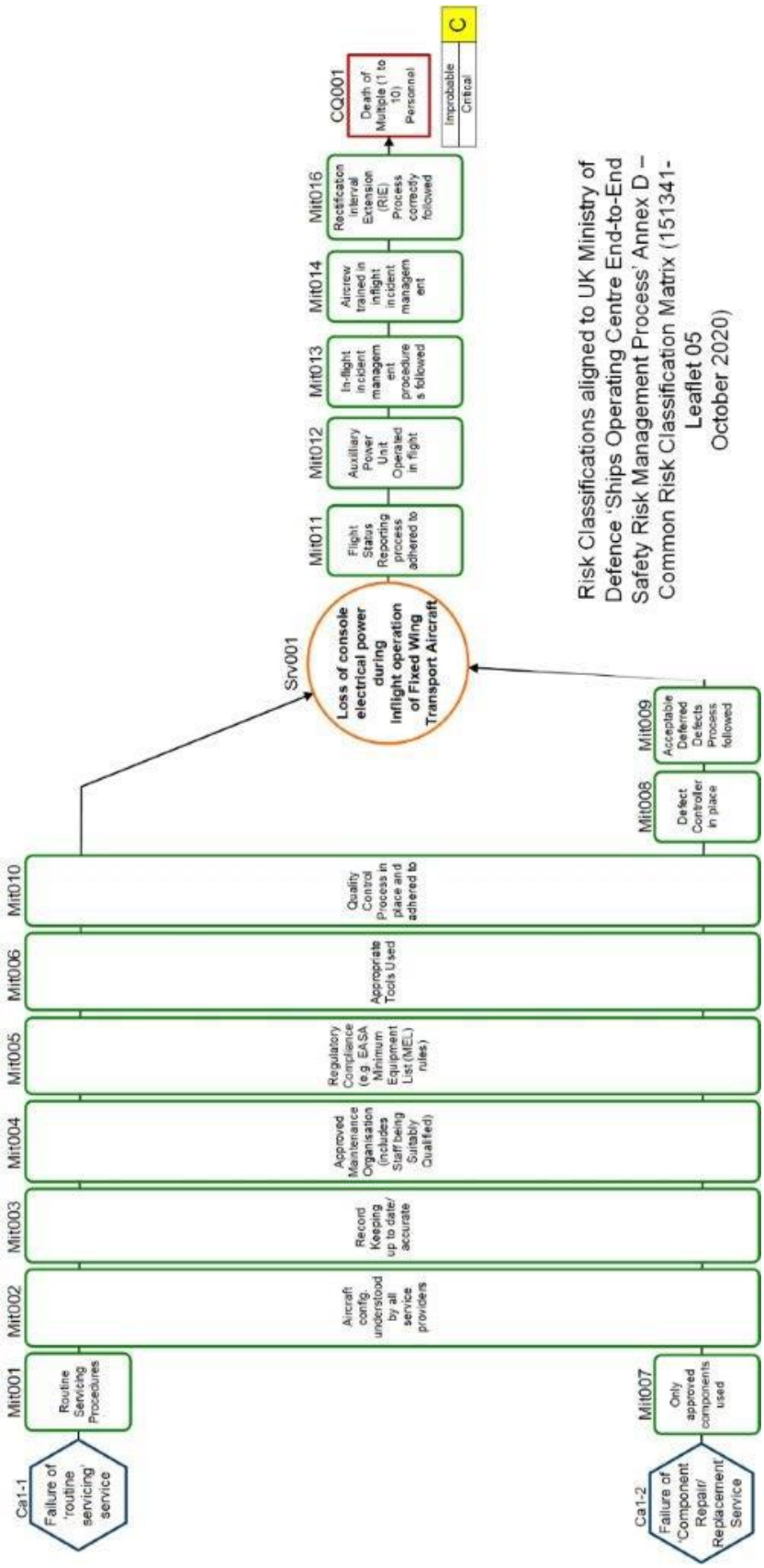


Figure 7 – Service Bow-Tie Analysis Example

This page is intentionally blank

7 Service Mode Changes (Discursive)

"If we do not lay out ourselves in the service of mankind, whom should we serve?"

John Adams

7.1 Service Ramp-up and Rapid Creation

When a service is expanded rapidly to cope with increased demand (e.g. the UK Covid-19 Test and Trace service in 2020) there may be new and unexpected safety risks created. An increased level of service may require re-consideration of the aspects set out in Table 19.

Table 19 – Service ramp-up aspects

Service Aspect	Associated Risks
Technology	New technical risks (e.g. unexpected behaviours) due to changed hardware, software or data
Staff	Use of poorly trained, inappropriate or inexperienced staff who do not 'know the ropes' could lead to more errors being made. Shift and staffing arrangements will need to be reworked.
Connectivity	Bandwidth required may be estimated and not sufficient for full operation (e.g. network bandwidth). Unexpected dropouts may occur.
Operating modes	Additional or modified operating modes of the service may be required (e.g. sites operating at changed capacity, dual running), requiring new procedures, processes and staffing. Sites may need re-configuration.
Management and reporting	New management staff, tools and reports require recruitment, installation, and definition. All may have problems initially.
Geographical sites	Distance and location may present new risks (e.g. network delays, power problems, susceptibility to fire, flood.)
Suppliers and contracts	New arrangements will have to be made with new and existing suppliers involving working practices, contracts and agreements
Backup, failover and resilience	New arrangements need to be put in place to ensure the increased service can cope with failures e.g. to cover new geographical locations
Security	An increased footprint and more sites present more openings for security threats. New staff may not have been fully trained, checked and cleared.

Obviously, this depends largely on the scale of the increase. If the service is still within design limits, there may be limited change. However, there will come a point when the existing service design cannot cope and more resources or a redesign may be required.

There are then potential issues including:

- Transition to new technology
- Parallel and dual running
- Handovers
- Mixed systems
- Additional / duplicate service providers needed

7.1.1 Service Analysis Techniques for Ramp-up

Where a service is being ramped-up or rapidly created then it is likely time will be critical in ensuring all facets of the service remain acceptably safe. To achieve this the more appropriate Service Analysis techniques (see section 6) are considered in Table 20.

Table 20 –Beneficial analysis techniques for service ramp-up

Analysis Technique	Benefits
Service Functional Failure Analysis (SFFA)	It is expected that failures of all safety-related functions within the service being ramped up will have previously been analysed using this technique when the service was first created. That analysis could be revisited to understand the impact from increased pressures on those functions due to ramp-up.
Service Decision Analysis (SDA)	Ramping up a service, or indeed rapid creation of a service can result in an increase in the stresses and weaknesses across a service architecture and organisation. This is where SDA could provide benefit. It may also identify weaknesses in an organisation not previously considered due to the ramp-up.
Service Structure Analysis (SSA)	Like SDA, unexpected pressure could be put on some of the structures of a service's architecture due to ramping up or rapid creation of that service. Common sub-components of a service may be able to cope within scope of their original contracted provision, however when the parent service is ramped up they may be put under unexpected stresses that increase their risk of being unable to deliver their function, e.g. due to lack of competent resource or need for extra network bandwidth.
Service-Focussed Organisational Risk Analysis (SFORA)	In ramping up a service there may be a need to restructure an organisation. Until that new organisational structure has bedded in there may be weaknesses within it that impact on service delivery. By analysing organisational risk from a service perspective during design of the new organisation the impact on delivery of the service can be better understood.

7.2 Service Ramp-down

Conversely, when a service is shrunk rapidly to cope with reduced demand (e.g. Air Traffic Control services in 2020 were reduced drastically due to the Covid-19 pandemic) there may also be new and unexpected safety risks created. A much-reduced level of service may require re-consideration of the aspects set out in Table 21.

Related to this is where it is not possible to ramp-down as quickly or effectively as needed, creating *service under-utilisation*. This can be a major problem as staff can have issues of focus, boredom and loss of competency, systems may not be maintained properly and elements of the service depending on timeliness or throughput may suffer degradation e.g. supply chains providing fresh food.

Table 21 – Service ramp-down aspects

Service Aspect	Associated Risks
Technology	New technical risks (e.g. unexpected behaviours) due to removal/mothballing of sites, hardware, software or archiving of data
Staff	Experienced staff who 'know the ropes' may be moved to other areas or made redundant leading to more errors being made. Staffing may be spread too thin to be effective, or shifts may be extended, also staff may struggle to keep focused.
Connectivity	Bandwidth contracted/available may be reduced and may not be sufficient for operation
Operating modes	Reduced operating modes of the service may be required (e.g. sites mothballed or operating at reduced capacity)
Management and reporting	Reduced staff, tooling and reporting require changed procedures and oversight
Geographical sites	Loss or mothballing of a site may lead to issues with distance and location (e.g. power, connectivity, susceptibility to fire, flood)
Suppliers and contracts	New arrangements will have to be made with suppliers for reduced supply involving working practices, contracts, and agreements. Contracts may be de-scoped or cancelled altogether, invoking "Force Majeure" clauses.
Backup, failover and resilience	New arrangements need to be put in place e.g. to cover reduced geographical locations
Security	Reduced staffing may present more openings for security threats as there is less oversight. Remaining staff may lack experience in security issues.

7.2.1 Service Analysis Techniques for Ramp-down

Where a service is being ramped down then it could reasonably be expected that the resources in place to support that service will be reduced or reallocated, with potential consequential impact on safe delivery of the service. To ensure the service remains safe the more appropriate Service Analysis techniques (see section 6) are considered in Table 22.

Table 22 –Beneficial analysis techniques for service ramp-down

Analysis Technique	Benefits
Service Functional Failure Analysis (SFFA)	It is expected that failures of all safety-related functions within the service being ramped down will have previously been analysed using this technique when the service was first created. That analysis could be revisited to understand the impact from reduced resources in place to support the service due to ramp-down.
Service Decision Analysis (SDA)	The speed of decisions and promptness of reaction to address issues of service delivery could well be impacted if a service is ramped down, personnel allocated to support a service could see it as a lesser priority to a different task resulting in reduced focus and scope for increased risk of service failure. This is where SDA could provide benefit. It may identify areas in an organisation that require strengthening to avoid those increased risks, specifically due to the service being ramped down.
Service Structure Analysis (SSA)	Common sub-components of a service may be able to cope within scope of their original contracted provision, however when the parent service is ramped down the sub-components may be put under unexpected stresses due to reduced staffing or resources that in turn increase their risk of being unable to deliver their function.
Service-Focussed Organisational Risk Analysis (SFORA)	Equally in ramping down a service there may be a need to restructure an organisation. Until that new organisational structure has bedded in there may be weaknesses within it that impact on delivery of the reduced service. By analysing organisational risk from a service perspective during design of the new organisation the impact on delivery of the service can be better understood.

7.3 Service Reconfiguration

When a service needs to adjust to cope with changes in required provision (e.g. petrol/gas stations may require a complete change to cope with electric vehicles) there may be new and unexpected safety risks created. Any such changed service may require re-consideration of the aspects set out in Table 23.

Table 23 – Service reconfiguration aspects

Service Aspect	Associated Risks
Technology	New technical risks (e.g. unexpected behaviours) due to changed sites, hardware, software or data. Changes take time to 'bed in' and become established.
Staff	Staff who 'know the ropes' may be made redeployed / re-tasked to new areas leading to more errors being made. New and inexperienced staff may be brought in. Staff may be unsettled due to changes and uncertainty. Training materials may need to be updated and staff retrained.
Connectivity	Bandwidth contracted/available may be reduced and may not be sufficient for operation.
Operating modes	New or different operating modes of the service may be required.
Management and reporting	New or redeployed staff, tooling and reporting require changed procedures and oversight. Interfaces and contact points change.
Geographical sites	Change or re-purposing of a site may lead to issues with distance and location (e.g. staff travel, power, connectivity, susceptibility to fire, flood)
Suppliers and contracts	New arrangements will have to be made with suppliers for changed supply involving working practices, contracts, and agreements. Contracts may need to be updated, replaced or terminated.
Backup, failover and resilience	Changed arrangements may need to be put in place e.g. to cover different geographical locations.
Security	Changed staffing may present more openings for security threats as there may be new areas to cover or reduced oversight.

7.4 Re-purposing of Services

Services can often be re-purposed quickly as they are adaptable and flexible. For instance, the creation of a national vaccination service with the use of re-assigned NHS staff to deliver huge quantities of vaccine into the general public during the Covid-19 pandemic.

Re-purposing is different to the cases considered above, but there are similarities in terms of impact. The main thing to consider is have all the risks for the new intended use been considered and addressed in the new use of the service?

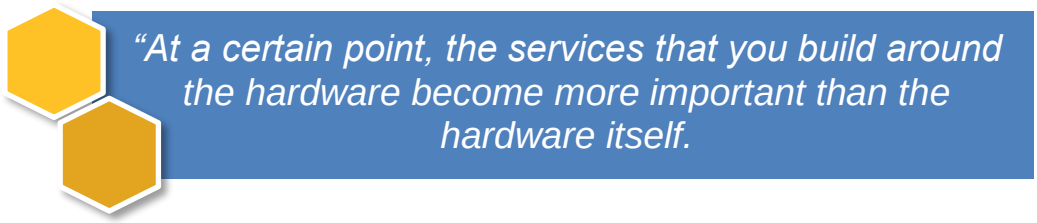
Table 24 – Service re-purposing aspects

Service Aspect	Associated Risks
Technology	New technical risks (e.g. unexpected behaviours) due to changed use, particularly with hardware, software and supporting data. Can the technology cope with the new use of the service as well as existing uses? Changed use will take time to 'bed in' and become established.
Staff	Staff who are well established may not be adaptable, aware, or familiar enough with the new use leading to more errors being made. New and inexperienced staff may be brought in. Staff may be unsettled due to changes and uncertainty. Training materials may need to be updated and staff retrained.
Connectivity	Bandwidth contracted/available may not be sufficient for operation.

Service Aspect	Associated Risks
Operating modes	New or different operating modes of the service will almost certainly be required and may require several phases of change.
Management and reporting	There may be new clients with different reporting needs. Interfaces and contact points may change. New or redeployed staff, tooling and reporting require changed procedures and oversight.
Geographical sites	Change or re-purposing of a site may lead to issues with distance and location (e.g. staff travel, power, connectivity, susceptibility to fire, flood).
Suppliers and contracts	New arrangements will have to be made with suppliers for changed supply involving working practices, contracts, and agreements. Suppliers may need to be notified of the new use. Contracts may need to be updated or replaced.
Backup, failover and resilience	Changed arrangements may need to be put in place e.g. to cover different geographical locations, particularly if any new clients are in new areas.
Security	New uses may create new threat vectors. Changed staffing may present more openings for security threats as there may be new areas to cover or reduced oversight.

This page is intentionally blank

8 When Services Go Wrong (Discursive)



This section recognises that services do not always work as intended and that failures in parts of a service can lead to reduced capability and revised assurance approaches.

In general, a service provision needs to consider:

1. Service collapse (i.e. part or all of the service is lost),
2. Reduced performance,
3. Contingency, and
4. Recovery.

Typically, a full or complete service is replaced by "contingent service" (degraded service) when something goes wrong. This can be because parts of the service are completely missing, as well as particular (sub)services not operating optimally. When this happens there are several mitigation approaches:

- A common approach is to revert to manual means i.e. people, paper and process, (e.g. as used in a hospital if there is an IT failure).
- It may be possible to use alternate service suppliers (possibly with less assured offerings), for example an alternate refuse collection service. It is recognised that backup or alternate services also need to be resilient – i.e. utilising simple backup systems and processes (e.g. phone, paper).
- If no workaround or alternate service supplier can be found, it is possible that limitations may have to be introduced, for instance by reducing throughput, e.g. slowing down the traffic on highways, railways or air traffic, so that a degraded service can cope.
- Alternate ways of managing the risk can be introduced using simpler (typically more manual) assurance processes (e.g. block operation on railways).
- The degraded or alternate service supply will often be much more people-focussed, i.e. often a failed or degraded IT-based service becomes a human-centric service implementation with people providing the functionality and assurance (e.g. by signing pieces of paper). This means staff need to be trained and ready to take over.
- Any contingent operating mode is likely to rely on knowledge and experience of trained operators. The people factor should not be forgotten, especially when things are operating normally. Skills and training for degraded modes of operation will need to be maintained and refreshed over time.

