15. I want you to protect the transmission system from cyber and external threats

What is this stakeholder priority about?

UK infrastructure is subject to many security threats and they are increasing in sophistication and persistence. These threats include terrorism, criminality and vulnerability in information technology (IT) and operational technology (OT) systems. Our network is part of Great Britain's Critical National Infrastructure (CNI) and appropriate protection from threats is therefore essential to underpin the safety, security and reliability of the nation's energy supply. The UK government sets the requirements for the appropriate levels of physical and cyber resilience that are to be achieved in the national interest.

What have stakeholders told us?

Stakeholders say that the way we manage security threats should be a priority. Since the publication of our July draft plan, they have challenged the significant increase in our proposed spending, particularly in relation to cyber resilience. Stakeholders seek assurance that we have considered alternative options including ways to avoid or reduce expenditure.

What will we deliver?

- Through a confidential Price Control Deliverable, our Cyber Resilience Plan (Operational Technology) will deliver a risk-based, strategic, long-term programme to replace key OT used for the safety and control of critical systems. We will replace compressor station control systems at high criticality sites. In tandem, we will strategically deploy a RIIO-1 innovation by enhancing our Supervisory Control and Data Acquisition (SCADA) system, in a nationwide programme to bring significant immediate cyber resilience benefits pending OT asset replacement (or decommissioning) e.g. at lower criticality sites.
- RIIO-2 costs for the following **OT assets** are included in this part of our plan (not in asset health): compressor station unit control and protection systems, fire and gas detection, anti-surge, boundary control, network control and instrumentation, metering, and, gas analysers.
- Our Business IT Security Plan will implement a suite of initiatives to improve cyber resilience across our enterprise IT environment and implement new capabilities in line with NIS guidelines.
- Our physical security plan includes delivery of new enhanced physical security upgrade programme (PSUP) solutions at sites identified by government and commencement of PSUP asset replacement across the portfolio.
- We will keep our programme under review and utilise uncertainty mechanisms to flex our delivery if circumstances change e.g. change in level of threat or criticality of sites.

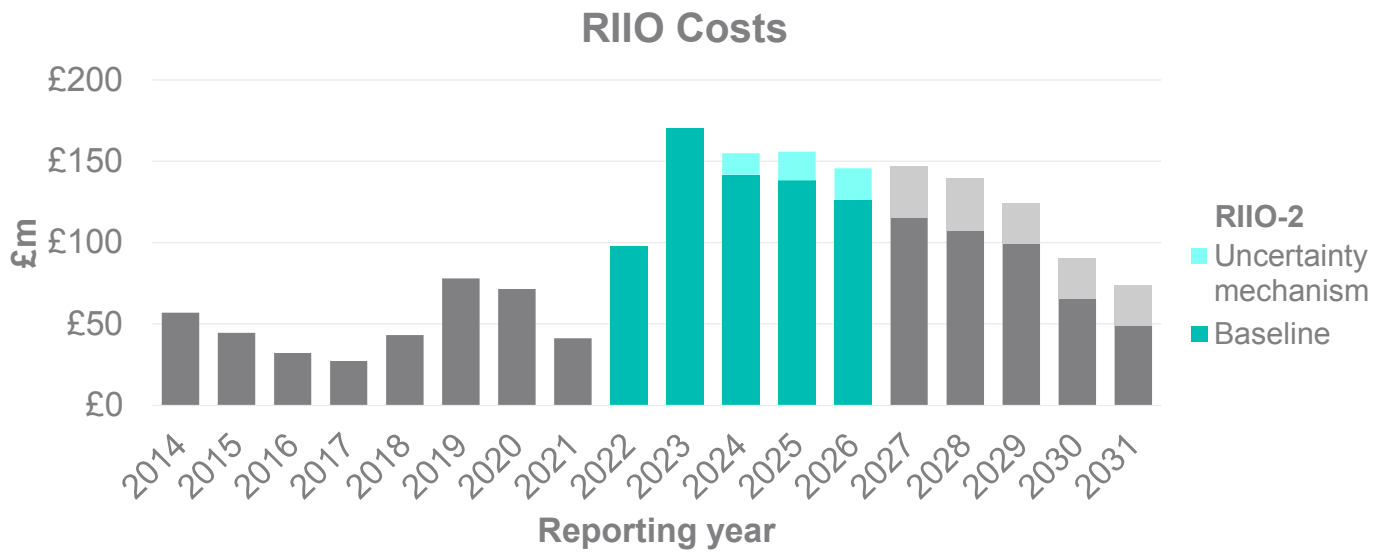
This is an area of significantly increasing expenditure, driven both by the growing level of threat and by new legislation steering the action that we must take to protect the network. Our plan proposes £118m per year (21.5% of our RIIO-2 total costs) is included within our baseline allowed revenue for known scope with agreed price control deliverables. We propose that uncertainty mechanisms allow adjustment to our scope and costs during RIIO-2 in response to changing circumstances.

What efficiencies have we included in our plan?

- Our physical security capex plan includes 15% cost reductions so far achieved in RIIO-1. In addition, we have pledged a cost reduction of £7.5m compared to our estimated capex costs at the time of our 2018 reopener submission.
- Our operational technology capex plan incorporates a series of initiatives to mitigate cost increases. These include: proportionate resilience enhancements based on site-based risk and criticality; the 'campaign' bundled contracting approach learning from RIIO-1; roll-out of the National Innovation Allowance (NIA) (SCADA) innovation initiative into RIIO-2 business as usual (BAU). We have quantified the latter as providing a **consumer value proposition** (CVP) consumer benefit of £9.2m.

