Resilience of Technology-Enabled Care Services

Steve Sadler

Technology Strategist, TSA

Resilience of TEC Services

Resilience: the capacity to withstand or to recover quickly from difficulties.

Failures happen, but services and their underlying technologies need to be designed so that they continue to meet the key performance criteria that are relevant to the intended purpose of the care services being offered.

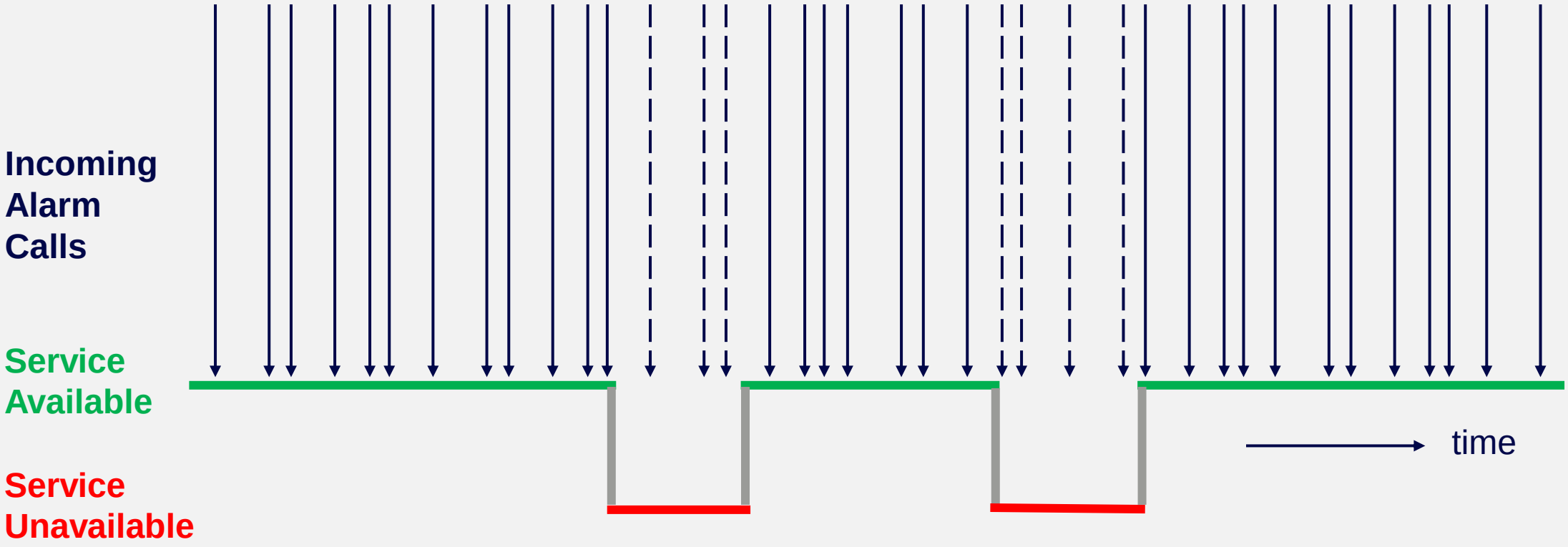
Key performance criteria:

- Availability of service on demand
- Timely transfer of information
- Data Protection and Security

} Minimum set of criteria defined by SIG8 (Resilience of ARC services)

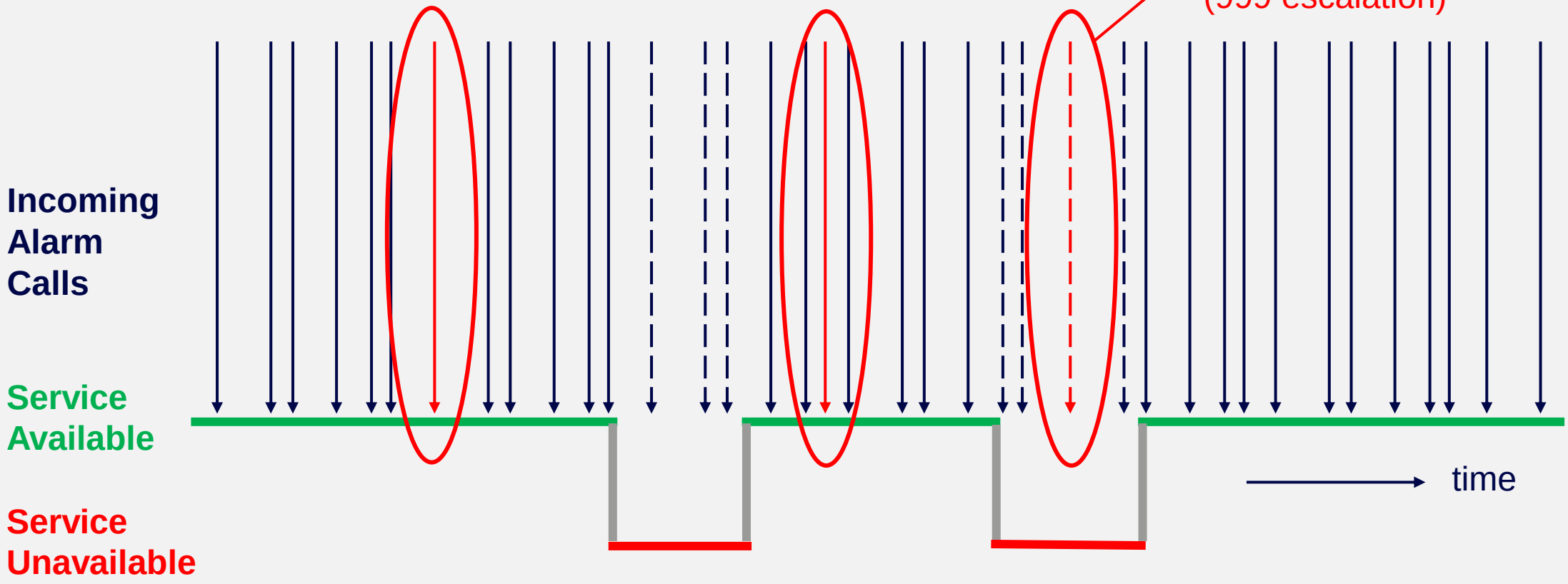
Availability of service on demand: Annualised Availability

Example: Reactive Service
Intended Purpose: Emergency Alarm Response



Availability of service on demand: Annualised Availability

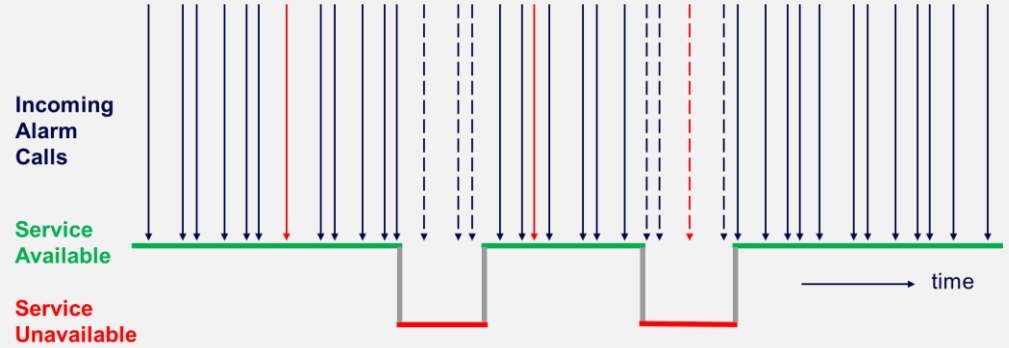
Example: Reactive Service
Intended Purpose: Emergency Alarm Response



Availability of service on demand: Annualised Availability

Example: Reactive Service
Intended Purpose: Emergency Alarm Response

Guiding Principle:
No TEC Service should fail to respond to a life-critical alarm call.



Calculating the target availability:
Number of service users
Number of calls per year (per service user)
% life critical calls
% annual downtime
Need to combine to deliver less than 1 missed life critical call per year

Example:
10,000 service users
12 calls per year (per service user)
3% of calls are life critical
48 hours annual downtime
(99.452% availability)

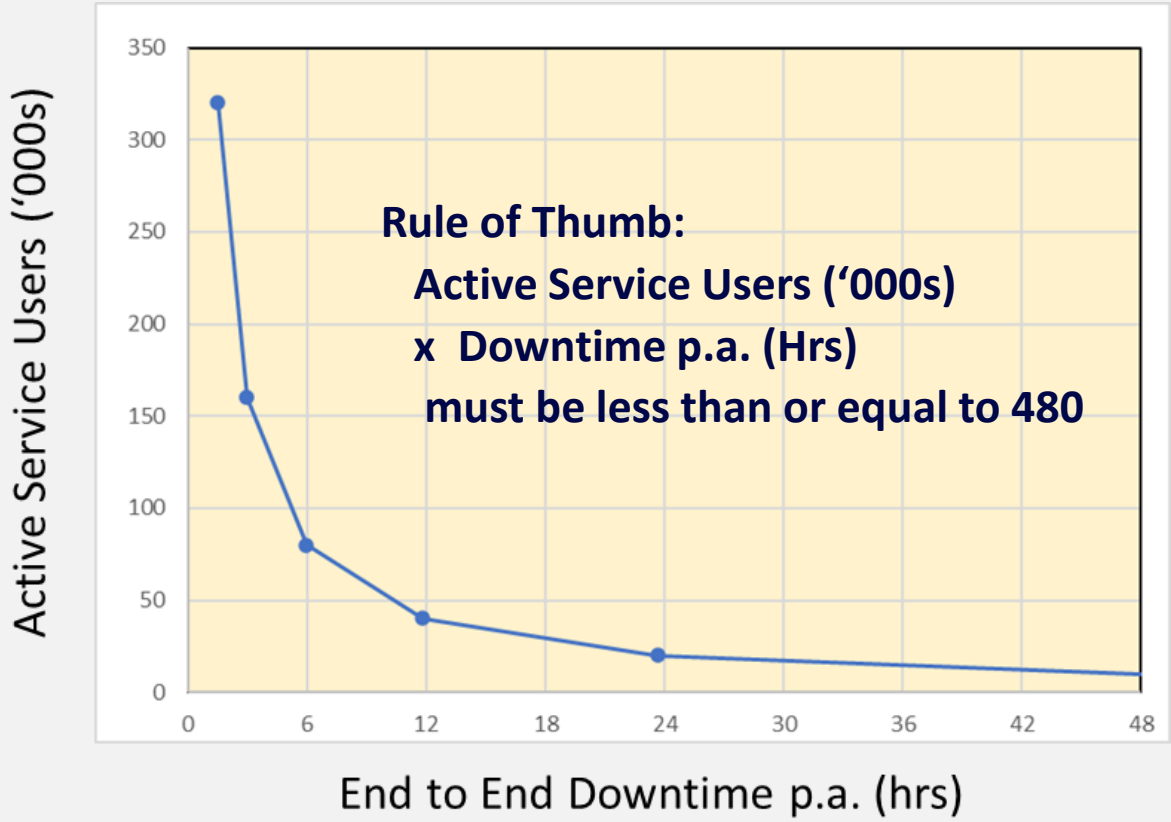
<= *1 missed life critical call per year*

Availability of service on demand: Annualised Availability

Example: Reactive Service
Intended Purpose: Emergency Alarm Response

Guiding Principle:
No TEC Service should fail to respond to a life-critical alarm call.

Calculating the target availability:
Number of service users
Number of calls per year (per service user)
% life critical calls
% annual downtime
Need to combine to deliver less than 1 missed life critical call per year



Availability of service on demand: Annualised Availability

Service Types

The concept of service types has been introduced, to allow for services with differing ‘intended purposes’, and to capture their distinctive requirements. The following service definitions and example use cases apply:

- **Critical & Reactive**: Real-time, life critical call handling, including telecare alarms, smoke detectors, fall detectors
- **Proactive**: Personalised outbound welfare check calls, medication reminders, activities of daily living monitoring, all typically in response to a care plan
- **Preventative**: Wellbeing apps, health questionnaires, advisory outreach services to a population of vulnerable people at risk

Availability of service on demand: Annualised Availability

Quality Levels and Service Types

levels of availability for a Critical Reactive service with 10,000 active end users

	Maximum Unavailability (Per annum)				
	96hrs	72hrs	48hrs	8hrs	2hrs
	= 98.91% Availability	= 99.18% Availability	= 99.45% Availability	= 99.91% Availability	= 99.98% Availability
			Minimum availability for a compliant Critical service		
Critical	Non-Compliant	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance

Availability of service on demand: Annualised Availability

Quality Levels and Service Types

levels of availability for a Critical Reactive service with 10,000 active end users

Maximum Unavailability (Per annum)				
96hrs	72hrs	48hrs	8hrs	2hrs
= 98.91% Availability	= 99.18% Availability	= 99.45% Availability	= 99.91% Availability	= 99.98% Availability

Increasing levels of quality

Critical	Non-Compliant	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance

Availability of service on demand: Annualised Availability

Quality Levels and Service Types

levels of availability for services with 10,000 active end users

Service Type	Maximum Unavailability (Per annum)				
	96hrs	72hrs	48hrs	8hrs	2hrs
	= 98.91% Availability	= 99.18% Availability	= 99.45% Availability	= 99.91% Availability	= 99.98% Availability

Proactive	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance	Outstanding Compliance
Critical	Non-Compliant	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance

Availability of service on demand: Annualised Availability

Quality Levels and Service Types

levels of availability for services with 10,000 active end users

Service Type	Maximum Unavailability (Per annum)				
	96hrs	72hrs	48hrs	8hrs	2hrs
	= 98.91% Availability	= 99.18% Availability	= 99.45% Availability	= 99.91% Availability	= 99.98% Availability
Preventative	Compliant	Advanced Compliance	Outstanding Compliance	Outstanding Compliance	Outstanding Compliance
Proactive	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance	Outstanding Compliance
Critical	Non-Compliant	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance

Availability of service on demand: Maximum single-instance downtime

Guiding Principle:
No Critical TEC Service should be unavailable to respond to life-critical calls for more than 1 hour

The longer a service is down, the more likely that a critical service user will be unable to receive assistance within the “golden hour”.

Examples of the serious impact of delay include:

- 1 extra hour on the floor after a fall can equate to 1 extra day in hospital
- Treatment is usually needed within 1 hour after a heart attack to avoid further heart damage or even death

Service Type	Maximum TEC Equipment & Monitoring Service Downtime				
	12hrs	4hrs	60mins	20mins	10mins
Preventative	Compliant	Advanced Compliance	Outstanding Compliance	Outstanding Compliance	Outstanding Compliance
Proactive	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance	Outstanding Compliance
Critical	Non-Compliant	Non-Compliant	Compliant	Advanced Compliance	Outstanding Compliance

Timely Transfer of Information
(from service user to monitoring service)

Guiding Principle: Service users need to be assured that their TEC service will provide timely responses.

The performance of a TEC service depends to a large degree on people and processes in delivering a suitably rapid response to user alerts. These issues are addressed in other TSA service standards.

However, any TEC service is also dependent on the end-to-end performance of the underlying technology. For Critical alerts this has been defined as the 'transit time' from initial alert identification in the user environment, to presentation of that alert to service operators.

Further work is proposed for Proactive and Preventative service interpretations.

Service Type	Max. time from alert activation in the user's environment to presentation to operators at the monitoring service (Transit Time)			
	>20secs	20secs	10secs	5secs
Critical	Non-compliant	Compliant	Advanced Compliance	Outstanding Compliance

Data Protection & Security

Guiding Principles:
Service users' personal data needs to be protected and TEC services need to be secure against cyber-attack.

Key standards applying to data protection and security in the UK are:

- Cyber Essentials - a simple but effective Government backed scheme that helps to protect against a range of the most common cyber-attacks. The scheme employs self-assessment tools, and its applications include Local Authorities.
- Cyber Essentials Plus - Cyber Essentials principles, but certified by an external body.
- Data Security & Protection Toolkit (DSPT) – is applied where services are provided to the NHS and those organisations that are registered with a care regulator.
- Information Sharing Toolkit – Scotland's equivalent of DSPT.
- Welsh Information Governance Toolkit – Wales' equivalent of DSPT.
- ISO 27001 - the international standard that specifies an information security management system (ISMS). It targets security through people and processes as well as technology.

Data Protection & Security

Compliance status by Quality Level and Service Type

Service Type~	Cyber-Essentials	Cyber-Essentials Plus	DSPT*	ISO27001
Preventative	Compliant	Advanced Compliance	Advanced Compliance	Outstanding Compliance
Proactive	Compliant	Advanced Compliance	Advanced Compliance	Outstanding Compliance
Critical	Compliant	Advanced Compliance	Advanced Compliance	Outstanding Compliance
Any regulated service	Non-compliant	Non-compliant	Compliant	Advanced Compliance

Notes:
~ SIG 008 found no reason to differentiate between non-regulated service types, given that risks to data loss and disruption apply across the service spectrum.
* DSPT or equivalents across Home Nations.

Responsibilities of Service Providers

A TEC service provider must:

- **define the intended purpose of the services being provided**
- **define the key operational parameters which ensure that the service is fit for the intended purpose**
- **demonstrate that these have been shared and agreed with buying customers and users**
- **employ processes which ensure that the service achieves the key operational parameters**
- **identify a Service Design Authority, who has end-to-end responsibility for ensuring that the combination of enabling technologies and the use of data is fit for use by care staff and users, and hence the intended purpose of the Service**

Phasing of TSA QSF Implementation

Phase	Date effective in QSF	Description
0	April 2022	Responsibilities of Service Providers
1	April 2023	Data Protection & Security standards
2	Nov 2023	Availability of TEC Services – Annualised
	Nov 2023	Availability of TEC Services - Maximum Single Instance Downtime
3	Nov 2024	Timely Transfer of Information