So, what happens to the assurance position when operating in this type of situation? There may be several possibilities:

- The assurance may be reduced or degraded in some cases. This may be acceptable as long as it has not dropped too far (i.e., beyond some defined threshold) or becomes out of date.
- It may be acceptable to have reduced assurance position for a specific duration, e.g., operating licences or working practices may allow assurance to be below normal for up to X hours within any defined period.
- In other cases, it may be that the manual or changed assurance position may be more robust (slower, simpler) and so less assurance is required.

One important factor is how the service is restored. This should be part of the service assurance position and should be regularly rehearsed and practised.

- It will require suitably detailed processes and procedures which minimise disruption.
- It may have to preserve data acquired by the contingent (degraded) service, and somehow add it back to the restored service (e.g., paper records have to be transcribed back into the electronic systems).
- Restoration must be scheduled carefully to minimise downtime and disruption.
- If the restoration fails, it must be possible to revert and continue with the degraded service for the time being.
- Parallel running of both the restored and degraded services should be considered.

So, it is clear that the whole service assurance position has to include:

- The assurance for the main (normal operating) service.
- Assurance for any foreseeable degraded service mode(s).
- Assurance for the service restoration.

9 Services Across Boundaries (Discursive)

> *"We shall never be able to remove suspicion and fear as potential causes of war until communication is permitted to flow, free and open, across international boundaries"*
>
> Harry S Truman

It is recognised that services do not always cleanly lie within one region or indeed, country or jurisdiction. In fact, the way that many web-based services are now constructed using multiple distributed sub-services in the cloud makes it hard to see where services are coming from (and also where they are going to).

The accident in the Mont Blanc tunnel in 1999 in which 39 people died is an example of services across national boundaries, https://en.wikipedia.org/wiki/Mont_Blanc_tunnel_fire (this accident is further analysed from a services point of view in a paper presented at SSS'23: https://www.amazon.co.uk/gp/product/B0BQ9N23YY). The accident highlights many aspects of cross-boundary services that have potential problems - in this case uncoordinated actions on both ends of the tunnel made things much worse. This accident then led to changes in the operation of tunnels to require one operating authority to be in charge rather than individual national authorities.

Boundaries within a service are not always explicit or obvious to the service consumer. An example might be the way the NHS (the UK **National** Health Service) is decomposed into regions which have their own budgets. Long-term care patients (in this case the service consumer – of a national service) may be bounced from one region to another because one region does not want to fund their care costs.

There may also be temptations to push parts of the overall service provision to lower-cost geographies where employee welfare is at a lower standard than where the service is consumed (e.g. use of call centres in lower cost geographies where working practices are not subject to the same regulatory / standards environment as that in place where the service is consumed). There is a then an obligation on the overall service provider to make the case that the overall service-based-solution is appropriate.

The table below highlights some of the things to consider when service provision is across boundaries, especially where there are complex services constructed of other systems or services:

Table 25 – Potential Issues with Services Across Boundaries

Service Aspect	Potential Issue
Contract and Contract Duration	Contract end dates need to be synchronised across sub-services. An example is a supply delivery contract for a part of a service (or for, e.g. contract staff) which runs out before the overall top-level contract, leaving the service without key staff. Also some contracts (e.g. for insurance) may be renewed regularly (e.g. annually), with different providers each year, possibly creating new boundaries on a regular basis.
Legal	There may be different legal or risk management regimes in play on different sides of the boundary, especially where safety is involved. For instance ALARP is only applicable in the UK and other countries have different schemes.

Service Aspect	Potential Issue
Languages	Language and communication across international boundaries can present real problems. International organisations such as the UN or EU expend a lot of effort to ensure that legislation and communications are translated to overcome these barriers. Important information about service aspects can also get lost in translation, for instance what is expected of a 'working day' or physically lost if paper documents.
Cultures	Different cultures and expectations of staff (e.g. working hours and national holidays) are important, not only between the organisations involved but also across national / international boundaries. Special efforts have to be made to enhance integration and joint working in such situations, e.g. creation of a single set of working practices.
Standards	Different standards (including safety standards or guidelines) may be in use for the various subcontracts and sub-services, especially if these are international. The difference with systems here is that many services will be consumed as-is, and there may be limited opportunity to flow-down safety requirements and standards to international service providers. An example might be the supply of electricity across the channel connector via the HVDC Cross-Channel (https://en.wikipedia.org/wiki/HVDC_Cross-Channel). In this case some sort of assurance wrapper may be required to map from one standards regime to another. Note also HS1 in UK was largely built to French standards.
Units	Different units or technical norms may be an issue (e.g. metric/imperial)
Business Practices	Different business practices, expectations and ways of working may be used across the range of service providers, for instance covering hours of availability, approaches to staff absences, etc.
Agreements	It may be necessary to create specific agreements to cover who is responsible, is in charge or who takes over in certain situations, particularly in service introduction, contingency or recovery stages. There may also need to be specific agreements for liabilities. Note a joint agreement on how to handle a situation may become null and void if one organisation decides to walk away from their contract or goes bust.
Communications	Special communication provisions may need to be provided, e.g. hotlines, so that urgent and critical communication can be ensured across the boundary if there are problems.
Jurisdiction	Jurisdiction may need to be modified for the service (e.g. it is sometimes useful to consider part of a railway to be in another jurisdiction).
Boundary Definition and Gaps	Poorly defined or ambiguous boundaries is a real issue, as both parties may think they are covering the gap, or in fact, neither are. Gaps between service boundaries may be explicit or implicit and may open inadvertently. For example the Wimbledon derailment, https://www.gov.uk/government/publications/safety-digest-012018-wimbledon/derailment-of-a-passenger-train-near-wimbledon-south-west-london-6-november-2017
Environmental and Ethical Aspects	Service provision may be delivered using organisations that are located in areas of the world that don't or can't want to work to high environmental or ethical standards. In this case the overall service provider, who is presumably moving the service provision element to reduce costs, needs to justify to their stakeholders (shareholders, consumers, …) that what they are doing is appropriate.

10 Further work (Discursive)

"No enterprise can exist for itself alone. It ministers to some great need, it performs some great service, not for itself, but for others; or failing therein, it ceases to be profitable and ceases to exist.."

Calvin Coolidge

Several areas for further work in service assurance have been identified during discussions in SAWG meetings. All of these are considered useful research areas in which to identify and document best practice.

- The issue of possible **Inter-service Interference** (e.g. where consumption of two or more apparently independent services causes degradation of one or both as they make use of the same underlying resources: common sub-services or people, equipment, IT infrastructure, etc.)
- Problems due to **Unintentional or Undesired Service Provision** (e.g. where a service is consumed because it is readily available, but the service provider has no knowledge or intention for the service to be consumed this way. Examples might be the harvesting of radio waves to power small Internet of Things (IoT) devices, or use of unsecured WiFi networks.)
- Problems of **Obtaining Information** from some service providers. In particular it may be difficult to obtain technical details to allow completion of safety analyses and other evidence, as often service implementation is hidden.
- It can be difficult in a complex service hierarchy to see how the risks are completely addressed, as **Risks may be Managed at Different Service Layers**. Related to this is the issue of managing and transferring risks between Service Layers (risks not properly managed at one level may need to be addressed at a higher level). A mechanism for formally transferring risks between service layers is needed. This may be similar to risk transfer in systems, but there are added complications due to wrappers.
- **Identification and Management of Emergent Properties** (the way a service is constructed may lead to undesired or detrimental properties emerging through the interaction of services in the hierarchy). New analysis methods will likely be needed to identify these.
- **Analysis of Contractual Documents** (i.e. technical and legal analysis of Service Level Agreements (SLAs) and Statement of Work (SoW) documents may be required, and conclusions for the assurance case produced. This may require specialist legal or commercial skills. This is to be covered in one the proposed analyses in section 6.
- The Service Level Agreements become very important and will determine behaviours of the service provider. It is therefore paramount to have some degree of **SLA Confidence** (i.e. there needs to be a way of establishing that a specific SLA will be met). This is to be covered in one of the proposed analyses in section 6.
- **Meeting As Low As Reasonably Practicable (ALARP)** may need to be considered for services. This is especially true when a service provider potentially doesn't know which of

their services (or specific characteristics of specific services) will subsequently be relied on to satisfy some higher-level safety claim.

- **Who is Responsible for Assurance?** It is necessary to establish who is (i) responsible for the assurance for each service in a service stack, and (ii) who will produce the assurance. However, the picture could be complex and not all providers will want to do this or be able to do this. It seems clear that each service provider or supplier is responsible for their "level" in the stack, but they may use 3rd party assurers to produce the assurance. In some cases the next level up in the stack may have to produce the assurance.
- **Contracts May Need Additional Assurance Aspects.** Note that failures may propagate across service layers which may result in the need for assurance requirements for notification, including auditing, corrective actions, etc. to be placed in the procurement documents and contractual set.
- **Security**. It will be necessary to feed in outputs of security analyses into the service assurance picture to give "security informed services".
- **Examples of Convincing and Compelling Arguments** that a Service-Based Solution is acceptably safe (e.g. using Goal Structuring Notation (GSN) or Claims, Argument and Evidence (CAE)) would be very useful.
- It would be useful to provide a set of **Assurance Argument Patterns**, i.e. a limited number of common patterns for typical Service Assurance arguments. These need to be identified, abstracted, and established. This will need to refer to modular assurance: there is a natural mapping from service decomposition to modules within a modular assurance argument. The service definitions and SLAs may also map to interfaces between modules.
- **Changes to COTS**. It is noted that many COTS items may be utilised to deliver services, but they are often modified or configured through their deployment in the service stack, and this usage may be different from a reference architecture. Understanding how any configuration or usage changes can influence service behaviours is essential to constructing the assurance picture.
- It would be useful to explore **Mappings** between this guidance and other related guidance and standards, in particular in the areas of risk classification and assurance levels,
- **Links between Analysis Techniques**. The guidance would benefit from a table identifying linkages between different service analysis techniques.
- Development of a detailed **Worked Example** for inclusion in future versions of this guidance.
- Examine synergy with the **UK NHS health informatics standards** DCB0129 and DCB0160 re: deployment, use, maintenance or decommissioning of Health IT Systems within the health and care environment.
- Consideration needs to be given to **notify identified but unmitigated hazards to all users across all service instances** (a bit like the recall of goods approach used in manufacturing)

- In terms of **Software as a Service** the following need to be considered:
    - How to safely manage the introduction into service of multiple releases a year of platform-based software
    - How to safely manage software that by its nature contains a large amount of end-user configurable components
    - How to manage growth limits and the unexpected consequences of running out of storage on cloud platforms
    - For healthcare, how to safely manage clinical decision support and AI driven components
    - Perhaps one of the biggest challenges in healthcare is around the growing use of internet of things devices and also apps for specific health condition which often have no integration into the wider system landscape

If you are interested in any of these areas please contact the SAWG via the SCSC web site (scsc.uk, thescsc.org).

This page is intentionally blank

Annex A Service-Related HAZOP Guidewords (Informative)

"A company is a group organized to create a product or service, and it is only as good as its people and how excited they are about creating..."

Elon Musk

A.1 Interpretation of guidewords to support identification of Service-related Hazards

In support of the analysis techniques proposed in section 6 a set of service-related guidewords (Table A-1) and trigger words for service-related hazards (Table A-2) have been developed. These will be evolved further in the next version of this guidance.

Table A-1 - Service-Related Guidewords

Guideword	Meaning
No (not, none)	The Service is not provided. None of the activities are completed to maintain the service.
More (more of, higher)	Quantitative increase in service provision
Less (less of, lower)	Quantitative decrease in service provision
As well as (more than)	An additional activity occurs as part of the service
Part of	Only some of the service design intention is achieved
Reverse	Logical opposite of the service design intention occurs
Other than (other)	Complete substitution of service component activity — another component service activity takes place, or an unusual service component activity occurs, or uncommon condition exists
Where else	Applicable for service flows, transfer of service provision and sources of service
Before/after	A service step (or some part of it) is affected out of sequence
Early/late	The timing of one or more service component activities (or the whole service) is different from the intention
Faster/slower	One or more service component activities (or the whole service) is provided/not provided with the right timing

A.2 Trigger Words to consider when identifying Provision of Service Hazards

Table A-2 - Trigger words for Service-Related Hazards

Guideword	Meaning
Provision of Service	
Design Compliance	Service is compliant with its design intent.
Operational Manuals	Operational manuals support safe provision of the service.
Performance Parameters	Performance parameters support safe provision of the service.
Reliability	The reliability of the service conforms with contracted expectations.
Availability	The availability of the service is within expected/contracted boundaries.
Incompatibility of components	Safe service provision is negatively impacted by incompatibilities across components of the service.
Emergency Shutdown Procedures	Emergency procedures ensure the service is shutdown in a safe manner.
Options for isolation of service in an emergency	The service can be safely isolated in an emergency.
Utility failure	Service provision caters for utility failure (e.g. electricity).
Exposure to external sources	Safe service provision is not negatively impacted by external sources of fire, hazardous materials etc…
Corrosion	Service provision is negatively impacted by corrosion.
Leakage/Spills	Service is impacted by the leakage/spillage of constituent chemicals (e.g. lubricants) that support a safe provision of service or are a component of maintaining the service.
Service Maintenance	
Materials	Materials required to support the service are appropriate in conformance with the design intent.
Storage	Materials that support the service are appropriately stored.
Storage	Where the service includes data management sufficient/appropriate storage is available.
Data	Data generated by or required by the service is appropriately managed and in a format that meets the design intent.
Time Constraints	Service delivery or maintenance is not constrained by time.
Tools	Appropriate tools are used to deliver or maintain the service.
Ordnance, Munitions, Explosives (OME)	Appropriate measures are in place to ensure a service managing any items classed as OME can be conducted or maintained safely.
Orientation/Layout	The system structure, orientation and layout does not hinder safe use or maintenance of the service.
Service Manuals	Manuals describing the service provision are clear, and straightforward.
Improper Access/Egress	Service guards against improper access/egress during use and maintenance.

Guideword	Meaning
Evacuation	Service facility supports evacuation for service personnel in the event of an incident/emergency.
Electrical Hazards	The service is encapsulated to prevent exposure to electrical hazards during use or maintenance.
Safeguards during Maintenance	Safeguards are in place during maintenance of the service.
Potential ignition source(s) during maintenance	There are no potential ignition sources that service users or maintainers can be exposed to in an unsafe manner.
Environment	
Extreme Weather	Safe service provision is not adversely affected by extremes of weather.
Extreme Temperatures	Safe service provision is not adversely affected by extremes of temperature.
Radio Activity	Safe service provision is not adversely affected by radio activity.
EMC	Safe service provision is not adversely affected by issues of Electro Magnetic Compatibility (EMC).
Location	The location of a system does not adversely affect safe service provision.
Incompatibility of stored material	Materials required to support the service are appropriately stored, separate from other conflicting materials.
Fire	Service is not susceptible to fire, and where it is suitable preventative measures are in place.
Human Factors	
Training	Personnel delivering the service are appropriately trained.
Competence	Personnel delivering the service have appropriate knowledge and experience to undertake it safely.
Hazardous Materials Exposure	Personnel are not exposed to hazardous materials in provision of the service.
Heavy Loads	Personnel are not exposed to heavy or awkward loads (e.g. equipment requiring multiple person lifts without additional support) in provision of the service.
Confined Spaces	Personnel are not exposed to unacceptably confined spaces to safely provide the service.
Security	
TBD	

This page is intentionally blank

Annex B Incidents and Accidents (Discursive)

"I entered the health care debate in response to a statement in the United States press… which claimed the National Health Service in Great Britain would have killed me off...I felt compelled to make a statement to explain the error.."