I want you to protect the transmission system from cyber and external threats

Figure 15.01 RIIO-1 and RIIO-2 spend profile 'I want you to protect the transmission system from cyber and external threats'



Note: In addition to the expenditure portrayed in the graph we are spending approximately £131m in the RIIO-1 period on asset health interventions on operational technology assets. This is not shown here to avoid double counting with chapter 14.

1. What is this stakeholder priority about?

This priority is about protecting our network from threats that could otherwise disrupt continuity of GB energy supply, with serious consequences for society. We rely on industrial control systems to control and protect processes ranging from valves to compressor machinery. Loss or compromise of these systems could pose a serious safety risk – for example, failure to contain gas could result in fire or explosion with a knock-on impact on adjacent assets and facilities.

Our key activities and costs covered in this chapter include:

- strategic capability to monitor, detect, respond to (and recover from) malicious threats
- enhancing cyber security resilience
- delivery of the Physical Security Upgrade Programme (PSUP)
- policing at gas facilities as required by the Counter-Terrorism Act 2008
- response to actual or new threats that emerge during RIIO-2.

We have included our asset replacement justification and costs for operational technology and enhanced physical security in this chapter rather than in chapter 14. We have done this because protection from threats is the primary cost driver and we expect specific RIIO-2 outputs (PCDs) to be attached to this work, separate to the network asset risk metrics (NARMs) asset health outputs.

Evolving threat

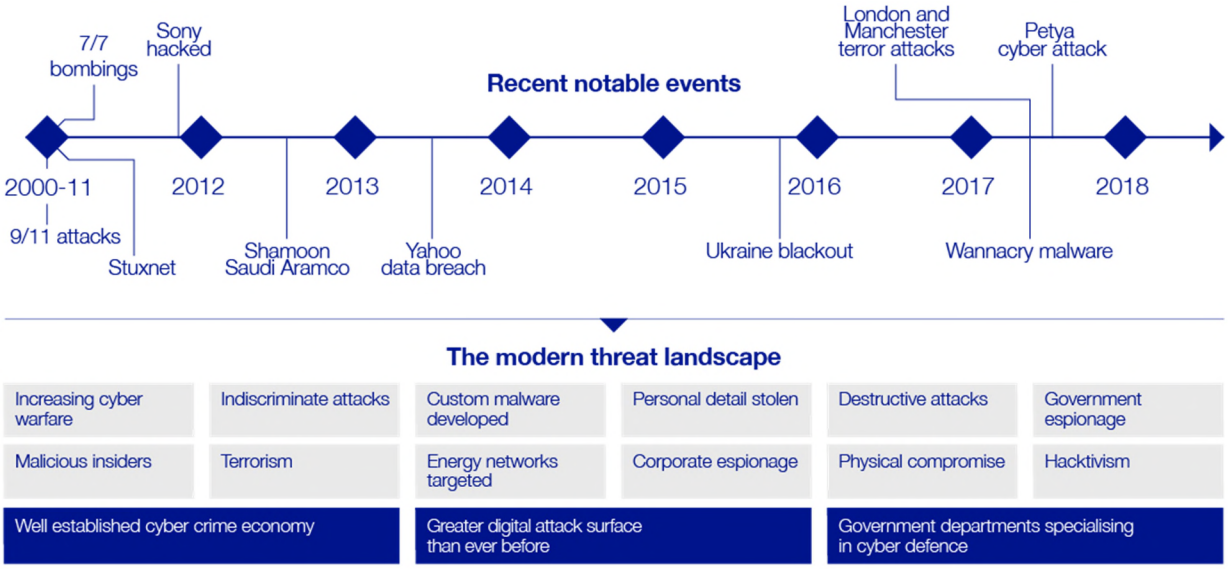
The network was designed with sound engineering and safety considerations at the forefront, rather than with a mindset of protection from malicious threats. As threats emerged, we mitigated them through a programme of physical security upgrades at our sites.

Cyber security threat is the risk to computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide. The danger to energy systems is increasing due to the rapid digitisation of energy assets and the convergence of information technology (IT) systems (used for data-centric computing) with operational technology (OT) systems (used to control industrial processes and equipment).

The cyber threat landscape is evolving rapidly, and security experts think that, for every major cyber-attack in the public domain, four more major attacks are not reported. The energy sector has experienced a significant increase in the volume of reported attacks since the Iranian Natanz nuclear facility was attacked by 'Stuxnet' malware in 2010. Since then, Ukrainian energy companies have experienced attacks in 2015, 2016 and 2017.

I want you to protect the transmission system from cyber and external threats

Figure 15.02 the evolving threat landscape



Security services process

Elements of our network are classified as critical national infrastructure (CNI). This means loss or compromise would have a major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.

The UK government, in conjunction with the Centre for the Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC), set requirements for the appropriate levels of physical and cyber resilience to be achieved in the national interest. We work closely with these agencies to identify the most efficient way to meet these requirements, which call for significant operating and capital expenditure.

Some of our assets are co-located with those of other energy companies and it is important that we work closely and share best practice with these and other operators of essential services to achieve joined-up protection across the energy industry. When considering the impact of any loss of gas transmission supply, the consequential impact on both the gas and electricity markets must be considered; gas is our largest primary fuel source for electricity generation, typically accounting for around 40% of electricity production.

