Engineering Justification Paper

IT Communications Refresh

Version: Final

Date: December 2019

Classification: Highly Confidential

Reference: SGN IT – 004 Comms EJPDec19

1 Table of Contents

2 Introduction

This paper provides architectural justification to support SGN's proposal to refresh its communications network during GD2. The scope of this investment covers project activity necessary to ensure that the SGN communications network remains fit for purpose and continues to underpin SGN's ability to run and maintain a safe and reliable gas network to meet the needs of its customers throughout the GD2 period.

2.1 General Background

As part of SGN's licence obligations it is necessary to capture and have access to information in real time, so network connectivity is essential. This includes Priority Services Register data and the ability to refer customers to appropriate agencies (instant response in the home).

Greater use of video technology in applications such as CitNow is totally dependent on good connectivity, as is the use of Skype which has resulted in a recent reduction in travel with the associated environmental benefits. Other solutions such as the ability to measure customer satisfaction at the point of operation and use of Learning Management tools for customer experience training and stakeholder engagement surveys are also all dependent on this technology.

The managed IT network infrastructure within SGN will be approaching end of life during GD2 and will struggle to deliver key services that are critical to the company's ability to deliver its obligations under the GD2 licence terms. A programme of refresh and replacement is proposed primarily over the final two years of the GD2 period, which will start with the refresh of critical infrastructure and new circuits in all relevant sites; but there will also be some spend in the first year to replace the legacy comms infrastructure that is end of life.

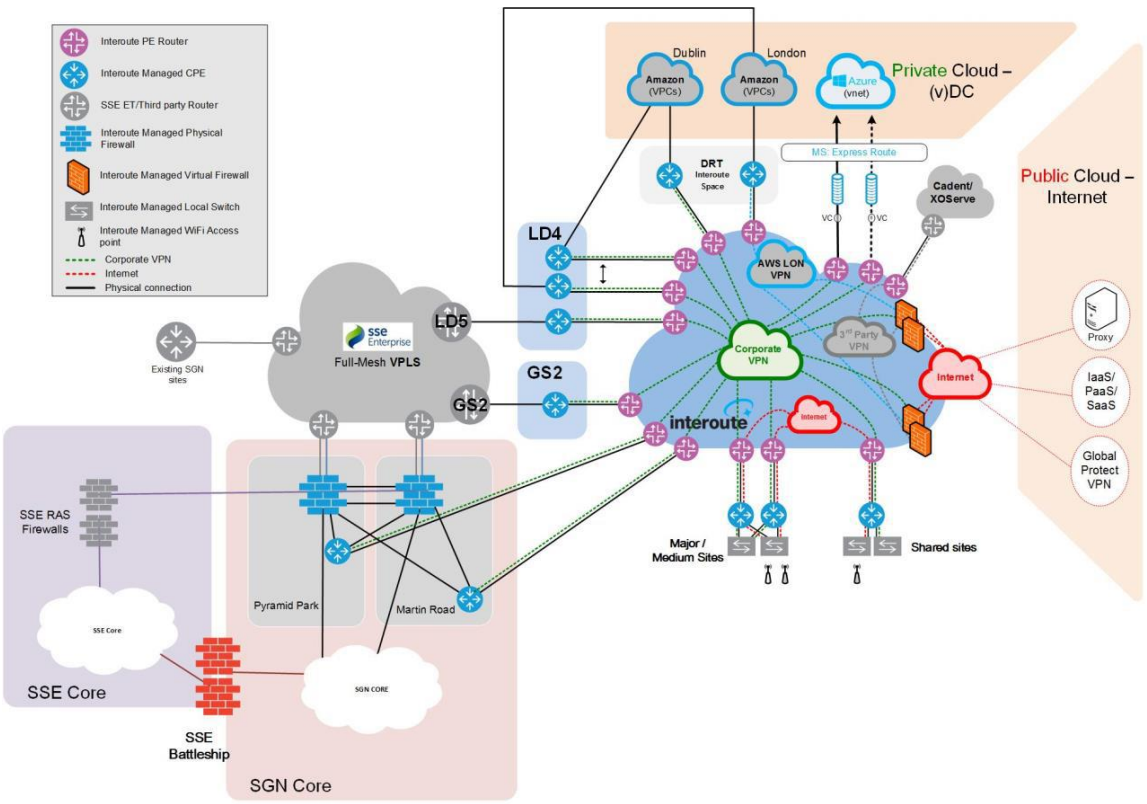

Figure 1: Example network topography from SGN (as at 2019) to demonstrate complexity

