SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

SAWG

SCSC Service Assurance – WG Meeting 3

21st June 2017, NATS, London

Minutes and Actions

Attendees

Mike Parsons (MP) – NATS, Jose Faria (JFa) - Safe Perspective Ltd, Simon Scutt (SS) - Thales, Jane Fenn (JFe) - BAE, Philippa Ryan (PR) - Adelard, Sean White (SW) - NHS Digital (by phone), Kevin King (KK) - BAE, Craig Harris (CH) – Leidos, Katrina Attwood (KA) – University of York, Catherine Menon (CM) - Imperial College

Apologies

Alan Simpson (AS) – Ebeni, Andy Scott (ASc) – NATS, Paul Hampton (PH) – CGI, Mark Machin (MM) – CGI, John Findlay (JF) – QinetiQ, John Penny (JP) – CAA, Kevin Holland (KH) – NHS Digital

Agenda

1. Scoping Inputs – Service Context
2. Update on STAMP/STPA approach to Service Assurance
3. Assurance of Services in Health IT
4. Hatfield Rail Accident
5. Skeleton of Guidance Document
6. WG Meeting and Communications Schedule

NOTE: All comments or opinions in these notes are attributed only to individual attendees of the meeting, not to their respective organisations.

*[Note that actions are presented in the form **N.Mx** where **N** is the meeting number, **M** a reference number for the action raised in that meeting and **x** is an optional letter that differentiates related actions arising from the same discussion point*

Meeting slides are available [7].

1. Scoping Inputs

Discussion of straw man *"The Service Context for Service-Based Safety Assurance"*

The group discussed the "straw man" document [1] produced by CH and ASi. The ITIL definition of an IT service ("a means of delivering value to customers by facilitating the outcomes customers want to achieve without the ownership of specific costs and risks") has wide currency, and was the basis for the group's discussion. The meeting agreed that it was essentially a "fool's errand" to define a service a priori, and that using examples to illustrate common characteristics of "things that can be put through the service assurance approach" is a more sensible way forward. The focus of the

discussion was on the distinction between services and traditional systems assurance, i.e. what characterises a safety service:

- The service provides/supports/underpins some safety-related functionality
- The service is provided from one or more organisations (loosely defined) to another
- The service comprises a combination of people, technology, processes, products, etc. – i.e. it is more than functionality or data which would be normally delivered from one company to another
- The consumer of the service does not necessarily have visibility of how the service is delivered – i.e. it is not always possible to "see inside the box"
- The provider of the service may not have visibility of the context in which the service is consumed, but can provide limitations on usage (e.g. minimal hardware requirements, etc.)
- The service may include many COTS components, which are difficult to assure by established methodologies (because, e.g. the component was not developed to be safety-related or because commercial issues prevent "opening the box")
- The complexity of the components of the service (especially software) make established safety assurance methods impractical
- Changes to the implementation of the service may not be under the control of the service consumer

Terminology

The group agreed that there was a need to clarify terminology and concepts.

Action 3.1 [CH] Create a glossary alongside the straw man document, and keep it active during future discussions/reviews etc.

Initial concepts for inclusion in the glossary included 'service', 'SLA', 'contract', 'consumer'. There was also some discussion as to whether a term other than 'black box', 'opening the box' and so on, was needed in discussing the characteristics of a service.

Accountability and Contracts

JFe raised the issue of accountability arising from the ITIL service definition (see above), which defines a service as facilitating outcomes "without the ownership of specific costs and risks". Obviously, this presents issues in an assurance context – generally safety risk cannot be "handed down" in this manner. It was agreed that a clear understanding of who controls what, throughout the service, and of where accountability lies is necessary. Service provider and consumer need to be clearly defined. Dependencies and risk need to be clarified, 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). 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.

There was considerable discussion of the commercial framework for services, the essential point being that the service provider is at liberty to not to meet the contract (e.g. for availability of the

service) and to pay a financial penalty in compensation. This model does not work for services contracted in a safety-related environment: issues other than availability of the service may need to be compensated for (e.g. reputation, loss of life, wider impact). The notion of a *service wrapper* at the contractual level was discussed – where the delta required for safety was clearly stated (for example, that the service provider needed to provide evidence of an effective SMS). There was also a need to consider a designer's responsibilities here: as a designer, you cannot assume that providers meet a SLA just because there is a financial penalty for failure – what are the responsibilities on the designer, in terms of accommodating service issues?