Mitigating cyber threats – the NIS Regulations, 2018

Heightened awareness of cyber threats is underlined in the UK Government's National Cyber Security Strategy[54] and evidenced by the launch in October 2016 of the NCSC[55]. The NCSC provides a single point of contact for expertise and guidance in the prevention of, and response to, cyber security incidents.

The requirements for a coordinated response across network companies have been established through the Security of Network and Information Systems (NIS) Regulations 2018[56]. The NIS Regulations aim to minimise the risk of cyber-attack and the resulting impact on UK CNI, the economy and consumers. This is in keeping with the NIS Directive[57] aiming to co-ordinate and raise overall levels of cyber security across the European Union (EU).

The NIS Regulations apply to a defined list of operators of essential services (OES), each with a relevant 'competent authority' (CA) supporting and monitoring compliance. We are a designated OES, and within the energy sector, the CA role is jointly held by the Department for Business, Energy and Industrial Strategy (BEIS) and Ofgem.

Mitigating physical threats – the Physical Security Upgrade Programme

The Secretary of State initiated the Physical Security Upgrade Programme (PSUP) and it is now governed by BEIS. It is a national programme to enhance physical security at CNI sites. Requirements arising from this programme have been a key driver of our activity both before and during the current regulatory period. This will continue through RIIO-2. We follow standards and guidelines for good practices endorsed by BEIS and CPNI[58].

2. Our activities and current performance

Track record: Cyber resilience

We have adopted **new management systems** underpinned by a security standard in keeping with NIST[59] good practices. The approach focuses on five key principles: identify, protect, detect, respond and recover.

[54] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
[55] https://www.ncsc.gov.uk/
[56] http://www.legislation.gov.uk/uksi/2018/506/pdfs/uksi_20180506_en.pdf
[57] https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[58] https://www.cpni.gov.uk/protecting-my-asset
[59] https://www.nist.gov/cyberframework

I want you to protect the transmission system from cyber and external threats

We have focussed on **building the capability of our people**. We are consciously competing to bring cyber talent in-house. All our personnel who work with operational technology undertake mandatory cyber security training.
Working with the security services and external specialists, we have carried out **cyber risk assessments** and gap analysis, using best practices including NIST, IEC62443[60], HSE OG86[61] and NIS Regulations. We have completed our NIS self-assessment and improvement plans acting upon feedback from the NIS Competent Authority.

We are currently delivering **targeted risk mitigation projects** during RIIO-1. These have been supported by Ofgem through the enhanced security reopener[62] process:

- **New data centres** (a joint project with NGGT and NGESO). The establishment of new high resilience centres to host the data that underpins our CNI services such as the operation of the GNCC.
- **Cyber security programmes 1 & 2** (joint with NGGT, NGESO and NGET). A suite of interrelated and foundational cyber resilience projects. These create the building blocks for enhanced capabilities such as the formation of our 24/7 cyber security operations centre, monitoring national and worldwide threat and event intelligence.
- **Gas specific cyber investments** (NGGT only). Includes projects to improve Intrusion Detection Systems and to define a strategic asset replacement approach to the impending challenge of how best to replace our ageing industrial control systems. This strategy is to be deployed as part of our cyber resilience plan in the RIIO-2 period.

We are delivering two key **security innovation projects**: Opensource SCADA (scheme NGGT0114) and Secure AGI Intrusion Detection System (scheme NGGT0138). These projects[63] are piloting new lower cost methods to raise cyber resilience of our Supervisory Control and Data Acquisition (SCADA) systems.

We have **maximised the useful lives** of our ageing operational technology assets in the RIIO-1 period, harvesting grey spares to extend service from equipment which is obsolete and for which original equipment manufacturer support is no longer available. Where we have replaced OT assets, our "campaign" approach of bundling work has brought **30% cost efficiencies**. The unit costs behind our RIIO-2 plan include this cost efficiency.

Track record: Physical security
We are installing **enhanced PSUP measures at [redacted] gas sites** in compliance with BEIS requirements. The total number of sites with enhanced protection is increasing from [redacted] at the start, to [redacted] at the end of RIIO-1.

We have proactively challenged and reviewed PSUP requirements using BEIS and CPNI principles and our assessment of system risk and criticality. Where appropriate this has led to certain sites being added or dropped by BEIS. The sites dropped have **avoided £23.8m expenditure** on behalf of consumers.

We have instigated changes in our contracting and delivery approach **reducing capital cost by 15%** compared to what we could achieve at the start of the RIIO-1 period. We currently forecast completing our in-flight RIIO-1 work in line with Ofgem's 2015 reopener determination of efficient costs.

We **comply with the Counter-Terrorism Act 2008**, sections 85 to 90, which governs the arrangements for policing at gas facilities. The security requirements and associated costs are set by the government and are outside our control. Because of this, our policing costs are recovered via a cost pass-through uncertainty mechanism.

