Scottish & Southern Electricity Networks

TRANSMISSION

Safe and Secure Network Operation

A Network for Net Zero
Draft RIIO-T2 Business Plan

Scottish Hydro Electric Transmission plc

Safe and Secure Network Operation

Strategic Objective

Safe and Secure Network Operation
Using data efficiently to understand, predict and get the best network performance.

Energy networks, and especially the high voltage transmission motorways, must be reliable, available and resilient to changing circumstances, be these opportunities or threats.

Clear Goal

100% network reliability for homes and businesses
Make cost-effective investment in technology to achieve 100% transmission system reliability for homes and businesses by 2026.

Targets for RIIO-T2

We are developing a set of targets which our stakeholders can judge our progress against our strategic objective and clear goal. The indicative targets currently proposed are set out below, with reference to performance during the RIIO-T1 period as a benchmark where available.

		RIIO-T1	2025/26
Energy Not Supplied* The volume of electricity that is not supplied to homes and businesses due to interruptions of longer than three minutes on the transmission network. Excludes specified events	MWh pa.	46†	TBC
Faults Total number of unplanned interruptions, of all durations and with no exclusions, on the transmission network	Number pa.	131†	72
Coverage of smart monitoring Critical plant items with smart monitoring equipment installed and operational	Number of critical sites	0‡	61
Network monetised risk Value of asset-driven interventions as assessed by the Network Asset Risk Methodology (delta target)	£ billion	N/A	1.92
International benchmarking - Operations Out-turn position in the composite service-cost metric in the International Transmission Operations and Maintenance Study (ITOMS)	Relative position	Quartile 3 (Lower right)‡	Quartile 4 (Upper right)
International benchmarking – Asset Management Out-turn position in the composite service-cost metric in the International Transmission Asset Management Study (ITAMS)	Relative position	Quartile 1 (Lower left)‡	Quartile 4 (Upper right)

* Financial incentive
† Average of full six years completed
‡ At end 2018/19

What's in this section?

Being safe... our safety licence – "if it's not safe, we don't do it" – covers everything we do, and our draft Business Plan adheres to our best in class safety practices.

Security of supply... the role of networks in providing security of supply and what that means to our main stakeholder groups.

About resilience... the four strategic components of infrastructure resilience – reliability, redundancy, resistance, and response and recovery – that together provide a framework for safe and secure network operation. What each of these four components mean for the operation of an electricity transmission network.

Improvements we have made during RIIO-T1... keeping pace with the growth of the network and the needs of stakeholders, including the cost effective use of targeted innovation.

Proposals for reliability... for ongoing inspection and maintenance, and a gradual transition to risk-based operations. How we have used a risk-based methodology to identify the need for intervention on 29 existing asset schemes during RIIO-T2, along with the business case for a modern secure Control Centre.

Proposals for redundancy... how we actively assess the cost effective level of installed redundancy on the network. Our proposals to upgrade the storage of back up assets.

Proposals for resistance... including the ongoing programme to replace obsolete system protection and control systems, and to target growing physical threats, natural hazards and cyber security.

Proposals for response and recovery... as part of the Business Continuity Planning we undertake as a provider of Critical National Infrastructure. We propose investments in our substation systems, communications equipment and provision of temporary transmission masts.

Overview

The safe and secure operation of the north of Scotland transmission system provides security of electricity supply to homes and businesses. It also ensures that generators have network availability to transport the power they produce to energy consumers.

Safe and secure operation is needed 24/7 and, in our modern energy dependent society, customers expect a fast response to any event that disrupts supply. Our and others stakeholder research consistently concludes that energy consumers place a high value in continuity of electricity supply.

There are many elements to providing a safe and secure network, but fundamentally it requires excellence in asset management. Our ambition is for world class asset management. We will measure our performance through participation in international benchmarking studies. We have set a clear goal that we will demonstrate world class asset management – that goal is 100% network reliability for homes and businesses.

We have used the strategic components of infrastructure resilience to put in place a comprehensive programme of activities for RIIO-T2 that are necessary for safe and secure network operation. This includes incremental improvements, where it is cost effective, to gradually reduce the risk of faults on our network.

Reliability is the day-to-day design and operation of the network. The GB transmission system is currently >99.99% reliable. This is achieved through inspection, maintenance, and asset intervention. As monitoring technology improves, we propose to adapt our processes and procedures to modernise how this is performed. In RIIO-T2 we also propose to replace our control centre with a more secure, modern facility to improve network management.

Redundancy is concerned with the availability of back up should the network be disrupted. Our requirements for back up equipment has grown as the network has grown and so we propose to establish new warehouse facilities.

Resistance requires providing protection from natural hazards or malicious acts. Threats continue to emerge, and technological advancement rapidly makes existing systems obsolete.

Finally, response and recovery is about the preparation for a fast and effective response to disruptive events. Much of the preparation for catastrophic failure is undertaken at GB level, but there are cost effective actions that we propose to take to improve our business continuity.

What is a safe and secure network?

Energy networks, such as the north of Scotland transmission system, provide an essential public service to GB society and its economy. Everyone needs energy to conduct their daily life and everyone expects reliable access to energy when and where it is needed.

A safe network

Electricity can be dangerous. There are very high voltages in transmission networks which can kill if not managed correctly.

The day-to-day running of a transmission system also brings dangers. In addition to live electricity, it involves construction, working at height or in confined spaces, and the use of toxic liquids and gases, amongst many other risks to our employees and the public.

All GB energy networks operate to the highest safety standards in partnership with the Health and Safety Executive. Through our trade body, the Energy Networks Association (ENA), we share best practice and learning with a shared ambition for continual improvement.

Our approach to safety is simple: if it's not safe, we don't do it **(Figure 3.1).** All of our employees and contractors we work with are given this mandate to be able to stop work if they believe the situation is unsafe. We celebrate and take learning every time this safety licence is used.

Everything in our draft Business Plan adheres to our best in class safety practices.

Figure 3.1 Our safety licence

A secure network

In the context of the energy industry 'secure' means that the energy reaching homes and businesses is certain and dependable. Many will refer to the security of supply, or to network reliability.

Security of supply is the fundamental objective of the businesses involved in producing, transporting and supplying energy. If the end consumer cannot access the energy they need then, overall, the industry has failed.

Security of supply

Each year the UK Government reports to Parliament on security of supply[1]. The Government will intervene when required to ensure consumers have the electricity and gas they need. A recent example of such intervention was the establishment of the Capacity Market which makes payments to parties that can balance supply and demand when required.

The criticality of security of energy supply to the GB economy cannot be understated.

There is a high economic and social cost for households and businesses if their supply of electricity is interrupted. A report commissioned by the Scottish Government forecast that a total shutdown of the Scottish electricity networks would cost the Scottish economy in the region of £930 million per day.[2]

It is unsurprising, therefore, that both household and business electricity users report that they would pay significant sums to avoid power cuts. A recent European study reported the value of 1kWh of energy, equivalent to boiling a kettle ten times, to be €4.62-15.90 (approximately £4-14) depending on the consumer group and duration of the power cut[3].

We commissioned a GB Willingness to Pay study to measure the value that domestic and non-domestic consumers place on the service provided by the electricity transmission network. Consistent with similar previous studies, consumers placed a high value on avoiding power cuts. To reduce the duration of power cuts from six to four hours, households report an average willingness to pay of £7.70 and businesses £43.30[4].

[1]Statutory security of supply report (BEIS, 2017) available at: https://www.gov.uk/government/collections/statutory-security-of-supply-report
[2]EY Report to the Scottish Government, "Black Start Event – Assessment of the Socio-Economic Costs and Recovery Standards for Scotland", April 2018
[3]Study of Value of Lost Load (VoLL) in electricity supply (ACER, 2018) available at:
http://cepa.co.uk/news-details-acer-publishes-study-on-the-value-of-lost-load-in-the-electricity-supply?selYear=2018
[4]Willingness to pay (2019) available at: https://www.ssen-transmission.co.uk/information-centre/industry-and-regulation/riio-t2/

The role of networks in security of supply

There are three essential parts to this role:

1. To make sure there is a **continuous** network between generators and consumers;
2. To provide sufficient **capacity** for the maximum volume of electricity that needs to be transmitted; and
3. To maintain the power **quality** within the levels that can be safely used in homes and businesses.

For electricity transmission networks, such as the our network in the north of Scotland, the consequences of failing to achieve any one of these three parts can be severe.

This is because many electricity consumers depend on the operation of a single overhead line for their energy. Thus, a failure in the operation of the transmission system can result in a power cut to homes and businesses across a significant geographic area (see Quioch Landslide example below).

The security of supply performance of the GB transmission system is measured by:

- Availability of the transmission system
- Loss of supply events: number, duration and impact
- Power quality: voltage and frequency

The Electricity System Operator (ESO) publishes a performance report each year.

Overall, the GB electricity transmission system has a high standard of performance. For the most recent reporting year 2017/18, the reliability of the GB transmission system was 99.999975% and there were 21 events that resulted in a loss of supply to customers[5].

The exceptional performance of the electricity transmission system reflects the ongoing focus of the network operators on security of supply. Continued high expectations from consumers, changes to the use of the network and emerging global risks mean that providing a secure network remains one of our strategic themes for the RIIO-T2 period.

Quioch Landslide

On 12 November 2018, a massive landslide of 9,000 tonnes of rock and soil occurred near Loch Quoich in the northwest Highlands. The landslide cut across the 132kV transmission overhead line that provides electricity supplies to more than 20,000 homes and businesses in Skye and the Western Isles. Emergency plans, including welfare services and back up generators, were implemented to restore power within 24 hours. A temporary line was constructed within seven days. The road which was also destroyed by the landslide is not expected to re-open until mid-2019.