Stephen Hawking

B.1 Overview

The examples discussed in this annex are incidents and accidents from across industry where service failures are considered to be significant contributory factors. Viewing these incidents from the services perspective demonstrates that a service assurance case based around the principles in this guidance is relevant, necessary and should be considered as a key element when developing a systems safety case. The events discussed herein have been pulled from publicly available reports and selected arbitrarily. They cannot be considered in anyway exhaustive.

Note: The analysis presented has no legal standing whatsoever. The purpose of this appendix is not to discredit, contradict or challenge any existing accident analysis; the aim is simply to view these events from the perspective of service failures.

B.2 Case Study – Deepwater Horizon

On the evening of 20th April 2010, a well control event allowed hydrocarbons to escape from the Macondo Well onto Transocean's Deepwater Horizon which resulted in explosions and fire on the rig. Eleven people lost their lives, and seventeen others were significantly injured. The fire, which was fed by hydrocarbons from the well, continued for 36 hours until the rig sank. Hydrocarbons continued to flow from the reservoir through the wellbore and the blowout preventer for 87 days, causing the largest oil spill in US waters. The US Coast Guard estimated 5000 barrels a day were leaked into the Gulf of Mexico (BBC, 2010).

The Deepwater Horizon Accident Investigation Report (BP, 2010) summarised the accident was propagated by a well integrity failure, followed by a loss of hydrostatic control of the well. Subsequently, a failure to control the flow from the well with the blowout preventer equipment, allowed the release and subsequent ignition of hydrocarbons. Ultimately, the blowout preventer emergency functions failed to seal the well after the initial explosions.

Figure B-1 - Platform supply vessels battle the blazing remnants of Deepwater Horizon.

A Coast Guard MH-65C dolphin rescue helicopter and crew document the fire aboard the mobile offshore drilling unit Deepwater Horizon, while searching for survivors. Multiple Coast Guard helicopters, planes and cutters responded to rescue the Deepwater Horizon's 126-person crew. (US Coastguard via Wikimedia Commons).

The application of these service assurance principles and objectives may have likely prevented certain events which occurred during the accident chain. Eight key findings relating to the causes of the accident were detailed in the accident investigation report. Sufficient evidence detailed in accident investigation report would suggest service management failures more than likely contributed to the disaster.

Regulatory oversight of leasing activities and overseeing offshore operations for the Outer Continental Shelf, was performed by the Minerals Management Service, under the authority of the Department of Interior.

BP Exploration & Production Inc. was responsible for obtaining seismic data and assessing the subsurface formation, engineering design of the well, and submitting detailed plans of the intended operations to the Minerals Management Service. BP Exploration & Production Inc. was the lease operator of Mississippi Canyon Block 252, which contains the Macondo well. This lease from the US government enabled BP Exploration & Production Inc. to drill and explore for natural resources (DHSG, 2011).

The Macondo Well was a joint venture between BP Exploration & Production Inc. (65%), Anandarko (25%), and MOEX Offshore 2007 (10%) (DHSG, 2011). As the major shareholder, BP was the operator, in charge of overseeing operations of the well. The drilling of the Macondo Well was a complex operation and involved several oil and gas, offshore and subsea companies which provided

services to BP Exploration & Production Inc. The companies and the services they were contracted to provide are detailed in Figure B-2.

Following approval of plans and issuing of permits, BP Exploration & Production Inc. became the general contractor. At this point they became responsible for the service provision required to support the drilling operations and the design and construction of the well. BP personnel were present on board the Deepwater Horizon providing oversight of the operations (DHSG, 2011).

The Deepwater Horizon was an ultra-deepwater, dynamically positioned, semi-submersible offshore drilling rig (Transocean, 2010). This vessel was owned by Transocean and was leased to BP Exploration & Production Inc. to provide drilling operations, following commissioning in 2001 until September 2013. Transocean was responsible for operations and maintenance of the rig, including subsea equipment such as the Blowout Preventer. Transocean carried out the drilling activities based on the well plan provided by BP Exploration & Production Inc. (DHSG, 2011). As the operator, BP Exploration & Production Inc. held the right to approve and inspect the work carried out on its behalf by Transocean. Transocean was responsible for the actual performance and supervision of the work.

BP Exploration & Production Inc. had contracted Haliburton to provide a cementing service to inject a cement casing within the drilled oil well (BP, 2010). The purpose of cementing service was to seal the well so that hydrocarbons were prevented from entering the wellbore and rising to the surface. Once cement is in place, drilling mud is no longer needed to control the reservoir pressures. Halliburton service provision also included providing advice concerning the design, modelling, testing, and placement of the cement (DHSG, 2011). Once the oil well was completed, the Deepwater Horizon was due to move shortly to its next role as a semi-permanent production platform at the Tiber site.

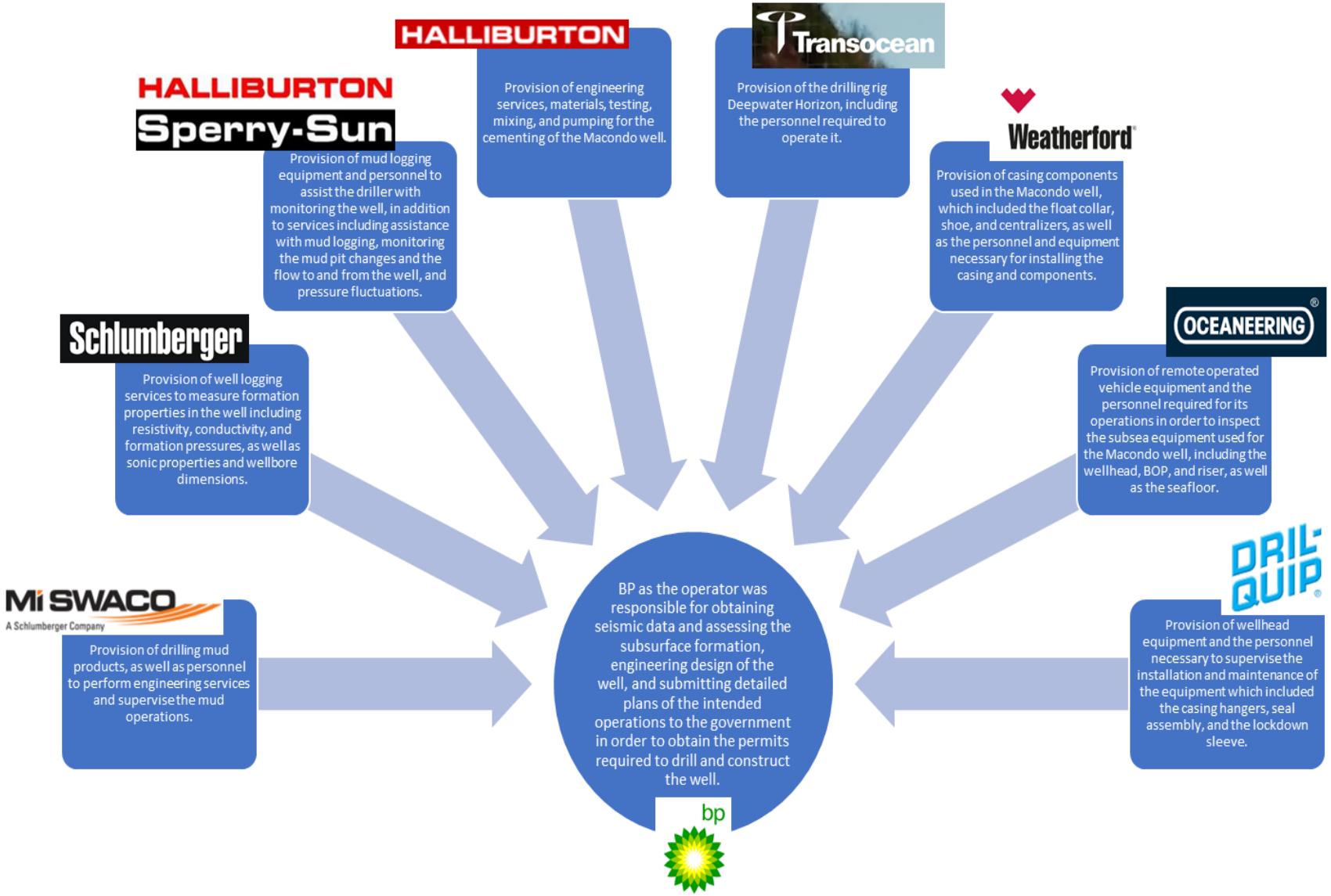


Figure B-2 - Organisations involved and the services provided

It can be assumed that key stakeholders were identified, since BP Exploration & Production Inc. was responsible for the assurance of their service provider and accepting Haliburton's cementing service proposal (BP, 2010). Insufficient evidence is detailed but the objective 1c) was likely satisfied.

The first key finding focused on the failed cement casing. The annulus cement barrier did not isolate the hydrocarbons. The day before the accident, cement had been pumped down the production casing and up into the wellbore annulus to prevent hydrocarbons from entering the wellbore from the reservoir. The annulus cement that was placed across the main hydrocarbon zone was a light, nitrified foam cement slurry. The context and intended use of the SBS (annulus cement slurry) was most likely to have been established. Therefore, satisfying objective 1a). Appropriate historical service-related accidents and incidents were most likely reviewed. Therefore, probably satisfying objective 1b).

During the accident investigation a challenge was presented to the investigation team. They did not have access to cement samples used in the Macondo well. This demonstrates that service assurance requirements for the SBS were not established. This also demonstrates that service assurance requirements were not likely allocated to service elements within the service architecture of the SBS. Service assurance requirements tracing through the service architecture was likely not established. Insufficient evidence is detailed but the objectives 1d), 2a) and 2b) were likely not satisfied, respectively.

As a solution to this challenge, an independent laboratory review of slurry design was initiated. This enabled the construction of representative cement samples based on Haliburton's slurry design to be analysed.

This analysis yielded four conclusions (BP, 2010). Firstly, a high percentage of nitrogen made it difficult to create a stable cement foam slurry. Secondly, there were no fluid loss additives in the foam. Thirdly, a small volume of cement was pumped in comparison to the required displacement volume. This resulted in an increased risk of cement contamination.

BP Exploration & Production Inc. were required to confirm the Top of Cement location. This location is calculated based on an assessment of lift pressures and full returns during the cementing operation. BP Exploration & Production Inc. requested a service from Schlumberger to provide a logging crew and instrumentation. The purpose of this service was to confirm the Top of Cement location and the integrity of the cement to the shoe.

Additionally, no cement had been poured above the top wiper plug of the shoe. Therefore, it is more than likely that the Top of Cement location in the annulus could have been confirmed. If the Top of Cement location was grossly above that calculated, the hazards associated with severe channelling could have been identified and risk assessed. The required lift pressures and measurement of full returns were confirmed by the sensor recordings during the placement. This indicated that the cement had been placed as per the plans.

Consequently, the well team concluded that this phase of the cementing operation was successful, and that Schlumberger logging service was no longer needed. A cement bond log was not run. The Schlumberger logging crew departed the Deepwater Horizon on the morning of the day of the disaster.

Finally, Haliburton did not conduct a comprehensive cement laboratory testing regime. Such testing could potentially have identified potential defects with the cement slurry design. The independent laboratory review demonstrated that cement stability could not be achieved. This demonstrates a service assurance assessment was not likely planned, service analyses not likely performed. Insufficient evidence is detailed, therefore, not likely satisfying the objectives 1e) and 1f), respectively. This also demonstrates service assurance requirements were not verified at an appropriate level within the service architecture of the SBS because they were not likely derived. Insufficient evidence is detailed, therefore, not likely satisfying the objective 3a). This also demonstrates that proven-in-use and service history evidence was not used and therefore, objective 3c) was not likely satisfied.

The cement slurry experienced nitrogen breakout, resulting in nitrogen migration, slurry contamination and incorrect cement density. This demonstrates undesirable behaviours resulting from the service architecture and service elements were not identified, analysed, and managed. Therefore, not satisfying the objective 4a).

The investigation of the cement service also included an analysis of BP Exploration & Production Inc.'s decision to use six centralisers and a long string production casing in the well. It was concluded that the casing design was well-centralised around the primary hydrocarbon zones. The long string design was comprehensive and consistent with other wells in the area. It was also concluded that BP Exploration & Production Inc. had an additional fifteen centralisers which were erroneously believed to be the incorrect type. The use of six centralisers rather than twenty-one, increased risk of the possibility of channelling above the main hydrocarbon zone. This is of significance only if the flow comes up through the annulus and through the seal assembly, which was realised in the accident chain.

The investigation concluded that BP Exploration & Production Inc. and Haliburton should have worked more collaboratively to identify and address these issues underlying the cement service. It was concluded that there were weaknesses in the cement slurry design and service governance concerning testing, quality assurance and risk assessment. This demonstrates that methods were not used to provide service assurance within each level of the service architecture. These were not defined and implemented, therefore not satisfying objective 2c).

The application of the first four service assurance principles would likely mitigate the risk of the annulus cement experiencing nitrogen breakout and migration, allowing hydrocarbons to enter the wellbore annulus and propagate the Deepwater Horizon disaster's accident chain. These first four service assurance principles would provide the assurance evidence required to assure the design and verification of the SBS.

Improved technical assurance, risk management and management of change by BP Exploration & Production Inc. personnel could have been realised if service assurance requirements were derived for Haliburton's cement service and expected usage, detailing service definitions, levels, architectures and agreements made at service interfaces. Application of this second service assurance principle could have resulted in BP Exploration & Production Inc. gaining a greater awareness to make more informed decisions regarding the acceptance of and implementation of Haliburton's cement service offering.

Similarly, the application of the third service assurance principle to satisfy service assurance requirements would contribute to an enhanced engineering rigour and design validation and verification regime of Haliburton's cement slurry design. This would likely enable Haliburton to better identify the reliability of the cement foam slurry and communicate any risks to BP well team to identify

mitigation strategies and where appropriate identify and implement additional service wrappers to make good the assurance shortfall.

If BP Exploration & Production Inc. and Haliburton were in a position to work in collaboration to identify, assess and manage any undesired behaviours within the usage context of the cement service, such as, nitrogen breakout, nitrogen migration, slurry contamination and an incorrect cement density, it is more than likely that an appropriate cement slurry design be accepted into service and implemented into the offshore drilling operation.

This could have been realised through the application of the fifth service assurance principle and the use of LSAs. The establishment of LSAs based on the level of risk will support service assurance activities. Defined and implemented methods, analyses and tools will enable the generation of appropriate service assurance artefacts to provide the evidence required to substantiate service assurance argument goals.

B.3 Summary Analysis

A selection of incidents and accidents from across industry have been analysed from a service perspective with a summary provided (see Table B-1**)** to show how service deficiencies can contribute to unwanted events. The year specified is when the incident/accident occurred, the related accident reports were published subsequently and are accessible through the links provided.

