Service Assurance Guidance

By the SCSC Service Assurance Working Group (SAWG)

The SCSC Service Assurance Working Group (SAWG) gives insights into the Service Assurance Guidance document, published in February 2020, which provides guidance for the assurance of services when working in a safety context.

The Service Assurance Guidance document [1] was produced because many safety-related systems are now implemented and used in a service context, specifically:

- There is a significant shift to a service-based approach for delivery, especially in information technology with the use of cloud computing
- It is now recognised that collaborative working of systems, organisations, people and processes all contribute to safety
- A service-based approach to assuring safety provides a different perspective that extends beyond system analysis

The guidance document applies to the assurance of services when there are safety implications associated with the use of those services. These services are '*Safety-Related Services*'. Examples might be an ambulance dispatch service or an air traffic control service.

Introduction

Many safety-critical systems utilise services that are designed, developed, operated and maintained outside the immediate boundaries of the system. 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 technologies.

Example: Passengers struck by a flying cable at a station

As a brief example, here is an excerpt from a service-related accident in the rail sector. This example is discussed in more detail in the paper (King et al 2020) [5].

"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) [6].

This incident highlights the importance of services that should be utilised at regular intervals. In this case the 'cable inspection' service and 'station safety checks' service both of which were probably carried out by the same staff some time prior to the incident. Both services

involve people, process and equipment, and should have been carried out with a level of assurance. A case of over-familiarity was likely a flaw in the service execution.

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 technologies

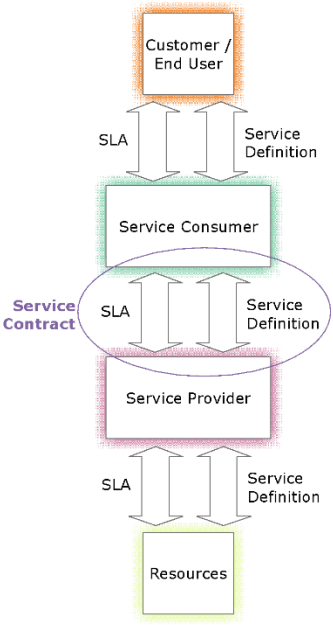
A Service View of Safety

A service-oriented view of safety may be able to identify and manage safety risks more effectively since it highlights the collaboration of various elements of the socio-technical situation (people, organisations, processes, maintenance, change, automation, through-life aspects etc.) 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).

What is a Service?

The term "Service" is not clearly defined across standards and has many uses. The way that a Service is normally described or defined is very different from the specifications and descriptions more commonly employed in safety-related systems. An individual Service (or *Service Component*) is typically described by a Serv*ice Provider* via an entry in a *Service Catalogue*. The Service Catalogue describes the externally visible capabilities/functionality offered to a *Service Consumer* without providing implementation detail, in fact, it is unusual for any aspects of the design and implementation of the Service to be visible to the Consumer.



A summary of key terms is given below:

- A **Service Provider** provides one or more Services.
- A **Service Consumer** consumes one or more Services.
- A **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. It often includes a service catalogue.
- A **Service Level Agreement (SLA)** is 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.
- The **Service Contract** is the contractual agreement between Service Provider and Service Consumer.
- 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.

Characteristics of Services

It is 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. Six key service characteristics are given in the following table:

ID	Service Characteristic	Context	Compared to Systems / Products
C1	Services are provided for the duration of the service contract	By definition, services provide features with a given performance for the duration of the contract between provider and consumer. So e.g. the consumer does not have to be concerned with the design, maintenance or disposal of the service components.	Products usually provided with warranties but there may be no further involvement from the provider after product acquisition. The consumer is responsible e.g. product maintenance and disposal.
C2	Services 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 too many bespoke solutions	Similar, but products often designed to exacting specifications. Can be easier to remove features of products for particular customers.
C3	Services likely to be used by more than one consumer	Providers usually desire to sell similar service offerings (catalogues) to a wide range of customers, so multiple consumers can be using the same service offering at the same time (or sharing resources of other services)	Not so easy to segregate services or have sufficient visibility to understand and control potential forms of interference and disruption
C4	Services are implemented through a combination of people, procedures, products and other services	Service implementation requires the collaborative working of people, processes, products and other services to deliver a set of features with the desired performance	Similar to 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 desire a quick route to market, so may release their 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 decide to exploit (unexpected uses).	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. Changes in the underlying service provision may increase the likelihood of undesired emergent properties.

ID	Service Characteristic	Context	Compared to Systems / Products
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 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 consumer.

Service Assurance Principles

The following table presents the Service Assurance Principles as a way of structuring the service assurance activity together with brief rationale:

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 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 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.

The principles are similar to those used for software safety assurance, with the addition of #6 which is concerned with change and evolution. This set has been developed over the last few years [2], [4]. This set of principles are considered necessary and sufficient for assurance of services in a safety context; how they are achieved is through objectives, see below.