3. What have stakeholders told us?

Table 15.03 stakeholder engagement summary

Stakeholder segments engaged	Key stakeholders: NIS Competent Authority, Ofgem, BEIS, HSE. Wider stakeholders: Customers, GDNs, consumers.
Objectives	To inform our priorities for RIIO-2, understand government requirements including from new NIS regulations, inform our risk assessment and develop our RIIO-2 scope of work.
Channel / method	Confidential bilateral meetings with NIS Competent Authority, Ofgem, BEIS, HSE. Wider stakeholders: Shaping the Future events and consumer research.
Key messages	Cyber and physical threats should be high priority. *"Agree 100% with the critical need to protect the transmission system against cyber and external threats…"* – [redacted], **customer (entry)** *"Cyber security is very important to us"* – [redacted], **customer (entry)** *"Outputs need to include cyber security and this needs to be funded"* – [redacted], **supply chain**
SUG and Challenge Group feedback	The SUG have provided helpful feedback on calling out efficiencies and providing further detail on options considered which we have included in this chapter. We have also listed the assets related to cyber to allay the concerns of double counting between asset health.

[60] https://www.isa.org/intech/201810standards/
[61] http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf
[62] https://www.ofgem.gov.uk/publications-and-updates/informal-consultation-riio-1-price-control-reopeners-may-2018
[63] https://www.nationalgridgas.com/document/127991/download

I want you to protect the transmission system from cyber and external threats

In autumn 2018, the independent stakeholder user group looked at how we are developing the physical and cyber security elements of our business plan. The group noted that the measures we take are mandated by government and the security services. To protect national security, the government restricts what we can say publicly about our current level of resilience and the specific measures we will take in the future to reduce vulnerability. For these reasons, it is not appropriate for us to engage the group or wider stakeholders on the detail of our plan and the substance of it can't be influenced by customer or consumer preferences. Our approach is therefore to build the confidential detail of our plan with government agencies, while providing transparency about the process that we follow. In its role as economic regulator, Ofgem protects consumers by scrutinising our costs to ensure that only efficiently incurred costs are allowed.

The key stakeholders whose requirements have shaped our plan for dealing with external threats are the government (BEIS), its security specialists (CPNI and NCSC), Ofgem (in its role as Competent Authority for the NIS Regulations) and the Health and Safety Executive (HSE). We collaborate on best practices across the National Grid group where we own gas and electricity transmission and distribution networks across the north eastern United States. Working closely with our US colleagues helps us to gain more powerful insights in our 24/7 analysis and management of global security information and event data. Where our assets are co-located with other parties, such as gas distribution networks, we work with them to ensure an efficient, joined-up approach.

In its 2018/19 business plan[64], the HSE reflects an increased focus on the emerging risks of cyber security and it has recently updated its operational guidance[65] on cyber security for industrial automation and control systems. This is specifically relevant to us because we operate these systems for major hazard risk reduction and continuity of gas supplies, and our planned RIIO-2 cyber resilience activities are in line with latest HSE guidance:

"Operators subject to both health and safety and NIS legislation should carry out risk assessment(s) that cover both major accident and loss of essential services consequences and then use the highest risk to determine the countermeasures to be applied."

4. Our proposals for RIIO-2 and how they will benefit consumers

We have set out further details of the business plan proposals for each area in the supporting annexes A15.01-A15.10. Annex A15.13 sets out our stakeholder engagement summary. In keeping with Ofgem business plan guidance, our cyber resilience proposals are set out in two sections: (i) a business IT security plan focused primarily on cyber security for business systems, and (ii) a cyber resilience plan focused primarily on production systems operational technology. Separate EJPs are provided for our physical security proposals. Collectively, these annexes explain in greater depth the drivers for the activity, the options considered (including 'do nothing'), and the analysis of costs and benefits. We have used further templates to set out our proposed outputs in the form of price control deliverables and, where appropriate, our proposals for the design of uncertainty mechanisms

Table 15.04 our proposals

What our stakeholders have told us	Commitment	Output type	Consumer benefit
Protect the system from increasing cyber threats in line with government and HSE requirements	Comply with obligations as an operator of essential services (OES) pursuant to the NIS regulations 2018.	Commitment	We improve the safety and resilience of the network to ride through and recover from malicious events that threaten to disrupt continuity of GB energy supplies. Our plan delivers security enhancements that the government has identified as being in the national interest. This reduces the risk of actual events that could have severe societal consequences for GB consumers. **Applying a security innovation is a consumer value proposition valued at £9.2m (for more information on CVP2 please see annex A10.05).** Proportionate deployment of the enhanced SCADA solution leverages maximum future consumer benefit from a project already
	Implement a prioritised programme of replacement and security hardening of our operational technology (e.g. industrial control systems, telemetry, metering, gas analysers and boundary control) for our compressor, terminal and above ground installation sites, including; • Replace [redacted] station control systems across [redacted] sites, making interventions on [redacted] remote operable valves. • Deploy RIIO-1 innovation learning to enhance our SCADA system, as a faster and lower cost cyber resilience mitigation in tandem with the prioritised asset replacements.	Confidential PCD (£417.4m) We propose ex-ante funding plus totex incentive mechanism for well-defined scope (rather than use it or lose It) regulatory treatment.	