It also seemed likely that the notion of *contract stacks*: an overarching framework contract, with layers of lower-level contracts supporting particular aspects of the overall service would be useful. Further visibility of the current contractual context for safety-related services was required.

Action 3.2 [JFe] Talk to BAE contracts people and attempt to do a "contractual comparison", indicating where contracts for safety-related services differ from non-safety related ones (e.g. a mobile phone).

Further issues

Things that may need to be covered in the guidance:

- The guidance needs to bring out the idea of the **resources being shared**, with the assurance issues which arise from this. One example would be generic, public Cloud services.
- The **openness of the system** also needs to be considered: 'bring your own device'-type of arrangements, or situations where connections are made accidentally to public services.
- The issue of **accidentally providing a service** (e.g. by starting a mobile hotspot to which others can connect), and the assurance/accountability issues arising from this.
- The guidance needs to discuss **requirements flowdown** through the architecture: how do we translate high-level safety requirements into lower-level requirements on the service (e.g. availability, accuracy of data, etc.), and how can we be sure that the translation is good enough for safety?
- This raised the need for **resilience requirements**, over and above the service itself. Open questions (on which we will need to provide guidance):
    - How can resilience requirements be derived from an SLA?
    - How do they interact?
    - How is this managed contractually – especially in terms of a secondary supplier arrangement where there may be no direct link with the prime?
- Part of the guidance will need to address the **application of safety analysis techniques to SLAs** – we will need to be clear about the need to analyse both the services and the SLAs.
- This in turn requires explanation of **how risks flow up and down the service stack,** and **where the mitigations are.** Is there a need for some entity outside the SOAs with an overall understanding of the flow of risk? (If that is even possible - the complexity is extensive and multi-dimensional; the correlation with the safety-case contract work was noted).
- **Failures will propagate across services**, 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 needs to be reflected in contractual arrangements.

- We need to consider the issue of **Services of Services** (i.e. services are layered and may consume other services).
- **Audience**: we also need to clarify who the guidance is targeted at: providers, consumers, regulators, etc.

Additional Inputs

MP reported that he had received comments on the strawman document (in accordance with Action 2.1 from the previous meeting) from ASc. These were not examined in the meeting, but were passed to CH as input to the next iteration (see Action 3.3b below).

MP also mentioned that there is a NATS document, 'Assured ITSM for ATM' which outlines a NATS approach to some of the assurance challenges in the services space. See Action 3.4 below.

Action 3.3a [CH]: Revise the strawman document in accordance with the discussion.

Action 3.3b [CH]: Have a look at Andy Scott's comments and incorporate as appropriate in revising the strawman document.

Action 3.4 [MP]: **Make the NATS 'Assured ITSM for ATM' document available on the Share for the group [See ref: [6]].**

Action 3.5 [PR]: Ensure that the structure for the guidance document includes a section on the application of safety analysis techniques to SLAs.

2. STAMP/STPA and Service Assurance

JFa had not received any comments on his presentation at the previous meeting (cf. Action 2.3). Therefore, there had been no update to his slides [2]. There was discussion of the possible use of STAMP/STPA as a possible model to draw out the hazards relating to the issues relating to the 'breach of contract' ideas under discussion in the meeting (see section above): the control process model seems to fit this kind of relationship reasonably well. Abstract SOAs could be used as interfaces at various levels – they are not necessarily unique to the service, and would need to be different for different customers of the service. There was also discussion of the need to draw out the distinctions between the Statement of Work, the Contract and the SLA, in terms of where the requirements on the service itself and on monitoring of the service sit (typically, SoW has requirements on the service, while SLA identifies potential metrics). These relationships tend to be commercial, rather than related to assurance – could STAMP be used to help us map out the assurance-related requirements at different levels here?