Table B-1 - Incidents and Activities from Services Perspective

Para.	Event	Sector	Year	Services that failed
B.4	Near miss at Gatwick Airport station	Rail	2018	Management Oversight, Planning,
B.5	Runaway of a road-rail vehicle at Bradford Interchange	Rail	2018	Procedure Adherence, management oversight
B.6	Passengers struck by a flying cable at Abergavenny (Y Fenni) station	Rail	2017	Cable Inspection, Station Safety Checks
B.7	Collision with a collapsed signal post at Newbury	Rail	2014	Competence Management, Examination/Inspection
B.8	Catastrophic engine failure, resulting in a fire and serious injuries to the engineer on board Wight Sky off Yarmouth.	Marine	2017	Maintenance, Re-Installation, oil monitoring
B.9	Crush incident involving a falling hatch cover on general cargo vessel SMN Explorer with loss of 1 life	Marine	2018	Maintenance, Planning
B.10	Unintentional release of carbon dioxide from fixed fire-extinguishing systems on ro-ro vessels Eddystone and Red Eagle	Marine	2016	Inspection, Maintenance
B.11	Collision between high-speed passenger catamaran Typhoon Clipper and workboat Alison	Marine	2016	Maintaining Lookouts
B.12	Boeing 737-800 Failure of nose landing gear axle, on departure from London Stansted	Aviation	2017	Maintenance
B.13	DHC-8-402 No. 2 engine shut down due to loss of oil pressure, during descent into Manchester Airport	Aviation	2017	Installation
B.14	Boeing 737-4Q8, loss of electrical power en-route to East Midlands Airport	Aviation	2018	In-Flight Incident Management, Defect Management, Record Keeping

Para.	Event	Sector	Year	Services that failed
B.15	Collision at London Waterloo	Rail	2017	Installation, Design, Procedure Adherence, Staff Competence Management, Staff Tasking
B.16	Investigation into the transition from child and adolescent mental health services to adult mental health services	Healthcare	2017	Transition
B.17	Implantation of wrong prostheses during joint replacement surgery	Healthcare	2017	Prosthesis Verification
B.18	Collision between prawn trawler Achieve and general cargo vessel Talis	Marine	2020	Lookout
B.19	Freight train derailment at Sheffield station	Rail	2020	Maintenance Inspection
B.20	Freight train derailment at Eastleigh	Rail	2020	Maintenance Inspection
B.21	Airbus Helicopters AS355 Engine fire due to exhaust clamp failure	Aviation	2021	Installation Maintenance Design
B.22	Mont Blanc Tunnel Fire	Road	1999	Ventilation, Control Room Operations, Tunnel Maintenance
B.23	Failure of a suspended buoy on workboat Annie E	Marine	2021	Maintenance, Examination/Inspection
B.24	Flooding and sinking of survey workboat Bella	Marine	2021	
B.25	Forced landing following engine failure on Piper PA-23-250	Aviation	2022	Maintenance
B.26	Hard landing following loss of tail rotor drive on Enstrom 280FX	Aviation	2022	Maintenance
B.27	Runaway of a road-rail vehicle at Belle Isle Junction	Rail	2021	Maintenance
B.28	Collision between a passenger train and a hand trolley at Challow	Rail	2021	Maintenance, Line Clearance

B.4 Near miss at Gatwick Airport station

"At 23:24 hrs on 2 December 2018, a track worker narrowly avoided being struck by a train between Horley and Gatwick Airport stations, on the boundary between Surrey and West Sussex. The track worker, a controller of site safety (COSS), was undertaking work related to the electrical isolation of conductor rails and moved out of the path of the train just before it reached him.

The Network Rail isolation planning process meant that BAM Nuttall planners lacked the information needed for them to establish the exact location at which work was to be carried out on the track. The planners lacked the skills and experience needed to understand this and so provided a system of work which provided no protection from train movements at the actual location of the task. The COSS recognised that the planned system of work lacked adequate protection from train movements but undertook the task without implementing an alternative safe system of work. A second track worker involved in the isolation task did not challenge the COSS about the unsafe method of working. The underlying factor was that Network Rail isolation processes did not provide planners outside Network Rail with sufficient information to always be able to plan safe systems of work." (RAIB, 2019)

The Rail Accident Investigation Branch (RAIB) saw this as a failing by both parties in the 'management oversight' services where they did not provide relevant levels of information to enable a Safe System of Work to be established by the COSS. Failings were also identified with the 'planning' service where plans were developed without the necessary information needed to plan a safe system of work.

Link: https://www.gov.uk/raib-reports/report-12-2019-near-miss-at-gatwick-airport-station (Accessed 22nd October 2019)

B.5 Runaway of a road-rail vehicle at Bradford Interchange

"At about 01:40 hrs on Friday 8 June 2018, a road-rail vehicle (RRV) ran away while being on-tracked at a road-rail access point south of Bradford Interchange station. The RRV ran downhill for approximately 340 metres, before coming to a stop as the track levelled out in the station. The RRV's machine operator and machine controller were able to run along with it and warned a member of track maintenance staff, who was able to move clear in time.

The RRV ran away because its rail wheels were, incorrectly, partially deployed and because the rail wheel braking system had not been correctly maintained.

Partial deployment of the rail wheels was a result of the machine operator not following the standard industry procedure for on- and off-tracking. He had routinely been on- and off-tracking in this manner and this had not been detected by his employer, Readypower.

The braking system on the rail wheels had not been correctly maintained because fitters were not following the original equipment manufacturer's instructions and Readypower had not detected this. An underlying factor was that the industry's competence management system for machine operators focuses on the renewal of qualifications, rather than demonstrating ongoing competence." (RAIB, 2019)

The obvious causation was failure to enact the service of '*procedure adherence*' by the machine operator. Secondary to this routine failure to follow procedure was not picked up by management indicating a failure of the '*management oversight*' service. The last point in the summary is interesting as this would seem an industry wide Human Factors issue around competence management; however, it could also be considered a factor of the '*management oversight*' service that failed with management relying on paper qualifications and not undertaking regular on-site audits to maintain confidence in staff expertise.

Link: https://www.gov.uk/raib-reports/report-01-2019-runaway-of-a-road-rail-vehicle-at-bradford-interchange (Accessed 22nd October 2019)

B.6 Passengers struck by a flying cable at Abergavenny (Y Fenni) station

"At about 18:05 hrs on 28 July 2017, as a northbound passenger train entered Abergavenny (Y Fenni) station, a cable drooping from the station footbridge became caught on the train's roof. The train dragged the cable and caused it to be pulled from the footbridge until its end broke free from a distribution cabinet. Once free, the end of the cable struck a group of passengers on the footbridge stairs and caused minor injuries to three of them. A member of station staff who was on the platform, close to the footbridge, was nearly struck by the cable. The accident also caused damage to cabling running over the footbridge, the station buildings, and a signal at the end of the platform.

The cable, which provided the signal box at Abergavenny with its electrical power supply, had become detached from the cable tray running over the footbridge and was drooping down to the extent that it was foul of the train. It then caught on an antenna fixed to the roof of the rear vehicle. The cable was drooping because the nylon cable ties used to attach it to the cable tray had broken. The RAIB

found that the cable had not been inspected periodically as required for electrical installations and the drooping cable was not identified during footbridge inspections. It was not reported during routine station safety checks, or after it was drooping below the bottom of the footbridge. An underlying cause was that Network Rail had no controls in place for the management of low voltage electrical supply cables that cross operational railway lines via its overline structures." (RAIB, 2018)

This incident highlights the importance of services that should occur at regular intervals and may seem mundane and allow for loss of focus by those carrying out the service. In this case the 'cable inspection' service and 'station safety checks' service both of which were likely carried out by the same staff for some time prior to the incident. A case of over familiarity potentially being a flaw in the service execution.

Link: https://www.gov.uk/raib-reports/report-06-2018-passengers-struck-by-a-flying-cable-at-abergavenny-y-fenni-station (Accessed 22nd October 2019)

B.7 Collision with a collapsed signal post at Newbury

"At about 14:35 hrs on 17 November 2014, a train travelling at 110 mph (177 km/h) struck the top of a signal which had collapsed and fallen across the railway line near Newbury. The signal post completely obstructed one track and partially obstructed a second (the one on which the train was travelling). There were no injuries, and the train did not derail, but it did sustain some exterior damage. The outcome could have been much more serious if the first train to encounter the collapsed signal had been travelling at speed on the completely obstructed track.

The signal collapsed because the base of the post, which was of hollow tubular steel construction, had corroded through, causing an almost complete loss of wall thickness at and just above ground level. Corrosion had occurred to both internal and external surfaces; internally because water had entered the post and there was no drainage for it to escape, while the external corrosion was affected by the base being buried in ballast, which held water around the base and damaged the protective coating on the signal post.

Signal posts are subject to annual visual examinations, but the examinations of this signal did not detect the problem because the main area of corrosion was hidden by ballast, and the examinations regime was vulnerable to missing such defects. A separate examination in 2012 for a re-signalling project in the area also did not detect the defect for similar reasons. Because the defect was not detected, it was not reported and remedied through maintenance." (RAIB, 2015)

On investigation the RAIB determined a failing in the '*competence management*' service at Amey, specifically pertaining to structures examiners and amongst four recommendations to Network Rail a deficiency in the '*examination/inspection*' service pertaining to signal structures.

Link: https://www.gov.uk/raib-reports/collision-with-a-collapsed-signal-post-at-newbury (Accessed 22nd October 2019)

B.8 Catastrophic engine failure, resulting in a fire and serious injuries to the engineer on board Wight Sky, off Yarmouth

"At 2133 on 12 September 2017, while approaching Yarmouth, Isle of Wight, the ro-ro passenger ferry Wight Sky suffered a catastrophic failure of one of its main propulsion engines, followed by a

fire. The fire was brought under control in less than 2 minutes, but the vessel's engineer, who had been standing near the engine, suffered serious burn injuries to his hands and face. Although he was discharged from hospital 7 days later, he was subsequently diagnosed with post- traumatic stress disorder." (MAIB, 2018)

The maintenance or the delay in re-installing the engine was the likely cause. "*Maintenance*" and "*re-installation*" are clearly service activities, and the suggestion is that these were carried out in such a way to leave the engine oil contaminated. Hence the "*engine maintenance*" service can be considered to have operated deficiently.

The engine oil samples indicating accelerated wear were not acted upon – this can be considered a failure of the "*oil monitoring*" service.

Link: https://www.gov.uk/maib-reports/catastrophic-engine-failure-and-fire-on-board-ro-ro-passenger-ferry-wight-sky (Accessed 22nd October 2019)

B.9 Crush incident involving a falling hatch on general cargo vessel SMN Explorer with loss of 1 life

"A crewman from the Liberian registered general cargo vessel, SMN Explorer, died when he was crushed by a falling hatch cover. The crewman was part of a working party stowing cargo slings used for the discharge of the ship's cargo. The accident occurred when the crewman climbed up the inside of the open hatch cover after its locking pins had been removed." (MAIB, 2019)

As the accident occurred in UK waters (Alexandra Docks, Kings Lynn) the Marine Accident Investigation Branch (MAIB) undertook an investigation and determined several safety-related failings derived from a weak safety culture on board the vessel. These had in turn led to two key service failings, '*maintenance*' of the Explorer's lifting appliances and '*planning*' of safe systems of work, including risk assessments.

Link: https://www.gov.uk/maib-reports/crush-incident-involving-a-falling-hatch-cover-on-general-cargo-vessel-smn-explorer-with-loss-of-1-life (Accessed 22nd October 2019)

B.10 Unintentional release of carbon dioxide from fixed fire-extinguishing systems on ro-ro vessels Eddystone and Red Eagle

"On 8 June 2016, the roll on, roll off (ro-ro) vessel Eddystone experienced an unintentional release of carbon dioxide (CO2) from its fixed fire-extinguishing system while in the Red Sea. A similar incident took place on 17 July 2017 on board the ro-ro passenger ferry Red Eagle while on passage from the Isle of Wight to Southampton. In both cases, gas leaked into the CO2 cylinder compartment, but was prevented from entering the engine room by the main distribution valve which remained closed. Fortunately, no one was harmed in either of these incidents. However, the unintended release of CO2 from fire-extinguishing systems has caused 72 deaths and 145 injuries, mainly in the marine industry, between 1975 and 2000."

Essential services in any sector in support of fire prevention systems are routine 'inspection' and 'maintenance' to ensure ongoing utility and compliance with the latest regulations and standards. Such inspection and maintenance were found by the MAIB to be inadequate on the fire extinguishing

systems on both Eddystone and Red Eagle, not helped by inadequate guidance from the marine industry.

Link: https://www.gov.uk/maib-reports/unintentional-release-of-carbon-dioxide-from-fixed-fire-extinguishing-systems-on-ro-ro-vessels-eddystone-and-red-eagle (Accessed 22nd October 2019)

B.11 Collision between high-speed passenger catamaran Typhoon Clipper and workboat Alison

"At 1108 on 5 December 2016 the high-speed passenger catamaran Typhoon Clipper and the workboat Alison collided adjacent to Tower Millennium Pier on the River Thames. Alison sank and its two crewmen were rescued out of the water by Typhoon Clipper's crew after the collision. Both Alison's crewmen were suffering from cold shock but were released from hospital later the same day."

The MAIB highlighted ambiguities in the regulations laid down by the Port of London Authority (PLA) regarding the keeping of lookouts in vessels with 'restricted visibility', an essential service in the very congested waterways of the River Thames where continuously monitoring the risk of collision is a major priority. It is of credit to the crew of the Typhoon Clipper that they were well versed in the '*emergency response*' service and able to rapidly enact a rescue of the Alison's crew.

Link: https://www.gov.uk/maib-reports/collision-between-high-speed-passenger-catamaran-typhoon-clipper-and-workboat-alison (Accessed 22nd October 2019)

B.12 Boeing 737-800 Failure of nose landing gear axle, on departure from London Stansted

As the aircraft was lining up on the runway to take off, the flight crew heard a noise like a nose wheel passing over a runway centre light; they did not consider the noise to be unusual. During the take-off roll, the flight crew in an aircraft holding near the start of the runway noticed one of the nose wheels depart EI-DLV and be blown off the runway into the area behind the threshold. They informed Air Traffic Control (ATC) who informed the crew of EI-DLV, which was now in the climb. A diversion was carried out to East Midlands Airport where an uneventful landing was made.

The nose wheel was found to have separated from the aircraft because the nose landing gear axle had failed at the left inboard journal (the part of the axle that rests on bearings). This was the result of heat-induced cracking and material property changes due to abusive grinding of the chrome plate during the part's last overhaul almost three years earlier. Limitations in the inspection regime at the Maintenance and Repair Organisation (MRO) that performed the overhaul were picked up as a service failing by the Air Accidents Investigation Branch (AAIB) and seen as a significant contributory factor in the incident. That MRO subsequently introduced a new inspection protocol for detecting abusive grinding.

Link: https://www.gov.uk/aaib-reports/aaib-investigation-to-boeing-737-800-ei-dlv (Accessed 22nd October 2019)

B.13 DHC-8-402 No. 2 engine shut down due to loss of oil pressure, during descent into Manchester Airport

Towards the end of the flight the Central Warning System indicated an oil pressure loss on the No 2 engine. The engine was shut down and an uneventful single engine landing was carried out. It was found that a cap locating the propeller overspeed governor test solenoid had detached, allowing most of the oil from the No 2 engine lubrication system to be lost. Investigation of the component revealed that the four cap securing bolts had failed, predominantly in fatigue. Extensive investigation failed to identify conclusively the root cause of the bolt fatigue damage. Although three similar in-service failures of these bolts have occurred on other aircraft types utilising this design of governor, no others have been recorded on DHC-8-400 types and all those that have occurred have been on units of an earlier modification state.

Although unable to make absolute conclusions as to the causation of the incident the AAIB report suggests that it could have been due to issues during the '*installation*' of the No 2 engine overspeed governor a critical service in ensuring safe operation of that engine.

Link: https://www.gov.uk/aaib-reports/aaib-investigation-to-dhc-8-402-g-prph (Accessed 22nd October 2019)

B.14 Boeing 737-4Q8, loss of electrical power en-route to East Midlands Airport

"The aircraft was operating a night flight to East Midlands Airport, with the left engine generator disconnected, and had just commenced its descent when the crew faced an unusual array of electrical failures on the flight deck. Despite the loss and degradation of several systems, the aircraft landed safely at East Midlands.