[5]National Electricity Transmission System Performance Report 2017–2018 (National Grid, 2018) available at: https://www.nationalgrideso.com/insights/transmission-performance-reports

Stakeholder-led outcomes

Different stakeholder groups have different expectations for the secure operation of the north of Scotland transmission network.

In section 2, we have discussed who our stakeholders are but, for the purposes of security of supply, we broadly recognise three groups:

End consumers

These are the homes and businesses that consume electricity.

In the north of Scotland, there are only two demand customers that are directly connected to the electricity transmission system. In addition, there are 740,000 homes and businesses connected to the local distribution network, in turn connected to the transmission system at a Grid Supply Point (GSP). Increasingly these end consumers are also micro-producers of electricity with solar panels.

For end consumers, a reliable supply of electricity is consistently reported to be their number one expectation from electricity networks. This expectation was re-affirmed in the most recent research undertaken for RIIO-T2 **(Figure 3.2)**, including Willingness to Pay expressed preferences[6].

We are the only GB transmission licensee to offer a compensation scheme for homes and businesses affected by a power cut on our network.

Figure 3.2 Factors affecting electricity transmission

Factors	Score (1-10)
Security of supply	9.46
Environmental impact	8
Cost to customers	7.88
Economic impact (local / national)	7.2
Impact on local communities	6.88
Consequences for employees	6.44

From Stakeholder Workshop, March 2018[7]

Connected customers

These are the generators of electricity that are connected to the electricity network in the north of Scotland.

Around two thirds of the generating capacity in the north of Scotland is connected directly to the electricity transmission system. These customers are wind farms, hydro electric power stations and the Peterhead gas-fired power station. Some of these customers have connection agreements that limit access to the transmission system at certain times.

The remaining third of the generating capacity in the north of Scotland is connected to the distribution network, i.e. is embedded. Some of these customers will export onto the transmission system and may be compensated where they are requested to cease generating by the ESO (known as 'constraint payments') for certain network conditions.

All connected generators, whether direct to the transmission system or embedded, rely on network access to get their generated power to market. Put simply, without an available network, the power station cannot operate and so does not produce electricity to sell.

Connected generators rank network availability as their number one expectation from electricity networks[8]. Where these customers have connection agreements that limit their access they want good information about when these constraints will occur.

Future consumers and customers

As the energy system changes, future consumers and customers might have different expectations from current consumers and customers for the secure operation of the north of Scotland transmission network. This is an important consideration when actions we take today can have consequences for many years ahead.

We take direction from national policy objectives (see Section 1) to decarbonise and digitise the economy. The consequence of this is likely to be continued focus on network reliability and availability (including for new capacity).

Our research indicates that security of supply is the priority of our stakeholder groups. **Is this an appropriate assumption for the duration of RIIO-T2 until 2026?**

[6]Willingness to pay (2019) available at: https://www.ssen-transmission.co.uk/information-centre/industry-and-regulation/riio-t2/
[7]Our Stakeholder Workshop (SSEN, March 2018) available at: www.ssen-transmission.co.uk/media/2730/ssen-transmission-stakeholder-workshop-report.pdf
[8]https://www.ssen-transmission.co.uk/media/3405/ssen-riio-t2-commercial-connections-policy-paper-28pp-22782-artwork.pdf

Resilience

Being resilient

Our engagement with stakeholders has led us to conclude that a secure network remains a priority for the RIIO-T2 period, where they place significant value on not having power cuts.

End consumers expect reliability and connected customers require network availability. Our attention is focused on having a network that is resilient to the events that might affect these outcomes.

We use the definition of Resilience from the Cabinet Office report on Keeping the Country Running: Natural Hazards and Infrastructure[9]:

"Resilience is the ability of assets, networks and systems to anticipate, absorb, adapt to and / or rapidly recover from a disruptive event."

The report identifies four principle strategic components to infrastructure resilience: Reliability; Redundancy; Resistance; and Response and Recovery **(Figure 3.3).** For the risks facing our network, we must act proportionately on all four of these components to deliver the most cost effective risk management response.

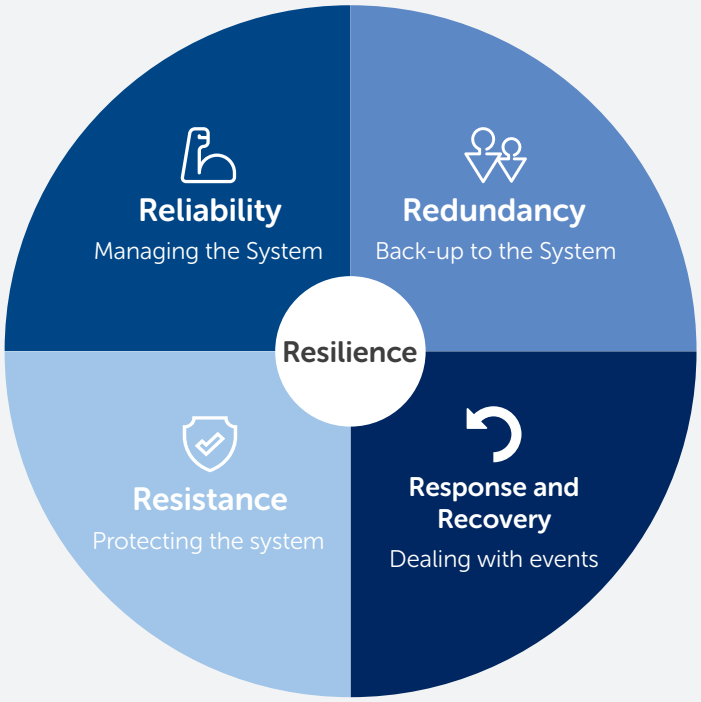


Figure 3.3 Components of network resilience

Reliability

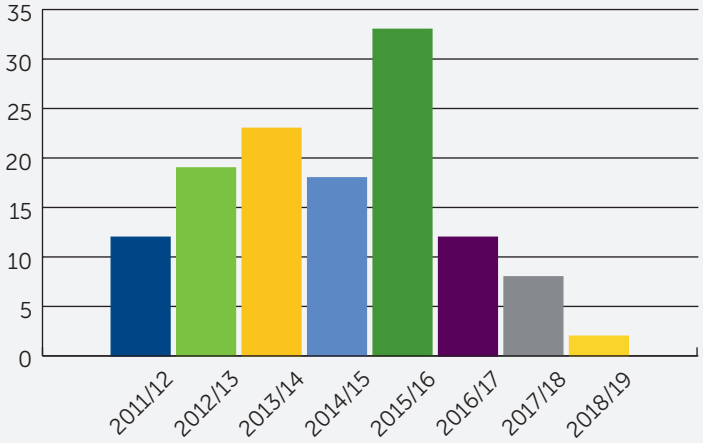
The reliability component of resilience is concerned with the design and operation of the network under a range of conditions. It includes taking steps to maintain, replace or refurbish assets before their performance deteriorates below expected standards.

Reliability performance is measured using the lagging indicator of the number of loss of supply events and the impact of these on the end consumer **(Figure 3.4).** Since 2010, we have had 127 loss of supply events that have resulted in power cuts for end consumers. The longest duration event in 2013 lasted 1,450 minutes (around 24 hours). This was due to a tower collapse in blizzard conditions.

For some connected customers, we have agreed that they will not have 100% network reliability. For example, when we are undertaking essential maintenance and there is no network back-up. For these customers, our planning for future network availability and engagement in this planning process is critical.

Over the past five years, working with the other Transmission Owners and Ofgem, we have been working to develop a leading indicator for reliability. This is called the Network Asset Risk Methodology (NARM). In essence this is a risk-based approach to assessing the need for asset replacement or refurbishment.

Figure 3.4 Loss of supply events



From ESO System Performance Reports. Loss of supply events of >3 minutes duration resulting in a power cut to end consumers.

[9]Keeping the Country Running: Natural Hazards and Infrastructure (Cabinet Office, October 2011) available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61342/natural-hazards-infrastructure.pdf

Redundancy

The redundancy component of resilience is concerned with the availability of back-up installations or spare capacity. These back-ups would enable operations to be switched or diverted to alternative parts of the network in the event of disruptions to ensure security of supply.

The design of the GB transmission system is governed by a common standard: the Security and Quality of Supply Standard (SQSS). We are obliged under our licence to comply with the SQSS[10].

For large demand centres (such as towns and cities) and the main parts of the transmission system, the SQSS requires redundancy in planning and operation. This means that if one part of the system were to fail then a back-up would already be installed and there would be no interruption to service.

However, for more remote parts of the network and for many generator connections, redundancy is not a requirement of the SQSS. This is the norm for the transmission system in the north of Scotland. There is no common standard or methodology for redundancy over the requirements of the SQSS.

When the system fails without redundancy the options are (i) non-transmission network power sources, and (ii) replacement of the failed assets. In the example of the Quoich landslide (see box on page 65), the first step was to use back-up generation already installed for this risk. This restored power to consumers while a new transmission line was constructed.

The availability of spare equipment is essential for timely restoration. New transmission equipment like transformers and cables can take many months to manufacture. For us, as we install new types of equipment on our network (including High Voltage Direct Current (HVDC)) we must make sure we have plans in place, and the spares available, to deal with asset failure.

Resistance

The resistance component of resilience is concerned with providing protection from natural hazards or malicious events.

The safe operation of an electrical network requires inherent system protection from, for example, poor power quality, electrical overloads and network damage. This system protection is similar to a fuse box where disruption to the flow of power will trigger the fuse and protect the wider system. Our fuse box comprises automated and remotely operated communications equipment, electrical switches and relays.

Physical threats to the integrity of the GB transmission system can be by accident or due to criminal activity. The security of our sites must be sufficient to deter or avoid such threats. Over recent years we have worked closely with the national security services to protect key sites.