There was also some discussion as to whether the layered model works for services – i.e. is it reasonable to assume that "layer I looks after level i-1"? For assured services, there needs to be visibility across the layers. We need to provide guidance on this, as well as on what needs to happen for assurance when the end customer does not have visibility of relevant aspects of the provision of the service: how much visibility is required? There also needs to be some recognition of the implications of change (e.g. use of different suppliers for underlying contract).

It was decided that a more tangible example of the application of STAMP/STPA to a service framework (i.e. a system with the characteristics defined in section 1 above) would be useful. Suggested examples included some part of NATS functionality, taxi service, ambulance service, etc.

Action 3.6 [JFa]: Prepare a STAMP/STPA example using a real service framework.

3. NHS Presentation

SW gave a presentation outlining the assurance of services safety in Health IT (slides available at [3]). He stressed that NHS Digital is outside the scope of the regulatory framework for medical devices, in the context of the Health and Social Care Act 2012. SW outlined the role of the NHS Digital Clinical Safety Group in reviewing and approving deployment (potentially with caveats) and their interactions with Clinical Safety Officers (within organisations – roughly aligning with Safety Engineers), First-of-Type sites and the independent Governance Board (whose input aligns roughly with a critical design review in an engineering organisation).

SW then presented a case study: the NHS Electronic Prescription Service. There was a discussion of the contractual context – including incentivisation and requirements-based contracting. The incident-management arrangements were also outlined (triggers, the role of the end user in alerting NHS Digital, classification and appraisal processes). Provision of a Minimum Data Set (if something happens, what do we need to know for safety?) and the application of severity levels to SLAs were also discussed.

SW identified a number of potential problem areas: brevity of the information received by NHS Digital, disparity in severity classifications across multiple parallel programmes, indeterminate nature of "care delivery" (services are a "best fit"), lack of safety competency in the manufacturer organisations, transition from ITIL-type service management to DevOps.

4. War Stories

Hatfield Rail Accident Summary

PR presented a summary of the Hatfield Rail Accident which took place in 2000. The presentation (slides available at [4]) was the result of a thorough reading of the Accident Report, from which PR had extracted issues relating to services which either did contribute to the accident or which could have contributed. PR raised a number of issues relating to the nature of the contract between Railtrack and Balfour Beatty, the political context of the industry, the limited choices available in terms of suitable maintenance service providers, technical changes in the understanding of the nature of track defects and technology available to detect them which took place prior to the accident but after the contract. This raised a general point about the need for SLAs to provide flexibility to incorporate improved service practices – including the recognition that there will be a cost implication here. PR also examined the service aspects in place immediately after the accident occurred – the availability of comms equipment, location services etc. She also explored the question of oversight and auditing (including across contractual boundaries), requirements creep, changes to the usage of the service in operation.

Discussion of the case study reflected on the need for the contract and SLA to reflect what the real drivers of a service are – i.e. safe operation of the railway, safety of maintainers. There was also a

discussion of the situation in terms of ALARP: does the service provider have a responsibility to consider whether he is presenting/contributing to a risk that is not ALARP? Does he have a responsibility if he has some knowledge of the service consumer's behaviour?

It was felt that the guidance to be produced by SAWG should include generic material on the legal position with regards to ALARP and the Service Provider. It seems likely that we would need to seek advice on this from someone with appropriate legal experience. Chris Elliott was mentioned. The cost implications of this would need to be examined.

Other War Stories

JFe reported that there had been no progress on preparing the Parachute Packing example (see Action 2.6 below).

SS offered to work up the Überlingen Incident as an example.

Action 3.7 [SS]: Explore the Überlingen Incident as a War Story example from the services point of view.

5. Skeleton of Guidance Document

PR presented the first version of the skeleton Guidance Document (see action 2.7 from previous meeting). The current version of this document is available at [5]. There was discussion relating to the need to include bottom-up communication and analysis of risk, (potentially) the provision of Service Integrity Levels (and a discussion of proportionality in the application of this) and generic advice on how safety cases could be constructed to reflect the service-based safety assurance approach. A section on existing guidelines and standards was also proposed.

Action 3.8 [PR]: Revise document skeleton in accordance with the discussion and send to MP.

6. WG Meeting and Communications Schedule

The next meeting is on 7th September 2017 at BAE Systems, Farnborough, http://scsc.org.uk/e523 .