The electrical failures were caused by the right engine Generator Control Unit (GCU) which had been incorrectly secured in its mounting tray and had disconnected in flight. The investigation also uncovered a number of contributory factors including: the management of defects and Acceptable Deferred Defects (ADD), recording of maintenance, and a number of weaknesses in the operator's Safety Management System with regards to managing risk." (AAIB, 2018)

All flight crews are trained to provide an '*in-flight incident management*' service to analyse abnormal and emergency situations in line with Boeing's Quick Reference Handbook (QRH) and their employer's decision-making strategy. At no time leading up to the incident did the crew seek to enact such a service. The AAIB determined that the flight-crew had sufficient time without impacting negatively on a safe landing.

The ADD was in place for a faulty generator. This was permissible under European Union Aviation Safety Agency (EASA) Minimum Equipment List (MEL) rules provided a fully functional second generator was available, and an Auxiliary Power Unit (APU) was operated during flight. EASA rules also allowed for the operator to approve a Rectification Interval Extension (RIE). Incorrectly, the operator saw the MEL and RIE as means of supporting continued operational commitments rather than prioritising defect resolution. Consequently, partial fault finding, and defect resolution occurred with aircraft wrongly pressed into operation with unresolved defects. Alas, the underlying fault in Gen 1 remained extant as the aircraft operator continued to overlook opportunities to fully enact a '*defect management*' service.

Pertinent to this incident there were also instances of failings in the service of 'record keeping'. GCUs were swapped out during defect rectification work on the faulty generator in support of addressing the ADD in the days prior to the incident. These were recorded in the Operator's Flight Status Reporting system (FSR) but not the records specific to this aircraft.

Link: https://www.gov.uk/aaib-reports/aaib-investigation-to-boeing-737-4q8-g-jmcr (Accessed 22nd October 2019)

B.15 Collision at London Waterloo

At around 05:42 hrs on Tuesday 15 August 2017, a passenger train collided with a stationary engineering train shortly after leaving London Waterloo station travelling at a speed of 13 mph. Both trains were damaged and there was serious disruption to train services until the middle of the following day; fortunately, there were no injuries.

A set of points which had been positioned erroneously because of uncontrolled wiring added to the signalling system led to the passenger train being diverted away from its planned route and derailing into the engineering train. The wiring had been added to overcome issues when testing modifications to the overall signalling system as part of a project to increase capacity at London Waterloo. The test equipment design process had not allowed for alterations to the signalling system after the test equipment was designed.

Because of a functional tester lacking appropriate competence Network Rail safeguards were not applied and the uncontrolled wiring was added and moreover, remained in situ when the line was returned to service. A planned decision to secure the set of points back to their correct position was also not implemented.

The RAIB investigation identified issues with competence management processes across Network Rail and its supply chain. Of even greater concern their report observed similarities between the causal factors of this incident and those which led to 35 fatalities in the serious accident at Clapham Junction in 1988, raising concerns that some of the lessons from that accident may be "fading from the railway industry's collective memory" (RAIB, 2018).

The incorrect positioning of the set of points and subsequent signalling to the passenger train to run over them was the immediate cause of the collision. However, several service-related causes led to the line being returned to operational service with the points incorrectly set.

An '*installation*' service failed when uncontrolled wiring was added to the detection circuits leading to unrestrained switch blades moving to an intermediate position that was incorrectly indicated as satisfactory. The root cause of a malfunctioning test desk was identified as an incomplete '*design*' service across a number of organisations.

The temporary wiring was applied to the local signalling system, but the requisite risk assessment was not enacted in accordance with the relevant handbook, a '*procedure adherence*' service, as the Contractor's Responsible Engineer (CRE) understood the spur wires would not remain connected whilst the interlocking system was operational.

A functional tester should have been tasked to simulate the points operation on the test desk and then remove the uncontrolled wiring prior to the line being returned to operation, neither task was requested or completed. Clear failures of the '*staff tasking*' service. Also, that individual had only recently had his certificate of competency re-instated after a period of assessed deficiency against the minimum standard. His failure to apply three key aspects of the signalling works testing standard were highlighted by the RAIB, raising questions over his employers' '*staff competence management*' service.

Protocol requires points within a rail-line blockade to be electrically disconnected and secured using scotches (wooden blocks) and padlocked clips. Although a test plan was drafted, no accountable person was identified to enact the plan as the points lay just outside the section of rail being modernised, another '*staff tasking*' service failure.

Link: https://www.gov.uk/raib-reports/report-19-2018-collision-at-london-waterloo (Accessed 31st January 2020)

B.16 Investigation into the transition from child and adolescent mental health services to adult mental health services

According to Healthcare Safety Investigation Branch (HSIB) Report I2017/008 (HSIB, 2017), 18-year-old Ben (not the person's real name) committed suicide during the period of transition from Child and Adolescent Mental Health Services (CAMHS) to Adult Mental Health Services (AMHS). Ben had been diagnosed with Autism Spectrum Disorder (ASD) during childhood, and already had a documented history of attempted suicide. Owing to Ben's low moods, anxiety and suicidal tendencies, Ben was referred by his GP to CAMHS. Ben was put on medication and a care plan was established. Subsequently, Ben was seen by different professionals.

After about 3 months Ben's care coordinator went on sick leave, and Ben was allocated a new care coordinator. As Ben was approaching his 18th birthday, a transition request to AMHS was put in. The referrer noted in the transition re-quest that Ben had expressed the intention of ending his life once he turned 18. Ben expressed great anxiety about the transition to AMHS, which was explained in part by his dislike of change associated with his ASD.

Over the next few months Ben's low moods and negative thoughts increased, and Ben's medication was increased further. Ben's mother informed his care co-ordinator that he had self-harmed. Ben met with his care coordinator, and he ex-pressed again his anxiety about transitioning to AMHS, and his desire to continue to remain with CAMHS. Ben was told that he needed to transition to AMHS at the age of 18, but that a handover would be put in place.

The same night, Ben died by suicide.

When a child or young person dies by suicide it is, by default, a failure of the health service that was supposed to look after and care for that person. This is especially true in Ben's case. Ben had a history of suicidal episodes and low moods and had been in frequent contact with mental health services. There were many warning signs, and Ben had even announced his intention to end his life on his 18th birthday. And yet, it is hard – and misleading – to point, in hindsight, the finger at any one individual and assign blame or identify their actions as the cause of this tragic event.

However, adopting a service perspective provides further insights that can help explain this death, and from which we might be able to identify lessons for improvement. The service element, which crucially failed in this case, is the '*transition*' service provided by CAMHS and AMHS in collaboration. This transition period is recognised as being critical, and it is known from the literature that young adults often disengage from the health service (not just mental health) during transition, which leads to suboptimal outcomes, or death as in this case. The HSIB report emphasises that Ben's case is not an isolated case, but that similar issues linked to failures in transition have occurred throughout England.

Even though CAMHS and AMHS are providing this transition service together, they are each very different services, and the transition is complex. This is further exacerbated by variability in practice, with some CAMHS providing care flexibly up to the age of 25, while others transition more rigorously to AMHS at the age of 18.

The transition request was initiated by CAMHS quite close to Ben's 18th birthday, and this was, in part, caused by the 3-months absence of Ben's initial care coordinator due to sickness. As a result, plans for handover and shared care arrangements were not in place, and this caused Ben significant additional anxiety. Ben's ASD diagnosis and his struggle to deal with change were known and documented, and the HSIB report suggests that a longer and better planned transition period would have supported Ben.

Shared care arrangements between CAMHS and AMHS are facilitated by joint meetings, but frequently these do not take place due to high workload, difficulties in managing and aligning diaries, and the young person's and their families' availability. This was the case with Ben, where no joint meeting was held in the run up to Ben's transition to AMHS.

Link: https://www.hsib.org.uk/investigations-cases/transition-from-child-and-adolescent-mental-health-services-to-adult-mental-health-services/ (Accessed 22nd October 2019)

B.17 Implantation of wrong prostheses during joint replacement surgery

"A 62-year-old man was admitted to hospital for a planned total hip replacement following routine pre-operative checks he was taken to theatre and his operation began. A theatre nurse collected from the stockroom the first two prostheses needed to create the man's new hip joint. The theatre team checked they were the correct ones before opening the packaging. The surgeon then implanted the prostheses.

About 15 minutes later, the third and fourth prostheses were collected and checked by the theatre team as before. This check did not identify that these prostheses were made by different manufacturers and not compatible to be implanted together. The packaging was opened and both prostheses were implanted.

Unaware of this error, the operation was completed, and the patient was discharged a few days later.

Following joint replacement surgery, all hospitals are required to enter details about the patient, the prostheses and the operation into the National Joint Registry. The registry generates an automatic alert if incompatible prostheses have been implanted into a patient. So, when the details of this patient's prostheses were entered into the registry several days after the operation the system identified the problem and alerted staff to the error.

The patient was informed of the error, and it was also reported to relevant external bodies as a serious incident. The hospital began an internal investigation to understand what had happened. Expert advice was sought to decide if the patient would need another operation to replace the incorrect component. After consideration of all relevant information, a further operation was not judged necessary. The hospital made arrangements to review the patient regularly to check for any problems that might be related to implantation of the wrong prosthesis." (HSIB, 2018)

The HISB identified several findings, notably that there were variations in the service of 'prosthesis verification' with some underlying human factors that could hinder the safe application of that service in the pressure of the operating theatre environment. Some theatre teams have developed specific approaches to reduce the risk of incorrect prostheses being implanted, however not in this case.

Link: https://www.hsib.org.uk/investigations-cases/implantation-wrong-prostheses-during-joint-replacement-surgery/ (Accessed 31st January 2020)

B.18 Collision between prawn trawler Achieve and general cargo vessel Talis

"On 8 November 2020, the UK registered fishing vessel Achieve collided with the Panama registered general cargo ship Talis in fog. The fishing vessel was severely damaged and sank while being towed to port. The cargo ship suffered minor damage. There were no injuries and only minor pollution from Achieve." (MAIB, 2021)

The MAIB identified that neither vessel was operating an effective lookout service, especially important given the restricted visibility. Furthermore, Achieve's wheelhouse was unmanned at the time of the collision, contravening the obligation to always keep a proper lookout, as required by the International Regulations for Preventing Collisions at Sea, 1972, as amended (COLREGs). Talis's radar detected the fishing vessel at close range, but the watchkeeping officer's action was hesitant and too late to avoid a collision.

Link: https://www.gov.uk/maib-reports/collision-between-prawn-trawler-achieve-and-general-cargo-vessel-talis-and-subsequent-sinking-of-achieve (Accessed 8th December 2021)

B.19 Freight train derailment at Sheffield station

"At 02:44 hrs on Wednesday 11 November 2020, 16 wagons of a freight train … derailed at the north end of Sheffield station. A number of wagons were damaged and there was significant damage to the track, resulting in a partial closure of the station. No one was injured.

The train was coasting through the station at a constant speed of around 12 mph (19 km/h) when the leading right-hand wheel of the twelfth wagon dropped into the space between the two running rails, because the rails were too far apart: a problem known as gauge widening. The train stopped when the signaller observed a number of signalling equipment failures indicated on a display screen and alerted the driver to a problem.

The track gauge had widened because a number of track screws, that secured the rails and baseplates to the wooden bearers, had broken, allowing the rails to spread apart under the loads from passing trains. The track screws had failed several weeks, or perhaps months, before the derailment, but the failures had not been identified by Network Rail's maintenance inspection activities.

Although this was a location with a potentially high risk of derailment, it had not been recognised as such because Network Rail's guidance for identifying such risk had not been applied. Additional mitigation had therefore not been considered." (RAIB, 2021)

Link: https://www.gov.uk/raib-reports/report-07-slash-2021-freight-train-derailment-at-sheffield-station (Accessed 8th December 2021)

B.20 Freight train derailment at Eastleigh

"At about 11:32 hrs on Tuesday 28 January 2020, a freight train derailed while travelling over a set of points at Eastleigh West Junction, immediately south of Eastleigh station. The locomotive hauling the train ran derailed for about 35 metres, causing significant damage to the infrastructure. Four wagons subsequently derailed on the damaged track. Nobody was injured in the accident.

Some of the fastenings that hold the rails to the concrete bearers that support them had fractured, prior to the passage of the train. This allowed one of the rails to move outwards under the train, breaking further fastenings and causing the locomotive's wheels to drop inside the rail, as it moved further outwards. The design of these fastenings made them more prone to this type of failure when subjected to high lateral forces, which were present at these points due to the track geometry at the site and the curving characteristics of the locomotive. The local track maintenance team had not identified any relevant faults prior to the derailment as the fastenings had fractured below the surface of the concrete bearer and these failures were not apparent during visual inspections. Despite previous faults of a similar nature elsewhere, Network Rail had not developed an effective inspection regime to detect such failures. Measurements of the track geometry of this set of points had also not detected any indication of deterioration in the track fastening system." (RAIB, 2021)

The RAIB found the local maintenance delivery unit was not effectively managing the maintenance of its track assets, a clear failure of the 'track asset management' service. Recommendations were made to Network Rail to develop a clear track asset management strategy to address increased risks around the failure of the type of track fastening systems involved in this derailment and the service of inspecting them effectively.

In their efforts to promptly bring the rail network back into service Network Rail failed to preserve evidence for the RAIB investigation, they were strongly reminded of their legal duty to do so.

Link: https://www.gov.uk/raib-reports/report-02-slash-2021-freight-train-derailment-at-eastleigh (Accessed 8th December 2021)

B.21 Airbus Helicopters AS355 Engine fire due to exhaust clamp failure

"Whilst hovering at 20 ft, agl smoke was observed coming from the engine exhaust. A member of the operational team on the ground informed the pilot, who then landed immediately. A fire warning subsequently illuminated, and the pilot activated the fire extinguishing system. The fire was determined to have been caused by the loss of retention of the right engine inboard exhaust nozzle, which was released because of the failure of its securing clamp. The released nozzle had blocked the overboard exhaust outlet and allowed hot exhaust gases to impinge on the engine cowlings leading to local overheating.

The clamp failure was attributed to a combination of an incorrect locking washer being fitted during maintenance and elevated engine vibration which caused the clamp to loosen. A crack then propagated in low-load high-cycle fatigue until final rupture of the clamp.

The helicopter manufacturer is taking safety action to amend the Aircraft Maintenance Manual (AMM) highlighting the correct installation of the clamp." (AAIB, 2021)

An '*installation'* service failed during maintenance when the wrong locking washer was used. A washer supplied with the clamp should have been swapped out for a serrated washer specified in the AMM. However, that was not the only service failing. There was no requirement in the AMM to re-torque the locking screw after a ground run that was required post maintenance. That led to an issue of high engine vibration which was identified after the incident and is felt, coupled with the incorrect washer led to the clamp working loose. A failure in the '*maintenance design*' service.

Link: https://www.gov.uk/aaib-reports/aaib-investigation-to-airbus-helicopters-as355-f1-g-bosn (Accessed 18th December 2021)

B.22 Mont Blanc Road Tunnel Fire

"On 24th March 1999 a transport truck caught fire while driving through the Mont Blanc tunnel between Italy and France. Other vehicles travelling through the tunnel became trapped and fire crews were unable to reach the transport truck. The fire burned for 53 hours and reached temperatures of 1,000 °C producing toxic smoke. Authorities compounded the problem by pumping air from the Italian side, feeding the fire and forcing poisonous black smoke through the length of the tunnel. A total of 39 people were killed. In the aftermath, major changes were made to the tunnel to improve its safety." (Catmur, King et al, 2022)

The key service that contributed to the accident was the *'control room'* service. There were two separate command and control stations, one for each half of the tunnel operated by its respective national concession with the *'control room'* services delivered by those stations not synchronised. This led to fresh air being pumped into the tunnel from the Italian side which drove smoke from the fire towards the French side and fed the fire. The *'ventilation'* service was also inadequate to cope with extracting exhaust fumes, being less than half the rate of comparable tunnels. This was not helped by the vastly increased volume of traffic, with heavy goods traffic in 1999 more than double that predicted.