In addition to the key site refreshes, there are a number of other critical networking and connectivity elements, circuits to third parties such as National Grid, Cadent, Xoserve etc., that are required to also be periodically refreshed to maintain connectivity. These will be included in the scope of this delivery.

SGN field users are often interacting directly with customers and sharing information from their screen, gathering data from the customer and accessing corporate asset data across the IT network in real-time - credibility for the user is severely damaged if the connectivity fails, resulting in reduced customer satisfaction scores and directly impacting one of our primary licence measures. As such it is important to maintain a regular refresh of this communications infrastructure while ensuring good value for money by only implementing what is fit for purpose and future proof.

SGN would look to replace obsolete hardware and circuits while keeping costs low and delivering best value. This approach is in line with SGN's architectural principles around connectivity and SGN's investment is in line with industry standards as evidenced by the recent Gartner benchmarking. It is recognised that although the data volumes for SGN are likely to continue to rise significantly (IIOT, more remote working, more connected devices), the cost per unit will fall as the technology continues to advance.

Failure to refresh in a timely cycle would result in SGN's operatives being impacted in their ability to perform their duties, ultimately impacting on safety to both themselves and the public.

Vendors are continually embedding security components and solutions into the core of their IT network hardware, so it is essential that we do look to upgrade and refresh the network to avoid a potential security risk to our critical national infrastructure.

2.2 Site Specific Background

The communications network is critical for users to access business applications, to communicate effectively and to collaborate. Office based staff typically use desktops, and field-based or mobile staff use laptops and tablets depending on their role and their technology requirements, and these devices all rely on reliable connectivity to become productive tools for users.

SGN field users are often interacting directly with customers and sharing real time information from their screen, gathering data from the customer and accessing corporate asset data. This is all achieved using the communications network. Credibility for the field user is severely damaged if the connectivity to support them is not resilient and reliable, resulting in reduced customer satisfaction scores and directly impacting one of our primary licence measures.

3 Equipment Summary

SGN’s network is made up of a wide area network (WAN) connecting all medium to larger sites to each other and to the various hosted business applications, and a number of local area networks (LANs) to support each site and allow users to connect to the network. Wifi is also provided in larger sites to support productivity and flexible working.

The network is supported by physical hardware on sites (switches, routers, access points etc) which have a finite lifespan and support window – typically 3-5 years. This hardware comes with a level of embedded security features that will become less effective over time as threats evolve and become more complex and devious, and this adds to the necessity to refresh this hardware periodically.

4 Problem Statement

IT network connectivity is essential for field operatives to be able to receive jobs (emergency or planned), to locate assets and to record data about those assets. Connectivity in customer facing situations such as providing quotations, measuring customer satisfaction and accessing information such as the new Priority Services Register is all critical to our day to day operations ensuring that our staff have access to the latest information so that they can respond appropriately for the situation. New digital based solutions around delivery of training, management of competencies, capturing timesheets electronically and delivering policies and procedures online all make it essential that SGN's operatives have reliable and secure up to date connectivity to meet these requirements. Real time connectivity also means that operatives can minimise travel and the associated environmental impacts through the use of technology such as Skype. In a scenario where connectivity fails or is intermittent manual processes would need to be reverted to, introducing risk to operatives and customers, damaging credibility and confidence. This in turn would impact SGN's ability to meet its licence obligations and hit its targets.

Due to the pace of change of technology in this area, along with the ever-changing cyber security threat, SGN operates a technology refresh for connectivity every five years, and as this is in the process of being refreshed in the last couple of years of GD1 the expectation is that it will need to be revisited during the latter part of GD2 to maintain operational integrity.