Natural hazards also present a physical threat to the network. In recent years we have experienced flooding, wild fires, landslides and extreme weather. Most commentators expect the frequency and intensity of these events to increase.

An emerging concern, again expected to increase, is cyber security. In common with much of the economy, we now rely on information systems in our business. We distinguish between operational systems necessary for security of supply and business systems that are used for non-operational reasons. For example: word processing and financial systems.

Under the Network and Information Systems Regulations 2018 we are an Operator of Essential Services. This means we have a statutory responsibility to manage cyber security and cyber resilience in such a way as to minimise the threat.

[10]Security and Quality of Supply Standards (National Grid ESO, 2011) available at: https://www.nationalgrideso.com/codes/security-and-quality-supply-standards

Response and recovery

The response and recovery component of resilience aims to enable a fast and effective response to and recovery from disruptive events. The effectiveness of this element is determined by the thoroughness of efforts to plan, prepare and exercise in advance of events. It can be referred to as Business Continuity Planning.

Business Continuity Planning is for significant events, typically at a national scale. No business can be free from such risks, and hence active risk management is essential. We operate under the risk framework of the SSE Group. This framework includes regular simulation events to test preparedness and procedures[11].

As a provider of critical national infrastructure, we also participate in national forums such as the Centre for the Protection of National Infrastructure. This ensures we can share learning and maintain best practice.

The most significant event that could occur on the GB transmission system is a full or partial shut down; termed a Black Start (see box).

The current standard for a Black Start event, set in 2010 by the Energy Emergency Executive Committee (E3C), is for the main substations to be resilient against loss of system supplies for a minimum period of 72 hours. This time is considered the duration that may be required to achieve a full system restoration. This is reflected in the industry standard Engineering Recommendation G91[12].

In light of changes to the GB energy system, the Government and Ofgem are currently reviewing the GB restoration standard for a Black Start. Our stakeholder feedback has demonstrated strong support for this review of the Black Start expectations, and the necessary investment to be able restore power in a timely manner[13].

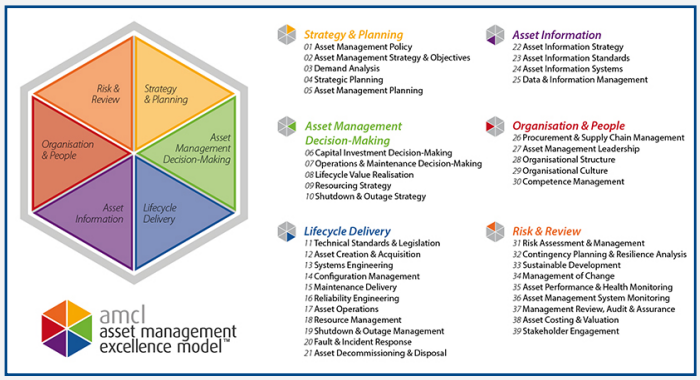


Figure 3.5 AMCL Asset Management Excellence Model

World class asset management

To deliver a resilient network - reliability, redundancy, resistance, and response and recovery – effective asset management planning and delivery is required. The SSE Group has a strategic ambition to be a "world class asset and infrastructure business", and we share that ambition.

To assess and measure our asset management capabilities, we use the Asset Management Excellence Model developed by international consultancy AMCL[14] **(Figure 3.5)**. This provides a comprehensive framework of 39 business activities that are essential to world class asset management outcomes.

For our stakeholders, excellence in asset management means no power cuts. Hence we have set a clear goal of 100% network reliability for homes and businesses.

Black start

Black Start is the rare and unlikely situation where the GB transmission system has shut down, in whole or part, and needs to be re-energised. Historically, large thermal (gas or coal) power stations would have been used to restore the system. However, as the GB energy industry has decarbonised, these large power stations have been closing down. This is of particular concern in Scotland, where the ESO, TOs and Government have been working to establish a new Black Start procedure

Peterhead gas-fired power station

[11]SSE plc Group risk report 2017/18 (SSE plc Group, 2018) available at: https://sse.com/media/522431/sse_plc_risk_report_2018_interactive.pdf
[12]Energy Networks Association engineering documents (ENA) available at: http://energynetworks.org/electricity/engineering/engineering-documents/engineering-documents-overview.html
[13]In response to our Emerging Thinking consultation, Future Operation of our Network consultation and stakeholder events.
[14]https://www.amcl.com/

Improvements during RIIO-T1

We have an operating model of continuous improvement and, as shown in the examples below, during RIIO-T1 we have made significant improvements in our network resilience.

Asset information and systems

At the time of preparing our Business Plan for the RIIO-T1 period, we relied on dated IT systems and business processes for the management of our network assets.

As a consequence of these legacy arrangements, our Business Plan was based on incomplete asset information. This meant, as we gathered accurate data after the price control was set, we identified the need to do more asset replacement works than we had planned.

We have remedied this business weakness by investing in new asset information systems. In parallel, we have undertaken a fundamental review of our asset information including condition and performance data for each lead asset. Lead assets are the primary assets on our network and include transformers, underground cables, circuit breakers, reactors and overhead lines.

Our Business Plan for RIIO-T2 is based on these new systems, along with the risk-based NARM for making asset intervention decisions.

Protection

The resistance of the transmission system to electrical damage is due to the protection and control "fuse box".

In April 2014, we had a major loss of supply event that affected more than 200,000 homes and businesses in the north and west. The investigation into this event identified weaknesses in the procedures for setting and managing the network protection and control in some substations.

An 18-month project undertook a re-design of our protection and control arrangements. A key part of this was to verify and risk assess all of the existing network communications equipment.

High fault circuits

Analysis during RIIO-T1 identified that the majority of interruptions on our network are short duration (<3 minutes), and cluster in discrete parts of the network. We have targeted the assets with high events. Our fault volumes have fallen significantly over the price control to date, from their peak of 182 in 2014/15 to just 79 in 2017/18.

Outage planning

At the start of RIIO-T1 we introduced our Network Availability Policy[15] (NAP). This has fundamentally changed our approach to the planning and delivery of network outages.

Generator communications

We have provided forecast outages for up to five years ahead for customers. This has resulted in generators modifying their inter-trip arrangements, or connections, via already established procedures with the ESO to reduce the impact of some of these future outages. For RIIO-T2, we propose to enhance this service by submitting outage plans for the full price control period to the ESO in advance. This means both the ESO and customers have a clear picture of the draft outage programme and can plan accordingly.

Accuracy of outages

Over the course of RIIO-T1, motivated by the needs of our customers and the ESO, we have focused on improving the accuracy of our outage plans. This has resulted in significant improvements in the accuracy of the start date, the duration and the completion of outages.

Enhanced service provision

Through industry working groups, we have supported the establishment of a process whereby the ESO can request modifications to outage delivery plans to reduce constraint costs. A fund of around £1.5 million is available each year to use the constraint cost savings to invest in this provision.

Asset Fleet Hubs

These groups have been created to develop and implement strategies for the whole lifecycle management of each key equipment type and are a key component of our Asset Management System.

The asset fleet hubs bring together subject matter experts from across our organisation to review the performance of each asset family (including assessment of condition monitoring results, faults, defects and investigation reports) and the impact of asset performance. These reviews have led to the development of enhanced policies and strategies to ensure that plant runs optimally and revisions to intervention/replacement approaches.

The hubs also explore new technologies and innovation, and how these might be applied to the technical specifications for our assets.

[15]Network Access Policy RIIO-T1 (ofgem, 2012) available at: https://www.ofgem.gov.uk/sites/default/files/docs/2012/10/7_network_access_policy_shetlandsptl_0.pdf

The role of innovation

Cyberhawk

Cyberhawk[16] is a company that SSE helped establish and develop through partnership funding. Together we have jointly developed an inspection and database system.

Visual inspections are completed via drone or our employees for overhead lines and by employees for substations. The results of these inspections are fed into databases which allow us to build up a condition matrix of our network. As this way of working has been developed and rolled-out over the past five years, this has become our standard maintenance procedure.

Benefits include:

- Efficiency in our maintenance programme;
- Better investment decisions supported by a higher resolution of asset condition information; and
- Supporting better management of our network defects.

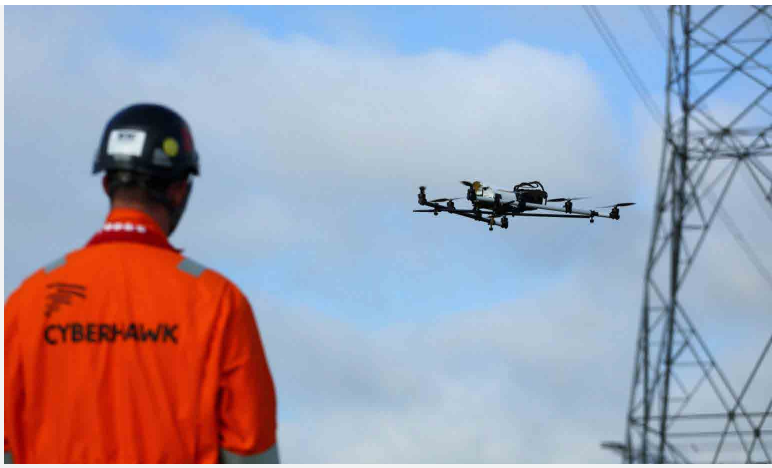
SF_6 camera

Sulphur Hexafluoride, or SF_6, is an excellent insulating medium and is commonly used within switchgear and busbars on electrical networks. However, it is very bad for the environment, with a Greenhouse Warming Potential (GWP) of 23,000 times that of Carbon Dioxide.