B.23 Failure of a suspended buoy on workboat Annie E

"At approximately 1315 on 3 April 2021, a deckhand on board the workboat Annie E was injured when he was struck by a grid buoy that had been lifted out of the water by the workboat's forward crane at a fish farm off the Isle of Muck.

Annie E's skipper had noticed that the grid buoy was out of position and needed to be lifted in order to recover and re-lay its mooring anchor. The workboat's forward crane was used to lift the buoy and its anchor connection out of the water. The buoy was suspended 9m above the water when its metal components experienced a mechanical failure, resulting in the buoy falling and striking the deckhand.

First aid was administered to the injured deckhand, who was evacuated by a coastguard helicopter to hospital, where he underwent surgery. He has since received further surgery and treatment." (MAIB, 2022)

In addition to the failure of staff to comply with the workboat owner's risk assessments, method statements, lifting plan and industry guidelines, the MAIB identified failures in the 'maintenance' service. The grid buoy's metal components were worn, and the top washer was missing, both of which resulted in its failure and should have been identified as part of routine maintenance and inspection.

Furthermore, the risk assessments and method statements did not fully mitigate the risks associated with a suspended load, the buoy was not certified as lifting equipment, and the lifting technique used did not comply with the manufacturer's recommended procedure, which the vessel's owner and crew were unaware of.

Link: https://www.gov.uk/maib-reports/failure-of-a-suspended-buoy-on-workboat-annie-e-with-1-person-injured (Accessed 5th January 2023)

B.24 Flooding and sinking of survey workboat Bella

"On 6 July 2021, the UK survey workboat Bella flooded and sank while carrying out hydrographic survey operations in the approaches to Lynmouth, England. Bella's crew abandoned into the life raft and were rescued uninjured by a local boat owner; there was no pollution." (MAIB, 2022)

The MAIB assessed that workboat Bella was vulnerable to swamping, even in moderate sea conditions, because it carried a multibeam echo sounder gantry across its bows which reduced its forward freeboard. Although the vessel was certified it was not considered compliant with The Workboat Code, primarily due to failings in the '*certification*' service, which did not pick up deficiencies in the boat's construction, notably its means of flotation. The surveyor had relied heavily on the Recreational Craft Directive which was not applicable for the boat's intended purpose.

There were also failings in the safety management system supporting the boat which allowed for inexperienced crew to underestimate the risks of operating the boat in open seas.

Link: https://www.gov.uk/maib-reports/flooding-and-sinking-of-survey-workboat-bella (Accessed 9th January 2023)

B.25 Forced landing following engine failure on Piper PA-23-250

"During an IFR flight from Le Touquet to Wellesbourne, the pilot observed oil leaking from the left engine followed by engine vibration. He shut the engine down and descended but elected to continue the flight toward Wellesbourne. On reaching 2,000 ft he found he was unable to maintain level flight on one engine and decided to land in a field.

The investigation found the left engine failed due to a fatigue crack in one of the cylinder barrels. It is likely that the pilot was unable to maintain level flight on the right engine due to a combination of engine wear resulting in reduced power available and the prevailing weather conditions. His decision to continue the flight following the engine shutdown was likely to have been influenced by high workload and plan continuation bias.

The maintenance organisation has taken safety action to enhance its maintenance programme for aircraft fitted with piston engines operating beyond the manufacturer's recommended overhaul life." (AAIB, 2023)

Link: https://www.gov.uk/aaib-reports/aaib-investigation-to-piper-pa-23-250-g-bjnz (Accessed 9th January 2023)

B.26 Hard landing following loss of tail rotor drive on Enstrom 280FX

"The helicopter suffered a loss of thrust from the tail rotor while hovering close to the ground near a mountain top, resulting in a loss of control and hard landing. Subsequent examination of the tail rotor gearbox revealed damage to the bevel gears and failure of a bearing, which was consistent with a lack of lubrication. The investigation found inconsistencies in the way maintenance was performed on the tail rotor gearbox, compared to the helicopter manufacturer's maintenance instructions. It is likely that insufficient oil was added to the tail rotor gearbox when it was serviced 25 flying hours prior to the accident.

Three Safety Recommendations are made relating to information in the helicopter Maintenance Manual regarding the required oil quantity and maintenance servicing interval for the tail rotor gearbox." (AAIB, 2023)

Link: https://www.gov.uk/aaib-reports/aaib-investigation-to-enstrom-280fx-g-ojbb (Accessed 9th January 2023)

B.27 Runaway of a road-rail vehicle at Belle Isle Junction

"At around 03:30 hrs on Sunday 16 May 2021, a road-rail vehicle ran away while being on-tracked at a road-rail access point near Belle Isle Junction in north London. The RRV ran downhill for approximately 600 metres before coming to a stop in a tunnel. Although no one was injured, the operator jumped from the road-rail vehicle before it entered the tunnel.

The road-rail vehicle ran away because it entered service with ineffective rail-wheel brakes and staff working with it were unable to stop the runaway. The brakes were ineffective because a valve in the braking system had been left open following maintenance. The possibility of this had not been recognised during the design or risk assessment of the brake system, and the situation had not been identified during operation or regular in- service testing.

Two underlying factors were identified. These were that the risk assessment undertaken in support of a modification to the machine to fit a direct rail wheel braking system was incomplete, and that the company responsible possibly did not have a thorough understanding of the unmodified machine or its original conversion for rail use." (RAIB, 2022)

Link: https://www.gov.uk/raib-reports/report-04-slash-2022-runaway-of-a-road-rail-vehicle-at-belle-isle-junction (Accessed 13th January 2023)

B.28 Collision between a passenger train and a hand trolley at Challow

"At 06:09 hrs on 21 October 2021, a passenger train travelling at 123 mph (198 km/h) struck a hand trolley on the track near Challow, Oxfordshire. The train was the first to pass through the area after the completion of overnight maintenance work. There were no injuries among the passengers or crew

on board and the train did not derail. The hand trolley was destroyed by the impact and debris from it caused damage to equipment under the train. The collision also resulted in minor damage to the track.

A maintenance team had carried out overnight work at Challow and no one noticed the team had left its hand trolley on the track. The checks undertaken before handing back the railway for normal operation also had not identified the hand trolley's presence. A process which formed part of these checks was the line clear verification process. It was used to monitor what vehicles, including hand trolleys, were placed on and taken off the track during the overnight work. However, there were weaknesses within this process, and these were compounded by the maintenance team not following the process as it was required to on the night concerned.

Underlying factors related to the weaknesses within the line clear verification process were:

It was reliant on human actions for its successful implementation, which the rail industry had recognised, but not yet implemented any measures to avoid or mitigate errors.

It was separate to the work planning process as defined by Network Rail's company standards. This was a possible underlying factor.

Network Rail's assurance activities had not detected that staff in the Swindon delivery unit welding and grinding section were not complying with the line clear verification process. This was a possible underlying factor.

A further probable underlying factor was that hand trolleys were being routinely used at night without displaying any red lights and that no assurance activities were taking place within work sites to monitor compliance to this requirement." (RAIB, 2022)

Link: https://www.gov.uk/raib-reports/report-11-slash-2022-collision-between-a-passenger-train-and-a-hand-trolley-at-challow (Accessed 13th January 2023)

Annex C A Stepwise Methodology for Applying the Guidance (Discursive)

> *"Service is the rent we pay for being. It is the very purpose of life, and not something you do in your spare time."*
>
> Marian Wright Edelman

This appendix outlines a step-by-step methodology for applying the guidance to a typical service hierarchy. There is a natural workflow, starting with contracts, then organisational structure diagrams, identification of services, service hierarchies then allocation of LSAs and identification of wrappers and flow down of requirements.

This methodology has been established to work on top of the existing guidance document. It is appropriate for a typical commercial service model involving explicit service contracts and a service hierarchy. It allows flow down of assurance levels and identification of supplementary assurance activities to be allocated to specific stakeholders. It is therefore considered suitable for the typical legal and commercial models used for a wide variety of services, for example for highways maintenance contracts or hospital IT support contracts.

The methodology has eight basic steps:

1. Identify Organisations Involved
2. Identify Organisational Provision
3. Determine Service Hierarchy
4. Determine Levels of Service Assurance
5. Identify Assurance Wrappers
6. Flow Requirements Through the Service-Based Solution
7. Define Assurance Wrappers
8. Meet the Principles and Objectives

These are explained in more detail below. A paper from SSS'22 (Catmur, Parsons and Sleath, 2022) gives a worked example.

C.1 Step 1 - Identify Organisations Involved

Initially the organisational hierarchy defined or implied by the contracts that are let to form the delivery of the overall service is identified. Starting with the organisation letting the contract or the prime contractor, the group of organisations delivering the service is expanded and elaborated. Many different organisations may be involved, and most will have some sort of contract or agreement with

the prime or next level contractor. It is useful to include organisations directly supporting the service and other stakeholders. It is helpful to draw this as a contractual hierarchy.

C.2 Step 2 - Identify Organisational Provision

The next step in the method then identifies the services being provided by each element of the organisational hierarchy to the level above. Often these will be defined by service catalogues or service blueprints at each level. Only the services consumed by the next level up need to be included.

C.3 Step 3 - Determine Service Hierarchy

The third step is to establish the agreements in place at each level of the hierarchy. These are typically contracts which involve a Service-Level-Agreement (SLA). In some cases there will not be any explicit contract or agreement (i.e. nothing written down or signed, for instance in the agreement between an NHS patient and doctor), but there will be an **implied expectation of level of service** which can be described and formalised. Note that this step should also identify who is accountable and/or responsible for each service within the hierarchy.

C.4 Step 4 - Determine Levels of Service Assurance

Step 4 is to identify the levels of service assurance (LSA) across the service hierarchy, i.e., assign an LSA for each element of the service based on the table from Section 4 starting with the top element of the hierarchy. The rule followed is that **at least one element below must inherit the LSA of the higher-level element**.

C.5 Step 5 - Identify Assurance Wrappers

The next step is to identify where there may be assurance shortfalls; this then requires an assurance wrapper (Section 5.2) around the lower-level element, where a wrapper is **supplementary assurance that augments that provided by the service provider**. A wrapper may be produced by the service provider or a third party, or by the service consumer themselves. In this way the wrapper enables a service with limited assurance or a non-safety assured service to be consumed by higher-level service which requires safety assurance i.e., it *"turns a non-safety service into a safety-assured service"*.

C.6 Step 6 - Flow Requirements Through the Service-Based Solution

Step 6 is to identify and allocate requirements through the developed Service-Based-Solution (SBS) ensuring that safety requirements are met by a service suitable that can meet them, i.e., one supported by appropriate assurance information.

C.7 Step 7 - Define Assurance Wrappers

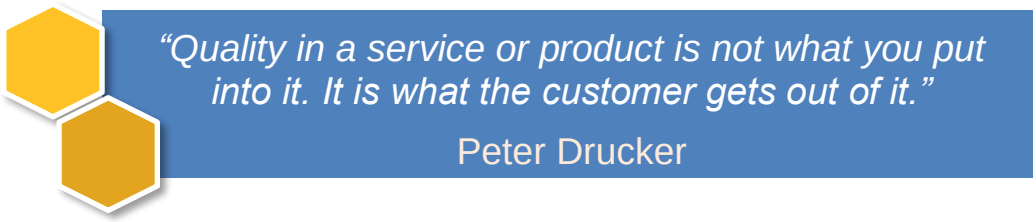
This stage considers how requirements need to be translated through a wrapper. Generally, only non-safety requirements flow through a wrapper, i.e., safety requirements are typically translated or transformed into non-safety requirements (e.g. by changing safety requirements into availability requirements). However, it may be that part of a safety requirement can be flowed down to a sub-service provider or supplier, depending on their capability and willingness to accept it.

C.8 Step 8 - Meet the Principles and Objectives

The last step is to go through the objectives contained in the guidance document tables (Section 4.2) and produce or obtain evidence that shows they are met, or explain why not (e.g. they may not be applicable in this situation or alternate assurance may be provided). If the objectives are met, then it is assumed that the principles are given.

This page is intentionally blank

Annex D Relationship with BS EN 17371: Provision of Services (Discursive)



During the evolution of this SCSC Service Assurance Guidance, BSI Technical Committee (TC) SVS/21 (European Service Standards) has been responsible for providing the UK input to CEN/TC 447 in areas of service procurement, service contracts, performance assessment, terminology, provision of information to customers and customer satisfaction measurement. The product of the TC is BS EN 17371 – Provision of Services, which is currently in three parts as follows:

Part 1: Service procurement - Guidance for the assessment of the capacity of service providers and evaluation of service proposals.

BS EN 17371-1:2021 is a published standard.

Part 2: Services Contracts - Guidance for the design, content, and structure of contracts.

BS EN 17371-2:2021 is a published standard.

Part 3: Management of Performance Measurement – Guidance on the mechanism to measure performance as part of service contracts.

BS EN 17371-3:2020 is a published standard.

BS EN 17371 is specifically focused upon procurement of services that can be subject to a contract with associated measures of performance. For such services, it provides a valuable framework to support the assurance of services addressed by this Guidance document. Those areas pertinent to this Guidance Document include the following aspects:

- Terminology is broadly consistent – see Table D-1 - Terminology Comparison between SCSC & BS EN 17371.
- The setting of performance measures and monitoring against them using, for example, Service Level Agreement (SLA), is comprehensively addressed.
- Safety is acknowledged as an attribute of the service provision but is not further explored, which is appropriate for a procurement-focused document. For example, failure to achieve a performance measure is considered only in the context of financial penalties against an SLA, not that such failure may have safety consequences.
- Part 3 Annex A introduces a Service Assurance Model which presents 5 different Assurance Levels, where the levels address the maturity against which a service provided can be assessed. While the Assurance Levels have a different focus to those considered within this guidance document, these maturity levels do provide a useful input to establishing how achievement of

an assurance level may be constrained by the maturity of the Service Provider. This would then influence what Service Wrappers may be applied for overall service provision (see Section 0 on Service Wrappers).

Table D-1 - Terminology Comparison between SCSC & BS EN 17371

SCSC Term	BS EN 17371 Term	Comment
Service	Service	BS EN 17371-3 specifically calls up ISO 9000:2015.
Service Provider	Service Provider	Aligned
Service Consumer	Service Recipient	Aligned
	Service Buyer	Procurement focused

Given the procurement focus of BS EN 17371, it assumes that the Service Provider is in full control of the service provision in order to meet the requirements of the Service Buyer whereas this Guidance document acknowledges that the Service Consumer may be seeking more than the Service Provider is able or willing to provide (e.g. safety assurance of the service). Additionally, there are Services Consumers that are not necessarily subject to contract with a Service Provider, hence do not fall into the remit of BS EN 17371 (e.g. use of GPS as a time source). This Guidance document does seek to encompass such matters, largely through the concept of Service Wrappers.

Annex E Service-Related Standards (Discursive)

"I am much obliged by the favourable sentiments you express towards me, and shall be happy if I can be of service in carrying into execution your plans."

George Stephenson

This Service Assurance Guidance was borne out of a growing requirement across industry to consider the assurance of safety-related or safety-critical services as set out in applicable standards. This Annex holds requirements extracted from the applicable standards and will be extended when requirements are identified.

Where text is presented in *blue italics* it is directly extracted from the relevant standard or regulation.

E.1 DEF STAN 00-056 Part 1 Issue 7

This standard applies to Defence Contracts across the United Kingdom and has a section that relates to "Service Provision".