Why are we doing this work and what happens if we do nothing?

Failure to refresh the network in a timely cycle would result in SGN operating with non-performant and potentially vulnerable connectivity, which in turn would result in the staff being unable to perform their duties, ultimately impacting on safety to both themselves and the public, and impact to licence obligations.

Due to the nature of ever more demanding connectivity requirements, hardware obsolescence, changing security requirements, it is necessary to budget for a complete refresh of the communications network every 5 years.

The network providers are continually embedding enhanced security components and solutions into the core of their network, so it is essential that we do not over extend the life of assets that could pose a security risk to our critical national infrastructure.

What is the outcome that we want to achieve?

New digital based solutions around delivery of training, management of competencies, capturing timesheets electronically and delivering policies and procedures online all make it essential that SGN's operatives have reliable and secure network connectivity to meet these requirements. In a scenario where the network failed or became unreliable, manual processes would need to be reverted to, introducing risk to operatives and customers, damaging credibility and confidence. This in turn would impact SGN's ability to meet its licence obligations and hit its targets.

How will we understand if the spend has been successful?

We will know if the spend has been successful if we adhere to our service levels and users are able to perform their jobs in an efficient and productive manner. An effective communications network should be a basic hygiene factor and invisible to users.

4.1 Narrative Real-Life Example of Problem

Following a major IT network failure in late 2016, SGN's lost the ability to connect with critical scheduling applications and to allocate jobs automatically out to field operatives. As a result, BCM processes were invoked and we reverted to manual, voice-based scheduling. This had a knock-on impact on response times, and in some instances meant that SGN missed SLAs.

The network was down for around 12 hours, during which time efforts were made to resolve the issue, but due to the age of the hardware, there was limited knowledge to find a solution. In the end a network appliance had to be switched out for a spare taken from another site to resolve the issue.

4.2 Spend Boundaries

This paper only covers the capex and opex costs associated with procurement of and implementing an updated communications network. It does not cover any ongoing costs associated with operating this network. These ongoing costs are covered in our GD2 opex run costs.

5 Probability of Failure

Evidence from GD1 suggests that by year 6 the failure rate of hardware to support the network has a material impact on productivity, and therefore safety. This has a knock-on impact on credibility with customers, users and productivity and after a period of time we will reach a point where we are unable to perform our licence obligations as the hardware will be incompatible or obsolete and we will have no ongoing support or imposable SLAs. It also does not support changing security requirements leaving SGN vulnerable to attack.

5.1 Probability of Failure Data Assurance

As stated previously, from SGN's first-hand experience and from industry measures, the failure rate of devices in year 6 increases significantly; this combined with changing connectivity requirements and security threats means that we have no option but to refresh our network every five years.

6 Consequence of Failure

In the event that our communications network was to fail, we would be unable to meet our licence conditions as our office users would not be able to access any applications, and our field operatives would not be able to receive jobs (emergency or planned), locate assets and record data about those

assets. Under the new Priority Services Register legislation it is also important that our operatives have access to the latest information so that they can respond appropriately for the situation.

Effective network connectivity also means that operatives and office-based staff can minimise travel and the associated environmental impacts through the use of technology such as Skype. Failure of the network would result in users having to travel more, with consequential increases in non-productive time, delays, and impact on the environment through increased use of vehicles.

7 Options Considered

It is important to ensure that we maintain an effective and reliable communications network, while ensuring good value for money by only implementing what is fit for purpose and future proof.

The options outlined below are in line with our current refresh approach which aims to ensure best value is achieved from all assets, while ensuring cost is managed.