To reduce our SF_6 leakage, we have deployed FLIR[17] GF306 infrared cameras. We have a long-standing relationship with FLIR for other inspection equipment. They developed this camera to detect SF_6 leakage from network assets. Initially we used this reactively to respond to SF_6 leakage alarms. However, as we built up an understanding of its capabilities we moved to more proactive use as part of our standard maintenance procedures. Benefits include:

- Quicker identification and location of leaks against previous standard process;
- Faster leak repair times; and
- Reduction in leakage volumes.

A good example of this was when a design issue was identified with one of our standard fleet of 132kV circuit breakers. The design flaw led to a leakage from a consistent place on the switchgear, which allowed us to proactively check for leakages, thereby reducing the amount of gas leaked, whilst a permanent solution was identified.



Future innovation focus

These two innovations are part of a number that have delivered benefits to stakeholders in RIIO-T1. We use innovative approaches across our operations and asset management such as new asset types, technologies and design standards, and ways of working.

We see innovation as an important tool to help us better understand and manage risk associated with future network and industry change. In this way, we see that innovation will continue to deliver value to stakeholders as long as our trials are specifically aligned with our strategic objective and measurable stakeholder benefits.

The Innovation Policy published alongside our draft Business Plan lays out a framework for how all innovation will be delivered, regardless of topic or funding source. The framework defines our core principle of being a responsible innovator. This ensures that we do the right things at the right time for our current and future stakeholders. All innovation must: support the customer; be user driven; delivered efficiently; maximise collaborative efforts; and support our sustainable ambitions.

Building on that framework, we have defined what we will innovate on to achieve our strategic objective and principal goals. It is essential that opportunities are assessed for alignment before being developed. In this way our innovation programme will only test topics that support a transition to a low carbon future and are what our stakeholders have told us is important. In this way we can guarantee targeting value for our current and future stakeholders.

Read more about our Innovation Policy and the benefits of targeted innovation here:
https://www.ssen-transmission.co.uk/media/3390/111regulatory-framework_final-draft.pdf

[16]www.thecyberhawk.com
[17]www.flir.co.uk

Planning for RIIO-T2

We have used the four principle components of infrastructure resilience in our planning for safe and secure network operation during RIIO-T2.

Drivers for Change

There are substantial differences in our planning for infrastructure resilience during RIIO-T2 when compared to the RIIO-T1 period **(Table 3.1).**

Three of these are of particular importance:

1. The north of Scotland transmission system

In terms of asset value, the system is three-times the scale it was in 2013. It has a different age profile, topology and technology. It now incorporates 220kV and HVDC assets on land and subsea.

2. Our organisation

As the network has grown, so we have had to change our organisation, ways of working and capabilities (see box on next page).

3. Data as an asset

Communications and analytical technologies have changed dramatically over the past decade. The evolution and cost reduction of sensor technology, advances in mobile data capture, storage of data, speed of access and machine learning mean that the capabilities of the Transmission Owner can be greatly enhanced, and data driven evidence means that timely intervention in the asset's life cycle are justifiable, efficient and improve safety, resilience and availability of the network.

Table 3.1 drivers for change in RIIO-T2

Component	Key change from RIIO-T1 period	Material impact on...
Reliability	• Generator type and location • Consumer behaviour and energy use • Implementation of NARM • New technology, including digitisation and dynamic data	• Risk-based decisions on asset replacement and refurbishment • Risk-based approach to inspections and maintenance • Constraint costs and consequences of unavailability for generators • Cost-effective to implement smart monitoring and data control room
Redundancy	• Network growth • New technology • Risk-based approaches to planning and operations	• Risk associated with critical single points of failure • Need for asset spares and warehousing
Resistance	• Network growth • New technology • Growing physical and cyber threats	• Need for physical site security • Many protection systems now obsolete • Consequences of a changing climate
Response and Recovery	• Generator type and location • New Government standards (tbc)	• Business Continuity Planning • Expectations for emergency response • System tools available for Black Start

Uncertainty during RIIO-T2

Although we have confidence in our plans for a secure network during RIIO-T2, there are always things we don't know.

NARM

At the time of writing our draft Business Plan, the NARM has yet to be fully developed for use during RIIO-T2. This means we have not yet established a baseline position or a methodology for deriving our risk-based target. This Business Plan is prepared on a provisional basis and we expect these issues to be resolved for our final December 2019 Business Plan.

As NARM is a new methodology, and only applies to lead assets, we expect improvements to be made during RIIO-T2. Such improvements, and new information, might result in changes to the intervention outcomes. As such we believe a relative (or "delta") target and 'substitution' process are essential to avoid inefficient actions driven by a position fixed at the time of the price control settlement.

Black Start

We expect the standards for Black Start restoration to be revised either before or during RIIO-T2. As part of this revision, it is likely that consideration will be given to market-based options. Given this uncertainty, we believe it is prudent to establish a regulatory mechanism where the ESO can direct TOs to take action when the need is established. The price control settlement should then 'flex' to allow the TO to recover the efficient cost of meeting the ESO's requirements.

Cyber security

Cyber threats are quickly evolving, as are the actions available to Operators of Essential Services to manage cyber security and resilience. It is extremely challenging to apply the five-year forward planning horizon of the RIIO price control process to cyber security. We propose that outputs and allowances for cyber security are 'reopened' in summer 2023 to account for new information.

Subsea cable faults

While we take all the actions we can to ensure that we have no faults on our network, it is not always possible to avoid events outwith our control. For subsea cables, this might be due to subsea landslides or third party damage. Should a fault occur on a subsea cable the time and cost associated with repair can be significant. In this circumstance we propose a mechanism to allow us to recover the efficient cost.

Our changing organisation

As our network has grown, so has our capability for managing and operating the asset.

Some of the key changes over the past decade are:

November 2013
International benchmarking of our operations starts through ITOMS

April 2014
New asset management team established to begin development of NOMs / NARMs begins

May 2015
Protection Task Force established

October 2015
Field operations team brought in-house, with transfer of 90 employees

October 2015
Kintyre - Hunterston 220kV subsea cable energised

November 2015
Beauly – Denny final energisation – first 400kV network in north of Scotland

December 2017
International benchmarking of asset management delivery starts through ITAMS

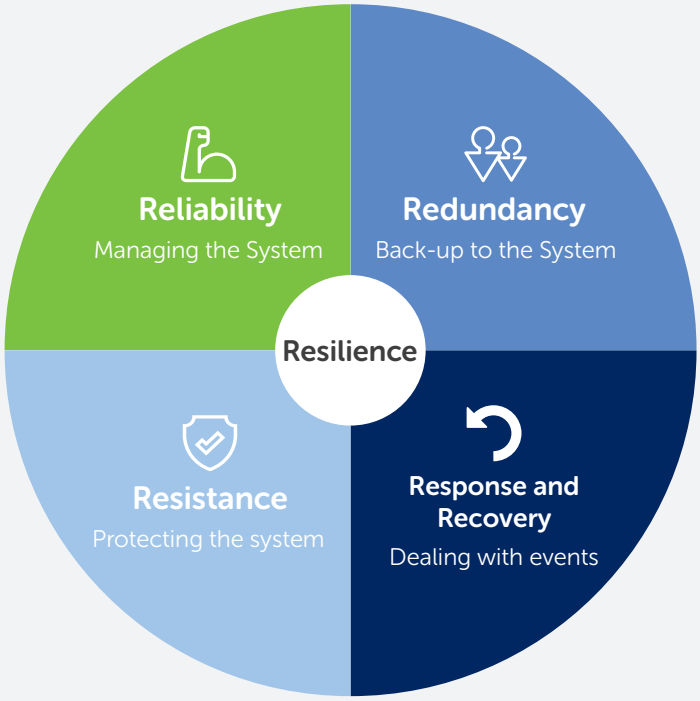
April 2018
Customer interruptions for 2017/18 due to faults on our network reduced to 2 (from a peak of 33 in 2013/14)

December 2018
Energisation of Caithness Moray HVDC

March 2019
Operations team has grown to 170 employees coveting all aspects of AC and HVDC operations on the north of Scotland network

April 2019
New governance model implemented

Our RIIO-T2 Plans: Reliability



The reliability component of resilience is principally concerned with the day-to-day management and operation of the transmission network.

Fundamentally, the focus of reliability is on delivering the security of supply that customers want and expect. For consumers, many surveys (including the Willingness to Pay research we have carried out for this Business Plan) evidence the high value placed on uninterrupted, unconstrained access to electricity.

Participants in the GB energy market, such as generators, storage providers or demand-side solutions, pay for access and use of the transmission system. For these customers, the unavailability of the network means they are not able to run their business and meet their commitments to their customers.

Our day-to-day operations are the front line of providing a reliable, available network to our customers. We break these operations activities into four main elements:

1. Inspections and maintenance
2. Risk-based asset interventions
3. Control Centre
4. Network availability

Each of these elements is risk-based and seeks to balance the efficient cost with network outcomes.

Inspection and Maintenance

Undertaking inspection and maintenance of installed assets, and the surrounding environment, is fundamental to the operation of any infrastructure business.

Inspection allows us to collect information about the condition, performance and operating environment of the equipment on the network. Routine maintenance activities and inspection ensure that the assets are in the best possible operating condition and environment.

It is through inspection and maintenance that we meet many of our statutory and licence obligations for the safe and secure operation of the network. The information gathered is a critical input to our risk-based asset intervention decisions.

Historically inspection and maintenance has been undertaken to time-based schedules that follow manufacturers' recommendations and industry best practice. For example, there are specified activities every 6 and 12 months for transformers. Vegetation management, likewise, is done to a routine schedule. This approach allows for scheduling of site visits and tasks for weeks and months ahead, supporting efficiency in operations.

We intend to continue to follow time-based schedules for inspection and maintenance during the RIIO-T2 period. We forecast the cost of these activities to be at least £101 million for the Certain View, and higher if the network continues to grow (section 4).

As we look forward beyond 2025, and as we develop our risk-based approach to asset management, we expect the opportunities of new technology will allow us to change our inspection and maintenance model. Integrated monitoring of asset condition and performance, including the collection and analysis of real time data, will enable risk-based inspection and maintenance. In the first instance we expect this would supplement time-based schedules but, over time, would become the standard approach.

We are taking a cautious approach to the introduction of new monitoring equipment such as drones, robots and sensors. We are mindful of the cost associated with large-scale roll out and, hence, are applying Cost Benefit Analysis to direct targeted projects. These projects are of material value to high access cost locations in the remote north of Scotland and islands.

Integrated monitoring

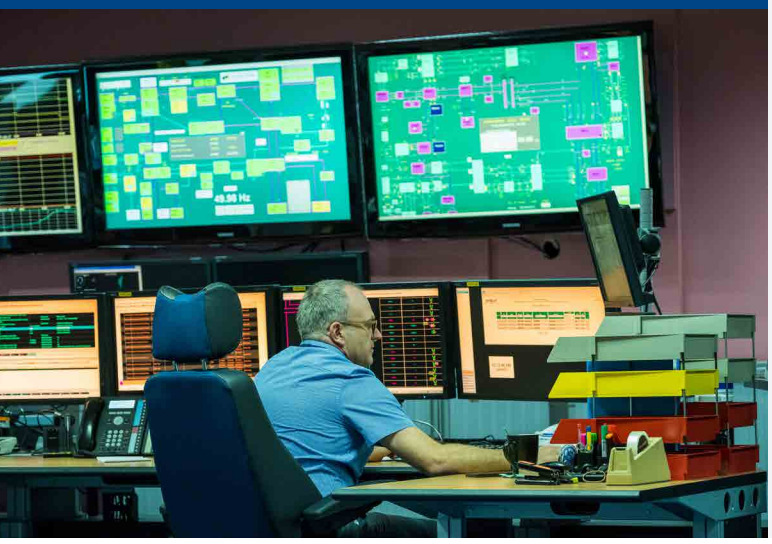
Effective system and condition monitoring within asset management plays a significant role in improving the performance, reliability and longevity of electrical and mechanical assets. Accurate and timely diagnosis of critical or high value, long lead time assets, such as power transformers, is critical for the reliable and cost-effective operation of the transmission network.

During the RIIO-T2 period, we forecast expenditure of £13 million to undertake projects at 61 sites across the network. These projects will deliver integrated condition monitoring of key assets, along with the development of data collation and analytical tools.

Integrated monitoring will enable us to view the performance and operation of plant on our network in real time, undertake trend analysis and enable risk-based intervention on equipment to ensure the network is performing optimally. It removes the need to undertake maintenance on a routine, time based frequency, instead allowing us to take action when required. This should realise operational efficiencies, in addition to improved network performance.

A key component of integrated monitoring is the use of IEC 61850, an international standard for communications in substations. It enables integration of all protection, control, measurement and monitoring functions and facilitates high speed substation protection applications.

The roll out of this technology in our substations will further improve network operation and the availability of real time information.



Monitoring and improving the efficiency of our direct operations remains a primary concern. Our inspection and maintenance costs have increased from £3 million in 2013/14 to forecast nearly £20 million by 2025/26.

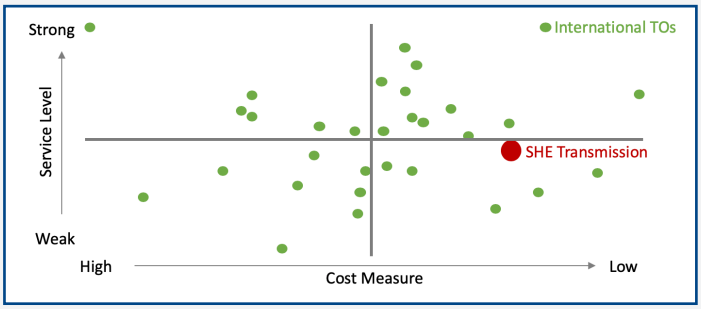
This increase in costs is unsurprising given the significant growth in the number and type of assets installed on the north of Scotland transmission network. It also reflects the increasing age of the pre-2010 network and the associated greater need for regular maintenance.

To ensure that the network growth does not mask the introduction of inefficiencies, we participate in a number of international benchmarking studies of our direct operating costs and service outcomes.

The most significant of these is the International Transmission Operations and Maintenance Study (ITOMS), which we are currently engaged in the fourth cycle of benchmarking. Our performance in previous ITOMS benchmarking has shown that for our service outcomes, we benchmark as in Quartile 3 – Lower Right **(Figure 3.6).** Our target during RIIO-T2 is to rank in Quartile 4 – Upper Right.

We take lessons and best practice from each ITOMS iteration that we use to drive performance improvements across our operations. Previous action plans have focused on emergency response planning, performance monitoring of our Control Centre, and management of stock.

Figure 3.6 Results from 2017 ITOMS benchmarking



The graph above shows relative cost on the horizontal axis and network performance on the vertical axis. We are low cost compared to most of the peer group and network performance is around average.

Risk-based asset interventions

One of our clear goals for the RIIO-T2 period is 100% network reliability for end consumers. We defined this goal from the strong and consistent view from electricity users of the importance of security of supply.

At the heart of achieving this goal is successful asset management. Asset management is a rigorous and systematic approach to achieving the desired performance of individual or network assets over the whole asset lifecycle. When successful it enables cost-effective performance outcomes.

All of the GB TOs have developed, and are in the process of implementing, a common risk-based model for asset management during RIIO-T1. This approach is used to determine the asset risk held on our network with a focus on lead assets (transformers, reactors, circuit breakers, cables, overhead line conductor, overhead line fittings and towers). The need for intervention can be assessed using the Network Output Measures (NOMs) Methodology[18].

We will continue the use of this model into RIIO-T2 (though it will now be known as NARM). We would highlight that this model is still relatively immature, and so we expect it to continue to develop and improve during the RIIO-T2 period. For example, we intend to incorporate the dynamic data being delivered by the integrated condition monitoring project into the NARM modelling approach to ensure that our long-term planning is supported by the best possible data.

Asset type	Volume	
275kV Transformers	11	nr
275kV Circuit Breakers	3	nr
132kV Transformers	24	nr
132kV Circuit Breakers	62	nr
132kV Overhead Lines	451	km
132kV Underground Cables	12	km
Reactors	12	nr

Table 3.2 Schedule of assets for intervention during RIIO-T2

We also have plans to develop new risk-based models during the RIIO-T2 period to expand the type of assets covered by the metric. Our objective is to have models established by 2026 that cover all electrical assets. This will provide a complete picture of network risk and support an improved decision-making process to deliver best value for the consumer.

For the purpose of our draft Business Plan we have made three key assumptions about the application of the NARM to inform our programme of asset management interventions:

1. The NOMs methodology as published on 14 June 2018 will apply;
2. The risk-based target for the RIIO-T2 period will be for relative monetised risk (i.e. a 'delta' target) and substitution will be permitted; and
3. Our target for 31 March 2016, assuming no network growth, will be for level of monetised risk to be the same as our forecast for 31 March 2021.

There remains ongoing development of the monetised risk target, and how this will be applied to RIIO-T2 interventions. We continue to engage with stakeholders during this process and adjust our assumptions as required.

For our Business Plan, we have identified 29 asset schemes (each of multiple assets) that will require intervention in order to maintain the monetised risk target on the network **(Table 3.2).** Each of these assets has been taken through our Strategic Optioneering Methodology to determine the preferred option for intervention, as described in the next section.

Attendees at our March 2019 workshop supported the undertaking of work in RIIO-T2 where it can be demonstrated to lead to more efficient outcomes in the future. **Do you support this approach?**

[18]NOMs Methodology Issue 18 (ofgem, 2018) available at: https://www.ofgem.gov.uk/system/files/docs/2018/08/noms_common_methodology_issue_18.pdf

Network Asset Risk Metric

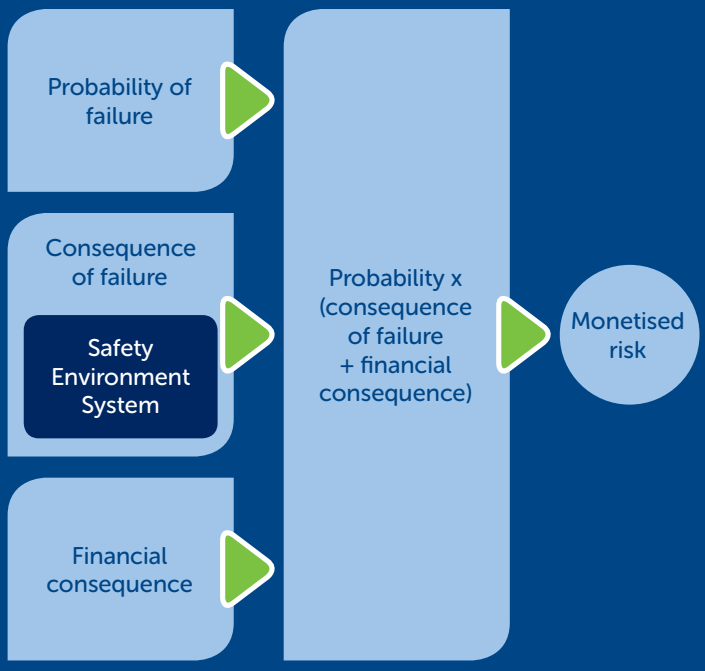
Since 2014 the three TOs have been working, with the guidance of Ofgem, to develop a common risk-based approach to assessing the need for asset intervention. This has resulted in the Network Output Measures (NOMs) methodology.