16 Service Provision

Note. These clauses apply only when the Contractor is supporting the MOD by providing a Service, which may include operating a PSS. It is intended that they cover development operations, eg test firings, sea trials, flight trials, etc. These are general requirements for such activities and there may be domain- specific requirements or regulations. These clauses will not be applicable if the scope of contract does not include service provision.

16.1 Safety Case Report

The Contractor shall produce a Safety Case Report and Command Summary and deliver them to the MOD for approval before commencement of services.

16.1.1 The Contractor shall maintain the Safety Case, Safety Case Report and Command Summary so they are accurate representations of the service.

16.1.2 The Contractor should produce Command Summaries so that each provision of the service can be properly assessed and controlled in terms of risk.

16.1.3 The Contractor should provide information to support domain specific processes providing essential information for the duty holder responsible for the service to manage Risk to Life.

Notes:

i. The Command Summary is intended to provide essential safety information on the provided service for the mission commanding officer or manager to manage Risk to Life, and may be mission or sortie specific. Therefore, this may lead to the production of more than one Command Summary.

ii. The Command Summaries and Safety Case Reports will be reviewed and accepted by the MOD Regulators, duty holders and stakeholders, prior to commencement of operations.

iii. In the DAE, the Operating Duty Holder is responsible and accountable for the Air System Safety Case. All Duty Holder Facing organizations have a responsibility iaw RA1020 in the management of Risk to Life.

16.2 Service Provision Planning

The Contractor shall produce plans for management of service operations, covering all reasonably foreseeable situations including abnormal and emergency situations.

16.2.1 The Contractor should ensure that the plans cover the safety of the full range of normal services and operations, including but not limited to defining standard operating procedures, resourcing, training, and oversight arrangements.

16.2.2 The Contractor should ensure that the plans cover the safety of emergency situations, including but not limited to defining emergency response, coordination and decision making, including liaison with the service duty holder and relevant stakeholders.

16.2.3 The Contractor should ensure that these plans cover safe update, including ways of making changes on continuously running systems, if necessary, building on installation instructions supplied from support, as appropriate.

16.2.4 The Contractor should ensure that the communications plan, detailed in the SMP, includes processes for delivery of in-service data and build state definition.

Note. These plans may be part of the SMP or in a separate plan as agreed with the MOD where the Contractor provides a service that supports an in-service/operational capability. It is essential that the coordination mechanisms between relevant roles, responsibilities and delivery communication mechanisms are clear.

16.3 Risk Management

The Contractor shall support the MOD in managing predicted or emergent Risk to Life arising from hazards and accidents associated with the service, according to the ALARP principle, throughout the Contract life, and as defined in the Safety Case Report.

16.3.1 The Contractor shall cooperate with the duty holders for interfacing or interacting services or operations to enable effective management of Risk to Life.

16.3.2 Where necessary and with the duty holder agreement, the Contractor shall implement immediate action to manage Risks to Life until a longer-term resolution is identified.

Notes:

i. As these requirements relate to a service upon which a MOD military capability may depend, there is an explicit requirement on the Contractor to support the management of Risk to Life (as opposed to providing information to enable the MOD to do so). This is necessary and appropriate when the Contractor has responsibility for a service that may contribute directly to the in-service Risk to Life and will necessitate demonstrable compliance with the ALARP principle. This will be agreed with the MOD and defined in the scope

of supply and documented in the SMP. Decisions on whether a Contractor service that impacts on the Risk to Life is compliant with the ALARP principle will be made by the MOD duty holder endorsed through the mechanism of the MOD SMS.

ii. Guidance on ALARP in a military equipment context is available on the ASG.

iii. DAE specific guidance on ALARP is contained in RA1210.

iv. It is essential that plans ensure that the roles, responsibilities, communications and decision and action mechanisms are in place so as to manage the emergent risk. This is particularly essential where immediate action is necessary to deal with an emergent risk.

E.2 DO-178C Software Considerations in Airborne Systems and Equipment Certification

This standard governs the certification of software for airborne systems in commercial aircraft. Dated 2011 there is no consideration in this standard for the services that are provided in supporting airborne systems.

E.3 ISO 26262:2018 Road vehicles – Functional safety issue 2

This is an international standard for functional safety of electrical and/or electronic systems that are installed in production road vehicles. The body of the standard considers the safety lifecycle applying to road vehicles and their functional operation. It does not make any reference to or consideration of the services that are provided in supporting such vehicles and the electrical/electronic systems they incorporate.

E.4 The General Product Safety Regulations 2005

This is the statutory regulation that applies to any organisation placing a product on the market in the UK. It makes clear that no producer shall place a product on the market unless the product is a safe product. It does not make any considerations for where that product may be the provision of a safety-related or safety-critical service.

E.5 ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

This is an Aerospace Recommended Practice (ARP) used to demonstrate compliance with applicable U.S. Federal Aviation Administration (FAA) airworthiness regulations for transport category aircraft. It is also harmonised with equivalent European Aviation Safety Agency (EASA) regulations. This ARP sets out an appropriate range of analysis techniques (e.g. Functional Hazard Assessment (FHA), Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA)) that can be used to support the Safety Assessment Process. It does not consider where the safety assessment required is pertaining to a provision of service 'Product'.

This page is intentionally blank

Annex F Service Blueprints

"Do some selfless service for people who are in need. Consider the whole picture, not just our little selves."

A Service Blueprint is a high-level way of describing a service and its implementation, https://en.wikipedia.org/wiki/Service_blueprint. There are many different forms and levels of detail in various blueprint diagrams. It is relevant to service assurance as a blueprint could be used to identify potential failures of the service via its workings.

Some definitions of a Service Blueprint are:

i *The service blueprint is a technique originally used for service design. The service blueprint is an applied process chart which shows the service delivery process from the customer's perspective. The service blueprint has become one of the most widely used tools to manage service operations, service design and service positioning.*

ii *A service blueprint is a template defining potential services, either as basic services or as service compositions. It may include interface, parameters, internal structure, and other elements. Like classes in object-oriented programming, blueprints build a specialization hierarchy. This concept enables polymorphic instantiation of services and is the key concept supporting unconstrained reconfiguration at run-time.*

iii *A service blueprint is a diagram that visualizes the relationships between different service components — people, props (physical or digital evidence), and processes — that are directly tied to touchpoints in a specific customer journey.*

A typical blueprint diagram is shown in Figure F-1.

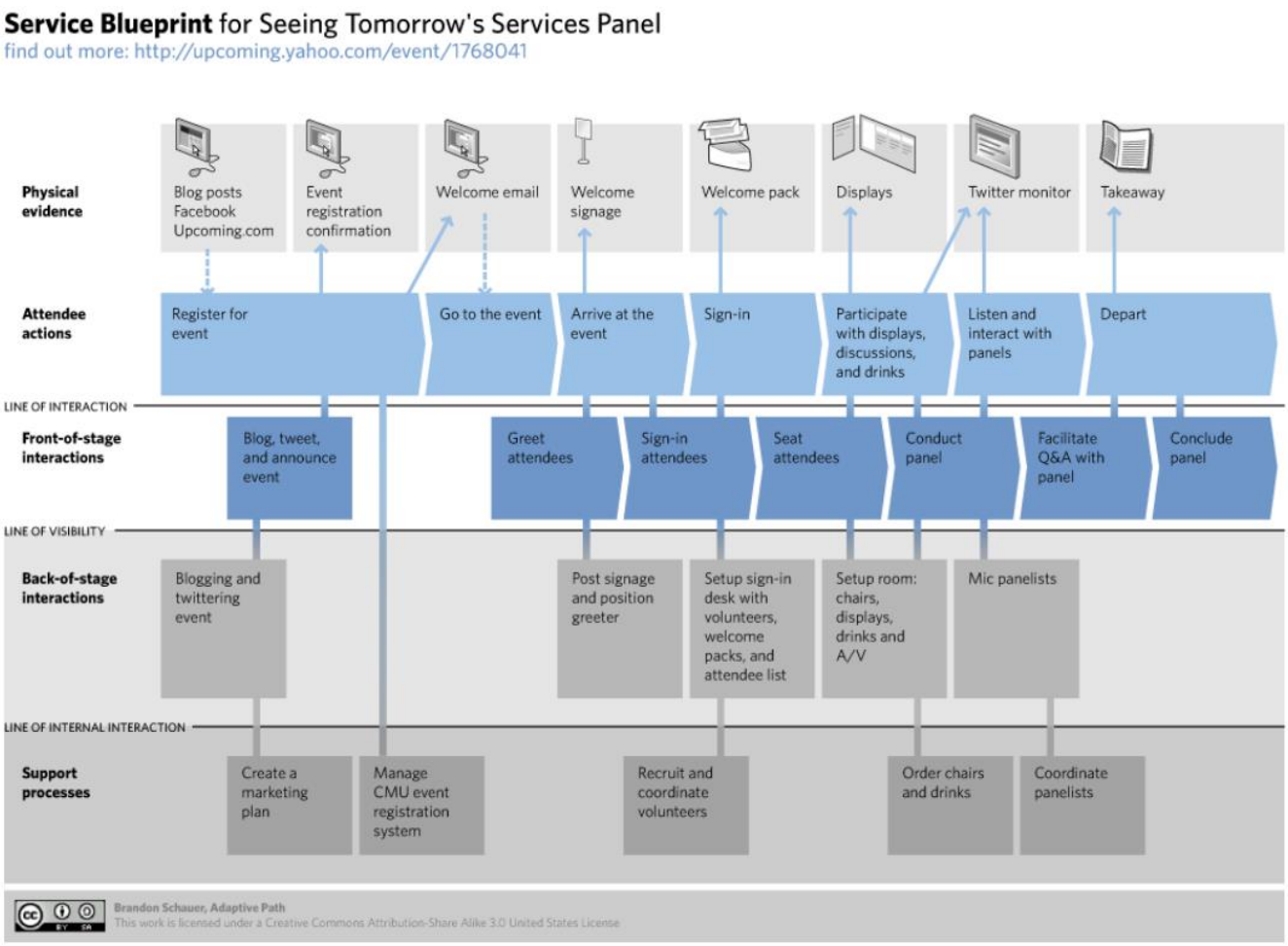


Figure F-1 - Organisations involved and the services provided

A failure analysis could then consider failures of each entity, interaction, and activity, looking at how these would impact on the rest of the service by following the elements of the diagram. This is thought to be a useful way of establishing failures and associated mitigations for a specific service. SPMN is a related technique (see Table 18 – Service Analysis Techniques).

Annex G Key Terms and Acronyms (Discursive)

"How can I be useful, of what service can I be? There is something inside me, what can it be?"

Vincent Van Gogh

G.1 Key Terms

Term	Definition	Source	Already adopted by SCSC?
Assurance	Grounds for justified confidence that a claim has been or will be achieved	ISO/IEC 15026-1: 2019; Systems and Software Engineering - Systems and Software Assurance Part 1: Concepts and vocabulary	Assurance Case Guidance
Consequence	Outcome of an event affecting objectives Note 1: An event can lead to a range of consequences. Note 2: A consequence can be certain or uncertain and can have positive or negative effects on objectives. Note 3: Consequences can be expressed qualitatively or quantitatively. Note 4: Initial consequences can escalate through knock-on effects	ISO GUIDE 73:2009, Risk Management - Vocabulary	Assurance Case Guidance
Event	Occurrence or change of a particular set of circumstances Note 1: An event can be one or more occurrences, and can have several causes. Note 2: An event can consist of something not happening. Note 3: An event can sometimes be referred to as an "incident" or "accident". Note 4: An event without consequences can also be referred to as a "near miss", "incident", "near hit" or "close call".	ISO GUIDE 73:2009, Risk Management - Vocabulary	Assurance Case Guidance
Hazard	A hazard is anything that can cause harm to people	HSE Risk Toolkit	No
	A potential source of harm.	ISO GUIDE 51: 2014 Safety Aspects - Guidelines for their inclusion in Standards	No
Likelihood	Chance of something happening Note 1: In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically [such as a probability or a frequency over a given time period]. Note 2: In risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.	ISO GUIDE 73:2009, Risk Management - Vocabulary	Assurance Case Guidance

Term	Definition	Source	Already adopted by SCSC?
Risk	Combination of probability of occurrence of harm and the severity of that harm.	ISO GUIDE 51: 2014 Safety Aspects - Guidelines for their inclusion in Standards	No
	Effect of uncertainty on objectives [of a stakeholder] Note 1: An effect is a deviation from the expected - positive and/or negative. Note 2: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. Note 3: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Note 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. [thus providing the basis for a risk metric]	ISO GUIDE 73:2009, Risk Management - Vocabulary	Assurance Case Guidance
Safety	Freedom from risk [of harm] which is not tolerable.	ISO GUIDE 51: 2014 Safety Aspects - Guidelines for their inclusion in Standards	Assurance Case Guidance
Service	See Section 1.3		No
Service Consumer	Consumer of one or more services.	SAWG Service Assurance Guidance Section 1.4	No
Service Provider	Provider of one or more services.	SAWG Service Assurance Guidance Section 1.4	No
Tolerable	level of risk that is accepted in a given context based on the current values of society Note 1 to entry: For the purposes of this Guide, the terms “acceptable risk” and “tolerable risk” are considered to be synonymous.	ISO GUIDE 51: 2014 Safety Aspects - Guidelines for their inclusion in Standards	No
Wrapper	An assurance augmentation which addresses the assurance deficit inherent in the consumed service in some way.	SAWG Service Assurance Guidance Section 3.1, Table 3: Principle 3	No

G.2 Abbreviations and Acronyms

Acronym	Meaning
AAIB	Air Accidents Investigation Branch
ADD	Acceptable Deferred Defects
ALARP	As Low As Reasonably Practicable
AMHS	Adult Mental Health Services
AMM	Aircraft Maintenance Manual
APU	Auxiliary Power Unit
ARP	Aerospace Recommended Practice
ASD	Autism Spectrum Disorder

Acronym	Meaning
ASG	Acquisition System Guidance
ATS	Air Traffic Service
BPMN	Business Process Model and Notation
BPMA	Business Process Models Analysis
BS	British Standard
CAA	Civil Aviation Authority
CAE	Claims, Argument and Evidence
CAMHS	Child and Adolescent Mental Health Services
CBDI	Component-Based Development and Integration
CC/CMA	Common-Cause / Common-Mode Analysis
CONOPS	Concept of Operations
COSS	Controller of Site Safety
COTS	Commercial Off The Shelf
CRE	Contractor's Responsible Engineer
DAE	Defence Air Environment
DEF STAN	Defence Standard
DNA	Deoxyribonucleic Acid
DO	Document
DSIWG	Data Safety Initiative Working Group
EASA	European Aviation Safety Agency
EMC	Electro Magnetic Compatibility
EN	European Norm
EU	European Union
FAA	Federal Aviation Administration
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FSR	Flight Status Reporting
FTA	Fault Tree Analysis
GCU	Generator Control Unit
GP	General Practice / General Practitioner
GSN	Goal Structuring Notation
HAZOP	Hazard and Operability study
HSE	Health & Safety Executive
HSIB	Healthcare Safety Investigation Branch
ID	Identifier
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
LSA	Level of Service Assurance
MAIB	Marine Accident Investigation Branch
MEL	Minimum Equipment List
MOD	Ministry of Defence
MRO	Maintenance and Repair Organisation
NHS	National Health Service
OLA	Organisational Level Agreement
OME	Ordnance, Munitions, Explosives
ORA	Organisational Risk Analysis

Acronym	Meaning
PCR	Polymerase Chain Reaction
PLA	Port of London Authority
PSS	Products, Systems and Services
QRH	Quick Reference Handbook
RAIB	Rail Accident Investigation Branch
RIE	Rectification Interval Extension
RRV	Road-Rail Vehicle
SA	Service Analysis
SAWG	Service Assurance Working Group
SBS	Service-Based Solution
SBTA	Service Bow-Tie Analysis
SC	Service Contracting
SCC/CMA	Service CC/CM Analysis
SCSC	Safety-Critical Systems Club
SDA	Service Decision Analysis
SF	Service Staffing
SFA	Systems-Focussed Analysis
SFFA	Service Functional Failure Analysis
SFMEA	Service Failure Modes and Effects Analysis
SFORA	Service Focussed Organisational Risk Analysis
SFRAM	Service Functional Resonance Analysis Method
SFSA	Service Focussed Systems Analysis
SH	Service Change
SHA	Service Hazard Analysis
SHAIR	Service-Related Historical Accident and Incident Report
SIA	Service Interaction Analysis
SLA	Service Level Agreement
SMCA	Service Metrics and Contracts Analysis
SMP	Safety Management Plan
SMS	Safety Management System
SP	Service Process
SPFA	Service Process Failure Analysis
SPMN	Service Process Modelling Notation
SoW	Statement of Work
SOA	Service Oriented Architecture
SR	Service Regulation
SS	Service Assurance
SSA	Service Structure Analysis
SSPFA	Service Single-Point Failure Analysis
SSS	Safety Critical Systems Symposium
STAMP	System-Theoretic Accident Model and Processes
STPA	Systems Theoretic Process Analysis
SV	Service Verification
SY	Service Delivery
TBD	To Be Defined
TC	Technical Committee
UK	United Kingdom
UML	Unified Modelling Language

Annex H References

"Wealth, like happiness, is never attained when sought after directly. It comes as a by-product of providing a useful service.