7.1 Option 1 - Refresh of circuits, hardware and LAN services to replace the existing service

This option predicts a similar level of investment will be required as in GD1 (approx. £6m) to refresh IT network circuits, and hardware (proxy servers, firewalls, switches, routers etc) that support user connectivity. The IT network was last refreshed in 2019/20 and the contract will expire in 2025 by which time the hardware will be obsolete and network technology is likely to have advanced, meaning we would most likely need to replace circuits as well. We will also need to meet the latest network security standards that will be required at the time, especially around proxy servers and firewalls. As always, a regulated tender process will be run to ensure best value from recognised vendors. Failure to refresh the network would result in degrading connectivity with the mobile workforce and between offices, which would seriously impact SGN's ability to hit regulatory targets. The refresh is likely to take between 1-2 years depending on the scale of the change (e.g. whether existing circuits can be ported and reused or have to be reordered with subsequent lead times)
The above option represents a safe and reliable approach for SGN users by ensuring replacement of an aging service with a newer, fit for purpose solution based on current technology and security standards.
The scope of the change proposed would be a like for like (or current equivalent service. For example, that would mean that at present there is no provision for 5G services in these figures as currently it is not clear what a 5G based network would look like in five years' time.

7.2 Option 2 - Extend existing contract with current IT network service provider for a further term

This option would propose that SGN extend the network service to beyond the end of GD2, which would not be recommended as hardware will be end of life, circuit technology will most likely be obsolete, and in-network security requirements will have evolved which could leave SGN exposed and unable to meet its licence obligations. For the above reasons this option was rejected as not safe and reliable. Under the Utilities Contract Regulations 2016 we would be obliged to retender for this

service anyway at the end of the current contract period (3 +2 years), which would make a contract extension impossible. We have not costed this option as it is not perceived to be viable.

7.3 Options Technical Summary Table

Table 1: Options Technical Summary

Option	First Year of Spend	Final Year of Spend	Volume of Interventions	Equipment / Investment Design Life	Total Cost
Option 1 – Refresh the Network	2021	2026	Finalisation of current communications refresh (telephony) in 2021 and the full refresh over two years at end of GD2 – c. 25 sites and 1500 office-based users	New network hardware (switches, routers etc) for each site. 5 years	£6m
Option 2 – Extend the existing service provision and sweat the hardware assets for a further term	This option has not been costed as it is not economically or legally viable and is not supported by our hardware vendors. It would breach regulated tender procurement rules.				

7.4 Options Cost Summary Table

Table 2: Cost Summary

Option	Cost Breakdown	Total Cost (£m)
Option 1 – Refresh the Network	Hardware - £4.5m (to cover cost of fibre cabling, network switches, routers, proxy servers, firewalls, etc.) Project costs - £1.5m (to cover resources, contractors, expenses etc.)	Total £6.0m (all Capex)

Please note the costs outlined in the Options Technical Summary Table are based on the following assumptions:

Option 1 Assumptions:

- The refresh cycle for communications equipment has been put at 5 years. If the rate at which technology changes continues to increase this refresh cycle may not be sufficient.
- The phasing has assumed that the first year of GD2 will complete the network refresh that was started in GD1. There will then be a break of a year prior to the next refresh cycle commencing.
- The rollout of 5G technology will not impact the cost of our current 4G services.
- We have assumed that if we have not updated our communications network by year 4 of GD2 that we would be subject to a breach of licence conditions and a potential fatality as we would not be able to communicate with our field force in a secure and reliable way.

Baseline Assumptions:

- SGN manage its IT estate in line with the HSEs ALARP (as low as reasonably practicable) risk management principles. On that basis SGN have assumed a failure to invest in required (see engineering justification paper for more detail) upgrade, replacement or refresh activity for safety critical systems, would lead to catastrophic system failure as well as a lack of 3rd party support (based on support contracts, 3rd party roadmaps, architectural standards and internal policies, designed to ensure upgrade, replacement or refresh activity is carried out at the appropriate point in time to in order to prevent a non-recoverable functional, technical or security failure).
- SGN have assumed that a lack of investment combined with a lack of support would prevent the reinstatement of systems should they fail.
- SGN have assumed a catastrophic failure of safety critical systems and an inability to reinstate systems after failure would lead to an inability to respond to gas emergencies, an inability to know where our assets are and an inability to track performance and regulatory outputs.
- SGN have assumed a catastrophic failure of safety critical systems and an inability to reinstate systems after failure would lead to an inability to manage Personal Identifiable Information and would inevitably lead to a significant breach of GDPR legislation (up to £40m fine)
- SGN have assumed an inability to respond to gas emergencies, an inability to know where our assets are and an inability to track performance and regulatory outputs would inevitably lead to a catastrophic incident e.g. explosion and loss of life (£17.73m). This assumption is supported by section 2 of the Health and Safety at work act which identifies scenarios that would result in loss of life.
- SGN have assumed an inability to respond to gas emergencies, an inability to know where our assets are and an inability to track performance and regulatory outputs would inevitably lead to an inability to operate. This would lead to a catastrophic breach of license conditions (up to £100m fine)
- SGN have assumed catastrophic failures in regard to loss of life (£17.73m), a breach of license conditions (up to £100m) and/or a breach of GDPR legislation (up to £40m) will occur within a year of failing to adhere to support contracts, 3rd party roadmaps, architectural standards and internal policies designed to ensure upgrade, replacement or refresh activity

is carried out at the appropriate point in time to in order to prevent a non-recoverable functional, technical or security failure.

8 Business Case Outline and Discussion

8.1 Key Business Case Drivers Description

There is only one viable option to consider here and the key drivers for this are shown below.

Table 3: Summary of Key Value Drivers

Option No.	Desc. of Option	Key Value Driver
1	Refresh Network	SGN has an effective and secure communications network which allows us to meet our licence obligations.

Table 4: Summary of CBA Results

NPVs based on Payback Periods (absolute, £m)								
Option No.	Desc. of Option	Preferred Option (Y/N)	Total Forecast Expenditure (£m)	Total NPV	2030	2035	2040	2050
Baseline	Do Nothing / Do minimum	N	0.00	-117.73	**-117.73**	**-117.73**	**-117.73**	**-117.73**
1	Refresh of circuits, hardware and LAN services to replace the existing service **Absolute NPV**	Y	-6.00	-27.15	**-5.94**	**-9.51**	**-12.88**	**-18.69**
1	Refresh of circuits, hardware and LAN services to replace the existing service **NPV Relative to the Baseline**	Y	-6.00	-27.15	**111.79**	**108.21**	**104.85**	**99.04**

8.2 Business Case Summary

This project is primarily driven by SGN's need to deliver a secure and robust communications network to its users in offices and out in the field, which in turn ensures they can meet licence obligations. The level of investment requested is purely to deliver safe and reliable communications as today.

Table 5: Business Case Matrix

Comms Refresh	
GD2 Capex (£m)	6.00
Number of Interventions	50.00
Carbon Savings ktCO2e (GD2)	0.00
Carbon Savings ktCO2e /yr	0.00
Carbon Emission Savings (35yr PV, £m)	0.00
Other Environmental Savings (35yr PV, £m)	0.00
Safety Benefits (35yr PV, £m)	17.73
Other Benefits (35yr PV, £m)	100.00
Direct Costs (35yr PV, £m)	-21.71
NPV (35yr PV, £m)	96.01
High Carbon Scenario	
Carbon Emission Savings (35yr PV, £m)	0.00
High Carbon NPV (35yr PV, £m)	96.01

9 Preferred Option Scope and Project Plan

9.1 Preferred option

The preferred option recommended in this paper is to refresh the communications network during the latter part of GD2 as outlined above.

9.2 Asset Health Spend Profile

Table 6: Asset Spend Profile

Asset Health Spend Profile (£m)						
	2021/22	2022/23	2023/24	2024/25	2025/26	Post GD2
Refresh of circuits, hardware and LAN services to replace the existing service	0.50	0.00	1.50	2.00	2.00	Spend profile continues

9.3 Investment Risk Discussion

The primary risk associated with this investment is that the technology associated with networking and communications could change significantly once the investment has been made, which would result in a need to expedite further change and shorten the life of the asset. This is a low likelihood risk and experience to date has shown that a five-year refresh window allows SGN to maintain currency around technology and security standards, while not being at the cutting edge and therefore facing higher costs and risks. In other words, SGN's investment approach remains safe and reliable, like the network itself.

Risk Description	Impact	Likelihood	Mitigation/Controls	Comments
Change in timescales	Capex expenditure	>40% & <=60%	Ensure network architects are monitoring technology trends and advising appropriately.	Network technology may evolve faster than anticipated and so the investment in refresh might need to be brought forward.
Change in scope	Capex expenditure	>40% & <=60%	Ensure network architects are monitoring technology trends and advising appropriately.	The predicted impact of 5G is unknown at this point but may change the connectivity model in use at SGN.
Change in capital expenditure	Capex expenditure	>40% & <=60%	Ensure network architects are monitoring technology trends and advising appropriately.	There is a risk that advances in security threats may leave SGN exposed.
Change in capital expenditure	Capex expenditure	>40% & <=60%	The cost per unit should reduce which should mitigate any increased demand.	There is a risk that increased data consumption may outstrip forecast demand.

Table 7: Sensitivity Results

	Low	Mid	High
GD2 Capex (£m)	4.80	6.00	7.20
Number of Interventions	50	50	50
Carbon Savings ktCO2e (GD2)	-	-	-
Carbon Savings ktCO2e /yr	0	0	0
Carbon Emission Savings (35yr PV, £m)	0.0	0.0	0.0
Other Environmental Savings (35yr PV, £m)	0	0	0
Safety Benefits (35yr PV, £m)	3.5	17.7	17.7
Other Benefits (35yr PV, £m)	20.0	100.0	100.0
Direct Costs (35yr PV, £m)	-17.4	-21.7	-26.1
NPV (35yr PV, £m)	6.2	96.0	91.7

Low case: SGN have applied a reduction of 20% to the costs. This could be achievable if the cost of communication technology reduces significantly within GD2. Furthermore, an 80% reduction has been applied to the Safety Benefits associated with the risk of a fatality and Other Benefits associated with the impact of a Breach of Licence Conditions.

Mid case: No changes have been applied, this is the expected investment.

High case: SGN have applied an increase of 20% to the costs as the impact of 5G on our existing network is not known. The increasing cyber threat may also result in an increase in costs to secure our networks.

Project payback has not been carried out as part of this analysis due to the effect of the Spackman approach. For a cash-flow traditional project payback period please see scenario 4 of our Capitalisation Sensitivity table.

Capitalisation Sensitivity

Consumers fund our Totex in two ways – opex is charged immediately though bills (fast money – no capitalisation) and capex / repex is funded by bills over 45 years (slow money – 100% capitalisation). The amount deferred over 45 years represents the capitalisation rate. Traditionally in 'project' CBA's the cashflows are shown as they are incurred (with the investment up front which essentially is a zero capitalisation rate). Therefore, we have developed scenarios that reflect both ways of looking at the investment – from a consumer and a 'project'.

The scenarios are summarised as follows:

- Scenario 1 - we have used the blended average of 65%, used in previous iterations of this analysis.
- Scenario 2 - we have represented the Capex and Opex blend for the two networks, as per guidance.
- Scenario 3 - addresses our concerns on capitalisation rates whereby Repex and Capex spend is deferred (100% capitalisation rate) and Opex is paid for upfront (0% capitalisation rate).
- Scenario 4 - this reflects the payback period in 'project' / cash-flow terms and provides a project payback.

We have taken a view of the NPV in each of the scenarios, except for scenario 4, at the 20, 35 and 45 Year points, to demonstrate the effect of Capitalisation Rate on this value.

Table 8: Capitalisation Rate Variation

Scenario	1	2 SGN	3	4
Capex (%)	65	41	100	0
Opex (%)	65	41	0	0
Repex (%)	100	100	100	0
Output				
NPV (20yr PV, £m)	105.93	103.96	108.82	
NPV (35yr PV, £m)	97.44	96.01	99.53	
NPV (45yr PV, £m)	93.16	92.14	94.64	
Payback	3.00	3.00	3.00	3.00

Appendix A - Acronyms

Acronym	Description
BCM	Business Continuity Management
CBA	Cost Benefit Analysis
GDPR	General Data Protection Regulation
HSE	Health & Safety Executive
IIOT	Industrial Internet of Things
LAN	Local Area Network
SLA	Service Level Agreement
SGN	Scotia Gas Network
WAN	Wide Area Network