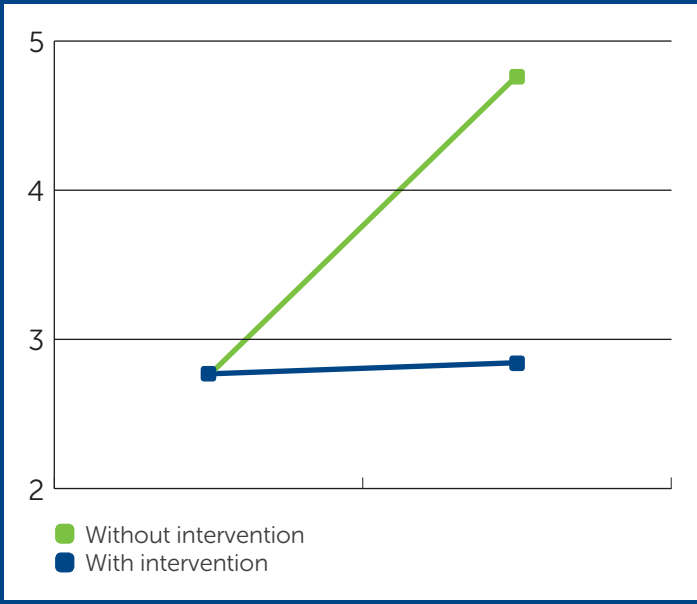
The diagram below illustrates the components of the monetised calculation of Network Asset Risk. This is done for each asset, and then aggregated to give an overall network view.

The probability of failure is largely a function of many data points of asset condition information gathered through regular inspection with specific condition monitoring for early indications of the deterioration of an asset. This information is input into a system, Condition Based Replacement Monitoring (CBRM), to determine the probability of failure.

Non-condition failure (e.g. extreme weather) is not considered in the model.

The consequence of failure takes asset and site-specific information to form a holistic view of the societal impact of the asset failing for a wide range of external factors grouped into categories of system, environment, financial and safety. Each consequence of failure is given a notional financial value. For example the cost to consumers of loss of supply.





The monetised risk is determined by multiplying the probability of failure of an asset within a given time period by the total financial consequence of that failure. As monetised risk can be determined for each asset, it is possible to rank the relative risk of assets and so prioritise the need for asset intervention.

As shown on the illustration above, asset condition degrades through time so without intervention overall network risk will increase. Our target during RIIO-T2 is to broadly maintain existing network risk.

It is important to note that this is a modelling tool and the financial consequences are notional, so critical engineering judgement is an essential part of the process. Moreso the input information is dynamic. For example the cost of carbon and cost of energy move daily. Thus monetised risk, and Network Asset Risk, are not fixed. To address this, a risk trading or substitution mechanism is required.

Monetised risk (£ billion)	
Start of RIIO-T2	2.77
End of RIIO-T2, without intervention	4.76
End of RIIO-T2, with intervention	2.84
Delta target	1.92

Control Centre

Our Control Centre works with the ESO and other TOs to manage the flow of electricity on the north of Scotland transmission system. For the majority of the time this is controlling power from renewable generation down to the Scottish Central Belt and on to England and Wales. As such, the Control Centre is a vital part of the national infrastructure.

We have a single Control Centre, with a back-up facility on a separate site. The Control Centre has been located in our main office in Perth for over 20 years. It is integrated into the open plan office environment. Overall the building is host to many SSE businesses, over 2,000 employees and daily external visitors. The area allocated for the Control Centre is shared with the SHEPD Control Centre.

As part of our organisational development to ensure our capabilities and facilities match the scale and challenges of our network, we undertook a review of the Control Centre. The key findings of this review were:

- Opportunities to strengthen site security and access to the Control Centre
- Space requirements to accommodate controls for real time system operation of a renewable-dominated system
- Planned expansion of the Control Centre function to incorporate real time asset monitoring
- The need for the back-up facility to include commissioning capability and operate for longer duration than current capability
- Learning from developments made by the ESO, other TOs and internationally in Control Centre facilities

Taken together, the findings of this review recommended significant improvement in our main and back-up Control Centre facilities.

Given the materiality of investing in our Control Centre, we undertook specific stakeholder engagement on the need, benefits and possible options. At our March 2019 Edinburgh event[19], we invited views on what we might do during RIIO-T2.

None of the stakeholders in attendance thought 'do nothing' was a preferred option. Two third of attendees favoured establishing new main and back-up Control Centres; and one third favoured the establishment of two full duty Control Centres. These new Centres would be secure and purpose-built to house the technology and personnel required to support our dynamic monitoring of the electrical and asset systems.

In line with the majority stakeholder view, we are proposing to establish new main and back-up Control Centres during the RIIO-T2 period. Our forecast cost for these works is £8 million.

Network Availability

Availability is the space, or capacity, which can be used at any specific time by our customers, typically generators exporting power. There are two aspects to availability:

- The available network capacity for new customer connections; and
- The available network capacity for the transportation of power.

It is of note that the GB transmission system is not designed to accommodate all of the electricity that can be generated from connected power stations at any one time. There are circumstances when generators may want to export, but are prohibited from doing so due to lack of network availability.

New connections

The energy market is increasingly diverse, which provides greater opportunity for these customers to share network availability and access. Higher utilisation avoids reinforcement to create new capacity, so saving customers money, but can restrict availability during periods of high usage.

The sharing of network availability and access is sometimes called flexible connections. Under these connection arrangements, generators agree upfront to the conditions under which export will be constrained. The flow of power can be managed by communications networks, such as intertrips or active network management schemes. Around one quarter of our customers have a form of flexible connection, and we expect this number to grow during the RIIO-T2 period.

Using the principles of Whole System Planning[20], this approach requires close collaboration with the customer, the System Operator and SHEPD. Flexible connections increase the complexity of network operations and can change the way that assets on the system are used.

In our stakeholder engagement about connections for RIIO-T2[21], customers have told us that their primary concern is that we must work together to arrive at the most optimal connection solution for their project, our network and the wider GB consumer. Specifically that they want a connection offer that meets the needs of their investment - whether this is a new connection, or the customer is looking to repower, or redesign their existing connection. The offer of optimal connections solutions, that would include quicker and low-cost flexible connections, is a key part of our Commercial and Connections Policy[22] ambitions for the RIIO-T2 period.

[19]www.ssen-transmission.co.uk/riio-t2-plan/
[20]www.ssen-transmission.co.uk/riio-t2-plan/
[21]RIIO-T2 Connections, Innovation and Whole Systems: Stakeholder Engagement Event, February and May 2019 output reports available at: https://www.ssen-transmission.co.uk/information-centre/industry-and-regulation/riio-t2/
[22]https://www.ssen-transmission.co.uk/media/3405/ssen-riio-t2-commercial-connections-policy-paper-28pp-22782-artwork.pdf

Network availability

In the most recent ESO report on the GB transmission system performance[23], the availability of the north of Scotland network was 97.29% (and 98.68% at winter peak). This figure is the % of the total circuits that are available to the ESO for the transport of power. As most circuits have a back-up, a circuit being unavailable generally does not interrupt supplies to consumers.

The main reason for network unavailability is construction during the summer months **(Table 4.3).** For both construction and maintenance there can be the need to de-energise the existing network in order to undertake works safely.

For this work to be done with the minimum impact on system security to consumers and users of the network, a process has been established that involves the ESO and Scottish TOs working closely together, known as the Scottish TO Network Access Policy[24] (NAP). The NAP covers the planning approach taken by the TOs and the ESO as well as describing the necessary consultation and stakeholder engagement that may be required.

Key to the success of the NAP is a flexible approach to outage planning and timing; close working with other stakeholders; innovative solutions to network issues; and a focus on cost-effective outcomes.

For our generation customers whose network access will be affected by planned outages, we are proposing a new outage engagement service. This forms part of our ambition to provide tailored customer services and products for our existing and future customers as set out in our Commercial and Connection Policy ambitions. This includes the customer being equipped with more information on our indicative outage plans as well as a dedicated contract manager post connection.

This would include an 'outage solution' product to work with customers to seek to minimise the disruption to them by either accelerating the outage or having alternative connections in place. At our May 2019 engagement event on connections, a majority of attendees said that they were satisfied with our ambition to provide this new service (the remaining attendees were neutral with no disagreements).

Table 4.3 Circuit unavailability (%) by reason, 2017/18

	System construction	Maintenance	Unplanned	Total
Apr	2.71	0.35	0.21	3.27
May	2.36	0.39	0.20	2.94
Jun	3.14	0.63	0.21	3.99
Jul	3.37	0.38	0.22	3.97
Aug	2.51	0.49	0.33	3.33
Sep	2.21	0.53	0.57	3.31
Oct	2.54	0.47	0.38	3.39
Nov	1.72	0.18	0.05	1.96
Dec	1.04	0.08	0.30	1.42
Jan	0.75	0.12	0.20	1.07
Feb	1.06	0.13	0.28	1.47
Mar	1.59	0.68	0.29	2.56

[23]National Electricity Transmission System Performance Report 2017–2018 (National Grid, 2018) available at: https://www.nationalgrideso.com/document/126551/download
[24]www.ssen.co.uk%2FWorkArea%2FDownloadAsset.aspx%3Fid%3D6131&usg=AOvVaw3o1y4rZbdbs7NGYyqxO_Yd

Our RIIO-T2 Plans: Redundancy

The redundancy component of resilience is, in essence, the availability of a back-up should something go wrong on the network. Redundancy addresses both equipment failure and unavailability. An asset might be temporarily unavailable due to the requirements of planned maintenance or during construction.

Our approach to redundancy is predicated on risk management. In this regard it complements our risk-based approach to reliability described above. While reliability is intended to pre-empt asset failure, redundancy plans for the timely resolution of asset failure or unavailability. This recognises that some circumstances that result in an asset not being in service cannot be predicted and avoided, for example extreme weather events.

A risk management approach to redundancy involves continual assessment of the consequence of failure or unavailability, and identification of the most cost-effective solution (including the 'do nothing' option).

With the changes to the nature and use of the north of Scotland transmission network, we have had to materially revise our actions on redundancy over the past decade. We anticipate this will continue during the RIIO-T2 period and redundancy will remain a key business focus.

Types of Redundancy

We define two types of redundancy:

1. Duplicate equipment or spare capacity that is installed on the system; and
2. Back up assets that are stored and can be quickly put into service.

The first of these has a 'near zero' time to deploy. Most commonly, this is the approach to planned maintenance. For example, a substation will have two transformers installed. When one transformer is being maintained, the other transformer continues to operate and there is no interruption to service.

The second has a material time to deploy, perhaps of several days. Back up assets are used where there is no duplicate already installed, or where the full system has been taken out of service. Most commonly, this situation arises for generator connections where no duplicate is installed.

Installed redundancy

The GB transmission system is designed and operated under common criteria and methodology: the Security and Quality of Supply Standard (SQSS). Adherence to the SQSS is one of our licence obligations.

The SQSS sets out the minimum standards for the design of the GB transmission system, noting that higher standards can be economically justified. In many, but not all circumstances, the minimum standard is for no loss of supply in the event of planned outages or faults. Thus the SQSS mandates installed redundancy for much of the GB transmission system.

Our risk-based approach to redundancy focuses on those parts of the network where the SQSS does not require installed redundancy. Examples of this are:

- Generator connections, where the generation customer has opted for a design variation to reduce the network design below the SQSS minimum standards; and
- Some small consumer demand connections, where the SQSS does not require immediate recovery from loss of supply.

While these potential single points of failure are acceptable, the associated risk must be actively managed.

For our Business Plan, we propose three main actions for installed redundancy:

1. We are committing to work with our generation customers to undertake regular design reviews of their connection arrangements. You can read more about this in our Commercial and Connections Policy.

2. There are single points of failure on the network where there is not an economic case for installing duplicate assets. We have risk management plans in place for each.

3. We will apply our new cost benefit analysis methodology to our assessment of single points of failure to determine whether there is a case for investment. We explain this new analytical approach on page 102.

In addition to these actions, we will maintain our compliance with the SQSS for installed redundancy. Some aspects of the SQSS are under review as part of the changes to decentralise and digitise energy networks (see whole system planning standard box).

Part of our risk management is to assess the economic justification for installed redundancy where it is not mandated by the SQSS. Using cost benefit analysis we can model whether the cost of duplicate equipment is outweighed by the benefits that result. We consider this on a 'whole system' basis, working with SHEPD and the ESO to determine whether duplication of equipment is the most cost-effective solution.

As the inputs to our cost benefit analysis or the options to achieve redundancy change then we must repeat this assessment.

A whole system planning standard

With increasing capacity of generation and flexible resources such as battery storage, microgeneration and demand side response on SHEPD distribution's network, we are seeing a greater need for working more collaboratively with SHEPD to understand the impact of this on power flows on the transmission system. Coupled with the increasing capacity of large renewable generation on the transmission system, we are seeing significant variability of power flows both on the transmission system and at the interface points with SHEPD (Grid Supply Points).

Currently, transmission system planning is underpinned by the SQSS, a largely deterministic standard, which was developed based on the traditional power system planning model with large centralized power stations and inflexible demand. Clearly, the system has transformed and is continuing to do so at pace, with the planned introduction of the DSO and management of flexibility services through the market to maintain the safe, secure and economic operation of the GB electricity system.

The level of installed redundancy stipulated by the SQSS depends on the size of demand and generation, both of which are increasingly flexible.

We are working collaboratively with the ESO to develop probabilistic system analysis tools to understand the likely curtailment of generation or demand and the risk this may cause to the safe, secure and economic operation of the system. This also helps us to identify cases where deviating from the redundancy criteria of the SQSS is the right thing to do. Where this is less than the SQSS compliance level, we seek derogation from the relevant SQSS criteria. An example of this is the derogation on the proposed rebuild of the 132kV line between Beauly and Loch Buidhe substations which was deemed uneconomic at this time by the Network Options Assessment (NOA) process. Equally, where a higher standard is justified, we demonstrate this based on balancing the costs of the additional redundancy against the benefits on a whole system basis.

We participate in the industry review of the SQSS and we are currently working with the ESO and other TOs to scope the review of the standard to address these challenges.

Back up assets

Back up, or spare, equipment that is stored with deployment plans is an essential part of redundancy.

Prior to the RIIO-T1 period and the significant growth of our network, it was not economic for us to establish and run warehousing facilities. We used operational locations as secure storage facilities, and worked with other network owners to ensure we had access to the spare equipment that we might need.

Over the past decade, as the north of Scotland transmission network has grown, so too has our stock of spares. In late 2018, our stock value was around £100 million.

The new technologies that we have energised mean it is less possible to share equipment with other networks. Our asset base now includes: HVDC, 220kV subsea cables, high voltage Gas Insulated Switchgear, Static VAR Compensators (SVCs) and Statcoms. In addition to electrical equipment, we have essential protection and control technology.

A detailed review of our approach to warehousing and stock controls has identified significant benefits from moving to a centralised approach. This approach would also enable improved physical and cyber security measures to be adopted.

We have explored a number of options to find the most cost effective approach to the storage of back up assets. Our assessment has taken into account the whole life costs of the options, including the time to deploy and risk of damage to or speed of degradation of stored equipment **(Figure 3.7).**

For our Business Plan, we are proposing a multi-element plan that continues to use equipment sharing and service level agreements with manufacturers. However we are also proposing:

1. Two new staffed warehouse facilities, with non-staffed secure satellite storage in strategic locations. Overall storage capacity would be increased from the current levels, and indoor storage would extend the life and ease of deployment of spares.
2. Secure Inventory Management System to manage stock incorporating prevailing order lead times. This would recognise the international demand and availability of critical network assets.

We forecast the cost of this will be £37.3 million.

Our proposed investment in warehousing and spares has been developed following a detailed review of the options. We presented three options to stakeholders at a workshop in March 2019: (i) single warehouse, (ii) two warehouses, and (iii) two warehouses with adjacent operations centre. We presented these options without and then with the associated cost.

There was a strong consensus of stakeholders in favour of the two warehouse option, both before and after the cost was revealed. Stakeholders also emphasised the importance of inventory controls and stock management systems to ensure back up equipment is maintained in good condition ready for immediate deployment.

Figure 3.7 Transportation of major infrastructure equipment

Our RIIO-T2 Plans: Resistance

The resistance component of resilience is about protecting the safe and secure operation of the network from natural hazards or malicious events.

Types of resistance

We define five types of resistance:

- System protection
- Control systems
- Physical threats
- Natural hazards
- Cyber threats

The first two types of resistance relate to the tools that are used to operate the transmission system and control the flow of electricity. We want to avoid too much or the wrong type of electricity damaging equipment or being a threat to people.

The latter three types of resistance relate to events that are outwith our control. These include malicious damage, theft, extreme weather or hacking. Again these events might damage equipment or threaten people.

System protection

System protection acts as a fuse box that immediately isolates parts of the transmission system that are faulty or damaged. The aim is to protect people and equipment, whilst maintaining security of supply.

On the high voltage transmission system, protective relays are deployed across the network to detect faults and send signals to circuit breakers to open. Relays operate at timescales of a few thousandths of a second. Modern relays are digital and so require a power source, input operational setting and communication channels to the switchgear.

In 2018, an industry protocol (STCP 27-01) was introduced which established arrangements for appropriate and accurate synchronised data to monitor asset and overall system performance. This data enables the cause and sequencing of system events to be established, and so improve system protection.

Like any asset with both hardware and software components, system protection requires both maintenance and risk-based replacement.

During RIIO-T2, we propose to replace 86 protection schemes.

This is largely to replace obsolete relay schemes, often where the software or operating systems are no longer supported by the original suppliers. These relay systems also do not have the capability to communicate with modern protection schemes and cannot provide the necessary data to comply with required monitoring standards such as STCP 27-01, mentioned above. This limits our ability to fully manage the transmission network and comply with expected UK grid standards.

We forecast the cost of these interventions to be £27 million.

Innovation: Digital substations

Ways for keeping the network resistant are closely linked to technology development. The fast paced technology changes driving digitisation and democratisation of the industry creates many opportunities for system and stakeholder benefit. System protection is one of those.

During RIIO-T1 we have applied innovation to this area by developing our use of the international standard IEC 61850 through business-as-usual funding. This standard looks to break substation design down to its component parts, identify the data requirements of each part and how they aggregate at a substation level. We have one of the first examples of an operational substation using multi-vendor IEC 61850 in the UK at our Spittal substation (below).

The initial benefits from this include less use of metallic cable and thus to reduced substation foot prints. As our understanding progresses then our substations will be safer and quicker to build as well as not being locked in to single suppliers.

Control systems

In order to monitor, process and act in real time to control the operation of the transmission network we use a supervisory control and data acquisition (SCADA) system. This is a package of automated hardware and software elements that gather data and issues commands.

As with most computing technology, the useful life of SCADA system components is short, typically less than 10 years. Technological improvements are rapid, so obsolescence occurs before the end of physical asset life. The speed of change also limits the opportunity for cost-effective repair and availability of spares.