Henry Ford

AAIB (2018) Aviation Accident Investigation Branch Report 04/2018, Available at https://www.gov.uk/aaib-reports, accessed October 2019.

AAIB (2018) Aviation Accident Investigation Branch Report 09/2018, Available at https://www.gov.uk/aaib-reports, accessed October 2019.

AAIB (2018) Aviation Accident Investigation Branch Report 10/2019, Available at https://www.gov.uk/aaib-reports, accessed October 2019.

AAIB (2021) Aviation Accident Investigation Branch Bulletin 1/2022, Available at https://www.gov.uk/aaib-reports, accessed December 2021.

AAIB (2022) Aviation Accident Investigation Branch Bulletin 2/2023, Available at https://www.gov.uk/aaib-reports, accessed January 2023.

BBC Website (2010), BBC Website Thursday, 29 April 2010 US declares oil spill of 'national significance'

BP (2010), BP Deepwater Horizon Accident Investigation Report September 8, 2010 Executive Summary

Catmur J, King K, Parsons P and Taradi F (2022) A Service Analysis of the Mont Blanc Tunnel Fire Accident in Nicholson M and Parsons M, "The Future of Safe Systems", SCSC-178, 2023, https://scsc.uk/r178, accessed January 2023

Catmur J, Parsons M and Sleath M (2022), "A Step-by-Step Methodology for Applying Service Assurance", in Safer Systems: The Next 30 Years, SCSC-170, https://scsc.uk/scsc-170, accessed October 2022

DHSG Deepwater Horizon Study Group. 2011, Final Report on the Investigation of the Macondo Well Blowout. Deepwater Horizon Study Group. March 1, 2011.

DSIWG (2018), Data Safety Guidance (Version 3.1) by the SCSC Data Safety Initiative Working Group [DSIWG], SCSC-127C, 2019, https://scsc.uk/scsc-127C, accessed October 2019

Harris C, Parsons M and Simpson A (2018) Service-Based Safety Assurance in Kelly T and Parsons M, "Evolution of System Safety", SCSC-140, 2018, https://scsc.uk/r140/8:1, accessed October 2018

Hawkins R, Habli I and Kelly T (2013), "The Principles of Software Safety Assurance", International System Safety Conference (ISSC) 2013, Boston, https://www-users.cs.york.ac.uk/rhawkins/papers/HawkinsISSC13.pdf, accessed October 2018

HSIB (2017) Healthcare Safety Investigation Branch Report I2017/008, Available at https://www.hsib.org.uk/investigations-cases/transition-from-child-and-adolescent-mental-health-services-to-adult-mental-health-services/, accessed October 2019.

HSIB (2017) Healthcare Safety Investigation Branch Report I2017/010 https://www.hsib.org.uk/investigations-cases/implantation-wrong-prostheses-during-joint-replacement-surgery/, accessed October 2019

ITIL (2018), ITIL - IT Service Management, https://www.axelos.com/best-practice-solutions/itil accessed October 2018

MAIB (2017) Marine Accident Investigation Branch Report 24/2017, Available at https://www.gov.uk/maib-reports, accessed October 2019.

MAIB (2018) Marine Accident Investigation Branch Report 14/2018, Available at https://www.gov.uk/maib-reports, accessed October 2019.

MAIB (2018) Marine Accident Investigation Branch Report 16/2018, Available at https://www.gov.uk/maib-reports, accessed October 2019.

MAIB (2018) Marine Accident Investigation Branch Report 21/2018, Available at https://www.gov.uk/maib-reports, accessed October 2019.

MAIB (2021) Marine Accident Investigation Branch Report 14/2021, Available at https://www.gov.uk/maib-reports, accessed December 2021.

MAIB (2022) Marine Accident Investigation Branch Report 10/2022, Available at https://www.gov.uk/maib-reports, accessed January 2023.

MAIB (2022) Marine Accident Investigation Branch Report 12/2022, Available at https://www.gov.uk/maib-reports, accessed January 2023.

RAIB (2015) Rail Accident Investigation Branch Report 15/2015, Available at https://www.gov.uk/raib-reports, accessed October 2019.

RAIB (2018) Rail Accident Investigation Branch Report 06/2018, Available at https://www.gov.uk/raib-reports, accessed October 2019.

RAIB (2018) Rail Accident Investigation Branch Report 19/2018, Available at https://www.gov.uk/raib-reports, accessed October 2019.

RAIB (2019) Rail Accident Investigation Branch Report 01/2019, Available at https://www.gov.uk/raib-reports, accessed October 2019.

RAIB (2019) Rail Accident Investigation Branch Report 12/2019, Available at https://www.gov.uk/raib-reports, accessed October 2019.

RAIB (2021) Rail Accident Investigation Branch Report 02/2021, Available at https://www.gov.uk/raib-reports, accessed December 2021.

RAIB (2021) Rail Accident Investigation Branch Report 07/2021, Available at https://www.gov.uk/raib-reports, accessed December 2021.

RAIB (2022) Rail Accident Investigation Branch Report 04/2022, Available at https://www.gov.uk/raib-reports, accessed January 2023.

RAIB (2022) Rail Accident Investigation Branch Report 11/2022, Available at https://www.gov.uk/raib-reports, accessed January 2023.

Reason, James (1990). "The Contribution of Latent Human Failures to the Breakdown of Complex Systems". Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences. 327 (1241): 475–84.

SAWG (2018), Working Group Pages on SCSC website, https://scsc.uk/gs, accessed October 2019

Spriggs J. (2016), "Assurance by Proxy" https://scsc.uk/re378.20, accessed November 2018

Sunrise Vimeo 2018, Sunrise Media and Entertainment, BP Deepwater Horizon Accident Investigation Vimeo

Transocean 2010, "Fleet Specifications: Deepwater Horizon". Transocean. Archived from the Original on 19 June 2010. Retrieved 9 June 2018

This page is intentionally blank

Annex I STPA Summary Example for Highways Services

"It's not the destination, it's the journey"
Ralph Waldo Emerson

I.1 Tools for the Technology Operations Capability (T-TOC) service STPA

Multiple asset and fault management systems overseeing England's road network have been introduced by third party contractors in recent years. Highways England (now National Highways) wanted to centralise these systems, consolidate all the information and services that have been outsourced, and bring the overall process back in-house. This involved delivering a software system capable of monitoring and managing the 100,000 intelligent infrastructure devices across England's strategic road network.

By logging, tracking and monitoring everything through ServiceNow (https://www.servicenow.com/uk/), National Highways gained a new level of continuity. It can directly manage its assets; control data collection, storage and access; reduce reliance on third parties; and develop its staff.

T-TOC will make the incident management process more efficient, with maintenance teams alerted directly through ServiceNow. (see: https://www.mottmac.com/article/62538/tools-for-the-technology-operations-capability-t-toc)

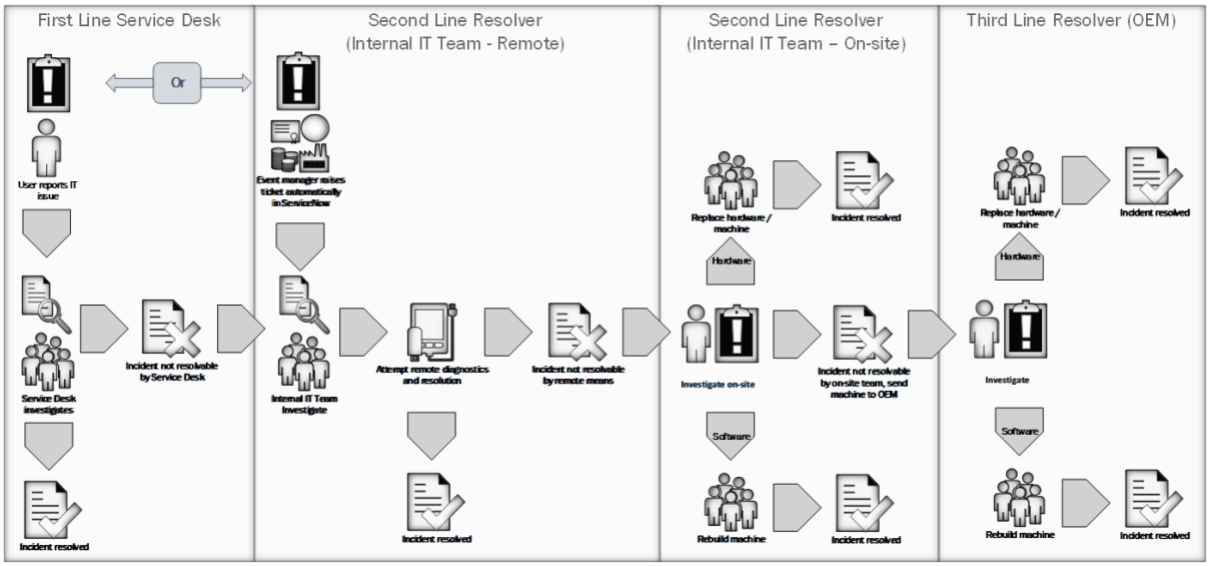


Figure I-1 – T-TOC Information Flow Through Service Levels

It was recognised that the T-TOC service would have safety-related aspects as the road assets include items such as detectors, signs and signals and so a safety review was needed.

STPA was used to review and analyse the service's safety. Prior to the STPA the relevant hazards were identified from their highway hazard register and then an STPA was performed on the defect

management service design to identify safety requirements for the overall system, its internal interfaces and also for the external interfaces between the service, sources of defects and parties managing defect resolution.

Both internal and external interface data flows were analysed using STPA and used to develop safety requirements at each step/interface. Each data flow 'chevron' in the diagram above was assessed using the STPA process and the safety requirements related to the data flow were identified. The intermediate steps are not shown due to commercial confidentiality, but the end result was a set of tables for attributes of requirements for process, organisation, etc. (Table I-1, below).

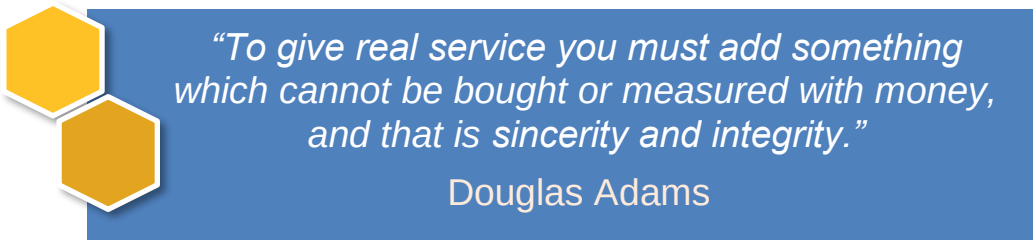
Table I-1 – T-TOC Required Attributes for Process and Organisation

Process	
P-01	Processes and procedures in place to verify and validate the information received and source before the ticket is passed on.
P-02	Triage information regardless of where the report has come from or whether the reporter is an expert.
P-03	Process is designed so that steps in the triage cannot be bypassed.
P-04	Processes and procedures in place to ensure tickets are being raised through the correct channels.
P-05	Report service interruptions and provide alternative channels when services are down. There should also be arrangements in place to manage the interruptions and restore normal service.
P-06	Procedures in place to guide people on how to use the tools including raising tickets, providing evidence, recording issues and interrogation methods.
P-07	Make people aware of the importance of providing information in a quick and structured way.
P-08	Process in place to allow information sharing / to support passing information between organisations defined in interface agreement.
P-09	Processes and procedures in place to set-up, check and update systems correctly.
P-10	Processes and procedures in place to feedback information to previous interfaces if relevant.
P-11	The reporting process should not cause action to be undertaken without verification.
P-12	Carry out analysis and problem management of reported technology incident before action to fix it is taken.
P-13	Process design and implementation shall be checked to make sure processes are correct.
P-14	Define process for access management to tool.
P-15	Record new technology incident when there is already an existing technology incident for this equipment to ensure multiple issues are captured.
P-16	Processes and procedures in place to deal with malicious technology incident reporting.

Process	
P-17	Providing clear processes and procedures.
P-18	Processes in place to ensure that the task can be done in a timely manner.
Organisation	
O-01	Provide training to obtain an understanding of assets that regularly need maintenance.
O-02	Training people on how to use the tools including raising tickets, providing evidence not solutions, recording issues, interrogation methods and best practice for communications.
O-03	Policy-makers and data analysts should work together to understand and prepare for malicious reports.
O-04	Share lessons learnt and best practice to optimise asset performance and minimise malicious reporting.
O-05	Security management in place including Customer Contact Centre security management.

This page is intentionally blank

Annex J Contributors (Discursive)



This guidance document has had the benefit of contributions from many people from across a diverse range of organisations from both industry and academia, covering the aviation, rail, maritime, defence and healthcare sectors. Note that contributions have been made on an individual basis and may not represent the views of the organisation that employs them or to which they are attributed. The inclusion of an organisation in the list below does **not** indicate that organisation agrees with the entire content of this guidance.

Contributors to this version of the guidance include:

- James Catmur, JC and Associates
- Kevin King, BAE Systems
- Mike Parsons, AAIP
- Mike Sleath, Consultant
- Andy Whitehead, Consultant

This page is intentionally blank

Annex K Acknowledgements (Discursive)

"Businesses often forget about the culture, and ultimately, they suffer for it because you can't deliver good service from unhappy employees.."

Tony Hsieh

The document contributors would like to thank:

- The Safety Critical Systems Club (SCSC).
- The editorial team. In particular Kevin King and Mike Parsons for performing updates, James Catmur for new material and Andy Whitehead for detailed reviewing.
- Mike Parsons for chairing the working group meetings.
- Alex King for support with cover image and branding.
- All the organisations that have provided support to the contributors to this guidance.
- Those that have supported this work despite being unable to attend meetings.

Service Assurance Guidance
by the SCSC Service Assurance Working Group [SAWG]

This document provides guidance on the assurance of services when there are safety implications associated with the use of these *safety-related services*. Examples of such services are: an ambulance dispatch service, a mountain rescue service or an air traffic control service.

A set of principles, objectives and analyses for assuring services is described. These are domain agnostic and can be used across a wide range of service scenarios in diverse sectors. Methods and techniques applicable to different service situations are covered. Techniques for identifying and assessing the undesired behaviours of the services are described.

The approach described in this guidance draws upon concepts from modular assurance and illustrates the different types of additional assurance, a "wrapper", that can be used to supplement the assurance positions presented by existing services.

SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY