The End-to-End Resilience of Technology Enabled Care Solutions – Questions Raised and TSA's Responses

Q1

We install our portfolio of technologies for various customers, and within each customer on various sites. Each site we install works independently to other sites we install even if for the same customer. In the event one site has an outage, is the maximum unavailability per annum calculated per individual site, or as a combined across every site even if the outage has no impact on other sites? For example, if we had 49 sites which all had a yearly outage of 1 hour (all unrelated issues at different weeks of the year), would it be classified as Advanced Complaint as the outage for the site was less than 2 hours, or non-compliant as the overall outages for all sites was 49 hours of the year?

The Resilience guidelines apply to any TEC Service that is supporting end users, including those than span multiple sites, and they take account of ARC availability, wide-area connectivity as well as on-site systems. Therefore, the compliance target responsibility lies with the design authority for each of your customers. You would need to make information available that allows end-to-end resilience to be evaluated by the services design authorities.

Q2

In the event a network switch dies on a site and takes down a portion of a site, but not the whole site, does this impact our downtime statistics?

This would depend on the impact on the alarm user themselves - if half of the scheme were offline and unable to raise alerts then yes, it would be downtime.

Please see the comment above regarding design authority responsibility for evaluating the end-to-end resilience.

Q3

The document claims exceptions will be made for national outages beyond control. Does this apply to outages on a particular site out of our control? On some sites we install, we might not be the IT provider. This would mean that the server we use is provided to us with a VM created and we configure the VM with whatever software we need. In this instance, if we were to have an outage relating to the server itself, the entire site could be down, but we would be unable to rectify the issue as we would not be contracted to resolve issues with the host server. Would this contribute to our downtime statistics? A similar scenario could be an external company is contracted to maintain a firewall. If they make changes which accidentally blocks our network traffic and therefore stops our system from working, is this downtime?

The Resilience guidelines apply to any TEC Service that is supporting end users, and they take account of ARC availability, wide-area connectivity as well as on-site systems. Therefore, the compliance target responsibility lies with the design authority for each of your customers. You would need to make information available that allows end-to-end resilience to be evaluated by the services design authorities.

Q4

Our systems call an ARC as a backup to calling onsite in the event an onsite care team is unable to answer. Would an outage relating to just onsite dialling or just offsite dialling (i.e. the other method works) contribute to downtime statistics?

You describe a primary and failover scenario, where in the event of a partial failure the system can failover immediately to another route. This behaviour should offer improved availability and should be included in the end-to-end system resilience evaluation by your customer's design authority.

Q5

How, and to whom, should we be reporting outages to?

For QSF certified organisations, in the event of an outage/major incident, all reports should be made via the reporting a serious incident tab within the Audit toolkit on the TEC Quality website- https://www.tecquality.org.uk/tec-quality-downloads

Q6

By whom, and how, would our system be graded to determine the compliance level? Would an external body come and survey us?

TEC Quality, who independently run the Quality Standards Framework (QSF), the only UKAS accredited TEC audit scheme, are the standards body implementing the resilience standards into their scheme changes. Please contact the TSA membership team to find out more on how to become QSF certified at **membership@tsa-voice.org.uk**

Q7

Are you working with platform providers to ensure ARCs have access to information and reports on availability?

Any services who are QSF accredited will be mandated to provide this information as part of their yearly audit.

Q8 Is there a possibility that TSA could put together a training course for someone who has been designated as a Design Authority within an organisation?

Detailed information regarding the role of a Design Authority can be found in the digital roadmap checklist, that can be used by all QSF certified organisations, and you can raise any questions on your pre/post audit support calls. If you require further support/ clarity, please contact the TSA membership team who can look to support further.

Q9 Is the transit time standard based on a particular technology such as current analogue ones? 20s may be unachievable in technologies such us GSM...

The work of SIG8 has indicated that the 'transit times' are achievable. However, this aspect of the QSF remains under review and at present is not part of the current scheme changes.

Q10 You mentioned addressing IoT so I may have missed this so apologies if so but besides the 2025 PSTN Switch off have you also been looking at the impact of the sunsetting of 3G by 2024 except for O2. Whilst 2G seems to be continuing for a while although at the whim of the operators I am well aware that there are many Telecare and Telehealth devices with 2G/3G modems sometimes used as a backup for the PSTN or has this all been dealt with nowadays?

Yes, we are aware of the 3G sunset, and TSA are working with TEC stakeholders and OFCOM on a statement regarding the future of 2G/3G networks and the impact on TEC devices.

Q11 The outage parameters seem to be looking at an outage that is affecting all users across all services within a service provider. Is there a model for partial outages e.g. one equipment supplier has an issue which only affects their installed devices.

Any outages that affect the delivery of service to the end customer are considered as downtime. We are exploring models that could be used by partial system suppliers to help design authority determination of end-to-end resilience.

Q12 What considerations are being given to the connectivity for delivering the required resilience when it comes to security, privacy and public safety?

SIG 8 considered security, privacy and public safety elements when creating the end-to-end resilience guidance.

Q13 Will QSF ARC suppliers have a similar set of targets for their respective platforms?

Any TEC supplier will contribute to the overall downtime measures from which the customers overall design authority will carry the target.

Q14 Where the ARC is SAAS is the ARC responsible for the target or the supplier?

The overall responsibility of the availability sits with the customer (and their overall design authority), although the ARC and any TEC supplier must provide 6 months rolling of downtime, RCA of any downtime and guidance of system configurations required to meet availability standards as stated within QSF supplier module SS30.

Q15 The “transit time”, whilst clearly important, is difficult to control for mobile alarm devices as they can be used in a variety of difficult locations such as the London Underground, fast-moving trains, aeroplanes, abroad, in remote areas with no mobile reception … etc. There will need to be some recognition of these complications, as I am sure you are already aware, between now and Nov

This aspect of the QSF remains under review and at present is not part of the current scheme changes.

Q16 Should there be a minimum annualised availability for Service Providers or Suppliers with very low numbers of connections where the formula would not give an acceptable threshold?

The availability target will sit with the customer, not with individual TEC suppliers.

Q17 Wide-area communications network (which include components of PSTN, mobile networks, IP-networks that connect remote TEC equipment to monitoring platforms or intervening applications). “ An ARC supplier will not necessarily have control over all of the elements listed here. Where an outage is caused by a communication failure outside the control of the ARC supplier our suggestion is that the outage is excluded from the availability measures?

The Resilience guidelines apply to any TEC Service that is supporting end users, and they take account of ARC availability, wide-area connectivity as well as on-site systems. Therefore, the compliance target responsibility lies with the design authority for any service. You need to make information available that allows end-to-end resilience to be evaluated by the services design authorities.

Q18

Consumer premises equipment (the combination of hubs, sensors and local connectivity that are provided in the home dwelling)" Given that an ARC supplier generally has limited control over customer premises equipment, our suggestion is that such equipment is not viewed as a sub-system of the ARC and therefore is not to be considered in the ARC availability measures. Are these measures aimed at a monitoring service?

The Resilience guidelines apply to any TEC Service that is supporting end users, and they take account of ARC availability, wide-area connectivity as well as on-site systems. Therefore, the compliance target responsibility lies with the design authority for any service. You need to make information available that allows end-to-end resilience to be evaluated by the services design authorities.

Q19

Page 8 table notes - Are these notes included as guidance only, or are they intended to form part of the audit criteria please confirm?

BC12 & BC13, within the QSF gap analysis document, state:

"A minimum set of key parameters are defined in this document and include availability of the service on demand, maximum downtime over a specified period, response and recovery times to outages and security requirements"

Q20

The alarm transit time is not directly controlled by the ARC supplier or the equipment supplier, as it can depend on communication services that sit outside the ARC infrastructure (ISP's etc). Can the TSA explain how this will be taken into consideration in this audit measure?

This aspect of the QSF remains under review and at present is not part of the current scheme changes.

Q21

Many telecare devices support "pre-alert" time windows which allow users to cancel alarms when triggered accidentally – can this be highlighted so that any measurement takes that into consideration?

This aspect of the QSF remains under review and at present is not part of the current scheme changes.

Q21 If we had 160k connections as you suggest in your rule of thumb but another ARC has 10k connections – on your current thinking the lower volume ARC has longer allowance for a fix.

Annualised availability targets are impacted by the number of service users at risk, and therefore larger services will need to deliver lower down-time as indicated. However, the measure for single instance downtime for services of all sizes, is the same.

Q22 Why does an ARC with fewer customers have a longer allowance of time to fix on your rule of thumb? Can we have a more specific measure than rule of Thumb and perhaps a % or explain "rule of thumb"

The 'rule of thumb' does not indicate any lack of precision in the measure, it simply provides a quick way for auditors to apply the measures to services of different scales. The calculations were derived by SIG8 and are explained in a recent webinar, please click on the link to view the webinar recording with slide deck (https://www.tsa-voice.org.uk/events/end-to-end-resilienc/).

Q23 We are seeing the emergence of new technologies, such as IoT connected alarms and peripherals. Are these covered or does this all apply to digital alarms only?

The intention is to cover all solutions that can be described as TEC. The impact on an IoT system for example would depend on the intended purpose of the service, perhaps the use of sensors and data may be part of a proactive service.