7. AOB, etc.

MP reported that a paper abstract relating to the work of the group has been accepted for SSS'18. The authors are CH, AS and MP and contributions from the WG members are welcome.

Action 3.9 [MP]: Circulate the SSS'18 paper abstract [See ref. [8]]

8. Thanks

Thanks to KA for taking the minutes and actions.

Thanks also to NATS for hosting the meeting.

9. Summary of Open Actions

Ref	Owner	Description	Action
1.2	**MP, CH, JFe, ASc**	Rework assurance properties + language + context of them	Ongoing

Ref	Owner	Description	Action
1.5	**All**	Everyone to find war stories related to services	Ongoing
1.7	**KK**	See if someone from BAE could explain how the service contracts work in their situation	Ongoing
2.0	**SW**	Talk to colleagues about potential examples of medical devices procured as services	Closed
2.1	**All**	Comment and feedback to MP on the strawman "The Service Context for Service-Based Safety Assurance" [1].	On hold until a new version produced
2.2	**ASc**	Examine safety requirements of service contracts at NATS	Ongoing
2.3	**All**	Review STAMP/STPA slides and feedback comments to MP or JFa	On hold until a worked example produced
2.4	**KH**	Send some relevant white papers to the group on these new topics (DevOps, SIAM) and also an ITIL introductory overview	Closed (see references to previous meeting)
2.5	**PR**	Produce summary of service aspects of Hatfield Rail Accident	Closed
2.6	**JFe**	Produce "Parachute Packing" story summary	Ongoing
2.7	**PR**	Produce first skeleton Guidance Document	Closed
2.8	**JFe**	Consider producing a sanitised version of the information on local sub-contractors.	Ongoing
3.1	**CH**	Create a glossary alongside the straw man document, and keep it active during future discussions/reviews etc.	Ongoing
3.2	**JF**	Talk to BAE contracts people and attempt to do a "contractual comparison", indicating where contracts for safety-related services differ from non-safety related ones, such as a mobile phone.	Ongoing
3.3a	**CH**	Revise the strawman document in accordance with the discussion in Meeting 3	Ongoing
3.3b	**CH**	Review Andy Scott's comments on the first draft of the strawman document and incorporate as appropriate in revising the document	Ongoing
3.4	**MP**	Make the NATS 'Assured ITSM for ATM' document available on the Share for the group.	Ongoing
3.5	**PR**	Ensure that the structure for the guidance document includes a section on the application of safety analysis techniques to SLAs.	Complete
3.6	**JFa**	Prepare a STAMP/STPA example using a real service framework.	Ongoing
3.7	**SS**	Explore the Überlingen Incident as a War Story example from the services point of view.	Ongoing

Ref	Owner	Description	Action
3.8	**PR**	Revise document skeleton in accordance with the discussion and send to MP.	Complete
3.9	**MP**	Circulate the SSS paper abstract	[See reference [8]]

References

[1]	The Service Context for Service-Based Safety Assurance	http://scsc.org.uk/file/gs/Service%20Context%20for%20Service-Based%20Assurance%2026Apr17-281.docx
[2]	STAMP/STPA and Service Assurance: A very draft introduction	http://scsc.org.uk/file/gs/SAWG--STAMP--JFaria-1-280.pptx
[3]	Sean White, Assurance of Services Safety in Health IT	http://scsc.org.uk/file/gs/Service%20Safety-324.pdf
[4]	Philippa Ryan, Hatfield Rail Accident	http://scsc.org.uk/file/gs/pt500Hatfield%20(1)-316.pdf
[5]	Skeleton Guidance Document	http://scsc.org.uk/file/gs/Services%20Safety%20Guidance%20Contents%20v02-313.docx
[6]	Assured ITSM for ATM	http://scsc.org.uk/file/gs/Mike%20Parsons%20Inputs-315.docx
[7]	Meeting slides	http://scsc.org.uk/file/gs/Meeting%20Agenda-314.pptx
[8]	SSS'18 Accepted Abstract	http://scsc.org.uk/file/gs/SSS18%20Abstract%20accepted-317.docx