In our Business Plan, we are proposing to invest £9 million to replace and upgrade 48 substation control systems. This investment includes third party testing of cyber security.

Physical threats

Physical security means ensuring the north of Scotland transmission network is resistant to physical interference, intended or accidental, and that the public is protected from coming into contact with electrical equipment.

Our objective is:

To deter Dissuade third parties from approaching or entering the transmission system by making the boundary appear too physically and technically difficult to overcome without likelihood of detection, failure or capture.

To detect Verify an intrusion that initiates the response by:

- Identifying suspicious behaviour at the perimeter boundary;
- Observing unauthorised intrusions across the boundary line;
- Raising an alarm to initiate further investigation; and
- Verifying all perimeter intrusion alerts with an appropriate timely response.

To delay Prevent the intruder from reaching the asset (including measures to minimise the consequences of an intrusion):

- Maximising the time taken for an intruder to breach the perimeter once detection has taken place
- Prevent an intruder from breaching the perimeter

We use a combination of measures to achieve this objective, but the starting point is identifying and understanding the risk to physical security.

We have an obligation to comply with the Electricity Safety, Quality and Continuity Regulation 2002 (ESQCR). The ESQCR requires us to continually undertake risk assessments on overhead lines and substations. Through these assessments we monitor the impact of changes to the electrical infrastructure and its local environment.

Based on our risk assessments, we are proposing in our Business Plan that we replace fencing at 27 substation sites, install CCTV and alarms at 35 network locations, and upgrade anti-climbing devices on around 1,000 transmission towers.

We forecast the cost of these actions on physical security would be £9 million.

The benefits of these interventions include ensuring that the safety of the public is maintained, enhanced protection against theft and contributing to the reliability of the network. Our rolling programme of works is designed for cost-effectiveness, and the timely deployment of new technologies.

In addition to these specific activities, we will continue to work with the national security services to ensure appropriate physical security for sites designated as critical national infrastructure.

Natural hazards

Environmental, climatic and landscape hazards pose a natural threat to the safe and secure operation of the transmission network. This includes extreme weather, landslides, wild fires and flooding.

While this has always been the case, the nature and potential impact of the threat is evolving and so must be kept under constant review. Many commentators argue that changes to our climate are causing new and increased risks.

For our Business Plan, we are proposing:

1 **Flood alleviation works at ten network locations**

2 **To maintain our programme of environmental risk assessment taking into account new forecasts and guidance.**

We forecast the cost of these activities to be £1.4 million.

You can read more about our plans to reduce our impact on the natural environment on pages 140-143

Cyber threats

The global profile, prevalence and sophistication of malicious cyberattacks continues to increase with a corresponding increase in the risk to the operation of the north of Scotland transmission network. This is compounded by the technological advances driving digitisation and democratisation as they see the expansion of connectivity and control.

As an Operator of Essential Services designated under the Network and Information Systems Regulations 2018, we must manage cyber security and cyber resilience in such a way as to minimise the threat. Managing this risk means regularly reviewing the design and operation of key systems, internal and third party testing, and employee and contractor training and awareness. We participate in national bodies that oversee the cyber security threat.

For our Business Plan, we have assumed that there will continue to be a significant cyber security threat and that the techniques for managing this threat will also continue to improve. We propose that in mid-2023 there is a review of requirements for the remainder of the RIIO-T2 period.

Wildfires spread across the north of Scotland in April and May 2019, impacting on the safe operation of the transmission system. This appears to be a growing issue and we are developing our understanding of these events, our planning to protect the network and our response. This includes participating in an international wildfire forum for electricity networks to share best practice from, for example, Australia, California and southern Europe.

Our RIIO-T2 Plans: Response and Recovery

The response and recovery component of resilience is to enable a fast and effective response to and recovery from disruptive events.

Business Continuity planning

We define Business Continuity as our capability to continue to operate the north of Scotland transmission network at acceptable predefined levels following a disruptive incident.

Business Continuity Planning is the overall management process that identifies potential threats and the impacts to operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, customers and necessary activities.

For the RIIO-T2 period, we have identified four activities necessary to maintain our capabilities for response and recovery:

- Black start
- Substation systems
- Communications
- Temporary masts

These activities have been identified through our comprehensive business continuity planning processes.

All parts of our organisation regularly review their business continuity arrangements using a four-step approach:

1. **Business Impact Analysis**
2. **Business Continuity Strategy**
3. **Business Continuity Action Planning**
4. **Exercising and improvement**

The resultant Business Continuity Plans are tested during simulation exercises that we conduct and that we participate in at a national level.

As a provider of critical national infrastructure, we also participate in national forums such as the Centre for the Protection of National Infrastructure. This ensures we can share learning and maintain best practice.

Black Start

Black Start is the process of restoring power to the transmission system after a full or partial shut down. These events are infrequent, but not uncommon as typically two or three such events occur globally each year.

As we describe on page 69, the decarbonisation of the energy system and associated closure of coal-fired power stations, has resulted in a review of the GB Black Start arrangements. In the north of Scotland, hydro and wind might provide significant energy enabled by system tools to provide inertia and voltage. There is sufficient capability to supply Scottish demand and provide surplus energy to assist further south.

It is our view that a GB-wide approach needs to be undertaken in planning for Black Start events. While we have a critical role to play in that planning and will continue to make an active contribution, it is the ESO that should co-ordinate the effort and take the lead in putting in place the arrangements to manage the GB transmission network in the event of a Black Start.

As a consequence, we have not proposed any significant investments for Black Start preparation in our Business Plan. Instead we propose to act at the direction of the ESO.

We propose the ESO should direct Black Start requirements for Scotland. **Do you support this approach?**

Substation systems

We design substations to be able to operate for a limited time without a mains supply of electricity using batteries or diesel generation. This is essential to maintain security of supply should there be an interruption in the local network or in a Black Start situation.

Our standard is for 72 hours of standalone operation, and all substations we have built during RIIO-T1 comply with this standard. A review of our older substations has identified 76 sites that do not meet the standard. In many cases the existing provision is inadequate for increased load of modern substation usage and operational technology networks (OTN).

In our Business Plan, we propose a programme of work to bring all substations up to standard. The most cost-effective solution is 72 hours of standby diesel generation capability and 12 hours of battery capacity. However, local constraints and network criticality mean the requirements at an individual site may vary.

We forecast the cost of these works to be £42 million.

Employee communications

Secure and reliable communication between our employees is essential for the safe operation of the network. For example, between the control centre and substations, between substations, and between field units activity across the north of Scotland. All methods of communication rely on electrical power and many of these systems are not resilient to a loss of power.

The substations we have built since 2010 are equipped with Voice-over-IP (VoIP) telephony. This supplements the public switched telephone network (PSTN) provided by OpenReach over copper circuits. The PSTN is resilient and designed to continue operating during power outages of several days. However, due to its age and technical obsolescence, we understand that the PSTN will be decommissioned by 2025 at the latest.

Our standard is for every substation to have two communications systems to ensure redundancy and to mitigate against the weaknesses of each. Our primary solution is VoIP, with a backup system using Personal Mobile Radio (PMR) where coverage allows. We propose to implement this two-part communications approach during the RIIO-T2 period and prior to the cessation of the PSTN.

We forecast the cost of the required 489 communications installations to be £1 million.

Temporary masts

During the Quoich landslide, customers on the Western Isles and Skye were off supply and reliant on diesel generation backup until a new transmission circuit could be constructed. This required design to be carried out in real time. A review of this event has highlighted that temporary towers would have enabled a faster response to secure customers supply via the grid and thus reduce the environmental impact from diesel generation. Cost savings would also have been significant, given the operational cost of the diesel power station.

In response to this, we propose to purchase 12 temporary towers at a cost of £1 million. The towers we have selected are in use by other UK transmission owners and therefore we will be able to pool resources and share their use in the event of a major system fault.

Safe and Secure Network Operation: Next steps

One of our four strategic themes is for safe and secure network operation. During the RIIO-T2 period, this means getting the best network performance through the effective use of data to manage risk. We have set a clear goal of ensuring 100% network reliability for homes and businesses.

We have described in this section our draft proposals to achieve safe and secure network operation using the four components of resilience:

Reliability of day-to-day network operation through cost-effective inspections and maintenance, risk-based asset intervention, engaged control room capabilities and optimising network availability;

Redundancy for assets being unavailable using installed system capability and back-up equipment;

Resistance to threats through strengthening our protection and control systems, and strengthening our physical and cyber security; and

Response and Recovery to disruptive events by business continuity preparations, including for a Black Start system recovery following full or partial shut down.

All four of these components are risk-based. We are continually assessing the network for risks that might interrupt safe and secure operation. We are planning and taking steps to manage and cost-effectively minimise those risks.

Our proposals are intended to reduce, as far as is cost-effective, the risk of network events and put in place cost-effective measures to address the consequences of any events that do occur.

Tell us what you think

We invite your views on the proposals we have set out here. We welcome comment on any aspect of our activities, and in particular the questions in this consultation that will inform our final Business Plan proposals for:

Our research indicates that security of supply is the priority of our stakeholder groups. **Is this an appropriate assumption for the duration of RIIO-T2 until 2026?**

Attendees at our March 2019 workshop[25] supported the undertaking of work in RIIO-T2 where it can be demonstrated to lead to more efficient outcomes in the future.

We propose the ESO should direct Black Start requirements for Scotland. **Do you support this approach?**

Find out more...

The Future Operation of our Network consultation
NOMs methodology
Network Access Policy
ESO System Performance Reports
Connections and Commercial Policy
Innovation Strategy
Whole System Thinking consultation
Reports from stakeholder engagement events

March 2019 stakeholder event on the future operation of the network

www.ssen-transmission.co.uk

[25]www.ssen-transmission.co.uk/riio-t2-plan/