Objectives for Principles

The principles form the high-level "mission statement" of service assurance. These are mapped to a set of Service Objectives forming the next level of specification. If the objectives for a principle are met, then the principle is considered satisfied. The following table shows how the principles may be mapped to lower-level 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 shall be undertaken 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 the defined set of these objectives f. Lessons learnt SHALL be incorporated in the SBS

The objectives can be treated as requirements (with further elaboration), and therefore give a means of compliance to the principles. The guidance document introduces selection of objectives depending on the level of service assurance required.

Who is Responsible?

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

Level of Service Assurance

The concept of Level of Service Assurance (LSA) is an important one. Differing amounts of assurance are required for different types and instances of service usage. The LSA is defined by the level of risk in using the service (defined by the consumer of the service):

LSA	Definition (Service Consumer View)	Additional Clarification
LSA 0	No safety aspects present in service	There is no obvious route to harm to humans or the environment from use of the service
LSA 1	Minor safety aspects with little impact of failures (minor injury possible but unlikely)	Harm is unlikely as there are many mitigations in place and plenty of time to recover the situation
LSA 2	Safety aspects with some impact of failures (several injuries possible)	Some harm is possible (to one or more people), but there are mitigations in place and some time to recover the situation
LSA 3	Significant safety aspects with service with major impact (could indirectly lead to single death or multiple injuries)	Significant harm is possible to several people; there are a few mitigations in place; there may be little time to recover
LSA 4	Service is safety-critical: service failures could have catastrophic impact (could directly lead to multiple deaths)	Major harm is immediately possible to many people and there are limited or no effective mitigations if the service fails. There is almost no time to recover.

NB: Here harm refers to people or the environment. This could be extended to cover other aspects if required, e.g. assets or platforms.

Five levels are considered appropriate and give enough granularity to be distinct. The key aspect to remember about these levels of service assurance, is that they are based on the service consumer's view. Services are often generic (e.g. a wireless communication system), used by many consumers and it all depends on how the service is used by this particular consumer (i.e. for what safety-related applications it is intended).

Objectives and Applicability

The guidance document has a table that 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. Hence the LSA defines the quantity, breadth and rigour of the service assurance required from the assurance provider.

Evidence to meet Objectives

The guidance gives tables of example techniques for the production of evidence against each objective. These are:

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

Service Analyses

It is recognised that different (or modified) safety analysis techniques may be required to analyse a safety-related service, including systems, people and process aspects. Some of these are:

- Service Functional Failure Analysis [SFFA]
- Service Failure Modes and Effects Analysis [SFMEA]
- Service Hazard Analysis [SHA]
- Service Business Process Failure Analysis [SBPFA]
- Service Interaction Analysis [SIA]
- Failure Analysis of Agreements [FAA]
- Service Structuring Analysis [SSA]

Further details are given in the guidance.

Case Studies

Examples are discussed in the guidance document, including incidents and accidents from across industry where service failures are considered to be significant contributory factors. The Deepwater Horizon accident is considered in some detail [3].

Conclusion

Services are increasingly being used to provide safety-related functionality to end users. There is currently no standard or guidance that addresses the general assurance of services in a safety context.

The service assurance guidance document is important because, for the first time, it recognises this delivery of safety functionality via services and gives a framework for assuring those services. The framework includes principles, objectives and means of achieving those objectives and assurance levels thus giving a method for achieving an assurance position in a particular situation.

The guidance has now been issued for comment and any feedback on its application is appreciated.

An updated version of the guidance will be issued at SSS'21 in February 2021.

References

[1] Service Assurance Guidance, The SCSC Service Assurance Working Group (SAWG), Feb 2020, https://scsc.uk/scsc-156

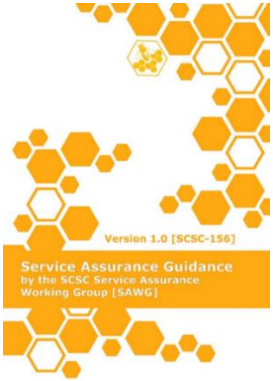
[2] Durston N, Scott A, Parsons M, Simpson A (2019), The Principles of Service Assurance, in Kelly T and Parsons M, "Engineering Safe Autonomy", SCSC-150, 2019, https://scsc.uk/rp150.6:1, accessed April 2020

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

[4] 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

[5] King, K, Parsons M, Sujan, M (2020) A Service Perspective on Accidents, in Nicholson M and Parsons M, "Assuring Safe Autonomy", SCSC-154, 2020, https://scsc.uk/rp154.6:1, accessed April 2020

[6] RAIB, Report 06/2018, Passengers struck by a flying cable at Abergavenny (Y Fenni) station https://www.gov.uk/raib-reports/report-06-2018-passengers-struck-by-a-flying-cable-at-abergavenny-y-fenni-station, accessed April 2020



scsc.uk/SCSC-156

SCSC Service Assurance Working Group (SAWG)

The SCSC Service Assurance Working Group (SAWG), led by Mike Parsons, has been set up to produce clear and practical guidance on how services should be managed in a safety related context, to reflect emerging best practice.

Comments or suggestions for the Service Assurance Working Group (SAWG) and the Guidance Document are welcome at:

sawg-comments@scsc.uk