[64] http://www.hse.gov.uk/aboutus/strategiesandplans/businessplans/plan1819.pdf

[65] http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

I want you to protect the transmission system from cyber and external threats

	Our business IT security plan will: • implement a suite of initiatives to improve cyber resilience across our enterprise IT environment and implement new capabilities in line with NIS guidelines. • deliver 5 cyber resilience projects specific to the CNI services operated by the SO, including enhanced vulnerability management to enable better prevention and detection of cyber-attacks.	Confidential PCD (£43.3m). We propose ex-ante funding plus totex incentive mechanism for well-defined scope.	funded in RIIO-1 by a Network Innovation Allowance.
Use a risk-based approach to enhance cyber resilience	We will use site specific risk-based criticality and security levels to determine a proportionate response. We will optimise our programme having regard to wider considerations of network capability, compressor fleet strategy, and possible future decommissioning of units/sites e.g. in response to emissions legislation. We will always consider least functionality options such as removal of remote control functionality.	Commitment	This approach ensures we do not 'gold plate' our solutions. For example, we avoid investing in measures that are excessively costly or complex compared to the level of risk reduction obtained, or where there is a high chance of regret (e.g. if the site in question might be decommissioned within the next ten years).
Adjust priorities, scope and work delivery inside RIIO-2 period in light of changing threat landscape	We will actively monitor potential changes in (i) intelligence on threats, (ii) site criticality security levels. We will discuss such changes with the relevant competent authorities and, where appropriate, seek changes to our programme and price control allowances through two uncertainty mechanisms.	Uncertainty mechanism Cyber resilience. ***Trigger**: Proposing 2 reopener windows (start of RIIO-2 and mid period).* Physical security ***Trigger**: Proposing 2 reopener windows (at mid period and end of RIIO-2).*	Including uncertainty mechanisms involving the security agencies to monitor and adjust our delivery during RIIO-2 will ensure our effort and expenditure continues to be directed at maximising consumer benefit even when circumstances change. The use of reopeners avoids the possibility of windfall gains/losses associated with us being over/under-funded for the appropriate level of work.
Deliver physical security upgrades at sites required by BEIS	We will deliver new physical security upgrade solutions [redacted] Begin a prioritised programme of replacement of first-generation security assets including replacing 34-year-old fence sections at [redacted] important sites. Maintain PSUP solutions in line with BEIS guidance and CPNI high level security principles	Confidential PCD (£131.9m)	Consumers are assured that relevant sites are secured to the level deemed appropriate by government. Monitoring and audit processes ensure compliance.
Facilitate policing at gas sites	Comply with our legislative requirements (the Counter-Terrorism Act 2008).	Uncertainty mechanism *Pass-through cost*	Consumers benefit from the enhanced security deemed appropriate by government. Consumers pay no more or less than the actual cost incurred.

5. How will we deliver?

To manage our cyber and physical security programmes, we will regularly monitor potential interactions with network developments. For example, if assets become more or less important as we review network capability or as customer activity changes (for example, disconnections) we will re-prioritise our work.

Through our portfolio planning process, we have confirmed that the proposed cyber resilience operational technology scope is deliverable as part of our longer-term programme that will continue through RIIO-3. The necessity to balance system access outages with maintaining secure supplies limits how many sites we can work on simultaneously. Our delivery programme is part of an enduring, sustainable asset replacement cycle that fits with the economic optimal average asset life of 15 years.

The programme of work will be subject to competitive procurement events to ensure we achieve value for money. With upfront funding for a longer-term, larger portfolio of work, this will provide confidence to the supply chain and in turn drive efficient delivery. We plan to grow our in-house cyber delivery capability by recruiting twelve more people so that we achieve the right balance between internal expertise and outsourcing.

Innovation in RIIO-2

Our business plan proposes strategic nationwide deployment of an enhancement to our SCADA system into business as usual during the RIIO-2 period to bring

significant immediate cyber resilience benefits while avoiding or deferring more costly full asset replacement decisions. We will continue to focus on applying innovation to drive efficiency in delivery of our work. We will also seek to improve how we can deliver and implement mitigations against cyber and physical threats, ensuring we investigate the potential of new technology such as artificial intelligence and machine learning for example.

Table 15.05 RIIO-2 innovation

Theme	Commentary
Fit for the future	Modernising our systems to prevent cyber threats, ensuring they are secure now and into the future.
Ready for decarbonisation	Utilising AI and ML improves threat detection and prevention. Smart 'self-monitoring' networks that provide notifications of threats.
Decarbonised energy system	Modernise our systems for a future decarbonised energy network, protecting it from cyber threats.

6. Risk and uncertainty

The threat landscape has changed significantly during RIIO-1, particularly in relation to cyber security. Our close work with the security agencies has helped us to have a good understanding of the work we need to deliver in RIIO-2 to meet current government requirements. We consider this known work to be 'no regret'. It constitutes around 80% of the scope in this part of our RIIO-2 plan. We propose that in relation to the known work, where the outputs and costs are sufficiently clear, base revenue funding should be included in our RIIO-2 price control allowance for the full scope of this planned work. We should be strongly incentivised to deliver this work efficiently in the interests of consumers.

We are working with the NIS Competent Authority to confirm our RIIO-2 scope informed by our NIS self-assessment and NIS improvement plans.
Within their Sector Specific Methodology Decision (SSMD), Ofgem stated that there would be two reopeners for works included within the cyber resilience plan and one reopener for works included within the business IT security plan. Whilst the threats we face on our IT systems is more advanced, it is the more traditional route of attack that provide a gateway to our OT network. The threats we face, no matter how advanced, still constantly evolve and provide new challenges in how we best protect our network. For this reason, we propose that two reopeners (start and mid-period) are allowed for both our cyber resilience plan and business IT security plan.

It should be noted that there are important interactions across the whole of our business plan. For example, elements of our asset resilience and cyber resilience programmes of work will also bring important safety and reliability benefits. The scope of work we have included in this chapter is consistent with the categories of work in the RIIO-1 enhanced security costs and/or it goes far beyond previous business as usual activity. We expect these areas of work to have their own RIIO-2 outputs, monitoring and reporting regimes.

7. Our proposed costs for RIIO-2

Our proposed total expenditure to meet this stakeholder priority is summarised in the tables below. The tables give references to the annexes which contain further details of options considered and engineering cost justification. References are also provided to the relevant tabs in the business plan data template (BPDT) where detailed historic and forecast cost information can be found. Subtotals for baseline and uncertainty mechanism (UM) costs are given.

Table 15.06 cyber resilience plan (operational technology) costs

Activity spend (£m in 18/19 prices) Annex ref & BPDT ref	2022	2023	2024	2025	2026	Total RIIO-2	Annual RIIO-2	Annual RIIO-1	Total RIIO-2 baseline	Total RIIO-2 UM
TO Cyber Security OT (capex & opex) Annex A15.07 BPDT 3.06(a)	44.1	95.3	101.8	106.0	102.3	449.5	89.9	0.0	411.4	38.1
People & resources (opex)* Annex A20.15 BPDT 2.02	1.2	1.2	1.2	1.2	1.2	5.9	1.2	1.7	5.9	0.0
Total (totex controllable costs)	**45.3**	**96.5**	**103.0**	**107.2**	**103.5**	**455.4**	**91.1**	**1.7**	**417.4**	**38.1**

Please note we have provided costs to one decimal place and hence some columns may not equal to the totals. Pension costs are based on proportion of total TOTEX.

Instead of 'Use It or Lose It' treatment described in the SSMD, we propose ex-ante funding plus totex incentive mechanism for the baseline element of our cyber resilience plan. This is because our scope is well defined, with clear, ring-fenced, outputs that can be recorded in confidential price control deliverables, and where a strong performance incentive on us will drive benefits for consumers. The uncertain costs we have given are for indication only. We would use the RIIO-2 reopener windows to bring forward final proposals for the relevant scope and costs as and when those details are firmed up.

I want you to protect the transmission system from cyber and external threats

Our transmission owner OT baseline scope includes:

- £215m totex for our prioritised programme of replacement of control and safety systems at our highest used compressor stations and terminals with partial cyber upgrades to the remaining compressor stations. Our plan is extensively built up from a unit cost times volume approach, with rates based upon evidence from outturn cost of previous/in-flight projects which have been competitively tendered. This programme will continue into RIIO-3 and beyond.
- £141m totex for a combination of refurbishment and replacement of our Gas Quality, Telemetry and Metering (GQMT) assets located at our Above Ground Installations. There is no double counting of costs with the rest of our asset health plan.
- £55m totex for specific projects to implement enhanced cyber resilience capability at the IT/OT interface. One of these projects is widescale deployment of our RIIO-1 innovation to our SCADA system, as a quicker measure to mitigate cyber risks pending replacement of underlying OT assets. We have provided an indication of future costs for our less-well defined IT/OT projects under the banner "costs relating to proposed uncertainty mechanisms". We would use the RIIO-2 reopener windows to bring forward final proposals for the relevant scope and costs as and when those details are firmed up.
- £6m opex including for an additional 12 personnel to implement new cyber processes; updating antivirus software, performing software sweeps, first and second line fault response, incident handling, training and emergency preparedness exercises.

In arriving at our proposed cyber resilience plan, we have considered and costed a wide range of options including:

- Scenarios explored in optioneering: do nothing, upgrade existing assets, partial system enhancement, repair or refurbish, full system replacement, acceleration/deferral of plan.
- Network resilience and safety: we have considered the network resilience impact and safety consequences posed by both equipment failure and cyber-attack.
- Risk-based security levels: we have compared the cost of a common resilience target at all sites versus different levels of cyber hardening proportionate to the risk and criticality of the individual sites in question.
- Future of gas and compressor fleet strategy: We have considered the prioritisation and scope of work at individual sites to mitigate the risk of stranded investment at sites for which the long-term future need may be uncertain. We ensure our proposed spend is focussed on sites most needed to meet the network capability required by gas customers. We have ensured this plan 'fits' with our compressor strategy and that it is deliverable with regard to network outage constraints.
- Least functionality options: we have considered situations where remote operability functionality is necessary versus where alternative manual operating philosophy may be possible thereby avoiding the need for cyber hardening of these assets.
- We have compared our approach with our business in the US and with other energy network operators of essential services in Europe (members of the European Network for Cyber Security[66]). This provided insight and independent assurance that we are implementing best practices.

Table 15.07 business IT security plan costs

Activity spend (£m in 18/19 prices) Annex ref & BPDT ref	2022	2023	2024	2025	2026	Total RIIO-2	Annual RIIO-2	Annual RIIO-1	Total RIIO-2 baseline	Total RIIO-2 UM
TO Cyber Security IT (capex & opex) Annex A15.02 BPDT 3.06(b)	4.8	5.4	4.8	5.3	5.8	26.1	5.2	1.4	19.5	6.7
SO Cyber Security IT (capex & opex) Annex A15.02 BPDT 3.09(b)	9.5	5.2	4.8	4.9	5.0	29.3	5.9	7.7	23.8	5.5
Total (totex controllable costs)	**14.3**	**10.6**	**9.6**	**10.2**	**10.8**	**55.5**	**11.1**	**9.1**	**43.3**	**12.2**

In line with the regulatory treatment described in Ofgem's SSMD, we propose ex-ante funding plus Totex Incentive Mechanism for the baseline element of our NGGT Business IT Security Plan. The uncertain costs we have given are for indication only. We would use the RIIO-2 reopener windows to bring forward final proposals for the relevant scope and costs as and when those details are firmed up.

Key features of our NGGT Business IT Security Plan include:

- The allocation to Gas Transmission and Gas System Operation of corporate security function costs for a suite of initiatives to enhance the cyber resilience of National Grid's Enterprise IT environment. We benefit from the economy of scale of sharing common costs with other National Grid entities including NGET and NGESO.
- The initiatives are arranged into 11 categories and mapped to bring specific improvements in our cyber posture as monitored through the Cyber Assessment Framework. Confidential PCDs record the agreed outputs and their targeted improvements in CAF score.
- Gas System Operator (GSO) share of 5 cyber resilience projects that are specific to the CNI services operated by the GSO and Electricity System Operator (ESO) entities.
- In other respects, the GSO CNI systems are already hardened and segregated from business systems, so the RIIO-2 expenditure for the ongoing maintenance,

[66] https://encs.eu/

I want you to protect the transmission system from cyber and external threats

development or replacement of these systems is embedded elsewhere in our plan as business as usual activity and reported according to existing BPDT conventions.

- As well as project specific capex and opex, an allocated share of the indirect costs of resources in the National Grid security shared function is included here. The activities covered include 24/7 cyber security monitoring, training and recruitment.
- Compared to our July draft plan we have removed data centre capex because this project is scheduled to be completed in RIIO-1. We have checked that there is no 'double counting' between this chapter and costs elsewhere in our plan.

Table 15.08 physical security costs

Activity spend (£m in 18/19 prices) Annex reference & BPDT reference	2022	2023	2024	2025	2026	Total RIIO-2	Annual RIIO-2	Annual RIIO-1
Major Projects (baseline capex) Annex A15.09 BPDT 3.05	15.4	29.4	3.7	0.0	0.0	48.5	9.7	20.8
Asset Health (baseline capex) Annex A15.08 BPDT 3.05	0.6	12.1	15.4	14.3	6.9	49.2	9.8	0.0
Maintenance (baseline opex) Annex A15.10 BPDT 2.05	6.2	6.2	7.0	7.3	7.3	34.1	6.8	4.5
Total (totex controllable costs)	**22.3**	**47.7**	**26.1**	**21.6**	**14.2**	**131.9**	**26.4**	**25.3**
Policing (pass through) BPDT 2.02	16.0	16.0	16.3	16.7	17.1	82.2	16.4	13.3

In line with the regulatory treatment described in Ofgem's SSMD, we propose ex-ante funding plus Totex Incentive Mechanism for the baseline element of our physical security plan. Key features of our physical security plan include:

- Major projects spend is for delivery of new PSUP solutions at [redacted] sites during the first three years of RIIO-2. This is a reduction in volume compared to the RIIO-1 period in which we are delivering new PSUP solutions at [redacted] sites. Our cost estimates are informed by outturn costs of the [redacted] sites delivered or to be completed during RIIO-1. This data inherently reflects the outcome of native competition. Furthermore, we have embedded an efficiency ambition so that the allowance we are requesting for RIIO-2 is £7.5m lower than our equivalent estimate at the time of the May 2018 reopener.
- Asset health spend commences at the start of RIIO-2 as we begin a nationwide programme of planned replacement of first-generation security assets, including replacing 34-year-old perimeter security sections at [redacted] important sites. The programme will extend into RIIO-3. Most assets being replaced have useful lives of 7 to 15 years. We have separated this PSUP asset replacement spend from the generality of our asset health costs so that all PSUP capex costs are ring-fenced with their own Price Control Deliverable.
- Maintenance spend includes 24/7 alarm monitoring, routine maintenance and fault repairs. Costs are increasing because the number of sites being managed is more than doubling between RIIO-1 and RIIO-2. Efficiencies are obtained through the economy of scale of sharing an alarm receiving centre with Electricity Transmission and Cadent. We are pursuing further efficiency by in-sourcing first and second line support for fault resolution.
- Policing costs are dictated by the Counter Terrorism Act and treated as a cost pass-through. Our RIIO-2 figures have been updated since July 2019 to reflect a new estimate received from the Ministry of Defence.

Table 15.09 cost assessment criteria

Cost realised from RIIO-1 actuals	Cost forecast based on competitive process	External benchmark	NARM or volume-driven PCD
Yes – RIIO-1 actual costs for physical security and OT have been used to arrive at RIIO-2 forecasts	Yes – most RIIO-2 scope will be subject to native competition	Yes – physical security costs in line with Ofgem 2018 reopener benchmark	Yes - defined PCDs

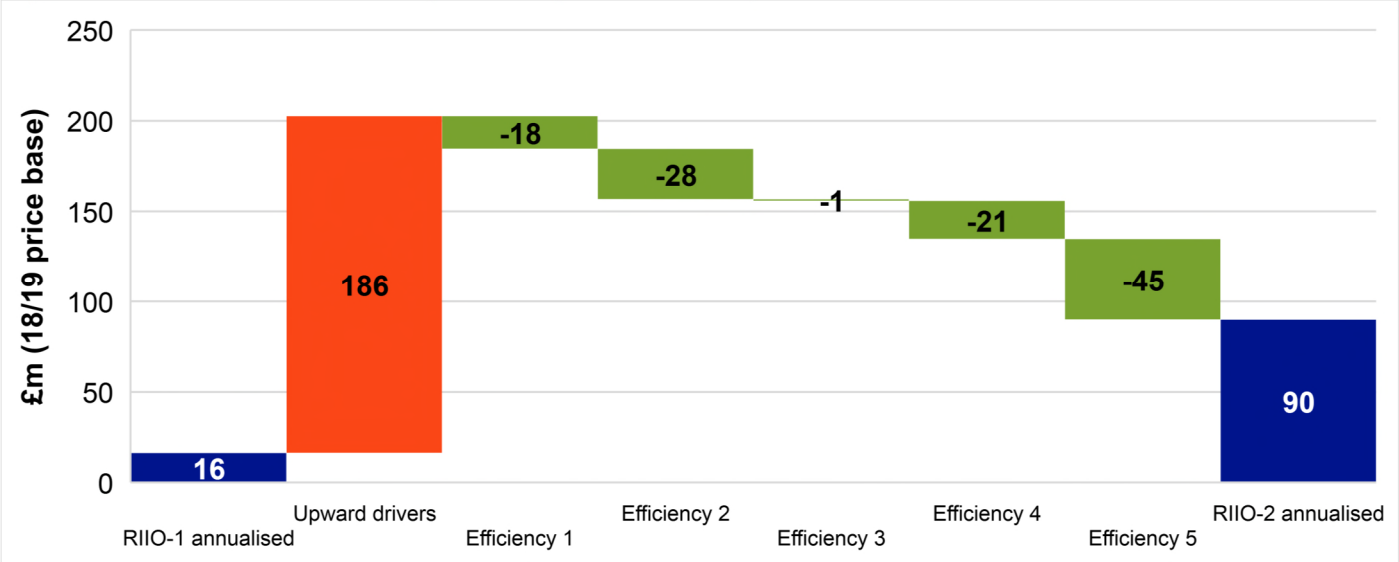
I want you to protect the transmission system from cyber and external threats

Table 15.10 summary of protect the transmission system from cyber and external threats costs by activity

Activity spend (£m in 18/19 prices)	2022	2023	2024	2025	2026	Total RIIO-2	Annual RIIO-2	Annual RIIO-1	Total RIIO-2 baseline	Total RIIO-2 UM
Cyber resilience plan (OT) (note 1)	45.3	96.5	103.0	107.2	103.5	455.4	91.1	1.7	417.4	38.1
Business IT security plan	14.3	10.6	9.6	10.2	10.8	55.5	11.1	9.1	43.3	12.2
Physical security	22.3	47.7	26.1	21.6	14.2	131.9	26.4	25.3	131.9	0.0
Sub-total – controllable costs	81.8	154.7	138.7	139.1	128.5	642.8	128.6	36.1	592.5	50.3
Policing – non-controllable	16.0	16.0	16.3	16.7	17.1	82.2	16.4	13.3	0.0	82.2
Total spend	**97.8**	**170.7**	**155.0**	**155.8**	**145.7**	**725.0**	**145.0**	**49.4**	**592.5**	**132.5**

Note 1: The RIIO-1 to RIIO-2 OT expenditure trend seen in this table is not a like-for-like comparison. This is because the RIIO-1 figure does not include some £16m p.a. of mostly asset health investment on our OT assets, which is reported separately in chapter 14 and must not be double counted. We have provided further insight regarding the like-for-like movements through the OT cost drivers and efficiencies waterfall that follows.

Figure 15.11 RIIO-1 to RIIO-2 Comparison: cyber resilience plan – OT cost drivers and efficiencies waterfall



Step	Explanation of cost drivers and efficiencies
RIIO-1 annualised	Forecast average annual spend over the 8 year RIIO-1 period for gas operational technology assets.
Upward drivers	Replace all control systems inside RIIO-T2, to achieve Security Level 3 at all sites, and to continue full remote operation functionality. In addition to very high costs, this is not deliverable due to network access constraints.
Efficiency 1	Phase the workload into a stable predictable programme with forward visibility to the supply chain. Avoiding peaks and troughs allows efficient planning of resources and avoids less preferred/more expensive contractors.
Efficiency 2	Deploy "campaign" approach learning from RIIO-1. i.e. bundling work drives efficiency from supply chain compared to standalone tenders. This reduces unit cost by 24-36% compared to actual costs incurred on non-bundled RIIO-T1 projects.
Efficiency 3	Apply proportionate security levels (SL1 to SL3) depending on the risk and criticality of sites, in line with CNI ratings for physical security at sites. Lower risk sites do not warrant same level of investment resulting in cost savings.
Efficiency 4	Review which sites are essential to meet customer requirements for network capability e.g. having regard to forecast compressor running hours. Prioritise highest criticality sites for full control system replacement inside RIIO-2. Defer work at remaining sites into RIIO-3 period enabling a subsequent retest of need (in light of site utilisation) in mid-2020's before commitment to spend. Deploy SCADA innovation on lower criticality sites as a lower cost intervention, accepting this doesn't mitigate asset health & obsolescence risks.
Efficiency 5	Delivery of ITOT capability in a controlled and logical manner, spanning RIIO-2 and RIIO-3. Post portfolio wide review of GQMT, security ratings and asset obsolescence, defer into RIIO-3.
RIIO-2 annualised	RIIO-2 period proposed average annual spend (across 5 years).